Unmarshal’s Decentralised Indexer Network: Transitioning to a Community-Owned AVS-Based Hybrid Blockchain

Abstract

Unmarshal has consistently set the benchmark for innovative indexing services in the blockchain space. We are now embarking on a transformative journey: transitioning to a decentralized indexer network. This white paper outlines our strategic shift, which is built upon a robust hybrid blockchain model.

In the near future, we will announce the specific platform that will power our decentralized network. Our new architecture will incorporate a multi-layered node system, featuring operator nodes that manage offline indexers, validators who commit proofs to the blockchain, and proofreaders who provide an additional layer of validation. This structure ensures the highest levels of data accuracy and reliability.

In response to the increasing demand for indexed data across more than 45 blockchain networks, our initiative aims to fully decentralize Unmarshal’s stack, fostering a community-driven approach. By integrating a cutting-edge architecture, we will achieve unparalleled scalability, enhanced security, and superior reliability. This white paper will detail the innovative architectural changes, operational dynamics, and governance model that will empower our community and redefine the landscape of blockchain data services.

Introduction

Unmarshal commenced as a centralized indexing service designed to cater to the expansive needs of blockchain applications. Guided by a vision to gradually decentralize the Unmarshal ecosystem, we aimed to bolster transparency and community engagement. Significant strides have been made toward this objective, including the pivotal implementation of the Unmarshal Governance Model.

We now embark on our most ambitious transformation yet—the full decentralization of our indexing services and operational frameworks. This transition leverages an Actively Validated Services (AVS) based hybrid decentralization model, marking a critical evolution in our journey. This initiative is driven by a desire to empower our supportive community that has grown over the last three years.

This strategic shift enhances the robustness, scalability, and security of our services, ensuring that we continue to uphold high standards while also paving the way for increased community ownership and involvement. In the decentralized framework we envision, all indexing operations will be managed by a consortium of decentralized operators, each a staked participant with a vested interest in maintaining the performance and reliability standards that have become synonymous with Unmarshal.

Decentralised Operations Management

Staked Operators

- **Security Deposit**: Operators within the network are required to stake tokens as a security deposit, aligning their interests with the integrity and efficiency of the service. This mechanism also serves as a quality control measure, penalizing operators who fail to meet the network's performance requirements.

Decentralised Execution

- **Global Distribution**: Indexing tasks are carried out globally by various operators, enhancing redundancy and eliminating single points of failure. This distributed approach significantly increases data processing robustness and availability.

Advanced API Routing and Tracking System

API Management

- **Decentralized API Layer**: To optimize response times and balance loads, Unmarshal will implement a decentralized API management layer that intelligently routes queries to the most appropriate indexer node.

Tracking System

- **Performance Monitoring**: A sophisticated tracking system will monitor each node's performance and health, ensuring transparency and accountability. This system provides real-time data on node performance, crucial for maintaining service level agreements (SLAs) and ensuring user satisfaction.

Through these strategic and operational enhancements, Unmarshal's transition to a decentralized indexing network is set to reshape our operational model to be more resilient, transparent, and community-focused. This restructuring not only utilizes blockchain technology for its inherent benefits but also redefines our engagement with the community, allowing them direct involvement in governance and operational execution, which is fundamental for nurturing a truly decentralized ecosystem.

Problem Statement

Scalability Issues

- **Demand Growth**: As the number of blockchain networks and decentralized applications (dApps) expands, centralized indexing services struggle to scale, impacting their ability to provide fast, accurate, and reliable data efficiently.
- **Resource Limitations**: Centralized systems face bottlenecks and inefficiencies due to limited resources, slowing data retrieval and processing capabilities.

Single Points of Failure

- **System Vulnerability**: Centralized architectures are vulnerable to single points of failure. A compromise or failure of a central server can render the entire indexing service unavailable, causing significant operational disruptions.

- **Security Risks**: These systems are particularly susceptible to cyber-attacks, such as Distributed Denial of Service (DDoS) attacks, posing severe threats to service continuity and data security.

Transparency and Trust

- **Opaque Operations**: Centralized services typically operate as black boxes with limited user visibility into data management and processing, undermining trust.
- **Community Engagement**: Conventional centralized models restrict community participation in governance and decision-making, diminishing ownership and accountability among stakeholders.

Cost and Efficiency

- **Operational Costs**: Centralized infrastructures are costly to maintain, requiring substantial investment in hardware, software, and ongoing maintenance.
- **Inefficient Resource Utilization**: These systems often do not fully utilize available resources, leading to inefficiencies and increased operational costs.

Data Accuracy and Reliability

- **Validation Challenges**: Centralized systems struggle with efficiently validating the accuracy and reliability of large data volumes.
- **Error and Fraud Detection**: There is often a lack of robust mechanisms to detect and rectify errors or fraudulent activities swiftly, compromising data integrity.

Data Integrity and Consistency

- **Centralized Control**: While easier to ensure consistency through a singular authoritative source, this central control poses a risk of being a single point of failure.
- **Integrity Verification**: Reliance on single verification points can be problematic; if compromised, the integrity of the entire dataset is jeopardized.
- **Data Provenance**: Centralized systems make it cumbersome to track data origin and history, complicating auditability and accountability.
- **Real-time Synchronization**: Achieving real-time data synchronization across all nodes in a centralized setup introduces significant latency and processing challenges, adversely affecting performance and user experience.

The Need for a Decentralized Approach

In response to these formidable challenges, Unmarshal is embarking on an ambitious journey to adopt a decentralized indexer network, anchored in a sophisticated hybrid blockchain model. This transformative transition is designed to enhance scalability, bolster security, elevate transparency, and foster robust community involvement, all while ensuring unparalleled levels of data accuracy and reliability. By harnessing the potential of decentralized architecture and embracing a community-driven governance model, Unmarshal aims to revolutionize the landscape of blockchain data services and set new industry benchmarks. The specific platform underpinning our decentralized network will be unveiled soon.

Unmarshal Decentralization

The challenges posed by centralized indexing services are being addressed through a strategic transition to a decentralized indexer network, leveraging a robust hybrid blockchain model. This section details the groundbreaking architectural innovations, dynamic operational procedures, and a community-centric governance model that collectively create a scalable, secure, and transparent ecosystem for blockchain data services.

Multi-Layered Node System

Operator Nodes

- **Function**: Run offline indexers, handling data from various blockchain networks.
- **Staking Mechanism**: Operators stake tokens as a security deposit, aligning their interests with network integrity. Failure to meet performance standards triggers penalties.
- **Redundancy and Distribution**: Positioned globally to ensure data redundancy and eliminate single points of failure, enhancing data robustness and availability.

Validators

- **Function**: Authenticate the integrity and authenticity of indexed data by committing proofs to the blockchain.
- **Consensus Mechanism**: A Proof of Stake (PoS) system selects validators based on their stake and historical performance.
- **Zero-Knowledge Proofs (ZKPs)**: Maintain computation integrity and data privacy by validating workloads without exposing underlying data.

Proofreaders

- **Function**: Review and cross-check the work of validators and operators.
- **Incentivization**: Rewards in tokens for detecting errors or fraudulent activities, enhancing data accuracy and reliability.

Operational Dynamics

Staked Operators

- **Security Deposit**: Participation requires staking tokens, ensuring high performance and network reliability.
- **Penalization**: Failing to meet network standards results in penalties, ensuring quality and reliability.

Decentralized Execution

- **Distributed Indexing Tasks**: Indexing tasks are distributed among operators globally, optimizing data robustness and system resilience.
- **Enhanced Robustness**: This distributed method improves data processing and availability.

Advanced API Routing and Tracking System

API Management

- **Decentralized API Layer**: Routes queries to the optimal indexer node, balancing load and optimizing response times.

- **Query Optimization**: Maximizes efficiency and reduces latency, improving user experience.

Tracking System

- **Performance Monitoring**: Real-time monitoring of node performance and health.
- **Transparency and Accountability**: Essential for upholding service level agreements (SLAs) and ensuring user satisfaction.

Security and Data Integrity

- **Consistency Across Nodes**: Leverages distributed ledger technology to ensure uniform data across the network.
- **Real-time Synchronization**: Maintains data consistency and minimizes discrepancies.
- **Integrity Verification**: Utilizes ZKPs to confirm computation integrity and employs fraud proofs to challenge suspicious activities.

Data Provenance

- **Provenance Tracking**: Mechanisms track data origin and history, boosting auditability.
- **Merkle Trees and MMRs**: Employed for efficient and secure data verification.

Governance Model

Decentralized Governance

- **Token-Based Voting**: Empowers token holders to propose and vote on platform changes, integrating community insights into decision-making.
- **On-Chain and Off-Chain Mechanisms**: Combines the immutability of on-chain actions with the inclusiveness of off-chain discussions.

Incentivization and Rewards

- **Staking and Rewards**: Aligns participant incentives with network success.
- **Reputation System**: Monitors and rewards participant performance, ensuring accountability and encouraging high-quality contributions.

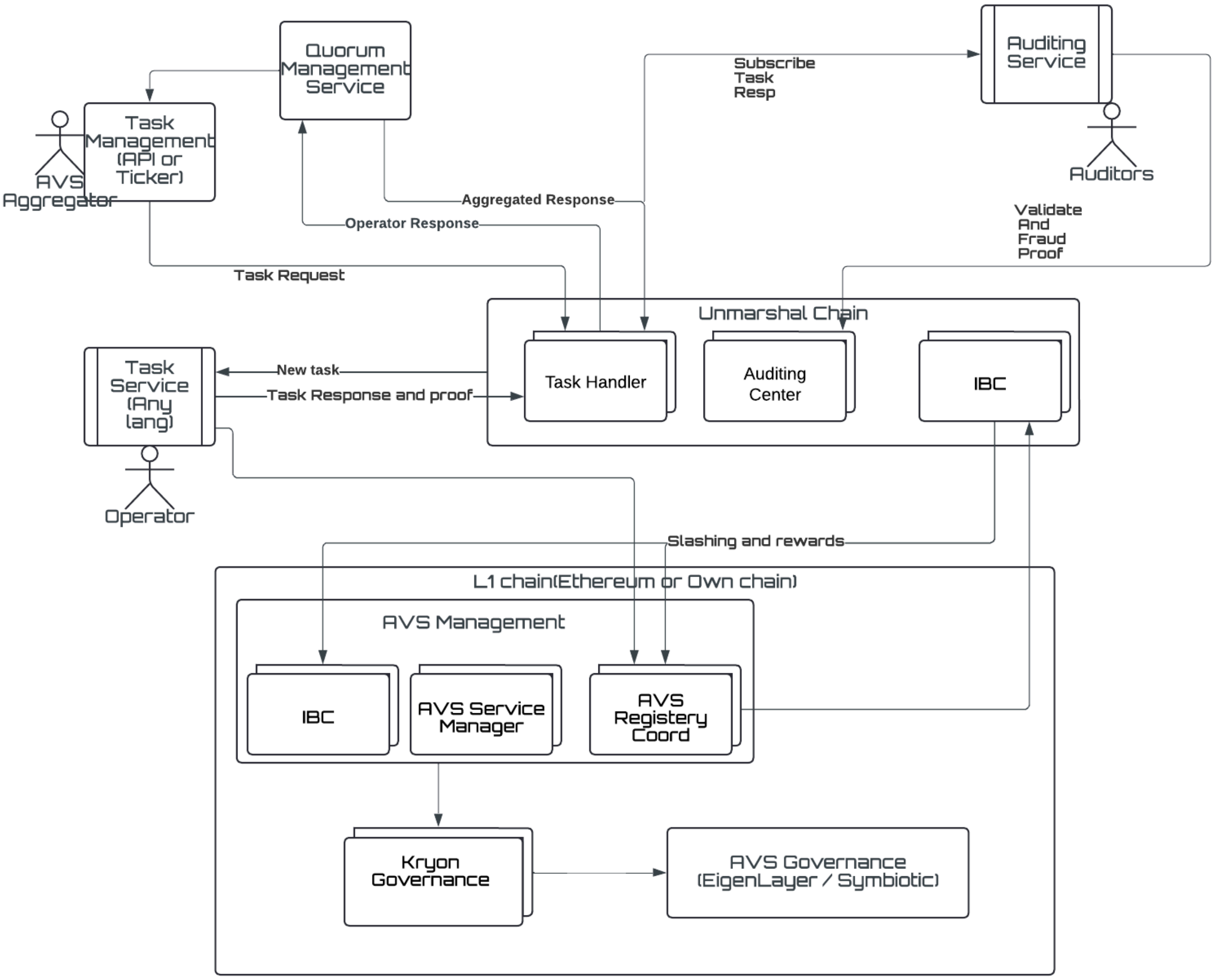
Unmarshal’s transition

to a decentralized indexer network, built on an advanced hybrid blockchain model, addresses the shortcomings of centralized systems by integrating sophisticated cryptographic techniques, decentralized operations, and a governance model driven by community involvement. This transformation is poised to redefine the standards of reliability, accuracy, and trust in blockchain data services, enhancing scalability, security, and transparency across the ecosystem. The details of the platform supporting our decentralized network will be disclosed in upcoming updates.

Technical Architecture for Unmarshal’s Decentralised Indexer Network

Overview

Unmarshal's decentralized indexer network leverages a sophisticated array of technologies and system designs to ensure efficient, secure, and reliable blockchain data services. This architecture is built on a network of distributed nodes, each specializing in distinct functions such as data indexing, validation, and query processing, ensuring high performance and robust data integrity.



1. Operator Nodes

Core Functions

- **Blockchain Data Indexing**: Operator Nodes are equipped with Docker containers that encapsulate all necessary dependencies and blockchain clients. These nodes autonomously fetch, index, and store blockchain data from various networks.
- **Local Data Storage**: Each node maintains a local database where indexed data is stored for quick access and query responsiveness.
- **Data Redundancy and Distribution**: Data is redundantly stored across multiple nodes using distributed file systems to enhance availability and fault tolerance.

Key Technologies and Systems

- **Docker**: Provides a consistent, isolated environment for each node, simplifying deployment and scalability.
- **Database Systems**: Such as PostgreSQL or MongoDB, used for storing indexed data efficiently.
- **Distributed File Systems**: Like IPFS or GlusterFS, facilitate the distribution and redundant storage of data.

2. Validator Nodes

Core Functions

- **Proof Generation**: Validator Nodes generate cryptographic proofs (e.g., Zero-Knowledge Proofs) for indexed data, ensuring its integrity without revealing the actual data.
- **Proof Commitment**: These proofs are committed to the blockchain, where they are verified and recorded, using smart contracts designed for this purpose.

Key Technologies and Systems

- **Cryptographic Libraries**: Such as libsnark, which are utilised for generating Zero-Knowledge Proofs.
- **Ethereum Smart Contracts**: Manage the submission and verification of proofs on the blockchain.
- **Consensus Algorithms**: Proof of Stake mechanisms are employed to select and reward validators based on their stake and the accuracy of their proofs.

3. Proofreader Nodes

Core Functions

- **Cross-Validation**: Proofreader Nodes independently verify the proofs submitted by Validator Nodes by cross-checking against their own data sets.
- **Error and Fraud Detection**: These nodes help maintain the network's integrity by identifying and reporting any discrepancies or fraudulent activities.

Key Technologies and Systems

- **Blockchain Interaction Tools**: Such as web3.js, used for interacting with the blockchain to fetch and verify proofs.
- **Data Comparison Scripts**: Custom scripts designed to efficiently compare data sets and validate proofs.

4. API Gateway

Query Handling

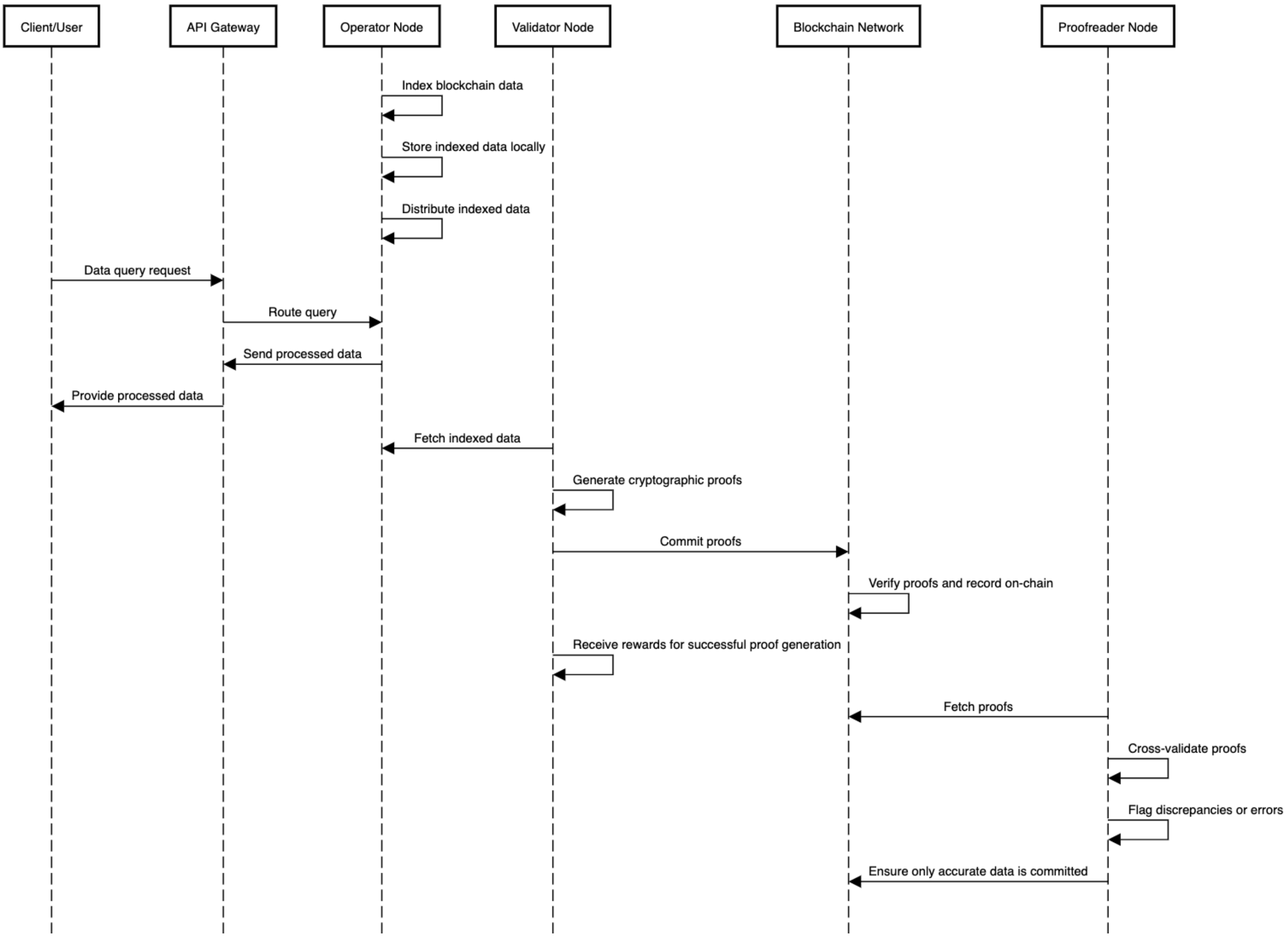
- **The API Gateway**: Serves as the interface for client queries, routing requests to the most appropriate Operator Node based on load balancing algorithms.

Data Delivery

- **Data Aggregation**: It aggregates responses from nodes and delivers them back to the clients efficiently.

Key Technologies and Systems

- **Load Balancers**: Software like Nginx or HAProxy to distribute incoming requests evenly across Operator Nodes.
- **API Management Platforms**: Such as Kong, which manage the APIs' lifecycle, ensure security, and optimize performance.



Operator Node Continuous Process

1. **Index Blockchain Data**: Operator Nodes continuously transform raw blockchain data into structured formats.
2. **Store Indexed Data Locally**: Operator Nodes retain indexed data locally to facilitate rapid access and retrieval.
3. **Distribute Indexed Data**: Operator Nodes disseminate indexed data to enhance redundancy and data availability across the network.

Client Interaction

1. **Data Query Request**: Clients send data queries to the API Gateway.
2. **Route Query**: The API Gateway directs queries to the appropriate Operator Node.

3. **Send Processed Data**: Operator Nodes process the queries and relay the results back to the API Gateway.
4. **Provide Processed Data**: The API Gateway delivers the processed data back to the client.

Validation Process

1. **Fetch Indexed Data**: Validator Nodes retrieve indexed data from Operator Nodes.
2. **Generate Cryptographic Proofs**: Validator Nodes create cryptographic proofs to verify the indexed data.
3. **Commit Proofs**: Validator Nodes upload these proofs to the blockchain.
4. **Verify Proofs and Record On-Chain**: The blockchain verifies and logs the proofs.
5. **Receive Rewards**: Validator Nodes earn rewards for producing and committing valid proofs.

Proofreading Process

1. **Fetch Proofs**: Proofreader Nodes obtain the committed proofs from the blockchain.
2. **Cross-Validate Proofs**: Proofreader Nodes check the proofs to detect any discrepancies or errors.
3. **Flag Discrepancies or Errors**: Proofreader Nodes flag any found discrepancies or errors.
4. **Ensure Accurate Data**: Proofreader Nodes confirm that only accurate data is recorded on the blockchain.

AVS-Based Hybrid Decentralization Model

The AVS-based hybrid decentralization model leverages the strengths of both decentralized and centralized architectures, providing an optimized solution for performance, security, and scalability. This model employs Actively Validated Services (AVS), staking requirements, and dynamic adjustments to ensure a robust and responsive network. Below, we go deeper into the operational dynamics and technology choices that underpin this model.

Concept and Functionality

- **Inspiration and Mechanism**: Inspired by EigenLayer, AVS enhances network security and reliability by requiring active participation from nodes in the validation process. Nodes perform continuous and crucial security functions such as generating and verifying proofs, ensuring that only accurate and trustworthy data is maintained within the network.
- **Security Contributions**: Each node contributes to the overall security posture of the network by actively participating in consensus and validation processes, helping to prevent fraud and maintain data integrity.

Technology Choices

- **Cryptographic Techniques**: Utilization of advanced cryptographic methods such as Zero-Knowledge Proofs (ZKPs) allows nodes to validate transactions or data states without revealing the underlying data, enhancing privacy and security.

- **Smart Contracts**: Deployed on platforms like Ethereum, smart contracts automate the verification of proofs submitted by nodes, ensuring transparency and reducing the possibility of human error or manipulation.

Staking Requirements

Dynamic Staking

- **Incentive Alignment**: Nodes are required to stake tokens as a security deposit, aligning their financial incentives with the overall health and integrity of the network. The staking mechanism ensures that nodes have a vested interest in the accurate and efficient performance of their duties.
- **Dynamic Adjustments**: The staking requirements are not static; they are adjusted based on real-time network conditions, node performance, and overall network security needs. This flexibility helps to maintain an optimal balance between security and performance.

Technology Implementation

- **Blockchain-based Staking**: Leveraging blockchain technology allows for transparent and secure management of staked tokens. The blockchain ensures that all staking transactions are immutable and verifiable by all network participants.
- **Automated Staking Adjustments**: Algorithms embedded within the network's protocol automatically adjust staking requirements in response to changing network conditions and node performance metrics.

Reward Distribution and Slashing

Dynamic Rewards and Penalties

- **Reward Mechanisms**: Nodes receive rewards based on their performance and the level of security they contribute to the network. Rewards are dynamically adjusted to incentivize nodes to maintain high standards of operation.
- **Slashing Protocols**: If a node fails to meet the network's standards or engages in malicious activity, a portion of its staked tokens is 'slashed' as a penalty. The severity of the slashing is dynamic and dependent on the nature and severity of the infraction.

Technology Implementation

- **Token Distribution and Management**: Smart contracts manage the distribution of rewards and the execution of slashing penalties, ensuring that all token transactions are processed fairly and transparently.
- **Performance Monitoring**: Continuous monitoring systems are implemented to assess the performance of each node. These systems utilize machine learning algorithms to analyze trends and patterns in node behavior, supporting the dynamic adjustment of rewards and penalties.

Conclusion

The AVS-based hybrid decentralization model represents a sophisticated blend of decentralized and centralized elements, designed to optimize network performance while maintaining high standards of security and scalability. By incorporating dynamic staking requirements, reward distributions, and slashing protocols, Unmarshal ensures that the network remains robust, efficient, and aligned with the interests of all stakeholders. This model sets a new standard in blockchain network design, offering a scalable and secure framework for decentralized data services.

Economic Model of Unmarshal’s Decentralised Indexer Network

Unmarshal’s economic model fosters a robust ecosystem by incentivizing high performance, honesty, and active participation among network participants. The model integrates token rewards, fee sharing, and a dynamic staking and slashing mechanism to align participant interests with the network’s overall health and security.

Token Rewards

- **Mechanics of Reward Distribution**: Participants, including operators, validators, and proofreaders, earn tokens based on their contributions to data processing, validation, and maintaining data integrity. Rewards are influenced by accuracy, response speed, and successful cryptographic proofs.
- **Technology Implementation**: Smart contracts automate reward distribution based on verifiable performance metrics, ensuring transparency and fairness.

Fee Sharing

- **Revenue Generation and Distribution**: Fees paid by users for querying and accessing data are collected and a portion is distributed among network participants based on their role and contribution.
- **Technology and Systems**: Decentralized finance (DeFi) protocols manage and distribute fees securely and transparently.

Staking and Slashing

- **Stake as Collateral

**: Participants must stake tokens as collateral, which incentivizes adherence to network protocols. Staking requirements are dynamic, adjusting based on network needs and performance.

- **Penalties for Non-Compliance**: Participants who act maliciously or fail to meet performance standards face slashing penalties. Smart contracts enforce these penalties automatically.

Security and Reliability in Unmarshal’s Decentralised Indexer Network

Unmarshal’s decentralized indexer network is designed with a focus on security and reliability through advanced data integrity protocols, fault tolerance mechanisms, and stringent security measures.

Data Integrity

- **Actively Validated Services (AVS)**: Multiple validation layers ensure data accuracy, employing advanced cryptographic techniques and recording on an immutable blockchain ledger.
- **Blockchain Implementation**: Cryptographic proofs are recorded on the blockchain, ensuring immutability and automated validation protocols via smart contracts.

Fault Tolerance

- **Redundancy and Distributed Processing**: Data is stored across multiple operator nodes and processed in a decentralized manner, enhancing availability and resilience against failures.
- **Load Management and System Continuity**: Dynamic load balancing and automated failover protocols maintain system performance and continuity.

Security Measures

- **Encryption and Node Authentication**: Data in transit is encrypted, and nodes undergo rigorous authentication processes to ensure network security.
- **Proactive Security Practices**: Regular security audits and real-time monitoring tools detect and address potential vulnerabilities.

Use Cases for Unmarshal’s Decentralised Indexer Network

Unmarshal’s decentralized network enhances its utility for critical systems where data integrity, security, and uptime are essential.

Decentralized Payment Gateways

- **Overview**: Securely processes transactions with enhanced security and immediate data availability.
- **Benefits**: Reduces fraud risk and improves payment efficiency.

Anti-Money Laundering (AML) Compliance

- **Overview**: Monitors and analyzes transactions to identify potential money laundering activities.
- **Benefits**: Enhances AML procedures and fosters trust among regulatory bodies and financial institutions.

Fraud Detection and Risk Assessment in DeFi

- **Overview**: Detects fraudulent activities and financial discrepancies in DeFi platforms.
- **Benefits**: Provides real-time risk assessment and reliable fraud detection.

Enhanced Blockchain Forensics and Incident Response

- **Overview**: Offers tools for tracing and analyzing blockchain incidents.
- **Benefits**: Enables detailed forensic analysis and quicker incident response.

Future Work

As Unmarshal evolves, several key initiatives will further enhance the platform's capabilities and community engagement:

Community Ownership and Governance

- **Decentralized Governance Model**: Transition to a DAO structure for community-driven governance, allowing token holders to propose and vote on network changes.
- **Enhanced Stakeholder Involvement**: Align platform development with user insights for a more responsive ecosystem.

Open Source Development

- **Commitment to Open Source**: Release core software components as open-source, encouraging collaboration and innovation.
- **Developer Incentive Programs**: Reward community developers for contributions and improvements.

Expansion of Blockchain Integrations

- **Broader Blockchain Support**: Integrate with emerging blockchains and develop custom solutions for enterprise and consortium blockchains.

Enhancement of Data Services

- **Advanced Analytical Tools**: Integrate AI for predictive analytics and deeper insights.
- **Real-Time Data Streaming**: Implement solutions for real-time data updates.

Sustainability Initiatives

- **Reducing Environmental Impact**: Optimize energy consumption and support eco-friendly blockchain practices.

Unmarshal's commitment to these areas ensures that the platform will not only address current challenges but also drive the future of blockchain technology, maintaining its position at the forefront of innovation and reliability.