Chainlink

Decentralized Oracle Networks

Understanding Decentralized Oracle Networks & their applications

Ade Fola-Alade | Solutions Architect

Agenda

- Oracle Problem and Chainlink
- Chainlink Data Feeds
- Chainlink Proof of Reserve
- Chainlink Functions
- Crosschain Interoperability Protocol
- Chainlink Verifiable Randomness
- Chainlink Automation
- Q&A

Decentralized Oracle Networks

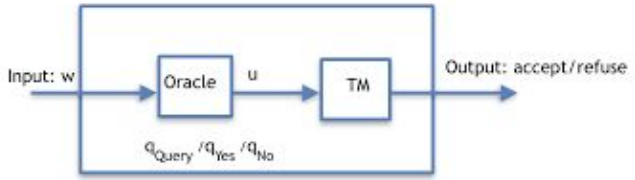
The Oracle Problem

How do we solve an unsolvable problem?

Alan Turing conceived the concept of Oracle machines are “super Turing machines”: they are machines encompassing a classic Turing machine connected to an “oracle” .

This oracle, is an abstract entity capable of solving some problem, which for example may be a decision problem or a function problem.

Put simply, an oracle is a "black box" that is able to produce a solution for any instance of a given computational problem even the famous halting problem!



“Let us suppose we are supplied with some unspecified means of solving number-theoretic problems; a kind of oracle as it were.. . . this oracle . . . cannot be a machine. With the help of the oracle we could form a new kind of machine (call them o-machines), having as one of its fundamental processes that of solving a given number-theoretic problem.”

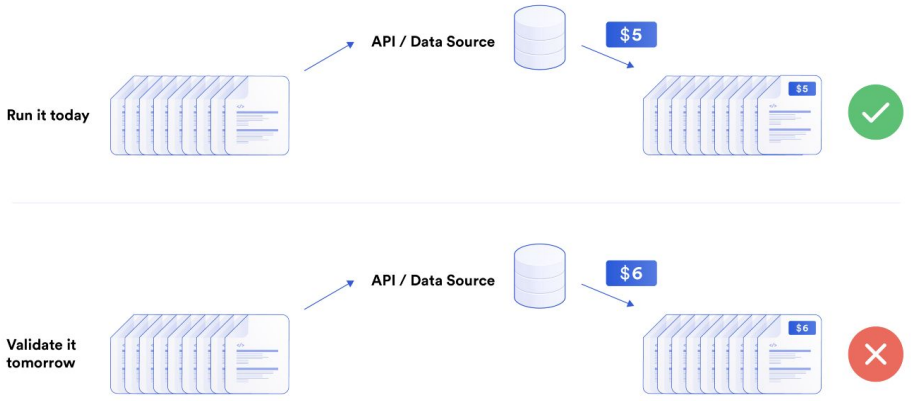
-Alan Turing, 1939

Chainlink

An unsolvable problem for blockchains?

Blockchain's are inherently deterministic, and given it's decentralized nature each node in the network has to be able to find the same end result given the same input.

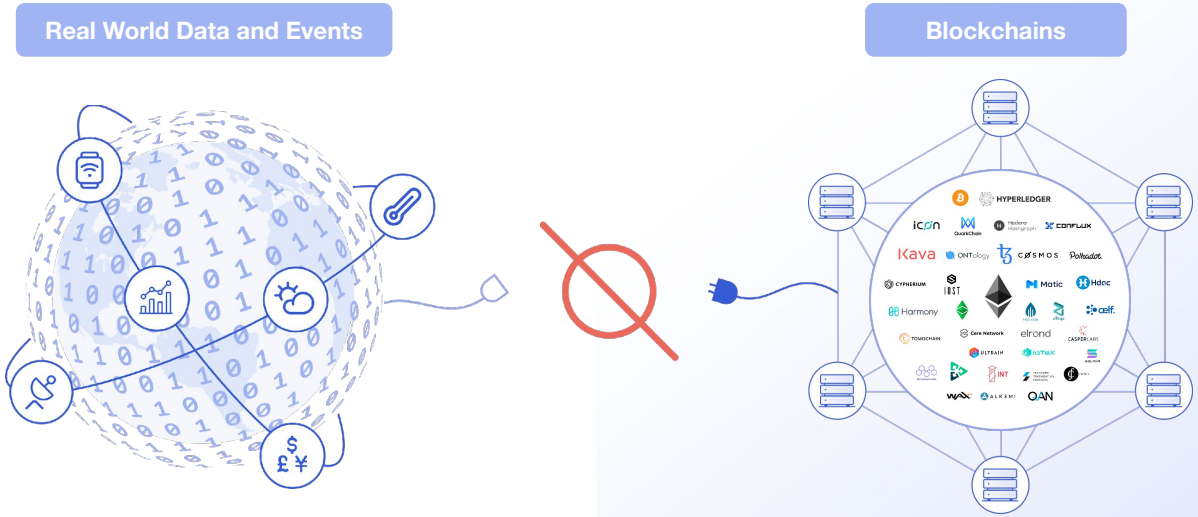
That means if we were to replay every transaction, we should end up in the correct state. If you include API calls or other non-deterministic sources into the infrastructure of blockchain, there is a good chance that the source will be depreciated, hacked, or even just broken, and we would not be able to validate transactions.



Consider a blockchain validating the price of a smart contract on 2 different nodes at various times

The “Oracle Problem” for Smart Contracts

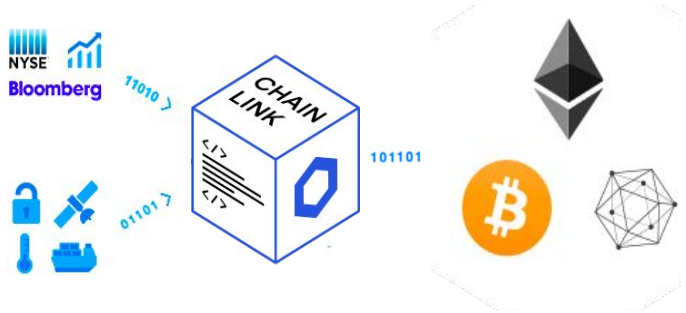
Smart Contracts are unable to connect with external systems, data feeds, APIs, existing payment systems or any other off-chain resources on their own.



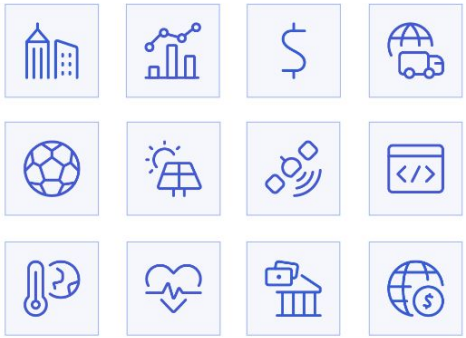
Chainlink

Blockchain Oracles

Blockchain oracles are entities that connect blockchains to external systems, thereby enabling smart contracts to execute based upon inputs and outputs from the real world.



Data Sources



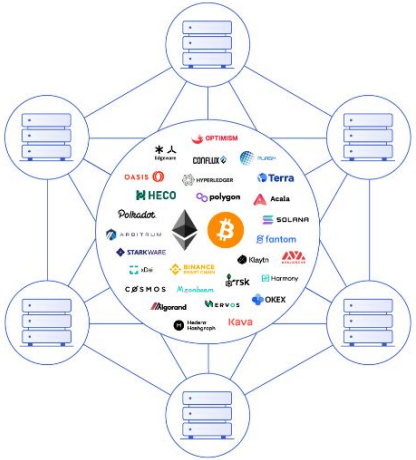
11001100100

Centralized Oracle

One node

10110100101

Decentralized Computation



Thousands of Nodes

Chainlink

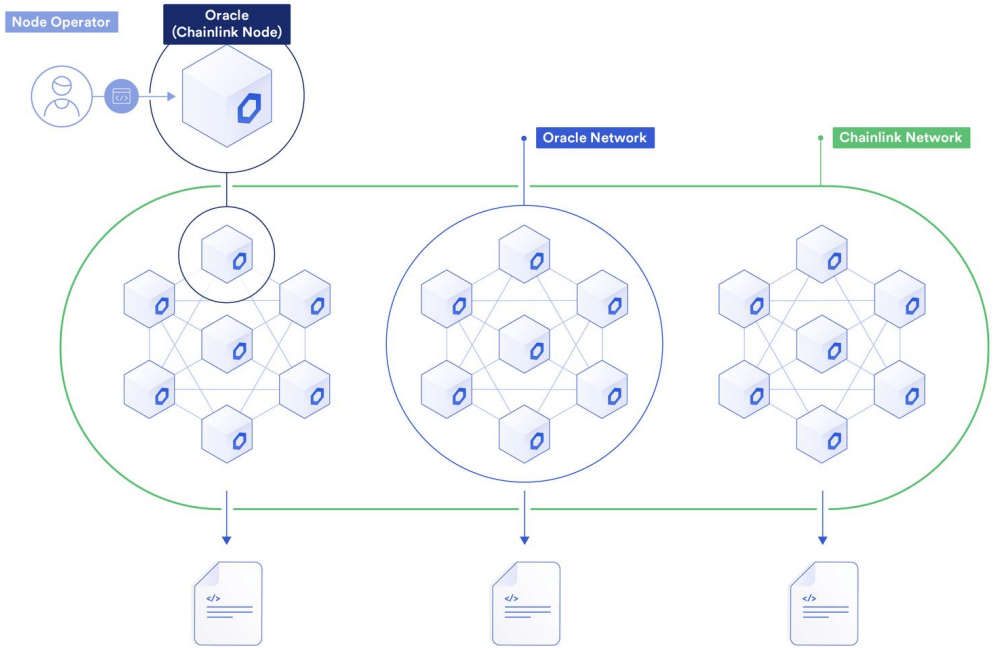
Chainlink Decentralized Oracle Network

Decentralized
network of
Independent/Sybil Resistant
Nodes into Oracle Networks

Provably Secure Nodes
with an established reputation
that provide cryptographic
proof of their overall security

Reliable High Quality Data
from multiple reliable sources and well
validated by multiple nodes

Blockchain Agnostic
Chainlink Nodes can be deployed to
any blockchain



Chainlink

Who are our Node Operators

Chainlink nodes are permissionless, & anyone looking to spin up a node can easily do so. However, given the stringent nature of our requirements for node operators on data feeds, it would be virtually impossible for a solo entrepreneur to run a node at the standard that is required. As a result we find that the node operators who qualify to run the data feeds infrastructure usually fall into 1 of 3 categories:

Web3 DevOps Nodes:

Organizations that specialize in operating blockchain infrastructure such as Proof-of-Stake validators, Proof-of-Work mining pools, and full node RPC providers. They are already well versed in securing billions in value across different blockchains.

Community Nodes:

Teams from within the Chainlink community can become node operators by successfully winning the Oracle Olympics: a 3-week event where teams prove their competence and reliability by fulfilling a series of challenges that mimic real world situations.

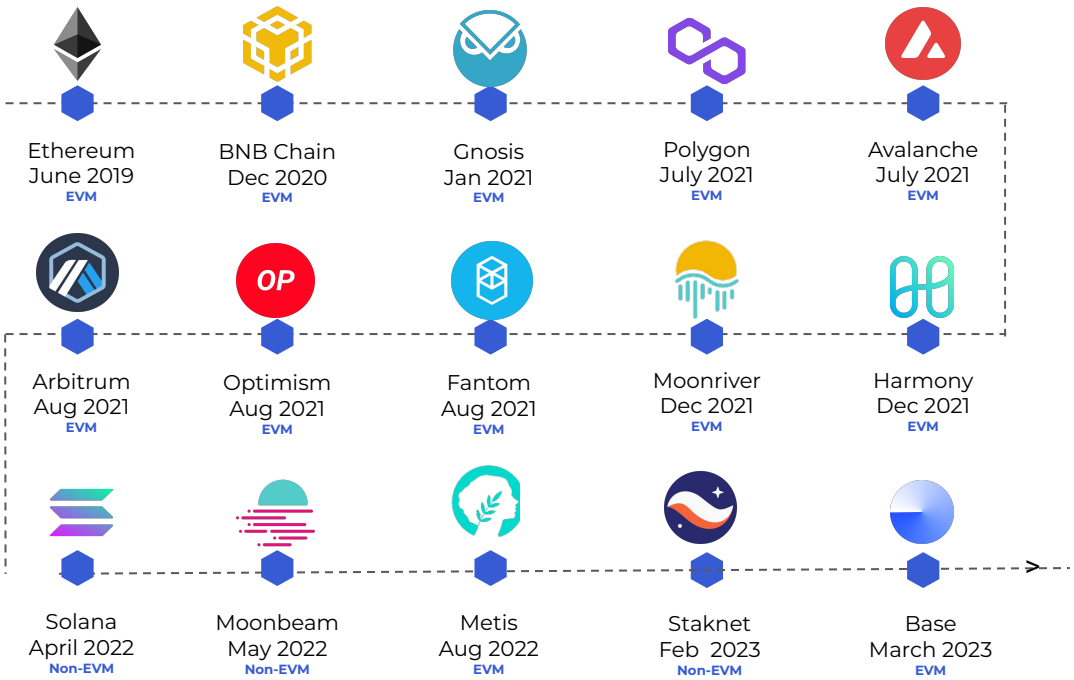
Enterprise Nodes:

Many enterprise organizations have the teams, infrastructure, resources & expertise required to be a node operator. Some of our nodes are operated by these entities such as Deutsche Telekom who have expressed a keen interest in participating within the Web3 economy.

stake·fish Staked VALIDATOR LinkPool NORTHWEST NODES always on course LexisNexis Deutsche Telekom swisscom

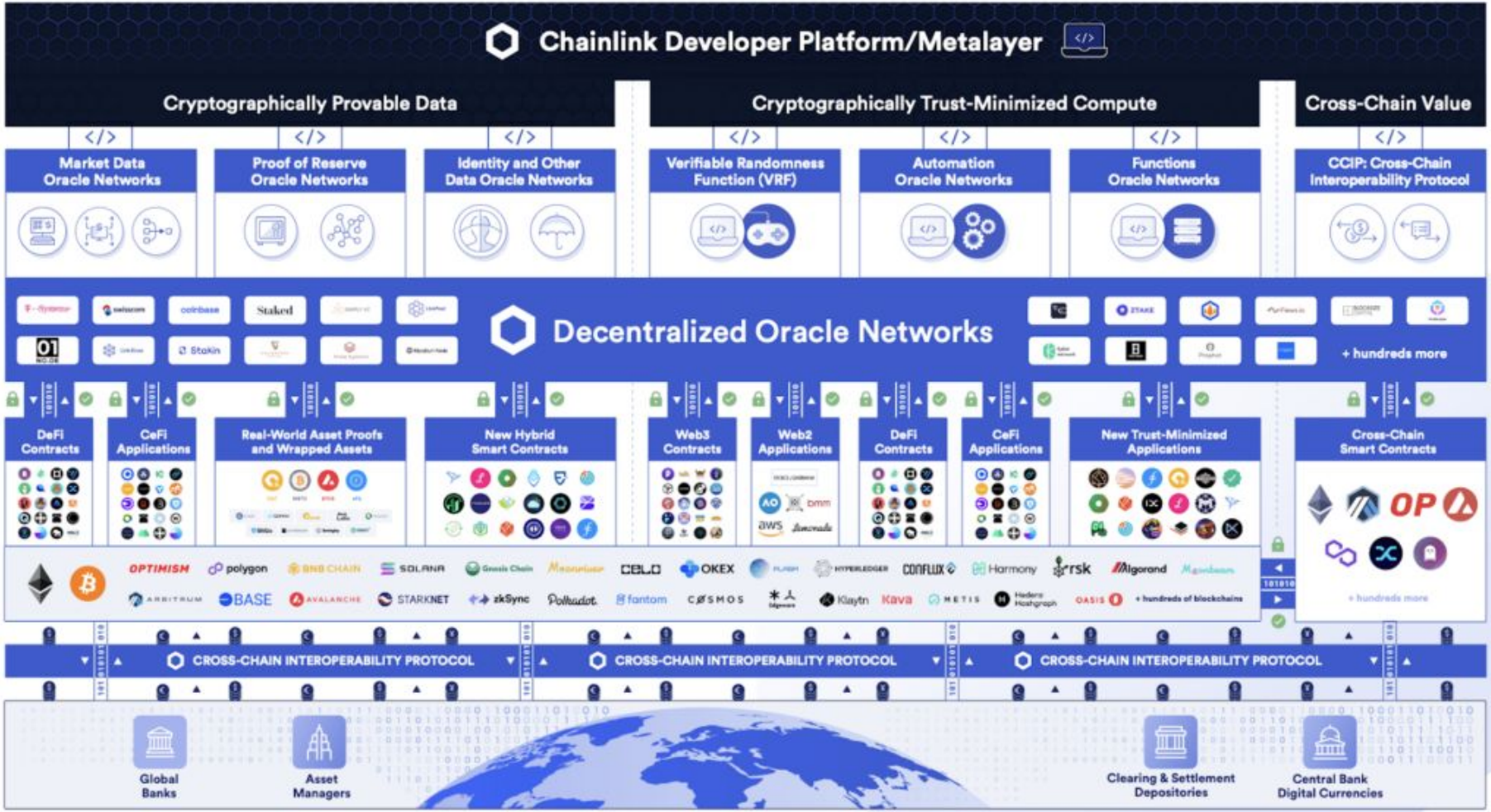
Chainlink

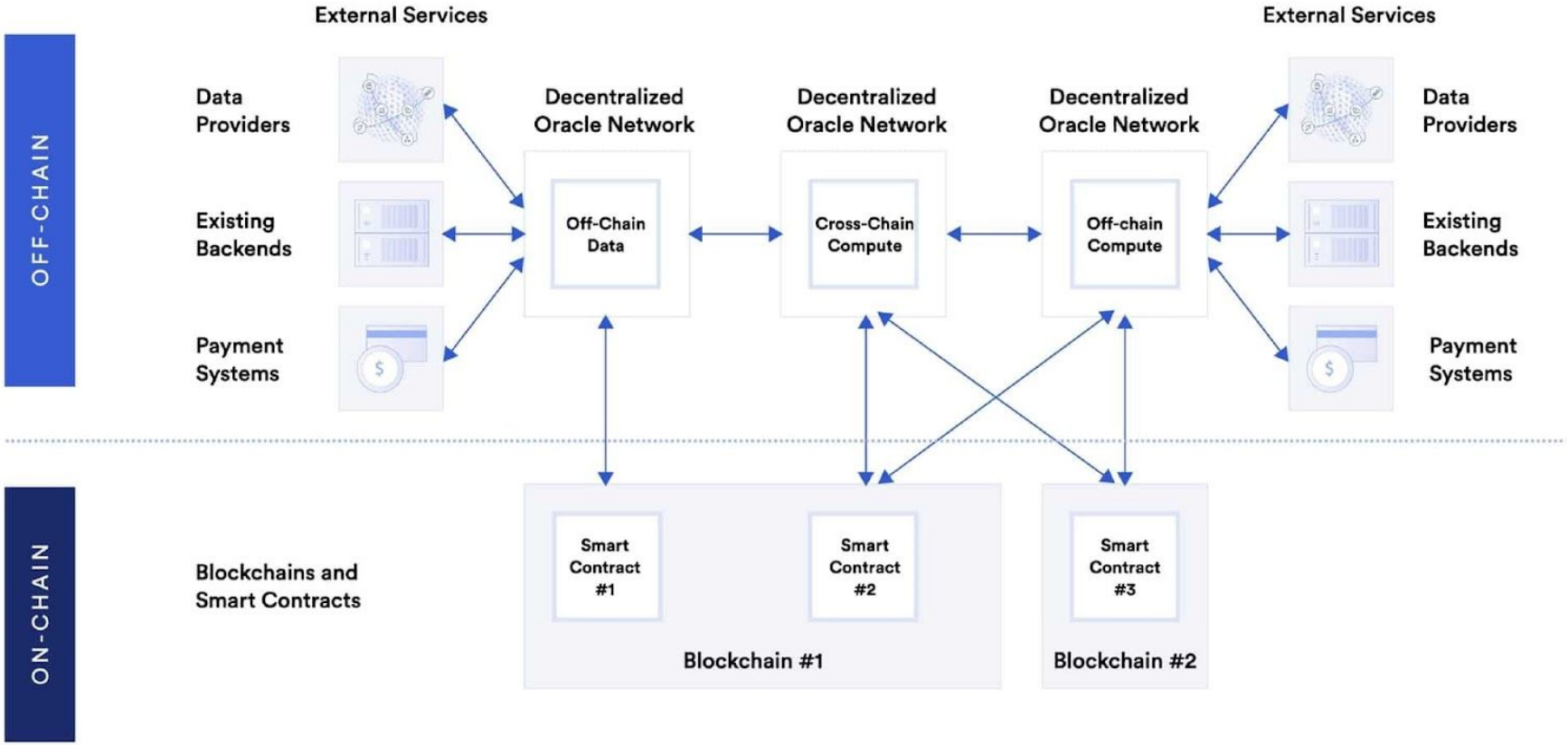
What Blockchains is Chainlink Integrated with?



& Many MOre

Chainlink


Chainlink Developer Platform/Metalayer
Cryptographically Provable Data
Cryptographically Trust-Minimized Compute
Cross-Chain Value
Market Data Oracle Networks
Proof of Reserve Oracle Networks
Identity and Other Data Oracle Networks
Verifiable Randomness Function (VRF)
Automation Oracle Networks
Functions Oracle Networks
CCIP: Cross-Chain Interoperability Protocol
Decentralized Oracle Networks
+ hundreds more
DeFi Contracts
CeFi Applications
Real-World Asset Proofs and Wrapped Assets
New Hybrid Smart Contracts
Web3 Contracts
Web2 Applications
DeFi Contracts
CeFi Applications
New Trust-Minimized Applications
Cross-Chain Smart Contracts
+ hundreds of blockchains
CROSS-CHAIN INTEROPERABILITY PROTOCOL
CROSS-CHAIN INTEROPERABILITY PROTOCOL
CROSS-CHAIN INTEROPERABILITY PROTOCOL
Global Banks
Asset Managers
Clearing & Settlement Depositories
Central Bank Digital Currencies


External Services
External Services
OFF-CHAIN
Data Providers
Existing Backends
Payment Systems
Decentralized Oracle Network
Decentralized Oracle Network
Decentralized Oracle Network
Off-Chain Data
Cross-Chain Compute
Off-chain Compute
Data Providers
Existing Backends
Payment Systems
ON-CHAIN
Blockchains and Smart Contracts
Smart Contract #1
Smart Contract #2
Smart Contract #3
Blockchain #1
Blockchain #2

Chainlink Solutions

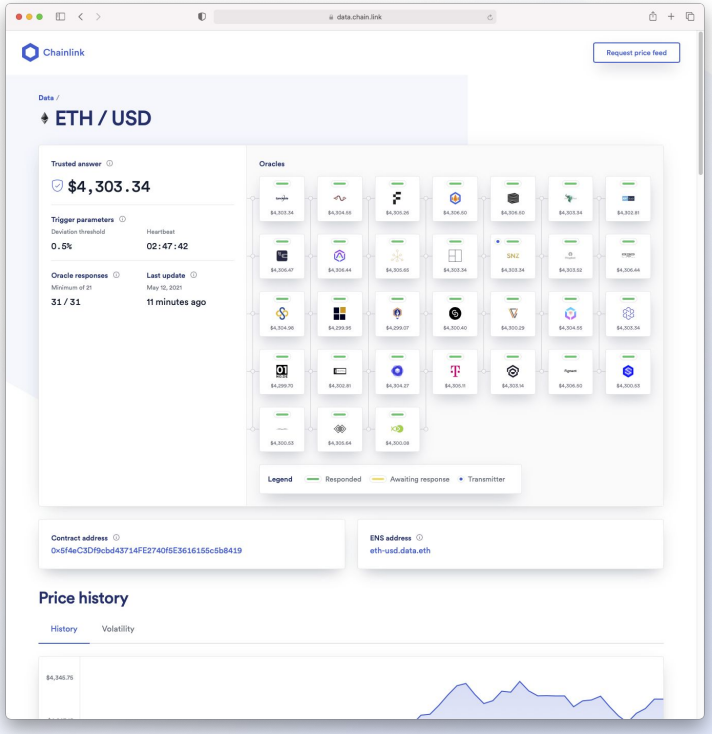
Data Feeds

Chainlink

What are Data Feeds

Chainlink Data Feeds (a.k.a Price Feeds) are the most reliable way to connect smart contracts to the real-world data such as the market prices of assets.

Data Feeds leverage chainlink's **decentralized** and **secure** architecture to provide this data reliably & securely on chain.



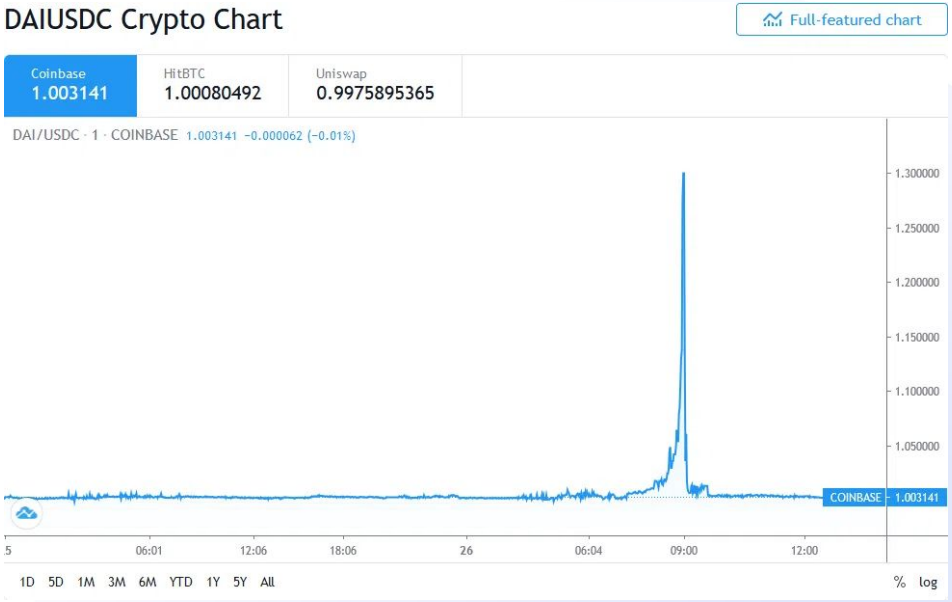
Why Not Exchanges?

SIngle Exchange Data Provider Risk

- Oracle networks that pull price data from a single exchange, not only have no protection against exchange downtime, flash crashes, and price manipulation; they also have minimal market coverage.

Decentralized Exchange Data Provider Risk

- Oracles that pull data directly from preselected exchanges are vulnerable to situations in which volume shifts to new exchanges that were not included in the original aggregation process. While the exchanges originally chosen as data sources for the oracle network may have been liquid during its initial creation, there is no guarantee that volume will stay on these exchanges into the future.



Coinbase DAI/USDC Price Nov 2020: Is this legitimate price action?

Chainlink

Case Study

Exchange Oracle Exploit: Compound

In November 2020, a massive liquidation volume on Compound occurred due to an error from the Dai (DAI) dollar peg data supplied by the Coinbase oracle.

Data from TradingView shows the DAI-dollar peg on Coinbase climbing to $1.34, a 34% premium on the actual value of the stablecoin. An inspection of the DAI price across the market shows the issue occurred only on Coinbase.

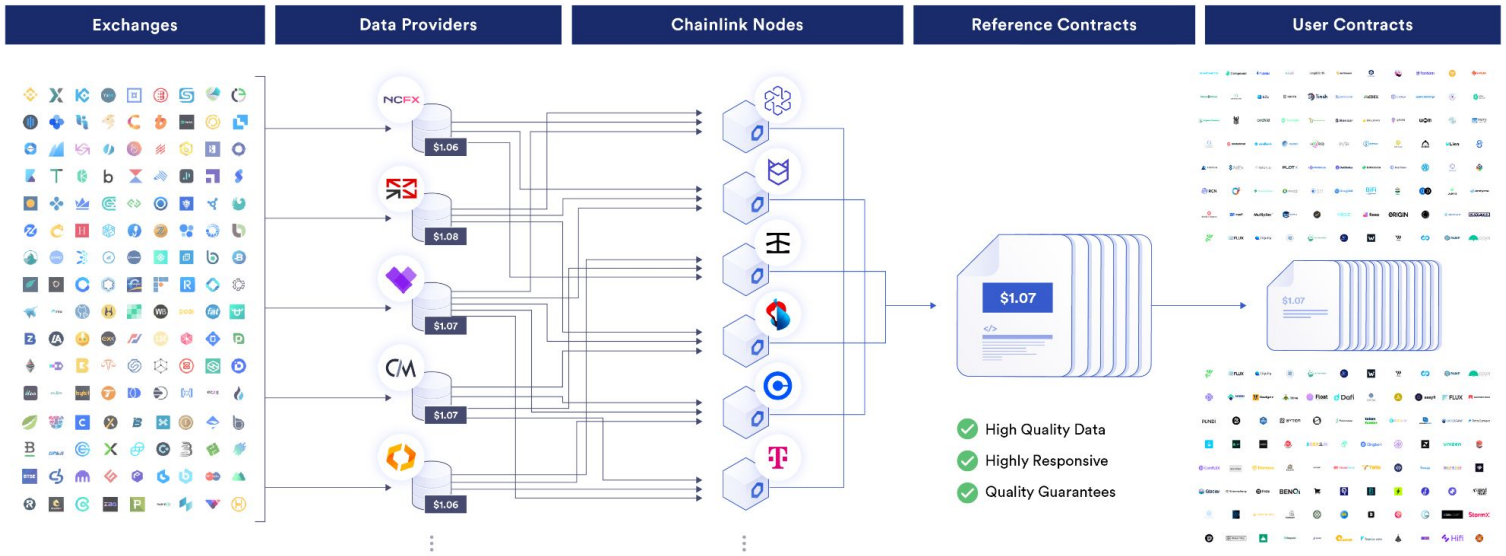
Due to the incorrect price feed from the Coinbase oracle, some Compound users became under-collateralized. Based on the baked-in protocol rules, this meant a forced liquidation of their positions.

With numerous flash loan arbitrage bots scouring the market for such opportunities, it's perhaps unsurprising that some entities benefitted from the situation. The third-largest COMP farmer was reportedly one of the affected users, losing about $49 million in the process.

For more information: [See this link]

Chainlink

Data Feeds powered by Decentralized Oracle Networks



Premium Data Providers aggregate raw price data from a multitude of centralized and decentralized exchanges accounting for volume (VWAP), uptime and outliers.

Independent Chainlink nodes fetch market price data from various premium data providers and combine the results into an aggregated value.

Multiple Chainlink nodes aggregate their results together off-chain to generate a tamper-resistant oracle report which is made available to smart contracts.

Chainlink

Aggregation Parameters

It is important to ensure price feeds remain sensitive to market fluctuations as a failure to do so may have severe ramifications for consuming smart contracts.

The **Deviation Threshold** and **Heartbeat Threshold** are parameters that can trigger price feeds to update during an aggregation round. Each aggregation round triggers based on one of these parameters. The first condition that is met triggers an update to the data.

1 **Deviation Threshold:**

A new aggregation round starts when a node identifies that the off-chain values deviate by more than the DeFined deviation threshold from the on-chain value. Individual nodes monitor one or more data providers for each feed.

For example: if the current Trusted Answer of ETH/USD is $3000 and the “Deviation Threshold” is 0.5%, a price update would automatically be pushed on chain when off-chain price reaches **$3015 (+0.5%) or $2985 (-0.5%)

2 **Heartbeat Threshold:**

A heartbeat enables a new aggregation round to start after a specified amount of time from the last update

A heartbeat is necessary for ensuring data does not become stale even during times of low volatility.

If a price feed moves outside it's “Deviation Threshold” and a new price is pushed on-chain, this heartbeat will reset. The default heartbeat for a new feed is 24 hours, but may be adjusted based on demand.

Security by Design

The security inherent in the Chainlink Data Feeds architecture can be summarized through the **OPEN** model. The key components of this security model are:

Overall Market Coverage

Hundreds of exchanges (CEX & DEX) providing full market coverage for data feeds

Premium Data Aggregators

Chainlink nodes use the best premium market data aggregators

Experienced Node Operators

Professional node operators with 24 hour monitoring.

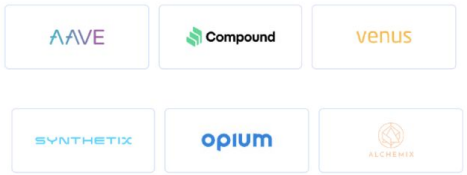
Native Integrations

Chainlink has the widest natively blockchain integrated data feeds network

Chainlink Data Feeds in the world of DeFi

$50B

Total Value Locked



DeFi is short for “decentralized finance,” an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries. Use cases include: Lending and borrowing with money markets, Synthetic assets and derivatives, Asset Management and portfolio allocation, Insurance, Etc.

DeFi solutions require accurate price data that is often not available on-chain for the efficient operation of their protocols.

Chainlink’s price data feeds (Price Feeds) play a crucial role in securing value across a wide variety of DeFi projects across the ecosystem by providing reliable external price data on-chain via our decentralized oracle network.

2017

First DeFi protocol based on borrowing and over collateralization with Maker’s release of DAI

2018

New DeFi projects such as Compound, Set Protocol, dYdX, Synthetix

2019

Boom of DeFi with increasing composability between protocols (e.g Interest bearing tokens)

2020

Yield farming, increased leverage positions, 30B+ USD in TVL

2022

75 B in TVL, multi chain DeFi ecosystem growing on other chains than Ethereum

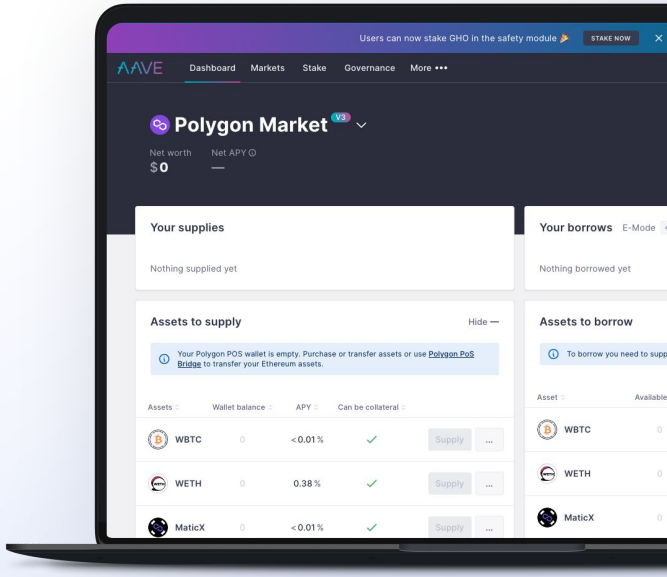
The deployment of Chainlink’s price feeds in 2019 was a huge catalyst in the growth of the DeFi Ecosystem

Use Case Examples

Aave’s Liquidation Engine

Aave uses Chainlink’s tamper proof price feeds to determine the price of assets they have in their pools. This helps determine key metrics like loan-to-value ratios, collaterization ratios, liquidation events, etc. These are critical for the operation of decentralized money markets like Aave.

“The security provided by the Chainlink Network's oracle infrastructure has served the Aave protocol well, and now users of the Aave protocol can leverage Chainlink's offchain service to participate in the Aave ecosystem as liquidators to secure the Aave protocol and its liquidity pools."
—Stani Kulechov, CoFounder of Aave



Chainlink

Chainlink Solutions

Chainlink Automation

Chainlink

Chainlink

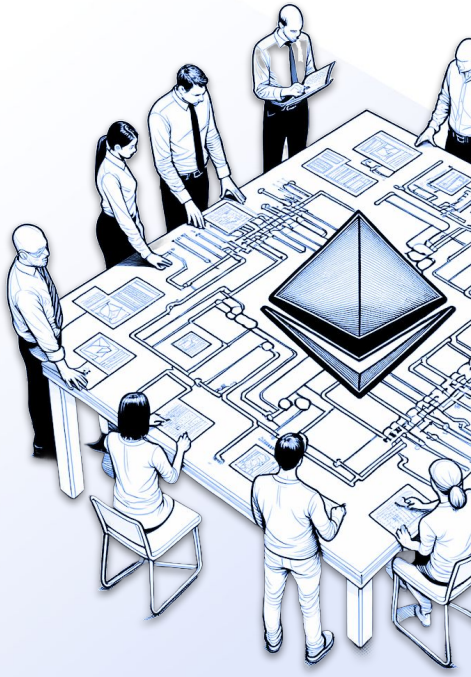
We've all heard this phrase before:

Smart Contracts cannot automatically call their own functions to execute

Why So?

Smart contracts are inherently passive. They are structured and optimized for defining the rules and actions for specific function calls rather than initiating them. The model relies on being reactive rather than proactive where transactions (including function calls) are initiated only by users, contracts or external services a.k.a **"Oracles"**. This design abstracts away the complexities of timing, veracity & consensus, focusing instead on executing predefined outcomes with precision upon being triggered. Here are some factors to consider why this design choice was necessary:

1. **Consensus Protocol:** Blockchains use consensus protocols to validate transactions and agree on the current state of the network. Autonomous execution of smart contracts could lead to inconsistencies and challenges in achieving consensus, as it would require the network to predict future states and validate them without external inputs.
2. **Resource Management:** Unlimited, self-initiated execution of smart contracts could lead to resource depletion, such as consuming excessive amounts of gas (Ethereum's computational effort cost), leading to network congestion and potentially making the network vulnerable to denial-of-service attacks.
3. **Security and Control:** Requiring an external trigger for smart contract execution provides an additional layer of security and user control, ensuring that contract functions are executed intentionally and with explicit consent.
4. **Deterministic Execution:** Blockchain transactions, including smart contract executions, must be deterministic to ensure that every node on the network can independently verify and agree on outcomes. Self-executing contracts could introduce non-deterministic behavior if they rely on external conditions or data not contained within the blockchain.

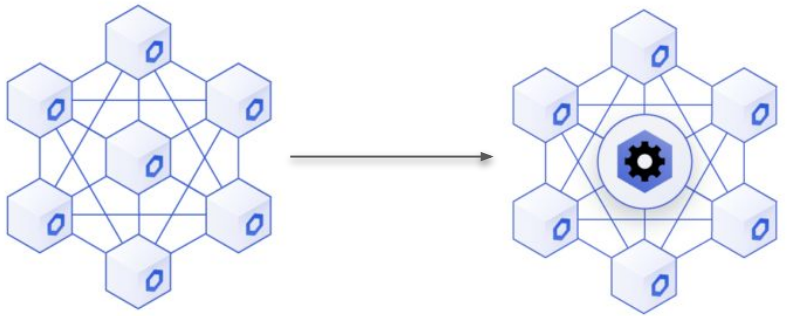


Chainlink DONs continue to solve the Oracle Problem

Chainlink solves this automation oracle problem by creating a specialized version of it's industry leading Decentralized Oracle Networks (DONs). This provides a reliable, trust-minimized way to trigger smart contract executions based on predefined conditions or schedules without relying on centralized servers or manual intervention.

This service is essential for enabling truly autonomous, decentralized applications while assuring users of Chainlink's 3 core guarantees:

Decentralization | Security | Reliability



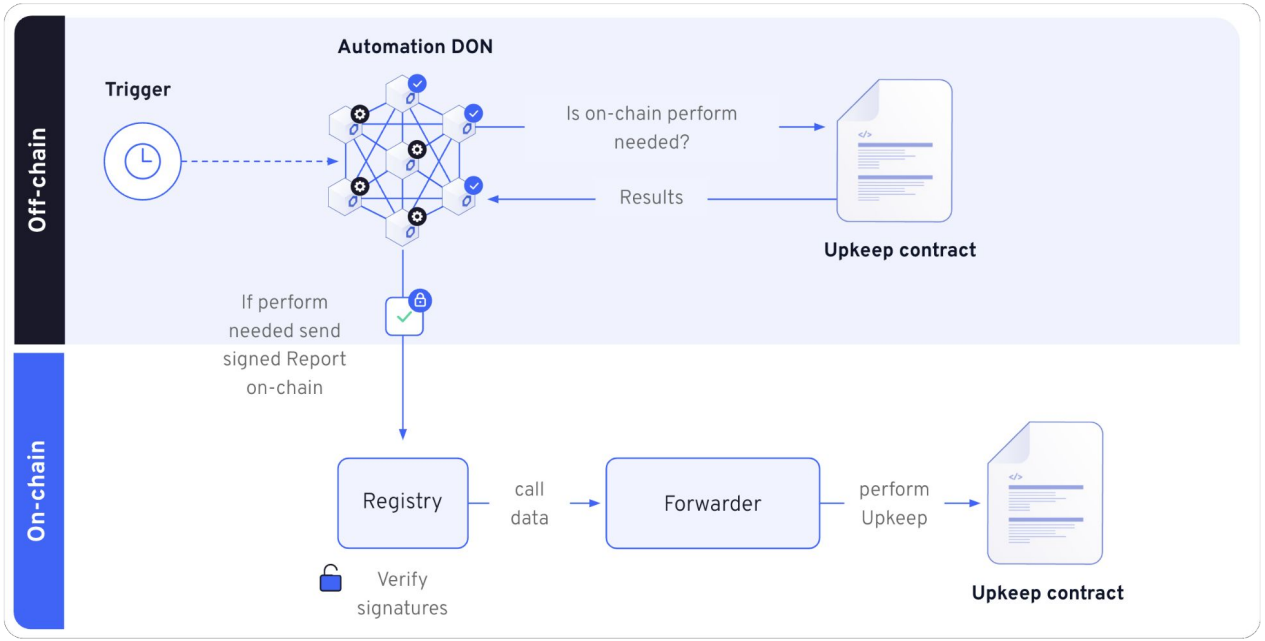
Chainlink

Automation

Chainlink Automation is a decentralized automation and compute network that allows you automate any smart contract at up to 1/10th of the gas cost

Chainlink

Automation v2 Architecture



Upkeep Contract
A user's contract specifying the automation tasks. This can be an Automation-ready contract or any contract with an external/public function for scheduled tasks

Automation Network
Chainlink decentralized oracle network of nodes that executes registered Upkeeps.

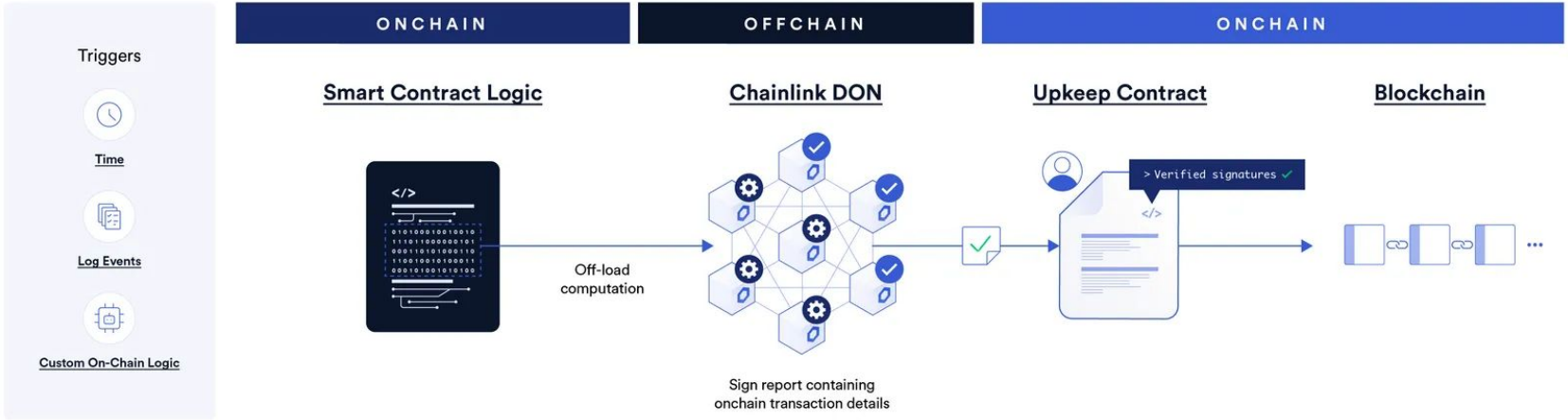
Automation Registry
Manages network participants and rewards nodes for successful upkeeps. Developers register their upkeeps here, and node operators sign up as Automation Nodes

Forwarder
Acts as a bridge between the registry and the user's contract, providing a stable address for authorization and access to the registry for programmatic interactions.

Automation Triggers

Automation nodes use triggers and logic to determine what needs to happen on-chain (and when). Nodes then come to consensus and the signed report is sent onchain to ensure the computation is verifiable, providing strong security and reliability guarantees.

The 3 key triggers are: **Time**, **Log Events** & **Custom On-Chain Logic**



Automation Triggers

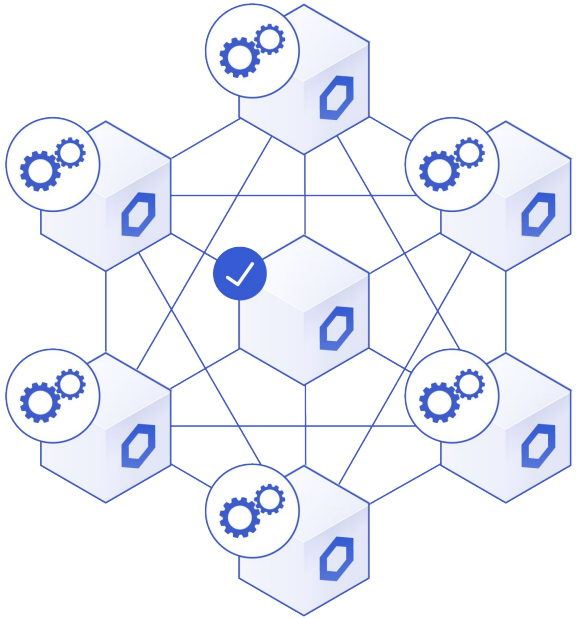
Any time interval
Every 30 seconds

Specific time of day/week/month
At midnight

Log triggers
When a *marketOrder()* event is emitted

When an on-chain condition is met
When the price hits $88

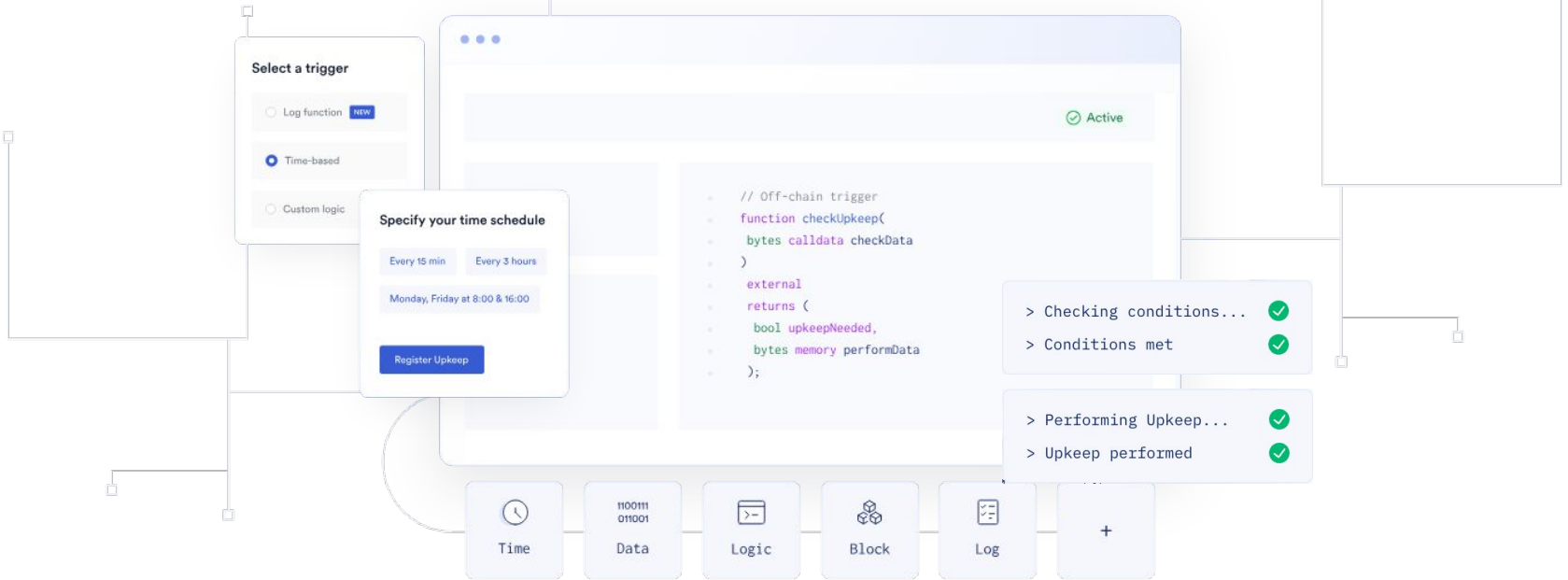
Any combination of the above
When the price hits $88 and within trading hours



Automation Upkeeps

Chainlink Automation keeps track of all actions to be triggered via upkeeps, a specific automated task or function that is executed by the Chainlink DON to maintain the proper functioning or update the state of a smart contract.

Upkeeps are monitored off-chain for predefined conditions or triggers that are monitored by a DON (**checkUpkeep**), and when met, perform predetermined actions on-chain on behalf of the smart contract (**performUpkeep**).



Verifiable Off-chain Computation

Chainlink Automation can do some work off-chain with zero gas costs and pass actionable results to an on-chain contract.

Testing for trigger conditions

Has one hour pass since the previous execution?

Looping through a data set - Limit orders

Find the subset of 1000 limit orders that are ready for execution

Performing calculations - Algorithmic trading

Are debt ratios and collateralization ratios within acceptable thresholds

Manipulating data - Auto-compounding

Create an array of all the vaults that need to be autocompounded and pass this data to an on-chain function.

Benefits: Increase/Decrease/Eliminate

Cost

Decreases gas expenses by up to 90% with Verifiable Compute.

Decentralization

Increases resilience and reliability.

Increases confidence within the project's community.
Looks good on the project roadmap.

DevOps

Decreases cost of DevOps.

Increases time developer spends executing on the roadmap.

Infrastructure

Eliminates single-point of failure - no servers.

Eliminates costs to procure, provision, and maintain servers/software or cloud infrastructure.

Eliminates reliance on system administrators.

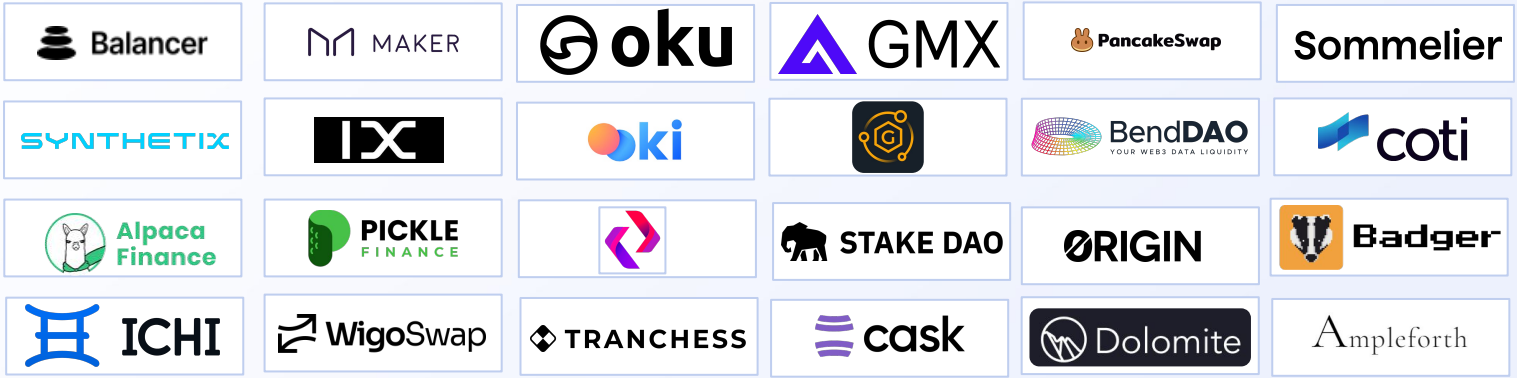
Integration

Decreases disparate skills needed to maintain separate applications as upkeeps are Solidity smart contracts.

Security

Decreases risk of key exposure because transactions are submitted by Automation nodes. Project's keys are not used - not stored on servers.

Chainlink Automation is the leading solution for decentralized workflows in the industry. Used by the top projects in the space



Chainlink

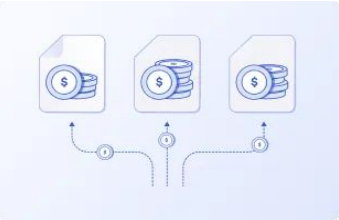
Use Case Examples

Automation enables a wide array of use cases

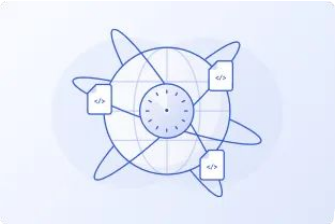
Limit orders, stop losses, liquidations

Trading strategies

Liquidity management



Reward payouts



Starting & Settling Rounds

NFT Staking Rewards

Rebasing & Rebalancing

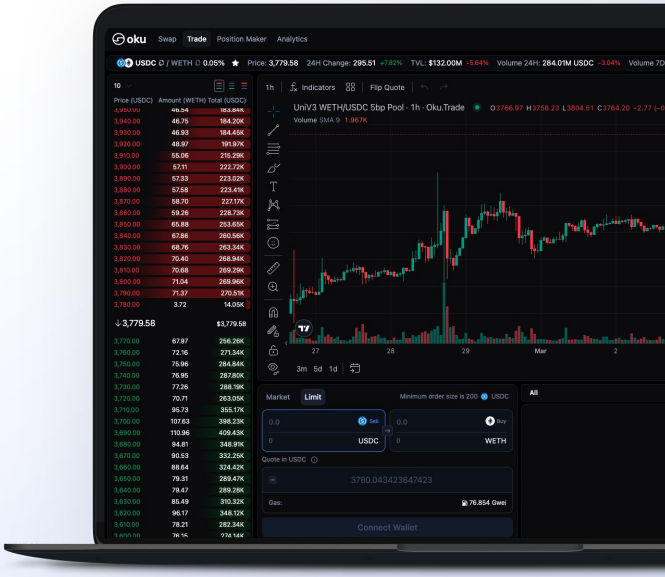
Chainlink

Uniswap V3 limit Orders by Oku

Segment	Solution	Use Case	Trigger	Complexity	Impact
Defi	Verifiable Compute	Limit Orders	On-Chain Logic	High	High

Oku, an enhanced user interface for Uniswap v3, is using Chainlink Automation to enable DEX limit orders by performing regular heavy computations offchain to calculate whether any limit orders need to be executed.

“We’re excited to be using Chainlink Automation to help users post limit orders on Uniswap v3 across all of the top chains. **Without the battle-tested automation service, we would need to maintain in-house infrastructure to enable limit order functionality**. Chainlink Automation helps make our lives easier so we can focus on building more advanced tools for Uniswap v3 users and the broader DeFi ecosystem.”—Getty Hill, Founder of GFX Labs & Oku



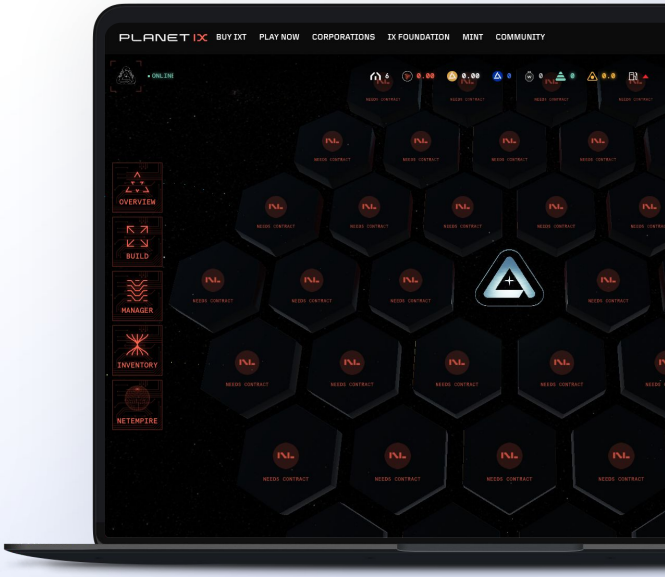
Chainlink

Batch Randomness Requests by Planet IX

Segment	Solution	Use Case	Trigger	Complexity	Impact
Gaming	CLA+	Batching NFT Mints	Time	Low	Medium

Planet IX leveraged Chainlink Automation to help securely and cost-efficiently trigger batch randomness requests to Chainlink VRF in order to help reduce costs associated with the creation of Planet IX NFTs

"As best-in-class smart contract automation infrastructure, Chainlink Automation provides us with a **secure and reliable execution service that helps us reduce costs** associated with the creation of Planet IX NFTs."
—Karl Blomsterwall, CEO of Planet IX



Chainlink

Chainlink Solutions

CCIP

Chainlink

Billions of Dollars have been lost to cross-chain hacks

Total Value Hacked in Bridges (USD) **$2.66B**

Source: defillama.com/hacks

What is CCIP?

Chainlink's single-messaging interface for all cross-chain communication

Cross-Chain Interoperability Protocol (CCIP) provides a universal, open standard for developers to build secure services and applications that can send messages, transfer tokens, and initiate actions across multiple networks.

Chainlink

Scaling security for reliable Cross-Chain

LEVEL 1

CENTRALIZED

- 1 Node
- 1 Centralized Operator

LEVEL 2

DECENTRALIZED THEATER

- Multiple Nodes
- 1 Centralized Operator

LEVEL 3

ONE NETWORK

- Multiple Nodes
- Multiple Operators
- 1 Network

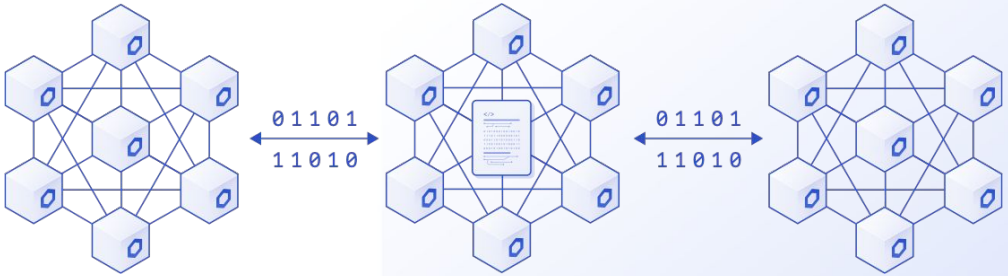
LEVEL 4

MULTIPLE NETWORKS

- Multiple Nodes
- Multiple Operators
- Multiple Independent Networks

LEVEL 5

Multiple Networks
& Risk Management



Committing DON

Risk Management Network

Executing DON

Chainlink

Proven risks with alternative models

LEVEL 1

CENTRALIZED

- Private key compromised
- Cloudflare Key Compromised
- Bus Factor of 1

CENTRALIZED

LEVEL 2

DECENTRALIZED THEATER

- Centralized Cloud Provider Outage
- Cloud Provider Attacked
- Significant Insider Threat

DECENTRALIZED THEATER

LEVEL 3

ONE NETWORK

- Inability to Reach Consensus
- Central Hub Exploited
- Access Control Exploit
- Doesn't Scale

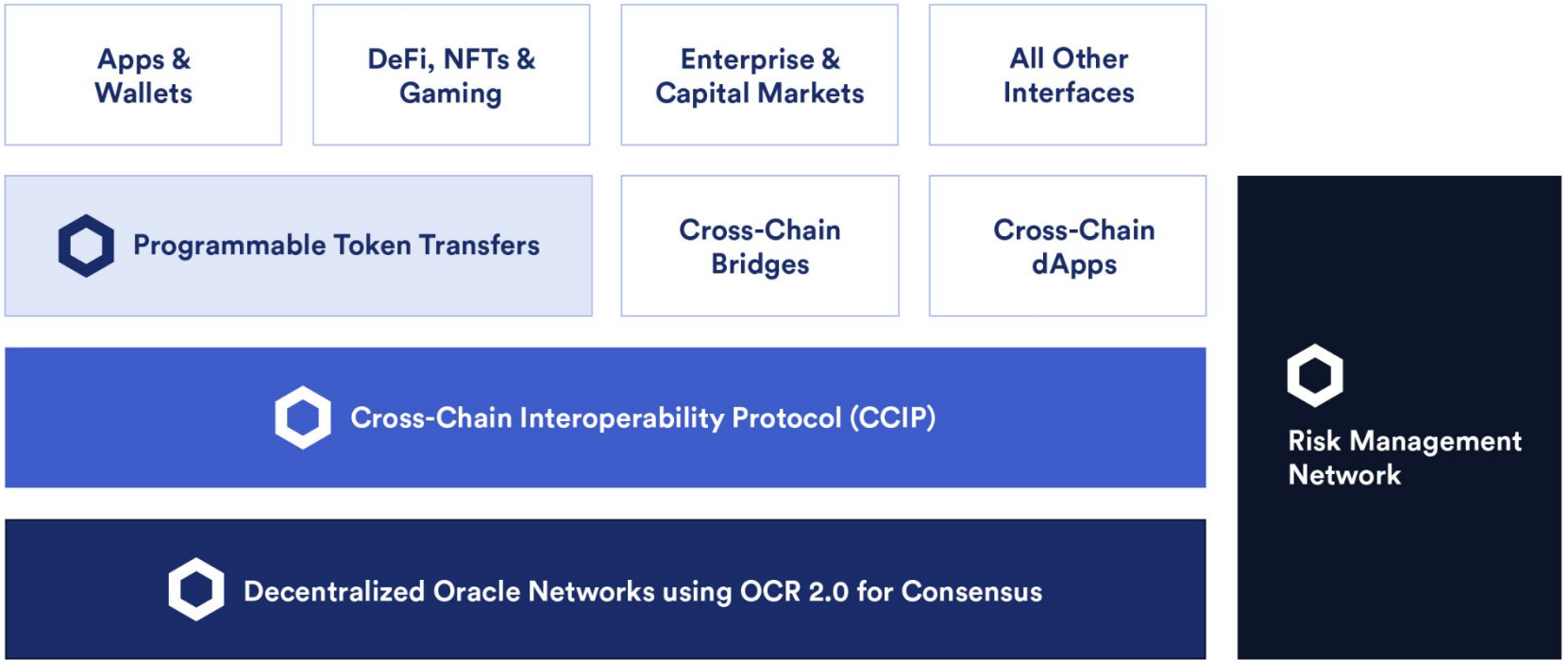
ONE NETWORK

Transaction Failure **Stuck Tokens** **Pools Drained**

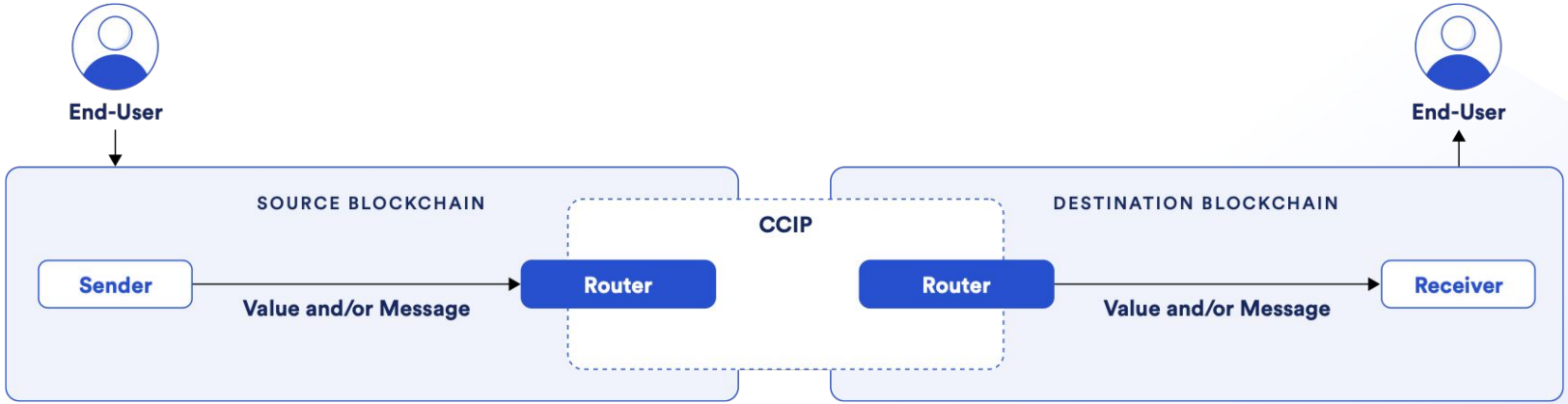
Bad Debt **Infinite Mint**

Chainlink

The CCIP cross-chain stack



A single and simple interface connecting dapps to many blockchains



Token Transfers

Tokens

The ability to transfer tokens to a receiving smart contract or wallet address (EOA)

Arbitrary Messaging

Data

The ability to send arbitrary data (i.e. bytes) to a receiving smart contract

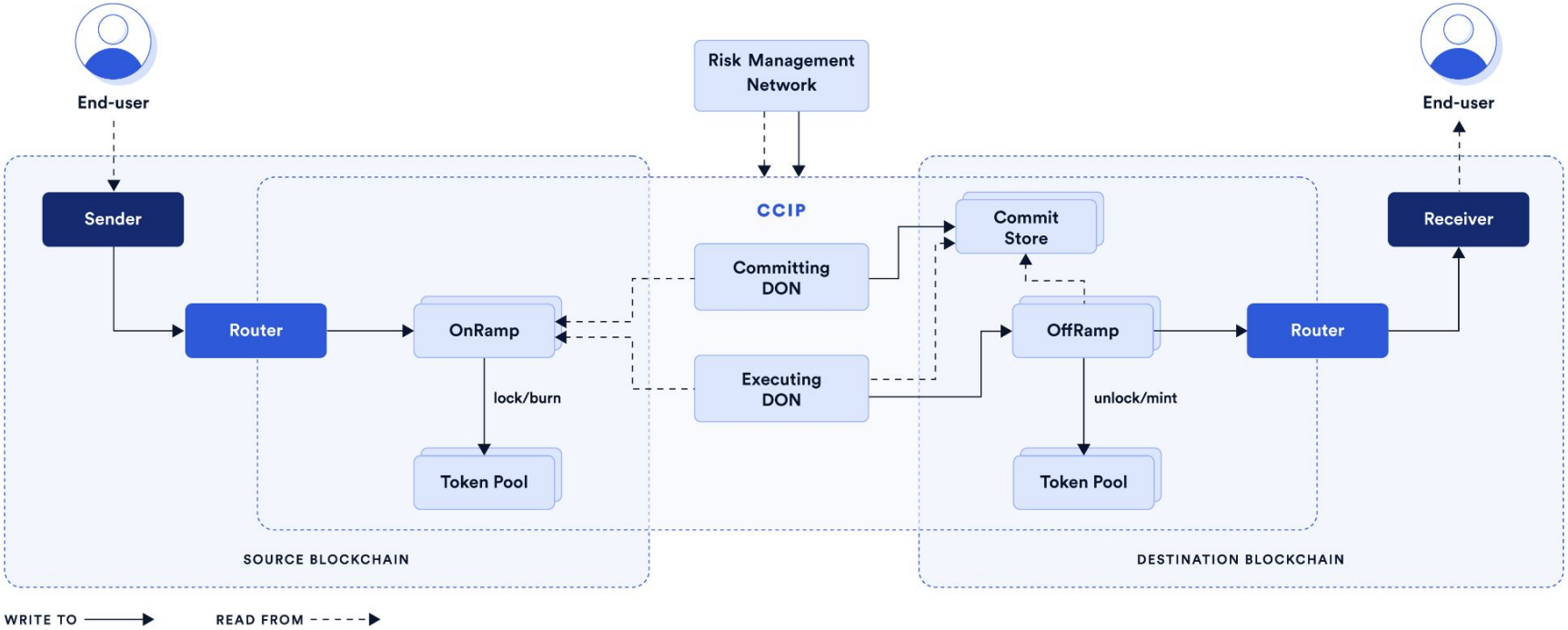
Programmable Token Transfers

Data + Tokens

The ability to transfer tokens along with instructions what to do with those tokens, to a receiving smart contract

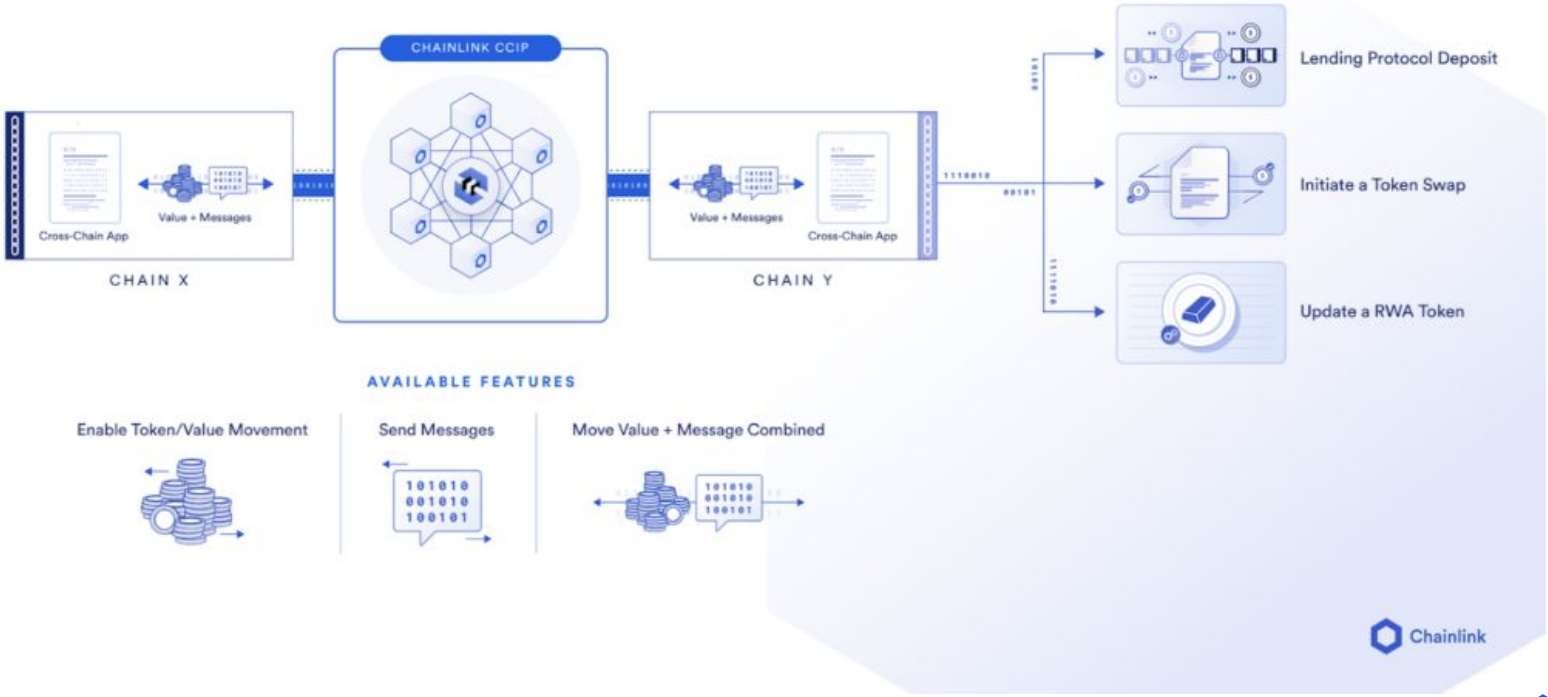
Chainlink

CCIP introduces risk management and greater decentralisation



Chainlink

Tokens + Messages Enables Easy Usage of Other Chains' Smart Contracts



Use Cases for CCIP are many ...

Cross-Chain Collateral

Money market protocol can deposit funds on one chain and use on another

Low-cost transaction computation

Offload computation of transaction data on cost-optimized chains

Cross-Chain Yield Optimization

Move collateral to new Defi protocols to maximize yield across chains

New kinds of dApps

Take advantage of network effects on Eth mainnet while harnessing compute and storage on other chains

Chainlink

Use Cases for CCIP in gaming are many ...

Cross-chain NFTs

Make any NFT natively available to users on their chosen blockchain

Cross-Chain NFTFi

NFTFi lending platform can post NFT collateral on one chain and borrow assets on another

Cross-Chain Gaming

Store high-value items on more secure chains while playing on more scalable chains

Expand your community

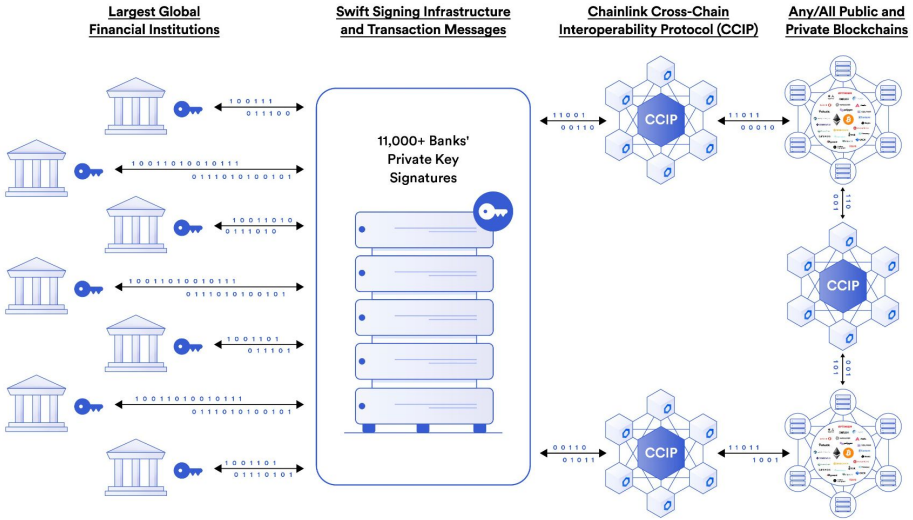
Capture more players, activity, and liquidity across the blockchain ecosystem by going cross-chain

Chainlink

Use Case Examples

SWIFT CCIP POC

Chainlink its collaborating with Swift and financial organizations within its community to test how institutions can use their Swift connection to seamlessly interoperate with the many #blockchain networks emerging around the world.



Swift DTCC LLOYDS BANKING GROUP BNY MELLON citi ANZ

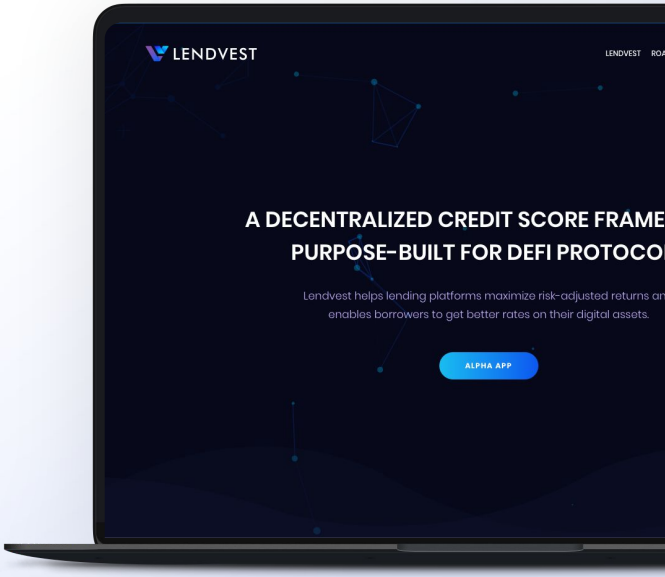
Chainlink

Lendvest's Crosschain Credit Score

Lendvest is leveraging CCIP's arbitrary messaging functionality to help build a cross-chain credit score system in DeFi, enabling the low-cost transmission of credit score messages between Ethereum and Avalanche.

"We're excited to integrate Chainlink CCIP to unlock a seamless cross-chain credit score system for DeFi. Since CCIP is built on the same foundation as other Chainlink services, such as Chainlink Price Feeds, integrating with DeFi lending protocols will enhance these protocols without introducing any additional trust assumptions." — Joshua Gottlieb, Co-Founder of Lendvest

Lendvest



Chainlink