Note: This is an initial draft of the proposal. The content will be refined and updated based on community feedback and discussions. Your input is crucial in shaping the final version.

Abstract

This AIP seeks funding for the development & integration of zkFetch, a zero-knowledge proof-based data fetching service, into the Arbitrum ecosystem. zkFetch will provide cryptographically verifiable, privacy-preserving oracle solution for any off-chain data, enhancing Arbitrum Ecosystems DApp's security and enabling innovative use cases like Prediction Markets, RWA and AI requiring trust and transparency.

Motivation

The integration of zkFetch into Arbitrum addresses some of the important challenges in the current web3 landscape while opening up new possibilities for the ecosystem:

Enhancing Oracle Security and Privacy:

- In web3, the Current oracle systems lack robust cryptographic verifiability and privacy preservation. This exposes DApps to manipulation risks and limits the integration of sensitive real-world data.
- zkFetch provides a zero-knowledge proof-based solution, offering unparalleled security and privacy.

Overcoming Existing Trade-offs:

- Traditional oracle solutions often compromise between security, privacy, and flexibility. These trade-offs restrict the types of off-chain data that can be reliably integrated.
- zkFetch's unique approach allows for secure, private, and flexible data integration without compromises.

Attracting Developers and Projects:

- By offering a zkTLS-powered oracle solution, Arbitrum can attract more developers and projects to its ecosystem. The enhanced security and privacy features will appeal to projects dealing with sensitive data or complex financial applications. This influx of talent and projects can significantly boost Arbitrum's ecosystem growth and diversity.

Enabling New Use Cases:

- zkFetch's ability to securely integrate any off-chain data opens up possibilities for innovative applications.
- Potential new use cases include:
- Dapps with cryptographically verified, temper-proofs price feeds.
- Verifiable real-world asset (RWA) tokenization
- Prediction Markets on any off-chain data integrations
- Dapps with cryptographically verified, temper-proofs price feeds.
- Verifiable real-world asset (RWA) tokenization
- Prediction Markets on any off-chain data integrations

Positioning Arbitrum as a Leader in L2 Innovation:

- Implementing zkFetch showcases Arbitrum's commitment to adopting new technology like zkTLS. Early adoption of zkTLS-powered oracle technology can give Arbitrum a competitive edge in the L2 space.

Facilitating Institutional Adoption:

- The enhanced privacy and security features of zkFetch can make Arbitrum more appealing to institutional players. This can potentially lead to increased liquidity and more sophisticated financial products on the platform.

Rationale

The integration of zkFetch aligns perfectly with Arbitrum's mission to provide a secure, scalable, and developer-friendly Layer 2 solution. Here's how zkFetch's unique features support Arbitrum's core values and objectives:

Enhanced Security without Compromising Performance:

- zkFetch's zkTLS infrastructure provides cryptographic guarantees for data integrity.
- Zero-knowledge proofs are generated in less than 4 seconds, even on low-compute devices, ensuring that Arbitrum's high-performance standards are maintained.
- This rapid proof generation allows for real-time, secure data updates without exposing API keys critical for Dapps on Arbitrum.

Scalability and Flexibility:

- zkFetch is compatible with any HTTPS endpoint, allowing Arbitrum to easily scale its oracle capabilities to any data source.
- The ability to generate data proofs for any reputed and trusted data providers ensures that Arbitrum can quickly adapt to new data needs.
- This flexibility supports Arbitrum's goal of being a versatile platform for a wide range of DApps.

Privacy-Preserving Operations:

- zkFetch enables the use of private API keys and sensitive endpoints without on-chain exposure.
- This aligns with Arbitrum's commitment to user privacy and opens up possibilities for handling confidential data in DeFi operations.

Developer-Friendly Integration:

- zkFetch's can seamlessly embeds in both Web2 and Web3 applications, lowering the barrier for developers to build on Arbitrum.
- No plugins or additional apps are required on the user-end, simplifying the development and user experience.

Proven Track Record:

- zkFetch leverages zkTLS Infrastructure by Reclaim Protocol, that has been successfully deployed on multiple chains (30+) including Arbitrum, Sui, Polygon, Solana, Optimism, Base and many others, also integrated with Ethereum Attestation Services.
- Within a span of one year, over 20 projects in production have already integrated this zkTLS infrastructure, building innovative use cases such as DID, Proof of Personhood, RWA, prediction markets, and more.

Future-Proofing the Oracle System:

- The modular design of zkFetch ensures adaptability to Arbitrum's evolving architecture.
- The underlying zero-knowledge proof system can be updated to more efficient protocols as technology advances, without requiring major changes to the Arbitrum infrastructure.

Expanding Use Cases:

- zkFetch's capability to handle various data types beyond crypto price feeds (e.g., Sport Data, News, Global Bonds, Commodities Prices) opens up new possibilities for innovative DApps on Arbitrum.
- This aligns with Arbitrum's goal of being a comprehensive platform for diverse blockchain applications.

By integrating zkFetch, Arbitrum not only enhances its oracle capabilities but also solidifies its status as a leading, secure, and developer-friendly Layer 2 solution. The synergy between zkFetch's features and Arbitrum's objectives guarantees that this integration will create substantial value for the entire ecosystem.

Key Terms

- zkFetch: A library that extends standard HTTP fetch operations with zero-knowledge proof components.
- zkTLS: An infrastructure that secures communication during the handshake mechanism in Transport Layer Security (TLS), provided by Reclaim Protocol.
- Zero-Knowledge Proofs (ZKPs): Cryptographic methods allowing one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself.

Specifications

zkFetch is a library that extends the functionality of a standard HTTP fetch operation by adding a ZKP component. It is built on top of the Reclaim Protocol, which provides the underlying infrastructure(Open-source) for generating and verifying zero-knowledge proofs. It can fetch data from any remote resources and generate a cryptographic proof of the fetch operation and its result, without revealing sensitive information like API keys or private headers.

Key Components -

Secure Data Retrieval:

- Initiates HTTPS requests to any specified endpoint
- Employs custom TLS implementation for secure communication
- Supports various HTTP methods and custom headers

Decentralized Proxy Witnessing:

- Routes requests through HTTP Proxies for additional security
- Mitigates man-in-the-middle attack risks

Zero-Knowledge Proof Generation:

- Utilizes Reclaim Protocol to create proofs of data integrity, source authenticity, and parameter correctness

On-chain Verification:

- Enables efficient verification of proofs directly on the Arbitrum.

[

image

777×630 16.8 KB

](https://global.discourse-cdn.com/flex029/uploads/arbitrum1/original/2X/9/994e1ed36663c753c676930dd7636e98d7cd405e.png)

Our approach with zkFetch is driven by several key factors:

1. Zero-Knowledge Proofs (ZKPs)

: We chose to leverage ZKPs because they offer a unique combination of data integrity and privacy. This allows us to verify the authenticity of data without revealing sensitive information, addressing a critical gap in current oracle solutions.

1. HTTP Extension:

By extending standard HTTP fetch operations, we ensure compatibility with existing web infrastructure while adding cryptographic guarantees. This approach allows for easy integration with a wide range of data sources without requiring significant changes to their existing systems.

1. Decentralized Proxy Witnessing:

Routing requests through HTTP Proxies adds an extra layer of security and decentralization. This mitigates risks associated with centralized oracle systems and enhances resistance to manipulation attempts.

1. Flexibility in Data Sourcing:

Our agnostic approach to data sources, supporting any HTTPS endpoint, maximizes the potential use cases for zkFetch. This flexibility is crucial for the diverse needs of the Arbitrum ecosystem.

1. Cross-Chain Compatibility:

Designing zkFetch to work across various blockchains ensures that Arbitrum can easily interact with other ecosystems, promoting interoperability and expanding the potential for cross-chain applications.

1. Customizable Proof Parameters:

This feature allows developers to tailor the security and compliance aspects of data fetching to their specific needs, enhancing the versatility of the solution.

We have already developed a DataDao, testing zkFetch’s capabilities with various data feed APIs, demonstrating our readiness to adapt the technology for Arbitrum. We are aiming to become the nexus for acquiring diverse, cryptographically verified, tamper-proof, and highly secure data across Web2 and Web3 ecosystems.

Our project depends on the Reclaim Protocol, specifically itsattestor network, to verify that data is received from the correct source. This dependency is essential because:

1. The Reclaim Protocol's attestor network is a core component of zkFetch's security model, ensuring the integrity and authenticity of fetched data
2. It provides the infrastructure for generating and verifying zero-knowledge proofs, which is crucial for zkFetch's privacy-preserving feature
3. The attestor network helps in maintaining the decentralized nature of the oracle system, enhancing its reliability and resistance to manipulation

The Reclaim Protocol's zkTLS infrastructure is integral to zkFetch's core functionality, providing a unique and irreplaceable foundation for secure data fetching. This established system offers unparalleled expertise in zero-knowledge proofs and decentralized attestation, making it essential for delivering a robust, tamper-resistant oracle solution on Arbitrum.

Steps to Implement

Milestone 1:

Research & Development Phase (6-8 Weeks)

- Adapt zkFetch for Arbitrum's architecture
- Develop and deploy specific smart contracts to handle data feed responses from various providers, ensuring they can publish proofs on-chain
- Effectively deploy Semaphore Contracts
- Optimize zkProof generation and verification
- Integrate with multiple data providers to demonstrate the capabilities of zkFetch.
- Estimated cost: $30,000

Milestone 2:

Testing and Documentation (4-5 Weeks)

- Comprehensive unit testing of core functions to ensure functionality and robustness
- Create detailed developer documentation and test guides
- Estimated cost: $10,000

Milestone 3:

Community Engagement and Marketing (2-4 Weeks)

- Publish a blog post and host a community call to detail zkFetch Oracle solution and its benefits to the Arbitrum ecosystem
- Initiate co-marketing efforts with Arbitrum to help onboard projects & Developers to integrate zkFetch in their applications.
- Estimated cost: $2,000

Milestone 4:

Integrate Diverse Data feeds (6-7 weeks):

- Adding APIs for data feeds like crypto prices, sport data, and others.
- Target to integrate at least 5-6 high-quality data providers initially.
- Estimated cost: $10000

Milestone 5:

Mainnet Deployment and Support (5-6 weeks):

- Conduct final testing and deploy to Arbitrum mainnet
- Integrate with 2 DApps from the Arbitrum ecosystem, focusing on use cases like Prediction Markets, RWA tokenization, and others
- Provide continuous development support post-integration, led by Integration Support Developer from Reclaim
- Estimated cost: $10,000

After successful integration and completion of all milestones, we will implement the following monthly budget to ensure the sustainability of the zkFetch oracle service:

- To keep the oracle service running after covering all the milestones, we will require funding of $10,000 per month for the next 4 quarters. This fund will help us cover various data feed APIs subscriptions, zkFetch development, research and maintenance. We will be sharing monthly reports detailing how this budget is being used and the ongoing developments of zkFetch.

We request co-marketing support from Arbitrum to:

- Promote the zkFetch oracle solution to Arbitrum Ecosystem and developers
- Highlight the unique value proposition of cryptographically verified data feeds in joint marketing materials
- Facilitate introductions to key projects and data providers in the Arbitrum ecosystem

By implementing zkFetch and integrating reputable data providers for diverse data sources, we aim to establish Arbitrum as the go-to platform for secure, verifiable real-world data in the blockchain space, driving significant ecosystem growth and innovation.

Timeline

- Milestone 1 (Research & Development): 6- 8 Weeks
- Milestone 2 (Testing and Documentation): 4-5 Weeks
- Milestone 3 (Marketing & Community Engagement): 2-4 Weeks
- Milestone 4 (Integrate Diverse Data feeds): 6-7 Weeks
- Milestone 5 (Mainnet Deployment and Support): 4-6 weeks

To accomplish the milestones outlined above, the entire project will require 1 Project Manager, 3 Developers, 1 BD manager, 1 Dev Relations Lead, and 1 Integration Support Developer.

Overall Cost

Total Cost: $62,000 (Covering all the milestones) + $10,000 per month (recurring cost)

Breakdown:

- Development: $30,000
- Testing and Documentation: $10,000
- Marketing & Community Engagement: $2000
- Integrate Diverse Data feeds: $10000
- Mainnet Deployment and Support: $10,000
- Monthly budget after covering all the milestones: $10,000 per month

Ongoing maintenance and developer support will be provided by the Reclaim Protocol team as part of their commitment to the zkFetch.

Revenue-Sharing Model

To ensure a mutually beneficial partnership and incentivize long-term collaboration, we propose a two-tier revenue-sharing model with the DAO based on the volume of data fetches processed through zkFetch in the Arbitrum ecosystem:

- 3% revenue share per month

for up to 250K data fetches

.

- 10% revenue share per month

for volumes exceeding 250K data fetches

.

This model allows for sustainable growth during the early stages of development while ensuring that as adoption scales, Arbitrum benefits proportionally from zkFetch's success. We believe this approach aligns our long-term goals with the Arbitrum ecosystem's growth and will enable us to contribute meaningfully to the broader community.

Team

zkFetch leverages the zkTLS infrastructure developed byReclaim Protocol, a project led by the team at CreatorOS Inc. We are a 35+ member engineering and web3 product development & research team including ZKP researchers and with previous affiliations to Stanford, Microsoft, Meta and Google . We have also built - Questbook.app, an industry leading on-chain grants management tool that is used by some of the major L1/L2s including Polygon, Arbitrum, Solana, Compound, Ton, among others. CreatorOS is a YC W21 company.

- Madhavan Malolan : CEO
- Building in crypto since 2016.
- Among first 5 contributors to Plasma (ethereum scaling solution) specifications.
- Open source contributor.
- ex-Microsoft, Computer Science IIIT-H.
- LinkedIn. Github
- Building in crypto since 2016.
- Among first 5 contributors to Plasma (ethereum scaling solution) specifications.
- Open source contributor.
- ex-Microsoft, Computer Science IIIT-H.
- LinkedIn. Github
- Max Allman, Mechanism Design Researcher
- PhD from Stanford in Mechanism Design and Game Theory
- Co- author of the Reclaim Whitepaper
- PhD from Stanford in Mechanism Design and Game Theory
- Co- author of the Reclaim Whitepaper
- Kirill Kutsenok, Cryptography & Security Researcher
- Adhiraj Singh: Lead Developer
- Aleksai Ermishkin: Lead Blockchain Developer

I warmly invite all members of our vibrant Arbitrum community to share your thoughts on this zkFetch integration proposal. I'm eager to engage in discussions and address any points you raise.

Relevant Sources:

GitLab

Integrations / Offchain / Zk Fetch · GitLab

GitLab Enterprise Edition

reclaimprotocol.org

Reclaim Protocol

Reclaim Protocol creates digital signatures, known as zero knowledge proof, of users' identity and reputation on any website.

GitHub

Reclaim Protocol

Reclaim Protocol has 29 repositories available. Follow their code on GitHub.

Social