

Aleph Protocol: An Enterprise-Grade Solution for the Blockchain Trilemma

ALEPH ZERO

Aleph Protocol: An Enterprise-Grade Solution for the Blockchain Trilemma

The rate of adoption of Decentralized Ledger Technology (DLT) is currently at its historic peak as various industry segments across the board rush to implement blockchain-based solutions to streamline their processes for increased efficiency. On the other hand, the crypto community continues to find new applications of blockchain technology, thanks to rising adoption of DeFi, NFTs and the more recent Metaverses.

While the popular layer 1 blockchain protocols like Ethereum are capable of catering to most of the industry requirements, they suffer from an inherent handicap – the Blockchain Trilemma as they try to strike a balance between decentralization, security, and scalability. It has led to the creation of Layer 2 solutions like Polygon, Plasma, and others as a part of the Blockchain 3.0 movement.

What is Blockchain 3.0?

Blockchain technology is as old as Bitcoin, performing a simple function of maintaining a transparent, immutable ledger of all transactions happening over the network. Obviously, this marks the beginning of the Blockchain evolution, with Bitcoin representing the Blockchain 1.0 stage.

The entry of the crypto industry into the Blockchain 2.0 era is marked by the introduction of Ethereum, and other protocols that soon followed. Blockchain 2.0 gave rise to programmable blockchains, enabling the development of decentralized applications through the implementation of smart contracts etc. As the adoption of Blockchain 2.0 protocols increased, its shortcomings when it came to handling large numbers of transactions became evident. It has led to the creation of solutions that can overcome these issues of scalability and efficiency, signifying the step into the Blockchain 3.0 era.

Blockchain 3.0 era explores the development of protocols and ecosystems that can overcome the blockchain trilemma. As a result, the current Blockchain 3.0 has given rise to various innovative layer 1 and layer 2 scalability solutions.

Aleph Zero – A Radical Layer 1 Solution

An advanced Blockchain 3.0 platform, Aleph Zero is a privacy-centric enterprise-grade Proof of Stake blockchain protocol capable of supporting a wide range of applications. Unlike a majority of Blockchain 3.0 solutions, Aleph Zero is a layer 1 blockchain that is based on a peer-reviewed Directed Acyclic Graph (DAG) consensus protocol with deep integration to the Substrate blockchain infrastructure stack. Aleph Zero's DAG consensus algorithm with a large rotating random committee for complete decentralization and support for oracles, decentralized IPFS cloud storage, scalable and private smart contracts enable it to deliver a highly flexible and composable blockchain ecosystem. Its support extends further to include a universal trustless wallet, decentralized exchange, dark pools and multi-chain capabilities, which makes it highly attractive to both individual and enterprise developers alike.

With its unique setup, Aleph Zero overcomes the issues related to speed, validation time, scalability, and security, while providing an option for either development over its public blockchain or the private instance of the protocol that syncs with Aleph Zero's public chain.

Features that Make Aleph Zero a Promising Blockchain 3.0 Solution

Not a Layer 2 Solution

A significant number of Blockchain 3.0 projects are layer 2 scalability solutions that are designed to augment the transaction processing capabilities of popular Layer 1 protocols. They achieve it by offloading a bulk of transactions from the primary blockchain to their own infrastructure and committing a condensed summary of the

activities back to Layer 1 for validation. By doing so, they help the underlying blockchain avoid network congestion, enabling it to handle more transactions than before. While the layer 2 solutions are successful in achieving scalability, they impact the composition of the underlying blockchain and introduce potential security and privacy vulnerabilities. Furthermore, they also affect the liquidity on the primary blockchain by splitting them across different layer 2 solutions.

As a Layer 1 blockchain protocol, Aleph Zero offers a much more stable environment. It has a state of the art consensus protocol – AlephBFT which is developed from scratch while accounting for all the issues faced by older blockchain ecosystems. The protocol is integrated with Substrate – a future-proof blockchain framework, to impart programmability and multi-chain capabilities. With this combination, Aleph Zero is able to offer a secure infrastructure, along with all the necessary tools for projects to leverage an entire ecosystem for their benefit.

Better Scalability

The Aleph Zero protocol is capable of processing as much as 100,000 transactions per second (TPS) with a block confirmation time of no more than 2 seconds. It is a significant amount in comparison to Ethereum's mere 20 TPS, Visa Network's 2000 TPS and Polygon's 65,000 TPS. The increased output combined with negligible transaction fees enabled by Free Value Transfer Transactions make Aleph Zero more desirable than its counterparts.

Decentralization at its Best

AlephBFT is an improved DAG-based proof of stake consensus algorithm with a large number of random rotating committee members (over 128 nodes) which helps it achieve superior decentralization over conventional DAG based protocols. The decentralization levels exhibited by Aleph Zero is comparable to that of a Proof-of-Work blockchain but without its latency. In addition, it also eliminates the need for heavy computing, making for a flexible and more energy-efficient solution.

As an asynchronous, leader-free, byzantine fault tolerant protocol, Aleph Zero eliminates single points of failures by ensuring that at no time a single node maintains control over ordering of units. In fact, the process is distributed across multiple random nodes, making it resistant to DDoS attacks. The lack of

dependency on timing assumptions for transaction processing and tolerance against up to 33% malicious committee members helps the protocol maintain integrity against network attacks and ensures easy recovery after network partitions.

The project is audited by Trail of Bits, a high-end cybersecurity firm that has worked with some of the well-known and elite organizations like Compound, Facebook, Stripe, DARPA, Cosmos, Loom, Linux Foundation and more. In addition to a comprehensive security audit of Aleph Zero's AlephBFT protocol and its integration with the Substrate framework, Trail of Bits also provides guidance for additional security features and enhancements.

A Combination of Transparency and Privacy

The Aleph Zero protocol can operate as a public ledger and a private instance connected to a public ledger. While the public ledger offers a transparent blockchain solution for dApps that rely on trustless transactions, the private smart contracts capabilities encourage enterprises to build custom blockchain solutions to automate and streamline their processes without worrying about their data being compromised. The privacy layer on Aleph Zero is managed by a combination of its original consensus protocol and Liminal, a custom privacy framework based on zk-SNARKs and sMPC (secure Multi-Party Computation) over Substrate technology stack. Liminal's application extends beyond Aleph Zero as it can be implemented across any bridged network.

Other prominent features that make Aleph Zero an all around Blockchain 3.0 solution are its capability to interact with multiple blockchain ecosystems through bridges and support for seamless integration with decentralized file storage protocols like IPFS and other proprietary data solutions through API hooks. These features turn Aleph Zero into a highly versatile blockchain ecosystem that can be used to develop standalone dApps or integrate with existing infrastructure, which is a huge advantage when it comes to enterprise solutions.

Aleph Zero's Endless List of Use Cases

The high levels of decentralization, scalability and privacy offered by Aleph Zero, combined with low transaction fees and support for multi-chain bridges and

integration with data storage solutions, makes it ideal for a variety of applications. The Liminal-based privacy features further enhance the value of Aleph Zero in Web 3.0 applications.

Apart from being capable of handling all the applications that are supported by other protocols, the Aleph Zero network finds itself uniquely capable of providing robust decentralized data storage and micropayments infrastructure for the IoT industry. When it comes to the internet, Aleph Zero's privacy blockchain has the potential to support a truly decentralized DNS, where it would act as a technological trust layer preventing unauthorized interference and censorship while enhancing user-privacy.

Implementation of Aleph Zero in governance can completely transform how the governments and bureaucracies work. The protocol has the capability of creating trustless systems that introduces transparency to the democratic processes, starting with accountability and verifiability. A combination of public and privacy blockchains can help the government manage different types of records across multiple departments while maintaining transparency by making public records easily accessible to all. With the help of decentralized storage integration and the hub and spoke model of public and private chains, governments and businesses can maintain private chains or spokes for sensitive or confidential information while making other records of public domain accessible over the hub, which is a public blockchain.

The use of decentralized cloud storage platforms like IPFS along with Liminal privacy solutions helps enterprises eliminate the risks associated with centralized data centres, without compromising on confidentiality. It will not only reduce the costs associated with maintaining multiple data centres across different geographies, but also eliminate the single points of failure like hacking, DDoS attacks etc. that are commonly associated with centralized data storage solutions.

\$AZERO

The native token of Aleph Zero ecosystem, \$AZERO serves as the medium of value exchange on the platform. At present, \$AZERO enables users to take advantage of

discount swap fees on Common, discounts on asset-wrapping fee, and access to Liminal bridge. \$AZERO will also serve as collateral for wrapped assets on Liminal and used for Validator node staking.

Aleph Zero in Practice

Aleph Zero is already on the path to providing real world solutions based on its world-class infrastructure. Multiple projects have already started exploring the various functionalities of Aleph Zero, and one among them is Aleph Zero's own product – Common.

Common

[Common](#) is a universal decentralized exchange (DEX) and multicurrency wallet solution that offers a user experience akin to centralized exchanges. Built using Aleph Zero's decentralized custody solution, Common presents itself as one of the fastest and secure decentralized exchange and a dark pool for private trades. The platform bridges multiple blockchain protocols to facilitate transfers of various cryptocurrencies including Bitcoin, Ethereum, Zcash and more, which can be traded in a low-latency, ultra-low transaction fee environment.

Common enables users to trade one cryptocurrency against another instantly. The asset prices are determined by an automated process, taking the supply-demand law for the respective assets into consideration. The platform also enables liquidity providers to participate in exchange functions by depositing various cryptocurrencies into the liquidity pool. They will receive Common tokens (CMN) in exchange, which has coverage on the entire deposit including the collected trading fees. Relative coverage of the deposits for different assets will be decided by DAO and automatically adjusted by rate and arbitrage to offer returns.

ReGen Future Capital

ReGen Future Capital, the global developer and operator of climate change solutions is creating a Carbon Registry using Aleph Zero infrastructure. The collusion-resistant decentralized registry will bring in transparency and traceability to Carbon Credits across the world.

Although Aleph Zero is a relatively young protocol, it has gained widespread recognition and support from some of the leading blockchain technology and investment houses. The combination of decentralization, scalability and privacy offered by Aleph Zero is expected to play a crucial role in the future of Web 3.0 applications. In the near future, the number of projects that will adopt this protocol is expected to increase.