Cycle Network: A Trustless Omni Distributed Ledger with a Global State View of All Blockchains

team@cyclenetwork.io

2023-12-04, v0.5

Abstract

In this paper, Cycle Network introduces the first Omni Distributed Ledger Technology (ODLT) as a solution to achieve trustless interoperability. ODLT seeks to enhance the development and utilization of decentralized applications (dApps) by addressing various challenges, including security, latency, and cost effectiveness, which have not been addressed in current solutions. ODLT framework, which includes essential components such as the Omni State Channel Indexer (OSCI), Trustless Cross Chain Protocol (TCCP), decentralized sequencer, Omni ZK-Rollup, and Extended Data Availability (EDA), enables secure and efficient global state proof with low latency and cost. Ultimately, the implementation of Cycle Network will facilitate the integration of innovative features for new trading designs, AI innovations, and DeFi mechanisms, to accelerate developers and users towards a more decentralized application centric future.

1 Introduction

1.1 Decentralized Application Centric Future

The blockchain industry is witnessing a remarkable increase in infrastructure innovation, particularly with the expansion of Rollup and Layer 1 solutions, which aim to address scalability issues in blockchain networks (blockchains). However, these advancements have also introduced new challenges for both users and developers. The complexities of deploying and providing a seamless user experience in the fragmented landscape of Web3 pose a significant obstacle to attracting a sizable audience.

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.

In response to this framework, Cycle Network introduces Omni Distributed Ledger Technology (ODLT) as the key enabler of DACI. ODLT aims to release developers from constraints posed by multi-chain environments while fostering an open atmosphere conducive to innovation. Additionally, ODLT seeks to reduce barriers for end users and promote broader integration of dAPPs into blockchains.

To implement ODLT, Cycle Network identifies two crucial elements: one is enabling global state proof on trustless state changes (execution) across any chain(s)-to-chain(s) requests; and the other is defining an omni-chain ledger. In pursuit of these goals, Cycle Network presents three foundational components: Omni State Channel Indexer (OSCI), Trustless Cross Chain Protocol (TCCP), and decentralized sequencer. These components aggregate fragmented world state proof, increasing security, low latency, and cost effectiveness in dApp deployment, and they play a central role in realizing a decentralized application-centric future.

Cycle Network is committed to ensuring ease of access, integration, security, and decentralization within the blockchain, facilitating an enhanced experience for both developers and users.

1.2 Characters in Technical Principles

In order to achieve a decentralized application-centric future and address the associated challenges, it is crucial to integrate three fundamental characteristics into mechanism design: security, low latency, and cost effectiveness. In this section, we elaborate on the significance of these traits and explain why these characteristics are critical.

1. **Security**

   The blockchain network is characterized by its open accessibility and the collaborative nature to allow all parties to observe, participate, and co-create. This stands in constrast to traditional Web2 security systems' assumptions. Consequently, vulnerabilities in code and flaws in the mechanisms are often exposed by unseen observers due to the blockchain open nature. Moreover, the substantial market size makes it an attractive target for attackers, leading to a high frequency of security incidents. On-chain data illustrates that up to 2023, cross chain transactions from decentralized applications have resulted in thefts of over $2.53 billion by hackers. [1]

   The blockchain industry confronts significant difficulties in establishing secure fragmented world state proof across various blockchains. Owing to the distributed nature of blockchain, with its independent consensus, the design of a trustless mechanism for information exchange across omni blockchains has become a complex topic. Unfortunately, many interoperability solutions currently in use rely on centralized or multi-centric methods, which have resulted in frequent security incidents. We will provide more details on the analysis of the existing blockchain interoperability solutions in Section 2.2.

   The design of Omni Distributed Ledger Technology (ODLT) by Cycle Network is driven by the above challenge. A crucial aspect of ODLT is the implementation of a trustless global state network that spans omni blockchains, thus ensuring secure interoperability.

2. **Low Latency**

   A decentralized application development often involves asynchronous programming, which, especially, is a critical element in the design of multi-chain dAPP mechanisms. In such setups, each blockchain operates at varying confirmation times, presenting distinct challenges, including:

   (a) The additional complexity in code logic may present challenges in terms of comprehension, maintenance, and enhancement, possibly leading to potential exploits.

   (b) The fragmented business process with interruptions and divisions across multiple chains may lead to poor user experience.

   It is essential for ODLT to focus on solutions to achieve a reduction in latency, facilitate smoother asynchronous programming across chains, and enhance the user experience.

3. **Cost Effectivenss**

   A substantial proportion of end users prioritize price considerations and are generally price-sensitive. However, the recurring expenses associated with transactions, operations, maintenance, and usability enhancements ultimately result in escalating costs for end users.

   One of the primary goals of ODLT is to reduce transaction expenses and attract more users to Web3.

1.3 Our Approach

In this section, we introduce how Cycle Network is designed to meet these three technical principles from the ground up.

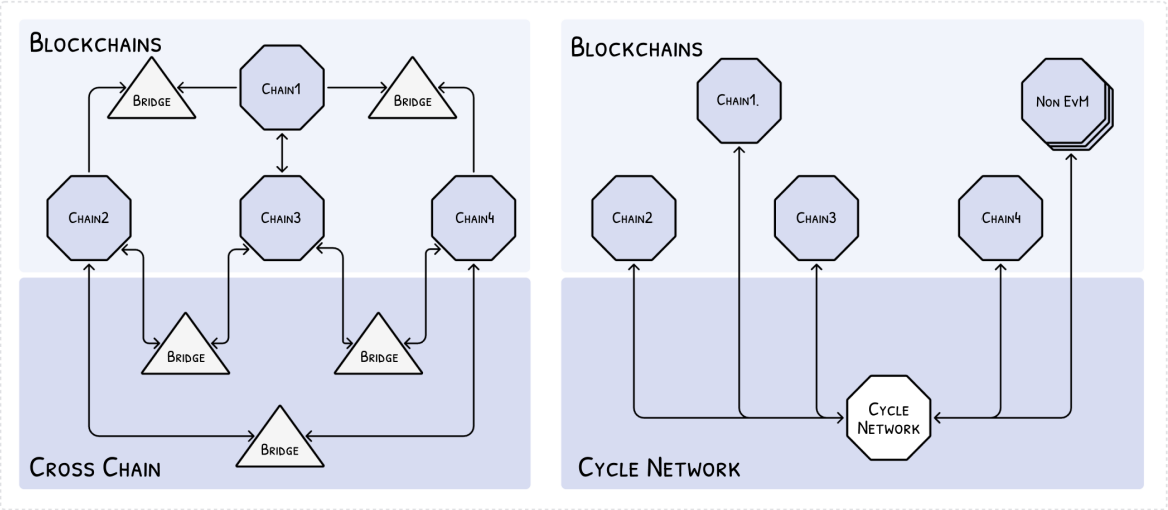

Figure 1: Fully Connected Network Topology Diagram

Cycle Network employs its Omni Distributed Ledger Technology (ODLT), and integrates it with Omni State Channel Indexer (OSCI) and Trustless Cross Chain Protocol (TCCP), to realize global state proof on trustless state changes (execution) across blockchain networks. Cycle Network utilizes the inherent trustless cross chain characteristic on Rollup, and expands to a decentralized omni-chain Settlement Layer by extending the DA layer of Rollup. This structure allows Cycle Network to support trustless global state proof across all Layer 1, Layer 2 and App Chain. Cycle Network also inherits the security provided by the security layer chosen from the Rollup, to achieve trustless global state proof. Omni ZK-Rollup enables provers to efficiently testify the existence of state change (execution) between related chains and Cycle Network. Therefore, any asset or message transferred across chains through Cycle Network can be transmitted trustlessly, while being synced on both Cycle Network and the target chains.

Figure 1 shows a topology diagram on an omni-chain network status based on different interoperability solutions. The left side of Figure 1 shows the current interoperability solution, where chains are independent, between each linked by a bridge. A fully connected bridge is high in complexity, whereas a non-fully connected bridge is high in router latency. The right side proposes an upgraded solution with a trustless connectivity topology, provided by Cycle Network. Any blockchain can achieve trustless interoperability with other blockchains through Cycle Network, whether it is in the EVM ecosystem, or Non-EVM ecosystems such as Bitcoin, Solana, Ton Networks, IBC ecosystem and Move ecosystem.

Three technical principles, security, low latency, and cost effectiveness, are crafted in Cycle Network mechanism: First of all, Omni ZK-Rollup ensures the trustlessness of cross chain transmissions. Although Optimistic Rollup can implement trustless cross chain transmission as well, the speed on withdrawing tokens to various networks is still pending for update. In addition to that, ZK EVM allows Cycle Network to provide smoother and more efficient token withdrawals from Cycle Network to other networks, expanding its potential use cases and applications. Moreover, Cycle Network, backed by its Omni State Channel Indexer (OSCI) and Trustless Cross Chain Protocol (TCCP), not only offers bridge capabilities, but also integrates the characters and advantages of Layer 2. It offers a flexible, rich decentralized platform capability, significantly reducing costs paid by end users, as well as enhancing user experience.

2 Preliminaries and Background

In this section, we introduce the concept of blockchain interoperability and provide a comprehensive overview of existing solutions. We also evaluate the challenges, limitations, and issues that must be addressed in order to achieve interoperability.

2.1 Preliminaries: Blockchain Interoperability

Wegner (1996) defines interoperability as the capacity for multiple software components to collaborate despite disparities in language, interface, and execution platform[2]. This concept not only influences the interoperability definition in computer science, but also has its impact on acknowledgement in blockchain industry. *National Institute of Standards and Technology (2018)* refers to the definition of blockchain interoperability as "a composition of distinguishable blockchain systems, each representing a unique distributed data ledger, where atomic transaction execution may span multiple heterogeneous blockchain systems, and where data recorded in one blockchain is reachable, verifiable and referable by another possibly foreign transaction in a semantically compatible manner "[3]. *Buterin (2016)* describes interoperable chains where "moving assets from one platform to another, or payment-versus-payment and payment-versus-delivery schemes, or accessing information from one chain inside another becomes easy and even implementable by third parties without any additional effort required from the operators of the base blockchain protocols"[4].

Based on the above definitions, we define blockchain interoperability as "the ability of a semantically compatible distributed ledger to confirm, process, and state-sync the application-level transactions and communications originated in another (or multiple) homogeneous and heterogeneous distributed ledger, without the authentication for participants to access the ledger".

2.2 Current Landscape of Blockchain Interoperability Solution

In this section, we present an overview of the current state of blockchain interoperability and discuss the challenges associated with various approaches.

Theoretical frameworks indicate that data security in blockchain interoperability should be equivalent to that of individual blockchains. Nonetheless, challenges related to security, and there is a contrast between technical trade-offs and the growing need for secure business solutions. With the continued growth of the blockchain market, efforts are being made within the industry to enhance the equilibrium between low latency, cost effectiveness, and security.

2.2.1 Centralized Solution

In the early stages, user interoperability requirements were quite straightforward, mainly focusing on token exchange and payment. As a result, most interoperability solutions were centralized.

The centralized solution acts as an interoperability "patch", allowing token exchanges across isolated chains. This is achieved by utilizing a centralized agent (agent), who facilitates token exchanges between different chains through a designated trading pair. The centralized agent holds users' assets until they are withdrawn from the custodian account. The agent maintains assets in separate wallets for each chain, overseen by a shared private key. Centralized exchanges, asset management firms, and dark pool dealers are instances of centralized agents that operate in this manner.

The main drawback of this solution is the reliance on agents who hold users' on-chain assets off-chain without executing their promises to users directly in code. Users must trust these off-chain promises to assume that all related parties, including centralized agents, custodian banks, and auditing firms, have completed their aversion regarding risk control and asset protection. This is far from "in code we trust", advocated by blockchain.

Reliance on agents leads to agency problems. Users and agents may have different purposes and risk preferences, which may lead to conflicts of interest. Considering that centralized agents have more knowledge and control over resources, those agents, self-interested, are more likely to take advantage of information asymmetries and act in their own interest, thereby placing users' assets under arbitrary control - instances have been validated where new listing tokens cannot be withdrawn after being deposited into centralized exchanges.

Additionally, it becomes challenging for users to verify the actions undertaken by agents, when their goals are in conflict. As agents are less interested in protecting tokens than token owners, they are more likely to engage in risky behavior to leverage their own fame, taking users' assets under implementation and operational risk. Once the agents get exploited or hacked, it is users' assets that will end up as a string of numbers.

Examples of wrecked cases regarding the centralized solution of interoperability include:

- (2014) **MT.GOX** got levelled and 850,000 BTC were robbed due to private key attack. After Bitcoin theft, MT.GOX declared bankruptcy. The affected users are still under the payout process in 2023. [5]
- (2016) **Bitfinex**, an affiliate of Tether (issuer of USDT), suffered a website security attack in which hackers stole approximately 120,000 BTC. Approximately 95,000 of the stolen BTC has been recovered through the cooperation of the U.S. Department of Justice and Bitfinex. As of 2023, the recovered funds are still in the government's address (*bc1qazcm763858nkj2dj986etajv6wquslv8uxwczt*), and have not yet been returned to Bitfinex. [6]
- (2021) SBF, the CEO of **FTX**, misappropriated users' assets and made aggressive investments that resulted in significant losses. The malicious act led to a tremendous loss on FTX's users. At present, FTX declares its bankruptcy, and users are still waiting for solutions.[7]

2.2.2 Multi-Centric Solution

Because of the agent reliance on centralized solutions, some projects have proposed a multi-centric solution to mitigate agency problems.

The primary advancement in the multi-centric solution is the incorporation of validator sets, which employ Multi-Party Computation (MPC) or multi-signature technology to achieve interoperability in multiple parties. The multi-centric solution manages these validator sets through the implementation of a signature threshold rule, which requires a predetermined number of validators to approve information before it can be considered verified. This threshold typically falls within the range of one-half to two-thirds of the total number of validators.

A potential drawback of adopting a multi-centric solution is the lack of independence. A trustless multi-party validation cannot realize the low latency requirement from users. To achieve low latency in verification, validator sets are delegated to certain entities. This approach, however, leads to inefficient decentralization and overlooks the potential for malicious behavior. Moreover, such delegation hinders the participation of independent third parties, limiting the opportunity to uncover vulnerabilities at an early stage.

Additionally, the absence of disincentives for validators, both economic and reputational, in the tokenomics design of the multi-centric solution, is a red flag when considering the interests of multiple delegators. This lack of penalties may reduce the cost of malicious behavior for validators, especially during periods of high total value locked (TVL).

We list some examples of wrecked cases regarding the multi-centric solution of interoperability:

- **Multichain** (former Anyswap) creates pools on multiple chains and build cross chain trading pair based on its multi-chain pools. Multichain assigns its shares/control power to its private key

through Multi-Party Computation (MPC). [8] However, this solution assumes trust in the MPC technology. While MPC can distribute control on private key, hackers can still attack cross chain assets by controlling the majority of private key shares. In 2023, an attacker managed to gain control of Multichain private key, and approximately $126.3M lockup assets on the Multichain MPC address were transferred to an unknown address abnormally. As a result, users' assets were drained out and have not been recovered yet. [9]

- **Ronin** is an Ethereum sidechain created for Axie Infinity. It uses a Proof of Authority model to validate cross chain transactions through the approval of over 50% of validators. The solution neglects the decentralisation and trustlessness[10]. In its early design, only nine validators are set up, four of which are operated by Sky Mavis (the company behind Axie Infinity). This means that a hacker is possible to compromise five validators and control Ronin. In 2022, a hacker was able to gain access to Sky Mavis IT infrastructure, and was able to get access on five validators from Sky Mavis and Axie DAO. The hacker drained around 173,600 ETH and 25.5M USDC. Sky Mavis got bailed out through a 150M raise led by Binance, in order to refund user losses[11].

- **Wormhole** deploys smart contracts on multiple chains, locks the token in the source chain, and issues the parallel token on the target chain (Lock and Mint) to complete cross chain transactions[12] .This solution is a custodial service by nature, and users need a trust hypothesis on Wormhole's capacity for asset authentication and verification. In 2022, a hacker exploited the Solana VAA verification and fake the signature to fraudulently mint and lock 120K wrapped ETH on Solana to obtain real ETH on Ethereum. The drained ETH was addressed by the support of Jump Crypto , the parent company of Certus One, which is the original code contributor to Wormhole, on the second day of the attack. The stolen ETH was traced back with the help of Jump Crypto in 2023[13].

2.2.3 A Multi-Subject with Relayers + Light Node Solution

Based on the above multi-centric solution with relayer and light node, some project parties have proposed to increase security through multi-subject verification thereby mitigating the risks associated with over-reliance on the relayers. Simultaneously, the deployment of light nodes across multiple chains speed up the verification process. As this methodology is still in its early stage, we take LayerZero as a case study to introduce the solution and the potential risk points.

LayerZero decentralizes its trust model into two types of verifiers: relays and oracles. The LayerZero V1 whitepaper explains that ultra light nodes are deployed across chains in form of endpoints, where they receive and send block header information on demand through an independent oracle. This information is then verified by an independent relayer. Oracles relay block header information from a source network to a destination network on-demand, while Relayers submit proofs that specific messages are valid according to the block headers submitted by Oracles.

The security of this mechanism depends on the reliability of the relayer and the oracle, with an underlying assumption that these two entities are unrelated and unlikely to collude. If this assumption is violated, the consequences could be severe. In January 2023, LayerZero was exposed to two vulnerabilities in its smart contract. The first vulnerability allowed fraudulent messages to be sent from the LayerZero multi-signature, while the second vulnerability allowed messages to be altered after the oracle and the relayer had signed the message or the transaction. Both vulnerabilities could result in the theft of funds from all users[14].

The second risk point of LayerZero is that it does not offer transport security. Instead, projects on top of LayerZero have to manage their own security, and are responsible for selecting a relayer and oracle, which can increase the cost of ensuring project security. LayerZero does not provide a unified, shared security mechanism from the ground-up.

In the recently released LayerZero V2 whitepaper, LayerZero attempts to improve its security model by performing a higher verifier approval threshold,as well as integrating ZK bridge.

The new verification method increases the verification threshold by requiring that the verification message requires a verification threshold of seven out of 11 entities. Although a higher porpotion of verifer approval is applied in comparison to the previous version, these verifiers are still trusted third parties. LayerZero does not address the security assumptions or security-sharing mechanisms previously mentioned.

The incorporation of the ZK bridge only enhances the efficiency and cost aspects of post-verification data transmission to other chains, not improving the transport layer's underlying problem.

3 Cycle Network Framework

3.1 Technology Background

In this section, we introduce some fundamental concepts that are essential to get aligned before we get into the architecture of Cycle Network. These concepts include Distributed Ledger Technology (DLT), Indexing and Indexer, Rollup, Zero-knowledge Proof (ZKP), and Data Availability (DA).

3.1.1 Distributed Ledger Technology (DLT)

A distributed ledger (referred as "a shared ledger", "distributed ledger technology" or "DLT") is the consensus of replicated, shared, and synchronized digital data that is geographically spread (distributed) across many sites, countries, or institutions[15]. In contrast to a centralized database, a distributed ledger does not require a central administrator, and consequently does not have a single (central) point-of-failure[16][17].

In general, a distributed ledger requires a peer-to-peer (P2P) computer network and consensus algorithms so that the ledger is reliably replicated across distributed computer nodes (servers, clients, etc.)[16]. The most common form of distributed ledger technology is blockchain (commonly associated with Bitcoin cryptocurrency), which can either be on a public or private network. The infrastructure for data management is a common barrier to implementing DLT. [18]

In this case, Cycle Network releases "Omni Distributed Ledger Technology", which expands upon the concept of DLT and defines it in two dimensions.

From a macro perspective, Omni DLT is a decentralized network that includes a mechanism framework and consensus algorithms to guarantee that world states in different blockchains are accurately replicated in an aggregative set and are kept in distributed nodes[19].

From a micro perspective, Omni DLT is composed of a module of distributed nodes that is used to aggregate, synchronize, and update the state change of each node to maintain an omni-world state. For more information on Omni Distributed Ledger (ODL), please refer to Section 3.2.3.1.

3.1.2 Indexing and Indexer

Indexing is a data structure technology used to improve the speed of database queries, optimize search efficiency, and enhance data retrieval performance. This technology is not restricted to database applications but is also widely used in various contexts, including file systems, search engines, and big data processing.

The main purpose of indexing is to establish an auxiliary data structure, which we call an indexer, to determine and accelerate the access to the primary dataset. The indexer can fetch data from a node, transform it, and store it in a decentralized database to provide easy access to blockchain data.

In this case, Cycle Network releases "Omni State Channel Indexer" as a crucial component for its global distributed ledger. This well-developed decentralized omni-chain indexer can significantly increase

the speed and efficiency of cross chain data retrieval. A detailed overview of the architecture of Omni State Channel Indexer can be found in Section 3.2.3.

3.1.3 Rollup

Rollup is a widely used Layer 2 solution in blockchain scaling, known for its batching multiple off-chain transactions into a single transaction set recorded on the host chain. A key feature of Rollup is its ability to inherit security. It can expose confirmation rules with equivalent security properties as the host chain. There are two primary types of Rollups: Optimistic Rollups and Zero-Knowledge Rollups, each offering distinct trade-offs between low latency, cost effectiveness, and security, as well as employing different approaches for transaction verification.

Rollup represents an emergent technology within the blockchain domain, characterized chiefly by the integration of Rollup Nodes and Endpoints. The Rollup Node undertakes a critical role in the transactional ecosystem, primarily tasked with the sequencing and bundling of transactions. Subsequently, these transactions are relayed to an Endpoint contract located within the Layer 1 infrastructure. An important feature of this framework is the incorporation of Merkle proofs, which are instrumental when users initiate withdrawal processes. This verification mechanism ensures the integrity and accuracy of withdrawals, underpinning the blockchain's reliability and trustworthiness.

3.1.4 Zero-knowledge Proof(ZKP)

Zero-knowledge proof (ZKP) allows a party to prove knowledge of information without revealing the information itself. A key component in ZKP, particularly in the context of Layer 2, is an interactive proof system that is represented mathematically as follows:

$$Verifier(PublicInputs, Proof) \rightarrow Accept, Reject$$

This formula illustrates how the verifier can accept or reject the proof provided by the prover, based solely on public input and the proof itself, without any private data disclosure.

3.1.5 Data Availability (DA)

In the field of blockchain, Data Availability is a crucial component designed to ensure that data within the blockchain network is not only securely stored but also accessible and verifiable by all network participants. This layer is essential for maintaining the transparency and security of the network, especially in Layer 2 solutions such as Rollups, where most transaction processing occurs off the main chain, with only aggregated data submitted to the main chain. To address the challenges of data availability arising from this architecture, Data Availability employs technologies such as sharding, erasure coding, and interactive proofs. These methods ensure that all users can access and verify the network's state, thereby promoting decentralization and maintaining the integrity and security of the entire system.

3.2 Cycle Framework

3.2.1 Cycle Framework Overview

Cycle Network presents an omni state solution based on an Omni Distributed Ledger. An Ominchain Distributed Ledger includes an omni-chain DA indexer built by Omni State Channel Indexer (OSCI), as well as zero-knowledge Rollups which inherit the security. Figure 2: Cycle Network Framework in Aerial View illustrates the three primary parties within the Cycle Network framework: the Security Layer, the Extend Layers, and Cycle Layer. This section offers a comprehensive overview of these parties, and their roles in global state proof, respectively.

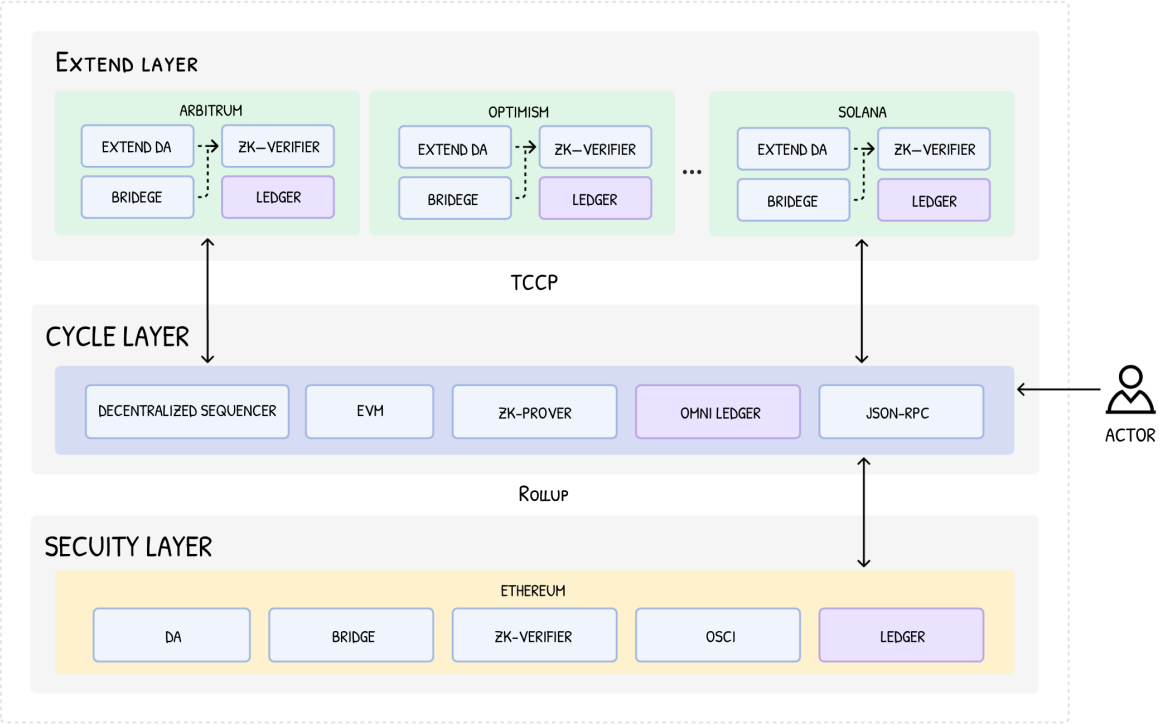

Figure 2: Cycle Network Framework in Aerial view

Security Layer is defined as a blockchain layer that provides the safety and liveness of transaction states. It's consensus mechanism guarantees the states safety that no two node states that are functioning properly will produce conflicting results. Additionally, it guarantees the liveness of states that transactions suitable for inclusion will be finalized by all properly operating nodes within a bounded time. Security Layer provides baseline security for Cycle Network as a high level decentralized blockchain through Rollup. This layer can be either Bitcoin, Ethereum, or any other highly decentralized blockchain.

Security Layer should be evaluated in a conservative assessment to ensure the safety and liveness of transaction states, therefore protecting the stable operation and data integrity of Cycle Network. Bitcoin and Ethereum, two blockchains reputed with their high degree of decentralization and challenging consensus mechanisms, are currently under consideration for the Security Layer of Cycle Network. Considering the security inherent probability, the Bitcoin Network is temporarily excluded due to its incapacity to achieve trustless two-way communication, which is mostly addressed through multi-signatures for off-chain verification in current solutions. This contrasts with the trustless goal of Cycle Network. Conversely, the Ethereum network is programmable and capable of supporting trustless off-chain verification, making it a more suitable choice for the Security Layer. Cycle Network deploys an Endpoint, and associates with Ethereum through the implementation of zero-knowledge proofs (ZKP).

Extend Layers refers to the source layers and destination layers where all transaction state and data state are located. This include all Layer 1s, Layer 2s, and App Chains. Cycle Network establishes an Endpoints on each Extend Layer for Extended Data Availability (EDA). The Omni Decentralised Indexer is deployed to achieve decentralized indexing of Extend Layers, reaching DA (Data Availability) data states for omni-chains. Essentially, Endpoints validate that received messages constitute a comprehensive set for each Extend Layer without any omissions. Synchronization takes place on Endpoints across all Extend Layers through Cycle Layer to ensure complete message retrieval.

Cycle Layer serves as a Rollup for both the Security Layer and each Extend Layer. It is constructed with a range of essential components, with particular emphasis on Omni State Channel Indexer (OSCI)

and Trustless Cross Chain Protocol (TCCP). Other fundamental modules of Cycle Layer include the decentralized Sequencer, access layer, execution layer, and ZK proof model. These modules process cross chain transactions across Extend Layers, as well as internal transactions within Cycle Layer, and generate omni-state root proof of the Omni Distributed Ledger (ODL). To complete the omni-chain transaction, Omni State Channel Indexer achieves decentralized indexing of Extended Data Availability, while Trustless Cross Chain Protocol ensures trustless two-way communication. A decentralized sequencer will be introduced in Cycle Layer with DAO governance to enhance decentralization among participants. More information about the Cycle Layer is available in Section 3.2.3.

3.2.2 Cycle Network Core Processes

The Cycle Network has two core processes, one is the processing flow for Cycle application transactions, and the other is the Cycle omni-chain transaction process.

3.2.2.1 The lifecycle of an Application Transaction in Cycle Network

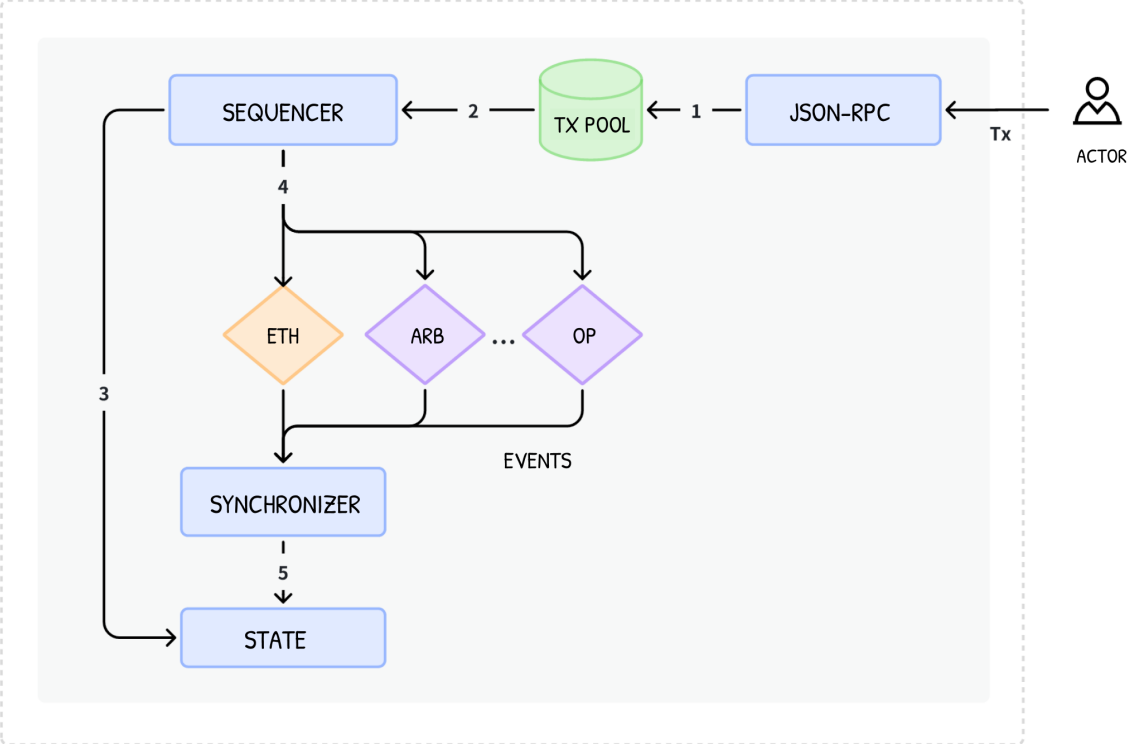

Figure 3: The Lifecycle of an Application Transaction in Cycle Network

Transactions on the Cycle Network are of two types: one is transactions of Applications on the Cycle Network, and the other is withdrawal transactions initiated by users on the Cycle Network. When a user initiates a transaction to the Cycle Network, the lifecycle of the transaction is as follows:

1. The user assembles the transaction through the Client, submits it to the access layer, and it enters the transaction pool;

2. The Sequencer retrieves some transactions from the transaction pool, packages them into a Batch, and writes them into the State Module;

3. The Sequencer submits the Batch to the Ethereum network and submits the Root State to the various other networks it connects to;

4. The Synchronizer, upon synchronizing the events of all networks receiving data, modifies the status of the related Batches in the State table.

3.2.2.2 The Lifecycle of a Cycle Omni-Chain Transaction

This section provides a comprehensive explanation of the omni-chain world state proof process used by Cycle Network, with Omni Stablecoin as an example. Figure 4 graphically represents the fundamental function of Cycle Network through the instance of Omni Stablecoin transfer.

In the following diagram, "Account State" represents the omnichain account state of each user. "Security Layer," "Extend Layer," and "Cycle" correspond to the security layer, the extend layer, and the omnichain ledger layer, respectively within the network. This diagram illustrates that stablecoins can circulate seamlessly across different chains for decentralized transactions through Cycle Network. It is important to highlight that the Security Layer has dual functionality as it can also act as an Extend Layer, enabling assets to circulate between chains via Cycle. The specific operational processes are detailed below:

1. **The initial account status is as follows:**

   a. Alice holds 8 USDT in the Security Layer;

   b. Bob holds 4 USDT in the Extend Layer;

   c. Jessy does not have a balance in any layer.

2. **Alice requests a Rollin command in Security Layer:**

   a. Alice calls the "Rollin" interface in the Security Layer to generate a deposit transaction, depositing 8 USDT into Cycle Layer. This transaction is then recorded in the Security Layer.

   b. Cycle Layer generates a corresponding deposit transaction and records it in the Omni Ledger. Once this operation is claimed, Alice's balance in Cycle Layer increases to 8 USDT.

3. **Bob requests a Rollin command in Extend Layer:**

   a. Bob calls the "Rollin" interface in the Extend Layer to generate a deposit transaction, depositing 4 USDT into Cycle Layer. This transaction is then recorded in the Extend Layer.

   b. Cycle Layer generates a corresponding deposit transaction and records it in the Omni Ledger. Once this operation is claimed, Bob's balance in Cycle Layer increases to 4 USDT.

4. **Transaction calls and state updates in Cycle Layer:**

   a. Alice initiates a transfer of 6 USDT to Jessy through transfer call on Cycle Layer.

   b. Bob initiates a transfer of 2 USDT to Jessy through transfer call on Cycle Layer.

5. **Jessy requests a Rollout command in Security Layer:**

   a. Jessy calls the "Rollout" interface in the Security Layer to generate a withdraw transaction, withdrawing 3 USDT out of Cycle Layer. This transaction is then recorded in ledger of the Security Layer.

   b. After this operation is confirmed, a claim is submitted at the Security Layer, resulting in Jessy's balance at Security Layer increasing to 3 USDT, and Jessy's balance at Cycle Layer decreasing to 5 USDT.

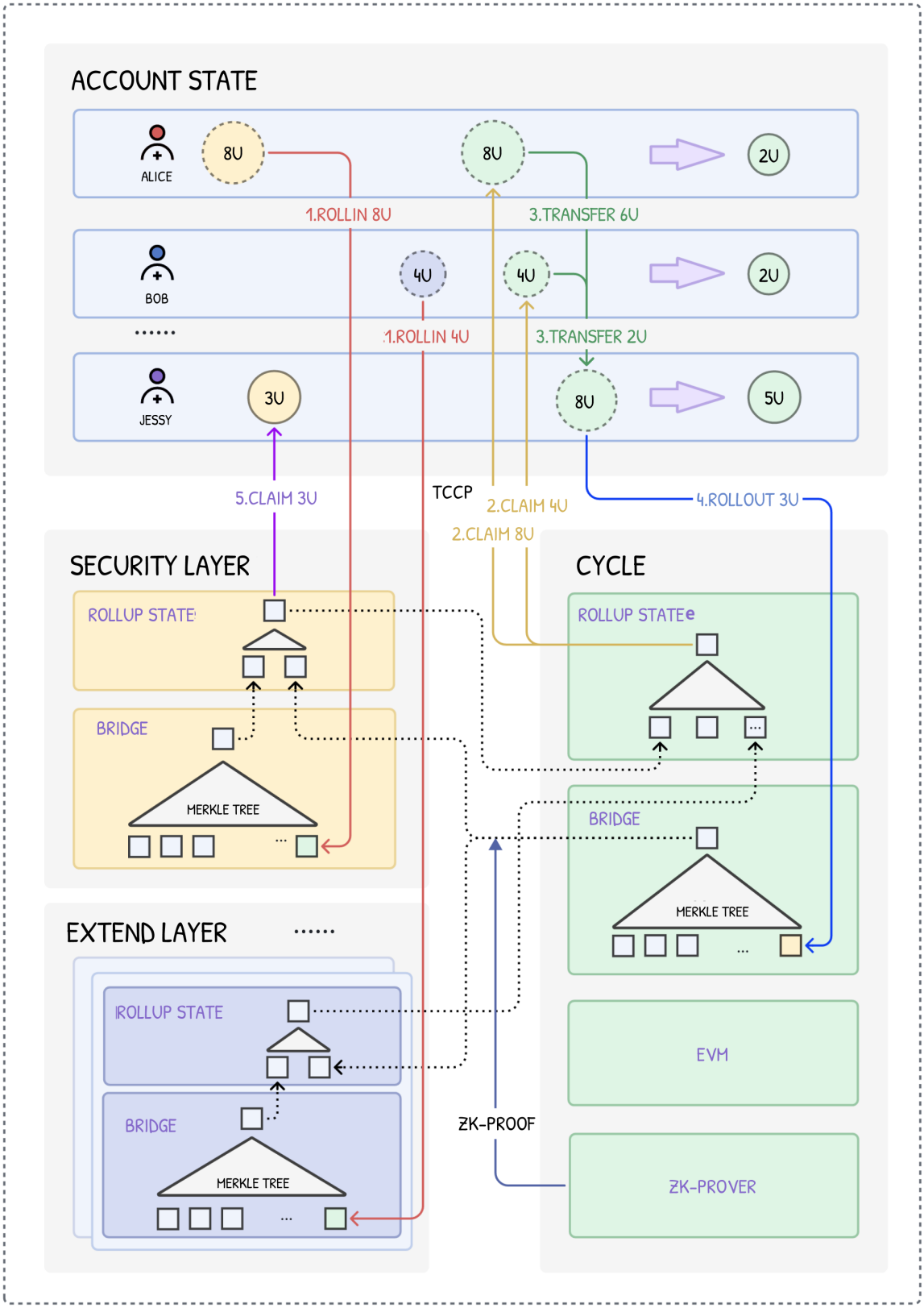

Figure 4: A Omni Stablecoin Example, Schematic Diagram of Asset Circulation

All transactions on Cycle Network, including cross chain transactions across Security Layer and Extend Layers, as well as internal transactions within Cycle Layer, collectively generate the Omni Distributed Ledger. The root state of this omni-chain distributed ledger 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 and Extend Layers.

In the described 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.

3.2.3 Cycle Network Detailed Module Explanation

This section provides a detailed introduction of Cycle Network modules, including both Cycle Nodes and Endpoints.

3.2.3.1 Cycle Node

Cycle Node is a fundamental component of Cycle Network Omni Distributed Ledger Technology (ODLT), as it maintains the complete omni ledger state. Cycle Node's code will be open source on Github, in order for all participants in the community to participate and co-build. The architecture of Cycle Node is divided into several key modules, among which Omni State Channel Indexer (OSCI), Trustless Cross Chain Protocol (TCCP), and Omni Distributed Ledger (ODL) are three key components for Cycle Network to implement an omni-chain ledger. In addition to these, Cycle Node also includes a decentralized Sequencer, an access layer, an execution layer, and a ZK proof model, each of which offers distinct functionalities and value to the operation and development of the entire network.

3.2.3.1.1 Omni State Channel Indexer(OSCI)

Omni Distributed Ledger, known as Cycle Node, connects various external chains in diiferent states. However, different blockchains have their own Finality, which presents challenges in determining the validity of the state of 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 5, 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 batch packing, and OSCI. Similar to a Block structure, Cycle Nodes string together in a tandem order using Batch ID, and therefore initiate the omni ledger.

3. Extend A, B, and C represent the networks that Cycle Node connects to.

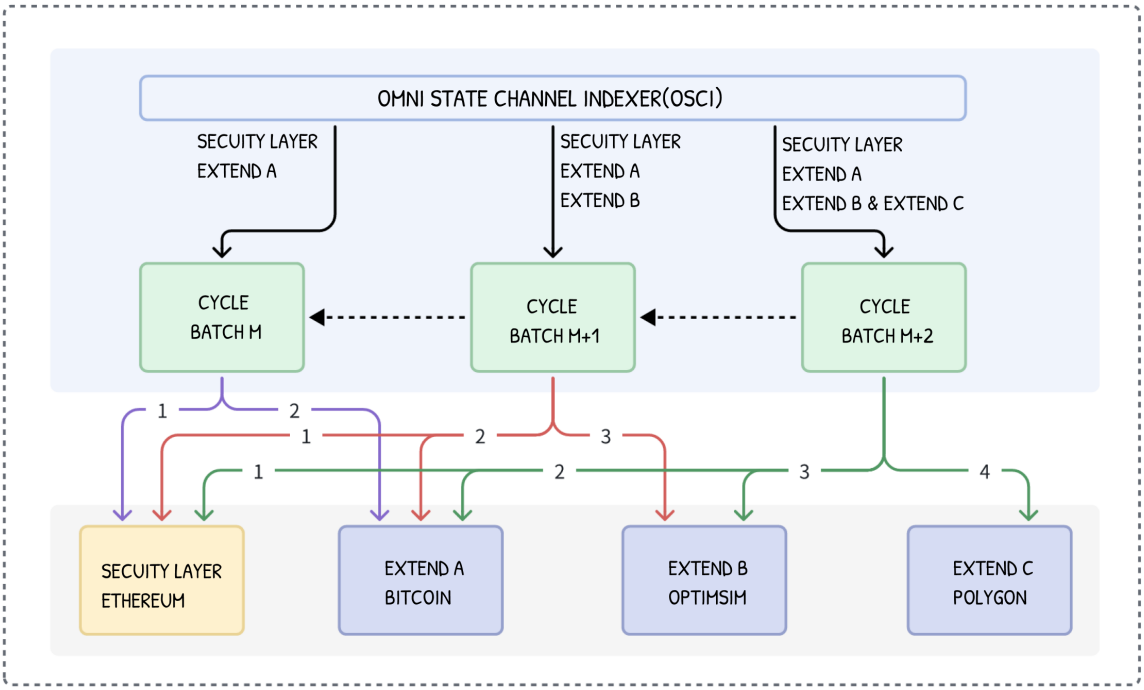

Figure 5: Cycle Omni State Channel Indexer

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

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

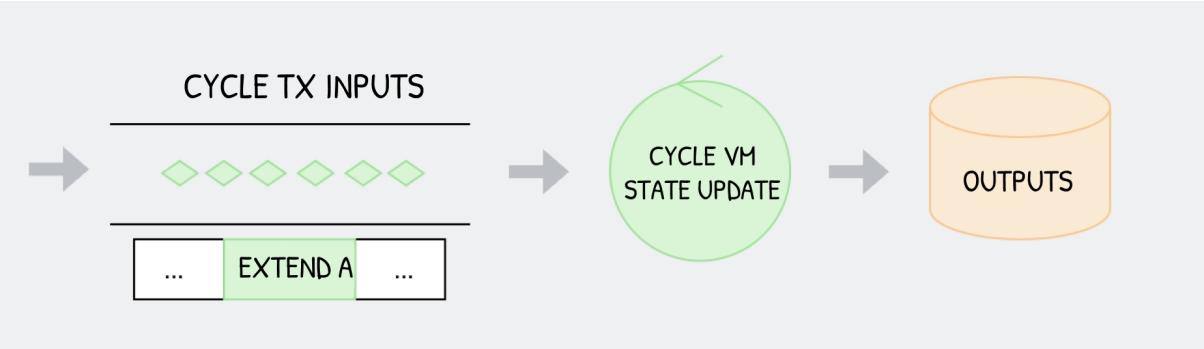

Figure 6-1: Cycle State Update With Extend A Txs

At Batch M+1 state, Cycle connects with Extend A and Extend B. The change of Cycle state flow is shown as follows:

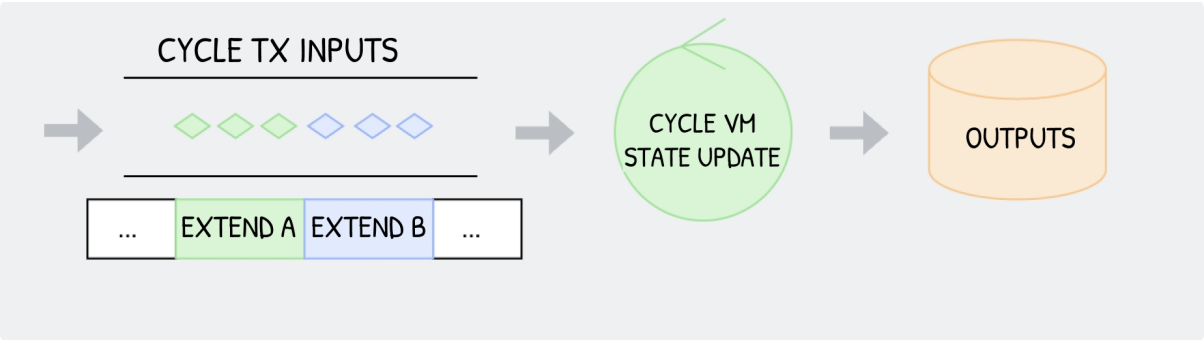

Figure 6-2: Cycle State Update With Extend A, B Txs

At Batch M+2 state, Cycle connects with Extend A, Extend B, and Cycle C. The change of Cycle state flow is shown as follows:

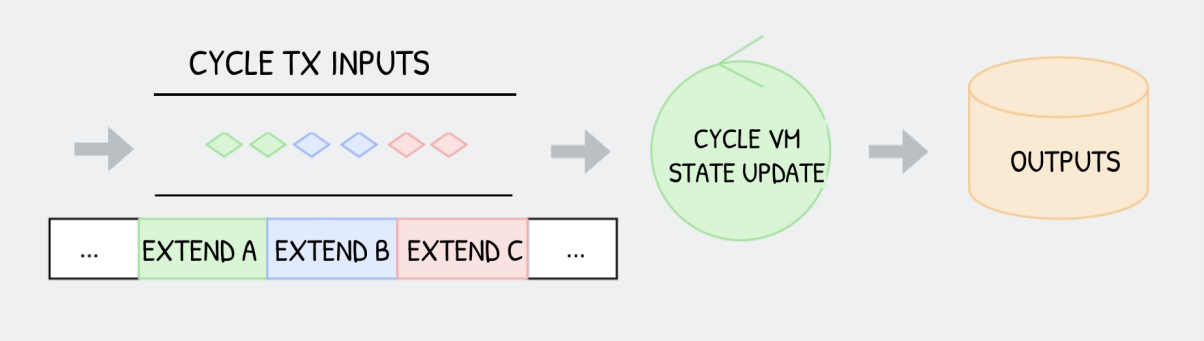

Figure 6-3: Cycle State Update With Extend A,B,C Txs

The subsequent state in a Batch 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.

3.2.3.1.2 Trustless CrossChain Protocol (TCCP)

Omni Distributed Ledger technology needs to be able to interoperate with other chains, which can be realized through Trustless Cross Chain Protocol (TCCP).TCCP has two interfaces as its core, Rollin and Rollout.Rollin is the interface to transfer assets or messages into the Cycle Network; Rollout is the interface to transfer assets and messages out of the Cycle Network.

```
Solidity
function rollInToken(
address destinationAddress,
uint256 amount,
bool forceUpdateGlobalExitRoot
)

function rollOutToken(
address destinationAddress,
uint256 amount,
uint256 destinationNetwork
)
```

rollInToken interface has 3 parameters:

1. destinationAddress: the address of the collection address on the Cycle Network;
2. amount: indicates the amount of the collection address on Cycle Network;
3. forceUpdateGlobalExitRoot: indicates whether to force update the Exit Root.

rollOutToken interface has 3 parameters:

1. destinationAddress: the address of the collection address from Cycle Network;
2. amount: the amount of money to be withdrawn from Cycle Network;
3. destinationNetwork: the destination network for withdrawing coins from Cycle Network;

By integrating these two interfaces, application developers can securely realize a free combination of assets and data for omni-chain programming.

3.2.3.1.3 Omni Distributed Ledger(ODL)

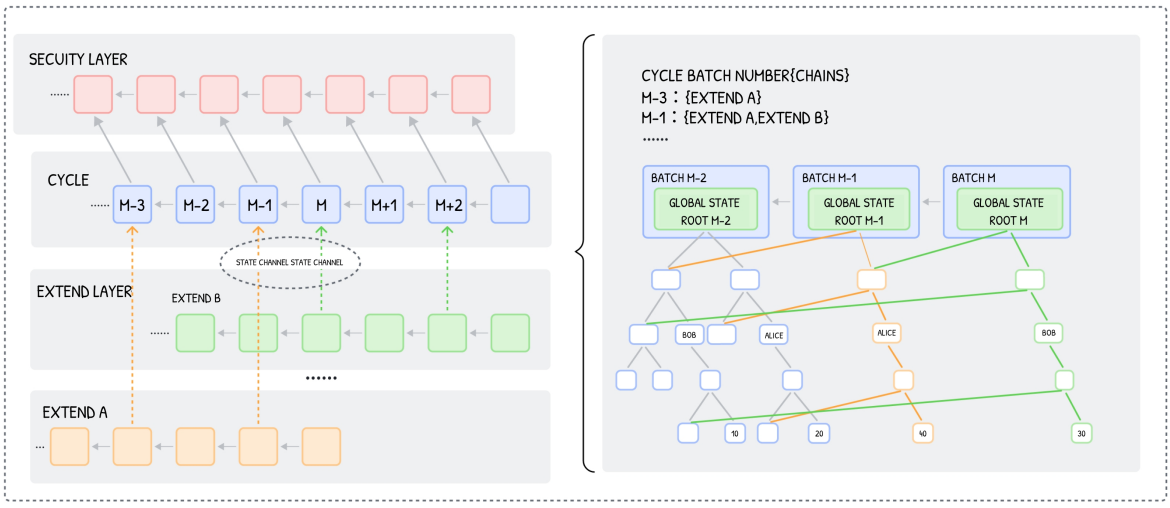

Figure 7: A Dynamic Process of State Transition in an Omni Distributed Ledger

Figure 7 illustrates the the dynamic process of state change in an Omni Distributed Ledger. Cycle Node employs Rollup to commit states to Security Layer, which ensures the integrity and security of

the state. By directly inheriting its state from Security Layer, Cycle Node increases the security of the entire network, and establishes a reliable omni-chain ledger.

The flexibility of Cycle Node is demonstrated by its capacity to engage with different Extend Layers in different states. Take Figure 7 as an example. In the Batch M-3 state, Cycle Node connects with Extend A, exclusively; however, in the subsequent Batch M-1 state, it expands the connection to include Extend B. This adaptability in the Omni State Indexer (OSCI) highlights Cycle Nodes' capacity to respond effectively to the requirements of Extend Layers, and the state of Cycle Nodes with other Extend Layers is dictated by the state of Cycle Nodes.

On the right side of Figure 7 is the process of omni state change with the examples.

1. When Cycle Node locates in Batch M-2 state, OmniStateRoot M-2 is the current state root of the entire Cycle Node, which is generated by the hash root in the blue box above. At this time Extend A initiates a top-up transaction to Cycle Node.

2. Cycle Node will process the above Extend A top-up transaction at Batch M-1, when a state change generated by an external transaction occurs, indicated by the orange box, and a new state root OmniStateRoot M-1 will be generated at this time. This state root is the root state generated by the OmniStateRoot M-1 changing orange leaf node, layer by layer computation, the paths above the orange leaf node are changed, the rest of the part is still in the previous state, the other state nodes need to change the state pointer to point to the new root node. At this point Extend B initiates another top-up transaction to Cycle Node .

3. Cycle Node will process the above Extend B top-up transaction at Batch M. At this time, a state change resulting from an external transaction will occur, represented by the green box, and a new state root OmniStateRoot M will be generated at this time. This state root OmniStateRoot M is the root state generated by the changing green leaf nodes, computed layer by layer, where all paths above the green leaf nodes change, and the rest is still in the same state as before, and the other state nodes need to change their state pointers to point to the new root node.

In this way, Cycle Node maintains an omni-chain state within the ecosystem, which is protected by Security Layer, thus ensuring the security and stability of the network.

3.2.3.1.4 Decentralized Sequencer

The majority of Rollup solutions deploy a centralized sequencer, which offers high performance and ensures security inherited from Ethereum. However, there is a risk of malicious behavior by the centralized sequencer, which, although unable to alter transactions, can potentially hide or maliciously order them, causing losses for certain users.

Cycle Network implements a decentralized sequencer through decentralized governance to reduce the likelihood of the above issues. However, while decentralized governance helps mitigate the problem, it cannot be eliminated, due to similarities with the Miner Extractable Value challenge in Layer 1, where validators with block finalization rights can engage in similar malicious actions at any time.

3.2.3.1.5 Access Module

The access layer presents a simple means for developers to access. With JSON-RPC, developers can access the nodes to construct EVM-compatible applications by leveraging Cycle Network's complete EVM (Ethernet Virtual Machine) compatibility.

3.2.3.1.6 Execution Module

Execution layer adopts ZK-EVM to ensure EVM compatibility, allowing users to build omni-chain applications using EVM and Trustless Cross Chain Protocol (TCCP) for cross chain interaction and data processing.

3.2.3.1.7 ZK Prover Module

Proof layer records the trace of a transaction when the transaction is executed by the execution layer. Proof layer then constructs a set of polynomial constraints which are verified if and only if the execution trace is valid . Those polynomial constraints provide zero-knowledge verification for on-chain consensus and smart contracts, increases the security and privacy for transactions with high efficiency of on-chain verification.

3.2.3.2 Endpoints

3.2.3.2.1 Data Availability

Cycle Network ensures the completeness and security of its data by storing the raw transaction data on the Security Layer through batch submissions. The batches are connected by calculating acc, then form a virtual blockchain. This feature ensures the immutability and security of Cycle Network's data.

3.2.3.2.2 Bridge Module

Bridge Contract implements cross chain transactions of messages and assets, locked asset management, and wrapped asset management at communication layer.Bridge contract achieves this by providing proof of existence through recording and organizing cross chain messages into a Merkel tree.Users can withdraw their assets or execute global state changes (execution) by submitting the appropriate parameters to Merkel Proof.

3.2.3.2.3 Verify Module

Verify Module is made up of a Zk-Snark proof verification which validates the proof submitted by the Prover from the execution layer. This process guarantees the validity of the Cycle Network world state.

3.2.4 Characters in Cycle Network Framework

Section 1.2 emphasizes the importance for ODLT to meet the character of security, low latency, and cost effectiveness. Cycle Network's technology framework, as outlined above, will be further explained in this section to demonstrate how the architecture allows Cycle Network to meet each of these characters.

3.2.4.1 Security

The security of blockchains typically refers to the security of data, which ensures the integrity of the ledger state. Cycle Network employs the Security Layer through Rollup to inherit the security of Security Layer's consensus mechanism and confirmation rules. In addition, Omni State Channel Indexer (OSCI) and Trustless Cross Chain Protocol (TCCP) in Cycle Node enable validity of the ledger state, as well as the sequence and state finality of the omni ledger. Therefore, Cycle Network is capable of achieving trustless high security.

3.2.4.2 Low Latency

There are two primary types of Rollups: Optimistic Rollups and Zero-Knowledge Rollups. Although both Rollups are able to guarantee security, in terms of latency of asset withdrawals, there is a relatively large difference between the two Rollups. Optimistic Rollups use fraud proof, assuming that all transactions are valid until proven otherwise. This means that there is a challenging period during which anyone can challenge the validity of a transaction. This will increase the latency to withdraw assets and also poor user experience.

Cycle Network applies Zero-Knowledge Rollups which ensures immediate finality, eliminating the waiting periods associated with fraud proofs in Optimistic Rollups. The omni-chain Zero-Knowledge

Rollups achieve immediate communication across all Extend Layers and Security, therefore enhance the encoding speed for developers, as well as end user's experience.

3.2.4.3 Cost Effectiveness

Rollups, with higher TPS potential, improves blockchain performance and reduces the average user cost to participate in on-chain activities. Cycle Network extends this technology by implementing Omni Distributed Ledger Technology, reducing the storage size through the global state proof in Merkle Root states, allowing Cycle Network to address the issue of interoperability and realize cost effectiveness.

4 Application

In this section, we provide some application showcases which can build on top of Cycle Network.

1. **OmniChain Piggy Bank:** In practice, it is inevitable for users to leave tiny amounts of tokens on various Layer 1s, Layer 2s, and application layers. Additionally, users often need to exchange small amounts of gas and test fees when trying out new projects on different chains. Unfortunately, there is no easy method for users to utilize their existing on-chain "petty tokens" , to exchange them for tokens required for new chains/projects, at the best rates. Cycle Network supports a trading tool that aggregates these changes, helping users to integrate changes on various layers, and swap them to the desired token at the best price, through the auto-routing of a sweeper bot.This way, users can manage and exchange their petty tokens in just one click.

2. **OmniChain 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 omnichain, building unified liquidity and enriching DeFi's trading pairs, security, and depth. Additionally, Cycle Network offers omnichain 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.

3. **OmniChain 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 omni 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

The document provides an in-depth overview of Cycle Network, a decentralized network designed to address the challenges of interoperability and global state proof across different blockchains. The primary objective of Cycle Network is to facilitate trustless off-chain verification across multiple chains and global state proof on trustless state changes (execution), thereby enabling a more interconnected and efficient ecosystem for blockchain applications.

The document then dives into the architecture and key components of Cycle Network, which include the Security Layer, Extend Layers, and Cycle Layer. These components work collectively to ensure the secure and efficient transfer of data and assets across blockchains. Additionally, the document outlines the global state proof process, and explains how Cycle Network enables cross chain interactions in a decentralized and trustless manner.

Furthermore, the document elaborates on the various modules and functionalities within Cycle Network, including Omni State Channel Indexer, Trustless Cross Chain Protocol, Omni Distributed Ledger Technology, decentralized Sequencer, access layer, and execution layer. It also highlights the innovative 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 scalability and interoperability 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. CHAINALYSIS. (2023). "2022: Biggest Year Ever for Crypto Hacking." Retrieved from https://www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/
2. Wegner, P. (1996). "Interoperability." ACM Computing Surveys, 28(1).
3. Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018). "Blockchain Technology Overview." Technical Report. NISTIR. https://doi.org/10.6028/NIST.IR.8202
4. Buterin, V. (2016). "Chain Interoperability." R3 Research Paper. https://r3.com/reports/chain-interoperability/
5. Bankrupt Bitcoin Exchange Mt. Gox Begins to Pay Back Account Holders in Bitcoin. Retrieved from https://www.abi.org/feed-item/bankrupt-bitcoin-exchange-mt-gox-begins-to-pay-back-account-holders-in-bitcoin
6. Reuters. Retrieved from https://www.reuters.com/article/idUSKCN10E0KL/
7. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Bankruptcy_of_FTX
8. MultiChain White Paper. (n.d.) Retrieved from https://www.multichain.com/MultiChain-White-Paper.pdf
9. Rekt News. Retrieved from https://rekt.news/multichain-rekt2/
10. Ronin Chain White Paper. Retrieved from https://docs.roninchain.com/basics/white-paper
11. The Defiant. Retrieved from https://thedefiant.io/axie-infinity-hack-600m
12. Wormhole Documentation. Retrieved from https://docs.wormhole.com/wormhole/

13. Elliptic Blog. Retrieved from https://www.elliptic.co/blog/analysis/stolen-funds-from-the-wormhole-hack-on-the-move-after-laying-dormant-for-almost-a-year

14. Prestwich, J. Retrieved from https://prestwich.substack.com/p/zero-validation?ref=www.sihuo.club

15. Government Office for Science (UK). (2016). "Distributed Ledger Technology: Beyond Blockchain." Retrieved from https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

16. Scardovi, C. (2016). "Restructuring and Innovation in Banking." Springer. ISBN 978-331940204-8.

17. Investopedia. "Distributed Ledgers." Retrieved from https://www.investopedia.com/terms/d/distributed-ledgers.asp

18. Sadeghi, M., Mahmoudi, A., Deng, X. (2022). "Adopting Distributed Ledger Technology for the Sustainable Construction Industry: Evaluating the Barriers Using Ordinal Priority Approach." Environmental Science and Pollution Research, 2022-08-09.

19. Ethereum White Paper. Retrieved from https://ethereum.org/whitepaper