CycleNetwork: A Universal, Secure and Verifiable Chain Abstraction Architecture

TEAM@CYCLENETWORK.IO - JULY 2024, V1.0

This paper presents Cycle Network, which employs Verifiable State Aggregation (VSA) to achieve chain abstraction. VSA aims to improve security, minimize latency, and reduce costs in decentralized applications (dApps) by incorporating key components such as the Omni State Channel Indexer (OSCI), decentralized sequencer, ZK-Rollup, and Extended Data Availability (EDA). The expansion of Web3 has resulted in a variety of blockchain platforms, leading to fragmented liquidity that affects user experience and operational efficiency. To address this, Cycle Network introduces Decentralized Application Centric Infrastructure (DACI), designed to streamline dApp development and expand Web3 accessibility. By integrating advanced technologies including OSCI, Verifiable Aggregate Sequencer, ZK hardware acceleration, and Fully Homomorphic Encryption, Cycle Network enhances security, reduces latency, and facilitates global state proofs, thereby improving accessibility, interoperability, security, decentralization, and privacy for both developers and users.

1 Introduction

1.1 Decentralized Application Centric Future

The growth of Web3 has been remarkable, with millions of users actively engaged on various blockchain platforms worldwide [1]. According to crypto.com, as of mid-2022, there are approximately over 300 million active Web3 users globally [2]. This rapid expansion has led to a diversification of blockchain platforms, each with its own unique protocols and assets. However, the emergence of these parallel ecosystems has resulted in fragmented on-chain liquidity, posing significant challenges for seamless user experiences and market operation efficiency. Since 2023, the explosion of Rollup technology has led to more applications being built as dApps, further exacerbating liquidity fragmentation and negatively impacting user interaction. Research from l2beat indicates that there are over 180 Layer 2 solutions [3], with assets totaling $45 billion in the entire Ethereum Layer 2 ecosystem, yet only 15% of liquidity is effectively interoperable across chains. This fragmentation creates barriers for users, who must navigate through complex bridges and solutions to manage their assets, and for developers, who must deploy their applications repeatedly to meet the needs of users across different ecosystems. Addressing these challenges is crucial to ensuring a coherent Web3 experience, fostering greater adoption, and maximizing the potential of blockchain technology.

To tackle these challenges, the industry is advocating for an open infrastructure that can adeptly support innovative decentralized applications (dApps). This proposed framework, which we refer to as Decentralized Application Centric Infrastructure" (DACI), has the potential to streamline the process of developing and utilizing dApps, thereby broadening access to the Web3 for a wider user base.

To achieve this goal, Cycle Network introduces Verifiable State Aggregation (VSA) as a key building block for DACI (Decentralized Application Innovation). VSA aims to lift the restrictions faced by developers in multi-chain environments while fostering an open atmosphere conducive to innovation. Additionally, VSA strives to reduce end-user barriers and promote broader integration of dApps into blockchains.

To implement VSA, Cycle Network employs various technologies such as the Omni State Channel Indexer (OSCI), Verifiable Aggregate Sequencer, ZK hardware acceleration, and Fully Homomorphic Encryption. These components aggregate decentralized global state proofs, enhancing the security, low latency, and cost-effectiveness of multi-chain dApp deployment. They play a crucial role in realizing a future centered around dApps, supporting global state proofs under trustless state changes (execution) to handle arbitrary chain-to-chain requests.

Cycle Network is committed to ensuring accessibility, integration, security, decentralization, and privacy within the blockchain, providing an enhanced experience for developers and users alike.

1.2 Related Work

The industry has proposed various solutions, including cross-chain, multi-chain, and chain abstraction, to address the challenges posed by current multi-chain liquidity issues. However, each of these solutions has its own set of drawbacks.

Regarding cross-chain solutions: The vast majority of cross-chain bridges currently rely on smart contracts and centralized off-chain services to synchronize states between different chains[4]. Due to the lack of provable security via decentralized cryptography, these smart contracts and centralized services often become the weak points in the security of cross-chain bridges, making them susceptible to attacks and resulting in significant asset losses. The attacks on Poly Network in 2021, and on Wormhole, Ronin Network, and Nomad Bridge in 2022 are well-known examples[5]. In these cases, assets worth billions of dollars were stolen by attackers, causing substantial financial losses.

Regarding multi-chain/omni-chain solutions: several approaches Extended cross-chain solutions to multi-chain scenarios, thereby inheriting the security vulnerabilities of cross-chain technologies. The typical omin-chain solutions are based on the rollup technology[6], which significantly enhances the security of cross-chain asset transfers in multi-chain scenarios. However, under rollup-based solutions, users still need to perceive and understand complex Web3 concepts and engage in frequent and intricate interactions with the underlying blockchains. This complexity presents a non-trivial entry barrier for users.

Finally, the chain abstraction solutions aim to abstract and encapsulate the functionality of multi-chain/omni-chain systems, allowing users and developers to interact with blockchains in a transparent manner (i.e., without interpreting the underlying operations)[7]. This approach addresses the high entry barrier for users in multi-chain/omni-chain scenarios. However, chain abstraction solutions also face their own challenges. In the context of multi-chain asset and message interactions, the choice of security model remains critical. Additionally, achieving complete decentralization is another significant issue that needs to be addressed in the current chain abstraction field.

Cycle Network emerges as a cutting-edge chain abstraction solution designed to address the existing shortcomings in the chain abstraction domain. By inheriting the security of the Ethereum mainnet, Cycle minimizes the risks associated with cross-chain operations. Furthermore, it introduces a comprehensive multi-chain ordering mechanism, enabling verifiable aggregation of multi-chain states within Cycle, thereby achieving complete decentralization in the chain abstraction architecture.

1.3 CycleNetwork: Enabling New Paradigm Shifts in WEB3 Development

Web3 marks a paradigm shift from Web2 by replacing centralized backend servers like IDC or cloud services with decentralized solutions. Over the past 16 years, the development of the Web3 technologies has evolved significantly. Initially, the focus was on building large Layer 1 blockchains like Ethereum[8] and Solana[9]. However, in recent years, as Rollup technology emerges[10], developers start to build their dApps on Layer 2 solutions or using independent Rollups. However, the negative impact of this multi-chain world is that the developers encounter increasing limitations imposed by different platforms, which hinder long-term projects and stifle industry innovation.

CycleNetwork addresses these challenges by inventing advanced chain abstraction technology. This enables developers to program for the entire Web3 user base via our SDKs and other middleware, achieving true chain abstraction. Cycle Network constructs chain abstraction infrastructure through verifiable state aggregation and combines the Omni State Channel Indexer (OSCI) with a Decentralized Aggregate Sequencer Architecture to realize secure state aggregation across blockchain networks in a fully trustless and verifiable manner. It builds on the inherent trustlessness and verifiability from Rollup and extends them through the Rollup's Data Availability (DA) layer to a decentralized omni-chain settlement layer. This structure allows Cycle Network to support

trustless global state proof across all Layer 1, Layer 2, and application chains. Crucially, Cycle Network inherits the security guarantees from the chosen Rollup's security layer while achieving trustless global state proof. The Omni ZK-Rollup enables verifiers to efficiently confirm the existence of state changes among the related chains and the Cycle Network. CycleNetwork further leverages ZK hardware acceleration to continuously optimize latency and improve the user experience, and can potentially Extended to enable fully encrypted state transition across different blockchains via homomorphic encryption.

2 Problem Space and Motivation

In this section, we introduce the concept of blockchain abstraction and provide a comprehensive overview of existing solutions. We also discuss the challenges that must be addressed to achieve secure and trustless blockchain abstraction.

Chain abstraction aims to aggregate the interfaces of different blockchain systems and uniformly abstract them into unified interfaces. From the user's perspective, chain abstraction can significantly flatten the learning curve for interpreting complex cross-chain operations in Web3 applications. From the developer's perspective, through unified interfaces, chain abstraction can significantly lower the development barriers to creating dApps and greatly enhance the portability of dApps across different blockchain ecosystems. In the current multi-blockchain era, chain abstraction reduces the implementation costs of blockchain interoperability, and enhances the flexibility and reachability of multi-chain applications. By establishing a unified security model, chain abstraction solutions can significantly reduce the security risks associated with the heterogeneity of various blockchains.

Specifically regarding the Ethereum ecosystem, the current total value locked (TVL) in Ethereum Layer 2 solutions is about $45 billion, while cross-chain liquidity assets account for roughly fifteen percent of the total assets. Chain abstraction can greatly improve the cross-chain liquidity of assets in various Ethereum Layer 2 solutions by reducing the cross-chain operation costs for users and the development costs for developers when creating multi-chain dApps. Since chain abstraction can be extended to multi-blockchain ecosystems, it also has the potential to stimulate cross-chain asset liquidity in ecosystems such as Bitcoin. By connecting multiple blockchain ecosystems, assets that were previously confined to a single blockchain ecosystem can expand their liquidity across all ecosystems through the chain abstraction. As a result, the intrinsic value of asset liquidity will experience exponential growth.

In the field of chain abstraction, some of the most prominent existing and emerging projects include Agglayer, Uniswap X, and many others.

Agglayer is a decentralized chain abstraction protocol proposed by the Polygon team [11]. This protocol, based on the Polygon ZKP architecture, provides a chain abstraction solution within the Ethereum ecosystem. As a specialized solution for Ethereum, Agglayer aggregates cross-chain bridges within the Ethereum ecosystem and extracts a unified cross-chain interface in the form of chain abstraction.

Uniswap X is an innovative chain abstraction solution [12] launched by the Uniswap team, aimed at further enhancing user experience and liquidity management in the decentralized finance (DeFi) sector. Uniswap X aggregates liquidity pools across multiple blockchains, enabling cross-chain transactions and asset exchanges. Users can seamlessly convert assets between different blockchains without leaving the Uniswap platform. However, Uniswap X's security mechanism is implemented through application layer mechanisms rather than blockchain protocol mechanisms. Therefore, its security guarantee is relatively weaker compared to solutions based on rollup protocols.

Particle Network is a chain abstraction solution addressing complexity and interoperability issues in the multi-chain ecosystems [13]. By providing unified interfaces and tools, Particle Network enables developers and users to interact more easily with different blockchains. Users can leverage Particle's account abstraction capabilities to delegate complex cross-chain operations to a unified Particle account abstraction interface. Particle's solution is

implemented based on a combination of centralized and decentralized architectures, which cannot fully meet the trustless prerequisite of the Web3 world.

The analysis of these typical projects reveals some flaws in current chain abstraction implementation solutions. **Cycle Network** is an advanced chain abstraction technology proposed to address these issues. Compared to solutions like Agglayer, which are specifically designed for the Ethereum ecosystem, Cycle extends the scope of chain abstraction to multi-chain ecosystems. Cycle can integrate with EVM-compatible blockchain systems and be compatible with the Bitcoin ecosystem and other mainstream blockchain ecosystems, enabling asset liquidity across heterogeneous blockchain ecosystems, and therefore allowing cross-chain assets to flow freely in our multi-chain era.

Thanks to the rollup mechanism, Cycle can inherit the security of the Ethereum mainnet. Any cross-chain operations based on Cycle are protected by Ethereum's security mechanisms, making it the most secure solution in the chain abstraction field. Cycle proposes a decentralized sequencer architecture. Through an innovative all chain aggregation Sequencer mechanism, it ensures that blockchain states in multi-chain scenarios can be sequenced so that any stakeholder can publicly verify Cycle network's operations. This fully meets the trustless premise of the Web3 era and makes democratic governance of chain abstraction possible.

3 Cycle Network

3.1 Technology Background

In this section, we introduce several fundamental concepts that are crucial for understanding the architecture of Cycle Network. These concepts include Rollup, Zero-Knowledge Proofs (ZKP), Sequencer, and Fully Homomorphic Encryption (FHE).

3.1.1 ZK-Rollup

Rollup is a widely adopted Layer 2 solution in blockchain scaling, known for batching multiple off-chain transactions into a single transaction which will be executed on the host chain. A key feature of Rollup is its ability to inherit the security guarantees of the host chain, maintaining equivalent security properties. There are two primary types of Rollups: Optimistic Rollups and Zero-Knowledge Rollups [14]. They employ different transaction verification mechanisms, and therefore offer different trade-offs between latency, cost-effectiveness, and security.

The Rollup technology is implemented by the Rollup Nodes and Endpoints. The Rollup Node plays a critical role in processing transactions, primarily responsible for sequencing and batching transactions. These transactions are then relayed to an Endpoint contract deployed on the Layer 1 blockchain. A key feature of this framework is the incorporation of Merkle proofs [15], which are essential during the withdrawal processes to ensure the integrity of transactions.

Figure 1 illustrates a typical state transition in the Rollup verification procedure. When a transaction is sent to Layer 2, it updates the blockchain's virtual machine (VM) state. Afterwards, the transaction details and the updated Layer 2 VM state are synchronized with Layer 1 via a smart contract call. Subsequently, Layer 2 generates a Zero-Knowledge (ZK) proof [16], enabling the Layer 1 contract to verify that the old VM state in Layer 2 correctly transitions to the new VM state after executing the transaction. This process demonstrates how transactions occurring on Layer 2 are validated on Layer 1, explaining why the security guarantees of Layer 2 are underpinned by the Layer 1.

Another critical concept in ZK-Rollup is data availability [17], referring to the assurance that all necessary data for validating and verifying Layer 2 transactions is publicly accessible to all stakeholders. In the context of blockchain, data availability ensures that all nodes in the network can retrieve and validate the data required to maintain the integrity and security of the blockchain.

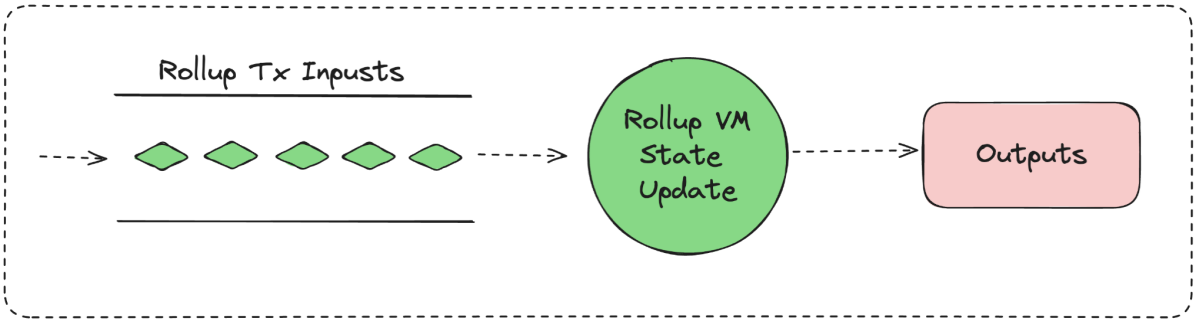

Fig. 1. Rollup State Update

3.1.2 *Sequencer*

A sequencer[18] is a specialized entity or component responsible for ordering and managing the sequence of transactions within a blockchain network. The primary role of a sequencer is to ensure that transactions are processed in a specific and consistent order, which is crucial to maintain the integrity and reliability of the underlying blockchain.

Sequencers are particularly important in Layer 2 scaling solutions. In a Layer 2 network, the sequencer collects transactions, orders them, and then submits the ordered block to Layer 1 for the final settlement. This process helps alleviate the congestion on the main blockchain and allows for faster and cheaper transactions.

The sequencer can be operated by a single entity or a decentralized group of participants, depending on the design of the blockchain protocol. In some implementations, the role of the sequencer may rotate among different nodes to enhance security and decentralization.

By ensuring a consistent transaction order, sequencers play a critical role in preventing double-spending attacks[19] and other forms of transaction manipulation. They also contribute to the overall efficiency and scalability of the blockchain network by enabling higher transaction throughput and reducing latency.

3.1.3 *Zero-knowledge hardware acceleration*

The hardware acceleration of Zero-knowledge Proofs[20] (ZKPs) can enhance the efficiency of (ZKPs) by using specialized hardware to execute the cryptographic operations involved in ZKP. Dedicated hardware accelerators generate and verify ZKPs much faster than software methods, handling intensive computations and reducing time and resource usage. This makes zero-knowledge hardware acceleration valuable for blockchain and decentralized applications, where efficiency and scalability are critical.

In the blockchain world, zero-knowledge hardware acceleration can act as a scaling technology, improving overall performance of rollups, and enabling efficient execution of complex smart contracts.

3.1.4 *Fully Homomorphic Encryption*

Fully Homomorphic Encryption (FHE)[21] is an advanced encryption technique that enables computations to be performed on encrypted data without requiring decryption. This means that data can remain encrypted and secure while being processed, making FHE particularly valuable for data-centric applications. By allowing operations such as addition and multiplication to be executed on ciphertexts, FHE ensures that sensitive information is never exposed during computation. This unique capability protects privacy and enhances security, offering a robust solution for handling confidential data in untrusted environments.

In the context of blockchain technology, FHE can significantly enhance the security and privacy of transactions and smart contracts. Blockchains are decentralized ledgers where all transactions are publicly recorded, which can lead to privacy concerns. By integrating FHE, blockchain platforms can perform computations on encrypted data, ensuring that the content of transactions remains confidential while still enabling validation and verification processes. This can help maintain the transparency and integrity of the blockchain while protecting user data.

Additionally, FHE can be used to secure smart contracts, allowing them to execute complex logic on encrypted inputs without revealing sensitive information. This would enable more sophisticated and secure dApps to be developed, further expanding the potential uses of blockchain.

3.2 Cycle Network Framework

3.2.1 Overview

Cycle Network presents an omni state solution based on Verifiable State Aggregation (VSA). From the perspective of layered blockchain architecture, the framework of Cycle can be represented as the Security Layer, the Extended Layers, and Cycle Layer.

Figure 2 illustrates the three primary components within the Cycle Network framework: the Security Layer, the Extended Layers, and Cycle Layer. This section offers a comprehensive overview of these parties, and their roles in global state proof, respectively.

The Security Layer is defined as a blockchain layer that provides the safety and liveness of transaction state. This layer can be either Bitcoin, Ethereum, or any other highly decentralized blockchain. The consensus mechanism of this layer guarantees state safety so that no two nodes that are functioning properly will produce conflicting results. Meanwhile, it provides some form of finality guarantees that the transactions will be finalized within a bounded time. The security Layer provides foundational security for Cycle Network as a high level decentralized blockchain through Rollup.

The security Layer should be evaluated in a conservative assessment to ensure the safety and liveness of the transaction state, therefore protecting the stable operation and data integrity of the Cycle Network. Bitcoin and Ethereum, two blockchains reputed with their high degree of decentralization and secure consensus mechanisms, have been considered to serve as the Security Layer in the Cycle Network. The Bitcoin Network is temporarily excluded since it is difficult to achieve trustless two-way communication in the Bitcoin network, which is typically addressed through multi-signatures for off-chain verification. This contrasts with the trustless goal of Cycle Network. On the contrary, the Ethereum network is programmable and capable of supporting trustless off-chain verification, making it a more suitable choice for our Security Layer. Cycle Network deploys an Endpoint, and associates with Ethereum via the implementation of zero-knowledge proofs (ZKP).

The Extended Layers refer to the source layers and destination layers where all transaction state and data state are located. This includes all Layer 1s, Layer 2s, and application blockchains. Cycle Network establishes an Endpoints on each Extended Layer for Extended Data Availability (EDA). The Omni Decentralised Indexer is deployed to achieve decentralized indexing of all Extended Layers to achieve the DA (Data Availability) for them. Essentially, Endpoints validate that received messages constitute a comprehensive set for each Extend Layer without any omissions. Synchronization takes place on Endpoints across all Extended Layers through Cycle Layer to ensure complete message retrieval. Cycle Layer serves as a Rollup for both the Security Layer and each Extended Layer. It is constructed with a range of essential components, with particular emphasis on Omni State Channel Indexer (OSCI), the decentralized Sequencer and ZK proof model. All transactions in the Cycle Network, including the cross chain transactions across Security Layer and Extended Layers, as well as internal transactions within Cycle Layer, collectively generate the aggregate Cycle state. The root state of Cycle is generated by a zk-EVM (Zero- Knowledge Ethereum Virtual Machine) Prover. Subsequently, this proof is submitted by the Prover for validation to multiple Layer 1 blockchains and Extended Layers. In the described

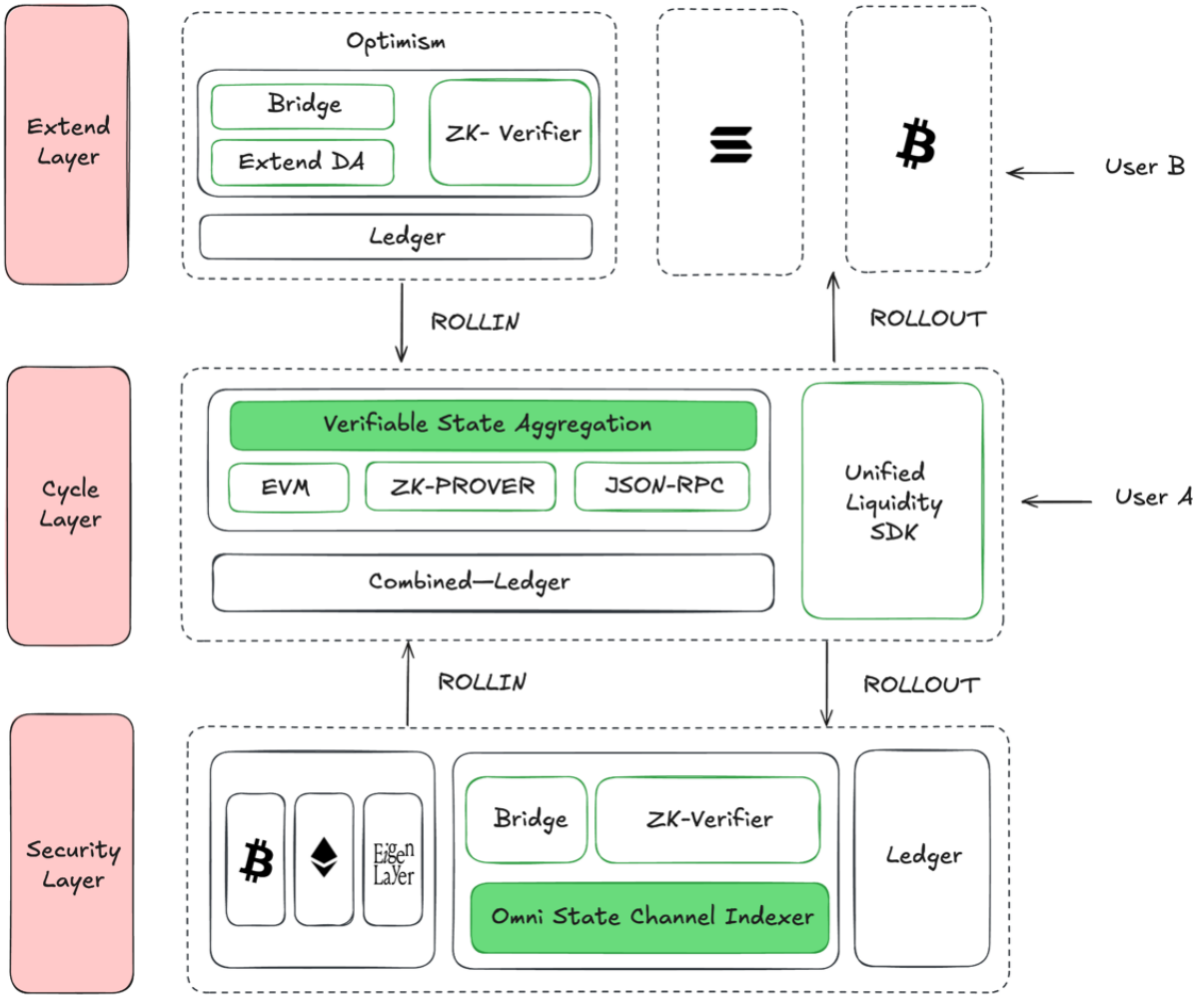

Fig. 2. Cycle Network Framework in Aerial View

process, Cycle Network functions similarly to a custodial system in a centralized exchange. However, users from different chains can trustlessly deposit their assets into Cycle Network and engage in seamless, self-custodied transactions and operations through Cycle Network. Users who employ Cycle Network for on-chain operations are unaware of the existence of multiple chains, making it easier for them to engage in more on-chain activities.

3.2.2 Module Explanation

In this section, we provide a comprehensive overview of the Cycle Network modules, highlighting key components such as the Omni State Channel Indexer and decentralized aggregate sequencer. We will also discuss our recent progress in ZK hardware acceleration and Fully Homomorphic Encryption (FHE).

3.2.2.1 Omni State Channel Indexer (OSCI). The Cycle Network is designed based on Verifiable State Aggregation (executed by Cycle Node) to connect various external chains in different states. However, different blockchains have their own definition of finality, presenting challenges in determining the validity of the state of each Cycle Node. An Omni State Channel Indexer (OSCI) is a decentralized multi-chain indexer that operates omni-chain indexing with decentralized governance to allow for a trustless validation and determination of the state of the Cycle ledger at any given moment. As illustrated in Figure 3, the Omni State Channel Indexer consists of three essential components:

1. OSCI serves as the indexer through which the recovery of the Cycle ledger can be determined and valid at any moment.
2. Cycle Node submits transactions by block packing, and OSCI. Similar to a Block structure, Cycle Nodes string together in a tandem order using Block ID, and therefore initiate the omni ledger.
3. Extended A, B, and C represent the networks that Cycle Node connects to.

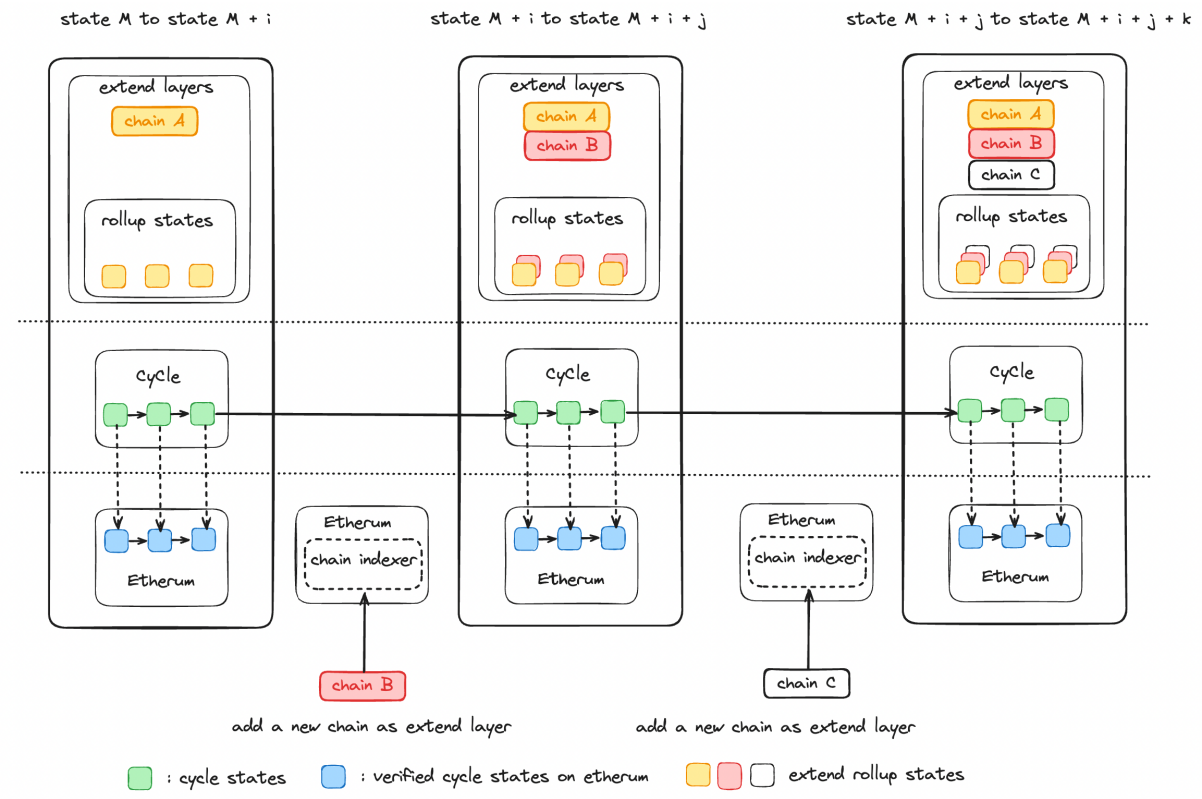

Fig. 3. Omni State Channel Indexer

Cycle Network presents examples to demonstrate Cycle state flow in different Extended Layer scenarios, which is observed by Omni State Channel Indexer.

At Block M state, Cycle connects with Extended A. The change of Cycle state flow is shown as follows:

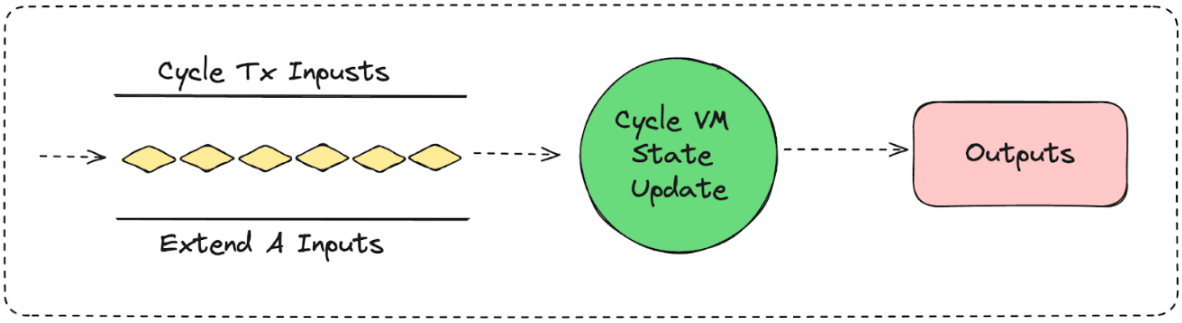

Figure 4-1: State Update With Extended A Txs

At Block M+i state, Cycle connects with Extended A and Extended B. The change of Cycle state flow is shown as follows:

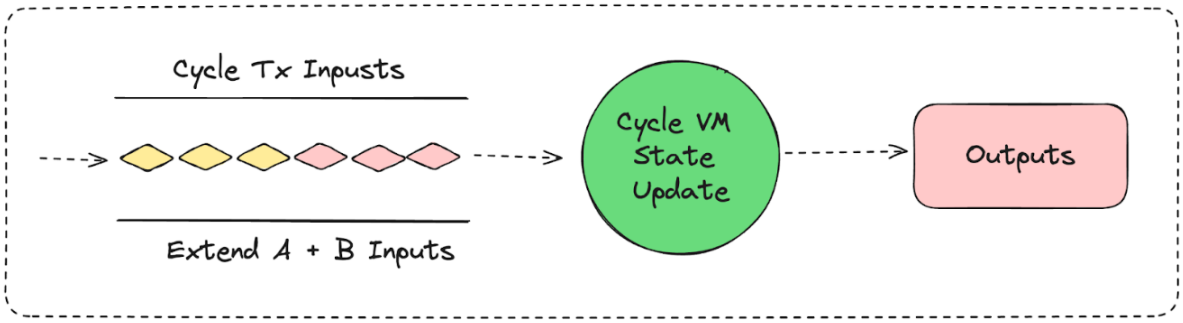

Figure 4-2: Cycle State Update With Extended A, B Txs

At Block M+i+j state, Cycle connects with Extended A, Extended B, and Extended C. The change of Cycle state flow is shown as follows:

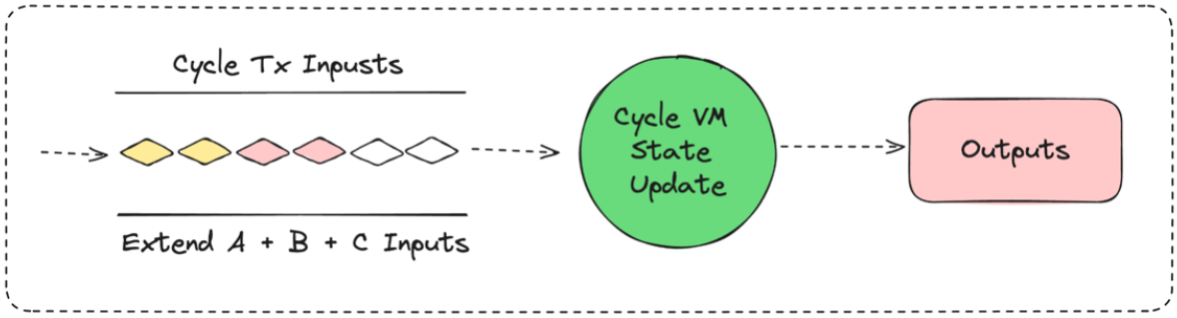

Figure 4-3: Cycle State Update With Extended A,B,C Txs

The subsequent state in a Block state of Cycle is determined by all inputs. At any given time, as long as the transaction arrangement is determined, the final state is determined. The state of the entire Cycle is solely dependent on the unified inputs of all Indexers, and the state of the transaction is verified upon submission. To safeguard the integrity of the data, Project can oversee Cycle by maintaining their trusted full nodes.

In practice, the finalized states of Cycle and all security/Extended layers can be acquired permissionless by any network service and the multi-chain state flow order can be accessed from OSCI under any circumstances. Since all necessary data to rebuild the entire Cycle is available, anyone can rebuild the comprehensive Cycle state flow. As long as the multi-chain states can be aggregated in blocks with a determined order which is guaranteed by the OSCI, any third-party service can verify every state finalized on Cycle, which is the prerequisite for achieving decentralized sequencer.

3.2.2.2 Decentralized Aggregate Sequencer. The Sequencer is a fundamental component of Cycle infrastructure which is responsible for managing transactions, generating blocks which are validated by mutual verification mechanism and aggregating transaction states. In Cycle, multiple decentralized sequencers operate simultaneously. By coordinating the cooperation of these sequencers via distributed consensus protocols, the decentralization of Cycle is ensured.

Cycle implements decentralized sequencer intending to enhance Cycle's security, fairness and network robustness. To this end, Cycle develops a mutual verification network for sequencers to ensure decentralization.

OSCI ensures that the multi-chain aggregate state is verifiable, and any stakeholder can rebuild the comprehensive Cycle state flow. That means, every state in Cycle history can be rebuilt and verified by the sequencer hosted by anyone. Further in multiple sequencers, every sequencer can verify the state transition. Besides, every sequencer can verify the order of transactions in every block match their packing priority, which is critical to ensure any valid transaction can be included in Cycle based on its public priority, preventing a single sequencer from intentionally excluding certain transactions. While OSCI makes aggregate sequencer verification possible, a pre-Consensus network of sequencer can be developed and thus the decentralization of sequencer is feasible.

Features of Decentralized Aggregate Sequencer: A Sequencer can manage the entire lifecycle of transactions it received, which involves sequencing, executing and recording each transaction on the Cycle Network and the Security Layer.

1. **Generating blocks:**
   Each Sequencer packs transactions according to their own order into a new block as it sees fit; By broadcasting the blocks that Sequencers packed up, a mutual verification will be made to determine the block's legitimacy.
2. **Aggregating transaction states:**
   Cycle transactions consist of two parts: transactions that occur within Cycle and the rollup transactions between Cycle and the related blockchains. All of these transactions are aggregated into ZK-proofs that are persistently stored on the Security Layer.
3. **Sequencer decentralization:**
   The Sequencer of Cycle is completely decentralized so that any stakeholder can run a Sequencer to validate transactions relevant to Cycle.

Technical architecture of Decentralized Aggregated Sequencer: A Decentralized Aggregated Sequencer consists of two key components: state manager and pre-consensus client.

• *State manager:* A state manager is the crucial part of the decentralized aggregate sequencer which features transactions management, block generation and state submission.

1. **Transactions Management:** Once a transaction is submitted to a sequencer, the state manager will store the transaction in the state database. Afterwards, the state manager executes suitable transactions, permanently changing the global states on Cycle. The state manager takes care of transactions until its state is verified on the Security Layer.
2. **Block Generation:** In Cycle, multiple transactions are aggregated into a block. After ordering all recorded pending transactions, the state manager decides which transactions are chosen to be packed in the block and then submits the block to the Security Layer.
3. **State Submission:** The state of a block has multiple status, the final status of a block is to be verified on the Security Layer. The state manager collaborates with the ZK prover, publishing the aggregate ZK proof of multiple transaction blocks to the Security Layer, and eventually finalizing the blocks included in the submitted proof.

• *Pre-Consensus Client:* The multiple sequencers forming Cycle's decentralized network need to achieve pre-Consensus to decide which block will be submitted to the blockchain. In Cycle, a general-purpose consensus architecture such as Symbiotic or Eigenlayer can be used to implement the pre-Consensus mechanism. The decentralized sequencers and the consensus architecture are integrated via smart contracts deployed on the Security Layer.

In conclusion, a Sequencer plays the role of a decentralized node in Cycle. It is responsible for transaction management, pre-consensus mechanism, and transaction states aggregation in a fully decentralized manner.

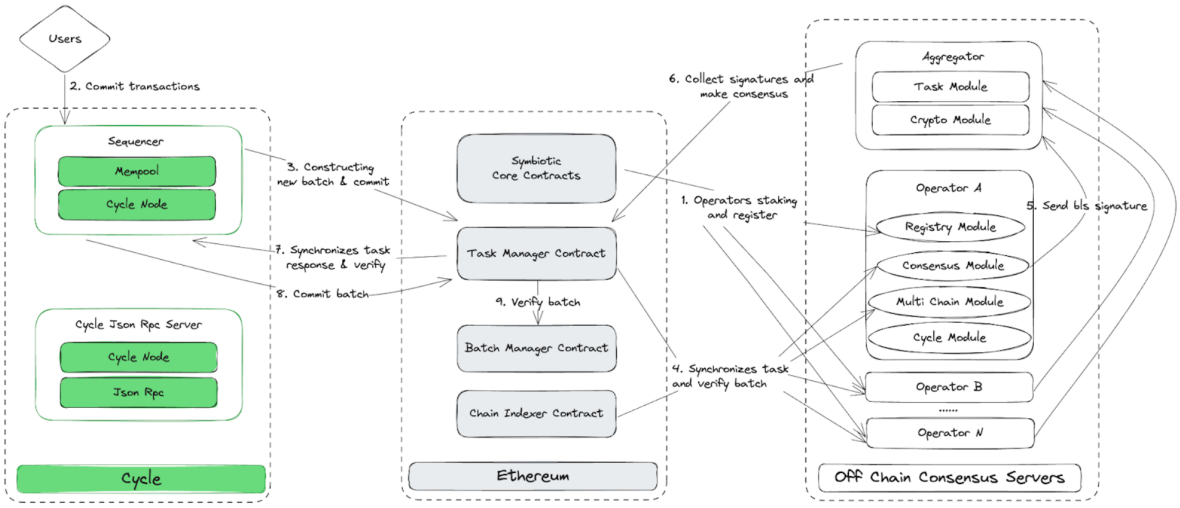

Figure 5: Decentralized Aggregate Sequencer

3.2.3 *Zero-knowledge hardware acceleration*

Cycle Network enhances the developer experience by using ZK Rollup to reduce the latency of Rollout. In this section, we discuss our recent effort on accelerating the ZK computation via hardware.

For polynomial-based Zero-Knowledge Proof (ZKP) systems, there are two primary components: the polynomial commitment scheme and the polynomial Interactive Oracle Proof (IOP). In the polynomial commitment scheme,

the main computational overhead arises from multiscalar multiplication. In the polynomial IOP, polynomial arithmetic presents a bottleneck, which we will discuss in detail below.

Prior to generating a proof, the program to be verified must be converted into either R1CS or QAP (such as Groth16 and Plonk), resulting in polynomials with millions of coefficients. Subsequently, these polynomials require numerous multiplications. For instance, ZeroCheck is a common operation in ZKP systems. During ZeroCheck, the prover computes $q(x) = f(x)/Z(x)$. The verifier then selects a random number r and verifies whether $Z(r) * q(r) = f(r)$. This process necessitates the use of NTT transform, which constitutes the primary bottleneck.

The polynomials used in ZKP systems exhibit high degrees. Therefore, decomposing large-scale NTT tasks into multiple subtasks becomes necessary due to constraints in GPU memory. These subtasks can then be computed in parallel to optimize performance.

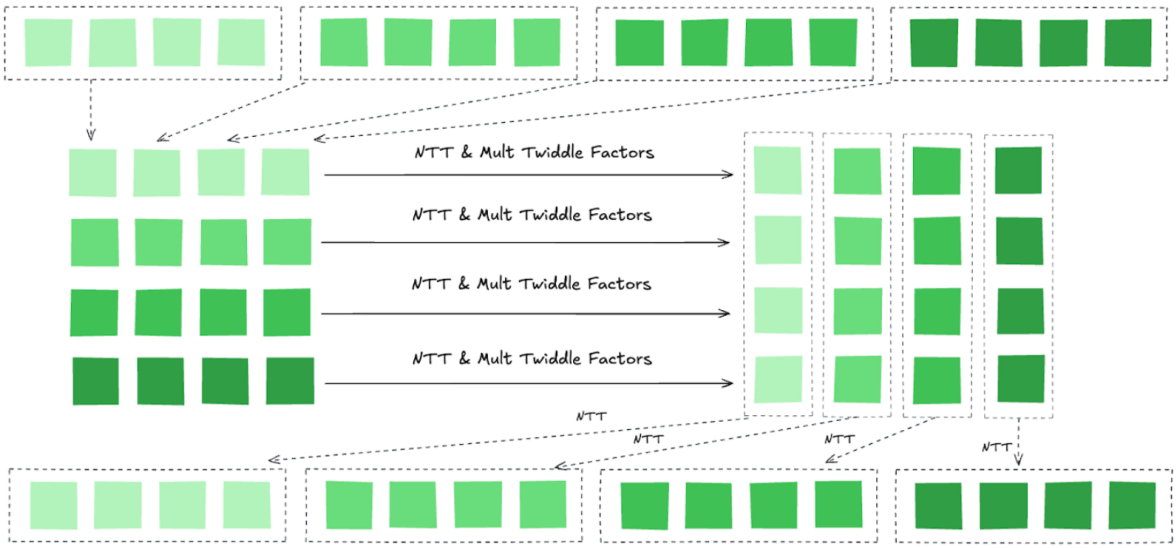

Figure 6: Parallel compute NTT tasks to optimize performance

Therefore, we can compute NTTs of size $\sqrt{N}$ in parallel instead of computing a single NTT of size N to accelerate ZKP protocols. The purpose of multiple scalar multiplication is to compute $Q = \sum_{i=1}^{n} x_i G_i$, where x_i is a scalar, g_i is the size of MSM, and is a point on elliptic curve. The Pippenger algorithm is commonly employed for Multi-scalar Multiplication (MSM) computations. It involves three main steps: partitioning scalars into windows, adding points for each window, and subsequently reducing the results from these windows. Due to its inherent parallelism, the Pippenger algorithm is well-suited for execution on GPUs, FPGAs, and other parallel hardware architectures.

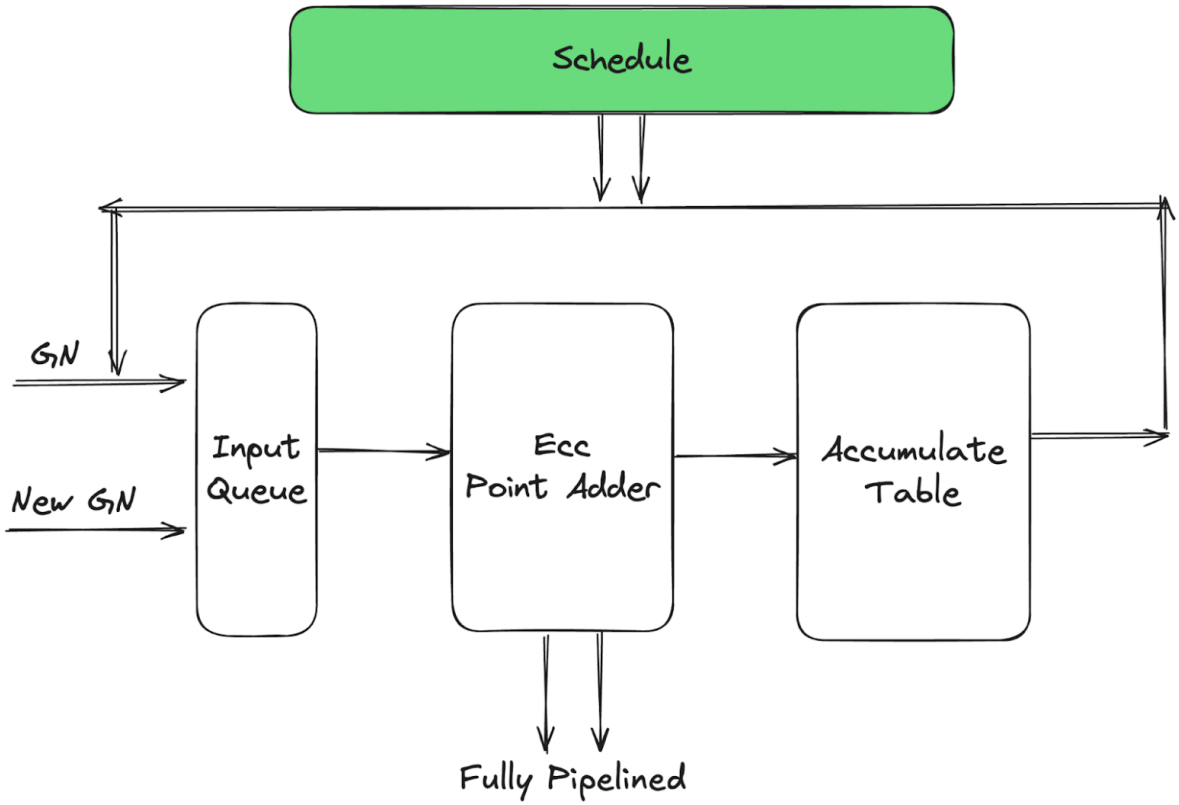

Figure 7: Pippenger algorithm optimization solution

Further optimizing the speed of ZK helps to lower latency even more. A key aspect of this optimization is the Pippenger algorithm, where the point addition process is pivotal. By leveraging FPGA technology, we can create a highly pipelined hardware design, contrasting with traditional GPU architectures. In a point addition operation, multiple additions and multiplications occur within a finite field, all of which can be efficiently processed through pipelining. The output of the point adder is stored in the accumulate table and can be re-entered into the input queue. Additionally, integrating a scheduler component effectively resolves read-write conflicts, further streamlining the process.

3.2.4 Fully Homomorphic Encryption

CycleNetwork employs Fully Homomorphic Encryption (FHE) to enable computations on encrypted data without needing decryption. This ensures that sensitive information remains secure throughout the cross-chain operations, offering complete privacy guarantees to users.

The homomorphic encryption schemes based on the RLWE problem, including the BFV, CKKS and BGV schemes, are built upon the polynomial ring algebraic structure. The RLWE assumption states that, given a fixed polynomial s, by observing an arbitrary number of samples

$$(b = as + e, a)$$

where a is sampled uniformly from the polynomial space, and e is sampled from a distribution with small norm (called noise distribution), the challenger cannot infer s . Based on this assumption, BFV, CKKS and BFV are constructed with polynomial arithmetic. For example, the asymmetric encryption algorithm of BFV is

$$pk = PubKeyGen(s) = (us + e, u)$$

$$c = Enc(m) = (as + \Delta m + pk_0, a + apk_1)$$

where u, a are sampled uniformly from the polynomial ring, e from the noise distribution. We observe that the main computation overhead comes from the polynomial arithmetic, i.e., addition and multiplication.

We identify the possibility of high parallelism in polynomial arithmetic and implement the basic polynomial operations with the CUDA parallel programming paradigm to utilize the GPU devices for a much faster homomorphic encryption library.

- For polynomial addition, since the coefficients do not interfere with each other and each RNS component is also independent, the degree of parallelism could be as high as NL, where N is the polynomial degree and L is the number of RNS components. Thus the complexity is reduced from $O(N\log N)$ to $O(1)$.
- For polynomial multiplication, the naive $O(N^2L)$ multiplication could be reduced to $O(N\log N)$ with NTT, and we can again exploit the NL parallelism and reduce the total complexity to $O(logN)$, as displayed in Figure 8. With CUDA parallel programming, the $logN$ effectively corresponds to kernel calls where each call handles one layer of butterfly computation. With kernel fusing, shared memory and thread synchronization, we could merge multiple kernel calls (e.g. 8 kernel calls corresponding to a block of 256 elements) into one call to further reduce kernel launch overhead.
- To fully support the HE schemes, we also implement RNS composition and decomposition, encoding and decoding algorithms, etc. with CUDA. The final homomorphic encryption library supports encryption, decryption, ciphertext addition, multiplication, rotation, key-switching and modulus switching operations of the BFV, CKKS and BGV scheme.

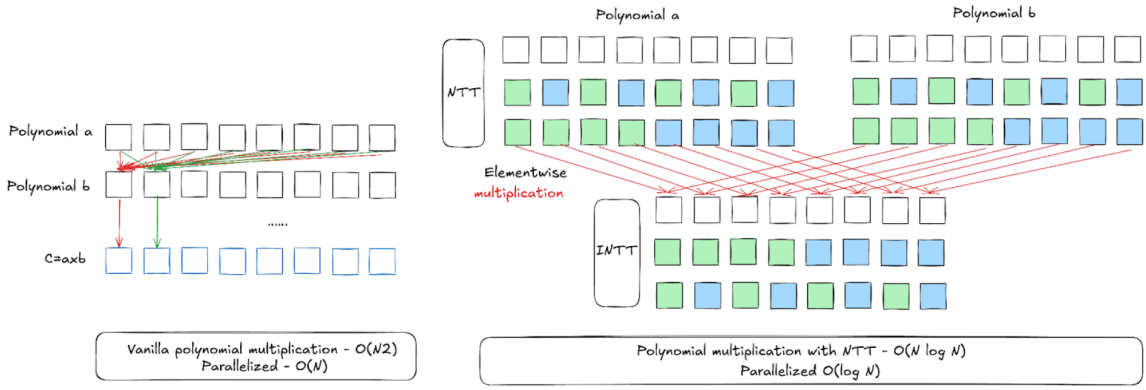

Figure 8: CUDA parallel programming

We notice that allocating and freeing GPU memory could be time-consuming if they are executed with every construction and disposal of a ciphertext/plaintext. Therefore, we use a memory pool to keep track of each piece of allocated memory, only freeing them when the program exits or when the total memory is exhausted. The memory of discarded objects is returned to the pool. When a new ciphertext or plaintext is required, the memory pool tries to find a piece of memory already allocated with a suitable size. If not found, allocation is performed.

We test the efficiency of our implementation and compare it to the CPU-based counterpart. The results show that the basic HE operations are accelerated by up to an order of magnitude.

	Time(us)		
Operation	CPU	GPU	Acceleration
Encode Vector	317.99	28.97	10.98
Decode Vector	316.68	51.8	6.11
Encrypt Asymmetric	8391	122.54	68.48
Encrypt Symmetric	9930	82.81	119.91
Decrypt	1869	50.68	36.88
Negate	38.02	8.37	4.54
Add	68.94	8.53	8.08
Add Plain	114.51	8.55	13.39
Multiply	16711	271.79	61.48
Relinearize	5687	205.86	27.63
Multiply Plain	3551	39.69	89.46
Mod Switch	378.18	21.49	17.6
Rotate Vector	6043	217.23	27.82

Table 1. Test result with our implementation compare with CPU and GPU

3.2.5 Benefits of Cycle

Cycle Network introduces a decentralized, bridgeless hub that seamlessly interconnects all blockchains. With the proliferation of Layer 2 solutions and numerous chains, this innovation ensures that end-users and developers are no longer isolated or fragmented. It enables everyone to share liquidity, pay gas fees, and sign transactions without the need for traditional bridges. In the next section, we will explore the impact of Cycle Network's integration on end users and developers—two of the most crucial participants in the Web3 ecosystem.

For End User: Cycle Network's bridgeless solution addresses the fragmentation in the Web3 experience. Users can seamlessly access and share liquidity across all chains, significantly lowering the costs associated with navigating a multichain environment. This integration greatly enhances the user experience by simplifying participation in multichain dApps and improving overall accessibility.

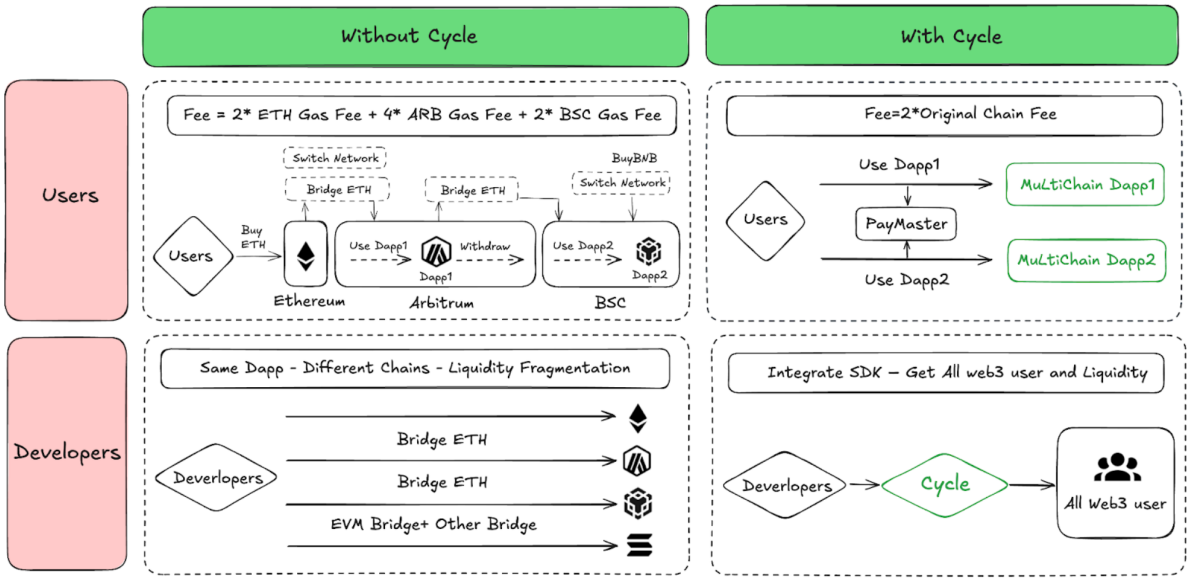

Figure 9: Benefit for Users and Developers with Cycle

Bridgeless UX:

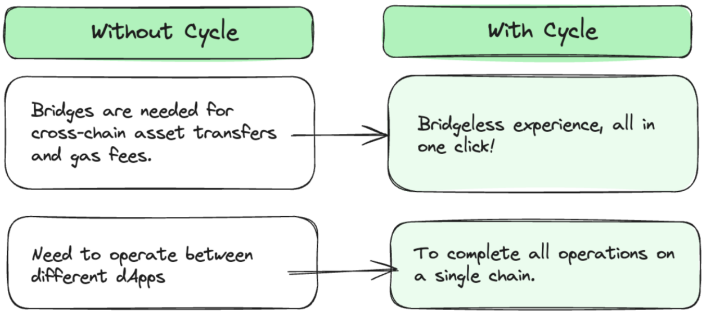

Figure 10: Benefit of Bridgeless UX

Sharing a liquidity layer across all chains dramatically increases yields:

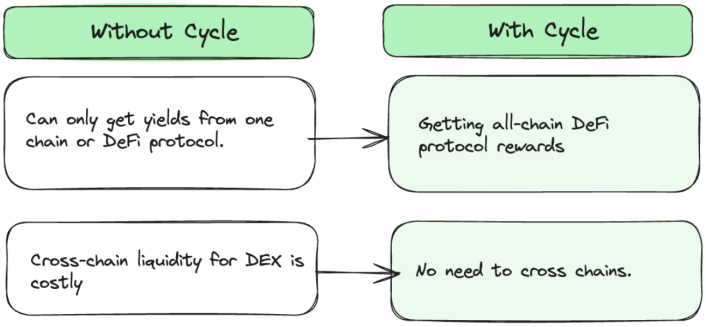

Figure 11: Benefits of Sharing a Liquidity Layer

Reduced cognitive and mental costs for users across different chains:

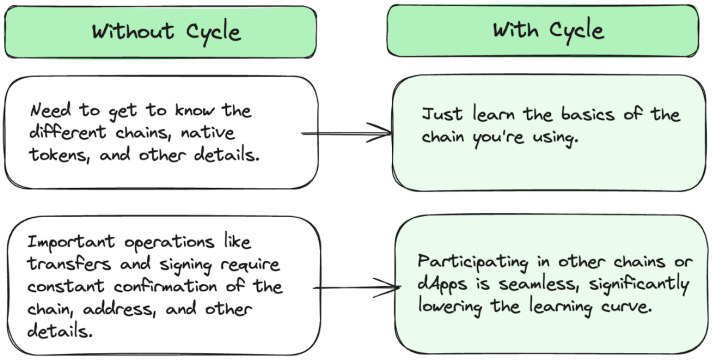

Figure 12: Benefits of Reduced Costs

For Developer: Cycle Network addresses key challenges developers face from three critical perspectives: user experience, technology, and cost.

Users: Cycle Network brings millions of Web3 enthusiasts to your dApp ecosystem in a bridgeless manner. Its seamless user experience, featuring one-click operations and innovative cross-chain integration, significantly lowers the entry barriers for Web3 users. This ease of access enhances user engagement, increasing user volume, transaction volume, asset volume, and liquidity for your project. Additionally, Cycle Network allows users to interact with all blockchains without leaving your dApp, effectively breaking down barriers between different chains.

Technology: Cycle Network introduces the Omni State Channel Indexer, which serializes and aggregates multi-chain states—key for achieving multi-chain abstraction. Compared to other chain abstraction solutions, Cycle offers universality (interconnecting heterogeneous blockchain ecosystems), security (providing Ethereum-equivalent security guarantees), and public verifiability due to its fully decentralized architecture.

Cost: Cycle Network's unified all-chain liquidity pool brings several cost benefits:

1. Reduced Cross-Chain Transfer Costs: By enabling users to share liquidity from all chains within a single pool, Cycle Network eliminates the need for complex cross-chain operations and multiple inter-chain bridges.

2. Lower Transaction Costs: With assets pooled together, trading pairs become more liquid, reducing slippage and transaction costs. Additionally, Cycle's intelligent routing algorithms optimize transaction paths, further minimizing expenses.
3. Improved Funding Efficiency: A unified liquidity pool mitigates fragmentation and idleness of funds across different chains, enhancing overall funding efficiency.

4 Application

In this section, we highlight the exciting applications integrated with Cycle Network and its bridgeless experience. These applications tackle key issues faced by Web3 users, such as liquidity fragmentation and gas fees.

4.1 Piggy Bank

What is Piggy Bank?

Piggy Bank is a pioneering all-chain asset management platform that leverages Cycle Network to deliver a revolutionary asset management experience. Designed to be a flagship product, Piggy Bank simplifies blockchain usage and serves as an accessible crypto asset management tool for everyone. It offers a bridgeless experience and harnesses Cycle's all-chain liquidity sharing solution to automate and optimize investment strategies across multiple chains.

Features of Piggy Bank (for end users):

1. **All-Chain Bridgeless UX**
   Piggy Bank eliminates the complexities of different chains for both Web3 and Web2 users. Managing, trading, investing, and minting assets is entirely bridgeless. Users can handle their crypto assets on Piggy Bank as effortlessly as they manage traditional financial products, without needing to understand the nuances of various chains, gas tokens, or third-party bridges.
2. **High-Yield Platform Aggregating All-Chain DeFi Protocols**
   Utilizing Cycle Network, Piggy Bank aggregates DeFi protocols from any network (L1, EVM, Non-EVM, BTC L2, etc.). AI-driven analysis evaluates security, yield, and stability, recommending personalized investment strategies. Users can select investment options with a single click, benefiting from superior returns due to aggregated and compounded yields across chains.
3. **Wide Range of Asset Classes**
   Piggy Bank supports a diverse array of assets by integrating with Cycle's all-chain DeFi Hub. Users can manage physical assets like real estate and artwork, access various financial derivatives (options, futures, leveraged tokens), and engage in asset borrowing, lending, and liquidity mining across all chains.

Features of Piggy Bank (for developers):

1. **Shared Liquidity Pool**
   Piggy Bank's integration with Cycle Liquidity Aggregator consolidates fragmented liquidity resources into a shared pool. This approach enhances overall liquidity and capital efficiency, maximizing returns and simplifying liquidity management.
2. **Secure and Low-Cost**
   Cycle Network provides Piggy Bank with a unified interface and protocol, streamlining blockchain operations and integrations. The shared liquidity pool reduces the risk associated with single-chain funding and minimizes potential for fraud.

Example: Bridgeless Mint NFT.

Piggy Bank's highly anticipated Piggy Box event has seen over 246K accounts, with nearly 190K assets minted in a bridgeless manner. Users from any chain can mint assets with a single click without leaving their native chain. Transactions, gas fees, and signatures are handled seamlessly on the user's preferred chain (such as IoTeX, BEVM (BTC L2), Arbitrum, BASE, BeraChain), while receiving assets on the project's issuing chain.

4.2 TapUp

What is TapUp?

TapUp is an all-chain Meme LaunchPad that combines the power of Telegram with the seamless integration of Cycle Network. Designed to facilitate the creation and launch of meme coins across all chains, TapUp allows users to mint meme coins without the need for traditional bridges. By bridging Web2 and Web3, TapUp extends its reach to Telegram's vast user base of 900 million active users, making Web3 accessible to a broader audience.

TapUp's Core Advantages.

1. **Integration with Telegram:**
   Extensive Web2 User Base: Telegram, a leading instant messaging app with over 900 million active users, provides a massive user base for TapUp. Leveraging Telegram's popularity, TapUp can attract a large number of users quickly and facilitate viral growth through its Tap to Earn feature. This opens up significant user traffic and value creation opportunities for projects and the blockchain ecosystem.
2. **Cycle Network Integration:**
   All-Chain Web3 User Source: Cycle Network's advanced chain abstraction technology enables seamless and bridgeless connections between users across any blockchain (L1, EVM, Non-EVM, BTC L2, etc.). TapUp's integration with Cycle Network ensures that users from any chain can participate in meme coin minting and other operations without incurring the complexities or costs associated with traditional cross-chain transactions.
3. **Ecosystem Cooperation:**
   Powerful Collaboration Platform: TapUp offers a robust platform for collaboration with other blockchain and Web2 game projects. By partnering with TapUp, project owners can enhance their user exposure, engage in joint marketing initiatives, and drive the development and adoption of blockchain technology.

Bridgeless User Experience.

1. **All-Chain Meme Coin Launch:**
   TapUp removes the limitations of traditional chain-to-chain interactions. Projects can launch meme coins from any blockchain (e.g., TON, Polygon, Solana, Base) and complete the entire process within TapUp without needing to leave their source chain.
2. **Universal Minting Experience:**
   Telegram users, Web3 users from any chain, and even new Web2 users can participate in meme coin minting without facing liquidity, asset, or chain split issues. Users simply pay for tokens on their native chain and mint meme coins directly within TapUp, bypassing the need for bridging or asset swapping.

TapUp has rapidly gained popularity, becoming one of the most popular MiniApps on Telegram Apps Center. User growth has been rapid within just one month of its launch, with the user base reaching 430K, many of whom have been highly engaged, with some spending over 300 hours online.

TapUp exemplifies how bridging Web2 and Web3 can create powerful, user-friendly applications that drive adoption and growth in the blockchain ecosystem.

4.3 Bridgeless All Chain Trading

For on-chain trading, Cycle Network enables native token issuance, both EVM and Non-EVM tokens, on any target chain. dApps can rapidly deploy on all chains, build- ing unified liquidity and enriching DeFi's trading pairs, security, and depth. Additionally, Cycle Network offers all chain data integration that assists on-chain dashboard and trading bot data observation and strategy deployment, ultimately maximizing the profit on DeFi. Moreover, meme tokens, tokens, and NFTs, including new concepts, such as Ordinals on BTC, and Meme tokens on Solana, with community consensus, can quickly go viral through fast deployment and marketing across chains.

4.4 Bridgeless All Chain AI Application

The idea of Web3 and AI combination is one of the inevitable trends in the industry. Cycle Network can help AI to perform machine learning and data analysis by providing all chain data and information. Cycle Network can also optimize predictive models in fields of DeFi, NFT, and GameFi. Meanwhile, with the help of Cycle Network, dApps can upgrade their creativity and innovation in multiple tracks such as Algorithmic Trading, Security Enhancements, Risk Modeling and Prediction, AI Chatbots and NPC Design, and Dynamic NFT.

5 Conclusion

Cycle Network presents a novel solution for blockchain interoperability, security, and efficiency by leveraging Verifiable State Aggregation (VSA) to achieve chain abstraction, enabling seamless interaction across multiple blockchains without the need for bridges. For end-users, it offers a unified liquidity pool, reducing complexity and increasing yields while simplifying multi-chain interactions for a streamlined and accessible experience. For developers, Cycle Network addresses key challenges by offering serializable and aggregatable multi-chain states, improving security, and reducing costs. The integration of advanced technologies like Zero-Knowledge Proofs (ZKPs) and Fully Homomorphic Encryption (FHE) further enhances security and innovation. In summary, Cycle Network delivers a decentralized, secure, and efficient infrastructure that benefits both users and developers, driving forward the Web3 ecosystem.

Furthermore, the document elaborates on the various modules and functionalities within Cycle Net- work, including Omni State Channel Indexer, Trustless Cross Chain Protocol, Omni Distributed Ledger Technology, decentralized Sequencer, access layer, and execution layer. It also highlights the innova- tive use of zero-knowledge proofs (ZK proofs) as a fundamental part of the network's security model, emphasizing the strength and privacy-preserving features it offers.

Throughout the document, the characteristics and benefits of Cycle Network are emphasized. These include heightened security measures, low latency for real-time data transfers, and cost effectiveness compared to traditional cross chain communication solutions. The network's potential to eliminate scal- ability and interoper-ability common issues in current blockchain ecosystems is a key focus, demonstrating its potential to unlock new possibilities for decentralized applications and businesses. Moreover, the document provides real-world application showcases of Cycle Network, detailing how it can power diverse use cases such as Omni-Chain Piggy Bank, Omni-Chain Trading, and Omni-Chain AI Application. These use cases illustrate the versatility and adaptability of Cycle Network, showcasing its potential to drive innovation and enhance the functionality of blockchain-based applications across various industries.

In summary, the comprehensive overview of Cycle Network presented in the document highlights its pivotal role in solving the challenges of blockchain interoperability and omni-chain world state proof. By providing an infrastructure for trustless off-chain verification and omni-chain world state proof on trustless state changes (execution), Cycle Network stands as a promising solution to enable a more interconnected, efficient, and secure blockchain ecosystem.

References

[1] D. Yaga, P. Mell, N. Roby, and K Scarfone. Blockchain technology overview, 2018. URL https://doi.org/10.6028/NIST.IR.8202.

[2] 2021. URL https://crypto.com/research/2021-crypto-market-sizing-report-2022-forecast.

[3] 2024. URL https://l2beat.com/scaling/tvl.

[4] 2023. URL https://uniswap.org/whitepaper.pdf.

[5] CHAINALYSIS. 2022: Biggest year ever for crypto hacking., 2023. URL https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/.

[6] V Buterin. An incomplete guide to rollups, 2021. URL https://vitalik.eth.limo/general/2021/01/05/rollup.html.

[7] 2021. URL https://discovery-domain.org/papers/the-official-near-white-paper.pdf.

[8] 2024. URL https://ethereum.org/whitepaper.

[9] 2018. URL https://github.com/solana-labs/whitepaper/blob/master/solana-whitepaper-en.pdf.

[10] V Buterin. Endgame, 2021. URL https://vitalik.eth.limo/general/2021/12/06/endgame.html.

[11] 2024. URL https://docs.polygon.technology/cdk/agglayer/overview/.

[12] 2023. URL https://uniswap.org/whitepaper-uniswapx.pdf.

[13] 2024. URL https://docs.pArticle.network/.

[14] 2024. URL https://ethereum.org/en/developers/docs/scaling/zk-rollups/.

[15] 2023. URL https://medium.com/evendyne/understanding-merkle-trees-and-proofs-5eca62ba3e83#:~:text=A%20Merkle%20proof%20is%20a,reserves%20to%20cover%20their%20balance.

[16] 2024. URL https://ethereum.org/en/zero-knowledge-proofs/.

[17] 2024. URL https://www.precisely.com/glossary/what-is-data-availability.

[18] 2024. URL https://limechain.tech/blog/what-are-rollup-sequencers/.

[19] 2024. URL https://en.wikipedia.org/wiki/Double-spending.

[20] Ying H. Optimized cpu–gpu collaborative acceleration of zero-knowledge proof for confidential transactions, 2022. URL https://www.sciencedirect.com/science/Article/abs/pii/S1383762122002922.

[21] Paulo M. A survey on fully homomorphic encryption: An engineering perspective, 2017. URL https://dl.acm.org/doi/abs/10.1145/3124441.