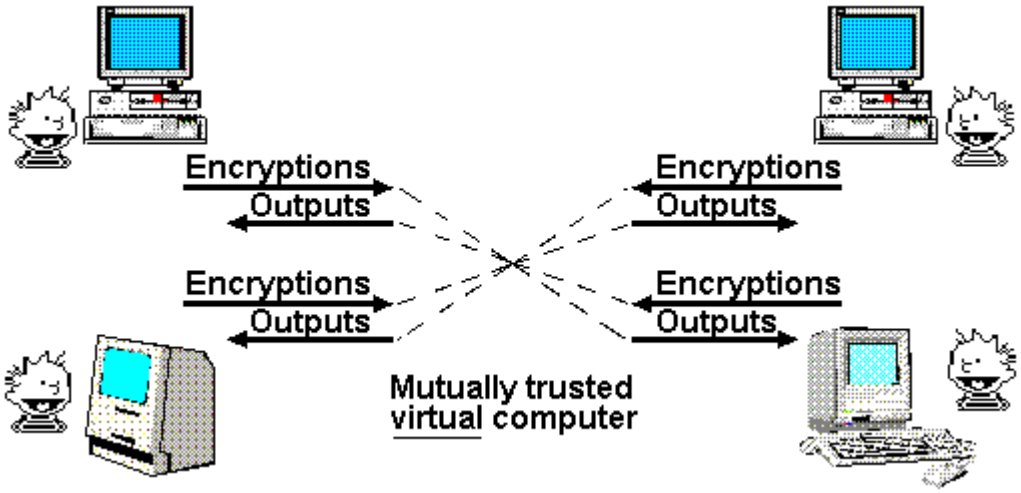
Completing The God Protocols: A Comprehensive Overview of Chainlink in 2021

SmartContent · Follow
45 min read · Jan 14, 2021

"Imagine the ideal protocol. It would have the most trustworthy third party imaginable — a deity who is on everybody's side. All the parties would send their inputs to God. God would reliably determine the results and return the outputs. God being the ultimate in confessional discretion, no party would learn anything more about the other parties' inputs than they could learn from their own inputs and the output." — Nick Szabo

In 1997, computer scientist Nick Szabo described what he termed the “God Protocols.” In short, the God Protocols refer to the general idea of a set of computer protocols that could arbitrate and facilitate processes involving an exchange of value between two or more independent parties without any bias, error, or privacy concerns. This perfect third party would be equally accessible to all participants, fairly and flawlessly execute actions according to mutually pre-agreed upon rules and commands, and wouldn’t leak sensitive information to unintended entities.

When extrapolated out to multi-party contracts, the God Protocols are designed to eliminate inefficiencies and counterparty risk by replacing human-based arbitrators/executors with math-based arbitrators/executors, resulting in the correct party consistently getting what they are owed, when they are owed, and from whom they are owed, based entirely on a provably objective interpretation of the events in which the contract is written about. Additionally, the Gods Protocols would extract as little value as possible from the process, only receiving what is needed to cover the costs of performing it.

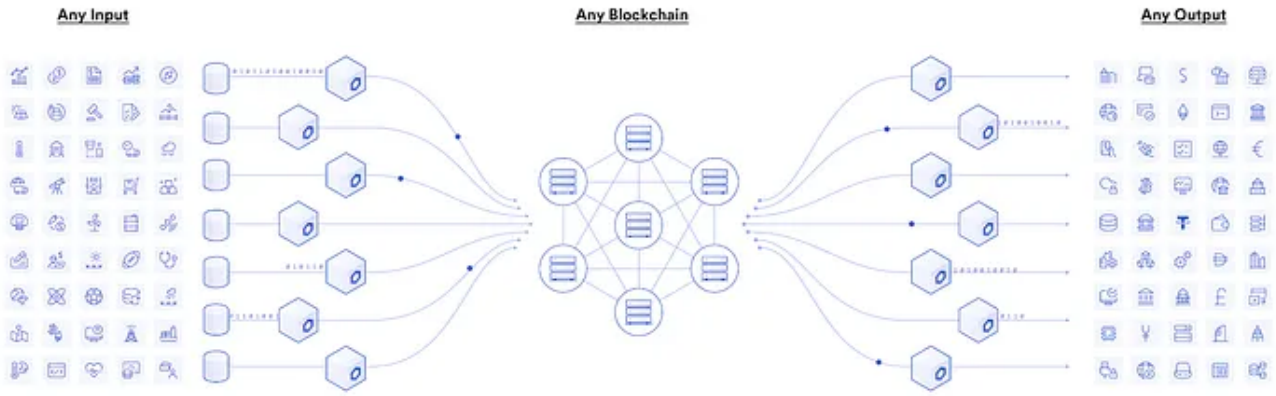


Nick Szabo’s original diagram in his first article on the subject titled The God Protocols.

While this may seem overly idealistic, and we wouldn’t say it’s fully realized or will ever be perfect, it does appear that three core technological pillars have emerged in the form of blockchains, smart contracts, and oracles, which combined create a potential foundation for God-like Protocols that are far superior to current third parties relied on today. This concept of impartial computing infrastructure acting as a neutral third party in an exchange of value between independent entities is what we believe to be the defining value proposition of blockchain technology, hence why it is often referred to as the Internet of Trust or Web 3.0. The idea of highly reliable infrastructure impervious to bias and manipulation is not only valuable for creating

and exchanging new forms of digital money like Bitcoin, but it can be applied across nearly every major industry, such as financial services, insurance, supply chain, gaming, and more.

This article is designed to explore this potential foundation of the God Protocols before going deep into the last piece of the puzzle, Chainlink. Given the wide adoption of the Chainlink decentralized oracle network, the God Protocols are closer than ever to reaching a more complete form, revolutionizing how society forms agreements and exchanges value.



Chainlink connects any blockchain to any input and output.

PART 1: PRIMER ON BLOCKCHAINS, SMART CONTRACTS, AND ORACLES

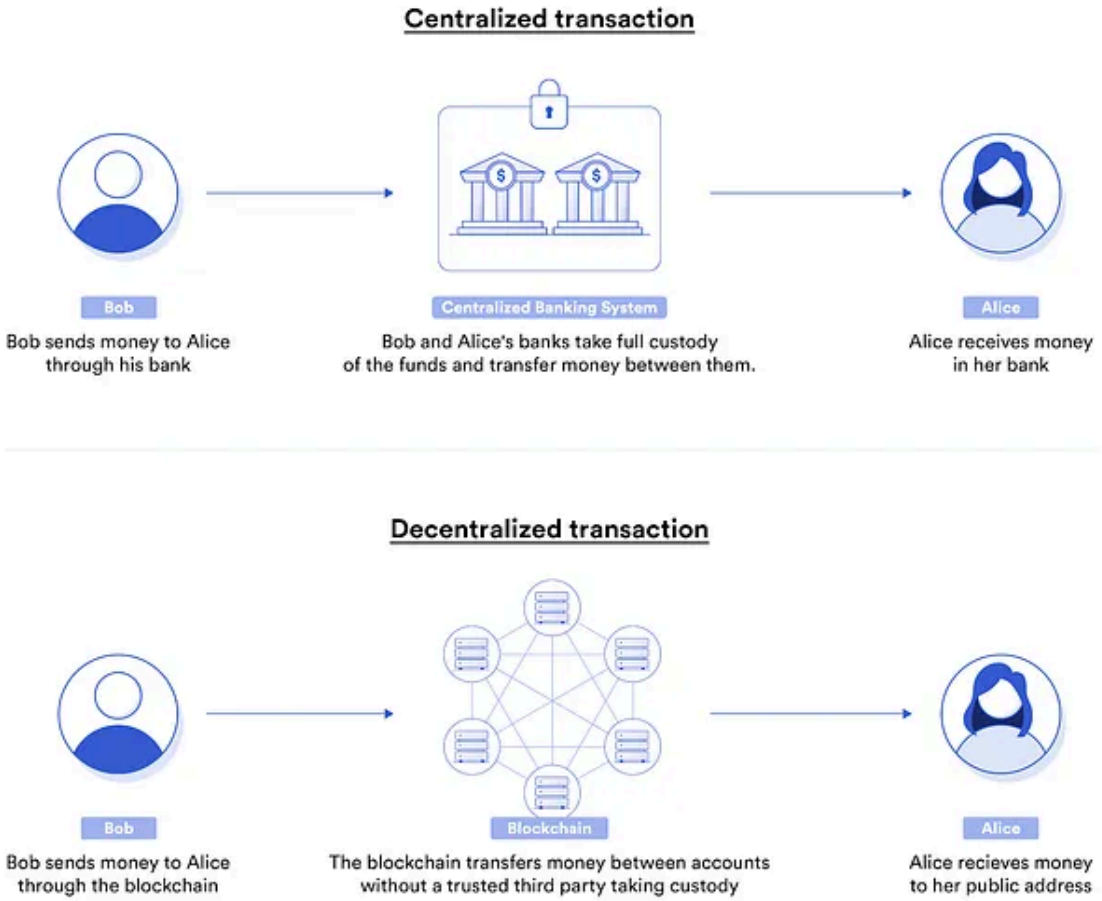
In a broad sense, the God Protocols require three distinct components: 1) the physical network that performs the work of a third-party, 2) the software for understanding a wide range of logic and triggering actions, and 3) external connectivity to the outside world so it can consume input data and generate output actions involving any combination of data sources and external systems. These components can be broken down into three core technologies: blockchains, smart contracts, and oracles.

Blockchain: The Physical Body / Decentralized Computer Network

The first component necessary to the God Protocols is the physical computing network responsible for processing the instructions sent to it and facilitating the actual exchange of value between parties (e.g., assets, rights, documents, etc.). Since the God Protocols must form a trustworthy and unbiased third party, the computing network cannot be run by a central administrator able to exercise authoritative control or influence over the process. There also needs to be a way for users to

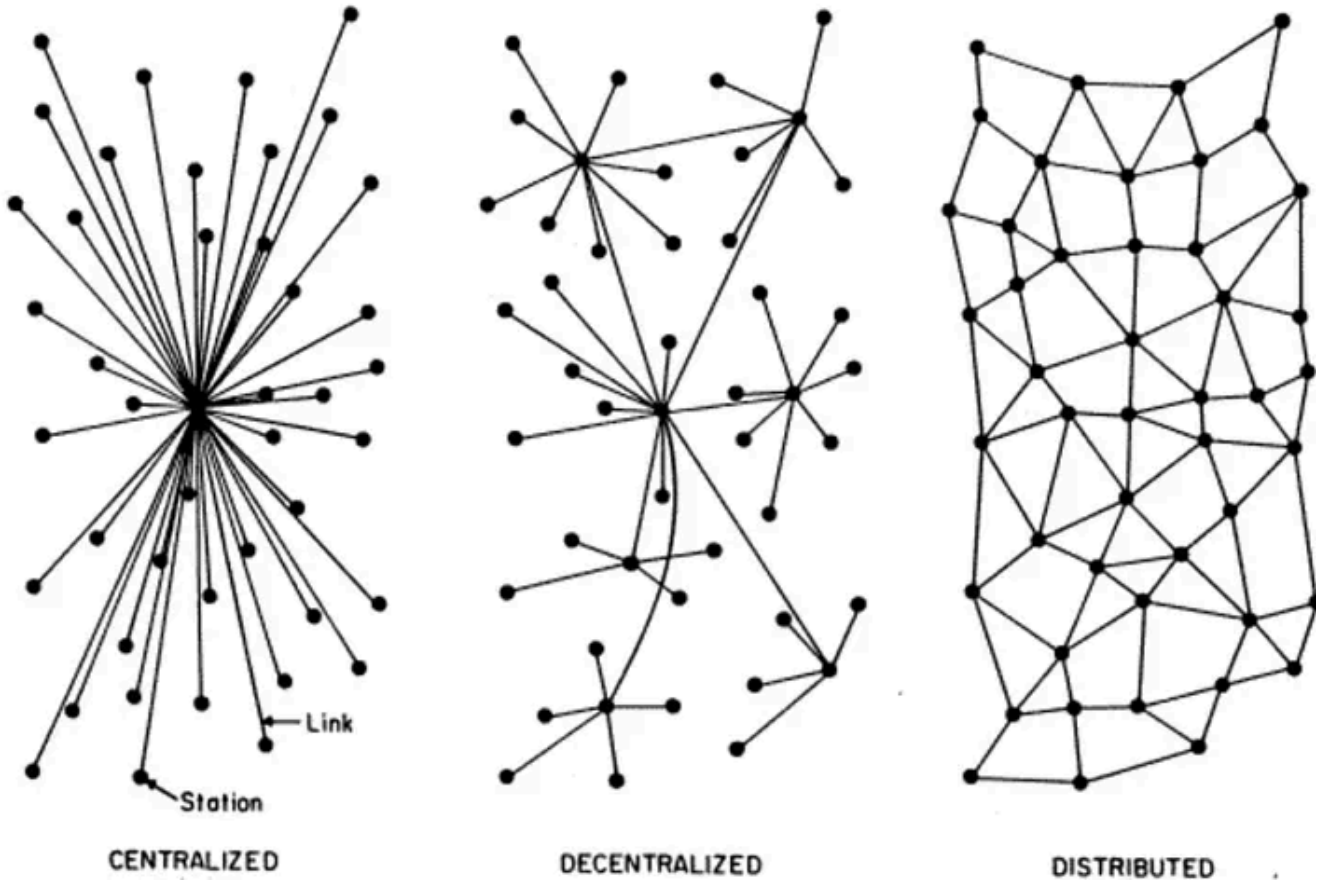
definitively prove that the computation performed by the God Protocols were done correctly.

This is where the blockchain comes into play, serving as a global computer network responsible for physically exchanging value between two or more parties in a non-custodial manner and documenting the results as data stored in an immutable ledger that anyone can verify as being valid. Blockchains achieve this by operating as a decentralized network of independent computers, which all run the same open-source software set to the same specification, redundantly validate the same transactions, and maintain an ongoing copy of the same ledger. The shared ledger (blockchain) consists of public key addresses (akin to user bank accounts) that prove ownership of cryptocurrency/tokens and can only be accessed by users in possession of the corresponding private key addresses (akin to the user's password), with only one unique private key for each public key.



Blockchains use a decentralized network to facilitate the exchange of value between parties without ever taking custody of the asset, whereas a bank takes custody conducting payments.

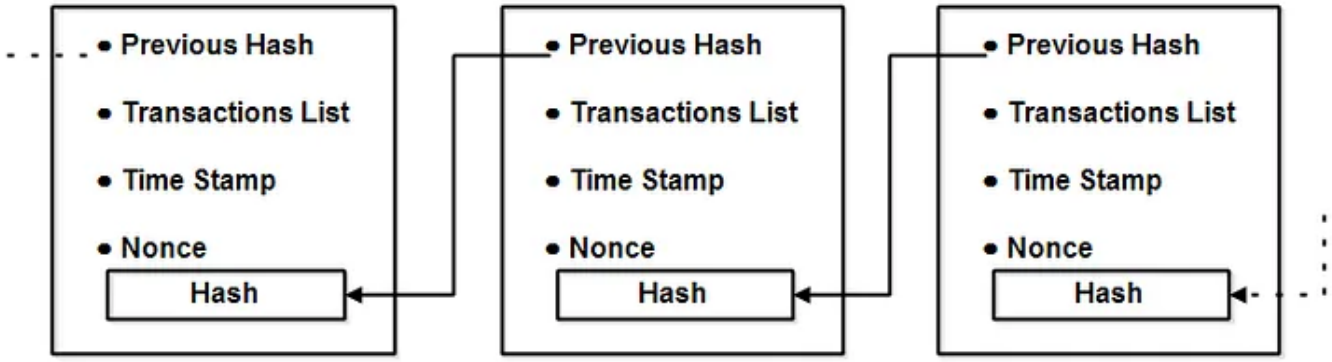
The question is, how does a network of computers reach a consistent agreement (consensus) about the state of a shared ledger despite malicious attempts to corrupt it? The answer: financial incentives and decentralization. In a Proof of Work (PoW) blockchain, each blockchain node (miner) batches together a bunch of pending transactions sent by users (called a block) and competes to get their block approved by being the first miner to generate a specific cryptographic hash through brute force (i.e., guessing random numbers until correct). The first node to generate a valid hash wins the block reward (newly minted cryptocurrency + transaction fees), and their block of transactions is confirmed by all other nodes on the network and added to the ledger.



Bitcoin is distributed because all miners store and maintain a copy of the ledger. Bitcoin is also decentralized because if some nodes were to go offline, the Bitcoin blockchain will continue to function as normal. (source)

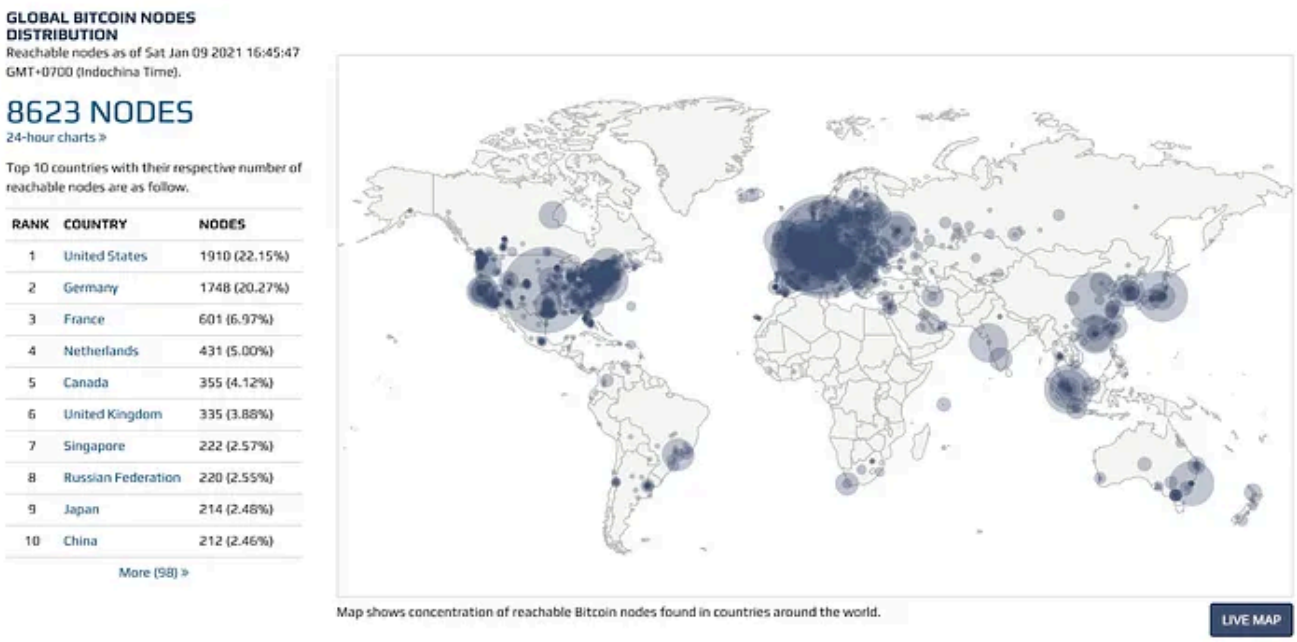
The process, which is similar to a lottery competition between computers for a reward, is designed this way in order to make it difficult for a single miner or small group of miners to consistently generate a valid hash, keeping the network decentralized. A decentralized network of financially incentivized nodes is inherently resistant to the actions of a few malicious nodes as long as they don't get control over a sufficient amount of the computing power of the PoW-based blockchain (which in most cases is 51%). Additionally, each block contains a unique

hash of the previous block, creating a continuous chain of blocks dating back to the first “genesis” block. If any historical block was tampered with, it would become immediately apparent to all network participants as the hashes from one block to another would no longer match.



A blockchain is quite literally a chain of blocks connected through cryptographic hashes; (source).

While there are different ways to achieve consensus in a decentralized network (e.g., Classical, Nakamoto, and Avalanche), numerous ways to generate Sybil control (e.g., Proof of Work, Proof of Stake, Proof of Authority), and various degrees of permissions about who can participate in the network’s consensus (e.g., Permissionless, Permissioned), the blockchain described above (Nakamoto, PoW, Permissionless) is generally how the two most widely used blockchains, Bitcoin and Ethereum, currently work. The value in such blockchain network designs is that it’s extremely expensive and highly impractical to achieve 51% control over the network, meaning users can trust to a very high degree that the data stored and computation performed on the network is secure, reliable, and accurate without any realistic possibility of manipulation or tampering of the ledger. Also, since blockchains are decentralized, run on open-source software, operate in a permissionless manner, and keep track of previous state, the network is always online for anyone with an Internet connection to access, ensuring that any user at any time is able to independently verify the validity of transactions.



The Bitcoin blockchain consists of thousands of independent nodes operating around the world.

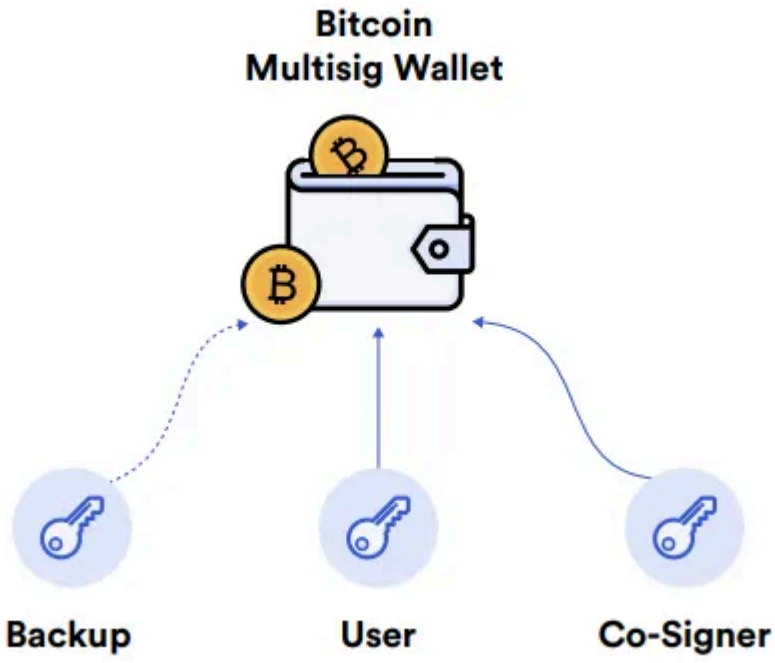
Bitcoin was the first implementation of a blockchain, which facilitates the exchange and tracks ownership of its own, newly created monetary asset, Bitcoin (BTC). The reason Bitcoin is seen as a reliable store of value is that there will only ever be 21 million Bitcoins in existence (with over 18M already circulating); a feature that is incredibly difficult to change or inflate given the network's decentralized nature, especially in comparison to central bank-issued fiat currencies. Any users attempting to alter the 21M hard cap on the supply will find it extremely difficult to achieve social consensus, resulting in a fork from the main chain (e.g., similar in concept to Bitcoin Cash, which forked from Bitcoin; however, the reasoning was due to network scaling differences, not supply disagreements).

In addition to decentralization, miners have to spend a lot of money on application-specific hardware only useful for mining Bitcoin if they want to participate in consensus. Thus, in order to turn a profit, they are incentivized to uphold the value of the Bitcoin network by keeping it secure, as a secure network will help maintain the value of the cryptocurrency (BTC) they are exclusively paid in. However, blockchains can be used for far more than tracking and trading cryptocurrency, as Ethereum has thoroughly demonstrated.

Smart contracts: The Brain / Decentralized Applications

The second component to the God Protocols is being able to comprehend a wide range of logic (if x event happens, execute y action), meaning the blockchain is able to process a variety of instructions sent to it by users in the form of applications. As the first blockchain in existence, Bitcoin has a very narrow range of logic that it can

process, namely moving BTC from one account to another on the Bitcoin blockchain upon certain conditions being met: 1) the sender signs the transaction with the correct private key and 2) the sender has enough BTC to cover the transaction. While Bitcoin has expanded slightly in the logic it can process to include multi-sig transactions (require multiple specific private key signatures before the transaction is considered valid) and Hash Time-Locked Contracts (transactions in time-bound escrow, used in payment channels like the Lightning Network), both of which can be considered some of the first "smart contracts," it has largely remained static since.



An example of a 2-of-3 multi-signature wallet on the Bitcoin blockchain.

Though there were some minor advancements in between, the Ethereum blockchain generated the next major advancement in 2015 by launching support for programmable smart contracts. This basically transformed the function of a blockchain from serving as a single application into serving as a world computer able to simultaneously support many different applications at the same time. Ethereum made it much easier for developers to write and maintain their own Turing complete smart contracts on top of the blockchain (written in Solidity), enabling anyone to deploy a decentralized application with a customized set of logic, along with the option to update the smart contract themselves without requiring any change to the underlying blockchain.

Programmable smart contracts lead to the creation of fungible tokens, where specific public addresses were assigned to specific assets. This allowed a single blockchain to support a wide range of digital assets outside of its native cryptocurrency (i.e., a ledger of ledgers). Smart contracts also expanded the types of computation the blockchain could assign to those tokens, such as the creation of Decentralized Autonomous Organizations (DAOs) for decentralized voting between specific token holders, as well as the Decentralized Finance (DeFi) ecosystem that combines tokens and smart contracts to facilitate decentralized lending and borrowing markets, trading exchanges, derivatives products, and more. However, there was still one key problem; the blockchain is inherently disconnected from data and systems in the outside world.

Oracles: The Outside World / Decentralized Internet

The third component to the God protocols is for smart contracts to become aware of events and interact with systems existing outside the native blockchain they run on. External connectivity entails two functions: 1) consuming data originating outside the blockchain and 2) passing instructional commands to external systems for them to perform (e.g., execute a payment on PayPal).

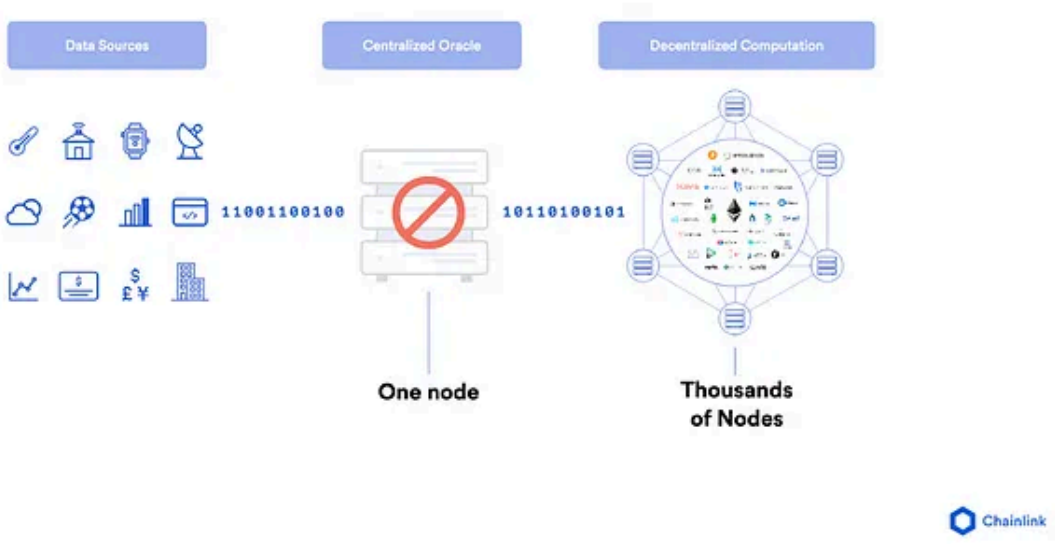
Chainlink connects the existing world to the new world; (source).

Blockchains are inherently closed and deterministic systems, meaning they have no built-in capabilities to talk to and exchange data between external systems (as doing so could break network consensus). While this generates the valuable security and reliability properties that users seek when using a blockchain, it also severely limits the types of data inputs that smart contracts can ingest and the types of output actions they can trigger on external systems. Most valuable datasets like financial asset prices, weather conditions, sports scores, and IoT sensors, as well as the currently preferred fiat settlement methods like credit cards and bank wires, exist outside the blockchain (off-chain). Given the importance of these resources to real-

world business processes, blockchains need a secure bridge to the outside world in order to support a vast majority of smart contract application use cases.

Providing smart contracts connection to the outside world requires an additional piece of infrastructure known as an oracle. An oracle is an external entity that operates on behalf of a smart contract by performing actions not possible or practical by the blockchain itself. This usually involves retrieving and delivering off-chain data to the smart contract to trigger its execution or passing data from the smart contract to an external system to trigger an off-chain event. It can also involve various types of off-chain computations in advanced oracle networks (discussed more below), such as aggregating data from multiple sources or generating a provably fair source of randomness.

Similar to blockchains, the oracle mechanism cannot be operated by a single entity, as that would give the centralized oracle sole control over the inputs the contract consumes, thus control over the outputs it produces. Even if the blockchain is highly secure and the smart contract logic is perfectly written, the oracle will put at risk the entire value proposition of the smart contract if it is not built to the same security and reliability standards as the underlying blockchain network, often referred to as the oracle problem. Why have a blockchain network of thousands of nodes when it's triggered by a single entity?



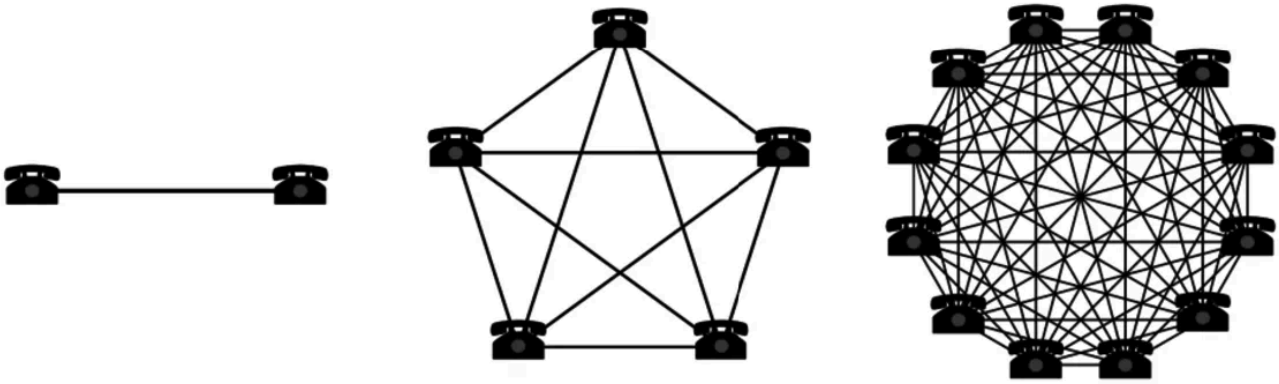
Centralized oracles are a single point of failure.

This is where Chainlink comes into play, providing smart contracts with a secure and reliable way of interacting with anything outside the blockchain, ultimately allowing it to overcome the oracle problem.

PART 2: HOW THE CHAINLINK NETWORK WORKS

While a substantial amount of focus has been placed on the development and understanding of blockchains and smart contracts, oracle networks are just as critical, given their importance to achieving mainstream adoption. To overcome the oracle problem, Chainlink launched the world's first decentralized oracle network in 2019. Chainlink has since become the most widely used solution for connecting blockchains and off-chain resources, and currently secures tens of billions of dollars in on-chain value for leading blockchain applications that rely on its oracle services to securely interact with assets.

Although other oracle implementations exist, Chainlink is the industry-leading oracle solution due to its underlying technology, market adoption, development team, token economics, and potential addressable market. Additionally, similar to the Internet, the oracle layer of the God Protocols is likely to be a winner take all, as standardization and network effects are critical when trying to get all of the world's systems to communicate and pass data between one another.



A growing network effect visualized; (source).

In order to fully understand why Chainlink is the undisputed market leader and poised to become a universal standard used to connect all blockchains and off-chain systems, we analyze in great detail the underlying architecture of the Chainlink Network, how it generates security and reliability, the types of oracle functionalities it provides, and how its native asset LINK is used.

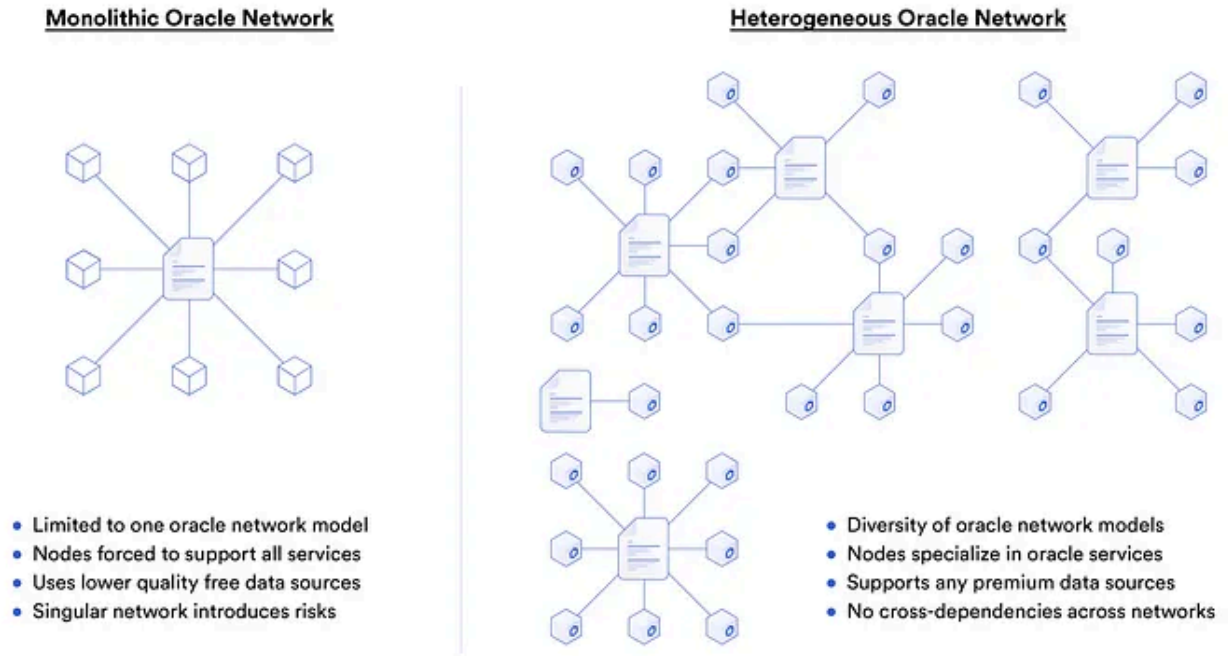
The Underlying Architecture of the Chainlink Network

The first thing to understand is that Chainlink is not a single monolithic network, but instead, a generalized heterogeneous framework where any number of independent oracle networks can be custom built and run simultaneously without any dependencies on any other oracle network. Chainlink is also open-source and

permissionless, meaning anyone can review the software code run by the oracles and launch their own oracle network to meet their specific external data and computation needs.

A Network of Networks

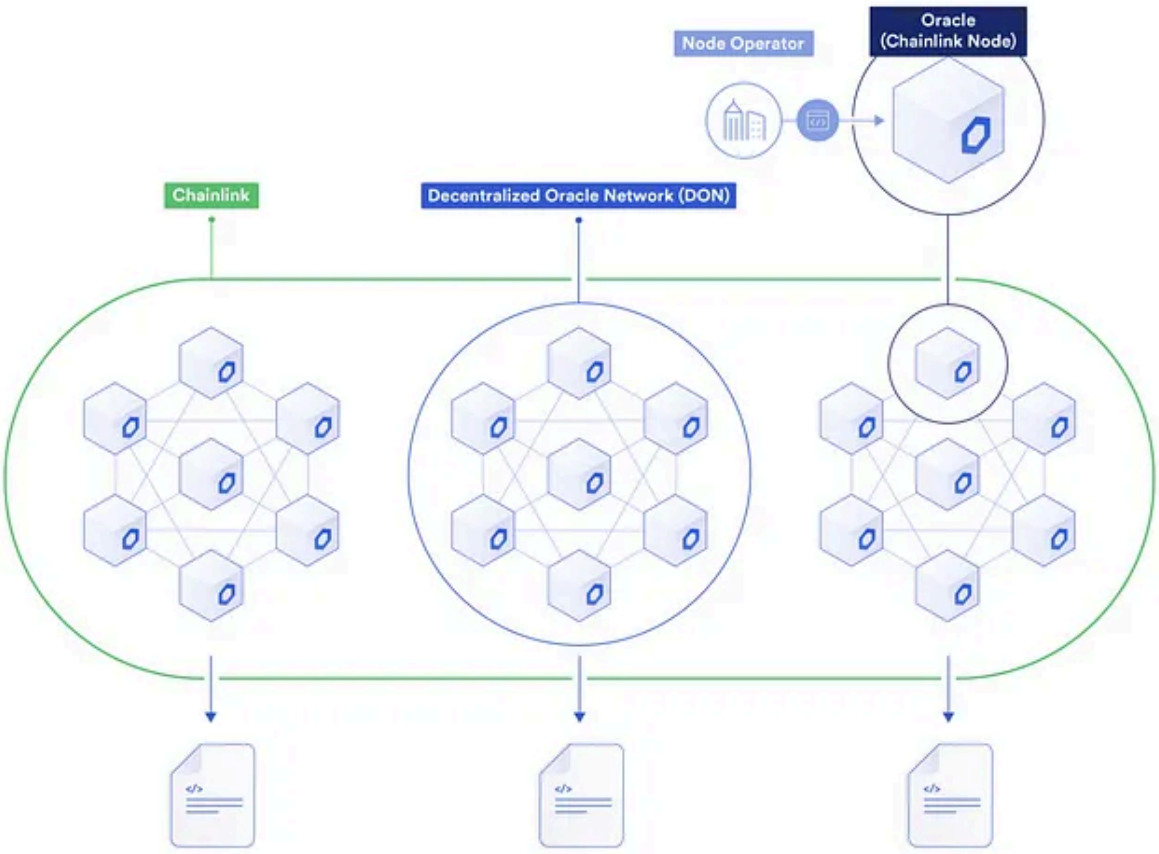
Given its heterogeneous, open, and permissionless nature, Chainlink users can decide exactly how they want their oracle network constructed, including the ability to choose any node operators, data sources, data aggregation strategy, update frequency, and various other security parameters like collateral amounts, reputational thresholds, and historical performance requirements. As a result, Chainlink is best described as being a network of networks, consisting of a free market economy where oracle nodes and networks compete with one another for jobs and/or specialize in providing different jobs.



The Chainlink Network consists of multiple independent oracle nodes and oracle networks running in parallel without cross-dependencies.

In contrast to a PoW-based blockchain, where every miner participates in processing every transaction, Chainlink is designed where not every oracle is involved in every oracle job requested by a smart contract. This flexibility and removal of standardization across all oracles allow Chainlink to support any/all types of data requests, regardless if every existing node is compatible or not. It would be impossible to service all types of oracle requests if every node were required in each job, specifically, because off-chain data feeds often cost money to

access or are permissioned to authorized users. Having all nodes paying for all the data feeds required by all contracts is not economically feasible, nor will many oracle nodes even be allowed to access most enterprise data types. Instead, oracles can specialize in providing certain oracles services like specific data types and specialized off-chain services, or simply serving certain blockchains (e.g.; permissioned oracle nodes used to service a permissioned blockchain).

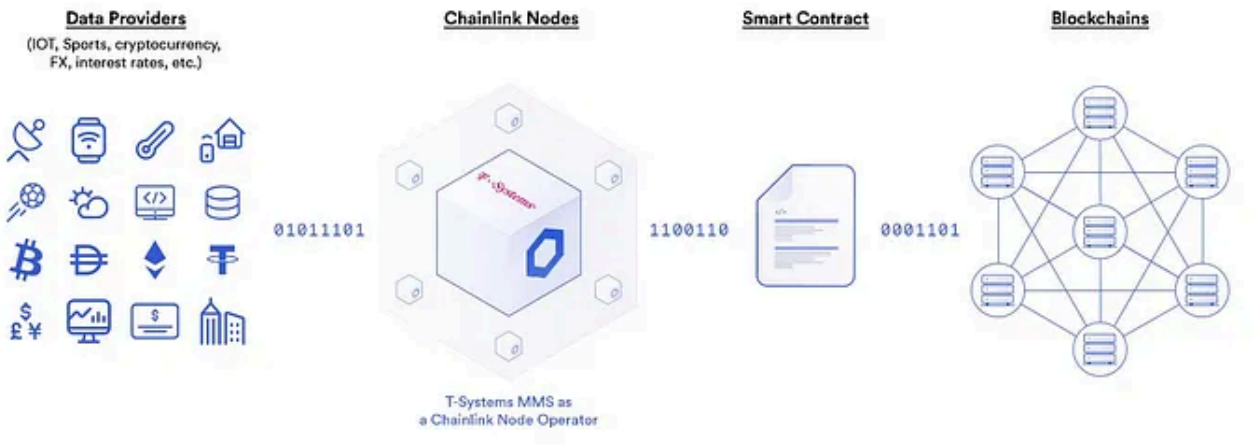


The various terms used when describing the Chainlink Network architecture.

Diversity of Chainlink Nodes

The Chainlink Network currently consists of two types of oracle nodes, 1) security reviewed node operators with known identities and approved by the Chainlink team to ensure that the initial set of oracle networks are highly secure and reliable, and 2) non-security reviewed nodes run by either known or unknown entities from the community or traditional markets that require no approval processes. While anyone can launch a Chainlink node today, most of the initial Chainlink oracle networks are being run by security reviewed node operators in order to ensure their reliability in the early stages of the Chainlink Network, particularly to guarantee consistent uptime and maintain Sybil resistance (preventing a single entity from pretending to be multiple independent nodes).

Over time, the Chainlink Network will consist of a diverse array of node operators, including security reviewed oracles for high-value use cases, specialized data providers running their own nodes directly (increasingly happening today), and non-security reviewed nodes for obtaining additional oracle services that require lower quality control measures, employ more decentralization, and/or make use of additional features to further guarantee security and reliability (e.g., staking).



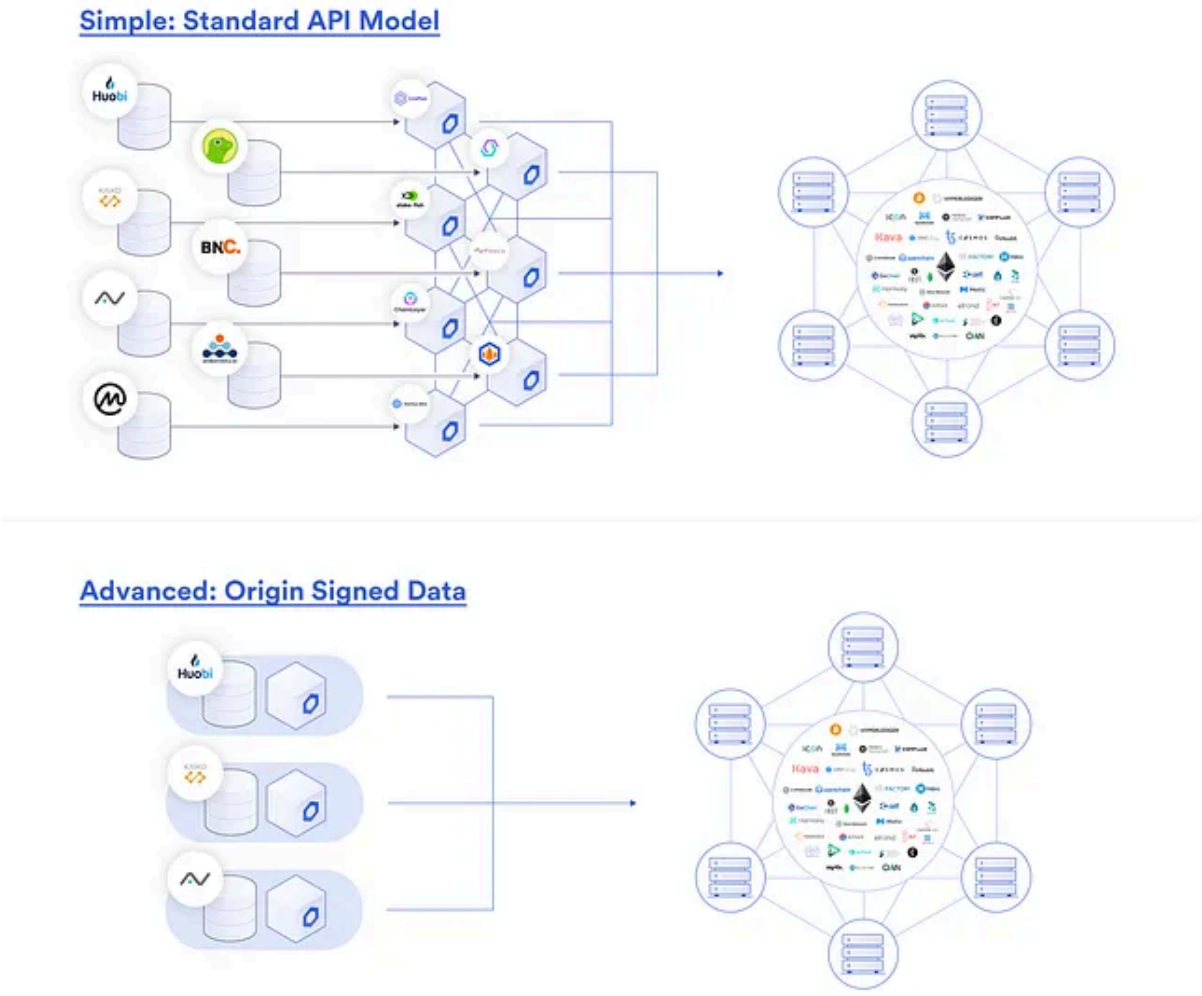
Deutsche Telekom subsidiary, T-System MMS, is an example of a Chainlink node operator running in-production (source).

Diversity of Data Sources

Chainlink brings data to blockchains by having oracles connect to Application Programming Interfaces (APIs) — the most commonly used way of allowing other companies/users to access your data and services within their own applications and systems (often for a fee), removing the need to build infrastructure from scratch. For example, Uber leverages three separate APIs to support their ride-sharing platform: a GPS API for location (MapBox), an SMS API for messaging (Twilio), and a USD API (Braintree) for payments. Through its external adapter technology, Chainlink oracles can establish a connection to any open or authenticated API; thus, allowing a smart contract to communicate with virtually any external system.

Chainlink oracles have two methods of getting API data into the blockchain: 1) a simple model where professional node operators transfer data between API providers and blockchain networks, meaning existing data companies don't need to change anything about their current business model or infrastructure, or 2) an advanced model where data providers operate their own Chainlink node to sell origin-signed data directly to smart contracts and get paid on-chain. These two models, in combination, mean the Chainlink Network can bring all of the world's

data onto the blockchain, either through direct participation by existing API providers or no participation at all in a business-as-usual approach.

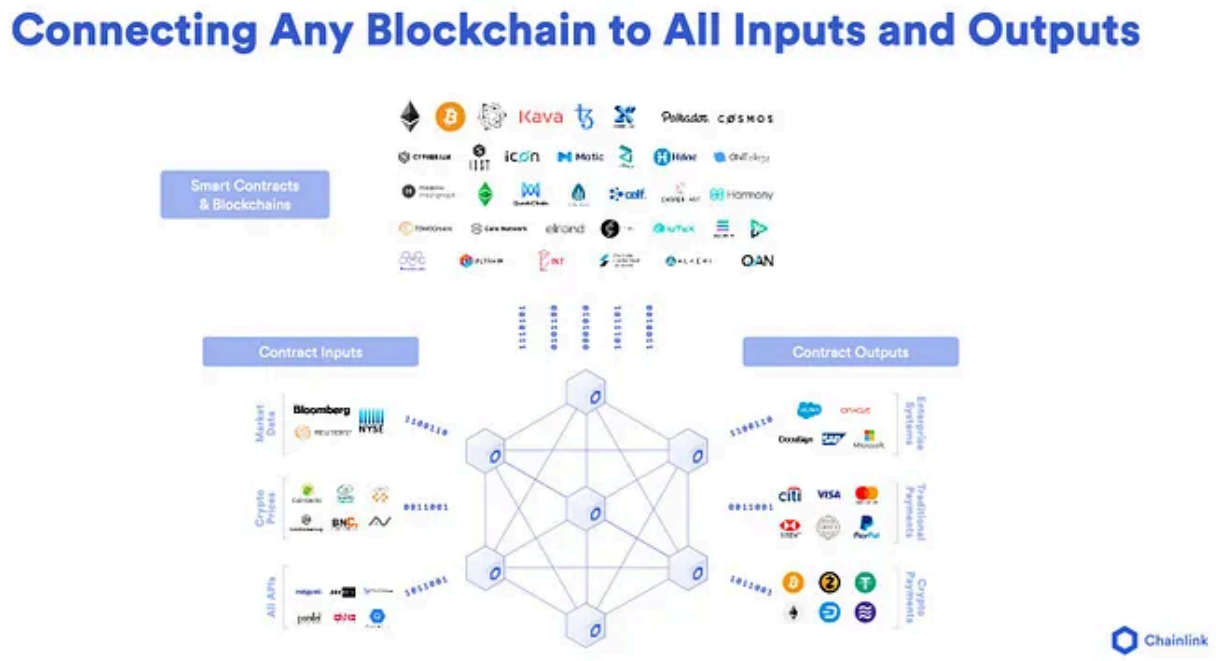


API providers have a high degree of flexibility on how they can leverage Chainlink to sell data to blockchain markets; (source).

Diversity of Blockchains

The Chainlink Network is also natively blockchain agnostic, meaning it can provide native oracle services to smart contract applications running on any blockchain without dependencies on any other blockchain. With the growing diversity of blockchains that specialize in providing certain features like decentralization, speed, and privacy, the demand for blockchain agnostic oracles is high and ever-growing. The ability to connect to any blockchain not only leads to Chainlink having cross-chain communication capabilities, but it futureproofs the Chainlink Network, ensuring data and API providers can quickly connect to any future blockchain that emerges. Chainlink is already running across many of the leading blockchains, with numerous others actively being integrated. The LINK token also has been bridged

across numerous blockchain networks such as Ethereum, Binance Smart Chain, Polygon, Avalanche, Arbitrum, Optimism, and more, which allows users to pay Chainlink oracles in the same environment as their smart contract application.



Chainlink can connect all blockchains to any off-chain input and output.

How Chainlink Provides Oracle Security and Reliability

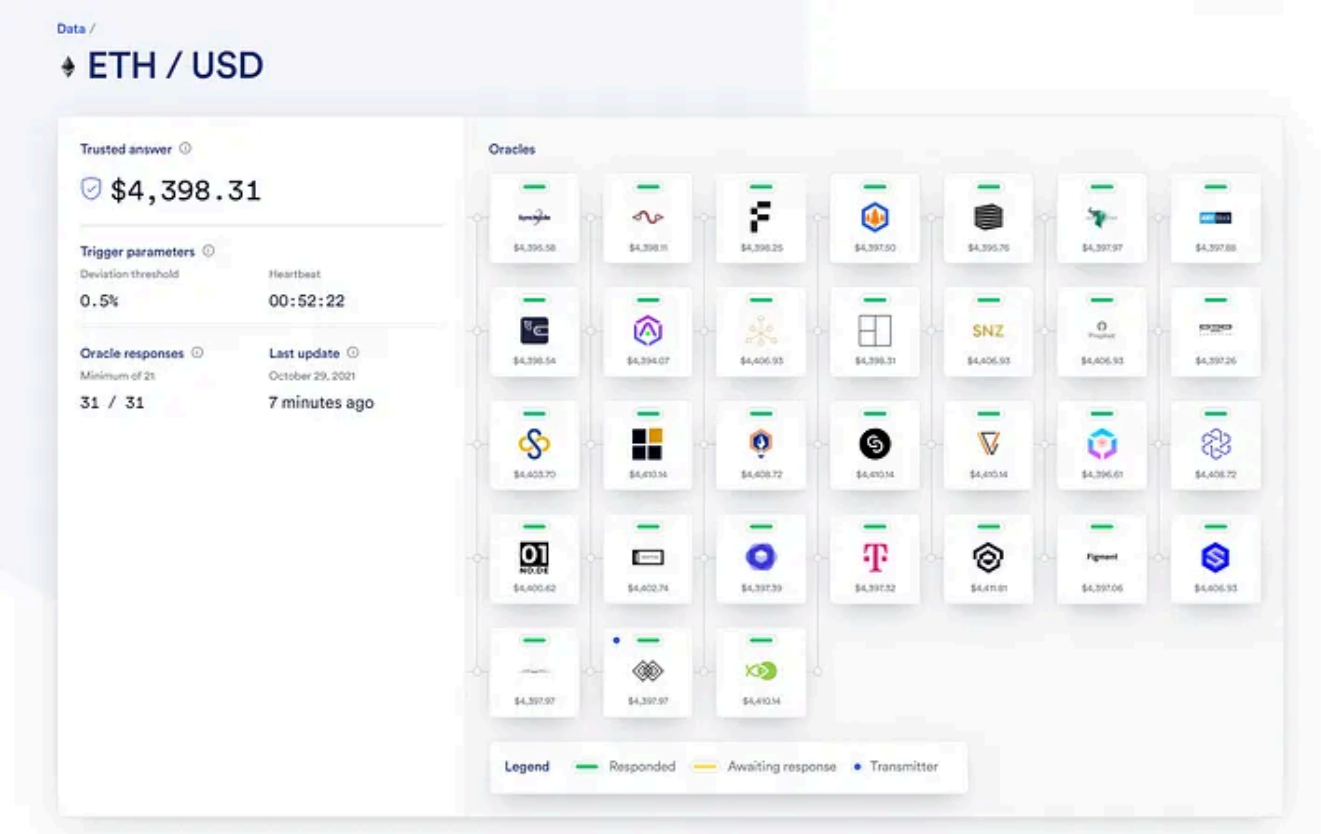
While flexibility is key to becoming a standardized solution capable of supporting all oracle requests, it cannot come at the expense of security and reliability. Unlike a blockchain, which has a single security approach, oracle networks require a multitude of security techniques due to the unique and broad set of functionalities they provide.

Chainlink provides the most expansive set of security techniques in the market, which is why it's able to protect smart contracts even during extreme black swan events. These security techniques include decentralization, data signing, crypto-economics, reputation systems, privacy, and scalability, all of which can be combined in different ways to create a defense-in-depth approach to security.

Decentralization

Just as blockchain networks generate their security through the decentralization of nodes, the Chainlink Network provides security through the same approach. Decentralization can be applied in the Chainlink Network in three ways, 1) employing numerous different node operators to source and retrieve data,

preventing one or a small group of oracles from being a single point of failure, 2) gathering data from multiple independent data sources, avoiding a single API being the only source of truth, and 3) utilizing data providers who specialize in aggregating data themselves across multiple sources depending on the type of data (e.g., using multiple IoT sensors for weather data or collecting from hundreds of crypto exchanges for price data). The multiple data points retrieved by the multiple oracle nodes are then aggregated (e.g., take a median) to create a single data point consumed by the smart contract. These multiple layers of aggregation ensure that data is accurate, delivered on-time, and resistant to manipulation despite any potential malicious activity from a small group of oracles or data sources, resulting in end-to-end decentralization of the smart contract.



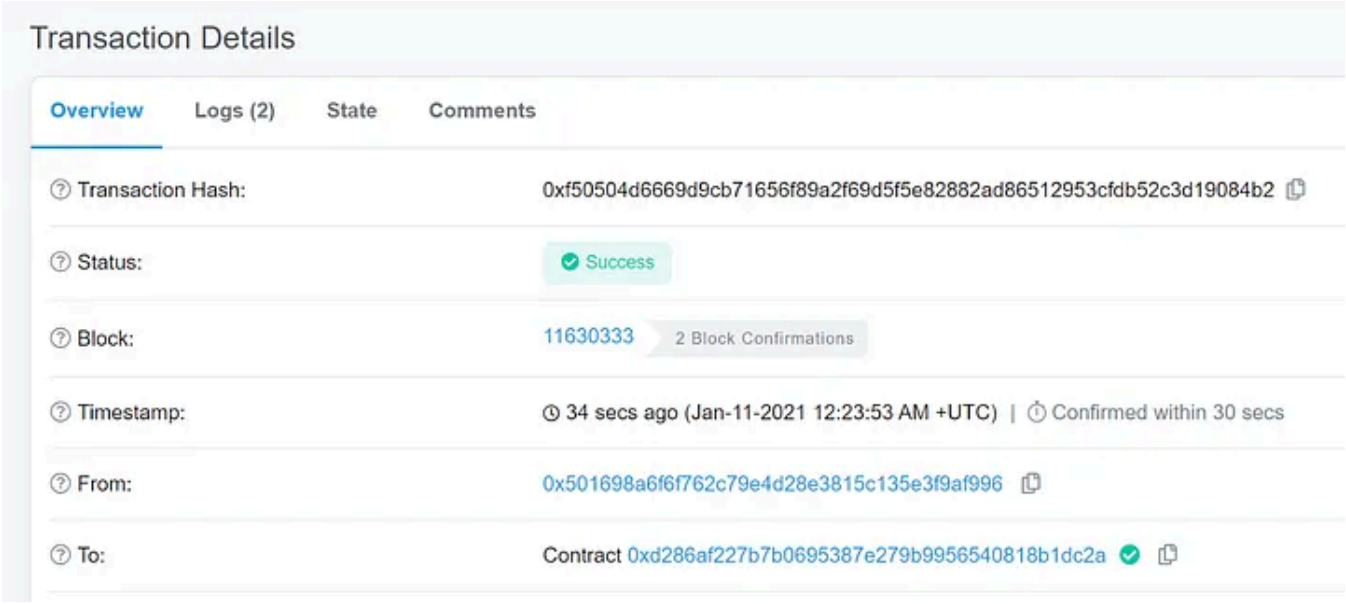
The ETH/USD price reference feed is an example of a decentralized Chainlink oracle network.

Additionally, most Chainlink nodes operating today run two versions of the Chainlink software, meaning in the worst-case scenario, they can failover to the previous software version and continue operating safely (such a situation has never happened). Smart contracts can also choose to implement optional circuit breakers for an additional level of redundancy. For example, using a historical circuit breaker in a Chainlink Price Feed, which compares the current price update delivered by the oracle network to the previous one, and if there is a difference greater than the threshold set by the user (e.g., more than 10%), the circuit breaker can trip and

trigger a preventive action like a temporary pause in the application. These further provide hyper-reliability to the Chainlink Network, even amidst an extremely rare black swan event.

Transparency and Data Signing

Chainlink oracles cryptographically sign each piece of data delivered to the blockchain, serving as irrefutable proof that the data came from a specific node operator. The act of signing data is achieved via a unique private key only available to that node operator, which cannot be falsified. Additionally, because the data is signed and stored on the blockchain, it serves as an immutable and tamper-proof record of a node's historical performance. Thus, node operators are always held accountable for their performance, as anyone can verify their performance history and know it hasn't been tampered with. Even with the introduction of off-chain aggregation, each oracle report delivered on-chain contains every node's individual observation and signature for transparency.



Each node's transaction is signed by a private key and stored on-chain as an immutable record; (source).

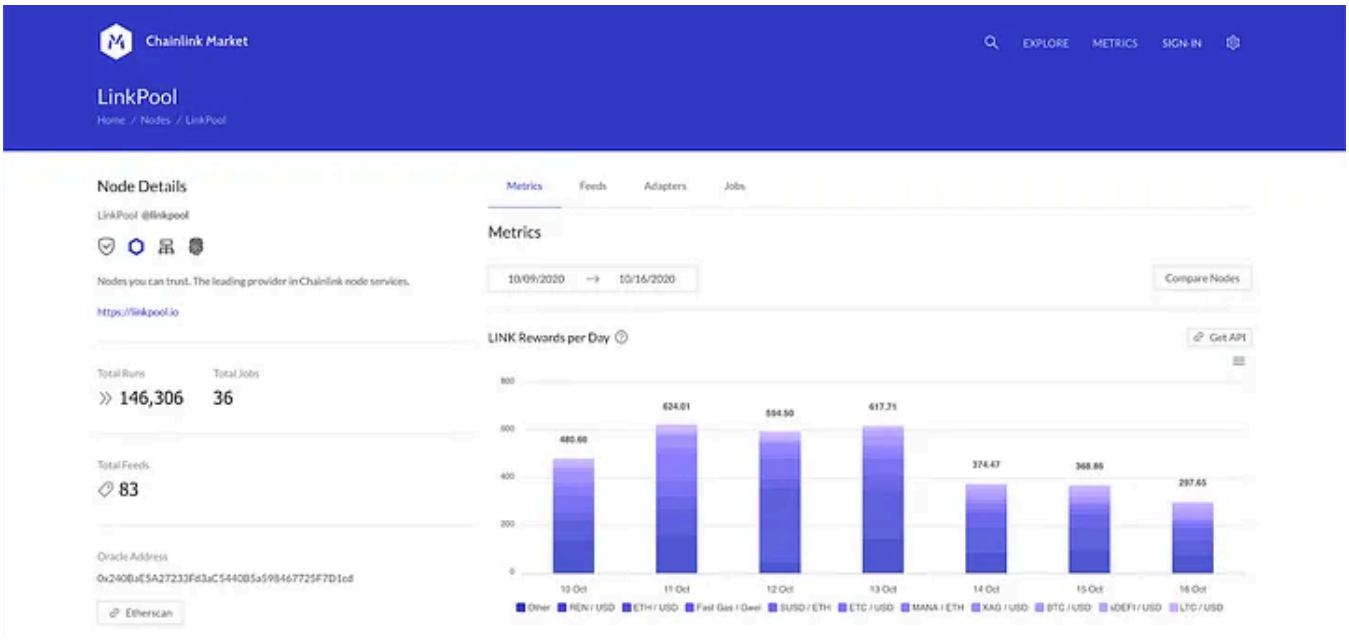
Traditional data providers running Chainlink nodes to sell their data to smart contracts can leverage this data signing capability to provide users cryptographic proof about the origin of their data (e.g., smart contracts know it came straight from the source). With oracle-delivered data triggering the automatic exchange of real assets, data signing allows blockchain applications to be certain that they received data from the correct source, making them even more reliable for automating processes.

Reputation System

Because each oracle signs data on-chain, the performance history of each node can be tracked and loaded into reputation systems that potential future users can reference and filter through when deciding which nodes they want to rely on for oracle services. Historical performance data can be coupled with other optional metrics about the node operator, such as their off-chain identity, specialized certifications, ethical contributions, geographic location, and the number of LINK tokens they hold and/or will stake. These metrics are key to node operators showcasing to users why they are high-quality and worthy of being selected for upcoming jobs.

Reputation systems bring additional Sybil resistance and accountability to node operations, wherein a node cannot act maliciously or pretend they are someone else and then hide away from sight and hope people forget about their past actions. Poorly rated node operators would likely be removed from the networks they support and lose potential future revenue in the Chainlink Network, as users are unlikely to select them for upcoming jobs. They could also destroy their off-chain reputation across other blockchain and non-blockchain related endeavors.

For example, if a Chainlink node also operates a validator on a PoS blockchain network like Cosmos, delegators may unstake their tokens to that validator due to fears that the poor services witnessed on Chainlink will carry over to Cosmos. Similarly, if a data provider runs a Chainlink node and provides bad data, they could lose subscriptions to their data feeds across numerous blockchain and non-blockchain markets. Not only could this lead to a reduction in business revenue, but it could end up in lawsuits from the harmed parties in a worst-case scenario (given that nodes are identifiable).



An overview of LinkPool's oracle node on the Chainlink Marketplace; (source).

Privacy

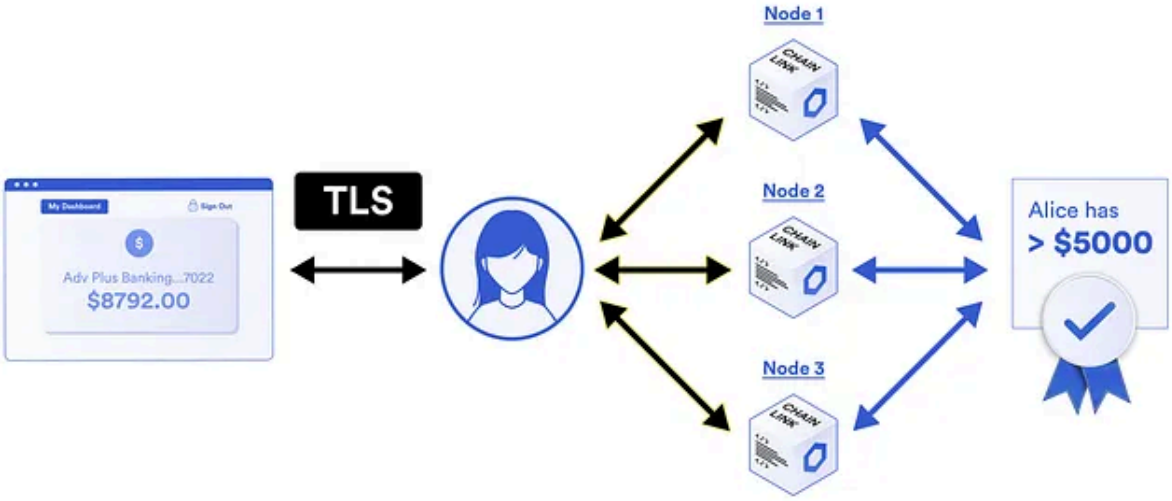
Chainlink is developing several novel approaches to data and oracle privacy, designed to mitigate concerns around the general public and/or the oracle node itself being able to read the data retrieved and/or see the computation it's asked to perform. Generating privacy will greatly expand the number of smart contract use cases, as it unlocks a large portion of data currently unavailable for consumption on the blockchain due to user privacy and data licensing laws. Chainlink's privacy solutions currently include:

- DECO — Zero-knowledge proofs that prove facts about data within a user's web session without any data ever leaving the web session or the oracle seeing any data it's not supposed to. For example, having the oracle accompany someone as they log in to their bank account in order to prove through a yes or no answer whether they are above 18 years old or have more than $100,000 USD.

- Mixicles — An oracle-powered mixer design that generates transaction privacy on the blockchain by separating the smart contract's logic from its resulting payment. The oracle is used as an intermediary between the two, preventing external actors from correlating a contract's terms to its subsequent settlement payments.

- Town Crier — Oracles that leverage trusted hardware (e.g., Intel SGX), referred to as a trusted execution environment. Essentially, the oracle runs in a black box computing environment where the node operator cannot see the instructions

sent by the smart contract or the data they generate/retrieve, giving smart contracts complete data, computation, and node operator privacy.

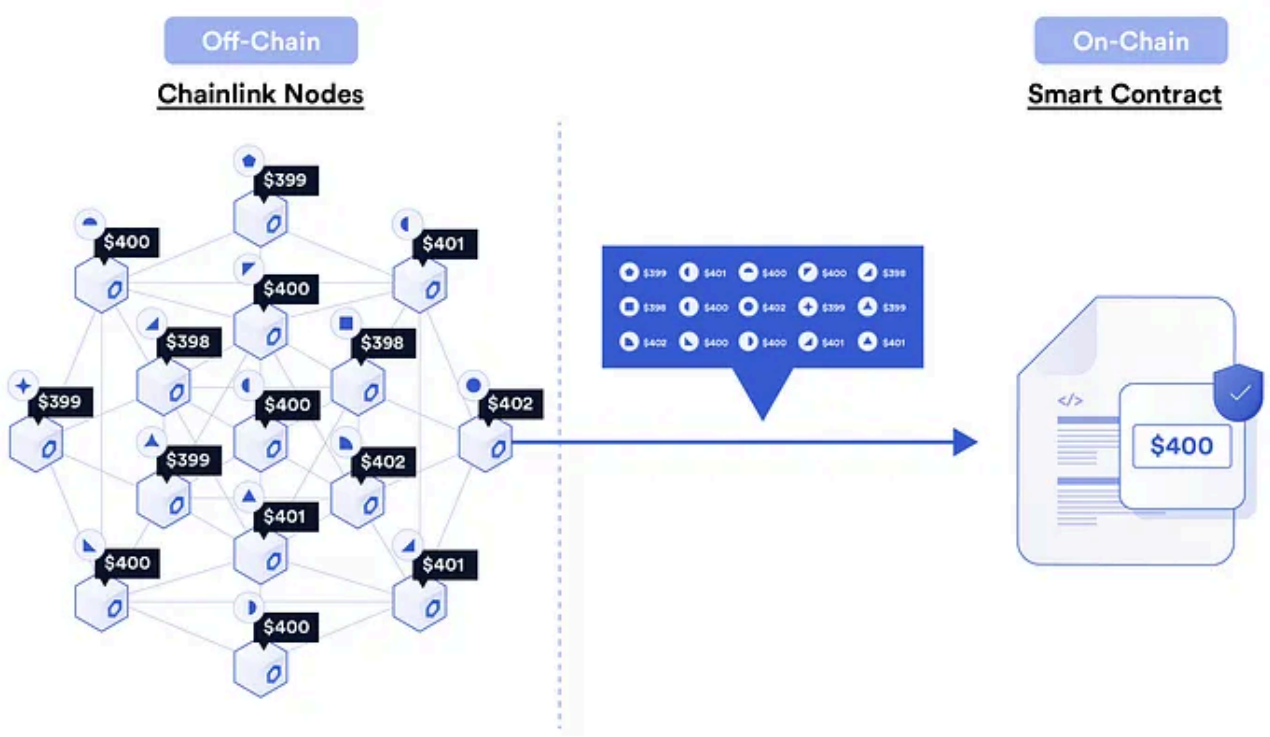


The Chainlink DECO technology uses zero-knowledge proofs to prove specific facts about a user's web session.

Scalability

To improve the performance of oracle networks, Chainlink created a scalability solution called "Off-Chain Reporting" (OCR) which increased data delivery throughput 10x by lowering the on-chain gas costs of updates by up to 90%. OCR provides these scalability gains by enabling Chainlink nodes to communicate directly with each other through a peer-to-peer network (LibP2P), allowing them to aggregate data off-chain at zero cost. This process involves each node individually fetching data from one or multiple APIs, signing it using their private key, and broadcasting the results to other nodes. Once a certain threshold of responses have been generated, a single transaction is created containing every node's cryptographically signed observation and is validated by an on-chain smart contract.

This order of magnitude improvement in scalability provided by OCR resulted in the increased decentralization of oracle networks, enabled higher frequency and lower latency updates, as well as allowed for the cost-efficient onboarding of more Chainlink nodes. OCR is currently being used in-production by Price Feeds across multiple blockchain networks.



Functionalities of the Chainlink Network

With the Chainlink Network offering a highly flexible framework that can generate a high degree of security, oracle networks built on Chainlink can provide a wide variety of services to smart contracts, leading to the creation of a much broader and more advanced set of digital agreements. Such Chainlink functionalities include:

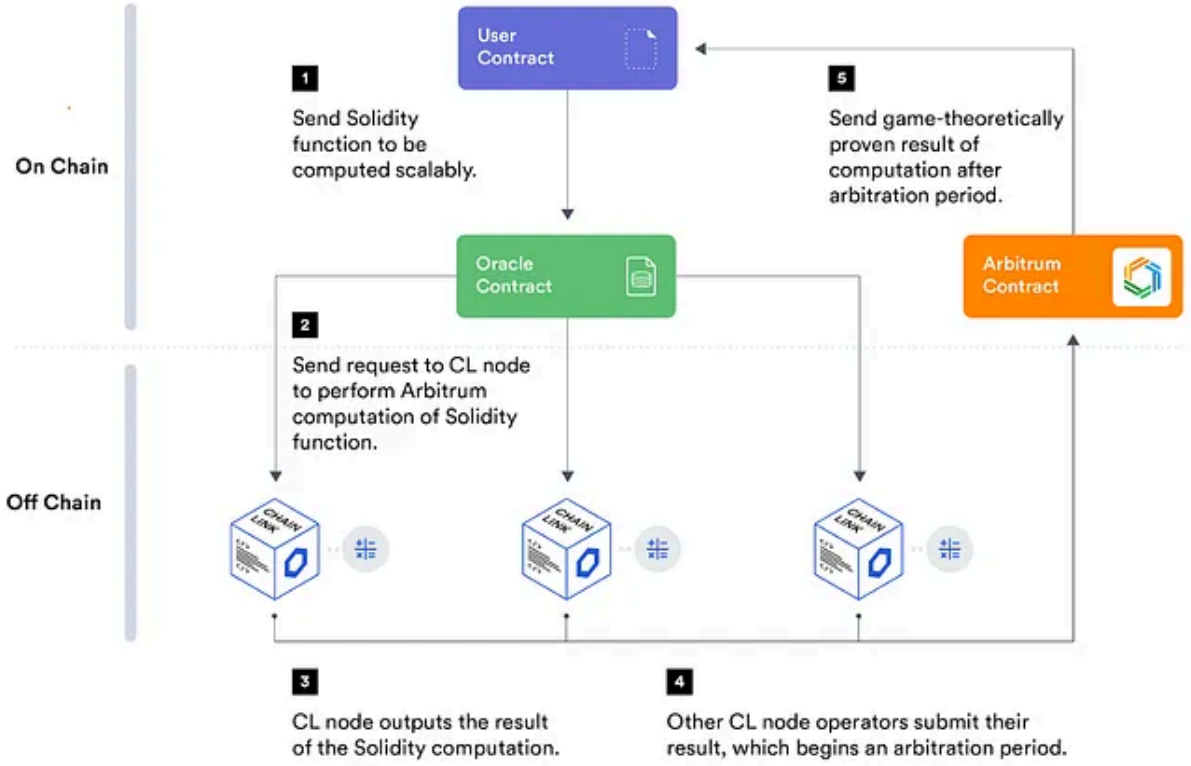
Data Sourcing and Delivery

The most widely recognized functionality of Chainlink oracles is fetching and delivering off-chain data to smart contract applications. Due to the blockchain oracle problem, smart contracts require external oracles to fetch data on their behalf. The data is then used to inform the smart contract about the current state of real-world events. For example, a smart contract may want to know the closing price of a barrel of oil, the amount of rainfall in New York City, the current location of a specific shipment in transit, the winner of the World Cup, or the current global price of Bitcoin. Chainlink oracles can fetch this data from any off-chain data provider (API) and deliver it to any blockchain network.

Chainlink powers the DeFi ecosystem by supplying key inputs and outputs

Off-chain Computation

In addition to data sourcing and delivery, Chainlink oracle networks can perform various types of off-chain computations, including the aggregation of multiple data sources into a single price point, generating a secure and fair source of randomness, operating layer-2 validators responsible for smart contract computation, running keeper functions to trigger smart contract maintenance and executions, and more. Off-chain oracle computation brings about more advanced and cost-efficient smart contracts, as expensive on-chain computations are offloaded off-chain to trust minimized oracle networks.

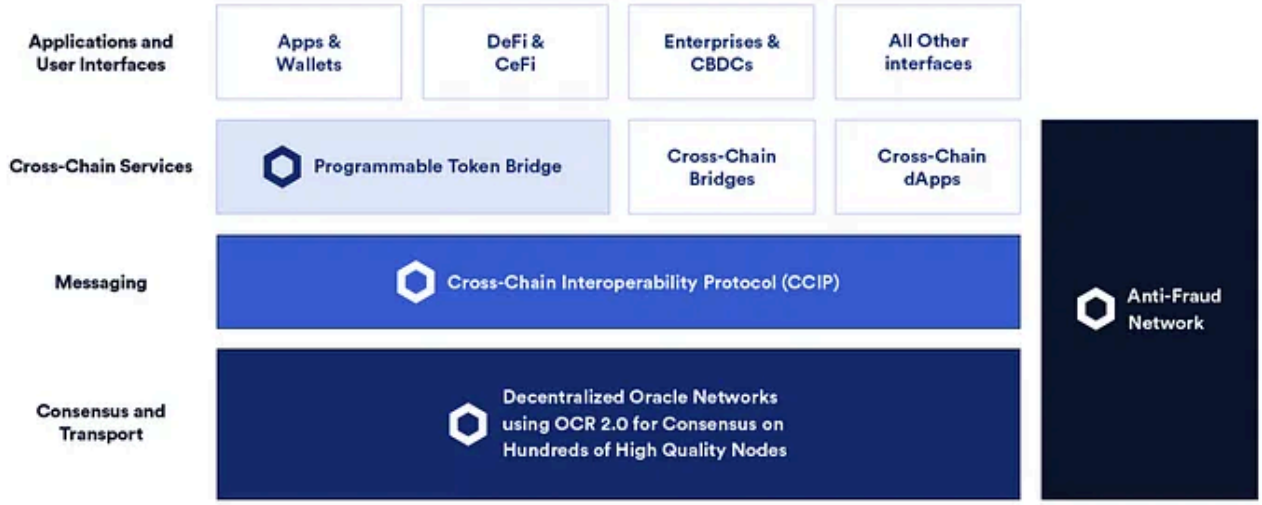


Chainlink nodes can act as validators on layer 2 Arbitrum Rollup chains.

Interoperability

The blockchain ecosystem is increasingly shifting towards a multi-chain world, where the adoption of smart contracts is not occurring on just one blockchain, but rather across many different networks with their own unique value propositions. With Chainlink oracles already integrated across a growing number of blockchains, the network is in an ideal position to serve as a universal interoperability solution to mitigate the problem of blockchain fragmentation and low quality cross-chain bridges.

The Cross-Chain Interoperability Protocol (CCIP) is an open-source standard being developed that leverages Chainlink infrastructure to establish a universal connection between hundreds of blockchain networks, both public and private, enabling the creation of secure token bridges and cross-chain applications. To further secure the services built on-top of CCIP is the Anti-Fraud Network, committees of nodes separate to those powering CCIP with the sole purpose of monitoring CCIP services for malicious activity that could lead to user loss. Ultimately, CCIP opens up a world of opportunity where developers can take advantage of multiple blockchain networks to create unified, truly cross-chain smart contract applications.

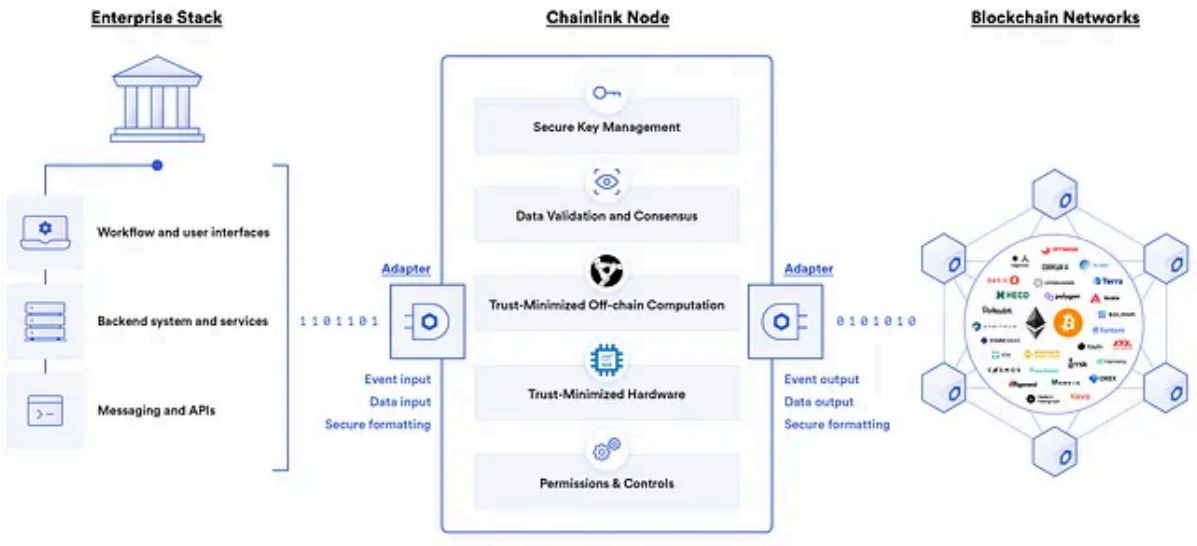


The architecture of the Cross-Chain Interoperability Protocol (CCIP)

Blockchain Abstraction Layer

Even with some consolidation over time, it's likely that various counterparties, industries, and entire geographic regions will be using a diverse set of blockchains that offer different trade-offs. As such, large enterprises or government entities dealing with globally distributed or even locally distributed counterparties will be expected to eventually operate on dozens or more blockchain environments simultaneously.

As a blockchain agnostic oracle network, the Chainlink Network provides a single integration gateway through which enterprises, institutions, and governments can get their existing systems 'blockchain-enabled' across all current and future blockchain networks. Instead of spending time and resources integrating with each network individually, they can use Chainlink as a secure middleware to connect to any blockchain, as well as write one set of documentation for how counterparties can interact with their systems from any blockchain via Chainlink. This concept of a blockchain abstraction layer was discussed in-depth in a co-written white paper between Chainlink Co-founder Sergey Nazarov and the World Economic Forum titled Bridging the Governance Gap: Interoperability for blockchain and legacy systems.

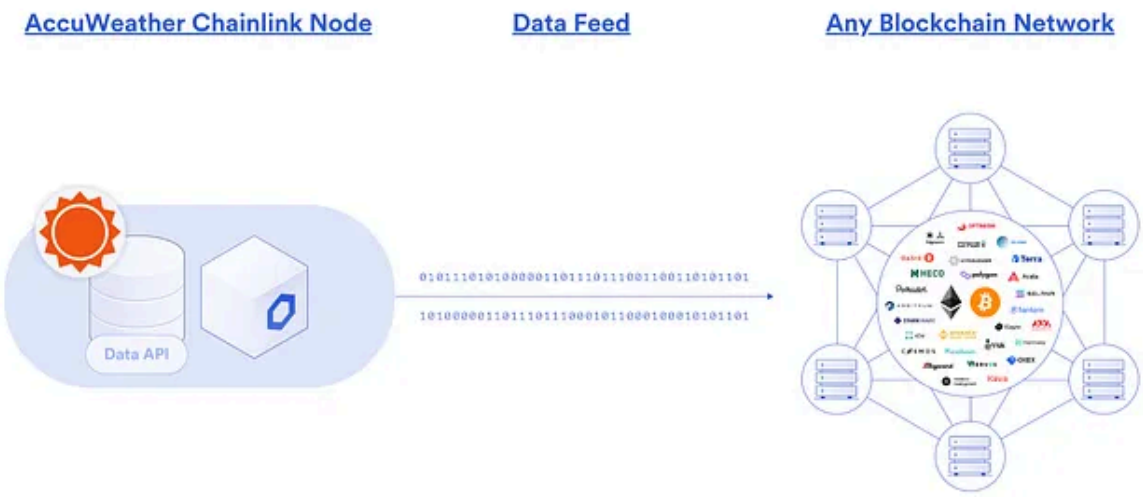


Similar to how enterprises use the internet to connect with a variety of partners, enterprises can use Chainlink to connect to any/all blockchains, as well as key external data/API providers, legacy systems, and traditional payments.

Sell Data and API Services

Using Chainlink as a blockchain abstraction layer, data/API service providers can quickly and easily expand their operations to blockchain markets. Whether selling their data through professional Chainlink node operators or running their own

Chainlink node, data/API service providers can expand their addressable market to emerging blockchain economies by making their entire suite of APIs blockchain-enabled. Additionally, they can bootstrap the security of their off-chain data by cryptographically signing it on-chain to prove its origin, as well as staking LINK collateral to ensure their data and services are high-quality. Numerous data providers are already running or planning to run a Chainlink node, including The Associated Press, AccuWeather, Kraken, Nomics, New Change FX, TheRundown, Tiingo, and dozens more.



AccuWeather is an example of a data provider bringing weather data on-chain by launching a Chainlink node; (source).

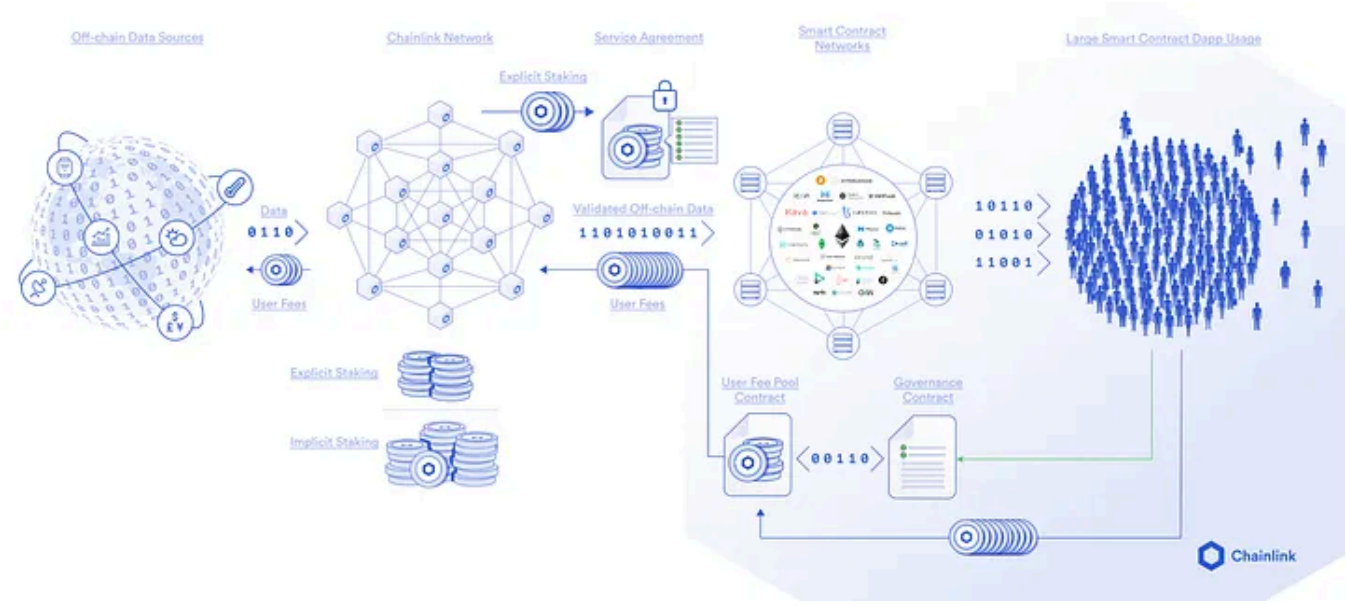
The Purpose of the LINK Token

The native LINK token is used to secure and bootstrap the growth of the Chainlink Network, empowering the creation of highly secure and reliable oracle networks that are sustainable long into the future. It's very similar to how BTC and ETH are used on the Bitcoin and Ethereum blockchains to incentivize secure and reliable decentralized computation of transactions.

The LINK token has 3 core functionalities in the Chainlink Network: **1)** a utility token where users must pay Chainlink nodes in LINK for oracle services, **2)** an oracle reward mechanism similar to a block reward to support the early costs of oracle networks until they reach self-sustainability, and **3)** a form of crypto-economic security wherein nodes stake LINK as collateral (security deposit) to back the honest and reliable performance of their oracle services.

Since every Chainlink node is paid in the native LINK token, they have a strong incentive to maintain a secure and high-performing Chainlink Network in order to ensure that oracle jobs continue and increase. This represents a form of crypto-economic security known as implicit staking, where any malicious behavior by Chainlink nodes that causes significant user harm would cause the value of the LINK token to drop due to a decrease in the Chainlink Network's reputation. In turn, this would directly decrease the value of each node's current token holdings and the potential future revenue they may earn by performing jobs on the network. It's akin to Bitcoin miners not engaging in malicious activity in order to prevent the devaluation of their BTC holdings and revenue.

As a further demonstration of LINK's utility, Chainlink nodes can be required to lock up a specific amount of LINK tokens in a service agreement smart contract in order to be selected to perform a specific oracle job, referred to as explicit staking. This serves as an additional financial incentive for nodes to provide reliable and honest oracle services; otherwise, their staked LINK tokens can be taken (slashed) as a penalty for not upholding the pre-agreed upon terms of the oracle job (e.g., data wasn't delivered on-time, data or computation was incorrect).



A generalized architecture of how the LINK token functions in the Chainlink Network

Described in detail within section 9 of the Chainlink 2.0 Whitepaper, explicit staking within the Chainlink Network is designed to achieve a super-linear staking impact, where malicious actors are required to have a budget significantly higher than the combined deposits of all nodes within an oracle network. This is achieved through two-tier oracle networks, involving a high-efficiency and low-cost first-tier network

made up of nodes that stake LINK tokens and continuously generate new oracle reports. Additionally, there is a maximum-security second-tier network that is used to settle any disputes and determine when first-tier nodes see their staked LINK slashed. This design optimizes for efficiency during normal use and security during the pessimistic cases.

The second-tier network consists of the large and growing collection of protocols relying on Chainlink oracles for accurate oracle reports. Because the correct operation of these protocols depends upon accurate oracle reports, each second-tier participant is highly economically incentivized to correctly resolve disputes so as to not jeopardize the security, reputation, or usability of their application or harm the value of their application's native governance token. More information on the exact mechanisms of explicit staking, including the math behind the super-linear impact, can be found within this Chainlink blog post.

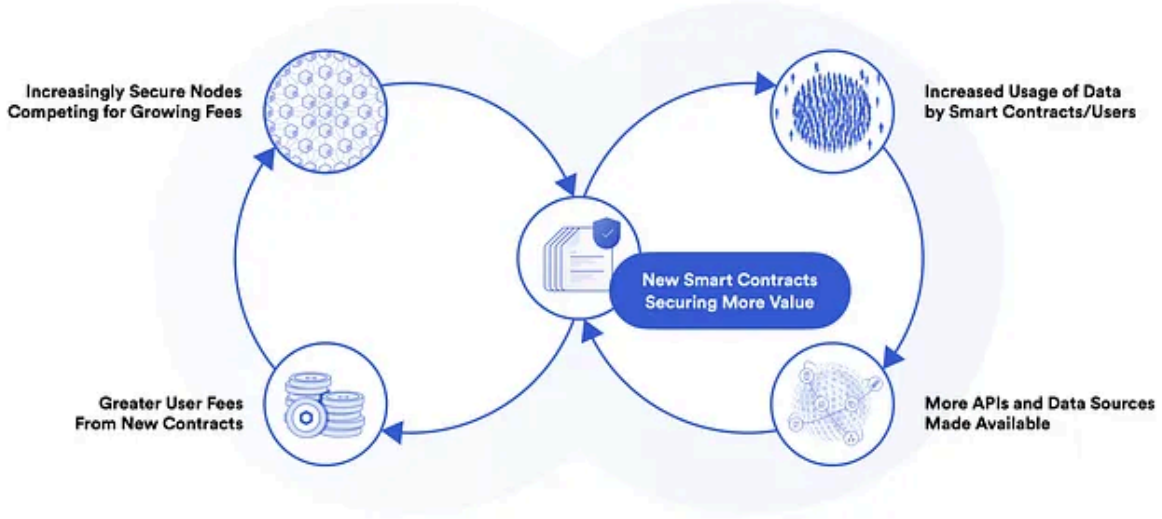
The threats of stake slashing, value reduction in current LINK token holdings, and loss of future revenue serve as both short-term and long-term financial punishments for undesirable network activity. This creates a skin-in-the-game approach to providing oracle services, as the LINK token is the sole means of making payments, creating economic security, and growing a node operator's business model (e.g., if a node has 100 LINK, then they can only provide 100 LINK worth of collateral at any given time. As such, they need to acquire more LINK to expand their node operations). Because the LINK token has a direct connection to the network and is necessary to take on more jobs and/or high-value jobs requiring stake, the long-term effectiveness of the token subsidy should further extend out if the network becomes increasingly adopted, providing even more runway to grow the network.

With effective use of the LINK network reward, Chainlink is creating secure and reliable oracle networks that service the current demand for off-chain data, as evidenced by many of the largest blockchain applications relying on Chainlink. The adoption of these networks is creating three complementary paths to self-sustainability, all of which are well underway today:

- Supporting the early launch of projects that go on to be major industry leaders, at which point they can easily fund the costs of the oracle networks they require.
- Having multiple projects collectively support a shared oracle network that provides data they all require. The more users that join a shared oracle network,

the less need there is for a subsidy. Eventually, no subsidy is required at all, and each new user from then on lowers the costs for all existing users

- Generating a large network effect wherein many of the world's largest data providers, institutions, blockchains, and smart applications collectively use Chainlink as the standard gateway between blockchains and traditional off-chain systems. Such a network effect leads to two positive feedback loops, which continually generate more data on-chain for smart contract developers and more user fees for node operators to compete for. The end result is an increasingly diverse set of smart applications that can secure increasingly higher value use cases.



The Chainlink Network effect is driven by two cycles: bringing more off-chain resources on-chain and making node operators increasingly more secure.

Additionally, exclusive LINK token utility within the Chainlink Network ties each node's own success directly to the quality of the overall network. It also ensures that node payments and staking are not tied to the security or reliability of any other network. Thus, the Chainlink Network is insulated against external failures from tokens and networks outside its control. As a blockchain agnostic network, Chainlink node operators only need to manage payments and staking in one currency (LINK), ultimately decreasing friction, lowering the barrier to running a node, and resulting in more network decentralization.

PART 3: THE CHAINLINK ECOSYSTEM

As the most widely used decentralized oracle protocol, the Chainlink ecosystem contains a vast array of products, users, and node operators. Chainlink is also a part of numerous enterprise working groups and supports a fast-growing team, an impressive list of advisors, and a flourishing community grant program.

Products and Services

Through these native capabilities, the Chainlink Network currently provides a wide range of oracle services to smart contracts operating across numerous different blockchains. While it's near impossible to generate a comprehensive list of all Chainlink use cases, these are the primary use cases that Chainlink is currently focused on providing:

Price Feeds

Chainlink Price Reference Data Feeds are a collection of oracle networks that provide financial market data on-chain regarding various in-demand exchange rates for cryptocurrencies, stablecoins, forex, commodities, and indices. These Price Feeds currently secure tens of billions of dollars worth of user funds for Decentralized Finance (DeFi) applications by pricing collateral, settling price predictions/derivatives contracts, calculating rewards, establishing staking amounts, setting exchange rates, and more.

Any API

Chainlink's highly generalized approach allows oracles to connect smart contracts to any off-chain API/data source, such as retrieving weather data or executing an off-chain payment. This includes free, open APIs, as well as paid, authenticated APIs that only nodes with passwords/credentials can access.

Randomness

The Chainlink Verifiable Random Function (VRF) provides smart contracts with a highly secure and verifiable source of randomness that cannot be manipulated by the oracle, developers, or end-users. This enables developers to create random in-game scenarios, fairly order ticket queues, and develop tamper-proof giveaways with associated proof that the winner was selected in a fair and unbiased manner.

Asset Collateralization

Chainlink Proof of Reserve (PoR) consists of on-chain data feeds that inform smart contracts about the current collateralization of on-chain assets backed by off-chain or cross-chain collateral such as stablecoins, tokenized assets, and more. This allows an application to prove that an on-chain asset is fully backed by the reserves it claims to have.

Data and Oracle Privacy

As stated earlier, Chainlink is currently developing multiple data and oracle privacy solutions, including DECO, Mixicles, and Town Crier, to unlock sensitive data for use in smart contracts without leaking it to the public and/or node operator.

Transaction ordering

The Chainlink Fair Sequencing Services (FSS) enables oracles to fairly order pending blockchain transactions based on different metrics like when they arrived in the mempool. Chainlink FSS is designed to prevent miner extractable value (MEV) such as through frontrunning, as well as lower transaction fees on blockchains like Ethereum.

Keepers

Chainlink Keepers enable the automation of on-chain transactions based on predefined conditions, such as triggering the liquidation of an under-collateralized loan, harvesting a vault on a time schedule, or settling an options contract at expiry using verifiable off-chain computation.

Layer-2 Validators

Chainlink oracles can provide validation services for layer-2 blockchain scaling solutions such as Off-Chain Lab's Arbitrum Rollups, which involves performing off-chain Solidity computation via the creation of transaction batches and the submission of fraud proofs to secure user funds.

Decentralized Identity

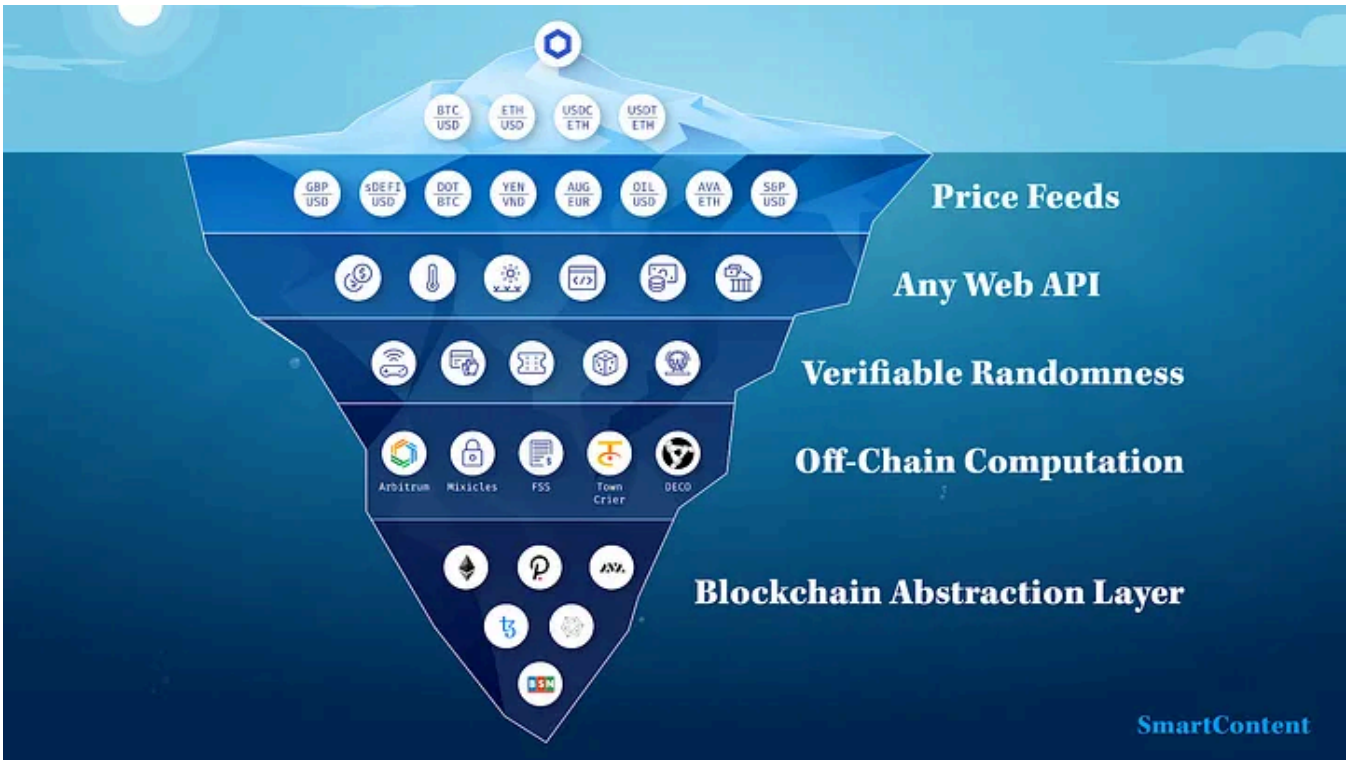
Chainlink oracles can power the creation of decentralized identity protocols such as IC3's CanDID. By leveraging DECO and/or Town Crier, users can securely import their credentials from existing web services like social media platforms, online bank accounts, or email accounts in a privacy-preserving and backward-compatible manner.

Cross-Chain Communication

Chainlink oracles are able to relay data from any blockchain network onto any other blockchain environment, including between base layer blockchains (public and private), layer-2 networks, or any combination of the two through the previously mentioned Cross-Chain Interoperability Protocol (CCIP).

While commonly recognized as being a price feed solution, Chainlink goes far beyond price feeds and data delivery to encompass a wide range of off-chain services conducted on behalf of smart contracts (potentially on behalf off-chain

systems as well in the future). We have only scratched the surface of the Chainlink Network and its functionality, as there will be many future use cases that we simply cannot imagine today, just as someone in 1994 could not possibly imagine all of the future use cases of the Internet.



Price Feeds are only the tip of the iceberg in regards to the oracle services Chainlink provides

Chainlink Users

Through these various oracle services, the Chainlink ecosystem has hundreds of in-production and in-development integrations, along with membership in numerous enterprise working groups, recognition from some of the world's most identifiable organizations, support from an expanding group of Chainlink-specific companies, and the launch of a fast-growing Chainlink Grant Program.

Within the smart contract industry, Chainlink powers a vast number of Decentralized Finance (DeFi) protocols, insurance products, on-chain gaming applications, and more. For a full list of use cases, refer to the blog post 77+ Smart Contract Uses Cases Enabled by Chainlink, however, we will summarize some below, along with a sample of some of the current users:

Lending and Borrowing

Chainlink enables lending and borrowing applications to exist by providing price feeds for calculating the value of collateral, ensuring loans are issued and liquidated according to fair market prices.

- **Aave**: Multi-chain money market protocol for borrowing and lending a multitude of on-chain tokens.
- **Compound**: Ethereum-based money market protocol that connects lenders and borrowers of on-chain tokens.
- **Sushiswap Kashi**: Lending and margin trading solution built upon the BentoBox contract design.
- **Venus**: Binance Smart Chain-based algorithmic money market for lending and borrowing.

Stablecoins

Chainlink Price Feeds enable the creation of decentralized and algorithmic stablecoins backed by on-chain cryptocurrency by determining the valuation of the collateral backed to help ensure the peg is maintained.

- **Liquity**: Interest-free lending platform that enables the minting of the LUSD stablecoin backed by ETH collateral.
- **Fei Protocol**: A decentralized and scalable, reserve-backed, stablecoin aimed at achieving governance-minimized central banking.

Derivatives and Synthetic Assets

Chainlink empowers derivatives markets and synthetic assets by supplying the current price of assets at the time of trades or settlement.

- **Synthetix**: Largest derivatives platform for zero slippage trading of synthetic assets.
- **Alchemix**: Future-yield backed synthetic asset platform and community DAO featuring self-paying loans.
- **Thales**: A permissionless, non-custodial, and uncensorable binary options trading protocol.
- **Lyra**: A options trading platform on the scalable layer 2 Optimism network.
- **MCDEX**: Perpetual derivatives platform using automated market makers and order books.
- **Jarvis Network**: Synthetic asset protocol which leverages the liquidity of existing cryptocurrencies like USDC.

- **Opyn**: A capital efficient options protocol with automated settlement at expiry.

Exchange and Trading

Chainlink provides price feeds to settle trades, determine the value of liquidity mining collateral, set market-making strategies, and secure the value of collateralized off-chain computation.

- **dYdX**: A layer 2 decentralized exchange for spot trading and perpetual contracts.
- **Loopring**: Layer-2 decentralized exchange providing high throughput, low-fee trading.
- **DODO**: Proactive automated market maker that mimics human market-making behaviors.

Insurance

Chainlink facilitates parametric insurance applications by informing the policy about insured events at the time of settlement, allowing it to determine the correct payouts and/or rebalance insurance funds.

- **Arbol**: Parametric crop insurance for farmers based on weather conditions.
- **Etherisc**: Parametric insurance for real-world events such as flight delays.
- **Nexus Mutual**: Decentralized discretionary mutual as an alternative to insurance.

Pegged Assets

Chainlink supports pegged assets by checking if their off-chain reserves match their on-chain token balances, as well as triggering reserve rebalancing if the peg is lost.

- **Paxos**: Brokerage and custody platform that provides tokenized real world assets such as US dollars and gold.
- **TrustToken**: Blockchain-agnostic stablecoin backed by USD held in reserves.
- **Wrapped BTC**: Tokenized Bitcoin on the Ethereum blockchain custodied by BitGo.
- **DefiDollar**: Meta-stablecoin backed by centralized and decentralized stablecoins.

Real-World Assets

Chainlink is used to bring real-world assets on-chain by providing data regarding the current valuations of the off-chain assets they represent.

- **RealT**: Tokenized real estate allowing users to buy fractions of a property's cash flows.
- **CrescoFin**: Tokenized invoice protocol providing interest-yielding insured deposited products.

Payments

Chainlink enables the usage of cryptocurrency on commence networks by providing a exchange to exchange tokens into fiat at the market-wide price.

- **Flexa**: Cryptocurrency payment platform for merchants to accept instant, guaranteed crypto payments while receiving the currency of their choice.
- **Crypto.com**: Crypto mobile app where users can pay merchants using tokens via a Visa debit card.

Rebase Tokens

Chainlink functions in rebasing tokens by triggering rebases based on a particular price or data feed update.

- **Ampleforth**: Algorithmic rebase token pegged to the inflation-adjusted dollar.
- **Base protocol**: Algorithmic rebase token pegged to the total crypto market capitalization.

Asset Management

Chainlink is used within asset management protocols to trigger the automatic rebalancing of on-chain portfolios using various indicators and/or to determine the current gas price before triggering a transaction.

- **Set Protocol**: Non-custodial asset management protocol for social trading and indices.
- **Tornado Cash**: Privacy mixer for sending confidential on-chain transactions.

On-chain collectibles and NFTs

Chainlink VRF is relied on to access a provably fair source of on-chain randomness, which is used to generate unique NFT traits and issue random rewards to users.

- **Bored Ape Yacht Club**: A collection of 10,000 unique Bored Ape NFTs on the Ethereum blockchain.
- **EtherCards**: NFT gamification and monetization platform that helps artists maximize the value of their art.
- **Axie Infinity**: Pokémon-inspired universe where users breed and battle Axies.
- **Aavegotchi**: DeFi-powered crypto-collectibles backed by interest-generating tokens.
- **Parallel**: A Sci-Fi digital collectible card game being built on the Ethereum blockchain
- **Ether Legends**: Physical and digital collectible trading card game with PvP and PvE.
- **Wildcards**: Non-fungible tokens representing a unique animal from a conservation org.
- **Illuvium**: A community governed AAA blockchain-based video game with collectable NFTs.

Betting platforms

Chainlink supplies randomness and data about off-chain events to determine lottery winners and settle bets.

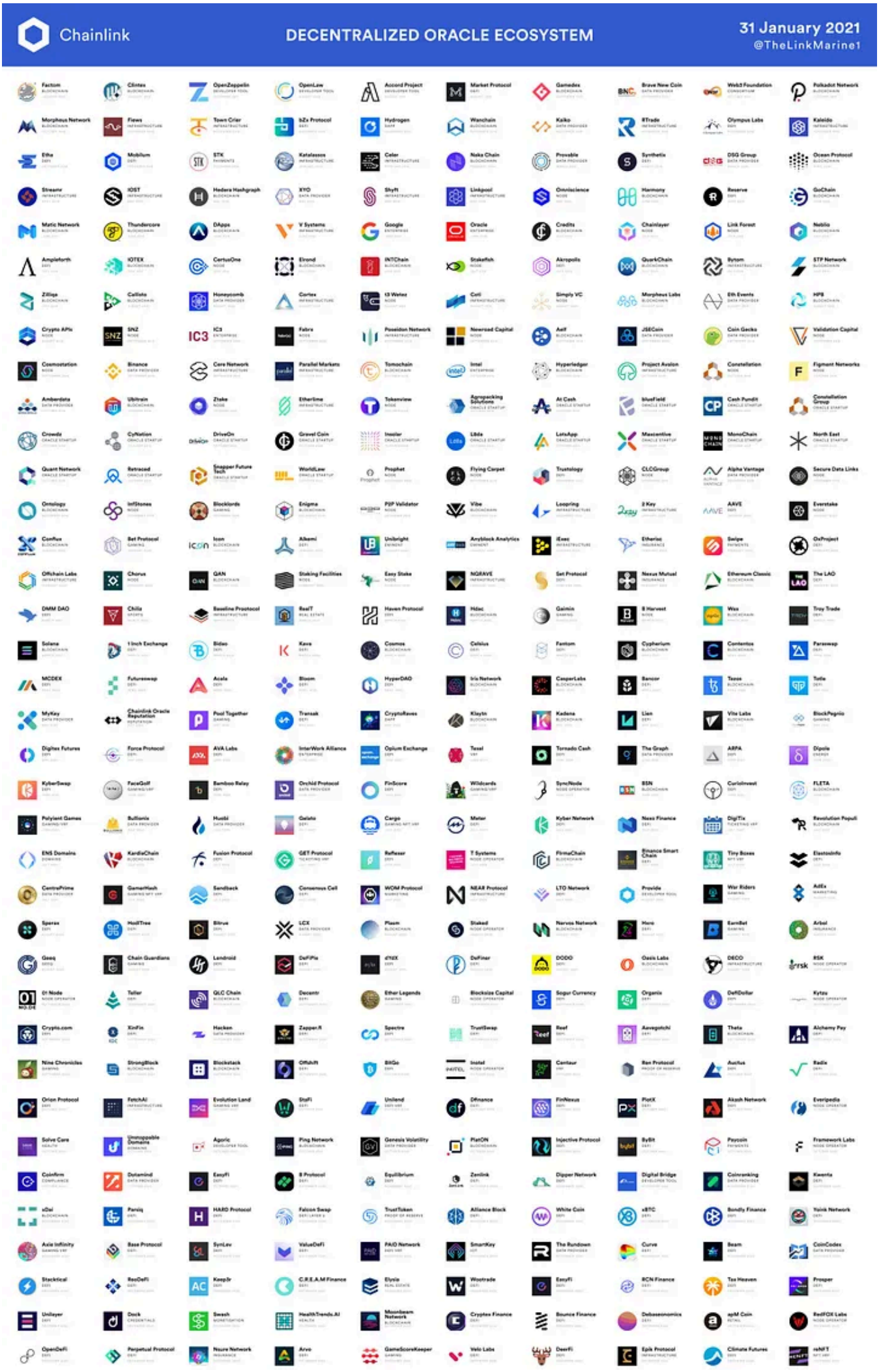
- **PoolTogether**: No-loss savings game for users to win prizes without risking deposits.
- **EarnBet**: Provably fair gaming platform operating in the WAX blockchain ecosystem.
- **Bet Protocol**: Esports and sports betting platform.

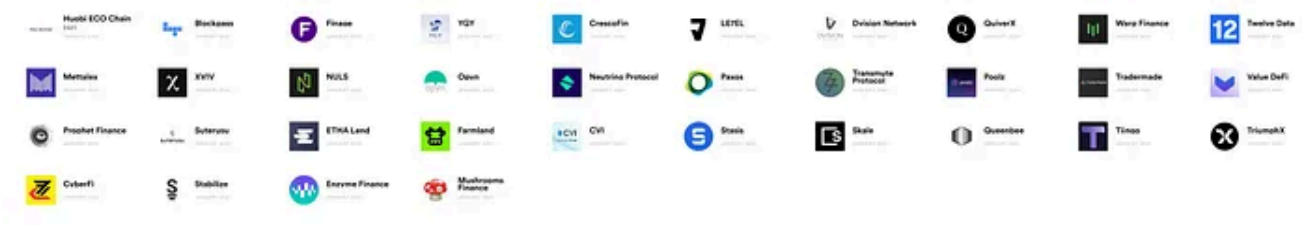
On-chain gaming

Chainlink VRF is key to generating random in-game scenarios and prizes in a manner which no one can manipulate or predict.

- **Blocklords**: Blockchain-based medieval grand strategy game on layer 2
- **Planetarium**: Ecosystem for community-powered online games via Libplanet network

- **Evolution Land:** Ecological cross-chain game application of the Darwinia Network
- **War Riders:** MMO game based on customizing war vehicles and battling opponents


Chainlink
DECENTRALIZED ORACLE ECOSYSTEM
31 January 2021
@TheLinkMarine1



The Chainlink ecosystem consists of hundreds of in-production and in-progress integrations; (source).

Enterprises, Working Groups, and Recognitions

In addition to integrations with smart contract applications across numerous use case verticals, Chainlink works with a number of enterprises on their blockchain strategy and participates in a variety of enterprise working groups around the world to help standardize how businesses securely leverage blockchain oracles within their smart contract powered digital agreements. Chainlink has also received multiple recognitions from well-known institutions and works with leading academics and consortiums. Some of which include:

Recognitions

- World Economic Forum: Public-Private consortium that co-authored a report with Chainlink Co-founder Sergey Nazarov on how oracles provide interoperability between blockchain networks and legacy systems, as well as recognizing Chainlink as a Technology Pioneer.

- Gartner: A global research and advisory firm that recognized SmartContract.com in 2017 as a leading blockchain project, and in 2019 discussed how Chainlink is key to Google's blockchain strategy.

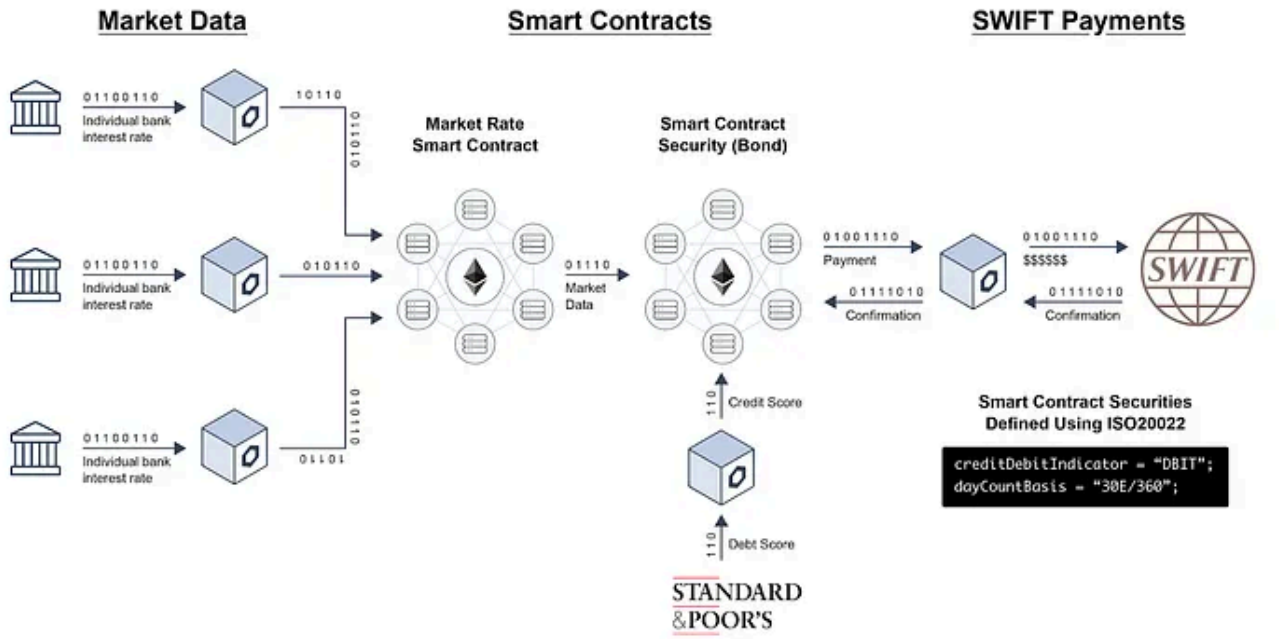
Enterprises

- Google: One of the world's largest tech companies collaborated with Chainlink to bring Big Query data and NOAA weather data onto the Ethereum blockchain via Chainlink oracles.

- Amazon Web Services: The world's largest cloud computing platform collaborated with Chainlink Labs to launch the AWS Chainlink Quickstart, a one-click workflow to deploy a security-hardened Chainlink oracle node on AWS across multiple blockchain networks.

- Deutsche Telekom T-Systems: A subsidy of Europe's largest telecommunications provider launched a Chainlink oracle node to feed real-world financial market data to smart contract applications, supporting and monetizing the growth of the DeFi ecosystem.

- **Swisscom**: The largest telecommunications provider in Switzerland (51% ownership by the Swiss government) joined the Chainlink network as a node operator to power DeFi applications with aggregated financial market data.
- **Oracle**: The world's largest database company collaborated with Chainlink to create a 'virtuous cycle of innovation' by launching Chainlink nodes for numerous API startups running on Oracle's Cloud Infrastructure.
- **SWIFT**: The global standard in interbank messaging, consisting of a consortium of the world's largest banks, collaborated to create a Smart Contract Securities Proof-of-Concept in which the interest rates of top banks were aggregated and then used by a smart contract to trigger a bond interest payment made on the SWIFT network using its ISO20022 messaging format.



SWIFT Proof of Concept showing how Chainlink enables the creation of smart security bonds

Enterprise and Academic Research Working Groups

- **Baseline Protocol**: Privacy-preserving framework for using the Ethereum Mainnet as a common frame of reference between enterprise backend systems.
- **InterWork Alliance**: Platform-neutral, non-profit organization dedicated to creating the standards frameworks needed to increase innovation across token-enabled ecosystems.
- **Hyperledger Avalon**: Collaboration between Hyperledger, EEA, and cloud service provider ecosystems to standardize attested off-chain computations for

smart contracts.

- **Blockchain Service Network (BSN)**: Chinese government-supported initiative to provide businesses access to low-cost blockchain cloud computing services and tooling.
- **Enterprise Ethereum Alliance**: The Ethereum Mainnet Integration for Enterprises taskforce provides specifications to integrate the Ethereum Mainnet with ERP, CRM, and other corporate systems of record.
- **The Initiative for Cryptocurrencies and Contracts (IC3)** — a leading academic research organization working with industry academics and business leaders to achieve mainstream adoption of cryptocurrencies and smart contracts.

A list of IC3 Partners, including Chainlink; (source).

Chainlink-Specific Companies

Outside of users and enterprise initiatives, several companies have sprouted up based solely around providing services specifically for the Chainlink Network, such as:

Chainlink Market

Created by LinkPool, market.link is an open and permissionless marketplace where Chainlink node operators can list their oracle services, data source connections,

credentials, security reviews, and on-chain performance in order for developers to review and use to construct their own oracle network consisting of nodes they deem trustworthy.

Chainlink Oracle Reputation (COR)

Created by Secure Data Links, reputation.link is a data analytics dashboard that displays the historical performance, uptime, revenue, and on-chain derived statistics of individual Chainlink node operators, data provider APIs, and the Chainlink Network as a whole.

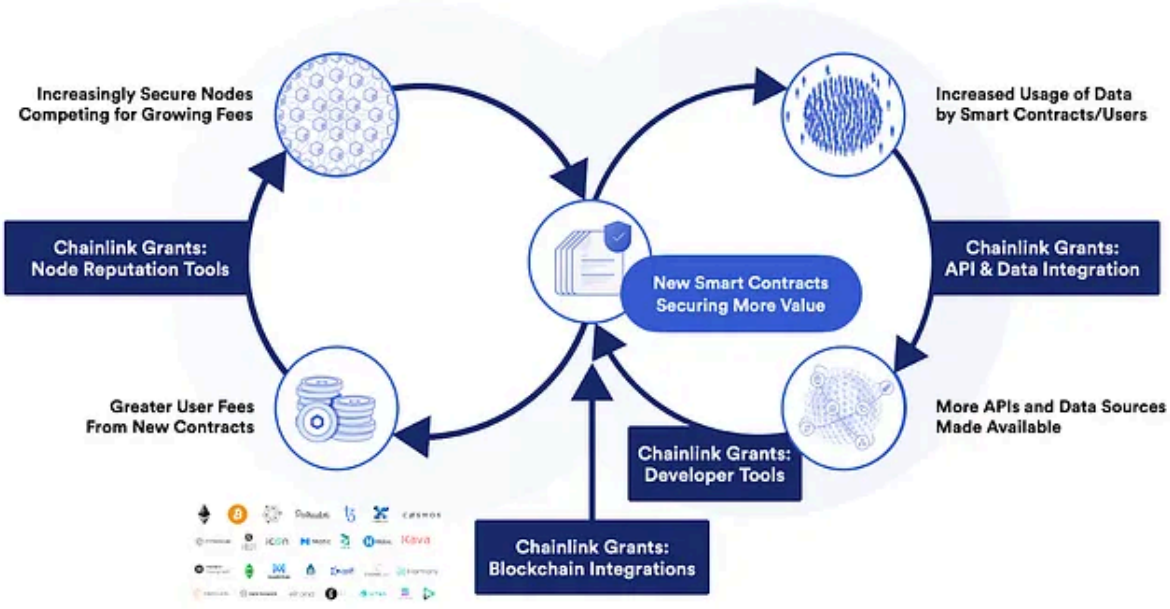
Node Operators

The Chainlink Network consists of a diverse range of node operators, including large telecommunications service providers such as Deutsche Telekom subsidiary T-Systems and Swisscom, experienced blockchain infrastructure providers like Stake.fish and Staked, as well as traditional data providers like Kaiko, Huobi, CryptoAPIs, and many more.

Chainlink Grant Program

The Chainlink Community Grants Program provides financial support for development teams and researchers who are building core infrastructure and tooling for the Chainlink Network. By accelerating virtuous cycles of growth around placing more data on-chain and increasing the security guarantees available to users, the grants program fuels the growth of the Chainlink ecosystem as a whole. Grants are currently given out around four main categories: **1)** integrating Chainlink on a new blockchain, **2)** improving Chainlink node and developer infrastructure, **3)** funding original, cutting edge oracle-related research, or **4)** supporting community initiatives.

By applying Grants to key areas of need, Chainlink is further accelerating its two positive feedback loops designed to increase Chainlink Network security and making more off-chain resources available on-chain. The culmination is developers being able to create more types of smart contracts across more blockchains that can be relied on to secure increasingly more value.



The Chainlink Grant Program is accelerating both the data and node security cycles, enriching smart contract economies across all blockchains.

Team and Advisors

The Chainlink co-founders have been studying and building externally-connected smart contracts and blockchain oracle technology since at least 2014 when their first company SmartContract.com launched (before Ethereum went live). The team has extensive experience, having worked directly with top enterprises and blockchain developers needing oracles for many years, as well as producing several original research developments like Town Crier, Threshold Signatures, Mixicles, and more. In fact, the first Chainlink whitepaper was one of the first academic research papers on decentralized oracles, essentially pioneering the industry.

Team

The 300+ person development team working on Chainlink features seasoned experts in blockchains, oracles, cryptography, machine learning, artificial intelligence, and business development.

Co-Founder Sergey Nazarov

- Started building smart contracts pre-Ethereum in 2014
- Built the first widely used interface for DEXes
- Built the first blockchain-based email service
- Built the first centralized oracle service

- Last but not least, built the first decentralized oracle network.

Chief Scientist Ari Juels

- Professor of Computer Science at the Jacobs Institute at Cornell Tech
- Former chief scientist of world-renowned cybersecurity company RSA
- Formalized Proof of Work consensus in 1999 (powers Bitcoin and Ethereum)
- Created Proof of Retrievability in 2014 (powers FileCoin and Sia)
- Co-author of the Chainlink whitepaper in 2017 and only works with Chainlink within the blockchain industry
- Co-author of the Chainlink Mixicles whitepaper in 2019
- Co-author of the CanDID whitepaper in 2020 in collaboration with J.P. Morgan
- Co-author of the Chainlink 2.0 whitepaper in 2021
- Co-founder of The Initiative For CryptoCurrencies & Contracts (IC3)
- 36,000 total scholarly citations

Head of Engineering Ben Chan

- Previously CTO of Bitgo, where he built the industry-leading crypto custody solution.
- Architect of Wrapped BTC, the most widely used form of tokenized Bitcoin on Ethereum
- Now building scaling solutions for the Chainlink Network to lower user costs.

CTO Steve Ellis

- Worked previously as a software engineer and team lead at Pivotal Labs
- Built mission-critical systems responsible for securing sensitive HIPAA compliant data and scalable payments automation software
- Oversees countless engineers and integration specialists who aid in the development and deployment of Chainlink oracle networks

CMO Adelyn Zhou

- Lead companies that have been acquired by Amazon
- Expert in applied artificial intelligence
- Best selling Amazon author
- Graduated from Harvard Business School

Advisors

The Chainlink Network is also supported by a top tier list of accomplished academic and business advisors.

Jeff Weiner

- Chief Executive Officer (CEO) of LinkedIn for 12 years, the world's largest professional network
- Executive Chairman of LinkedIn
- Facilitated the $26B acquisition of LinkedIn by Microsoft
- Founding Partner at Next Play Ventures
- Advisory board member of Intuit and DonorsChoose

Tom Gonser

- Founder of DocuSign, the market-leading e-signature provider around the world and pioneer of the e-signature industry.
- Investment partner at Seven Peaks Ventures
- Joined as a business advisor to Chainlink in early 2019

Balaji Srinivasan

- Former Chief Technology Officer (CTO) at Coinbase, the largest cryptocurrency exchange in the United States
- Former General Partner of Andreessen Horowitz, where he helped the venture capital firm move into the blockchain industry

- Co-founder of Earn.com, which was acquired by Coinbase
- Co-founder and CTO of Counsyl and won a Wall Street Journal Innovation Award for Medicine
- Co-founder of Teleport, which was acquired by Topia
- Co-founder and Board Member of Coin Center, the leading non-profit focused on cryptocurrency policy issues
- Angel Investor

Evan Cheng

- Former Senior Manager at Apple
- Director of Engineering Blockchain at Facebook
- Co-creator of the LLVM, which generates the low-level machine code running every Apple device, as well as much of Google, Nvidia, and Intel

Andrew Miller

- Decentralized consensus researcher
- Associate Professor at the University of Illinois
- Associate Director of the Initiative for Cryptocurrencies and Contracts (IC3)
- Board member of the Zcash Foundation and Ethereum Enterprise Alliance
- Advisor to both Zcash and Tezos

Lynda Smith

- Former Chief Marketing Officer (CMO) of Twilio, helping build it into the world's leading cloud communications platform
- Faculty member of Stanford University
- Lead marketing initiatives at top technology firms including Nuance and Genpact

Roberta Carraro

- Vice President of Design at HashiCorp, a leader in infrastructure automation software
- Experience designing developer products in cloud-based software companies including Salesforce and Heroku.

Hudson Jameson

- Former Developer Liaison, DevOps Engineer, and Security Engineer at the Ethereum Foundation
- Member of the Ethereum Cat Herders, a decentralized group that supports Ethereum through project management and consensus gathering.

Research Team

Chainlink is also supported by a full-time research team focused on developing the Chainlink Network so it can service all current and future market demand (pictured below).

Research team

Lorenz Breidenbach

Lorenz Breidenbach is a security researcher and former BRIDGE fellow from ETH Zürich and IC3. He previously conducted research at Cornell Tech and spent time in industry at Google and Open Systems.

Ari Juels

Ari Juels is the Weill Family Foundation and Joan and Sanford I. Weill Professor in the Jacobs Technion-Cornell Institute at Cornell Tech and a Computer Science faculty member at Cornell University. He is a Co-Director of the Initiative for CryptoCurrencies and Contracts (IC3). He was previously Chief Scientist of RSA.

Alex Coventry

Alex Coventry is working on improvements to Chainlink's reporting protocol which will allow orders-of-magnitude reductions in the costs of running smart contracts that faithfully respond to real-world outcomes. He has a PhD in Applied Mathematics from MIT, and has been following cryptocurrency since the Bitcoin whitepaper came out in 2009.

Andrew Miller

Andrew Miller is an Assistant Professor at the University of Illinois, Urbana-Champaign, where he leads the Decentralized Systems lab and carries out research in applied cryptography, smart contract programming languages, and other topics in blockchains and computer security.

Christian Cachin

Christian Cachin is a professor of computer science at the University of Bern, where he has led the Cryptology and Data Security Research Group since 2019. He worked for IBM Research for more than 20 years. He is an ACM Fellow, IEEE Fellow, recipient of multiple IBM Outstanding Technical Achievement Awards, and has also served as the President of the International Association for Cryptologic Research (IACR) from 2014-2019.

Dan Moroz

Daniel Moroz is a PhD candidate in Computer Science at Harvard University where he works on algorithmic game theory in cryptocurrency systems and helped found Harvard's first cryptocurrency research group. He is affiliated with the MIT Digital Currency Initiative and previously worked at Google and in quantitative trading.

Fan Zhang

Fan Zhang is a researcher working on blockchains, trusted hardware and applied cryptography. He created Town Crier and DECO as part of his PhD at Cornell. He is an incoming Assistant Professor at Duke University.

Farinaz Koushanfar

Farinaz Koushanfar is the Henry Booker Scholar Professor of Electrical and Computer Engineering at the University of California San Diego, where she is the founding Co-director of UCSD MICS (Center for Machine Intelligence, Computing, and Security). Her research is focused on automated holistic cross-layer co-design and optimization of Learning Algorithms, Security, and Privacy-Preserving Computing / Secure Multi-Party Computation.

Florian Tramèr

Florian Tramèr is a PhD student at Stanford University advised by Prof. Dan Boneh. His research interests are in the security of cryptocurrencies and cryptocommodities. He co-invented GasToken, and discovered and disclosed the first side-channel attacks on Zcash and Monero's anonymous transactions.

If you are a researcher and you want to collaborate with us, contact us here.

Kostis Karantias

Kostis Karantias is a software engineer and researcher in the cryptocurrency space with a Masters of Engineering in Computer Science from the University of Ioannina. He previously conducted research and development on cross-chain interoperability, light clients, and innovative consensus algorithms. Before working on blockchains, he worked at Bloomberg as a Software Engineer.

The Chainlink Research Team consists of numerous leading academics; (source).

These are just some of the many other highly experienced and knowledgeable engineers, business leaders, and academics that make up the Chainlink Ecosystem. Chainlink is rapidly expanding too, with numerous job openings for integration engineers and software developers, further evidence of the growing demand for Chainlink.

Smart Contract Summit

In order to support its community and thriving ecosystem, Chainlink launched the Smart Contract Summit (SmartCon) as an annual event designed to bring together DeFi developers, enterprises, dApp builders, node operators, researchers, and more focused on smart contracts. Through keynote speeches, panel discussions, live demos, developer workshops, and community networking, participants explored and shared their cutting-edge research and current thinking about the future of decentralized technology.

SmartCon #0 (2020)

As the largest DeFi conference of 2020, SmartCon #0 featured 8,000+ attendees, including those from 100+ countries and all 7 continents, as well as 130 speakers from leading blockchain protocols, DeFi applications, and beyond. Some highlights during this conference include:

- Ari Juels joined Chainlink Labs as Chief Scientist to lead the new Chainlink Labs Global Research Program.
- Chainlink Labs acquired DECO from Cornell University enabling privacy-preserving blockchain oracles.
- A panel discussion with DeFi leaders including Sergey Nazarov (Chainlink), Andre Cronje (Yearn.finance), Stani Kulechov (Aave), and Kain Warwick (Synthetix).
- OpenLaw developed a Microsoft Office extension to enable the usage of smart contracts within Microsoft Word documents.
- Off-Chain Labs explored how the launch of Arbitrum layer 2 technology will enable highly scalable smart contracts with orders of magnitude more transactional throughput.

SmartCon #1 (2021)

As a follow up conference, SmartCon #1 featured 15,000+ attendees from 140+ countries that listened in to hear from 200+ industry leading founders, researchers,

and developers. Some key highlights include:

- Announcement of the Cross-Chain Interoperability Protocol (CCIP), an open-source standard for cross-chain messaging and token movements.
- The mainnet launch of Chainlink Keepers, giving developers a highly secure and reliable way to automate smart contracts.
- Allen Day from Google Cloud collaborated with Chainlink to enable smart contracts to query NOAA weather datasets on Google BigQuery.
- Amazon Web Services (AWS) Partner Network collaborated with Chainlink Labs on the AWS Chainlink Quickstart.
- Swisscom, the leading telecommunications firm in Switzerland, began running a Chainlink node to further decentralize Chainlink Data Feeds.
- exMachina and GoodDollar discussed how blockchain technology and Chainlink decentralized oracles can solve critical problems in climate change
- Celsius Network began using Chainlink Price Feeds to determine the borrowing rates for its platform and announced its intention to use CCIP.
- Balaji Srinivasan announced a collaboration with Chainlink on funding the creation of a censorship-resistant inflation dashboard.

***Continued Improvements

While not the scope of this article, it should be noted that blockchains, smart contracts, and oracles are not yet complete components. Blockchains still need to strike the right balance between security and throughput, as well as provide better ways to obtain transaction privacy. Smart contracts need to mature their code base and expand their functionality through continued development and auditing. Finally, certain oracle features like privacy are still under development, particularly being pioneered by Chainlink.

Fortunately, many key developments are already underway, including layer-2 Rollups and base layer sharding for blockchain scaling, zero-knowledge proofs for transaction privacy, blockchains built specifically for high-throughput, formal verification of smart contract code, standardization of developer tooling, and more. Specifically, when it comes to oracles, Chainlink is providing an all-encompassing suite of generalized oracle solutions to satisfy any oracle need, including several

novel features for network scaling (OCR), data privacy (DECO), and crypto-economic incentives (Staking).

CONCLUSION: USING TECHNOLOGY TO BUILD A BETTER TOMORROW

Putting it all together, the Chainlink Network has many unparalleled qualities that make it primed to become an industry standard as the most widely used oracle network relied on by a variety of applications from all blockchains to get any off-chain resource. Some of the core qualities that allow it to achieve such a feat include: a flexible architecture to support an infinite number of customized oracle networks running in parallel without cross-dependencies, a multitude of security techniques to ensure secure and reliable oracle networks across any use case, market-leading adoption within numerous markets and blockchains, strong token economics to bootstrap the network until self-sustainability and ensure network security, and a world-renowned research and development team building cutting edge oracle technology and in-demand oracle solutions.

These features allow the Chainlink Network to help blockchains and smart contracts take the next major leap forward in reaching their true potential, particularly through connecting them directly with real-world data and legacy systems that currently power the world today. In many ways, Chainlink's effect on blockchains is very similar to computers being completely transformed upon the arrival of the Internet. Chainlink is poised to be that single standard Internet-equivalent for connecting smart contracts to the outside world and already has a large network effect taking root as many of the largest blockchains, top smart-contract applications, and best data/API service providers are choosing Chainlink as their oracle solution.

Having a universal connection layer will be critical to adding the final piece to the God Protocols, allowing blockchain-based smart contracts to exchange value using any input and output needed, along with security techniques to ensure that those inputs and outputs operate without bias, inaccuracies, or privacy concerns. While there is much work to do, it's fairly clear that blockchains (the body), smart contracts (the brain), and oracles (the senses) will form the foundation of a trustless third-party computing network that powers the world's next-generation of digital agreements.

The only component left then is the soul. Like any technology, the God Protocols are what we as human beings make them to be. Tools are simply that, tools, and it's up

to us to use these tools to make the world a more fair, equitable, and transparent place for conducting business and honoring contracts. It is the people who create the applications and send the commands to the God Protocols; thus, our ethics, commitment, and higher purpose must guide us in our efforts to apply blockchain-based smart contract and decentralized oracles to achieve the maximum social effect: users receive the outputs they deserve based on the true amount of input they put forward.

"*The end of science is not to prove a theory, but to improve mankind." — — Manly P. Hall*

List of Additional Resources

If you want to learn more, we encourage readers to explore the following introductory articles on blockchains, smart contracts, data & APIs, the oracle problem, Chainlink node operators, and 77+ Smart Contract Uses Cases Enabled by Chainlink.

If you already understand the basics, then go deeper with some of our past articles such as:

- Chainlink's Network Effect Creates More Secure and Lower Cost Oracles for Everyone
- Chainlink: Low-Level Infrastructure for Inter-Oracle Competition
- Chainlink: Beyond Price Feeds and Data Delivery
- How Chainlink Generates Definitive Truth About the Off-Chain World: Opening Up Multi-Trillion Dollar Markets For Smart Contracts
- Connect To All Blockchain Environments Through A Single Chainlink Integration

Follow us on Twitter @SmartContent777 to get up to date on the latest articles, as well as follow our individual accounts @Crypto___Oracle and @ChainLinkGod for a constant stream of information about the Chainlink, DeFi, and the blockchain space.

Chainlink | Smart Contracts | Blockchain | Oracles | Cryptocurrency

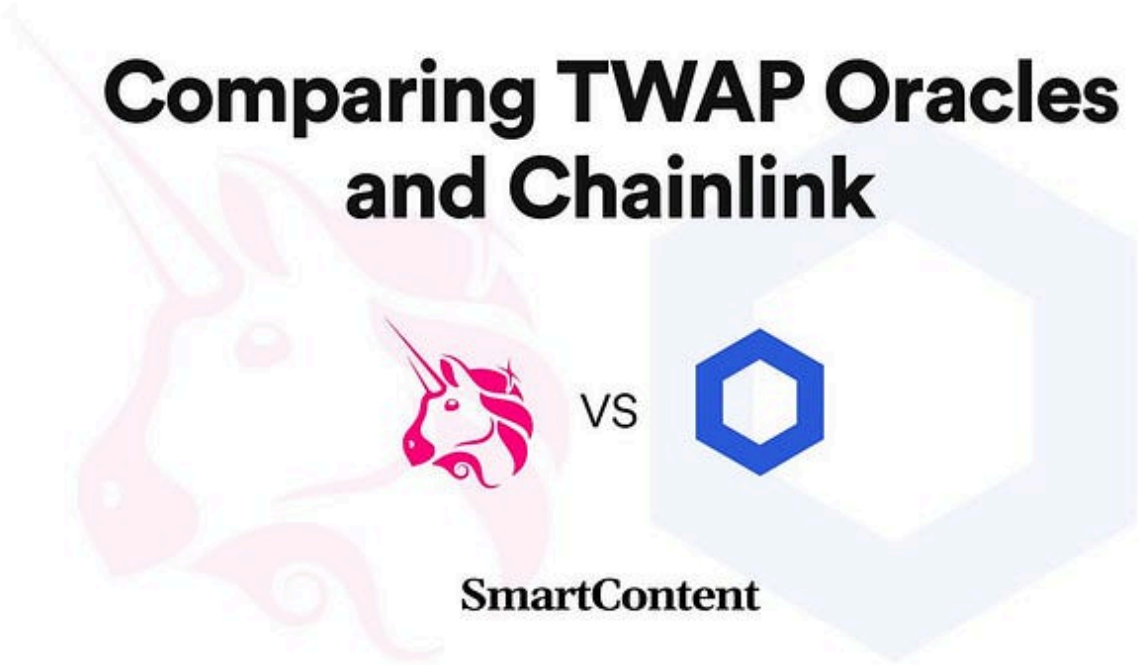
Follow

Written by SmartContent

1.5K Followers

Breaking down the information asymmetry on Chainlink, smart contracts, and the cryptocurrency ecosystem. Founded by The_Crypto_Oracle and ChainLinkGod

More from SmartContent



SmartContent

TWAP Oracles vs. Chainlink Price Feeds: A Comparative Analysis

The announcement of Uniswap V3 has given rise to various questions regarding how Uniswap's Time Weighted Average Price (TWAP) oracles...

23 min read · Apr 8, 2021

221 3

SmartContent

Defining Total Value Secured (TVS) In Decentralized Oracle Networks

Total Value Secured (TVS) is metric that tracks the economic impact of oracle networks within the decentralized economy.

12 min read · Dec 9, 2021

27

SmartContent

Debunking the ‘Zeus Capital’ Disinformation Report on Chainlink

Recently, an anonymous and fraudulent entity going by the name ‘Zeus Capital’ published and heavily marketed a hit piece on Chainlink as...

37 min read · Aug 15, 2020

367 3

SmartContent

The Purpose and Value of Cryptocurrency and Tokens

Cryptocurrencies and tokens are a completely new digital asset class never before seen in financial systems. It's why one of the first and...

22 min read · Feb 16, 2021

571 3

See all from SmartContent

Recommended from Medium

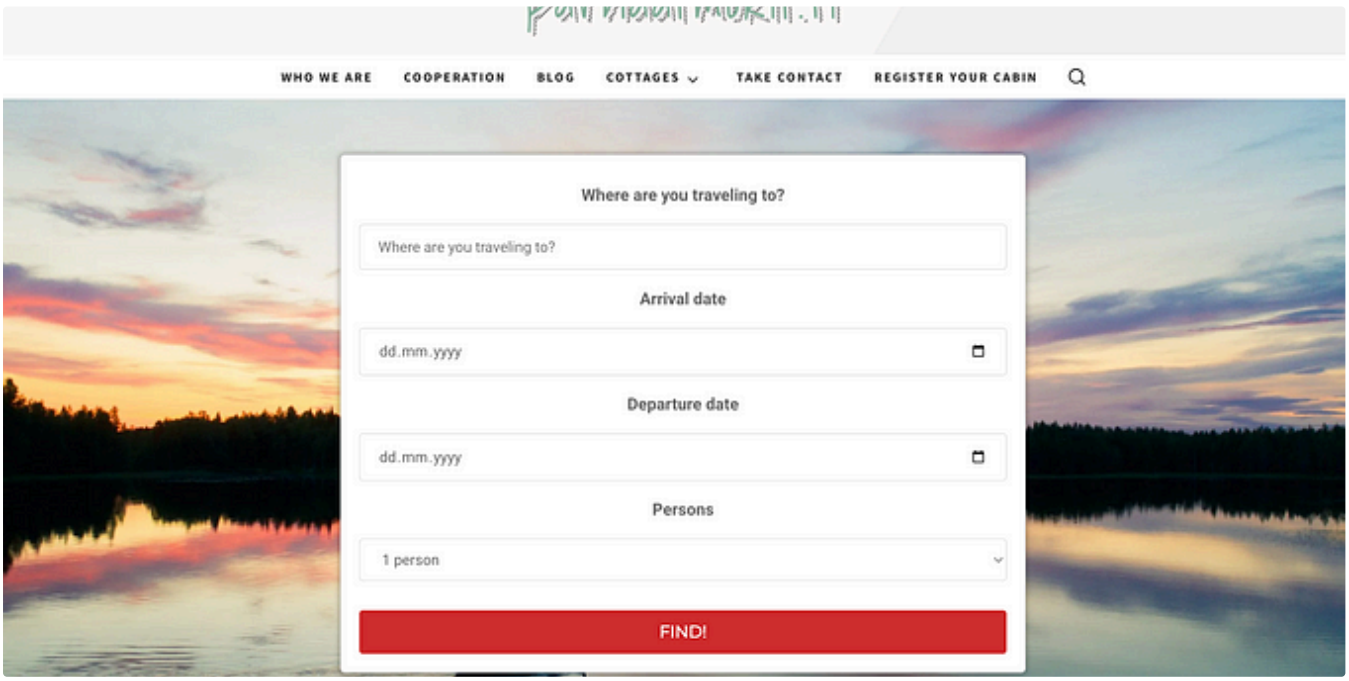
Karolina Kozmana

Common side effects of not drinking

By rejecting alcohol, you reject something very human, an extra limb that we have collectively grown to deal with reality and with each...

10 min read · Jan 21, 2024

34K 908



Artturi Jalli

I Built an App in 6 Hours that Makes $1,500/Mo

Copy my strategy!

✨ · 3 min read · Jan 23, 2024

18.4K 199

Lists

Modern Marketing

139 stories · 648 saves

Generative AI Recommended Reading

52 stories · 1074 saves

My Kind Of Medium (All-Time Faves)

83 stories · 353 saves

Arthur Hayes

The Easy Button

(Any views expressed in the below are the personal views of the author and should not form the basis for making investment decisions, nor...

17 min read · 6 days ago

604 3

Hazel Paradise

How I Create Passive Income With No Money

many ways to start a passive income today

5 min read · Mar 27, 2024

14.1K 330

Kallol Mazumdar in ILLUMINATION

I Went on the Dark Web and Instantly Regretted It

Accessing the forbidden parts of the World Wide Web, only to realize the depravity of humanity

8 min read · Mar 13, 2024

19.6K 358

Unbecoming

10 Seconds That Ended My 20 Year Marriage

It's August in Northern Virginia, hot and humid. I still haven't showered from my morning trail run. I'm wearing my stay-at-home mom...

· 4 min read · Feb 16, 2022

78K 1105

See more recommendations