UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

THEORY AND PRACTICE OF DECENTRALIZED BLOCKCHAIN ORACLES

A Master's Thesis

Submitted to the Faculty of the

Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

by

Vladimir Fomintsov Trukhaev

MASTER IN CYBERSECURITY (MCYBERS)

Advisor: Jose Luis Muñoz Tapia

Barcelona, July 2024

to my dearest parents and partner for their enduring love and unwavering support, which have been essential sources of guidance throughout the course of my master's thesis.

Acknowledgements

I would like to express my sincere gratitude to my esteemed professor for their invaluable assistance, expertise, and counsel which greatly supported me throughout the entire process of completing my master thesis. The insightful remarks offered, substantial contributions rendered, constructive critiques provided, and overall support extended have been instrumental in the successful completion of this research project. Said project has experienced a significant improvement in quality and rigor as a result of the extensive knowledge and expertise contributed by Professor Muñoz. Muñoz's astute observations and perceptive feedback have made a substantial contribution to the enhancement of my research methodologies and analytical approaches. Furthermore, the bestowing of guidance and mentorship that I have received have played a pivotal role in expanding my academic development and deepening my comprehension of the subject matter at hand.

In addition, it is important for me to acknowledge the support and financial assistance provided by my parents, for which I am grateful. Their steadfast dedication and selflessness have laid the bedrock for my scholarly expedition, enabling the successful completion of this master's thesis. Moreover, the unwavering emotional and financial support they have provided has played a crucial role in facilitating the accomplishments I have attained to date. The unhesitating belief in my abilities shown by them has been a significant motivator in overcoming obstacles and striving for scholarly excellence. All things considered, I wish to extend my profound gratitude for the steadfast love, support, and motivation they have been generously providing me during my academic endeavors.

Finally, I would like to extend my profound gratitude for the steadfast emotional and overall support provided by my partner throughout the entirety of this project. Their support and validation provided to me has functioned as a crucial source of motivation, effectively bolstering my resolve and enabling me to overcome a range of obstacles encountered during the course of said study. Their sustained presence and open-minded approach have consistently been a source of inspiration and resilience.

Abstract

The present study explores the field of decentralized oracles, paying specific attention to the Chainlink network. Additionally, the study includes the creation of a decentralized finance (DeFi) trader smart contract that integrates Chainlink's oracles and price feeds. Moreover, it is discussed how decentralized oracles play a crucial role in facilitating connectivity between blockchain systems and external data sources, thereby bolstering operational capabilities and broadening the scope of functionalities available to blockchain applications.

The principal aim of this research is to illustrate the incorporation and application of decentralized oracles in practical settings, particularly by means of the construction of a DeFi trader smart contract. The purpose of this contract is to utilize Chainlink's dependable and secure price feeds for the implementation of essential trading operations, including the initiation and processing of purchase and sale transactions, as well as the management of limit orders. The utilization of reliable and promptly available market data from Chainlink's decentralized oracle network enables the smart contract to facilitate efficient and transparent trading activities.

The primary elements of this study entail a comprehensive examination of Chainlink's complex architectural framework, consisting of decentralized oracle networks (DONs) that collate and authenticate data from various origins to safeguard the accuracy and integrity of the data. The research also examines pertinent security issues such as Sybil attacks, data manipulation, and node collusion, and delves into different strategies to mitigate these risks, including cryptographic proofs, multi-source data aggregation, and robust consensus mechanisms.

In summary, this investigation highlights the importance of decentralized oracles in enhancing the functionalities of blockchain technology and DeFi applications. The results emphasize the need for extensive implementation and incorporation of decentralized oracles in order to guarantee the sustained progress and prosperity of blockchain ecosystems. This study offers a thorough and technical analysis of the architecture, security, and practical uses of Chainlink decentralized oracles, providing valuable perspectives for the advancement of financial innovations based on blockchain technology.

Keywords: Blockchain, Decentralized Finance, Decentralized Oracles, Decentralized Oracle Networks, Chainlink, Smart Contracts, Staking Mechanisms, Decentralized Applications

Table of Contents

Introduction 1

Literature Review 5

Centralized vs Decentralized Oracles 9

- Centralized Oracles 9
- Decentralized Oracles 12

Technical Background 17

- Chainlink Architecture 17
  - Decentralized Oracle Networks (DONs) and its Functionalities 18
    - Executables 18
    - Adapters 19
    - Operational Model 19
  - Some of Chainlink's Design Goals 20
    - Scaling 20
    - Trust Minimization 23
    - Incentive-based Security 26
  - Node Operators 34
- Chainlink Price Feeds 39
  - Some of Chainlink Price Feeds' Properties 40
    - Layers of Decentralization and Data Quality 40
    - Data Delivery 42
    - Multi-Layered Defense in Depth 44

Implications for DeFi 47

Security Concerns 51

- Byzantine Faults 51
- Sybil Resistance 54
- DoS Resistance 56

Use Case Implementation 61

Conclusions 75

References 77

Introduction

The domain of blockchain technology is recognized for its dynamic and swiftly evolving characteristics, and in recent times, there has been a prominent emergence of decentralized oracles. The incorporation of oracles is essential in optimizing the operational capabilities and value of blockchain systems through the integration of external data. This study aims to undertake an in-depth analysis of decentralized oracles and their significance within decentralized finance (DeFi) applications that are built upon blockchain technology. The principal emphasis of this inquiry revolves around the formulation and execution of a resilient DeFi trading smart contract through the utilization of the Chainlink oracle network. The primary objective of this study is to showcase fundamental trading proficiencies, including the accurate placement and execution of buying and selling orders, as well as the management of limit orders, all of which are made possible by the accurate, punctual, and dependable data offered by decentralized oracles.

The blockchain technology, originally developed as a decentralized ledger for digital currencies, has evolved into a versatile platform with the capability to facilitate a diverse range of applications across multiple industries. Blockchains are intrinsically compartmentalized systems that lack the capability to directly retrieve or authenticate external data. This constraint presents a noteworthy obstacle for applications necessitating instantaneous, fluctuating data inputs, particularly in the financial industry. Decentralized oracles offer a solution to the fundamental limitation of integrating off-chain data into the blockchain by providing a secure and minimized-trust mechanism. This facilitates the expansion of the operational functionalities of smart contracts from basic token transfers to more intricate financial operations (Caldarelli et al., 2020).

Chainlink exemplifies an advanced implementation of decentralized oracles, crafted to securely facilitate the connection between blockchain systems and external data sources. The architecture of Chainlink entails a decentralized network comprising autonomous nodes that undertake the tasks of retrieving, validating, and delivering data. The utilization of a decentralized approach serves to reduce the potential risks linked with single points of failure and centralization, phenomena commonly observed in conventional, centralized oracle systems (Breidenbach et al., 2021).

The Chainlink 2.0 framework presents notable progressions, such as improved node decentralization, strengthened cryptographic data verification methods, and advanced

functionalities for oracle scripting. The cumulative improvements make significant contributions to the dependability, protection, and expansiveness of decentralized oracle networks. Chainlink's innovative methodology guarantees the integrity and genuineness of data transmitted to smart contracts, thereby cultivating enhanced trust and confidence in blockchain applications (Breidenbach et al., 2021).

The main aim of this thesis is to analyze the real-world implementation of a DeFi trader contract, specifically engineered to interface with Chainlink oracles for the purpose of accessing current asset pricing data. The objective of this smart contract is to demonstrate the functionalities of decentralized oracles in enabling intricate financial transactions in a manner that is devoid of trust, and characterized by transparency and efficacy. The implications of incorporating such integrations are far-reaching, as they enable decentralized finance (DeFi) applications to function with increased efficacy, by utilizing precise and promptly received external data, a critical component for the execution of dynamic trading strategies (Zhao et al., 2022).

The integrity of decentralized oracle networks is of paramount importance due to their fundamental role in guaranteeing the precision and trustworthiness of data utilized in smart contracts. This study investigates the susceptibilities linked with decentralized oracle systems, including but not limited to Sybil attacks, data manipulation, and collusion among nodes. This study explores various approaches to mitigate risks, such as cryptographic proofs, multi-source data aggregation, and robust consensus mechanisms, in order to improve the security and resilience of oracle networks (Cai et al., 2020).

Furthermore, this research contributes to the scholarly discourse by providing a thorough analysis of the theoretical foundations and practical implementations of decentralized oracles. This research is situated within the wider context of the progression of blockchain technology, with a focus on the capacity of decentralized oracles to mitigate the inherent limitations of traditional blockchains and enable the creation of more advanced and utilitarian applications. The empirical investigation and practical application discussed in this dissertation highlight the transformative capacity of decentralized oracles within the field of decentralized finance (DeFi), emphasizing the need for their widespread incorporation and utilization (Kamal Ezzat et al., 2022).

In summary, the present introduction lays the foundation for a comprehensive examination of decentralized oracles, elucidating their essentiality, operational characteristics, and ramifications within the blockchain environment. The following chapters will provide a

thorough examination of decentralized versus centralized oracles, an in-depth analysis of the technical architecture of oracle networks, and comprehensive case studies on the utilization of Chainlink oracles in decentralized finance (DeFi) applications. An in-depth examination of security frameworks will be conducted to assess their integrity and dependability. The principal aim of this thesis is to make significant contributions to the implementation and improvement of decentralized oracles, thereby advancing the progress of blockchain technology and its application within the domain of decentralized finance.

Literature Review

The scholarly discourse surrounding decentralized oracles within the context of blockchain technology is comprehensive and diverse, indicative of the notable progress and obstacles within this domain. Decentralized oracles seek to address the prominent issue known as the "Oracle Problem", which entails the difficulty of acquiring trustworthy external data for smart contracts while upholding the decentralized principles of blockchain technology (Beniiche, 2020). The utilization of centralized oracles, although characterized by efficiency and simplicity, is plagued by significant vulnerabilities including a singular point of failure and susceptibility to malicious attacks (Beniiche, 2020). This phenomenon has sparked considerable interest and scholarly investigation into decentralized alternatives that may provide greater security and reliability.

Provable (formerly Oraclize) and Town Crier have conducted research on the incorporation of Trusted Execution Environments (TEEs) such as Intel's Software Guard Extensions (SGX). The utilization of such environments creates a controlled and safeguarded platform for the execution of data processing operations, thereby guaranteeing the integrity of data during its transmission (Provable, 2020; Zhang et al., 2016; Costan & Devadas, 2016). Provable utilizes Trusted Execution Environments (TEEs) to produce cryptographic evidence of data integrity, which is subsequently transmitted to the blockchain alongside the acquired data. The utilization of SGX by Town Crier facilitates the establishment of a secure connection between external data sources and the blockchain, thereby enabling the provision of authenticated data feeds for smart contracts (Zhang et al., 2016).

One of the influential contributions to the field of decentralized oracles is the research on decentralized oracle networks was the introduction of Chainlink 2.0 (Breidenbach et al., 2021). Said whitepaper provides an overview of the architectural and functional characteristics of a decentralized oracle network (DON) that utilizes a multitude of autonomous nodes to retrieve, authenticate, and consolidate data prior to transmitting it to the blockchain. This methodology effectively reduces the vulnerabilities related to reliance on individual components by spreading trust throughout a network of nodes, thus increasing the integrity and accessibility of data. The structural design of Chainlink incorporates both on-chain and off-chain elements. The on-chain workflow of Chainlink encompasses three main stages, namely: oracle selection, data reporting, and result aggregation. Oracles are chosen based on service level agreements (SLAs) that outline the specific requirements for data retrieval. The oracles autonomously collect the requisite information, which is then consolidated and verified through a consensus mechanism prior to its transmission to the

smart contract (Breidenbach et al., 2021). The procedure is reinforced by sophisticated cryptographic methods, including the utilization of Transport Layer Security (TLS) to ensure the security of communications as outlined by Ritzdorf et al. (2018), as well as the implementation of DECO, a protocol developed by Zhang et al. (2020), which facilitates privacy-preserving data retrieval through the use of zero-knowledge proofs. The protocol DECO enables the verification of data without compromising its confidentiality, thereby upholding the integrity of the data while maintaining secrecy. This functionality proves especially beneficial in situations where there is a necessity to securely incorporate confidential data into smart contracts. This assertion is additionally supported by staking mechanisms, which necessitate nodes to immobilize cryptocurrency as security. If a node disseminates incorrect or deceptive information, it faces the potential loss of its staked assets, thereby serving as a deterrent to engage in malicious activities (Breidenbach et al., 2021).

Numerous research studies have examined a range of elements relating to decentralized oracles and their potential use cases. Cai et al. (2022) conducted a study that aimed to examine the implementation of veracious decentralized oracles, with the specific objective of ensuring data integrity and authenticity in the absence of central authority intervention. Similarly, the architectural framework proposed by Gigli et al. in the year 2023, was the development of a decentralized global market for the Internet of Things (IoT), utilizing a distributed oracle layer to enable secure and dependable data interchange between IoT devices and blockchain networks. Said framework aimed to tackle obstacles related to device diversity and trust administration (Gigli et al., 2023).

The utilization of decentralized oracles yields improvements in security and reliability, while also facilitating a more equitable dissemination of trust. Cai et al. (2022) identified that within a decentralized oracle network, inclusion in the data retrieval process is open to any node that satisfies the predetermined criteria. This structure promotes a permissionless and equitable environment for all participants. Said model has a substantial impact on decreasing the probability of collusion and bias, thereby guaranteeing the accuracy and reliability of the data supplied to smart contracts. The decentralized nature of these oracles presents challenges with regards to data consensus and aggregation. To guarantee the reliability of all participating nodes and the accuracy of the data they contribute, it necessitates the implementation of complex coordination and incentive mechanisms. Breidenbach et al. (2021) assert that Chainlink tackles these challenges through the integration of reputation systems and staking mechanisms, requiring nodes to allocate financial resources that may be at risk of forfeiture in cases of dishonest conduct. The

reputation system within Chainlink appraises nodes according to their past performance, encompassing factors such as precision, dependability, and promptness of response. There is a greater likelihood for high-performing nodes to be chosen for tasks, thus cultivating a competitive environment that incentivizes excellence. The implementation of staking mechanisms serves to provide additional incentives for nodes to exhibit honest behavior through the requisition of cryptocurrency as collateral, which may be subjected to forfeiture in the event of dishonest actions (Breidenbach et al., 2021).

The work by Basile et al. (2021) has also made notable contributions in this field. Said work put its emphasis on the integration of blockchain-based processes with decentralized oracles, highlighting the significance of ensuring availability, integrity, and trust in the design of oracles (Basile et al., 2021). Additionally, research such as that conducted by Al-Breiki et al. (2020) offers thorough evaluations of reliable blockchain oracles, with a focus on comparing various models and emphasizing key research obstacles, including scalability and the necessity for proficient consensus algorithms. Withal, the literature delves into the examination of consensus mechanisms in decentralized oracle networks as a means of improving data reliability. Adler et al. (2018) exemplify the utilization of a decentralized blockchain oracle called ASTRAEA that incorporates a voting-based consensus mechanism. In this system, nodes participate in voting to determine the accuracy of data prior to its acceptance by the network. This methodology serves to guarantee the integrity of the data entering the blockchain through the validation of multiple autonomous entities, thereby diminishing the potential for inaccuracies or malevolent data.

Furthermore, alongside Chainlink and ASTRAEA, other significant decentralized oracle projects encompass Witnet and Augur. On the one hand, the Witnet protocol, as delineated by de Pedro et al. (2017), demonstrates significant potential within the realm of decentralized data retrieval and consensus mechanisms. The decentralized oracle network employs a reputation-based mechanism to ascertain the reliability of its nodes. Incentives for nodes, also known as witnesses, are contingent upon their reputation and the precision of the information they furnish, thereby fostering an incentive system that encourages integrity. On the other hand, the decentralized oracle and prediction market platform known as Augur employs the collective wisdom of a crowd to authenticate and verify the accuracy of outcomes. In prediction markets, individuals stake reputation tokens as a means to report on market outcomes. Those who provide accurate reports receive rewards, whereas those who provide inaccurate reports are subject to penalties. The utilization of decentralized exchanges (DEXs) as sources of data for oracles serves to augment their dependability. Peterson et al. (2019) exemplifies the utilization of decentralized oracles with Augur to

furnish tamper-proof data for prediction markets. This approach leverages the collective power of the community to validate outcomes.

Moreover, the incorporation of sophisticated data aggregation techniques such as time-weighted average price (TWAP) and volume-weighted average price (VWAP) when using decentralized oracles contributes to the reliability of the data offered by said oracles (Aspembitova & Bentley, 2022). These methodologies effectively minimize the influence of aberrant data points and offer a more precise depiction of the dataset across a designated time frame. The confluence of these studies emphasizes the significance of decentralization, cryptographic verification, and consensus mechanisms in the establishment of dependable and secure decentralized oracle networks. The ongoing advancement of blockchain technology necessitates the imperative development of resilient decentralized oracles, which will play a pivotal role in facilitating the widespread adoption of smart contracts across diverse industrial sectors.

Centralized vs Decentralized Oracles

Centralized Oracles

Centralized oracles function within the parameters of governance by a singular entity that is accountable for furnishing external data to smart contracts. The architectural design, though admirably uncomplicated and effective in data access and organization, is inherently afflicted by pronounced vulnerabilities in security and reliability owing to its centralized configuration. Centralized oracles give rise to significant concerns regarding the vulnerability introduced by a singular point of failure and trust. Should a breach occur within the centralized entity, it will have an immediate effect on the security and reliability of all interconnected smart contracts. The vulnerability that has been identified poses a significant threat to the integrity of the system, rendering it vulnerable to malicious attacks and unauthorized manipulation. This in turn undermines the inherent trustless characteristics of blockchain technology (Beniiche, 2020).

The operational framework of centralized oracles involves the oracle acting as the sole source of data, retrieving information from external sources and subsequently integrating it into the blockchain. The centralized approach, despite its potential for expedited data processing and simplified system architecture, raises substantial concerns regarding data security and authenticity. Due to the reliance of all data transactions on a singular data pipeline, any type of interference, such as cyber-attacks, data manipulation, or inadvertent data corruption, has the potential to cause widespread system failures throughout the network that is dependent on this central source of information. This scenario has the potential to not only impact individual transactions, but also entire blockchain-based applications, leading to financial losses and a decline in trust among users. Moreover, centralized oracles are fundamentally at odds with the decentralized structure of blockchains, which aims to eliminate any single point of control or vulnerability. The dichotomy described imbues a reliance on trust within an ecosystem that is otherwise characterized by its lack of reliance on trust. Stakeholders are consequently reliant on the trustworthiness and competence of the oracle provider in order to ensure the security of data and the faithful execution of transactions. The trust requirement outlined in the aforementioned context carries significant implications, as it may precipitate situations in which the oracle becomes vulnerable to targeted attacks seeking to exploit the centralized trust paradigm.

The entity now known as Provable, previously operating under the name Oraclize, represents an illustrative instance of a centralized oracle service. Provable addresses trust concerns by furnishing cryptographic evidence of the authenticity of the data it accesses. The validity of data transmission can be guaranteed through the use of cryptographic proofs, such as those provided by TLSNotary or Trusted Execution Environments (TEEs) such as Intel's Software Guard Extensions (SGX). These technologies serve to establish the integrity of the data and prevent unauthorized tampering during the transmission process (Provable, 2020; Zhang et al., 2016; Costan & Devadas, 2016). Trusted Execution Environments (TEEs) offer a protected and secure setting for data processing, effectively safeguarding the data from potential disruptions caused by the operating system or other concurrently running applications on the same physical hardware. This methodology utilizes the security assurances offered by Trusted Execution Environments (TEEs) to establish a secure connection between external data sources and the blockchain, consequently upholding elevated levels of data integrity. Notwithstanding these measures, the fundamental dependence on a sole entity for the provision and authentication of data continues to pose a critical limitation.

The operational framework of Provable consists of retrieving data from designated web sources and subsequently affixing cryptographic proofs to the acquired data. The information, together with the evidence, is subsequently communicated to the smart contract, thereby ensuring the detection and invalidation of any attempts at tampering. The Provable system is capable of accommodating diverse data sources such as URLs, WolframAlpha, and IPFS, among others. This permits the system to retrieve a broad spectrum of data as necessitated by various smart contracts (Provable, 2020). Although this method offers a reliable means of verifying data integrity, it still requires a certain level of trust in Provable itself. The dependence on a singular centralized service for the provision of precise data and cryptographic evidence presents a potential vulnerability, as any compromise or malfunction within Provable's systems has a direct impact on the smart contracts that rely on it. This situation is not fully in line with the decentralized principles of blockchain technology. Provable's approach entails a series of steps designed to safeguard the integrity and authenticity of data in practical application. Initially, the request for data is transmitted to the external data source through a secure and encrypted connection. Upon reception of the data, Provable produces an authenticity proof using cryptographic methods to validate the integrity of the data. The evidence is subsequently transmitted to the smart contract on the blockchain concomitantly with the data, enabling any participant to autonomously validate the credibility of the data by means of the accompanying proof

(Provable, 2020). This mechanism serves to effectively reduce the risk of data tampering and promotes increased trust in the accuracy and reliability of the data sourced from the oracle.

Additionally, it is important to note that although TEEs and cryptographic proofs offer substantial security benefits, they do not entirely eradicate the reliance on Provable as the primary entity accountable for data retrieval and verification (Zhang et al., 2016). Furthermore, it is notable that centralized oracles, such as Provable, may encounter substantial scalability challenges. The increasing need for external data has the potential to create a bottleneck within a centralized service, thereby restricting its capacity to effectively process a high volume of requests. The inherent bottleneck stems from the centralized architecture, in which a singular entity is tasked with processing all data requests and producing cryptographic proofs, including TLSNotary or proofs using Trusted Execution Environments (TEEs) such as Intel's Software Guard Extensions (SGX) (Provable, 2020; Zhang et al., 2016; Costan & Devadas, 2016).

The scalability issue is compounded by the computationally and resource-intensive process of generating and validating cryptographic proofs for individual data requests. Every individual request made to the centralized oracle necessitates independent processing, and the cryptographic operations linked to it necessitate a substantial amount of computational resources. As the volume of requests grows, the centralized server's ability to process them promptly decreases, resulting in elevated latency and decreased throughput. The latency presents a potentially adverse impact on blockchain applications that depend on real-time or near-real-time data, as delays in data retrieval and verification can undermine the functionality and user experience (Provable, 2020). Moreover, the necessity to uphold high levels of availability and reliability in a centralized system requires significant investment in infrastructure. The centralized oracle is required to guarantee redundancy, failover mechanisms, and robust security protocols in order to minimize downtime and defend against potential security breaches. The stipulated criteria have the potential to result in increased operational expenditure and intricacy, consequently placing additional strain on the system's scalability (Provable, 2020).

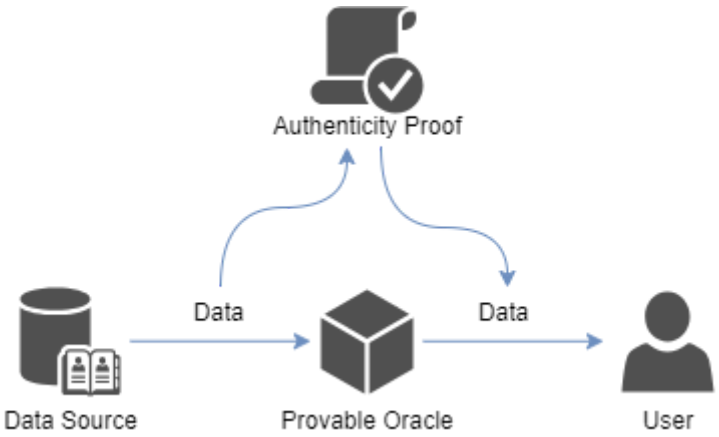

Figure 1. Provable Oracle Data Processing.

Decentralized Oracles

Decentralized oracles, as exemplified by the implementation of Chainlink, provide a more robust and secure option through the dispersion of data retrieval and validation tasks across an independent node network. The aforementioned phenomenon embodies a transition to a trust-minimized setting, achieved by the elimination of singular points of failure via the distribution of data sourcing and validation among numerous independent nodes. This model is consistent with the fundamental principles of blockchain technology, which place emphasis on decentralization and redundancy. The process of decentralization serves to reduce the vulnerabilities associated with singular points of failure while also bolstering the credibility of the information relayed to smart contracts (Breidenbach et al., 2021). In a decentralized oracle network, numerous nodes autonomously retrieve data from external sources. This data is subsequently consolidated and authenticated via a consensus mechanism prior to transmission to the smart contract.

The architectural design of Chainlink is intricately crafted to uphold data integrity and reliability by employing a comprehensive framework comprised of multiple components. The system is composed of both on-chain and off-chain elements that synergistically collaborate to facilitate the secure transmission of data. The on-chain elements encompass smart contracts responsible for overseeing reputation, order matching, and data aggregation,

whereas the off-chain infrastructure is comprised of autonomous Chainlink nodes tasked with carrying out data retrieval assignments (Breidenbach et al., 2021). The on-chain workflow of Chainlink comprises of three main stages: oracle selection, data reporting, and result aggregation. The process of selecting an oracle entails the delineation of service level agreements (SLAs) that specify the stipulations for data retrieval, encompassing the quantity of oracles required and their corresponding reputation scores. Upon the selection of oracles according to predetermined criteria, they autonomously retrieve the necessary data and submit it to the on-chain aggregating contract. The contract systematically records the responses and calculates a consolidated outcome, which is subsequently transmitted to the designated smart contract (Breidenbach et al., 2021).

Furthermore, Chainlink integrates sophisticated cryptographic methods to guarantee the integrity and authenticity of data while also offering a decentralized data retrieval mechanism. The implementation of Transport Layer Security (TLS) is utilized to ensure the security of communications between Chainlink nodes and external data sources, as discussed by Dierks and Rescorla in 2008. Moreover, advanced protocols such as DECO facilitate the retrieval of data while preserving privacy through the use of zero-knowledge proofs, thereby ensuring the authenticity of data without disclosing its content (Ritzdorf et al., 2018; Zhang et al., 2020). Decentralized oracles serve to bolster security and reliability, while also facilitating a fairer distribution of trust. The decentralized oracle network enables participation of any node in the data retrieval process, subject to meeting the specified criteria, thereby facilitating a permissionless and equitable environment (Cai et al., 2022). This model has a substantial impact on diminishing the probability of collusion and bias, thereby guaranteeing the accuracy and reliability of the data supplied to smart contracts. The decentralized structure of the network fosters a distributed trust model among numerous participants, thereby posing significant challenges for any individual entity attempting to manipulate the data. Nevertheless, the decentralized nature of these oracles gives rise to intricacies associated with data consensus and aggregation. The assurance of reliability of all participating nodes and the accuracy of the data they contribute necessitates the implementation of advanced coordination and incentive mechanisms. Chainlink tackles these challenges through the integration of reputation systems and staking mechanisms, requiring nodes to allocate financial resources that may be subject to forfeiture in cases of dishonest conduct (Breidenbach et al., 2021).

The reputation system implemented by Chainlink is a crucial element aimed at assessing and ordering oracle nodes according to various essential performance criteria, such as accuracy, reliability, and response time. The reputation mechanism fosters a competitive

environment that provides incentives for high-quality performance, thereby ensuring that only the most reliable nodes are chosen for data retrieval tasks. Chainlink 2.0's whitepaper written by Breidenbach et al. (2021) investigates the reputation system's ability to monitor the performance history of individual nodes, providing rewards for those that consistently and accurately contribute data. This promotes the development of a reliable and effective network. The consideration of accuracy is crucial in the assessment of reputation. Nodes with a consistent track record of delivering accurate and reliable data are prioritized, while those that transmit erroneous or misleading information experience a decline in their reputation scores. The accuracy metric plays a crucial role in upholding the integrity of the data provided to smart contracts, as it directly influences the dependability of the automated processes overseen by these contracts (Breidenbach et al., 2021). Additionally, reliability, an essential metric, evaluates the duration of a node's operational status and its capacity to promptly fulfill data requests. Nodes that demonstrate a high level of reliability are those that consistently remain accessible and possess the capability to efficiently process data queries without experiencing substantial delays. Chainlink 2.0's whitepaper, written by Breidenbach et al. (2021) demonstrates that the maintenance of a robust and dependable data pipeline is guaranteed, even in instances of high load conditions. The third crucial metric, response time, measures the speed at which a node is able to retrieve and transmit the necessary data. Applications that necessitate real-time or near-real-time data, such as those utilized in financial markets or supply chain monitoring systems, rely heavily on rapid response times. Preferential nodes are those capable of expeditiously processing and transmitting data, thereby augmenting the overall efficiency and responsiveness of the Chainlink network (Breidenbach et al., 2021).

Chainlink also incorporates staking mechanisms, in addition to its reputation system, in order to enhance data integrity and discourage potential malicious activities. In order to participate in the network, nodes must adhere to the requirement of staking a specified quantity of cryptocurrency as collateral. The staked asset serves as a financial security measure, ensuring the integrity and reliability of the node. In the event that a node is discovered to be disseminating falsified or erroneous data, it is subject to the potential loss of its staked assets. Breidenbach et al. (2021) emphasized that this loss represents a significant economic deterrent, mitigating the inclination of malicious actors to tamper with the data stream. The staking mechanism functions based on the concept of economic incentives, ensuring that the financial interests of node operators are in line with the overall integrity of the network. Node operators are incentivized to uphold high levels of performance and integrity through the risk they assume with their own assets. The economic alignment plays

a crucial role in a decentralized setting, particularly in the absence of traditional trust mechanisms (Cai et al., 2022).

Moreover, the decentralized nature of Chainlink is also reflected in its governance model, which enables community involvement in decision-making mechanisms. The aforementioned includes protocol upgrades, modifications to economic incentives, and the incorporation of novel features. The implementation of a participatory model ensures that the network develops in a manner that aligns with the preferences and requirements of its users, thereby improving its resilience and flexibility.

In conclusion, decentralized oracles such as Chainlink present substantial benefits in comparison to centralized equivalents, as they facilitate the dispersion of trust and guarantee the integrity of data through a decentralized network of autonomous nodes. The implementation of rigorous security protocols, in conjunction with the establishment of a solid reputation and staking mechanisms, establishes a complex system of defense against potential threats. This serves to uphold the integrity and reliability of the data supplied by Chainlink oracles. The distributed characteristics of Chainlink's oracle network, bolstered by its sophisticated mechanisms, represents a substantial progression in establishing trust-minimized environments for blockchain applications (Breidenbach et al., 2021). The decentralized model presents several challenges, however, its advantages in terms of improved security, reliability, and fair distribution of trust make it an appealing option for the integration of real-world data into blockchain ecosystems.

Technical Background

The fundamental underpinning of decentralized oracles for blockchain technology is founded on the essential requirement to establish a connection between off-chain data and on-chain smart contracts, all the while upholding the decentralized and trustless attributes of blockchain systems. Centralized oracles, under the control of a sole entity, furnish information to smart contracts but are beset by vulnerabilities such as singular points of failure and susceptibility to malicious attacks, thereby diminishing the trustless nature of blockchain technology (Beniiche, 2020). The emergence of decentralized oracles is designed to mitigate these concerns through the dispersal of data retrieval and validation tasks among a network of autonomous nodes, thereby bolstering security, dependability, and expansibility.

Chainlink Architecture

Chainlink is considered to be one of the groundbreaking decentralized oracle solutions that utilizes a network of autonomous nodes to collect, validate, and consolidate data. The architectural framework of Chainlink comprises components operating both on the blockchain and off the blockchain. The on-chain infrastructure constitutes of smart contracts that are responsible for the management of reputation, order-matching, and data aggregation, as outlined in Chainlink 2.0's whitepaper (Breidenbach et al., 2021). The reputation system assesses nodes by considering historical performance metrics, including accuracy, reliability, and response time. This approach fosters a competitive atmosphere that encourages high-quality performance. Nodes that possess a higher level of reputation are inclined to be chosen for the execution of data retrieval tasks. Moreover, staking mechanisms necessitate nodes to immobilize cryptocurrency as a form of collateral, thereby acting as a deterrent against potential malicious behavior by exposing staked assets to the risk of forfeiture in the event of dishonest actions.

Decentralized Oracle Networks (DONs) and its Functionalities

Decentralized Oracle Networks (DONs) play a crucial role in augmenting the functionalities of smart contracts on various blockchain platforms by furnishing foundational computational resources, including networking, storage, and computation. The aforementioned resources are provided with a strong emphasis on confidentiality, integrity, and availability, thereby ensuring resilient and dependable operations. These networks are comprised of oracle nodes, which have the capacity to either carry out specific tasks or form enduring partnerships to deliver uninterrupted services. The setup is designed to be compatible with any blockchain, rendering DONs a versatile resource for application developers seeking off-chain assistance for their smart contracts.

The integration of executables and adapters is essential in the establishment of Decentralized Oracle Networks (DONs) architecture to effectively realize their capabilities. The integration of these components forms a durable and adaptable framework for off-chain computation and data management, allowing for seamless interaction with a variety of external systems and resources.

Executables

Executables can be understood as the central operational logic of smart contracts, functioning within the decentralized architecture of a DON. These programs are deterministic in nature, as their operations result in predictable outcomes based on the input data provided, thus guaranteeing consistency and reliability. In contrast to conventional smart contracts, executables do not directly store main-chain assets but offer significant advantages such as enhanced performance and the capacity to execute confidential computations.

The executables operate independently on a DON, consistently carrying out their pre-determined logic without the need for human intervention. Initiators activate specialized programs that invoke entry points in the executable's logic in response to pre-determined events. Various events can occur, including time-based triggers resembling cron jobs, as well as conditional occurrences such as changes in price thresholds or other external data modifications. This mechanism bears resemblance to the role of Keepers in blockchain ecosystems, as it serves to guarantee that predetermined conditions trigger the activation of contract functions.

Adapters

Adapters facilitate the exchange of data between executables and off-DON systems by serving as interfaces for sending and receiving information. They extend the scope of Chainlink's existing external adapters, enhancing their flexibility and enabling two-way communication. Adapters facilitate bi-directional data exchange between external sources and the DON, enabling data retrieval from external sources as well as data transmission from the DON to external systems, including web servers. The bidirectional functionality facilitates increased intricacy in interactions and data exchanges between the DON and the external environment.

Adapters have the capability to utilize distributed protocols and cryptographic features, such as secure multi-party computation, in order to guarantee the integrity and confidentiality of data. The capability enables DONs to conduct secure joint computations while maintaining the privacy of the data in question.

In the preliminary implementation of DONs, a predetermined collection of building block adapters will be incorporated to establish connections with frequently utilized external resources. The underlying adapters will facilitate fundamental functionalities and can be expanded as developers design additional specialized and robust adapters. The creation of permissionless adapters is anticipated to empower users in the independent development and deployment of new adapters independently, thereby stimulating innovation and growth within the DON ecosystem.

Operational Model

The conceptual model depicted in *Figure 2* illustrates the process by which a DON may transmit off-chain data to a smart contract on a blockchain platform. The executable utilizes adapters to retrieve off-chain data, which is subsequently processed and transmitted through another adapter to the specified blockchain target. Said executable possesses the capability to engage with local DON storage for the purposes of managing its state and facilitating communication with other executables. This integration of adaptable networking, computational capabilities, and storage facilitates the development of numerous innovative applications.

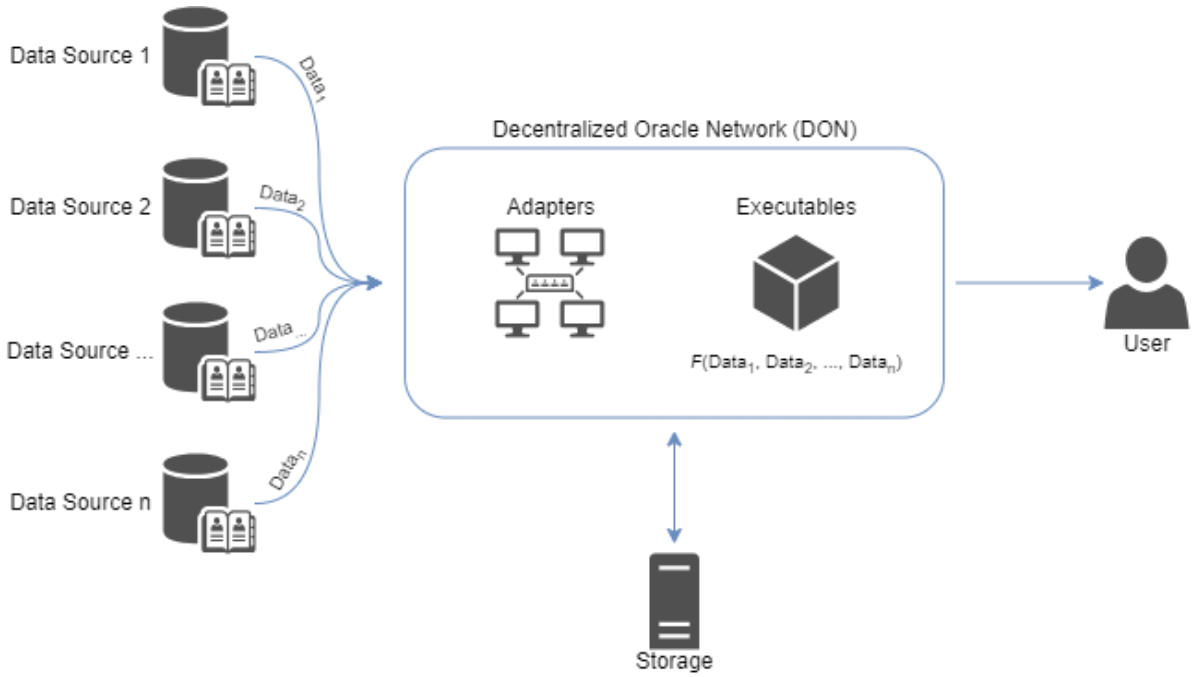

Figure 2. Decentralized oracle network data processing.

Some of Chainlink's Design Goals

The Chainlink platform is formulated with a comprehensive set of seven specific design objectives, including the implementation of hybrid smart contracts, the abstraction of complexity, scalability, confidentiality, order-fairness for transactions, trust minimization, and the incorporation of incentive-based (cryptoeconomic) security measures (Breidenbach et al., 2021). However, the following section will focus on the three components that have been considered to be most important.

Scaling

An essential objective in the progressive development of the Chainlink network is to tackle the increasing scalability requirements of the blockchain ecosystem. As the issue of network congestion becomes increasingly prevalent in permissionless blockchains, there has been a trend towards the implementation of innovative and more efficient blockchain designs, along with the use of supplementary layer-2 scaling technologies, in order to address and alleviate

these challenges. The oracle services need to adhere to strict latency and throughput demands of the systems, while also aiming to reduce on-chain fees, including gas costs, for contract operators and regular users. Therefore, the implementation of Decentralized Oracle Networks (DONs) within Chainlink is intended to exceed current constraints by achieving performance levels suitable for purely web-based systems (Breidenbach et al., 2021).

DONs experience considerable improvements in performance by employing rapid, committee-based, or permissionless consensus protocols. The integration of these protocols with the blockchains they support establishes a symbiotic relationship that contributes to the optimization of the system's performance as a whole. The simultaneous operation of multiple decentralized oracle networks (DONs) with diverse configurations enables a range of decentralized applications (DApps) and users to assess and make trade-offs in the underlying consensus mechanisms based on their specific application needs. The adaptability of DONs enables them to address a diverse array of performance requirements across various usage scenarios.

DONs can be regarded as layer-2 technologies within the context of network architecture. The duties of DONs encompass a wide array of responsibilities, including the provision of support for the Transaction Execution Framework (TEF). The TEF plays a crucial role in enabling the seamless integration of DONs with other advanced layer-2 systems, thereby enhancing overall system performance. One exemplification of such a system is rollups, which aggregate transactions off-chain in order to realize significant enhancements in performance. This framework facilitates the seamless integration of DONs with other sophisticated scaling solutions, thus augmenting the overall scalability of blockchain networks.

The conceptual model depicted in *Figures 3* and *4* provides a thorough explanation of how DONs contribute to the scalability of blockchain-based smart contracts. The conventional oracle architecture, as illustrated in *Figure 3*, involves the direct submission of transactions and oracle reports to the blockchain, thereby positioning the blockchain as the central hub for transaction processing. The traditional method frequently leads to elevated latency and augmented costs as a consequence of the blockchain's constrained ability to proficiently process a large number of transactions.

On the other hand, *Figure 4* illustrates the novel application of decentralized oracle networks to facilitate the implementation of smart contracts within the blockchain technology. The aforementioned DON executable conducts the processing of transactions in conjunction with

data sourced from external systems, thereafter forwarding the outcomes, such as aggregated transactions or changes in contract state resulting from the effects of the transactions, to the blockchain. By relocating the central point of computation from the blockchain to the DON, this architecture notably diminishes transaction latency and costs, alongside increasing transaction throughput. The DON which is visually represented in blue in *Figure 4*, serves as the central hub for transaction processing, effectively reducing the strain on the blockchain and improving the overall scalability of the system.

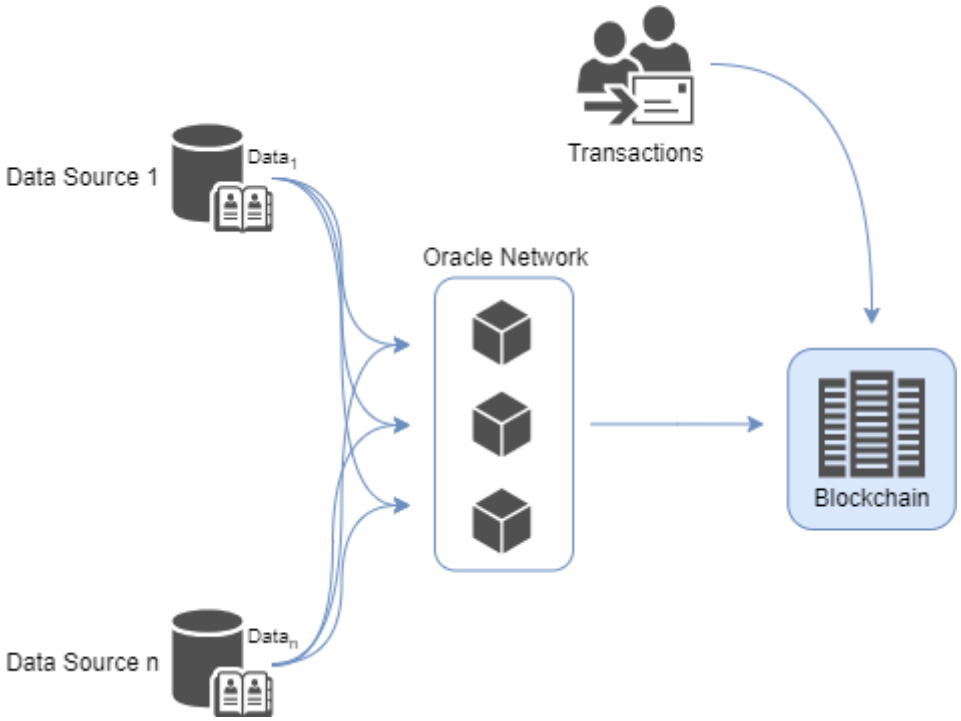

Figure 3. Conventional oracle architecture.

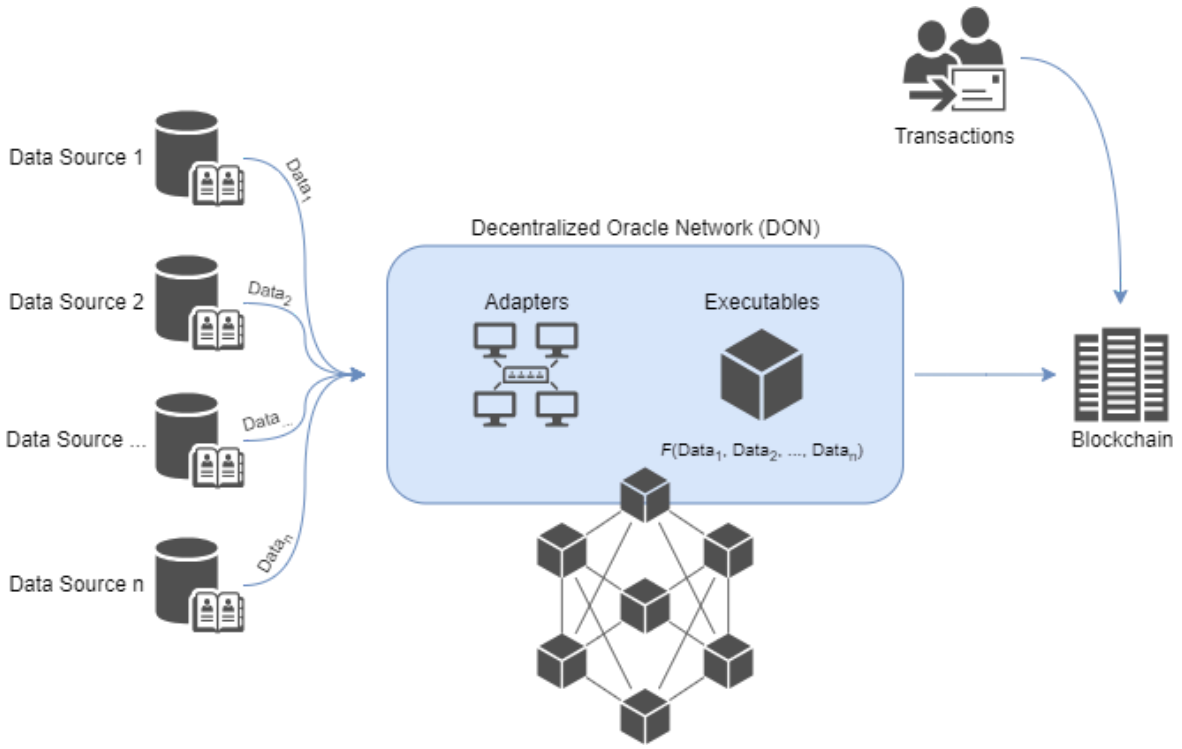

Figure 4. Use of a DON to support contracts on the blockchain.

Trust Minimization

The overarching objective of Chainlink in the development of Decentralized Oracle Networks (DONs) is to establish a robust and reliable infrastructure to support smart contracts and other systems reliant on oracles, utilizing decentralization, cryptographic mechanisms, and cryptoeconomic incentives. The decentralized nature of a DON allows users to select from a range of available DON options that align with their desired main chain, or alternatively create new DONs with trusted node committees. In certain use cases, particularly those involving smart contracts, users of Chainlink may exhibit a preference for a trust model that regards the primary blockchain upheld by a decentralized oracle network (DON) as more reliable than the DON. Chainlink has integrated various mechanisms into the architecture of the Chainlink network to provide security enhancements for contracts on a main chain, as well as to implement safeguards against potential corruption of data sources, such as web servers, from which the Decentralized Oracle Network (DON) gathers data (Breidenbach et al., 2021). Additionally, Chainlink plans to continue incorporating these mechanisms to further enhance the security assurances provided by DONs.

One salient factor in trust minimization pertains to the authentication of data sources. The implementation of digital signing tools by data providers serves to greatly enhance the integrity of the chain of custody, thereby bolstering the credibility and reliability of the data exchange process between the source and the recipient of the contract. At present, the operational frameworks for oracles are limited by the insufficient implementation of data signing on a broad scale, mainly attributable to the fact that Transport Layer Security (TLS) does not inherently incorporate data signing functionality. Nevertheless, the TLS protocol does employ digital signatures in its handshake protocol to facilitate the establishment of a mutually shared key between a server and a client. Servers that are enabled with HTTPS have certificates containing public keys which have the theoretical capability to sign data. However, it is uncommon for these certificates to be utilized for data signing. Consequently, the security of a decentralized oracle network (DON) is contingent upon the reliable transmission of data by oracle nodes from a designated data source to a smart contract, similar to contemporary oracle networks.

Chainlink's overarching goal of trust minimization includes the enhancement of data-source authentication by advocating for the adoption of tools and standards for data signing. The utilization of data signing can be advantageous in ensuring the enforcement of end-to-end integrity guarantees. If a contract is designed to accept data directly signed by a verified data source, the oracle network is unlikely to have the capability to tamper with such data. Numerous initiatives have been undertaken to facilitate the authentication and verification of data through the implementation of protocols such as OpenID Connect, TLS-N, and TLS Evidence Extensions. OpenID Connect has experienced a certain degree of adoption, however, the widespread adoption of TLS Evidence Extensions and TLS-N has not yet been achieved. A further possible option involves the utilization of Signed HTTP Exchanges (SXG) by publishers, which have the capability to be cached on content-delivery networks within the framework of the Accelerated Mobile Pages (AMP) protocol. This approach offers a straightforward and secure mechanism for Chainlink oracles to activate in response to significant events documented in valid SXGs. This capability may be especially valuable for contracts associated with real-world occurrences such as severe weather conditions or election results (Breidenbach et al., 2021).

It is commonly accepted that the simple deployment, sophisticated tools, and adaptability are essential for expediting the authentication of data sources. The utilization of Chainlink nodes as an authenticated API front end by data providers appears to be a promising strategy. Chainlink's objective is to establish a capability for nodes to operate in either a standalone mode or as a full-fledged oracle within the network. The capability known as authenticated

data origination (ADO) enables data sources to utilize the expertise and resources developed by the Chainlink community for integrating digital signing capabilities into their pre-existing suite of off-chain APIs. If individuals opt to operate their nodes as oracles, they have the opportunity to expand potential revenue streams by following the same business model as established data providers such as Kraken and Kaiko, who operate Chainlink nodes to offer API data on-chain.

An additional mechanism for reducing the reliance on trust within decentralized oracle networks (DONs) is the implementation of minority reports within the network. The flags are issued by a minority segment of DON nodes that detect prevalent misconduct within the network. A minority subset of honest nodes has the capability to produce a minority report of sufficient size, which is then transmitted to a dependent smart contract on the blockchain. The dependent contract has the capability to utilize this flag in accordance with its particular policy, which may include the solicitation of additional reports from another DON or the activation of a circuit breaker. The significance of minority reports persists despite the honesty of the majority, as any system for aggregating reports must function within a threshold framework to safeguard against potential failures in the form of unreliable or compromised information sources. By augmenting the DON protocol to ensure that every node is cognizant of the data utilized in creating a report, nodes could identify and highlight patterns of bias towards certain sets of reports, ultimately generating a dissenting report.

Guard rails further enhance security by identifying abnormal conditions and temporarily suspending or halting the execution of contracts. The aforementioned mechanisms may be integrated into smart contracts on the primary blockchain or directly within a subsidiary contract. Circuit breakers, for instance, have the capability to temporarily suspend or terminate state updates, either in response to the specific characteristics of the state updates or in response to external inputs. The implementation of these measures can effectively mitigate the risk of erroneous reporting by DONs and allow for the allocation of resources towards further interventions, such as escape hatches. Escape hatches provide the capability for a contract to cease operation in the event of unfavorable circumstances, thereby concluding any ongoing transactions and returning custodied funds to users. Failover mechanisms are implemented to ensure continuous service availability in the event of a DON failure or misbehavior. These mechanisms allow dependent contracts to offer alternative interfaces and enable users to submit reports in instances where the DON fails to do so.

Ensuring low levels of trust in governance is essential for the proper functioning of the Chainlink network. The methodology encompasses the implementation of incremental dissemination of updates for community scrutiny, as well as decentralized emergency interventions for prompt response in the event of system malfunctions. Evolutionary governance enables the community of a particular organization affected by proposed changes to approve non-urgent modifications, whereas emergency governance is responsible for addressing immediate threats to the integrity of the system. The governance of DONs must be flexible in accommodating variations in operational goals and parameters. Chainlink's current focus is on actively exploring design concepts to facilitate this requirement.

Finally, incorporating decentralized entity authentication through Public-Key Infrastructure (PKI) is of paramount importance in the identification of participants within the Chainlink network. Chainlink is poised to adopt decentralized name services, such as the Ethereum Name Service (ENS), to serve as the fundamental infrastructure for its Public Key Infrastructure (PKI) in the future. The Ethereum Name Service (ENS) facilitates the mapping of human-readable Ethereum names to blockchain addresses, thereby establishing a secure and immutable directory service for data feeds on the blockchain. The system provides robust security measures and automated on-chain dissemination of updates, effectively safeguarding the integrity and accessibility of oracle data feeds. The validation of names within the Public Key Infrastructure (PKI) is expected to undergo a transition towards a decentralized model that integrates a web-of-trust and incorporates validating data, thereby improving the assurance of network security.

Incentive-based Security

The decentralization of report generation across oracle nodes is of paramount importance in maintaining security, particularly in the event of compromised nodes. An equally significant factor pertains to the deployment of financial incentives that serve to encourage proper conduct among nodes. One major incentive used by numerous protocols and projects is staking.

Staking constitutes a foundational approach for enhancing the security of a decentralized system by implementing highly measurable economic incentives. In a staking arrangement, individuals contribute a cryptocurrency collateral that is subject to partial or complete forfeiture in the event of non-compliance with the designated protocol. In the framework of

Chainlink, oracle nodes participate in staking as a means to ensure the veracity of their data outputs, with the acknowledgment that any failure to deliver accurate reports will lead to the loss of their staked resources (Breidenbach et al., 2021).

Chainlink's staking mechanism introduces the notion of super-linear staking impact, which represents a significant advancement in the field. This principle posits that in order to successfully compromise the network, an adversary must have a financial resources that surpass the total deposits of all oracle nodes. To be more precise, the adversary's budget must demonstrate a super-linear increase in relation to the quantity of nodes within the network. In practical terms, assuming that each of the n nodes stakes an amount d, it can be inferred that the adversary would require a budget substantially exceeding the product of n and d in order to compromise the network. This framework provides a strong level of economic stability in guarding against bribery, particularly in networks where nodes have invested moderate amounts. As a result, attempts to carry out such attacks are deemed highly impractical.

Chainlink 2.0 Whitepaper presents a range of developments aimed at substantially improving the functionality of Decentralized Oracle Networks (DONs), particularly through the facilitation of secure off-chain computations. Decentralized oracles networks (DONs) expand the scope of smart contracts by granting them access to a wider range of decentralized services that go beyond the simple delivery of data. This enables the creation of a more comprehensive hybrid infrastructure for developers, allowing for the seamless integration of on-chain code with off-chain resources to produce more complex and advanced smart contracts. An essential factor in facilitating these sophisticated hybrid smart contracts is the establishment of a resilient cryptoeconomic security framework for decentralized oracle networks (DONs) that effectively mitigates the financial feasibility of potential attacks. It is imperative to recognize the significance of DONs undertaking increasingly critical responsibilities in safeguarding essential operations within high-value smart contracts that have significant effects on user funds.

In order to enhance resistance against tampering, the Chainlink 2.0 proposes the implementation of Explicit Staking, an advanced cryptoeconomic mechanism in which Chainlink nodes pledge LINK tokens as collateral, subject to potential reduction in cases of malevolent or undesired conduct (Breidenbach et al., 2021). The staking model is characterized by its unique design aimed at protecting against various well-capitalized adversaries, resulting in a super-linear staking impact. This mechanism serves to guarantee that the financial resources needed for malicious entities to successfully manipulate a

Decentralized Oracle Network (DON) are notably greater than the total deposits of all involved nodes. This ensures a considerable level of security for high-value smart contract applications in a cost-effective manner.

Said staking approach is characterized by an adversarial model that encompasses a comprehensive range of attacks commonly disregarded in current methodologies. A noteworthy concern is the potential for prospective bribery, which involves the provision of conditional bribes to randomly selected nodes with particular roles, such as those responsible for initiating report adjudication. The staking mechanism implemented by Chainlink is designed to mitigate potential threats posed by intricate, conditional bribery tactics. This system operates under the assumption that nodes, with the exception of the aggressor, behave based on economic rationality rather than inherent integrity. The model also posits the presence of a veritable source of truth that is cost-prohibitive for ordinary use but attainable in instances of discord, thereby serving as a contingency to safeguard the coherence of the network.

The explicit staking mechanism employed by Chainlink serves a distinct purpose when compared to staking in other blockchain networks. Proof-of-Stake blockchains implement staking in order to attain worldwide consensus on transactions, whereas Chainlink's specific staking mechanism is designed to guarantee the generation of trustworthy and tamper-proof oracle reports that faithfully represent the status of real-world occurrences beyond the confines of a blockchain. The principal objective is to optimize the cryptoeconomic security of Decentralized Oracle Networks (DONs), in order to offer users heightened confidence in the accuracy and promptness of external data and off-chain computations upon which their significant hybrid smart contracts rely.

Chainlink 2.0's Whitepaper (Breidenbach et al., 2021) provides an in-depth discussion of the implementation of explicit staking to ensure the security of decentralized oracle networks (DONs) in the delivery of financial market data on-chain. This data is widely recognized as a crucial resource for numerous decentralized finance (DeFi) applications. The explicit staking mechanism is composed of various autonomous elements that collectively contribute to considerable cryptoeconomic security. Each Decentralized Oracle Network (DON) operates under a service agreement that outlines the required stake of LINK tokens for each oracle node and establishes key performance metrics, such as acceptable variances in individual node responses and aggregate values in oracle reports. The service agreement also encompasses criteria such as data sources, update frequencies, and node compensation.

The outputs produced by a DON are structured into reporting rounds, wherein a new oracle report is generated for each round, comprising individual node responses pertaining to a specific data point. These responses are then aggregated to derive a single value. The service agreement pertaining to a DON outlines the specific protocols and requirements for generating reports, as well as the criteria for potential slash of a node's stake. Nodes chosen to participate in a DON can undergo a filtration process utilizing established Chainlink reputation frameworks, such as the Chainlink Market. This platform displays historical performance metrics of nodes, including uptime, latency, response deviation, supported networks, and data sources, to aid in the selection process.

In order to adhere to the terms stipulated in the service agreement, a two-tier oracle network design will be put into effect. The design under consideration encompasses a first-tier DON characterized by high efficiency and low cost. In this network, individual nodes engage in explicit staking of LINK tokens and routinely produce aggregated oracle reports. Moreover, a higher-cost second-tier DON with maximum-security measures will address and settle any disputes regarding the accuracy of first-tier oracle reports. The implementation of a two-tier system is designed to enhance operational efficiency under normal circumstances, while also placing emphasis on the importance of tamper-resistance and accuracy during second-tier arbitration. This approach serves to ensure that first-tier nodes are held responsible for any instances of malicious conduct or subpar performance.

The Chainlink Network, in its present state, is responsible for the execution of a significant number of on-chain transactions and the safeguarding of a sizeable amount of capital within the decentralized finance (DeFi) sector, amounting to tens of billions of dollars. The current cryptoeconomic incentives have effectively ensured the dependability of established Chainlink node operators, who consistently provide precise oracle reports on-chain even in the face of blockchain network congestion. The Chainlink 2.0 model has incorporated a secondary arbitration layer as a proactive measure to enhance security assurances. In the event of a dispute arising from an oracle report produced by the first-tier network, resolution would entail the involvement of a deliberative second-tier committee comprised of numerous independent Chainlink users, including but not limited to Aave, Synthetix, and Compound (Breidenbach et al., 2021). This process is characterized by its deliberative and inclusive nature, involving hundreds and potentially thousands of members. The individuals in question would participate in the assessment of the veracity of the initial oracle report by utilizing cryptographic TLS proofs generated by DECO. This would provide conclusive evidence based on Zero-Knowledge Proofs from one or more data providers.

Participants of the second-tier possess considerable economic motivations to effectively address conflicts in order to uphold the security, prestige, and usability of their applications, and to safeguard the value of their application's inherent token. Despite the potential for a minority of users to engage in malicious voting behavior, it is important to recognize that the majority of second-tier participants have substantial vested interests in the accurate and fair resolution of disputes. These participants are the core development teams responsible for the management of Chainlinked applications and Decentralized Autonomous Organizations (DAOs) which oversee the governance of said applications. The security of the second tier in terms of cryptoeconomics is positively correlated with the aggregate economic value of all governance tokens employed in the process of resolving disputes.

In order to guarantee the activation of the second-tier oracle network in the event of a dispute, any node within the first-tier network possesses the capability to function as a watchdog by issuing an alert in the event that it identifies a potential discrepancy in the aggregate value derived from an oracle report. In each reporting cycle, nodes within the primary network are arbitrarily assigned a public priority number which dictates the sequence in which their alerts are handled by the secondary network. In the event of a validated alert, the staked LINK held by the malicious majority of first-tier nodes is subject to slashing and subsequently allocated to the highest priority watchdog node. This results in a substantial financial motivation for first-tier nodes to serve as economically rational monitors, as they have the potential to receive substantial compensation for accurately detecting and reporting inaccurate aggregate reports.

The prioritized watchdog report system incentivizes the concentration of rewards, leading to a staking impact that grows at a super-linear rate. This suggests that there is a quadratic relationship between the number of nodes and the financial resources needed for a malicious actor to successfully compromise a DON. As the number of nodes increases, there is a proportional increase in the financial requirements, providing robust resistance against even well-funded adversaries. In order to evade the triggering of alerts, a malicious actor would be required to provide a bribe to every first-tier node equivalent to the complete aggregated reward amount, thereby substantially increasing the overall expense associated with a feasible bribe.

To quantify this super-linear staking impact, consider a first-tier DON with n nodes, each staking d amount, resulting in a total network stake of dn. Compromising the network requires corrupting a majority of nodes, representing at least $dn/2$ in staked funds. If an alert is raised and validated, the highest priority watchdog receives at least $dn/2$ from the

slashed malicious nodes. Consequently, the total budget an adversary needs to corrupt a first-tier DON is at least $dn^2/2$, a value that scales quadratically with the number of nodes.n nodes, each staking d amount, resulting in a total network stake of dn. Compromising the network requires corrupting a majority of nodes, representing at least $dn/2$ in staked funds. If an alert is raised and validated, the highest priority watchdog receives at least $dn/2$ from the slashed malicious nodes. Consequently, the total budget an adversary needs to corrupt a first-tier DON is at least $dn^2/2$, a value that scales quadratically with the number of nodes.

The explicit staking mechanism of Chainlink 2.0 delineates three possible results following the publication of an aggregated oracle report by a first-tier DON: full agreement, partial agreement, and alert. In complete agreement, the consensus among all primary nodes is unanimous in asserting the accuracy of the aggregated value, and each individual node is duly remunerated for their contributions. In partial agreement, it is noteworthy to consider that while a portion of nodes may be offline or have corrupted data, however, the majority of nodes consistently generates accurate values. Therefore, nodes that operate with integrity receive compensation, while those that exhibit faults experience a moderate reduction in their stake. In the event of an alert, if the second-tier network verifies that the combined report was inaccurate, the entirety of the stake held by the malicious nodes is slashed, with the resulting amount being awarded to the most prioritized watchdog. Should the alert be determined to be incorrect, the nodes responsible for alerting will have their stake reduced in a moderate manner.

This explicit staking mechanism implemented in the system serves to incentivize first-tier nodes to deliver precise and dependable data, as well as to disclose any malicious behavior exhibited by other nodes. Individuals are able to acquire misreporting insurance from underwriters, which offers indemnification in the event that an inaccurate oracle report is produced. This form of insurance can be implemented using on-chain smart contracts, which rely on authenticated reports from first-tier and second-tier networking sources.

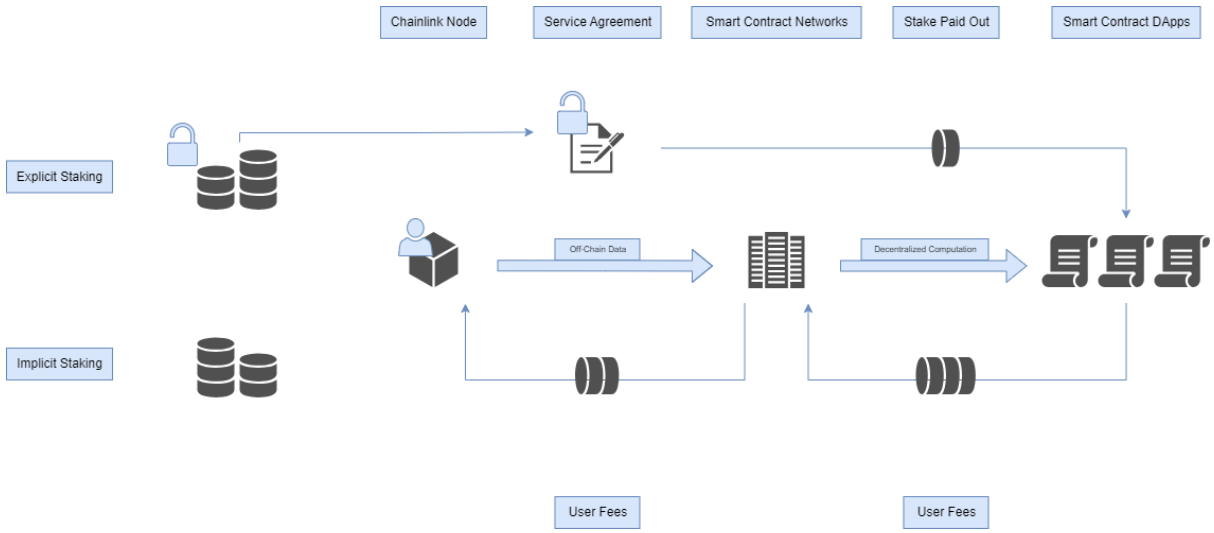

Figure 5. The concept of Chainlink staking involves the combination of implicit staking through oracle node reputation systems and potential future fee opportunities, as well as explicit staking through node deposits.

The Implicit-Incentive Framework (IIF) serves as an additional incentive, offering a novel model that expands beyond explicit staking deposits to encompass nodes' potential future fee opportunities (FFO). This framework incorporates a range of empirically measurable incentives, facilitating a holistic strategy for upholding economic security within the Chainlink network. The IIF incorporates various essential components, such as the past performance records of nodes, access to proprietary data, involvement in reputable decentralized organizational networks, and interaction across multiple platforms. The confluence of these factors exerts a collective influence on the financial interests of nodes, thereby providing them with incentives to adhere to proper behavior.

Nodes in the Chainlink ecosystem are engaged in activities not only to generate short-term profits, but also to strategically position themselves for prospective opportunities. The involvement of individuals in the project contributes to the establishment of a strong reputation, a successful track record, and specialized knowledge, consequently giving the project a competitive advantage in light of the introduction of new Chainlink services. Respected organizations like T-Systems and Kraken have demonstrated foresight in recognizing the long-term potential of the network and have proactively chosen to align themselves with it in order to capitalize on its inherent advantages. This speculative FFO may serve to strengthen the intrinsic motivations for nodes to uphold superior performance and dependability.

The total assets at stake for a given Chainlink node operator can be expressed as $S \approx D + F + FS + R$, where D represents the aggregate of all explicitly deposited stake across all networks in which the operator participates, F denotes the net present value of the aggregate of all future fee opportunities (FFO) across all networks, FS accounts for the speculative FFO based on potential future earnings, and R reflects the reputational equity of the operator outside the Chainlink ecosystem that might be jeopardized by identified misbehavior in its oracle nodes. This equation highlights the multiplicity of economic factors favoring high-reliability performance by Chainlink nodes, emphasizing that their incentives extend beyond immediate financial returns to include long-term reputational and operational benefits.$S \approx D + F + FS + R$, where D represents the aggregate of all explicitly deposited stake across all networks in which the operator participates, F denotes the net present value of the aggregate of all future fee opportunities (FFO) across all networks, FS accounts for the speculative FFO based on potential future earnings, and R reflects the reputational equity of the operator outside the Chainlink ecosystem that might be jeopardized by identified misbehavior in its oracle nodes. This equation highlights the multiplicity of economic factors favoring high-reliability performance by Chainlink nodes, emphasizing that their incentives extend beyond immediate financial returns to include long-term reputational and operational benefits.

The convergence of the Initial Interest Factor (IIF) and super-linear staking impact engenders a virtuous cycle of economic security for oracle networks. As the network attracts new users, the potential for future earnings from operating Chainlink nodes grows, thereby diminishing the marginal cost of economic security. The decrease in cost serves as a motivation for more individuals to employ the network, thereby sustaining a recurring pattern of ongoing acceptance and expansion as observed in *Figure 6*.

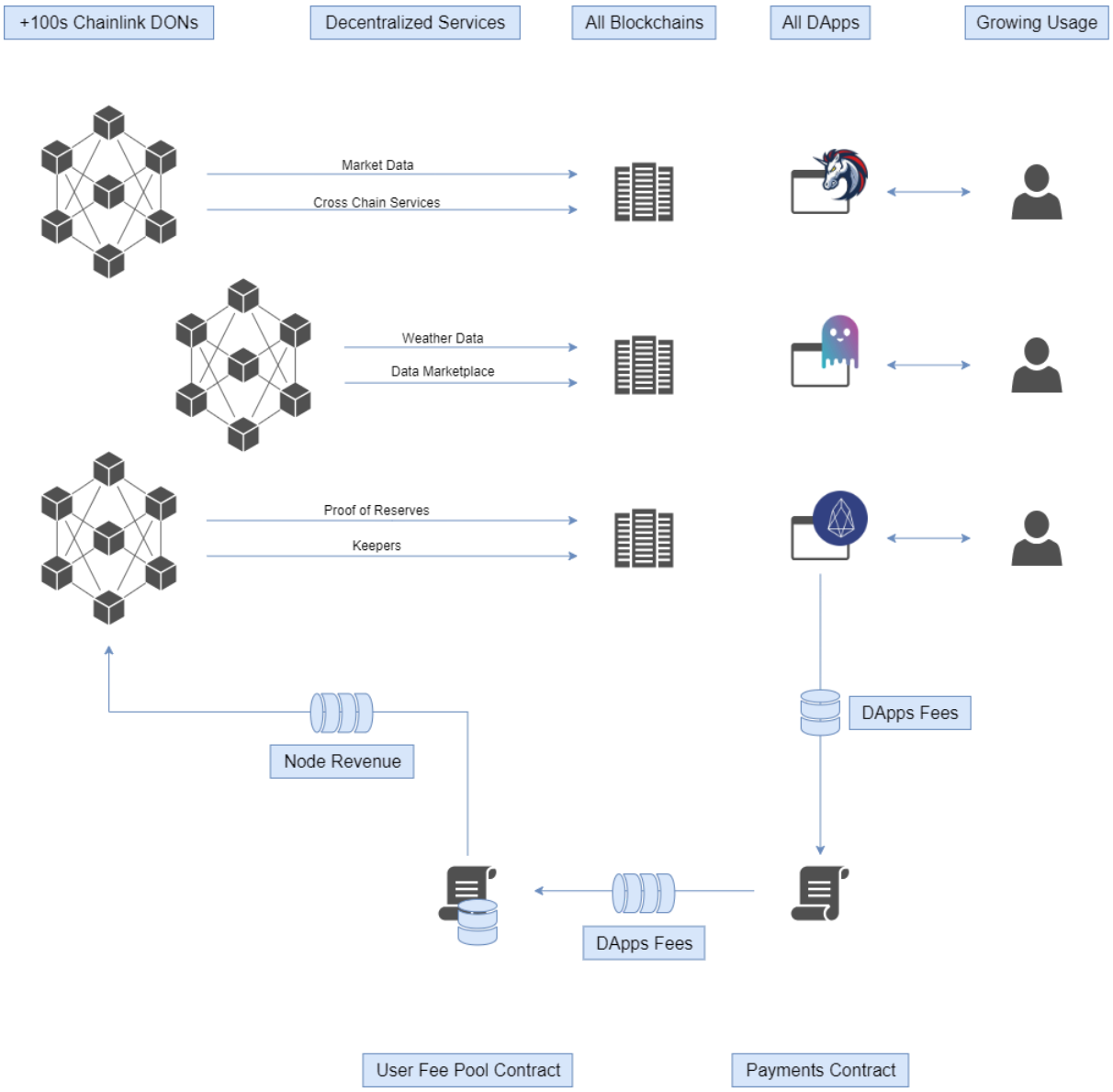

Figure 6. An increasing number of decentralized applications (dApps) are integrating trust-minimized Chainlink services, resulting in a higher influx of fees directed towards Chainlink's oracle networks.

Node Operators

Chainlink node operators are essential components of the Chainlink Network (which is depicted in *Figure 7*), possessing a critical function in guaranteeing the secure and dependable functionality of decentralized oracle networks. The operators are responsible for overseeing the fundamental oracle infrastructure, which facilitates the interaction of smart

contracts from different blockchains with the real-world data required for their execution. The Chainlink platform utilizes a wide variety of node operators to collaboratively support decentralized Price Feed oracle networks, which are currently responsible for securing more than $22 billion in value across prominent DeFi applications including Synthetix, Aave, Compound, dYdX, Liquity, and others (Breidenbach et al., 2021).

The oracle problem, which is intrinsic to smart contracts as a result of the security features of blockchains, creates a barrier for on-chain systems in accessing data directly from off-chain sources. This requirement underscores the necessity of employing oracles as a middleware solution to enable the seamless transfer of data between on-chain and off-chain ecosystems in a bidirectional manner. Chainlink node operators are responsible for managing the hardware and software infrastructure essential for the functioning and protection of each oracle network within the Chainlink Network. Said operators are responsible for actively monitoring the blockchain for incoming data requests originating from smart contracts. They are tasked with retrieving the requested off-chain data from designated APIs and subsequently delivering the data on-chain. This process ultimately allows smart contracts to execute functions based on real-world information. In essence, oracles function as an intermediary linking blockchains with external data and systems, essentially serving as a bridge between the two.

Smart contracts have the capability to transmit data requests to an individual Chainlink node and subsequently obtain a singular response. However, the full potential of Chainlink nodes is harnessed when they are amalgamated into decentralized oracle networks. The networks in question function to collect data from numerous nodes with the aim of mitigating potential single points of failure in both data sourcing and delivery to the blockchain. This subsequently serves to bolster the resilience and dependability of the provided data.

The Chainlink Network comprises an indefinitely scalable network consisting of independent oracles and oracle networks. Each individual oracle independently operates the Core Chainlink software, functioning without reliance on other oracles, and has the ability to engage in multiple oracle networks concurrently. The Chainlink Network operates on a permissionless basis, thereby enabling any user to operate an oracle. However, it is noteworthy that individual oracle networks may impose limitations on the oracles that can participate and may also tailor the manner in which data is acquired and aggregated. In contrast to blockchains, Chainlink does not employ a unified consensus mechanism or a single node network (Breidenbach et al., 2021). This absence allows for a significantly increased level of flexibility and adaptability within the system.

In order to assume the role of a node operator within the Chainlink Network and commence the provision of external data to smart contracts, there exist particular technical prerequisites that must be met. The fundamental elements of a Chainlink node configuration consist of the open-source Chainlink Node Client Software, which serves as the interface between on-chain and off-chain ecosystems; the on-chain oracle contract, responsible for tracking data queries and transmitting responses to the user's smart contract; subscriptions to data sources, comprising off-chain data source APIs accessed by a Chainlink node to retrieve data for requesting smart contracts; and external monitoring systems, which are ancillary off-chain infrastructures that monitor the real-time performance and reliability of a Chainlink node. Chainlink node operators regularly engage with these components to guarantee the secure delivery of data to any blockchain.

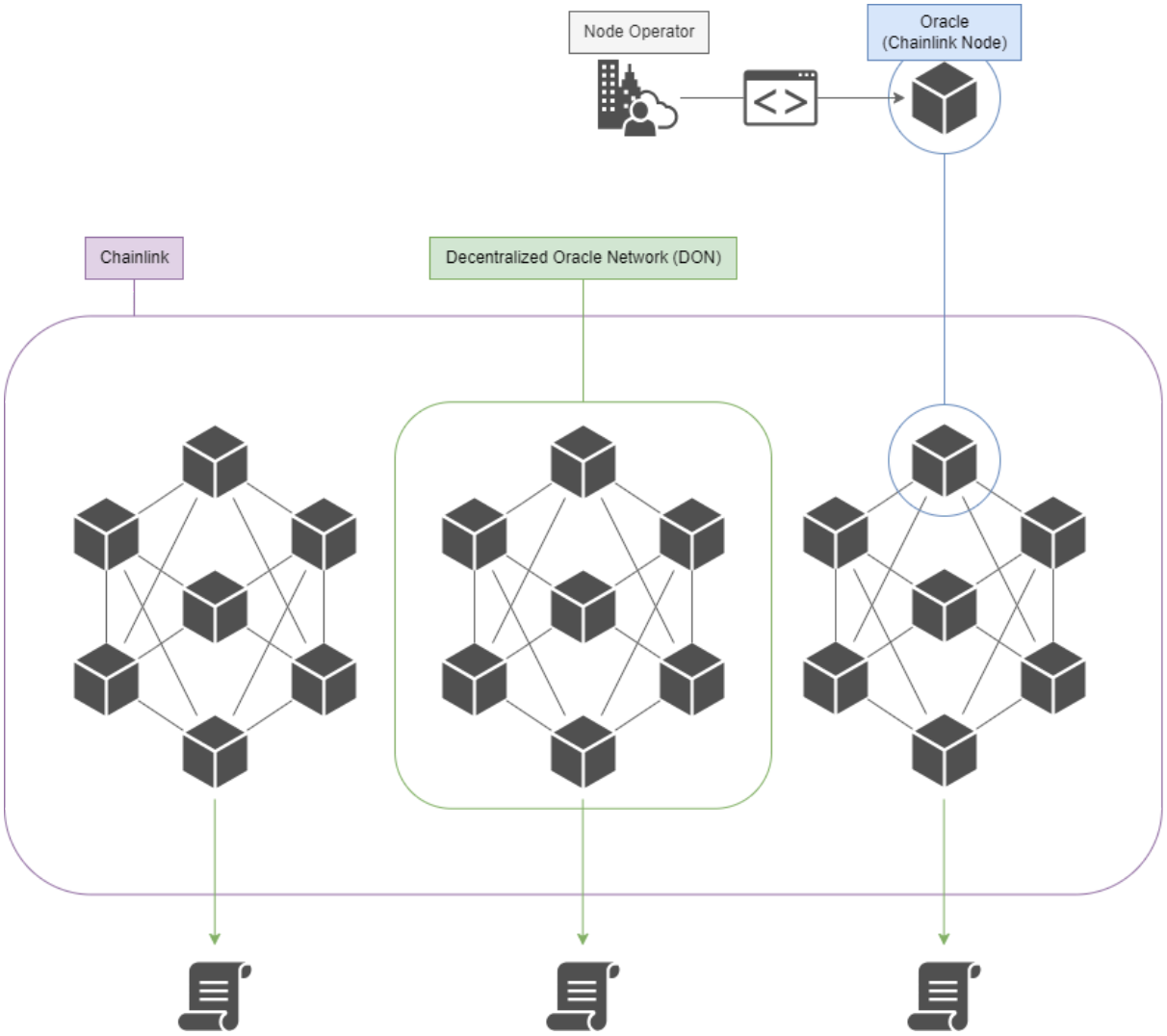

Figure 7. Chainlink's oracle network components.

The Chainlink Network provides support for two distinct models for Chainlink nodes: the Standard API Model and the Origin Signed Data Model.

The Standard API Model (*Figure 8*) delineates a clear separation between the node operator and the data source. Chainlink nodes procure data directly from data providers, thereby enabling its accessibility across various blockchains without necessitating the data provider to establish new infrastructure or modify their existing business model (Breidenbach et al., 2021). The seamless onboarding process facilitates the integration of data and API services into blockchains without imposing additional costs or responsibilities on data providers.

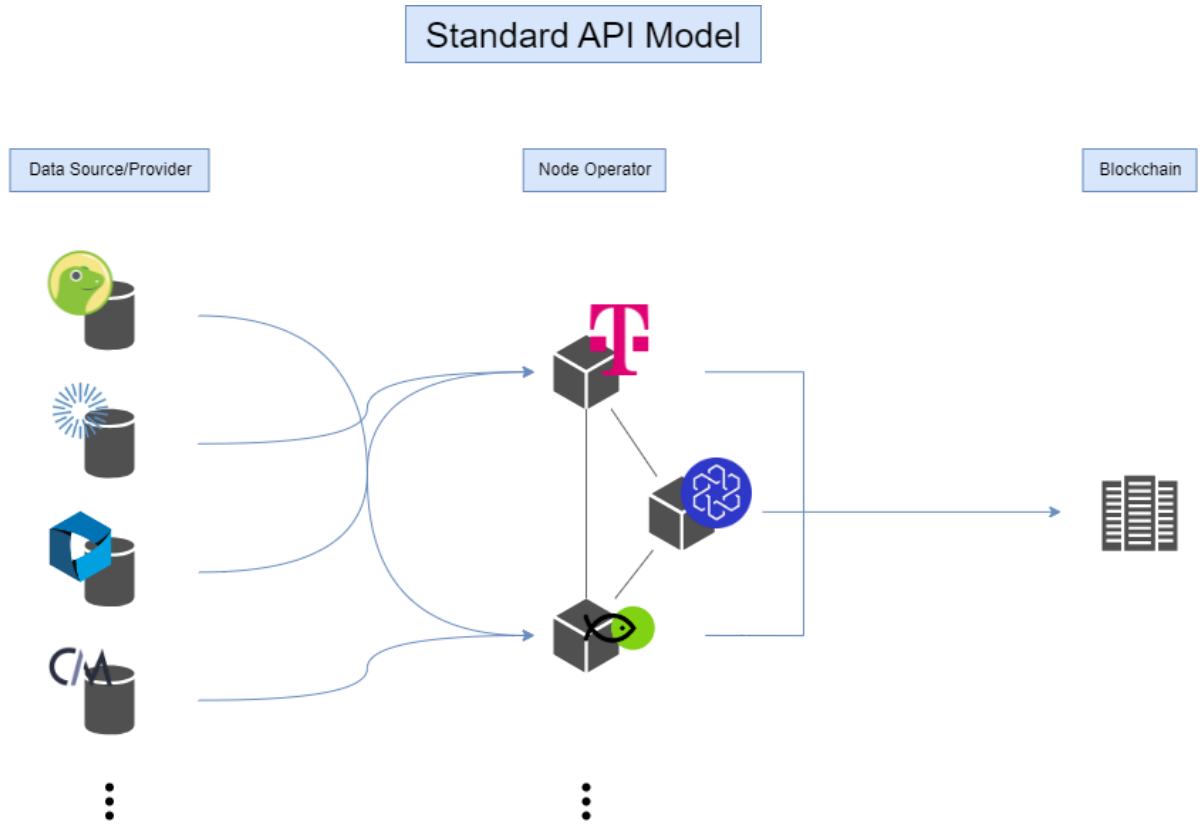

Figure 8. Standard API node model.

The Origin Signed Data Model (*Figure 9*) involves data providers operating their own Chainlink nodes, which enables them to digitally sign their data using a distinct private key and transmit it directly to smart contracts. This model has been designed to improve Sybil resistance by providing end-users with the capability to authenticate the source of the data. Furthermore, it eliminates intermediaries in the process of data sales to smart contracts, leading to an augmentation in the revenue of the data provider and solidifying their standing as trustworthy sources within the Chainlink ecosystem (Breidenbach et al., 2021). The integration of both models within a singular decentralized oracle network serves to lower the

barriers to entry into the Chainlink Network and enhance the accessibility of datasets to smart contracts, all while mitigating any additional burdens on current data providers.

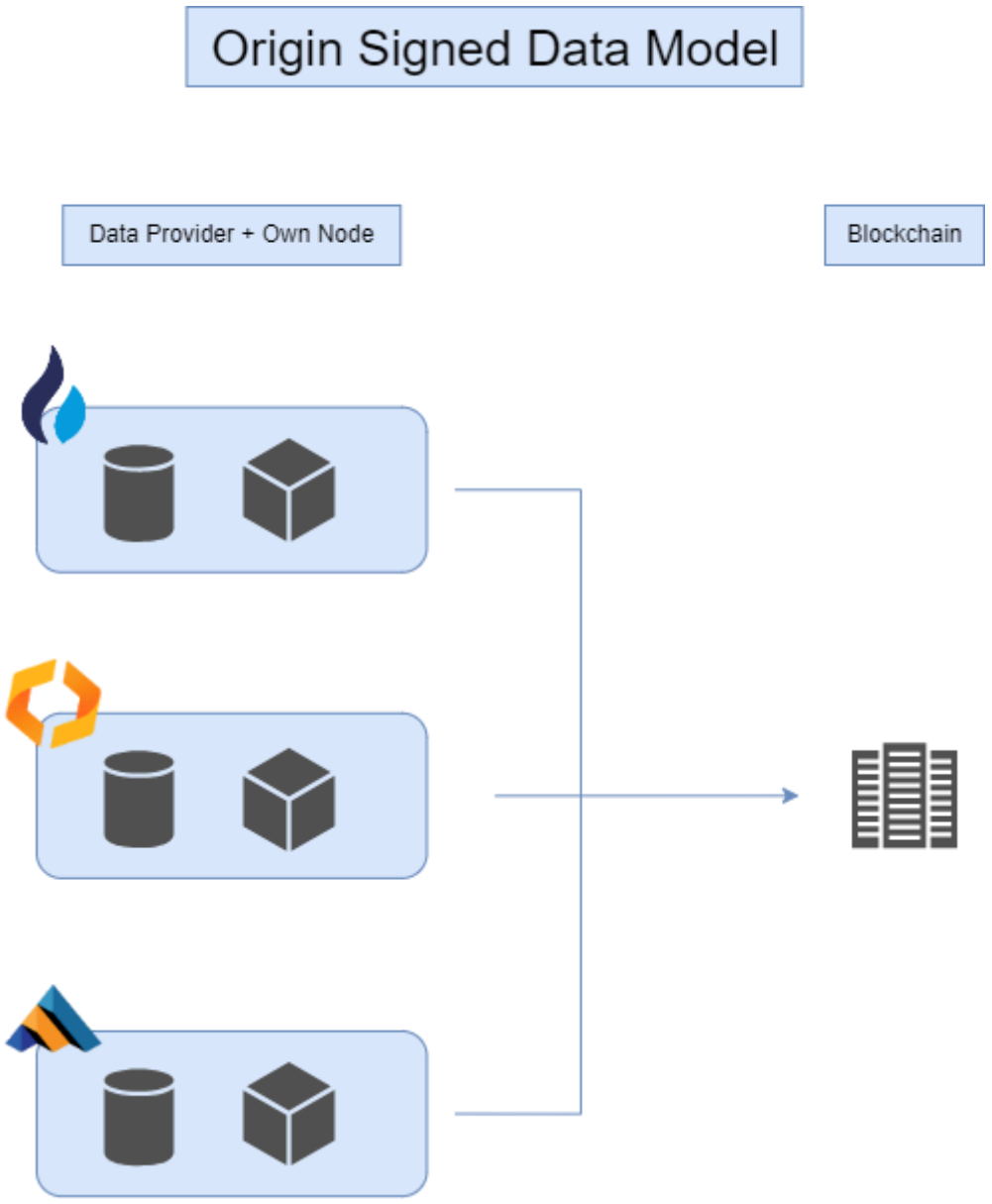

Figure 9. Origin signed data node model.

The Chainlink Network is guided by a philosophy of "security through transparency", wherein each node possesses a distinct public address through which they authenticate and endorse data using their corresponding private key. The utilization of publicly identifiable addresses, in conjunction with unalterable on-chain performance records, serves to uphold the accountability of node operators for the entirety of their provided oracle services. In order to ensure transparency and accessibility, a variety of independent websites and APIs provide comprehensive and carefully curated data on the performance of the Chainlink Network, as

well as each decentralized oracle network, node operator, and data provider (Breidenbach et al., 2021). The documentation of all requests made to and responses received from Chainlink nodes is permanently stored on the blockchain, thus enabling the possibility of conducting in-depth analysis of the network's dependability and precision.

The extensive array of resources provides an unparalleled degree of transparency, permitting users, developers, and node operators to acquire detailed insights into the real-time operations of the Chainlink Network. Chainlink's transparency has established it as the industry standard for node operator quality and reliability, guaranteeing that high-value smart contracts, both presently and in the future, are supported by unequivocal evidence of superior oracle performance. The increasing evolution of the Chainlink ecosystem is expected to result in a greater significance of the role of node operators. These operators will play a key role in supporting a widening range of decentralized services and in improving the security and functionality of blockchain networks overall.

Chainlink Price Feeds

Chainlink Price Feeds are decentralized on-chain reference contracts that are continuously updated by DONs consisting of Chainlink nodes. Every reference contract maintains current and past prices of an asset in the format of an exchange rate (such as ETH/USD), which can be accessed by smart contracts on demand. The Chainlink Price Feed is deployed on a designated blockchain network and undergoes regular updates in accordance with predetermined parameters to ensure the accuracy and timeliness of the data it provides.

In order to attain a thorough comprehension of the security and functionality of Chainlink Price Feeds, it is imperative to conduct an analysis of three among its seven distinctive attributes that play a role in fortifying the security of the decentralized finance (DeFi) ecosystem.

Some of Chainlink Price Feeds' Properties

Layers of Decentralization and Data Quality

Chainlink Price Feeds are engineered to maintain a high level of availability and data accuracy. This is achieved through the implementation of a complex multi-layered decentralized aggregation system (observed in *Figure 10* below), which is designed to mitigate the risk of single points of failure and deliver precise asset pricing across the market. The process comprises of multiple pivotal stages, commencing with the aggregation of data sources. The production of raw market data is initially carried out by a varied selection of centralized exchanges, such as Coinbase, Binance, and Kraken, as well as decentralized exchanges like Uniswap, Curve, and PancakeSwap. Reputable data aggregation companies such as CoinMarketCap, CoinGecko, and Tiingo are responsible for gathering and processing financial data, ultimately refining it into comprehensive and organized pricing datasets. Said process of refinement entails the computation of a volume-weighted average price (VWAP), which involves aggregating and weighting data from each exchange based on trading volume. Aggregators consider factors such as market depth, latency, and spread, while also identifying and eliminating anomalies such as flash crashes and wash trading in order to ensure the accuracy and integrity of the data. This approach ensures that every data aggregator is able to furnish a data point encompassing a wide market coverage, thus presenting an accurate representation of all trading environments, as opposed to a limited market segment, thereby increasing precision. The precise data points, which are also produced for various asset categories such as fiat currencies, commodities, and equities, are accessible via application programming interfaces (APIs) and are frequently offered through subscription models. This arrangement motivates data aggregators to uphold elevated levels of precision and operational availability through service-level agreements (SLAs).

The subsequent layer entails the consolidation of data at the level of the node operator. The Price Feed associated with each Chainlink node is connected to several high-quality data aggregator APIs, some of which necessitate the management of credentials. In instances where a revision of pricing is necessary, each individual node retrieves data from the specified aggregators and subsequently provides a response in the form of the median numerical value. This methodology enhances the resilience of individual nodes by utilizing outlier data filtering and minimizing the potential effects of API downtimes. The ultimate layer of decentralization is realized at the level of the oracle network, in which numerous independent Chainlink nodes collectively establish a DON. These DONs consistently

generate collective oracle reports that include the individual observations (medianized price points) and cryptographic signatures of each node. The consolidated report is subsequently preserved on the blockchain within the appropriate smart contract associated with the particular dataset, for instance, the Ethereum-based ETH/USD reference contract. When an oracle report is published on-chain, the authentication of each node's signature is examined, and the medianized value of all responses is securely stored in the reference contract in an immutable manner. In order to maintain resistance against tampering, a minimum of two-thirds of the nodes in a DON are required to provide their observations and signatures in order for a new oracle report to be accepted on the blockchain. This requirement serves to prevent any single node or small group from influencing the final value or disseminating an incomplete report. Furthermore, the final median value is established after the publication of the data. In order to influence the final value stored on-chain, at least fifty percent of the nodes would need to be compromised.

The multi-tiered aggregation strategy employed involves the integration of data sources, node operators, and oracle networks levels, with the intention of ensuring that each update of a Chainlink Price Feed is based on a meticulously curated data point. This approach is designed to yield a comprehensive and reliable representation of an asset's market-wide price. This rigorous implementation of decentralization and data quality significantly improves the reliability and security of the Chainlink Network, thereby facilitating the execution of resilient and high-value smart contracts on diverse blockchain networks. Chainlink Price Feeds are noted for their ability to minimize single points of failure and utilize a consensus-driven method for data aggregation, thereby setting a robust standard for oracle performance in the decentralized finance (DeFi) ecosystem.

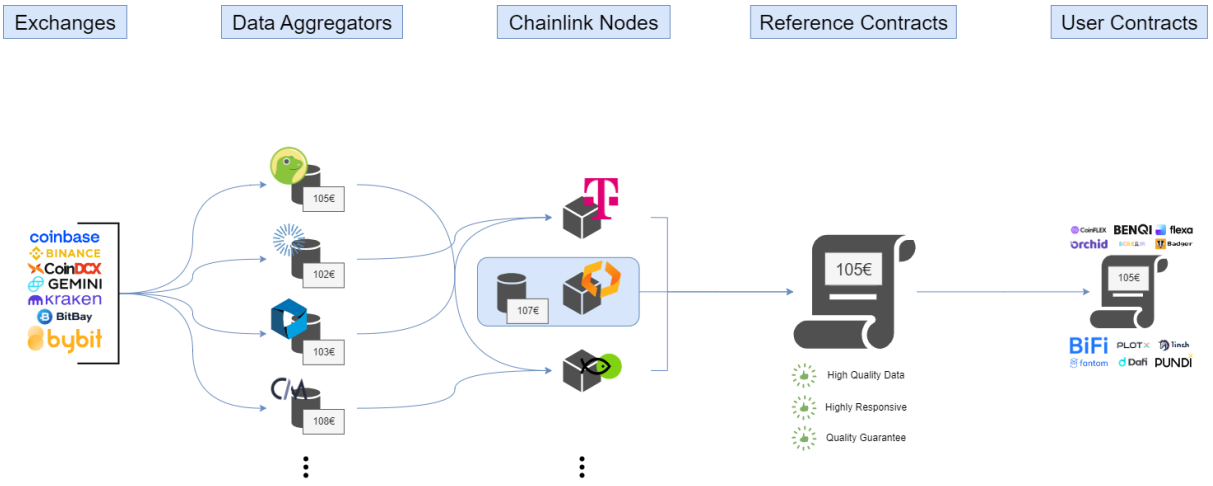

Figure 10. Different layers of decentralized aggregation for Price Feeds.

Data Delivery

Chainlink Price Feeds have been intricately designed to strike a balance between the necessity for precise market data and the incurred expenses of delivering data on-chain. The equilibrium is established through the implementation of a highly customizable system that governs the timing and manner in which oracle reports are produced and made accessible on the blockchain. The function of the system is largely determined by two critical triggering factors: the Deviation Threshold and the Heartbeat.

The Deviation Threshold parameter is used to indicate the percentage change in the price of an asset that is required to initiate a new update from the oracle. For instance, when the threshold is established at 0.05%, a revision will be instigated each time the overall value of an asset experiences a minimum adjustment of 0.05% subsequent to the most recent on-chain update. This parameter is critical for ensuring frequent updates during periods of elevated market volatility, thereby upholding high levels of data accuracy and relevance. On the other hand, in times of decreased volatility, there is a lesser requirement for updates, resulting in a reduction of superfluous on-chain transactions and their associated costs.

The parameter known as Heartbeat is responsible for determining the upper limit for the time interval within which updates are permitted. For example, in the event that the heartbeat interval is established at one minute, a system update will be initiated following the passage of at least one minute since the issuance of the last update, irrespective of any fluctuations in prices. This parameter serves to guarantee the ongoing currency and dependability of the data, particularly in instances where substantial price fluctuations are absent. The implementation of these parameters in the Chainlink Price Feeds allows for the dynamic adjustment of update frequencies in accordance with real-time market conditions. This practice serves to improve accuracy during periods of market volatility and reduce costs during periods of market stability.

The trigger parameters have been calibrated following a thorough assessment of multiple factors such as market demand, the value of the asset being safeguarded, gas costs on the target blockchain, specific requirements of the use case, and the expected market volatility of the asset. High-throughput blockchains have the capability to enable more frequent updates, a result of their ability to process larger volumes of transactions at reduced costs. In the context of higher-cost blockchains, it is imperative to prioritize cost efficiency in order to sustain long-term economic viability and to guarantee the consistent publication of oracle reports, particularly in the face of significant network congestion.

In early 2021, a notable improvement to the data delivery system of Chainlink Price Feeds was implemented through the incorporation of the Off-Chain Reporting (OCR) protocol, depicted in *Figure 11*. The OCR protocol utilizes off-chain computation and peer-to-peer networking to significantly minimize operational expenses, by as much as 90%, and facilitates the transmission of up to ten times more data on-chain as compared to prior methodologies. In the conventional approach, every Chainlink node would communicate its distinct response by initiating a separate on-chain transaction, resulting in the imposition of numerous gas fees. The utilization of the OCR protocol facilitates the capability of nodes to aggregate their responses in an off-chain manner, thereby producing a consolidated oracle report. Subsequently, the compiled report is transmitted onto the blockchain in the form of a unified transaction, with each node's signature undergoing individual verification, and the median value of all collected data being permanently recorded.

This method not only results in a substantial reduction in operational expenses but also improves multiple essential elements of the network. TMoreover, it facilitates greater node decentralization by providing the opportunity for a higher number of nodes to engage in the network without facing exorbitant expenses. Said implementation facilitates higher update frequencies and diminishes latency, thereby ensuring the timely and pertinent maintenance of data. Moreover, the utilization of the OCR protocol enables the implementation of advanced oracle computations tailored to specific requirements, thereby augmenting the adaptability and effectiveness of the Chainlink Network.

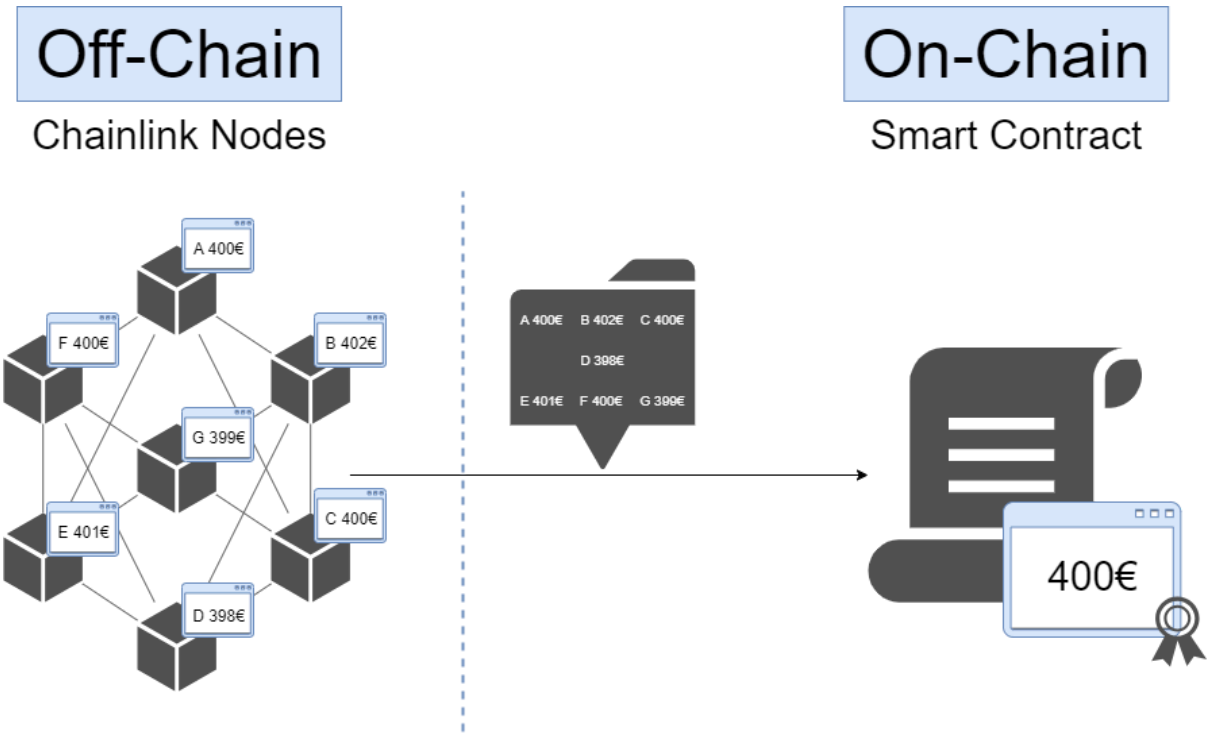

Figure 11. Chainlink's OCR protocol.

Multi-Layered Defense in Depth

Chainlink Price Feeds utilize a complex, multi-layered defense-in-depth strategy aimed at actively mitigating potential issues, such as black swan events, in order to ensure the resilience and dependability of the data supplied to smart contracts. This comprehensive approach encompasses numerous critical facets, commencing with the emphasis on on-chain transparency. Every oracle report produced by Chainlink Price Feeds is permanently recorded as a verifiable public record on the receiving blockchain network. The transparency inherent in this process enables widespread scrutiny on a global scale, providing the opportunity for individuals to assess the historical performance and precision of each update from the time of its commencement. Additionally, each oracle report contains the unique signatures and responses of the nodes involved, which allows for the retrospective examination of historical precision and operational availability for each node operator. The inherent transparency of on-chain data has spurred the creation of a range of public dashboards and visualization tools, including data.chain.link, designed to offer a comprehensive snapshot of the present status of different Chainlink Data Feeds. Said visualization tool encompasses metrics such as the most recent trusted answer, trigger parameters, latest update time, node composition, and contract address. Moreover,

Chainlink Market, along with other supplementary platforms, provides comprehensive analyses of the performance of Chainlink Price Feeds, thereby bolstering the transparency and dependability of the ecosystem.

Active monitoring plays a crucial role as a component of Chainlink Price Feeds' defense strategy. Node operators utilize active monitoring techniques within their infrastructure in order to detect and address issues in a proactive manner. This process includes the use of internal analytics tools to monitor both real-time and historical node performance, as well as the establishment of notification alerts in order to promptly identify potential issues. Several critical aspects are monitored, such as the balance of coins necessary for gas fees, price deviations, unexpected errors, unresponsiveness, and hardware resource consumption. Furthermore, data providers are carefully monitored for accuracy and availability, enabling node operators to transition to alternative providers in order to maintain ongoing data integrity and dependability.

In order to ensure the continuous operation of essential infrastructure, Chainlink node operators employ resilient failover mechanisms. The process commonly necessitates the concurrent operation of numerous instances of Chainlink nodes, encompassing a principal node as well as several supplementary nodes. In the case of a primary node failure or lack of responsiveness, a failover procedure is enacted to facilitate the immediate takeover of responsibilities by a secondary node, thereby reducing any potential downtime. The failover functionalities encompass the blockchain full nodes utilized for both reading and writing data to blockchains, frequently incorporating load balancers to distribute traffic among several self-hosted full nodes or resorting to premium full node RPC providers as backup alternatives. Node operators are responsible for implementing disaster recovery systems, which may include the establishment of regular snapshots and the utilization of cloud migrations. These measures are aimed at facilitating swift recovery from unforeseen catastrophic events, commonly referred to as black swan events, or from instances of data corruption.

In addition to bolstering the dependability of Chainlink Price Feeds, the incorporation of secondary oracle networks (*Figure 12*) and a wide range of clients further contributes to their resilience. Chainlink Price Feeds utilize supplementary redundancies by employing backup oracle networks, which encompass a primary DON and a secondary DON. The networks perform updates to individual reference smart contracts, utilizing a proxy smart contract that directs to either of the two versions. In typical situations, the primary DON operates as the default selection for the feed. In the event of a primary DON experiencing an issue, the proxy

contract may transfer responsibilities to the secondary DON. The secondary DON, which implements node software updates on a deferred timetable, facilitates software client diversity and enhances the overall resilience against unforeseen software anomalies. While the need to switch to a secondary DON has not arisen, the integration of this capability serves to bolster the overall robustness of Chainlink Price Feeds in mitigating the impact of rare and unforeseen disruptive events.

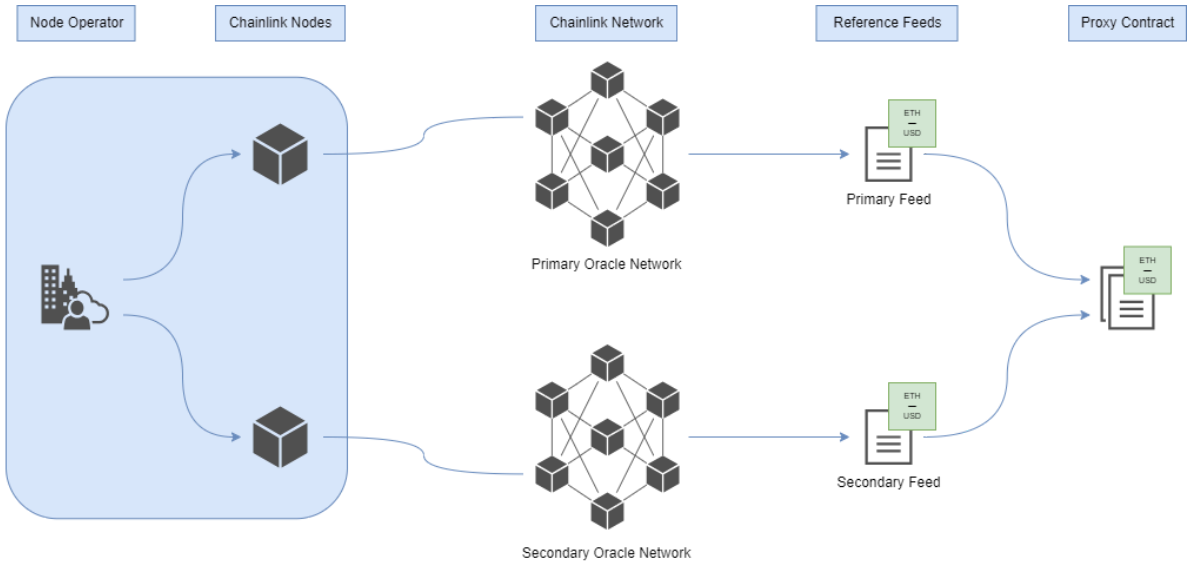

Figure 12. Primary and secondary networks of a Chainlink Price Feed.

Implications for DeFi

The robust growth of the Decentralized Finance (DeFi) ecosystem is closely linked to the progress and dependability of blockchain oracles, particularly those offered by Chainlink. The scalability and security of DeFi applications are inherently dependent on the strength and reliability of the oracles that they utilize. Oracles are integral to the maintenance of reliability and coherence of off-chain data when incorporated into on-chain processes. The inherent nature of this association serves as a cornerstone for numerous functions within the DeFi ecosystem, including the provision of pricing data for decentralized exchanges and the determination of collateralization ratios for lending platforms. Therefore, it is of great significance in promoting trust and enabling development within the ecosystem.

The integration of Chainlink into the DeFi ecosystem holds significant implications for augmenting the accuracy of data and bolstering security within this framework. Chainlink has created DONs designed to collect data from various high-quality data providers, guaranteeing the precision and dependability of the data delivered to smart contracts within DeFi applications (Breidenbach et al., 2021). The objective of this approach is to decrease the probability of isolated components causing system-wide malfunction, while simultaneously decreasing the potential for unauthorized data tampering. This is particularly critical for ensuring the integrity of financial contracts involving substantial monetary sums. Chainlink enhances the reliability and resilience of DeFi applications by aggregating data from multiple sources, thereby mitigating the susceptibility of these applications to market anomalies such as sudden price drops and fluctuations in trading volume.

Moreover, the implementation of decentralized oracles within the realm of decentralized finance (DeFi) brings about a novel level of trust and transparency. The reputation systems and cryptographic proofs employed by Chainlink facilitate the verification of the performance and reliability of individual oracle nodes by users and developers. Transparency plays a critical role in a decentralized setting, as it enables all parties involved to conduct autonomous audits and place reliance on the data inputs without dependence on a centralized authority. The capacity to evaluate the historical performance of nodes and their compliance with predetermined Service Level Agreements (SLAs) contributes to the cultivation of an environment characterized by accountability, which is a pivotal factor for the enduring development of DeFi.

The architecture of Chainlink enables the development of novel financial products that utilize real-world data in unprecedented ways. One illustrative instance involves the use of

parametric insurance products which have the ability to autonomously initiate payouts in response to weather data, and dynamic non-fungible tokens (NFTs) which are capable of adapting in accordance with external occurrences, such as fluctuations in social media engagement. The utilization of these applications expands the functionality of DeFi beyond conventional financial instruments, facilitating the development of novel asset categories and tools for risk mitigation that are dynamically tailored to real-time data.

Furthermore, Chainlink's architecture facilitates the smooth incorporation of diverse data sources, a vital requirement for ensuring the scalability of DeFi applications. By utilizing External Adapters, Chainlink nodes have the ability to establish connections to a wide range of application programming interfaces (APIs), enabling DeFi projects to seamlessly access a diverse array of data categories, encompassing financial market information as well as Internet of Things (IoT) sensor outputs. The adaptability of this feature allows developers to create bespoke and reactive smart contracts capable of interfacing with a wide range of data inputs and outputs, consequently expanding the range and capabilities of decentralized finance applications.

The economic incentives offered by Chainlink's staking mechanisms play a crucial role in bolstering the DeFi ecosystem. As previously discussed, Chainlink implements a mechanism in which nodes are obligated to stake tokens as a form of collateral, thereby incentivizing node operators to uphold honest behavior in their actions. The staking model, when integrated with the possibility of implementing slashing measures to address instances of malicious behavior, serves to ensure the alignment of node operators' incentives with the broader objectives of enhancing the robustness and dependability of the network. The presence of a financial disincentive serves as a crucial mechanism for upholding the security and integrity of DeFi platforms.

The impact of Chainlink on DeFi extends to the enhancement of reliability and efficiency in decentralized exchanges (DEXs). The precision and punctuality of price feeds from Chainlink oracles play a crucial role in facilitating the execution of trades informed by current market conditions. This serves to establish equitable trading environments and mitigate concerns related to unethical trading practices such as front-running and price manipulation often observed in less robust systems. Chainlink facilitates the development of advanced trading strategies and financial instruments within DEXs by offering high-quality data feeds, thereby enhancing the resilience and dynamism of the DeFi market.

Furthermore, the oracles provided by Chainlink serve as a critical component in facilitating automated risk management within the DeFi ecosystem, while also enhancing data reliability. One example of this application is seen in lending platforms which utilize Chainlink's price feeds in order to calculate collateralization ratios and initiate liquidation events when deemed necessary. The implementation of this automation results in a decrease in the requirement for manual intervention, thereby guaranteeing that the platforms can function effectively and securely on a large scale. The implementation of automatic enforcement of financial contracts through real-time data inputs greatly improves the operational efficiency and reliability of DeFi protocols.

An additional crucial implication is the facilitation of cross-chain interoperability. As mentioned before, Chainlink's decentralized oracle networks have been specifically crafted to be blockchain-agnostic, allowing for effortless integration across various blockchain platforms. The establishment of interoperability plays a critical role in fostering the growth and integration of a unified DeFi ecosystem, facilitating the seamless transfer of assets and information between diverse networks. The integration of diverse blockchains by Chainlink serves to augment market liquidity, facilitate more intricate financial transactions, and foster the development of a cohesive DeFi market.

Chainlink's dedication to transparency and open-source development cultivates a collaborative atmosphere that promotes rapid innovation in the realm of decentralized finance (DeFi). Moreover, Chainlink promotes the advancement of new applications and solutions that utilize their oracle technology by granting access to their protocols and tools to the wider community. The transparent approach not only fosters technological progression, but also guarantees that the environment remains diverse and open to a broad spectrum of developers and users.

The security implications of Chainlink's design hold particular significance. As elucidated earlier, Chainlink's implementation of decentralized data aggregation serves to alleviate the vulnerabilities typically associated with centralized systems, particularly the risks stemming from single points of failure. The decentralized approach serves to not only disperse the risk, but also to elevate the financial burden of an attack, rendering it economically impractical for adversaries to breach the network. In addition, the utilization of cryptographic methodologies, such as zero-knowledge proofs (ZKPs) and privacy-preserving credential issuance, enhances security measures by safeguarding sensitive data from unauthorized access while still allowing for verification.

The framework developed by Chainlink provides support for enhancing the scalability of decentralized finance (DeFi) applications. The capacity to tailor the degree of decentralization and the selection of data sources enables DeFi developers to effectively align cost considerations with security requirements in accordance with their individual operational requirements. The imperative nature of flexibility is paramount in order to accommodate the diverse needs of various DeFi applications, ranging from high-frequency trading platforms to intricate derivatives contracts. Chainlink provides precision control over these parameters, allowing for efficient scalability of DeFi applications while maintaining stringent security and reliability standards.

The incorporation of Chainlink into the decentralized finance (DeFi) ecosystem holds significant implications for the advancement of financial innovation. Chainlink enables the creation of advanced financial products by offering a resilient and adaptable framework for linking smart contracts with real-world data. These products have the capability to automate intricate processes, lower operational expenses, and offer enhanced visibility and effectiveness when compared to conventional financial systems. As the decentralized finance DeFi ecosystem undergoes continued development, the essential role of Chainlink as a foundational technology is poised to play a pivotal role in shaping the forthcoming wave of financial innovation.

Security Concerns

In order to guarantee the resilience and protection of DONs, such as those supported by Chainlink (Breidenbach et al., 2021), it is imperative to address three key concerns: Byzantine Faults, Sybil resistance, and Denial of Service (DoS) resistance. The prominence of these concerns is vital in ensuring the preservation of the integrity, accessibility, and reliability of the data supplied by oracles to smart contracts on blockchain networks.

Byzantine Faults

As outlined in the Data Delivery section, Chainlink's Off-Chain Reporting (OCR) security model is intentionally crafted to ensure resilient fault tolerance and operational integrity even in the face of adversarial circumstances. This framework can handle up to 33% of the oracles within a network demonstrating Byzantine faults, in which these oracles may exhibit unpredictable behavior or appear compromised. This capability allows for the maintenance of the protocol's overall integrity, contingent on the correct functioning of the remaining oracles. The fundamental premise for achieving optimal system operation is based on the utilization of a configuration consisting of $n = 3f + 1$ oracles, where f represents the maximum number of faulty nodes. This configuration allows for the attainment of maximal resilience against various faults, including network failures or crashes.

The OCR protocol upholds a high level of reliability and accuracy through the requirement of a minimum quorum of two-thirds of nodes for data consensus, thus safeguarding the network's integrity in the event that as many as one-third of the nodes exhibit Byzantine behavior. The precise equilibrium between the size of the quorum and the thresholds for fault tolerance is of paramount importance in guaranteeing the security and functionality of Chainlink's DONs in the face of adversarial circumstances. Moreover, the model encompasses provisions for benign faults, wherein nodes that experience temporary unresponsiveness or inaccessibility can regain functionality and recommence their proper protocol involvement. This ensures that the safety of the protocol is not compromised.

The implementation of the OCR protocol signifies a substantial progress in enhancing the decentralization and scalability of Chainlink networks. The communication among nodes is facilitated by a peer-to-peer (P2P) network, which utilizes a lightweight consensus algorithm. This algorithm allows each node to report its data observation and sign it for authentication. The process of aggregating transactions and subsequently transmitting them results in a considerable reduction in gas consumption. The report pertaining to this composite transaction is then officially endorsed by a quorum of oracles and encompasses the comprehensive observations provided by each oracle. The report is subsequently authenticated on the blockchain, thereby upholding the decentralized and trustless characteristics of Chainlink's oracle networks by validating the signatures within the quorum (Breidenbach et al., 2021).

Meaning that the Off-Chain Reporting (OCR) protocol involves the aggregation of node observations into a consolidated report using a secure peer-to-peer (P2P) network, which occurs off-chain. The present aggregated report is submitted to the blockchain through a singular node, aiming to optimize network resources by diminishing the quantity of transactions. The report is created through the aggregation of observations from multiple nodes and is subsequently authenticated by a quorum. These authenticated reports are then verified on-chain. This approach yields a number of significant advantages, including the reduction of network congestion, lowered gas costs for individual node operators, improved scalability of node networks to accommodate a larger number of nodes, and the ability to update data feeds more quickly with each round requiring only one transaction confirmation for the price to be recorded on-chain.

The execution of the protocol primarily takes place off-chain through a peer-to-peer (P2P) network involving Chainlink nodes. The nodes within the network engage in a periodic process of leader node election, in which the leader node assumes the responsibility of coordinating the protocol. This includes soliciting signed observations from follower nodes, combining these observations into a comprehensive report, and subsequently disseminating the report to the followers for their authentication. Upon securing approval from a quorum of followers through the submission of signed copies to the leader, the leader subsequently consolidates a final report bearing the quorum's endorsements and circulates it amongst all followers.

The nodes make an effort to transmit the ultimate report to the aggregator contract in accordance with a randomized timetable. The aggregator contract serves to validate the endorsements of a majority of nodes in the network on a given report, and subsequently

provides consumers with the median value, along with pertinent details such as the block timestamp and round ID. This protocol facilitates comprehensive monitoring of the blockchain by all nodes to ensure the integrity and reliability of the final report, thereby mitigating the risk of any potential single point of failure during data transmission. In the event that the specified node does not confirm its transmission within a prescribed timeframe, a round-robin protocol is initiated, enabling alternative nodes to transmit the final report until a confirmation is received.

Furthermore, the Off-Chain Reporting (OCR) protocol is inherently designed as a Byzantine Fault Tolerant (BFT) mechanism intended for use in a network that operates under partially synchronous conditions. This system guarantees liveness and correctness, even in the presence of f faulty nodes where f is less than $n/3$, ensuring the properties of Byzantine reliable broadcast. In contrast to a complete Byzantine Fault Tolerance (BFT) consensus protocol, the Off-Chain Reporting (OCR) protocol does not uphold message logs that exhibit consistency across all nodes' perspectives, and the protocol's leader has the ability to equivocate without breaching safety guarantees. The present design of Off-Chain Reporting (OCR) prioritizes the aggregation of values reported by participating nodes through a process of medianization. This design ensures that the median value in a reported document remains within the range of values reported by at least two honest nodes, thus upholding crucial safety conditions.

The functionality of OCR goes beyond traditional BFT protocols as it includes the implementation of all-or-nothing off-chain report broadcasting, ensuring reliable transmission at predefined intervals, and minimizing trust through contract-based mechanisms. The aforementioned properties play a critical role in guaranteeing equity, continuation of operations, and accuracy in the context of malfunctioning or malign nodes. Said protocol demonstrates heightened resilience through its capacity to effectively manage benign faults, whereby temporarily unresponsive nodes are capable of re-engaging in the correct protocol participation without compromising safety.

In its entirety, the OCR design places emphasis on resilience to a variety of failure types, implementation simplicity to mitigate defects, reduced transaction fees through the optimization of off-chain computations, and minimal latency to facilitate timely data updates for DeFi platforms. The system is comprised of a set of n oracles which engage in communication across an authenticated and encrypted network, thereby guaranteeing the integrity and security of messages exchanged. The protocol is designed to accommodate

adaptive fault occurrence, permitting the adversary to dynamically select faulty nodes while still ensuring the functionality of the protocol, provided that the condition $n = 3f + 1$ is met.

Furthermore, the protocol also considers potential vulnerabilities such as network partitions and guarantees that the correct nodes will eventually communicate once any network asynchrony has been resolved. The employment of cryptographic primitives such as EdDSA and ECDSA for digital signatures, as well as PRFs implemented through HMAC-SHA256 or Keccak256, serves to provide robust security measures against both external and internal threats.

Sybil Resistance

The implementation of Sybil resistance is integral in safeguarding the network from potential subversion by adversaries who could potentially exploit the system by generating a large number of pseudonymous identities in order to attain an undue level of influence. The approach employed by Chainlink to mitigate Sybil attacks involves the implementation of a variety of advanced techniques (Breidenbach et al., 2021). Initially, the utilization of staking mechanisms serves to ensure that oracle nodes are provided with economic incentives to act in an honest manner. In order to participate in the network, nodes are required to secure a substantial quantity of tokens as a form of collateral, the violation of which may result in a reduction of said collateral in instances of malicious conduct. The implementation of this strategy results in the imposition of a significant financial deterrent towards Sybil attacks, as the potential for economic repercussions renders such exploits economically unfeasible. Furthermore, the incorporation of reputation systems, where nodes accrue reputational scores derived from their past performance, serves to deter dishonest behavior. This is because nodes with higher reputations can demand higher fees and engender a greater degree of trust. This practice serves as an incentive for regular and sincere engagement, as there is a economic advantage in maintaining a strong reputation.

Additionally, the implementation of advanced cryptographic methodologies such as privacy-preserving credential issuance utilizing DECO and Town Crier facilitates the conversion of distinct real-world identifiers (e.g., Social Security Numbers) into on-chain

identifiers while safeguarding sensitive data from individual nodes. This guarantees that each individual's identity is distinctive and authentic, while also upholding confidentiality. Moreover, the utilization of Zero-Knowledge Proofs (ZKPs) is of significant importance in enabling nodes to demonstrate the legitimacy of their identity and the integrity of their data contributions without disclosing the underlying sensitive information. The utilization of said cryptographic primitives allows Chainlink to effectively prevent nodes from illicitly creating multiple identities in order to subvert the network.

Moreover, it is important to note that a DON has the capability to conduct a privacy-preserving conversion of distinct real-world identifiers into on-chain identifiers during the user registration process, as exemplified in platforms such as CanDID. The aforementioned transformation enables the system to identify duplicate registrations while preserving the confidentiality of sensitive information, thereby enhancing its resistance against Sybil attacks. These credentials can also be utilized to maintain orderly and equitable transaction processing, thereby ensuring the integrity of causality within the system. This approach is designed to uphold the temporal sequencing of transactions from their creation to their initial submission to the network. Nevertheless, conventional order-fairness fails to impede an adversary from inundating the system with transactions in order to leverage an advantage, as observed in token sales or the deliberate creation of network congestion to execute the liquidation of collateralized debt positions.

Furthermore, the Chainlink protocol incorporates economic incentives as a means of incentivizing node operators to engage in honest behavior. Instead of implementing slashing, the reputation of each individual node serves as a decisive factor in the selection of job assignments. When a node disseminates erroneous information contrary to the consensus, it may suffer reputational damage, subsequently diminishing its prospects for future employment. The implementation of staking LINK by each node during requests functions as a form of reimbursement in the event that a node is unable to furnish precise data or timely responses. The confluence of risk to reputation, financial penalties, and potential loss of future earnings serves as a motivational factor for nodes to engage in honest behavior. Moreover, the utilization of a greater number of nodes to meet requests decreases the probability of a deceitful majority, thereby strengthening the system's resilience against Sybil attacks. Additionally, reputation providers that conduct off-chain validation of nodes enhance the network's resilience by diminishing the impact of potential control exerted by a single entity over multiple nodes. This approach fortifies the network's resistance and limits the ability of any single entity to significantly influence it.

Chainlink utilizes a comprehensive strategy that incorporates staking mechanisms, reputation systems, privacy-preserving cryptographic techniques, and Sybil-resistant credentials to effectively reduce the risk of Sybil attacks (Breidenbach et al., 2021). This strategy ensures the integrity and reliability of its decentralized oracle networks. The implementation of these advanced techniques serves to enhance the resilience of the network to the establishment of numerous identities, thus safeguarding the authenticity and reliability of the information supplied to smart contracts. Chainlink's decentralized oracle networks demonstrate resilience against Sybil attacks through implementation of rigorous economic, cryptographic, and operational standards. This safeguarding of the ecosystem's overall security and stability is critical in ensuring the reliability and integrity of the network.

Furthermore, the Chainlink ecosystem acknowledges the possibility of nodes engaging in off-chain communication and collusion. In response to this challenge, reliable hardware-based mechanisms such as Intel SGX are considered as a means to thwart unauthorized interference by nodes in the processing of requests. The utilization of trusted hardware guarantees that in the event nodes engage in off-chain communication, they are unable to manipulate the data processing occurring within the secure enclave, thereby preserving the integrity of the data. Moreover, in the event that nodes were discovered to engage in malicious activities, reputation providers could make manual adjustments to their reputation after the fact, thereby increasing the deterrent against dishonest behavior.

DoS Resistance

Ensuring the resistance of Denial of Service (DoS) attacks is a crucial consideration in maintaining the availability and functionality of DONs such as Chainlink, particularly in the face of adversarial conditions (Breidenbach et al., 2021). The implementation of resilient contingency measures is crucial in this regard; such measures enable smart contracts to transition smoothly to secondary data sources or oracles in the event of primary system failure or compromise. The implementation of redundancy serves to guarantee uninterrupted data accessibility and serves as a preventive measure against the potential for a solitary point of failure. The decentralized management of oracle nodes involves the distribution of responsibilities and data feed tasks across numerous geographically dispersed nodes, thus

contributing to an elevated level of resilience. The dissemination of authority among multiple nodes guarantees the sustained operation of the network in the event of some nodes being incapacitated by a Denial of Service (DoS) attack, allowing for uninterrupted functionality at the network level.

Furthermore, the implementation of error handling and retry logic within smart contracts represents a crucial strategic approach. This process entails encapsulating oracle function calls within constructs capable of detecting errors and re-initiating data requests, thereby ensuring continued operability in the event of temporary failure of some oracle nodes. Additionally, the implementation of sophisticated monitoring systems and real-time analytical tools can effectively identify initial indicators of Denial of Service (DoS) attacks, allowing for proactive measures to be taken in response. Strategies such as implementing rate limiting, which restricts the number of requests from individual nodes, and utilizing CAPTCHA systems are effective measures to mitigate potential abuse. The integration of these tactics alongside economic disincentives for nefarious conduct, such as staking and slashing, serves to impose financial penalties on nodes engaging in Denial of Service (DoS) attacks. This effectively aligns their incentives with the overall well-being and resilience of the network.

In order to maintain the uninterrupted functionality of critical infrastructure, Chainlink node operators utilize robust failover mechanisms. The process typically requires the simultaneous operation of multiple instances of Chainlink nodes (as explained in the Multi-Layered Defense in Depth subsection), including a primary node and several secondary nodes. In the event of a primary node failure or unresponsiveness, a failover procedure is initiated to enable the prompt assumption of responsibilities by a secondary node, thus minimizing any potential downtime.

Moreover, commit-reveal protocols offer an additional defense mechanism against Denial of Service (DoS) attacks. This approach involves the dissemination of a cryptographic commitment to a transaction, rather than the transmission of the transaction itself in unencrypted form. Upon completion of all undisclosed transactions, the sender is required to unveil and disclose the transaction data within a specified time frame. Subsequently, the network proceeds to verify the conformance of the initial transaction with the preceding agreement. On the one hand, this approach has the potential to establish fairness in ordering and mitigate specific forms of attacks. On the other hand, it is associated with limitations such as the requirement for increased client interactions and the potential for a lack of initial access, which could itself become a vector for denial-of-service attacks.

Moreover, ensuring the validation of the initial stage in a coherent and widespread approach presents considerable complexities.

Threshold encryption is utilized as another method to improve the resistance against Denial of Service (DoS) attacks. This approach incorporates the use of threshold cryptographic operations in which a DON holds an encryption public key, while the corresponding private key is distributed among multiple oracles. Customers utilize encryption to secure their transactions using public key technology, and subsequently transmit the encrypted data to the DON. Upon receipt, the DON processes the transactions by decrypting them and then inserting them into the blockchain. This methodology guarantees that the ordering of transactions is not influenced by the content of the transactions, thus mitigating potential Denial of Service (DoS) attacks that exploit the visibility of transaction data. Upon decryption, transactions are capable of immediate validation, allowing for autonomous processing by the DON without the need for subsequent client intervention. However, securely managing the threshold key, particularly in the presence of dynamic node configurations, presents supplementary challenges.

Furthermore, within the framework of operational dynamics, it is imperative to consider the methods for ensuring node accountability and imposing penalties. The contract does not have the capability to detect a node failure on its own. Instead, it generates a log from the coordinator contract, which is then monitored by the nodes for any incoming requests. The Request Expiration Time is a specified parameter that determines the duration within which an oracle node must provide a response following the submission of a run request. If the node fails to provide a response within this specified time frame, it will result in the imposition of a penalty. The imposition of this penalty does not invariably entail the forfeiture of the entire deposit, but rather encompasses a negative impact on one's reputation and potentially a deduction from the penalty deposit. This system provides mechanisms to maintain accountability of nodes and discourages extended periods of downtime.

Finally, it is important to note that node operators do not experience significant disincentives as a result of potential Denial of Service (DoS) attacks. The transmission of communication to Chainlink nodes is initiated from verified and secure sources, including blockchain nodes, listing services, and external adapters (Breidenbach et al., 2021). The managed communication environment facilitates the process of protecting nodes from DoS or Distributed Denial of Service (DDoS) attacks. By implementing a policy of blocking all other inbound traffic, nodes can effectively protect themselves from these types of attacks. A wide

range of resources and proven methods for enhancing the security of servers against these types of attacks are easily accessible and can be utilized to protect Chainlink nodes.

Use Case Implementation

The interaction with the `OracleTrader` contract involves a series of transactions and function calls that are intentionally constructed to facilitate decentralized finance (DeFi) trading. This includes the utilization of real-time price data provided by Chainlink Price Feeds. The described process guarantees a smooth experience for users as they are able to effectively deposit funds, make trades, and oversee their limit orders within the decentralized Ethereum blockchain ecosystem. This section provides a comprehensive overview of the interaction process.

The commencement of the interaction generally involves the user depositing Sepolia ETH into the contract. The user initiates the `depositSepolia` function, which is designated as payable, signifying its capacity to receive Ether. The execution of this function necessitates that the user includes a positive quantity of Sepolia with the transaction, resulting in the subsequent crediting of this amount to their account balance within the contract. The function call is of the following form:

```
    /**
    * @notice Allows users to deposit Sepolia into the contract.
      * @dev Credits the msg.value (amount of Sepolia sent with the transaction) to the sender's balance.
    */
    function depositSepolia() public payable {
          require(msg.value > 0, "Deposit amount must be greater than zero.");
        sepoliaBalances[msg.sender] += msg.value;
    }
```

Upon the completion of a deposit, the balance of the user's Sepolia account within the contract is revised, allowing them to allocate these funds to engage in trading activities.

The following is a comprehensive list of the price feed pairs offered by Chainlink's oracles utilizing Sepolia that are present in this contract:

```
    constructor() {

                        // Initialize oracles with pairs from
https://docs.chain.link/data-feeds/price-feeds/addresses?network=ethere
um&page=1#sepolia-testnet

                                                oracles["AUD/USD"]      =
OracleDetails(AggregatorV3Interface(0xB0C712f98daE15264c8E26132BCC91C40
aD4d5F9), 8);

                                                oracles["BTC/ETH"]      =
OracleDetails(AggregatorV3Interface(0x5fb1616F78dA7aFC9FF79e0371741a747
D2a7F22), 18);

                                                oracles["BTC/USD"]      =
OracleDetails(AggregatorV3Interface(0x1b44F3514812d835EB1BDB0acB33d3fA3
351Ee43), 8);

                                               oracles["CSPX/USD"]      =
OracleDetails(AggregatorV3Interface(0x4b531A318B0e44B549F3b2f824721b3D0
d51930A), 8);

                                                oracles["CZK/USD"]      =
OracleDetails(AggregatorV3Interface(0xC32f0A9D70A34B9E7377C10FDAd885125
96f61EA), 8);

                                                oracles["DAI/USD"]      =
OracleDetails(AggregatorV3Interface(0x14866185B1962B63C3Ea9E03Bc1da838b
ab34C19), 8);

                                                oracles["ETH/USD"]      =
OracleDetails(AggregatorV3Interface(0x694AA1769357215DE4FAC081bf1f309aD
C325306), 8);

                                                oracles["EUR/USD"]      =
OracleDetails(AggregatorV3Interface(0x1a81afB8146aeFfCFc5E50e8479e826E7
D55b910), 8);

                                              oracles["FORTH/USD"]      =
OracleDetails(AggregatorV3Interface(0x070bF128E88A4520b3EfA65AB1e4Eb6F0
F9E6632), 8);
```

```
                                                    oracles["GBP/USD"]      =
OracleDetails(AggregatorV3Interface(0x91FAB41F5f3bE955963a986366edAcff1
aaeaa83), 8);

                                                    oracles["GHO/USD"]      =
OracleDetails(AggregatorV3Interface(0x635A86F9fdD16Ff09A0701C305D3a845F
1758b8E), 8);

                                                   oracles["IB01/USD"]      =
OracleDetails(AggregatorV3Interface(0xB677bfBc9B09a3469695f40477d05bc9B
cB15F50), 8);

                                                   oracles["IBTA/USD"]      =
OracleDetails(AggregatorV3Interface(0x5c13b249846540F81c093Bc342b5d963a
7518145), 8);

                                                    oracles["JPY/USD"]      =
OracleDetails(AggregatorV3Interface(0x8A6af2B75F23831ADc973ce6288e5329F
63D86c6), 8);

                                                   oracles["LINK/ETH"]      =
OracleDetails(AggregatorV3Interface(0x42585eD362B3f1BCa95c640FdFf35Ef89
9212734), 18);

                                                   oracles["LINK/USD"]      =
OracleDetails(AggregatorV3Interface(0xc59E3633BAAC79493d908e63626716e20
4A45EdF), 8);

                                                    oracles["SNX/USD"]      =
OracleDetails(AggregatorV3Interface(0xc0F82A46033b8BdBA4Bb0B0e28Bc2006F
64355bC), 8);

                                                   oracles["USDC/USD"]      =
OracleDetails(AggregatorV3Interface(0xA2F78ab2355fe2f984D808B5CeE7FD0A9
3D5270E), 8);

                                                    oracles["XAU/USD"]      =
OracleDetails(AggregatorV3Interface(0xC5981F461d74c46eB4b0CF3f4Ec79f025
573B0Ea), 8);

    }
```

Subsequently, the user has the option to acquire a set of assets by utilizing the deposited Sepolia. This objective is achieved through invocation of the `buy` function, in which the user specifies the desired asset pair for acquisition. The `buy` function, which is also made payable, necessitates that the user includes Sepolia with the transaction. The aforementioned function retrieves the most recent price of the asset pair from the Chainlink oracle by utilizing the `getLatestPrice` function, which interfaces with the `AggregatorV3Interface` to access up-to-date price information. The obtained price is subsequently modified to account for the buy spread through the utilization of the `adjustPriceForSpread` function, thereby ensuring that the price accurately reflects the associated trading fee. The calculation of the asset amount involves dividing the Sepolia by the adjusted price, resulting in the crediting of this calculated amount to the user's holdings within the specified asset pair.

```
    /**
     * @notice Allows users to buy assets at the current price adjusted for the buying spread.
      * @param assetPair The symbol of the asset pair to buy (e.g., "ETH/USD").
     * @dev The function uses the payable modifier to accept Sepolia directly with the transaction.
     *       It calculates the asset amount based on the current price from the oracle, adjusted for the buy spread.
     *       The purchased asset amount is then credited to the user's holding.
    */
    function buy(string memory assetPair) public payable {
        require(msg.value > 0, "No Sepolia sent");
        int rawPrice = getLatestPrice(assetPair);
        require(rawPrice > 0, "Invalid price data");

        uint256 price = adjustPriceForSpread(uint256(rawPrice), true);
```

```
        uint256 assetAmount = (msg.value * 1e18) / price;

        assetHoldings[msg.sender][assetPair] += assetAmount;



                emit  AssetPurchased(msg.sender,  assetPair,  msg.value,
assetAmount);

    }
```

On the contrary, should the user decide to divest themselves of a previously acquired asset, they would engage the `sell` function, in which they would specify the asset pair and the quantity of the asset they intend to sell. The `sell` function is designed to verify whether the user possesses an adequate balance of the asset in question. Subsequently, the system retrieves the prevailing market price from the oracle, accounts for the sell spread, and performs a computation to determine the Sepolia equivalent of the quantity of the asset being sold. The Sepolia amount is deposited into the user's balance within the contractual framework, while the equivalent amount is subtracted from their assets.

```
    /**

     * @notice Allows users to sell a specified amount of an asset at
the current price adjusted for the selling spread.

    * @dev Allows a user to sell an asset. The sell amount is converted
into Sepolia based on the current asset price

    * and includes a predefined spread to simulate trading fees.

    * @param assetPair The asset pair to sell (e.g., "ETH/USD").

    * @param assetAmount The amount of the asset to sell.

    */

     function sell(string memory assetPair, uint256 assetAmount) public
{

           require(assetAmount > 0, "Sell amount must be greater than
zero.");
```

```
            require(assetHoldings[msg.sender][assetPair] >= assetAmount,
"Insufficient asset balance.");



        int rawPrice = getLatestPrice(assetPair);

        require(rawPrice > 0, "Invalid price data.");



        uint256 price = adjustPriceForSpread(uint256(rawPrice), false);

        uint256 sepoliaAmount = (assetAmount * price) / 1e18;

        assetHoldings[msg.sender][assetPair] -= assetAmount;

        sepoliaBalances[msg.sender] += sepoliaAmount;



                emit AssetSold(msg.sender, assetPair, assetAmount,
sepoliaAmount);

    }
```

Furthermore, in addition to executing immediate trades, individuals have the capability to input limit orders, where they can stipulate the conditions at which they intend to purchase or sell assets at specified prices. The `placeLimitOrder` function serves the purpose of allowing the user to specify the asset pair, the quantity of the asset, the desired execution price, and the nature of the order (i.e, buy or sell). The specifics of each order are retained within the `limitOrders` mapping, wherein a distinct ID is allocated to individual orders. This feature empowers individuals to establish trading parameters that are automatically triggered upon the fulfillment of pre-defined market price conditions.

```
    /**

     * @notice Allows users to place limit orders for buying or selling
assets at a specified price.

      * @param assetPair The symbol of the asset pair for the order
(e.g., "ETH/USD").
```

```
    * @param amount The amount of the asset to buy or sell.

    * @param price The price at which the order should be executed.

      * @param isBuyOrder Specifies whether the order is a buy order
(true) or a sell order (false).

    * @dev The function records the order details in the "limitOrders"
mapping and emits an event.

    *      Each order is assigned a unique ID.

    */

     function placeLimitOrder(string memory assetPair, uint256 amount,
uint256 price, bool isBuyOrder) public {

        limitOrders[nextOrderId] = LimitOrder(msg.sender, true, amount,
price, isBuyOrder);

            emit LimitOrderPlaced(msg.sender, nextOrderId, assetPair,
isBuyOrder, amount, price);

        nextOrderId++;

    }
```

In the event of modifications in market conditions or at the discretion of the user, the cancellation of a pending limit order can be executed through the utilization of the `cancelLimitOrder` function. This particular function necessitates the utilization of the distinct ID of the order and validates the active status of the order, as well as the verification that it was placed by the party calling the function. Subsequently, the order is designated as inactive, thereby impeding its fulfillment.

```
    /**

    * @notice Allows users to cancel their active limit orders.

    * @param orderId The unique ID of the order to cancel.

     * @dev Checks that the order exists and is active, and that the
user is the order creator,
```

```
     *         before marking the order as inactive and emitting a
cancellation event.

    */

    function cancelLimitOrder(uint256 orderId) public {

          require(limitOrders[orderId].isActive, "Order not active or
does not exist");

          require(limitOrders[orderId].trader == msg.sender, "Not the
order creator");



        limitOrders[orderId].isActive = false;

        emit LimitOrderCancelled(msg.sender, orderId);

    }
```

In order to automate the execution of limit orders, the contract incorporates the `checkAndExecuteLimitOrders` function which systematically processes all active limit orders to determine whether the prevailing market price meets the specified order criteria. When the specified conditions are satisfied, the `executeLimitOrder` function is invoked to facilitate the execution of the order. This involves the transfer of assets and the subsequent update of balances in accordance with the transaction.

```
    /**

     * @dev Checks limit orders against the latest market price and
executes them if conditions are met.

    * This function is called after any market action that could affect
prices (e.g., a buy or sell operation).

    * @param assetPair The asset pair for which to check limit orders.

    */

        function checkAndExecuteLimitOrders(string memory assetPair)
private {
```

```
        int marketPrice = getLatestPrice(assetPair);
        uint256 currentPrice = uint256(marketPrice);

          // Iterate over all limit orders to find matching orders for execution
        for (uint256 i = 1; i <= nextOrderId; i++) {
            LimitOrder storage order = limitOrders[i];

            // Skip inactive orders
            if (!order.isActive) continue;

             // Check if the order can be executed based on the current market price and order type
                bool canExecute = (order.isBuyOrder && currentPrice <= order.price) || (!order.isBuyOrder && currentPrice >= order.price);

            if (canExecute) {
                executeLimitOrder(i, assetPair, currentPrice);
            }
        }
    }

    /**
     * @dev Executes a limit order. This involves transferring the asset between the contract and the trader's balance,
    * and marking the order as inactive.
```

```
    * @param orderId The ID of the order to execute.
    * @param assetPair The asset pair being traded.
    * @param price The execution price.
    */
        function executeLimitOrder(uint256 orderId, string memory
assetPair, uint256 price) private {
        LimitOrder storage order = limitOrders[orderId];

        // Ensure the order is still active
        if (!order.isActive) return;

         // Calculate the asset amount to be transferred based on the
order type and execution price
        uint256 assetAmount = order.amount;
        if (order.isBuyOrder) {
            // For buy orders, calculate the amount of asset that can
be bought with the order's amount of Sepolia
            uint256 sepoliaSpent = assetAmount * price / 1e18;
                require(sepoliaBalances[order.trader] >= sepoliaSpent,
"Insufficient Sepolia balance for buy order");
            sepoliaBalances[order.trader] -= sepoliaSpent;
            assetHoldings[order.trader][assetPair] += assetAmount;
        } else {
            // For sell orders, transfer the asset from the trader to
the contract and credit Sepolia
                    require(assetHoldings[order.trader][assetPair] >=
assetAmount, "Insufficient asset balance for sell order");
```

```
            assetHoldings[order.trader][assetPair] -= assetAmount;

            uint256 sepoliaReceived = assetAmount * price / 1e18;

            sepoliaBalances[order.trader] += sepoliaReceived;

        }


        // Mark the order as executed by setting it to inactive

        order.isActive = false;


         emit LimitOrderExecuted(orderId, assetPair, assetAmount, price,
order.isBuyOrder);

    }
```

Finally, users have the capability to inquire about their balances and holdings, by employing the `getMySepoliaBalance` and `getHoldings` functions. The aforementioned functions facilitate the user's ability to access their Sepolia balance and holdings in designated asset pairs exclusively for viewing purposes. This serves to promote transparency and enables users to closely monitor their financial positions.

```
    /**

     * @notice Fetches the Sepolia balance of the user for a specified
pair.

    * @return The Sepolia balance of the user for the specified pair.

    */

     function getHoldings(string memory assetPair) public view returns
(uint256) {

        return assetHoldings[msg.sender][assetPair];

    }
```

```
/**
* @notice Fetches the Sepolia balance of the user.
* @return The Sepolia balance of the user.
*/
function getMySepoliaBalance() public view returns (uint256) {
    return sepoliaBalances[msg.sender];
}
```

The `OracleTrader` contract offers a comprehensive workflow (sequence and class diagrams of which can be observed in *Figures 13* and *14* below) that establishes a robust and secure platform for decentralized finance (DeFi) trading. This platform leverages the reliability of Chainlink Price Feeds to guarantee the accuracy and real-time availability of price data for the execution of trades. The contract has been designed to prioritize security, transparency, and user control, in order to facilitate a smooth trading experience on the Ethereum blockchain.

Figure 13. Sequence diagram for the OracleTrader smart contract.

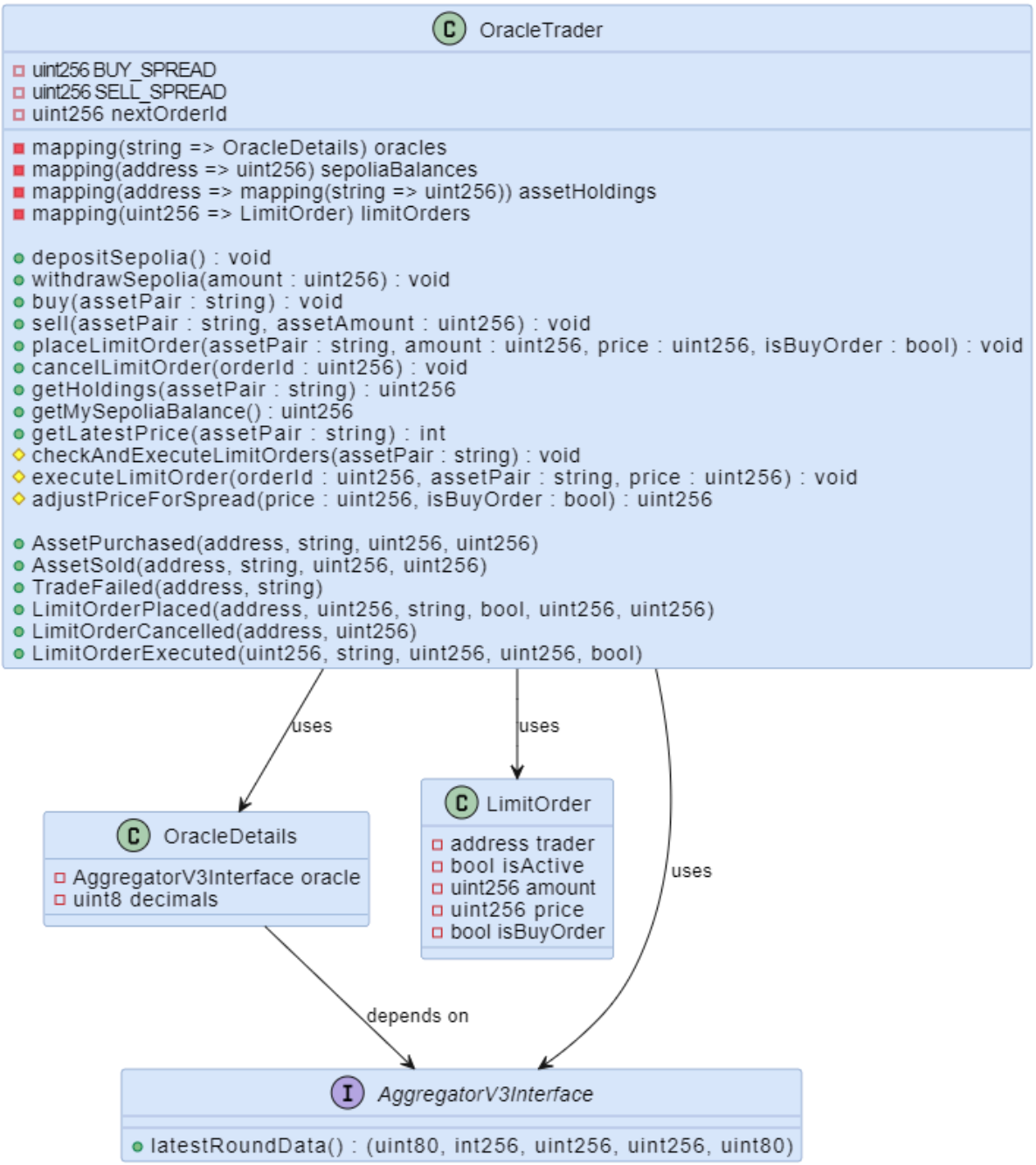

Figure 14. Class diagram for the OracleTrader smart contract.

Conclusions

This study on decentralized oracles, with a particular emphasis on the Chainlink network, has expounded upon the crucial function of decentralized oracles in bridging the inherent gaps between blockchain ecosystems and external data sources. The development of blockchain technology, which was initially conceived as a decentralized ledger for digital currencies, has undergone significant advancement and adaptation to encompass a wide array of applications across various industries. This emphasizes the crucial importance of decentralized oracles in enhancing the operational functionalities of blockchain systems. The Chainlink platform exemplifies an intricate deployment of decentralized oracles, specifically engineered to facilitate secure interoperability between blockchain networks and external data sources. Said decentralized network functions through autonomous nodes that are responsible for the acquisition, authentication, and propagation of information.

Chainlink 2.0's framework introduces significant advancements such as improved node decentralization, enhanced cryptographic data verification methods, and sophisticated oracle scripting capabilities. These cumulative improvements substantially contribute to the dependability, protection, and expansiveness of decentralized oracle networks. Said innovative approach ensures the integrity and authenticity of data transmitted to smart contracts, thereby enhancing trust and confidence in blockchain applications. The implementation of Chainlink oracles in decentralized finance (DeFi) trading contracts, which require real-time asset pricing data for executing buying, selling, and managing limit orders, demonstrates the practical applicability and essentiality of decentralized oracles in facilitating dynamic financial transactions.

Furthermore, this research examined the security issues associated with decentralized oracle networks, including but not limited to Sybil attacks, data manipulation, and node collusion. Numerous mitigation strategies were examined, encompassing cryptographic proofs, multi-source data aggregation, and robust consensus mechanisms, all of which play a critical role in augmenting the security and resilience of oracle networks. The incorporation of reputation systems and staking mechanisms serves to bolster the trustworthiness of the network through the provision of economic incentives that motivate nodes to consistently uphold high levels of performance and integrity. Said measures collectively contribute to the accuracy and dependability of the data provided to smart contracts, consequently reducing the potential risks arising from malicious activities and bolstering the overall security of decentralized oracle networks.

Moreover, the development of an oracle trader smart contract, specifically engineered to interface with Chainlink oracles, exemplifies the practical integration of decentralized oracles within DeFi applications. Said smart contract leverages Chainlink's robust infrastructure to access current asset pricing data, thereby enabling the accurate placement and execution of buying and selling orders, as well as the management of limit orders. The integration of real-time, reliable, and secure price feeds from Chainlink oracles is critical for the contract's functionality, ensuring that trading decisions are based on the most up-to-date market information. This practical implementation underscores the essential role of decentralized oracles in executing complex financial transactions transparently and efficiently.

In conclusion, the study highlights the transformative potential of decentralized oracles in the context of the blockchain ecosystem. Decentralized oracles, exemplified by platforms like Chainlink, are essential in addressing the limitations of traditional blockchains and providing a reliable and secure method for integrating off-chain data. Consequently, this facilitates the advancement of sophisticated and pragmatic applications. The findings of this study indicate a compelling rationale for the extensive adoption and integration of decentralized oracles, underscoring their fundamental role in improving the capabilities and dependability of decentralized applications. All in all, the ongoing progress and incorporation of decentralized oracles are of significant importance in the continual development of blockchain technology, providing the opportunity for smart contracts to effectively interface with real-world data in a smooth and secure fashion, thereby contributing to the sustained advancement of the field.

.

References

Ezzat, S. K., Saleh, Y. N., & Abdel-Hamid, A. A. (2022). Blockchain oracles: State-of-the-art and research directions. *IEEE Access*, *10*, 67551-67572.

Cai, Y., Fragkos, G., Tsiropoulou, E. E., & Veneris, A. (2020, September). A truth-inducing sybil resistant decentralized blockchain oracle. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 128-135). IEEE.

Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., ... & Zhang, F. (2021). Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. *Chainlink Labs*, *1*, 1-136.

Zhao, Y., Kang, X., Li, T., Chu, C. K., & Wang, H. (2022). Toward trustworthy defi oracles: past, present, and future. *IEEE Access*, *10*, 60914-60928.

Caldarelli, G. (2020). Understanding the blockchain oracle problem: A call for action. *Information*, *11*(11), 509.

Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2016, October). Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 aCM sIGSAC conference on computer and communications security* (pp. 270-282).

Costan, V., & Devadas, S. (2016). Intel SGX explained. *Cryptology ePrint Archive*.

Beniiche, A. (2020). A study of blockchain oracles. *arXiv preprint arXiv:2004.07140*.

Provable. The provable™ blockchain oracle for modern dapps. Available from: https://provable.xyz/

Cai, Y., Irtija, N., Tsiropoulou, E. E., & Veneris, A. (2022). Truthful decentralized blockchain oracles. *International Journal of Network Management*, *32*(2), e2179.

Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol, Version 1.2. Available from: https://tools.ietf.org/html/rfc5246.

Ritzdorf, H., Wust, K., Gervais, A., Felley, G., & Capkun, S. (2018). Tls-n: Non-repudiation over tls enabling ubiquitous content signing. In *Proceedings 2018 Network and Distributed System Security Symposium*. Internet Society.

Zhang, F., Maram, D., Malvai, H., Goldfeder, S., & Juels, A. (2020, October). Deco: Liberating web data using decentralized oracles for tls. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1919-1938).

Gigli, L., Zyrianoff, I., Montori, F., Aguzzi, C., Roffia, L., & Di Felice, M. (2023). A decentralized oracle architecture for a blockchain-based iot global market. *IEEE Communications Magazine*, *61*(8), 86-92.

Basile, D., Goretti, V., Di Ciccio, C., & Kirrane, S. (2021, August). Enhancing blockchain-based processes with decentralized oracles. In *International Conference on Business Process Management* (pp. 102-118). Cham: Springer International Publishing.

Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE access*, *8*, 85675-85685.

De Pedro, A. S., Levi, D., & Cuende, L. I. (2017). Witnet: A decentralized oracle network protocol. *arXiv preprint arXiv:1711.09756*.

Adler, J., Berryhill, R., Veneris, A., Poulos, Z., Veira, N., & Kastania, A. (2018, July). Astraea: A decentralized blockchain oracle. In *2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)* (pp. 1145-1152). IEEE.

Aspembitova, A. T., & Bentley, M. A. (2022). Oracles in decentralized finance: Attack costs, profits and mitigation measures. *Entropy*, *25*(1), 60.

Peterson, J., Krug, J., Zoltu, M., Williams, A. K., & Alexander, S. (2019). Augur: a decentralized oracle and prediction market platform (v2. 0). *Whitepaper, https://augur. net/whitepaper. pdf*.