Idea originally from Xiaohang Yu

TL;DR

- Ethereum's vision has always been building a World Computer.
- World Supercomputer supports Ethereum's vision for a World Computer and in addition high-performance computation like machine learning. Thus, we face the trilemma of consensus ledger, computing power, and storage capacity.
- We solve the World Supercomputer trilemma by linking three topologically heterogeneous P2P networks with zero-knowledge proof.
- Consensus: Ethereum will act as the consensus ledger for the World Supercomputer, providing the underlying consensus and using the block interval as the clock cycle for the entire system.
- Storage: Storage rollup will act as a storage network for the World Supercomputer, storing large amounts of data and providing a URI standard to access the data.
- Computation: zkOracle network will serve as the computation network for the World Supercomputer, running resource-intensive computations and generating verifiable proofs of computations.
- Data Bus: Zero-knowledge proof technology will act as the data bus for the World Supercomputer, connecting various components and allowing data and consensus to be linked and verified.
- Consensus: Ethereum will act as the consensus ledger for the World Supercomputer, providing the underlying consensus and using the block interval as the clock cycle for the entire system.
- Storage: Storage rollup will act as a storage network for the World Supercomputer, storing large amounts of data and providing a URI standard to access the data.
- Computation: zkOracle network will serve as the computation network for the World Supercomputer, running resource-intensive computations and generating verifiable proofs of computations.
- Data Bus: Zero-knowledge proof technology will act as the data bus for the World Supercomputer, connecting various components and allowing data and consensus to be linked and verified.

0. World Computer Concept

[

Ethereum: the World Computer

1788×530 114 KB

](https://ethresear.ch/uploads/default/original/2X/d/d5d802e400ac610f0cba5e8f4e688123c67e9ef2.jpeg)

Ethereum was founded on the goal of building a world computer. This vision hasremained unchanged for the past seven years.

According to Vitalik's definition of the classic blockchain trilemma, Ethereum prioritizes decentralization and security over scalability (i.e. performance).

In reality, we need a P2P network as a world computer that solves truly general-purpose intensive computing (especially machine learning and oracle) while preserving the full decentralization of the base layer blockchain.

1. World Computer Difficulty

a) World Computer Trilemma

To create a world computer, we encounter a trilemma based on the basic blockchain network trilemma.

[

World Computer Trilemma

2704×1520 163 KB

](https://ethresear.ch/uploads/default/original/2X/4/4575b957b5630e67b05ba7017d3875525756a761.jpeg)

Different priorities result in different trade-offs:

- Strong Consensus Ledger: Inherently requires repetitive storage and computation and therefore is not suitable for scaling storage and computation.
- Strong Computation Power: Needs to reuse consensus while performing a lot of computation and proof tasks and therefore is not suitable for large-scale storage.
- Strong Storage Capacity: Needs to reuse consensus while performing frequent random sampling proofs of storage and therefore is not suitable for computation.

b) Computation Demand for World Computer

To meet the demand and purpose of a world computer, we expand on the concept of a world computer as described by Ethereum and aim for a World Supercomputer.

World Supercomputer first and foremost needs to do what computing can do today and in addition in a decentralized manner. In preparation for large-scale adoption, developers, for instance, require the World Supercomputer to accelerate the development and adoption of decentralized machine learning for running model inference and verification.

Large models, like MorphAI, will be able to use Ethereum to distribute inference tasks and verify the output from any third party node.

In the case of a computationally resource-intensive task like machine learning, achieving such an ambition requires not only trust-minimized computation techniques like zero-knowledge proofs but also larger data capacity on decentralized networks. These are things that cannot be accomplished on a single P2P network, like classical blockchain.

c) Solution for Performance Bottleneck

In the early development of computers, our pioneers have faced similar performance bottleneck in computer as they made trade-offs between computational power and storage capacity. Consider the smallest component of a circuit as an illustration.

We can compare the amount of computation to lightbulbs/transistors and the amount of storage to capacitors. In an electrical circuit, a lightbulb requires current to emit light, similar to how computational tasks require computational volume to be executed. Capacitors, on the other hand, store electrical charge, similar to how storage can store data.

There may be a trade-off in the distribution of energy between the lightbulb and the capacitor for the same voltage and current. Typically, higher computational volumes require more current to perform computational tasks, and therefore require less energy storage from the capacitor. A larger capacitor can store more energy, but may result in lower computational performance at higher computational volumes. This trade-off leads to a situation where computation and storage cannot be combined in some cases.

[

trade-off

2704×1520 108 KB

](https://ethresear.ch/uploads/default/original/2X/5/55d104423bfb3081c4279d69fd0c03c8f71c8e7e.png)

In the von Neumann computer architecture, it guided the concept of separating the storage device from the central processor. Similar to decoupling the lightbulbs from the capacitors, this can solve the performance bottleneck of the system of our World Supercomputer.

[

von Neumann

2704×1520 118 KB

](https://ethresear.ch/uploads/default/original/2X/9/9dd3acb903b80454acbdea7136f67b8d2ccaf006.png)

In addition, traditional high-performance distributed database uses a design that separates storage and computation. This scheme is adopted because it is fully compatible with the characteristics of a World Supercomputer.

2. World Supercomputer Components

The final World Supercomputer will be made up of three topologically heterogeneous P2P networks: a consensus ledger, computation network, and storage network connected by a trust-minimized bus (connector) such as zero-knowledge proof technology. This basic setup allows the World Supercomputer to solve the world computer trilemma, and additional components can be added as needed for specific applications.

It’s worth noting that topological heterogeneity goes beyond just differences in architecture and structure. It also encompasses fundamental differences in topological form. For example, while Ethereum and Cosmos are heterogeneous in terms of their layers of network and internet of networks, they are still equivalent in terms of topological heterogeneity (blockchains).

[

topological heterogeneity

2704×1520 192 KB

](https://ethresear.ch/uploads/default/original/2X/2/209f0d3833c045044cdfcf6fa8beb505ecbed483.jpeg)

Within the World Supercomputer, a consensus ledger blockchain takes the form of a chain of blocks with nodes in the form of complete graph, while a network like Hyper Oracle network is a ledgerless network with nodes in the form of cyclic graph, and the network structure of storage rollup is yet another variation with partitions forming sub-networks.

We can have a fully decentralized, unstoppable, permissionless, and scalable World Supercomputer by linking three topologically heterogeneous peer-to-peer networks for consensus, computation, and storage via zero-knowledge proof as data bus.

3. World Supercomputer Architecture

Similar to building a physical computer, we must assemble the consensus network, computation network, and storage network mentioned previously into a World Supercomputer.

Selecting and connecting each component appropriately will help us achieve a balance between the Consensus Ledger, Computing Power, and Storage Capacity trilemma, ultimately ensuring the decentralized, high-performance, and secure nature of the World Supercomputer.

The architecture of the World Supercomputer, described by its functions, is as follows:

[

architecture

2704×1522 263 KB

](https://ethresear.ch/uploads/default/original/2X/4/4d1a49b51ed5643f9faa5571cf8429bd99b6da01.png)

The nodes of a World Supercomputer network with consensus, computation, and storage networks would have a structure similar to the following:

[

nodes

2704×1522 171 KB

](https://ethresear.ch/uploads/default/original/2X/6/6049041d7cca54ea140682273ef967d81b742767.jpeg)

To start the network, World Supercomputer’s nodes will be based on Ethereum’s decentralized foundation. Nodes with high computational performance can join zkOracle’s computation network for proof generation for general computation or machine learning, while nodes with high storage capacity can join EthStorage’s storage network.

The above example depicts nodes that run both Ethereum and computation/storage networks. For nodes that only run computation/storage networks, they can access the latest block of Ethereum or prove data redundancy/availability of storage through zero-knowledge proof-based buses like zkPoS and zkNoSQL, all without the need for trust.

a) Ethereum for Consensus

Currently, World Supercomputer’s consensus network exclusively uses Ethereum. Ethereum boasts a robust social consensus and network-level security that ensure decentralized consensus.

[

consensus network

2704×1522 172 KB

](https://ethresear.ch/uploads/default/original/2X/9/9336eaf8f773bd6f55cd35537af3ac49d6f3324a.png)

World Supercomputer is built on a consensus ledger-centered architecture. The consensus ledger has two main roles:

- Provide consensus for the entire system
- Define the CPU Clock Cycle with Block Interval

In comparison to a computation network or a storage network, Ethereum cannot handle huge amounts of computation simultaneously nor store large amounts of general-purpose data.

In World Supercomputer, Ethereum is a consensus network that reaches consensus for computation and storage networks and loads critical data so that the computation network can perform further off-chain computations.

b) Storage Rollup for Storage

Ethereum's Proto-danksharding and Danksharding are essentially ways to expand the consensus network offering temporal availability for large amount data. To achieve the required storage capacity for the World Supercomputer, we need a solution that is both native to Ethereum and supports a large amount of data storage persisted forever.

[

storage network

2704×1522 155 KB

](https://ethresear.ch/uploads/default/original/2X/a/a5887da8c0a1cc7af8fae36c39aaa42e6581fb2a.png)

Storage Rollup, such as EthStorage, is essentially scaling Ethereum for large-scale storage.

Furthermore, as computationally resource-intensive applications like machine learning require a large amount of memory and storage to run on a physical computer, it's important to note that Ethereum cannot be aggressively scaled in both aspects. Storage Rollup is necessary for the "swapping" that allows the World Supercomputer to run compute-intensive tasks.

Additionally, EthStorage provides a web3:// access protocol (ERC-4804), similar to the native URI of a World Supercomputer or the addressing of resources of storage.

c) zkOracle Network for Computation

The computation network is vital in a World Supercomputer as it determines the overall performance. It must be able to handle complex calculations such as oracle or machine learning, and it should be faster than both consensus network and storage network in accessing and processing data.

[

computation network

2704×1522 175 KB

](https://ethresear.ch/uploads/default/original/2X/5/59bcd3834eefa9313cb3c0018dd60caf9e4f2a87.png)

zkOracle Network is a decentralized and trust-minimized computation network that is capable of handling arbitrary computations. Any running program generates a ZK proof, which can be easily verified by consensus (Ethereum) or other components when in use.

Hyper Oracle, a zkOracle Network, is a network of ZK nodes, powered by zkWASM and EZKL, which can run any computation with the proof of execution traces.

A zkOracle Network is a ledgerless blockchain (no global state) that follows the chain structure of the original blockchain (Ethereum), but operates as a computational network without a ledger. The zkOracle Network does not guarantee computational validity through re-execution like traditional blockchains; rather it gives computational verifiability through proofs generated. The ledger-less design and dedicated node setup for computing allow zkOracle Networks, like Hyper Oracle, to focus on high-performance and trust-minimized computing. Instead of generating new consensus, the result of the computation is output directly to the consensus network.

In a computation network of zkOracle, each compute unit or executable is represented by a zkGraph. These zkGraphs define the computation and proof generation behavior of the computation network, just like how smart contracts define the computation of the consensus network.

I. General Off-chain Computation

The zkGraph programs in zkOracle's computation can be used for two major cases without external stacks:

- indexing (accessing blockchain data)
- automation (automate smart contract calls)
- any other off-chain computation

These two scenarios can fulfill the middleware and infrastructure requirements of any smart contract developer. This implies that as a developer of a World Supercomputer, you can create a completely decentralized application through an end-to-end decentralized development process, which includes on-chain smart contracts on the consensus network as well as off-chain computation on the computation network.

II. ML/AI Computation

In order to achieve Internet-level adoption and support any application scenario, World Supercomputer needs to support machine learning computing in a decentralized way.

Also through zero-knowledge proof technology, machine learning and artificial intelligence can be integrated into World Supercomputer and be verified on Ethereum's consensus network to be truly on-chain.

zkGraph can connect to external technology stacks in this scenario, thus combining zkML itself with World Supercomputer's computation network. This enables all types of zkML applications:

- User-privacy-preserving ML/AI
- Model-privacy-preserving ML/AI
- ML/AI with Computational Validity

To enable the machine learning and AI computational capabilities of World Supercomputer, zkGraph will be combined with the following cutting-edge zkML technology stacks, providing them with direct integration with consensus networks and storage networks.

- EZKL: doing inference for deep learning models and other computational graphs in a zk-snark.
- Remainder: speedy machine learning operations in Halo2 Prover.
- circomlib-ml: circom circuits library for machine learning.

e) ZK as Data Bus

Now that we have all the essential components of the World Supercomputer, we require a final piece that connects them all. We need a verifiable and trust-minimized bus to enable communication and coordination between components.

[

data bus

2704×1522 159 KB

](https://ethresear.ch/uploads/default/original/2X/7/7351541cbab7dcec7adf713a90c3227c8cd116b7.png)

For a World Supercomputer that uses Ethereum as its consensus network, Hyper Oracle zkPoS is a fitting candidate for zk Bus. zkPoS is a critical component of zkOracle; it verifies consensus of Ethereum via ZK, allowing Ethereum's consensus to spread and be verified in any environment.

As a decentralized and trust-minimized bus, zkPoS can connect to all components of World Supercomputer with very little verification computation overhead with the presence of ZK. As long as there is a bus like zkPoS, data can flow freely within World Supercomputer.

When Ethereum's consensus can be passed from the consensus layer to the Bus as World Supercomputer's initial consensus data, zkPoS with state/event/tx proofs can prove it. The resulting data can then be passed to the computation network of zkOracle Network.

As a decentralized and trust-minimized bus, zkPoS can connect all components of World Supercomputer with minimal verification computation of ZK. With a bus like zkPoS, data can flow freely within World Supercomputer.

In addition, for storage network's bus, EthStorage is developing zkNoSQL to enable proofs of data availability, allowing other networks to quickly verify that BLOBs have sufficient replicas.

f) Workflow

[

workflow

2704×1522 91 KB

](https://ethresear.ch/uploads/default/original/2X/f/fb5140a29b0e636b278a42f7edcfbc80fb1ee2b9.jpeg)

Here's an overview of the transaction process in Ethereum-based World Supercomputer, broken down into steps:

- Consensus: Transactions are processed and agreed upon using Ethereum.
- Computation: The zkOracle Network performs relevant off-chain calculations (defined by zkGraph loaded from EthStorage) by quickly verifying the proofs and consensus data passed by zkPoS acting as a bus.
- Consensus: In certain cases, such as automation and machine learning, the computation network will pass data and transactions back to Ethereum or EthStorage with proofs.
- Storage: For storing large amounts of data (e.g. NFT metadata) from Ethereum, zkPoS can act as an optional trust-minimized messenger between Ethereum and EthStorage.

Throughout this process, the bus plays a vital role in connecting each step:

- When consensus data is passed from Ethereum to zkOracle Network's computation or EthStorage's storage, zkPoS and state/event/tx proof generate proofs that the recipient can quickly verify to get the exact data such as the corresponding transactions.
- When zkOracle Network needs to load data for computation from storage, it accesses the addresses of data on storage from consensus network with zkPoS, then fetches actual data from storage with zkNoSQL.
- When data from zkOracle Network or Ethereum needs to be displayed in the final output forms, zkPoS generates proofs for the client (e.g., a browser) to quickly verify.

5. Conclusion

Bitcoin has established a solid foundation for the creation of aWorld Computer v0, successfully building a "World Ledger".

Ethereum has subsequently demonstrated the "World Computer" paradigm by introducing a more programmable smart contract mechanism.

The World Supercomputer is designed to extend and advance the existing decentralized network. We envision it unlocking the potential of Ethereum and enabling exploration of new scenarios.