EchoLink Protocol - High Performance Secure Decentralized Professional Network Through Zero Knowledge Homomorphic Smart Contract and Rollup Blockchain

EchoLink Team

contact@echolink.tech

GitHub: https://github.com/EchoLinkTech

Abstract

EchoLink Protocol provides innovative, high speed, and secure professional network on blockchain. EchoLink Protocol achieves efficient and fast execution through a rollup blockchain architecture. In addition, EchoLink Protocol provides users with privacy preserving smart contract capability through homomorphic encryption. Privacy preserving smart contracts removes one of the major concerns by blockchain users and enables the wide adoption of decentralized social network functionalities for real world use cases.

EchoLink Protocol is composed of a rollup blockchain infrastructure and privacy preserving smart contract system that is fully compatible with the Ethereum Virtual Machine. The EchoLink Rollup Blockchain provides a theoretical transaction throughput of over 40,000 TPS, and thus fully capable of real world applications. The EchoLink Privacy Preserving Smart Contract system offers full EVM compatibility and portability from existing Ethereum ecosystem.

Figure 1: EchoLink = Rollup Blockchain + Privacy Preserving Smart Contracts for Web3 Professional Network

Contents

List of Figures

1 Introduction

Web 3.0 technology is poised to revolutionize teaching and learning processes by harnessing tools like AI, Metaverse Blockchain, and IoT to streamline access to knowledge globally. With these advancements, teachers can create engaging assignments and provide immersive learning experiences using technologies like holoportation and holographic sharing. Learners will become active participants in content creation, developing not only subject-specific knowledge but also critical thinking and practical skills. These innovations offer a rich online teaching experience, where students can explore virtual spaces and interact with educational content in new ways.

Decentralized web technology in Web3 will save time for both educators and learners by automating processes and providing tailored search results. Teachers can access built-in tools to create student-centric study materials, analyze performance data quickly, and generate detailed progress reports. Additionally, the decentralized nature of Web3 enables learners to create secure, validated portfolios of their educational achievements, including micro-credentials, NFTs, and research papers, stored on Blockchain for authenticity.

Web3 introduces the concept of decentralized education, where learners have control over their credentials and participate in collaborative projects, internships, and peer-to-peer mentoring. This system fosters the development of educational DAOs that share power and value among participants, offering financial incentives for contributions and recording transactions on Blockchain. Learners can also explore earning opportunities through activities like NFT creation, supported by Web3's 'earn as you learn' concept.

The surge of micro-schooling and homeschooling, accelerated by the pandemic, will continue to gain traction with Web3, facilitating an interconnected network between parents, teachers, and students. Digital diplomas stored securely on Blockchain empower individuals to control and share their academic achievements conveniently. Platforms like EduDAO and LearnWeb3 further revolutionize education by empowering learners to own and control their educational data, fostering personalized learning experiences and enhancing transparency and accountability in the education system.

Web3 democratizes access to education, offering diverse learning resources and fostering global connections among learners. Students can shape their own educational paths, supported by efficient search tools, micro-credentials, and personalized learning journeys. With hands-on experiences and gamified learning opportunities, Web3 equips students with the skills needed for success in modern, technology-driven industries. Educational NFTs ensure fair compensation for creators and secure access to educational materials, ushering in a new era of learning experiences in the digital age.

2 EchoLink EKO - Web3 Learning and Professional Community

EchoLink applies Web3 technologies to revolutionize the education sector with several transformative features:

Artificial Intelligence (AI) : Web3 education platforms utilize AI algorithms to personalize learning experiences, offering tailored content and adaptive assessments based on individual student needs and learning styles, resulting in more effective learning outcomes.

Virtual Reality (VR) : Integration of VR in Web3 education provides immersive and experiential learning environments, allowing students to explore historical sites, scientific concepts, and realistic simulations, enhancing understanding and retention of knowledge.

Internet of Things (IoT) : Web3's integration with IoT enables smart classrooms and connected educational devices, fostering interactive learning, collaboration, and real-time feedback through devices like interactive whiteboards and smart wearables.

Decentralization : Core to Web3 is decentralization, which eliminates intermediaries and gives students and educators greater control over their educational journey, fostering a more open and equitable educational ecosystem.

2.1 Benefits of Web3 Education include:

Low Cost : By leveraging blockchain technology, Web3 education reduces administrative costs and streamlines tasks, while smart contracts automate credential verification, saving time and money.

Smart Searches : Advanced AI-powered search engines enable efficient access to relevant information, improving learning outcomes by saving time and providing accurate resources.

Improved Methods : VR, AR, and IoT technologies offer immersive learning experiences, making complex concepts easier to understand and facilitating experiential learning with real-world objects and scenarios.

Customized Content : Web3 platforms deliver personalized learning experiences by tailoring content to individual interests and learning styles, analyzing student data to provide customized materials.

Time-saving : Accessible anytime, anywhere, Web3 education allows for self-paced learning, eliminating time constraints and balancing education with other commitments.

Collaborative Learning : Web3 fosters global collaboration among students and educators through decentralized platforms, promoting peer-to-peer learning and knowledge sharing.

2.2 Use cases of Web3 in Education:

Distributed Autonomous Organizations (DAOs) : Blockchain-enabled DAOs redefine educational institutions by enabling transparent decision-making, community governance, and collective ownership, empowering stakeholders to shape educational direction collaboratively.

Blockchain-powered Credentials : Web3 enhances credential credibility and verifiability by securely storing and sharing achievements, ensuring authenticity and eliminating fraudulent certifications.

Virtual Reality (VR) and Immersive Learning : VR simulations and virtual environments offer interactive learning experiences, enabling exploration of complex concepts and real-world scenarios.

Peer-to-Peer Learning and Collaboration : Web3 empowers students to connect and learn from one another, fostering collaboration, community, and critical thinking skills.

Blockchain-based Content Creation and Distribution : Blockchain platforms enable collaborative content creation and sharing, promoting open educational practices and comprehensive, up-to-date content repositories.

2.3 Challenges

While Web3 education and professional network brings about unprecedented efficiency and convenience to the education and professional development industries and the overall economy, challenges exist to its wider adoption on an Internet scale.

One of the most prominent hindrances to the wider adoption of web3 education and professional network is privacy of transaction data. Blockchain based smart contract transactions are inherently open and available to public inspection. While this provides advantages such as transparency and accountability, it causes potential issues, such as front-running a large pending transaction by blockchain validators and inability to preserve privacy of transactions. EchoLink Protocol is designed to mitigate these challenges by solving the privacy issues associated with smart contract and blockchain data storage and enable the wider adoption of web3 education and professional network.

3 EchoLink Protocol

EchoLink Protocol aims to provide solutions to the challenges faced by web3 education and professional network by making available a privacy preserving smart contract system and rollup blockchain to the community.

Homomorphic encryption based privacy preserving smart contract system offers privacy of transaction data while preserving all the benefits of smart contract based financial transactions. Rollup blockchain offers high transaction speed and throughput suitable for real world financial transactions. [2]

3.1 Homomorphic Encryption and Privacy Preserving Smart Contract

Ensuring data privacy is a critical concern for smart contracts handling sensitive information. EchoLink Protocol adopts the ZeeStar system, a language and compiler that allows non-experts to create private smart contracts and perform operations on external data. The ZeeStar language enables developers to specify privacy constraints conveniently using zkay's privacy annotations. The ZeeStar compiler then guarantees the realization of these constraints by combining non-interactive zero-knowledge proofs and additively homomorphic encryption. ZeeStar is practical, as it prepares transactions for our contracts in at most 54.7 seconds, at an average cost of 339,000 gas.[2]

3.2 Rollup Blockchain

Practical usage of web3 education and professional network requires user experiences similar to that of traditional financial transactions. To achieve such an end, EchoLink Protocol employs a rollup blockchain architecture compatible with the EVM smart contract ecosystem. The EchoLink Rollup Blockchain is built on top of Arbitrum Rollup Stack, which has been proven in real world financial transactions. [1]

Armed with two key innovative features, privacy preserving smart contract based on homomorphic encryption and EVM equivalent rollup blockchain, EchoLink Protocol brings privacy and speed to real world asset transactions, and provides user experiences meeting real world expectations. [1]

4 Technical Implementation

Overview EchoLink Protocol consists of two major components:

1. EchoLink Privacy Smart Contact system - EPSC
2. EchoLink Rollup Blockchain - ERB

EchoLink Privacy Smart Contact system - EPSC is built on ZeeStar. EPSC consists of an expressive language to specify and a compiler to automatically enforce data privacy for smart contracts. EPSC not only supports homomorphic addition, but also multiplication for most combinations of owners. This allows expressing complex applications such as oblivious transfer. Furthermore, EPSC can mix homomorphic and non-homomorphic encryption schemes and is provably private.[2]

EchoLink Rollup Blockchain - ERB is a rollup based public blockchain, and can be deployed either as a layer 2 or layer 3 blockchain depending on how transactions are settled. ERB utilizes the Arbitrum technical stack customized and optimized for Real World Asset based financial transactions. EchoLink Rollup Blockchain utilizes the DYMO ERC20 token as form of payment for transaction fees. [1]

4.1 EchoLink Privacy Smart Contact with Homomorphic Encryption

A. Non-interactive Zero-knowledge Proofs A non-interactive zero-knowledge (NIZK) proof enables a prover to convince a verifier that she possesses a secret without disclosing the secret itself. Specifically, she can demonstrate knowledge of a secret witness w that satisfies a given predicate $\phi(w;x)$ for some public value x, without revealing any information about w other than the fact that $\phi(w;x)$ holds. Here, ϕ is referred to as the proof circuit, w is the private input, and x is the public input.

For instance, in a cyclic group G with generator g and $h \in G$, one can prove knowledge of the discrete logarithm z of h with respect to base g using the proof circuit $\phi(z;h)$, which is satisfied if and only if $g^z = h$.

Zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) are a type of generic NIZK proof construction that supports any arithmetic circuit ϕ and offers constant-cost proof verification proportional to the size of ϕ (plus a typically negligible linear cost in the size of x). Due to their efficient verification costs, zk-SNARKs are commonly utilized on the Ethereum blockchain.[2]

B. Additively Homomorphic Encryption An additively homomorphic encryption scheme enables the addition of plaintexts corresponding to a pair of ciphertexts without requiring knowledge of private keys. Formally, let pk_α and sk_α be the public and private keys of a party α, respectively, and $Enc(x, pk_\alpha, r)$ represent the encryption of plaintext x under pk_α using randomness r. This scheme is additively homomorphic if there exists a function $\oplus$ on ciphertexts such that for all x, y, α, r, r_0:

$$Enc(x, pk_\alpha, r) \oplus Enc(y, pk_\alpha, r_0) = Enc(x+y, pk_\alpha, r_{00})$$

for some r_{00}, where $\oplus$ can be efficiently evaluated without knowledge of sk_α. It's important to note that both arguments to $\oplus$ must be encrypted under the same public key. Typically, additively homomorphic schemes also allow the homomorphic evaluation of subtraction using a function defined analogously.

For instance, the Paillier encryption scheme is additively homomorphic in Z_n (i.e., addition in Eq. (1) is modulo n) for an RSA modulus n, and exponential ElGamal encryption over a group G is additively homomorphic in $Z_{|G|}$, where $|G|$ is the order of G (see App. B).[2]

Privacy Annotations and Types. To facilitate precise and user-friendly specification of privacy constraints, ZeeStar utilizes privacy annotations inspired by zkay. These annotations track ownership of values within a privacy type system: Data types τ (such as integers and booleans) are extended to types of the form $\tau@\alpha$, where α determines the owner of the expression. The value of an expression can only be accessed by its owner. The owner α may be "all" (indicating the value is public) or an expression of type address. Expressions with owner "me" are referred to as self-owned, while those with owner $\alpha \notin \{me, all\}$ are considered foreign.

To prevent implicit information leaks, private expressions with owner α cannot be directly assigned to variables with a different owner $\alpha_0 \neq \alpha$. Instead, developers can use the $reveal(e,a)$ function to explicitly disclose a self-owned expression e to another owner a.

It's important to note that the privacy annotations entail minimal overhead compared to existing non-private smart contract languages such as Solidity. As discussed further, privacy is automatically enforced by ZeeStar's compiler, eliminating the need for developers to manually instantiate cryptographic primitives.[2]

Compilation. ZeeStar compiles the input contract into an executable Ethereum contract that enforces the specified privacy constraints.[2]

In the output contract, values with an owner $\alpha \neq$ "all" are encrypted under the public key of α using an additively homomorphic encryption scheme. Private expressions are precomputed locally (off-chain) by the sender and only published on the blockchain (on-chain) in encrypted form. Expressions revealed to all are additionally published in plaintext.[2]

In essence, any expression involving only public and self-owned variables is computed by the sender as follows: First, decrypt any private input variables. Then, evaluate the expression using the plaintext arguments. Finally, if the expression is private, encrypt the result using the owner's public key.[2]

Leveraging Homomorphic Encryption. As the encryption scheme used by ZeeStar is additively homomorphic, it also permits the evaluation of expressions. First, the sender re-encrypts the plaintext value val under the public key of to to obtain a ciphertext c. Then, the sender computes bal. In the proof circuit ϕ, ZeeStar ensures that c is computed correctly. Interestingly, the operation $\oplus$ is also evaluated within the proof circuit. While not necessary for privacy, this practice leads to reduced on-chain costs. Additionally, as we will discuss shortly, it allows for greater expressivity.[2]

After constructing ϕ, ZeeStar inserts a proof verification statement into the output contract. When calling the transfer function, the sender must generate and provide a NIZK proof for the circuit ϕ as a function argument proof. The public arguments of ϕ are provided as arguments to verify. If verification fails, the transaction is rejected, and the contract state is reverted.[2]

4.2 EchoLink Rollup Blockchain

The EchoLink Rollup Blockchain is constructed on the Arbitrum technology stack, which addresses limitations commonly found in layer 1 smart contract systems. Arbitrum introduces a novel approach to overcome these limitations.[1]

Arbitrum contracts are highly cost-effective for verifiers to handle. When participants act in line with incentives, Arbitrum verifiers only need to verify a small number of digital signatures for each contract. Even in cases where parties deviate from their incentives, Arbitrum verifiers can efficiently resolve disputes regarding contract behavior without needing to inspect more than a single instruction execution by the contract.[1]

Additionally, Arbitrum enables contracts to execute privately, disclosing only hashed versions of contract states. EchoLink utilizes the Arbitrum technology stack as the foundation of its Rollup Blockchain. Moreover, the EchoLink Protocol customizes and optimizes the Arbitrum stack for web3 education and professional service operations.[1]

EchoLink Rollup Blockchain is further optimized for web3 education and professional network by providing customized middle-ware modules and precompiled smart contacts, including sub-block time data API. [1]

4.3 EchoLink Protocol - Privacy and High Performance for web3 education and professional network

Armed with privacy preserving smart contract and rollup blockchain, EchoLink Protocol solves two of the major hurdles hindering the wide adoption of decentralized finance transactions for web3 education and professional service, data privacy and transaction speed and throughput.

Privacy preserving smart contracts are usually computationally intensive. This translates into high gas consumption and fees in blockchain ecosystem. EchoLink Rollup Blockchain solves these drawbacks with a highly efficient and low cost EVM compatible ledger.

Together with privacy preserving smart contract and rollup blockchain, EchoLink Protocol offers community a viable and robust solution to bring web3 education and professional service and related content creation transactions to an industry scale.

5 EchoLink Protocol Economic System and Governance

EchoLink Rollup Blockchain utilizes the ERC20 token, EchoLinkV2 EKO, as a payment method for transaction fees. A portion or all of the transaction fees may be distributed to verifiers of transactions. A portion of the transactions fees may also be burned based on community decision.

Community decisions are based on votes by community members. Community members may vote in proportion of the number of EchoLinkV2 Token owned for a proposal.

6 Conclusion

EchoLink Protocol is a high performance, low cost, and privacy preserving system optimized for web3 education and professional service. Through innovative homomorphic encryption and rollup blockchain technologies, EchoLink Protocol provides the necessary technological foundation for the wide adoption of web3 education and professional service and related transactions.

6.1 Future Work

We plan to further strengthen the EchoLink system by focusing on the following areas:

- Production grade privacy preserving smart contract templates
- Real world data integration services

6.2 Acknowledgements

We would like to acknowledge 1) ETH and ZeeStar for providing the foundation for EchoLink Privacy Preserving Smart Contract system. 2) Arbitrum for providing the foundation for EchoLink Rollup Blockchain.

6.3 Whitepaper Versions

- EchoLinkV2 v. 1.0 – Jan. 2024, initial release

6.4 Code Base

Codebase: `https://github.com/EchoLinkTech`

References

[1] Xiaoqi Chen S. Matthew Weinberg Edward W. Felten Harry Kalodner, Steven Goldfeder. Arbitrum: Scalable, private smart contracts. `https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kalodner.pdf`, 2018.

[2] ROGER BAUMGARTNER MARTIN VECHEV SAMUEL STEFFEN, BENJAMIN BICHSEL. Zeestar: Private smart contracts by homomorphic encryption and zero-knowledge proofs. `https://www.sri.inf.ethz.ch/publications/steffen2022zeestar`, 2022.