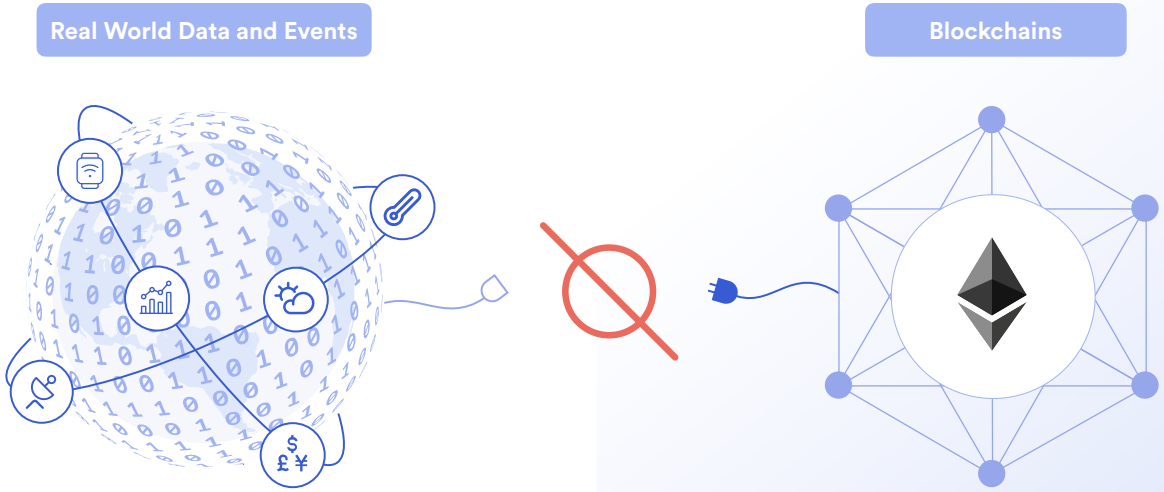
Chainlink

Externally Connected Smart Contracts

Ethereal 2020

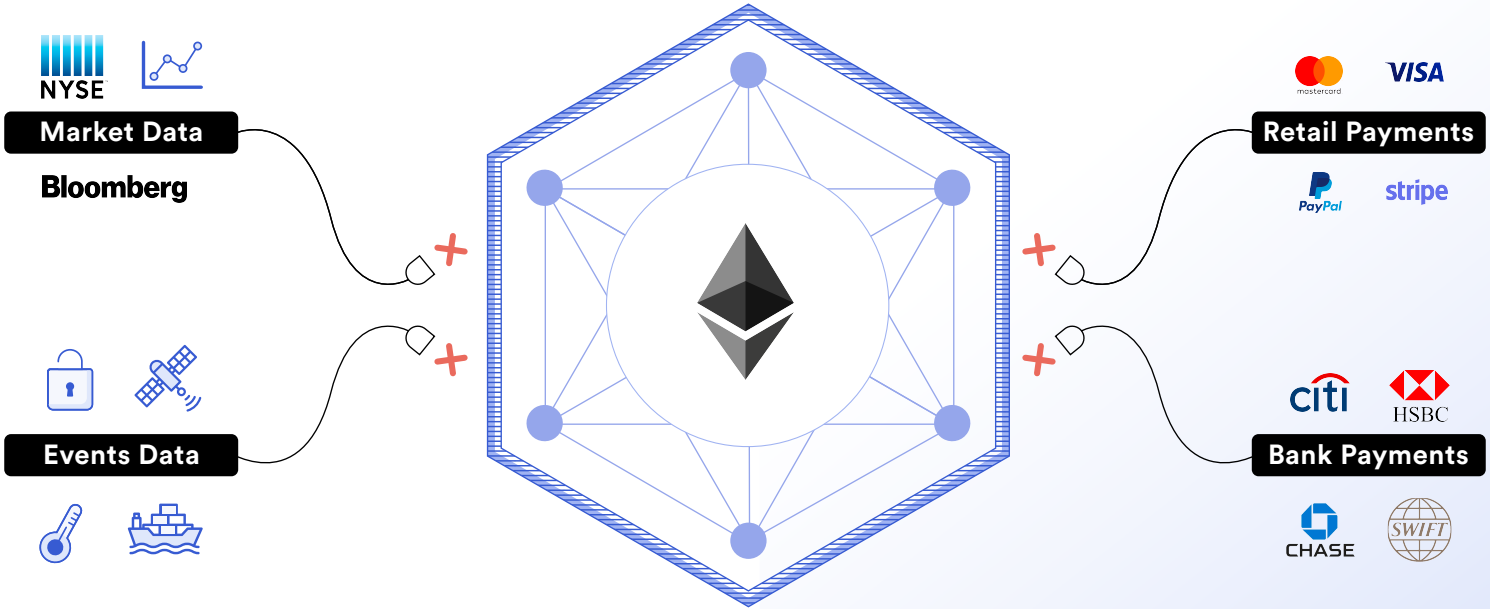
The “Oracle Problem” for Smart Contracts

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



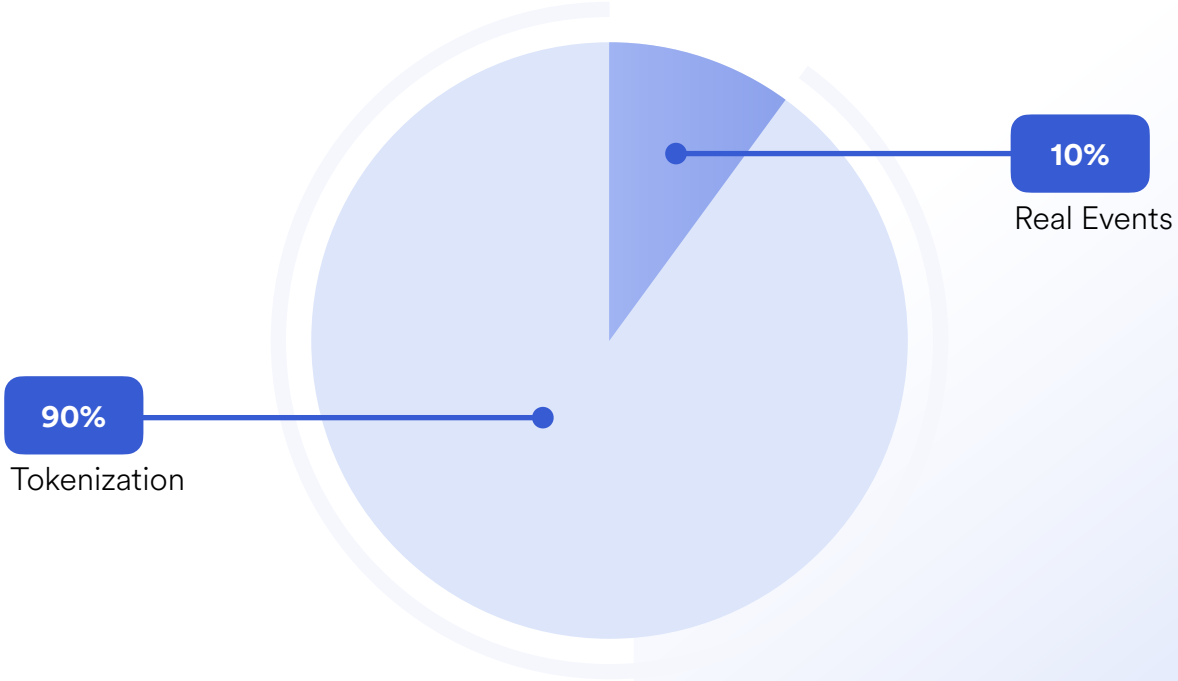
Chainlink

The “Oracle Problem” for Smart Contracts



Chainlink

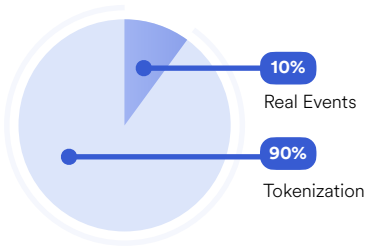
Smart Contracts are Currently Used for Tokenization



Chainlink

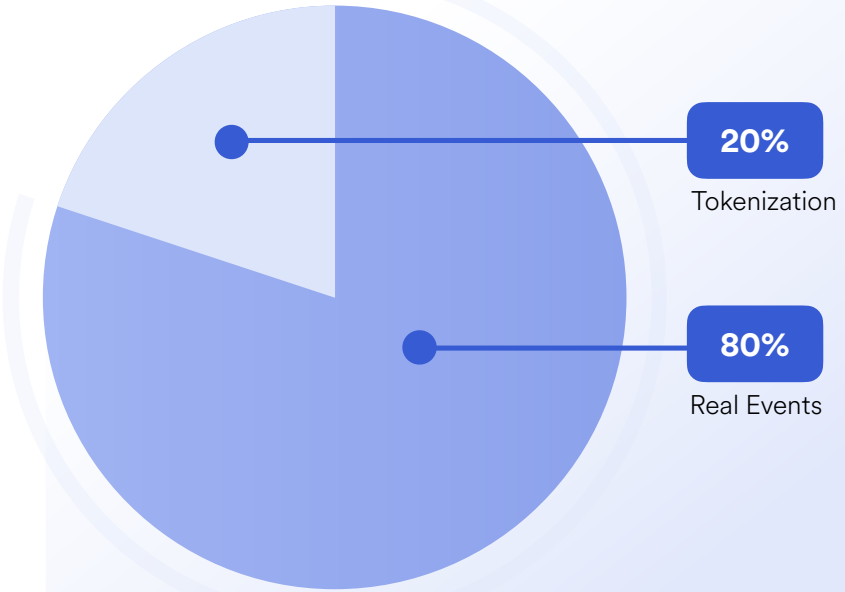
Redefining Smart Contracts With External Events

Current Distribution of Smart Contract Transaction Volume and Value Secured



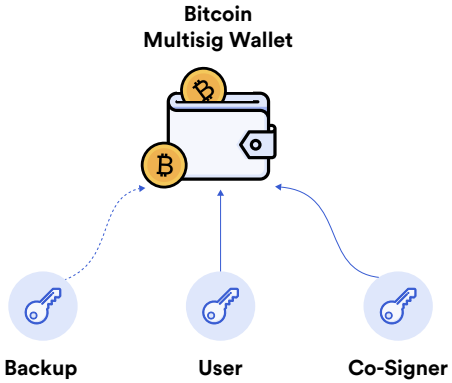
Externally Connected Contracts

Future Distribution and 1000%+ Growth of Transaction Volume and Value Secured



Chainlink

The Initial Leap Forward for Smart Contracts



Bitcoin Multi-signature as
“Programmable Money”

Protocol Smart Contracts =
Smart Contracts 1.0

Chainlink

The Scriptable Leap Forward for Smart Contracts

Protocol Smart Contracts =
Smart Contracts 1.0

```
pragma solidity ^0.4.16;

contract MyToken {
    // This creates an array with all balances
    mapping (address => uint256) public balanceOf;

    // Initializes contract with initial supply tokens to t
    function MyToken (
        uint256 initialSupply
    ) payable {
        balanceOf[msg.sender] = initialSupply;
    }

    // Send coins
    function transfer(address _to, uint256 _value) payable
        require(balanceOf[msg.sender] >= _value);
        require(balanceOf[_to] + _value >= balanceOf[_to]);
        balanceOf[msg.sender] -= _value;
        balanceOf[_to] += _value;
    }
```

Scriptable Smart Contracts =
Tokenization/Smart Contracts 2.0

Chainlink

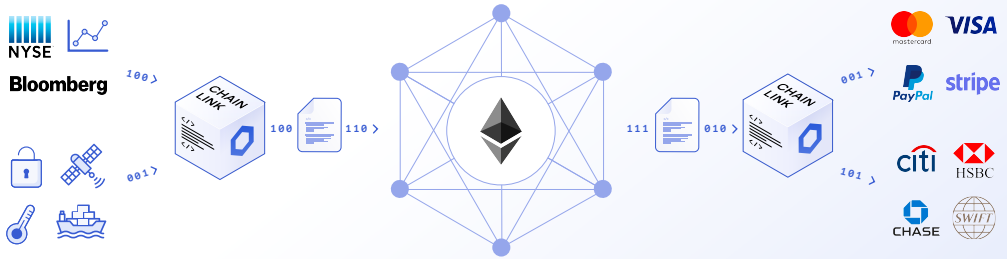
The Connectivity Leap Forward for Smart Contracts

```solidity
pragma solidity ^0.4.16;

contract MyToken {
    // This creates an array with all balances
    mapping (address => uint256) public balanceOf;

    // Initializes contract with initial supply tokens to t
    function MyToken (
        uint256 initialSupply
    ) payable {
        balanceOf[msg.sender] = initialSupply;
    }

    // Send coins
    function transfer(address _to, uint256 _value) payable
        require(balanceOf[msg.sender] >= _value);
        require(balanceOf[_to] + _value >= balanceOf[_to]);
        balanceOf[msg.sender] -= _value;
        balanceOf[_to] += _value;
    }
```



Scriptable Smart Contracts = Tokenization/Smart Contracts 2.0

Externally Connected Smart Contracts = All Other Dapps/Smart Contracts 3.0

Chainlink

DeFi is the Beginning of Redefining Smart Contracts

Total Value Locked (USD) in DeFi

DEFI PULSE

SYNTHETIX

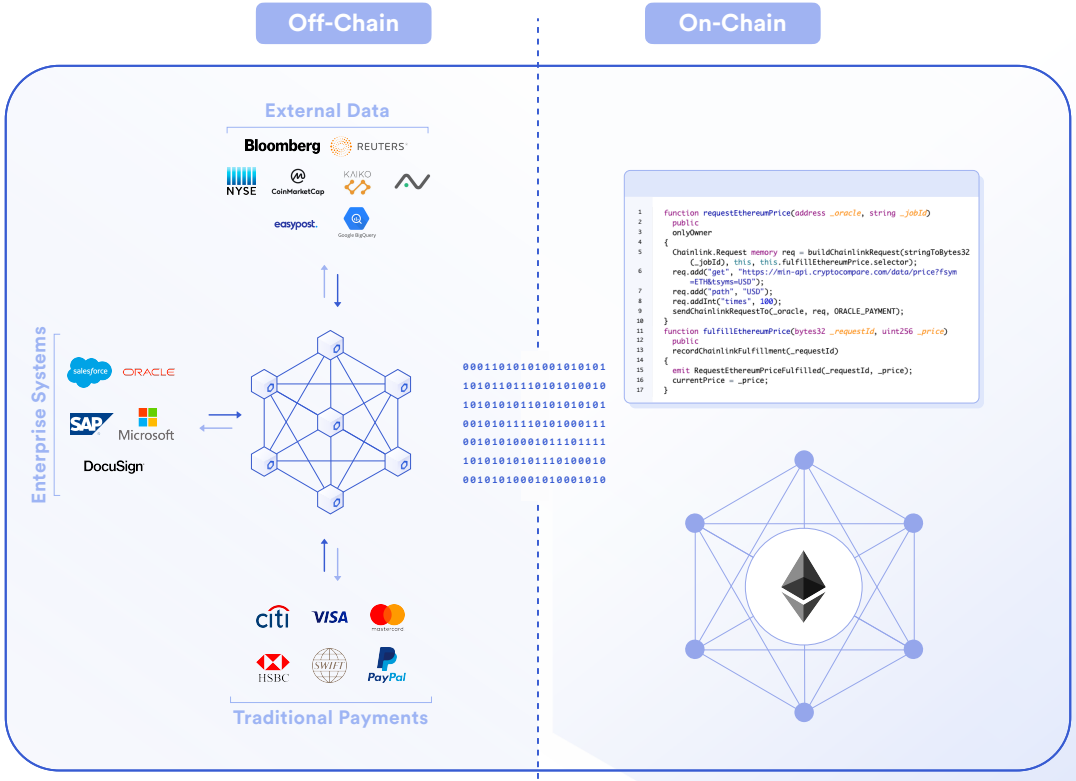
AAVE

bZx

Nexus Mutual

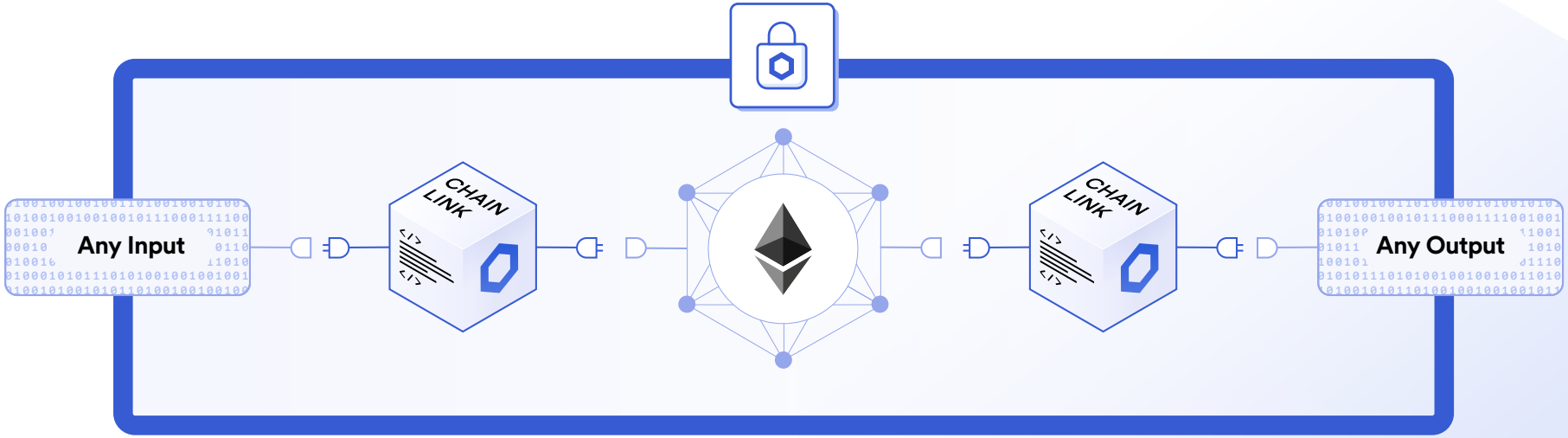
Chainlink

DeFi Smart Contracts Have Two Important Parts



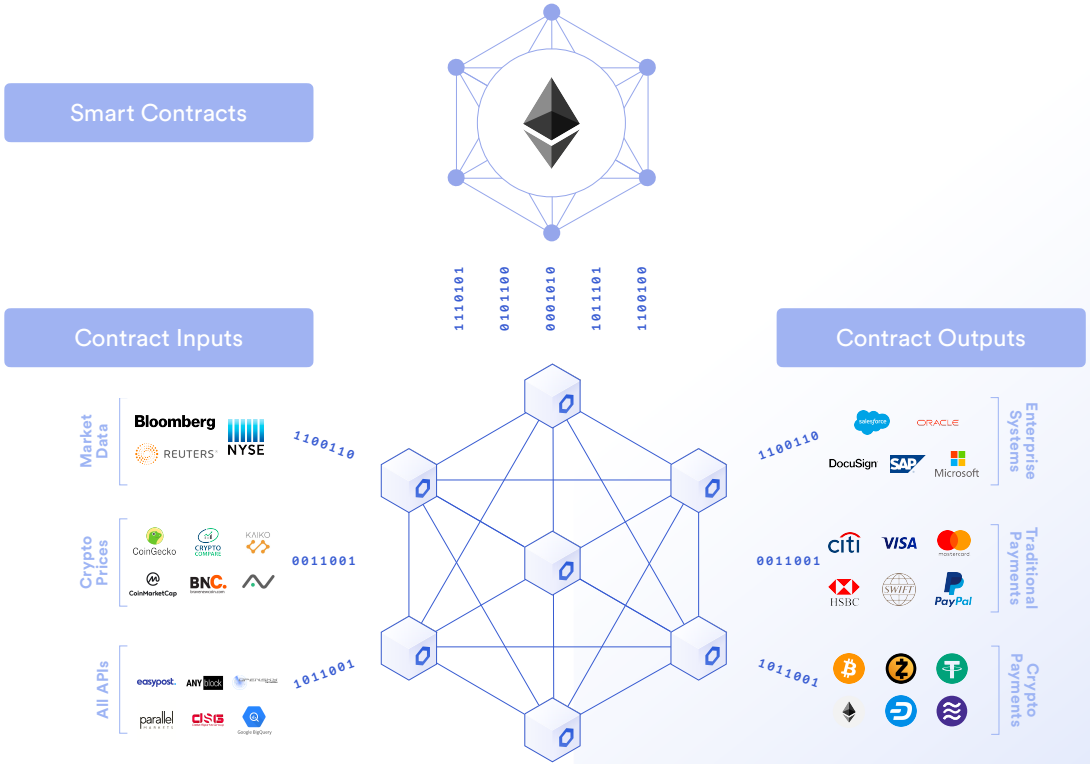
Chainlink

End-to-end Reliability Is The Promise of Smart Contracts



Chainlink

Connecting Any Blockchain to All Inputs and Outputs



Chainlink

Our Approach to Reliable & Secure Oracles for Web3

Decentralization of many
Independent/Sybil Resistant
Nodes into Oracle Networks

Chainlink

Our Approach to Reliable & Secure Oracles for Web3

Decentralization of many Independent/Sybil Resistant Nodes into Oracle Networks

Provably Secure Nodes that provide cryptographic proof of their overall security

Chainlink

Our Approach to Reliable & Secure Oracles for Web3

Decentralization of many Independent/Sybil Resistant Nodes into Oracle Networks

Provably Secure Nodes that provide cryptographic proof of their overall security

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

Chainlink

Our Approach to Reliable & Secure Oracles for Web3

Decentralization of many Independent/Sybil Resistant Nodes into Oracle Networks

Provably Secure Nodes that provide cryptographic proof of their overall security

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

Cryptoeconomic Security using binding service agreements to generate staking penalties

Chainlink

Our Approach to Reliable & Secure Oracles for Web3

Decentralization of many Independent/Sybil Resistant Nodes into Oracle Networks

Provably Secure Nodes that provide cryptographic proof of their overall security

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

Cryptoeconomic Security using binding service agreements to generate staking penalties

Defense in Depth, applying multiple layers of security (TEEs, ZK)

Chainlink

Our Approach to Reliable & Secure Oracles for Web3

Decentralization of many Independent/Sybil Resistant Nodes into Oracle Networks

Provably Secure Nodes that provide cryptographic proof of their overall security

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

Cryptoeconomic Security using binding service agreements to generate staking penalties

Defense in Depth, applying multiple layers of security (TEEs, ZK)

A Large Open Source Community of Node Operators, Developers, Researchers and Security Auditors

Chainlink

Our Approach to Reliable & Secure Oracles for Web3

Decentralization of many Independent/Sybil Resistant Nodes into Oracle Networks

Provably Secure Nodes that provide cryptographic proof of their overall security

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

Cryptoeconomic Security using binding service agreements to generate staking penalties

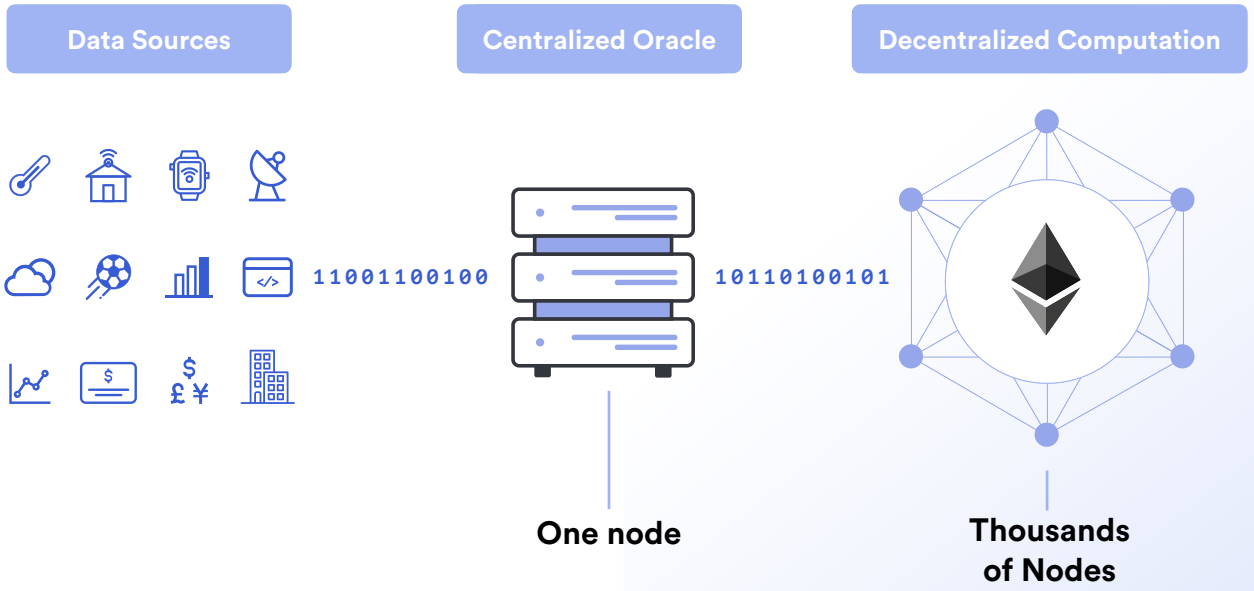
Defense in Depth, applying multiple layers of security (TEEs, ZK)

A Large Open Source Community of Node Operators, Developers, Researchers and Security Auditors

Connecting any blockchain environment to all inputs and outputs
Connected to the leading public and private blockchains. Accelerating what developers can build and the amount of places data can be sold on-chain.

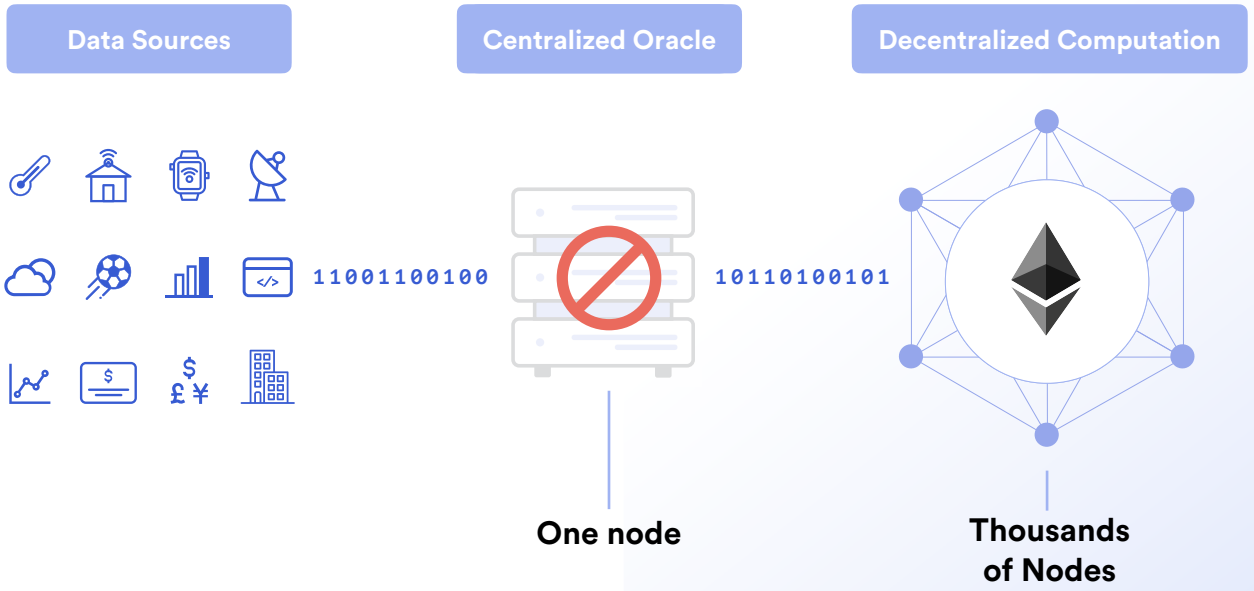
Chainlink

Centralized Oracles are a Point of Failure



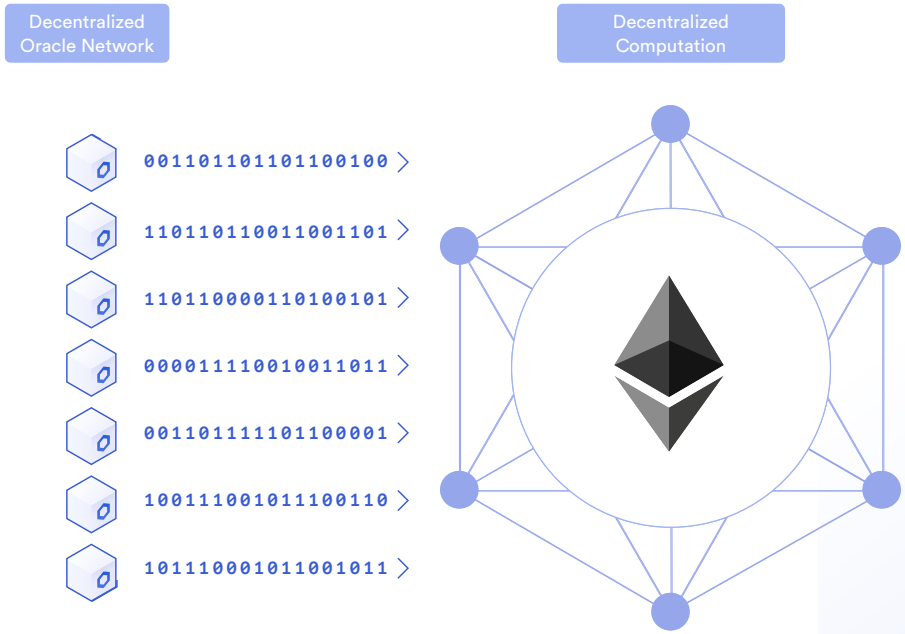
Chainlink

Centralized Oracles are a Point of Failure



Chainlink

A Decentralized Oracle Network



Decentralization

Full replicas being run by independent and sybil resistant node operators, coming to consensus about a computation.

Focused on data validation and consensus about individual off-chain values to make them reliable enough to trigger contracts.

Node Operators are security reviewed, can provide a proven performance history and are high quality and highly sybil resistant.

Data Quality is Important: Garbage In, Garbage Out

Unpaid/Free Lower Quality API

- Low Quality Data
- Unreliable Responses
- No Quality Guarantees

`10101110101011111011`

A Node Without Credential Management

`01010001101001010 11`

Smart Contract With Bad Data

Chainlink

Credentials are a Requirement for Premium Data Sources

Unpaid/Free Lower Quality API

- Low Quality Data
- Unreliable Responses
- No Quality Guarantees

`1010111010101111011`

A Node Without Credential Management

`0101000110100101011`

Smart Contract Broken with Bad Data

Paid/Premium APIs

- High Quality Data
- Highly Responsive
- Quality Guarantees

`1010111010101111011`

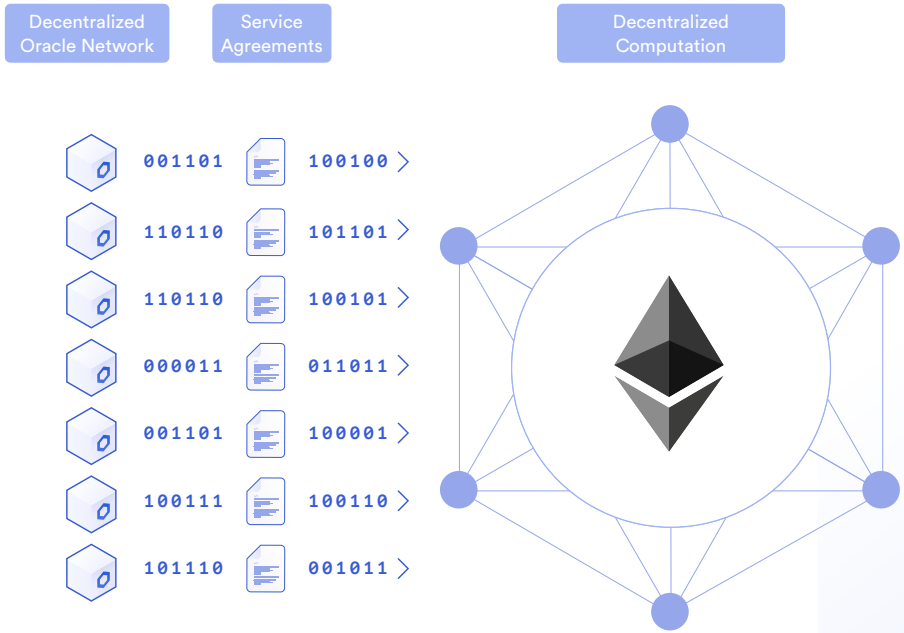
Chainlink Nodes With Premium API Credentials

`0101000110100101011`

Smart Contract Using Quality Data

Chainlink

Binding Commitments by Oracles to Contracts



Binding Service Agreements

Technically enforced commitments to meeting high security and data quality standards are made on-chain by the oracle, committing them to high levels of quality.

Both the commitment and the final performance of the commitment are both on-chain and fully verifiable.

Creating a cryptographically provable performance history that can be relied on. Oracles that don't fulfill their commitments won't be selected for future quoroms, losing large future revenue.

Chainlink

On-chain Service Agreements Provide Guarantees

Data Providers

Chainlink Node

- High Quality Data
- Highly Responsive
- Quality Guarantees

1010110111

1010110111

On- chain Service Agreement

1001010010100101001010

- Defined Data Delivery Parameters
- Defined Data Quality Parameters
- Quality Connected to Payment

Smart Contract with High Quality Data

Chainlink

On-chain Service Agreements Provide Guarantees

Data Providers

ALPHA VANTAGE · KAIKO · amberdata.io · CoinMarketCap · CoinGecko · Google BigQuery · CRYPTO COMPARE · BNC. · JSECOIN · BINANCE · ANYblock · easypost. · parallel MARKETS · CONSTELLATION · DLG · coti · FLCA · streamr · TRADE · RANDOM.ORG · fabr(x)

- High Quality Data
- Highly Responsive
- Quality Guarantees

1010110111

Chainlink Node

1010110111

On- chain Service Agreement

10010100101001010010

- Defined Data Delivery Parameters
- Defined Data Quality Parameters
- Data Quality Connected to Payment

Smart Contract with High Quality Data

Unpaid/Free OpenAPI

- Low Quality Data
- Unreliable Responses
- No Quality Guarantees

1010111010101111011

A Node Without Credential Management

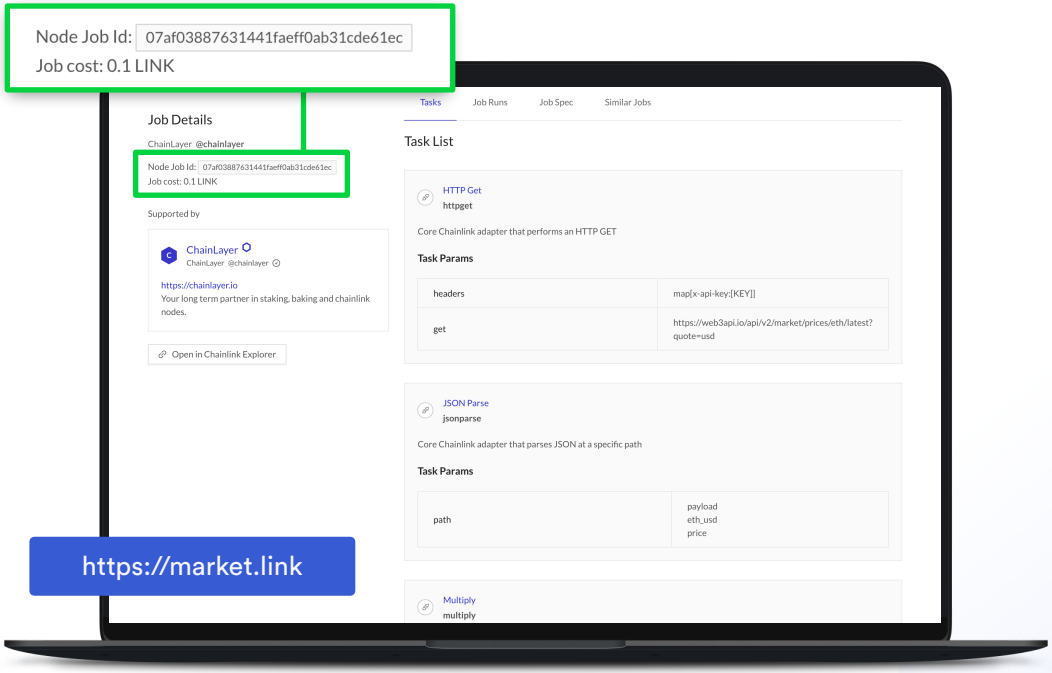
- Undefined Data Delivery Terms
- Undefined Data Quality Terms
- No Data Quality Guarantees

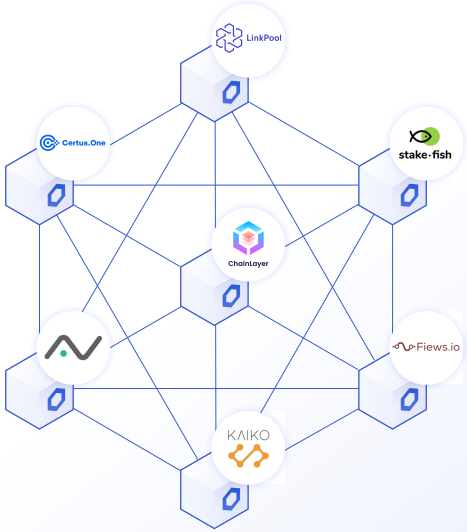
101011001 0 1 0 0

Smart Contract With No Data Delivered

Chainlink

Clearly Defined Data Quality

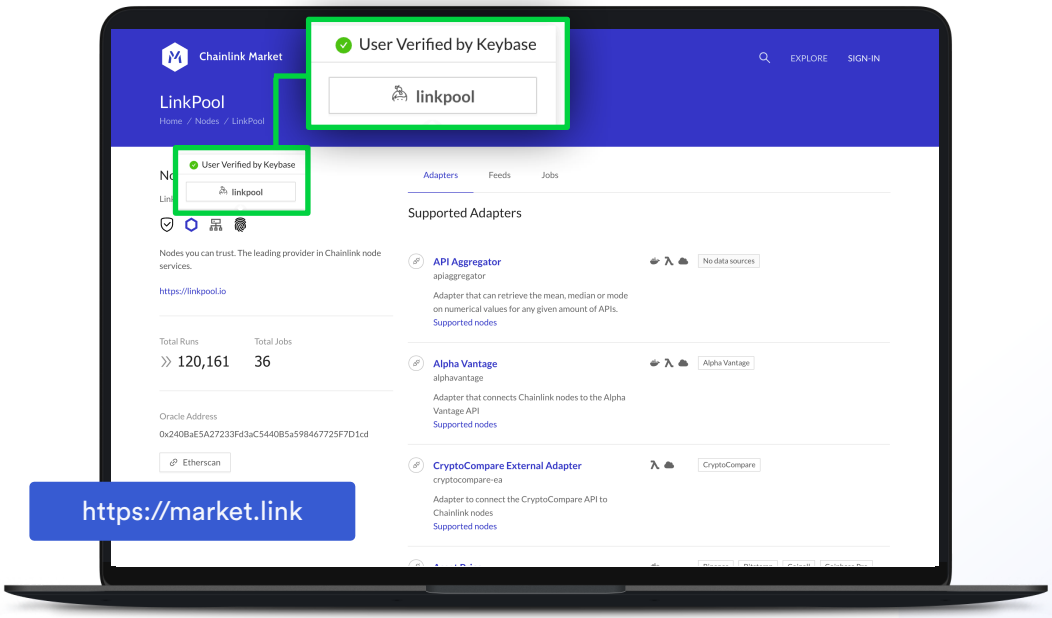


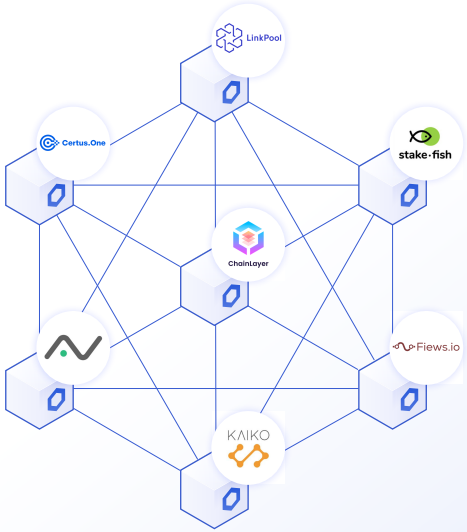


- Define How Data is Retrieved
- Rely on High Quality Data and Nodes
- Greater Revenue from Better Performance
- Users Avoid Security Through Obscurity

Chainlink

Informed Decisions about Nodes

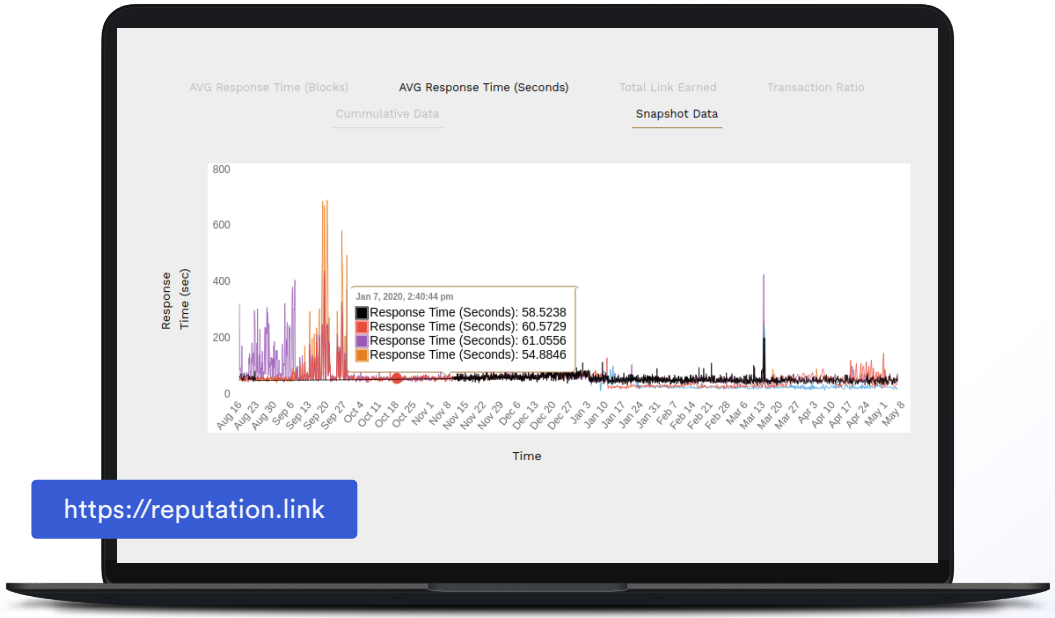




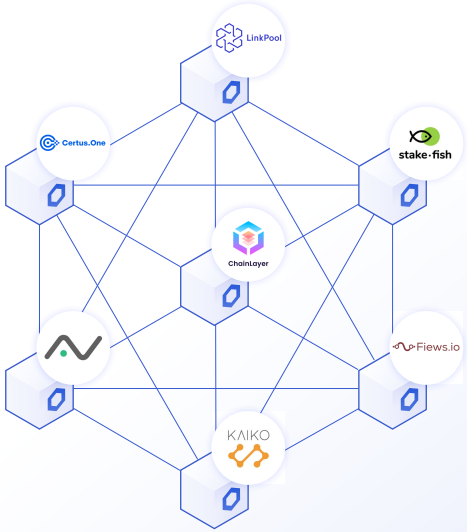
- Informed Decisions About Node Operators
- Cryptographically Provable Performance
- Greater Revenue from Better Performance
- Users Avoid Security Through Obscurity

Chainlink

A Provable Performance History



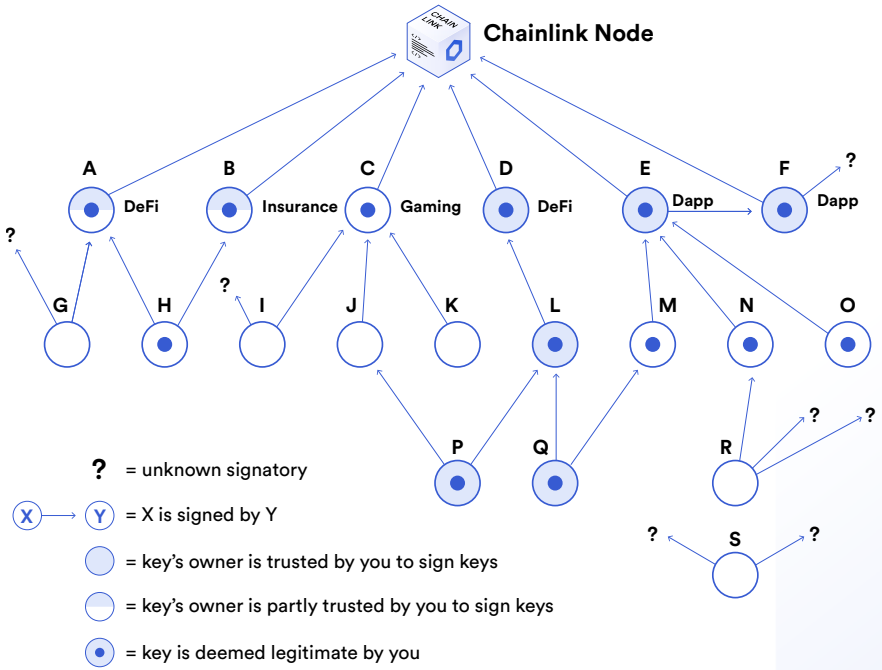
https://reputation.link



- Informed Decisions About Node Operators
- Cryptographically Provable Performance
- Greater Revenue from Better Performance
- Users Avoid Security Through Obscurity

Chainlink

A “Web of Trust” Grows to Prove a Nodes Security



Provable Security for Nodes

Aggregating provable security data across chains

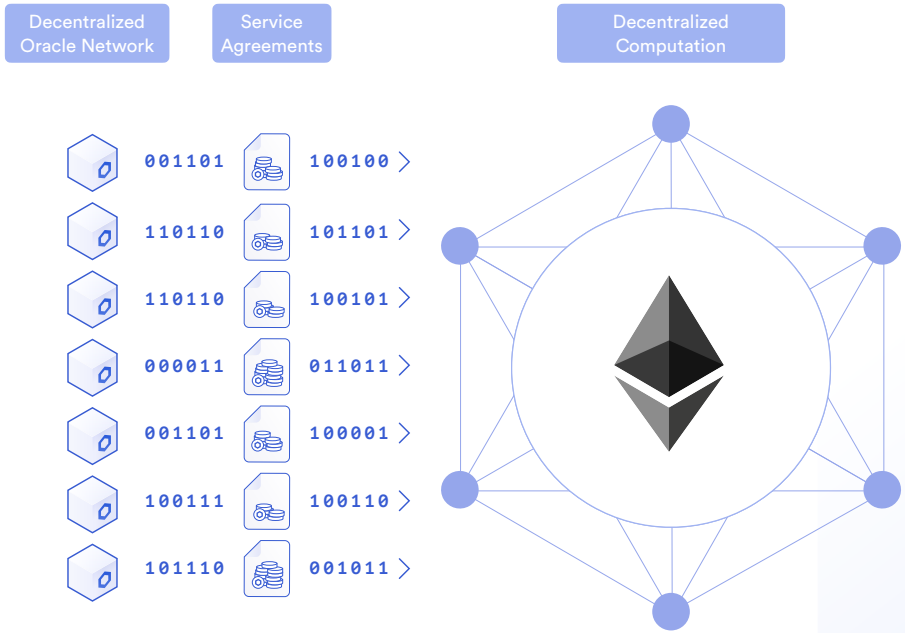
Usage by multiple real Dapps is a signal of trust

Multiple highly used, and reputation sensitive nodes make a stronger network

Sybil resistance improved by being able to prove full independence from users.

Chainlink

Crypto-economic Security from Staking



Cryptoeconomic Security from Staking

Using the commitments from binding service agreements, we can define clear parameters for the penalties for misbehaving nodes, bad data providers and any other point in the data origination and/or data transfer process.

Staking ensures that there is a penalty for node misbehavior, data inaccuracy and any other key condition specified in an on-chain binding service agreement. Staking guarantees are not only very specific and expandable, to properly manage new risks as they appear, but the amount of stake can be increased as value secured by an oracle rises.

Crypto-economic Security from Staking

Data Providers

ALPHA VANTAGE · KAIKO · amberdata.io · CoinMarketCap · CoinGecko · Google BigQuery · CRYPTO COMPARE · BNC. · JSECOIN · BINANCE · ANYblock · easypost. · parallel MARKETS · CONSTELLATION · DSG · coti · FLCA · streamr · TRADE · RANDOM.ORG · fabr(x)

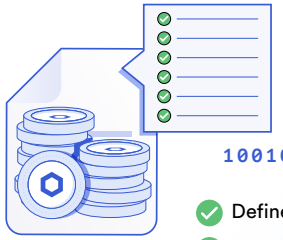
- High Quality Data
- Highly Responsive
- Quality Guarantees

1010110111

Chainlink Node

1010110111

Service Agreement



1001010010100101010

- Defined Data Delivery Parameters
- Defined Data Quality Parameters
- Quality Connected to Payment

Smart Contract with High Quality Data

Unpaid/Free OpenAPI

- Low Quality Data
- Unreliable Responses
- No Quality Guarantees

1010111010101111011

A Node Without Credential Management

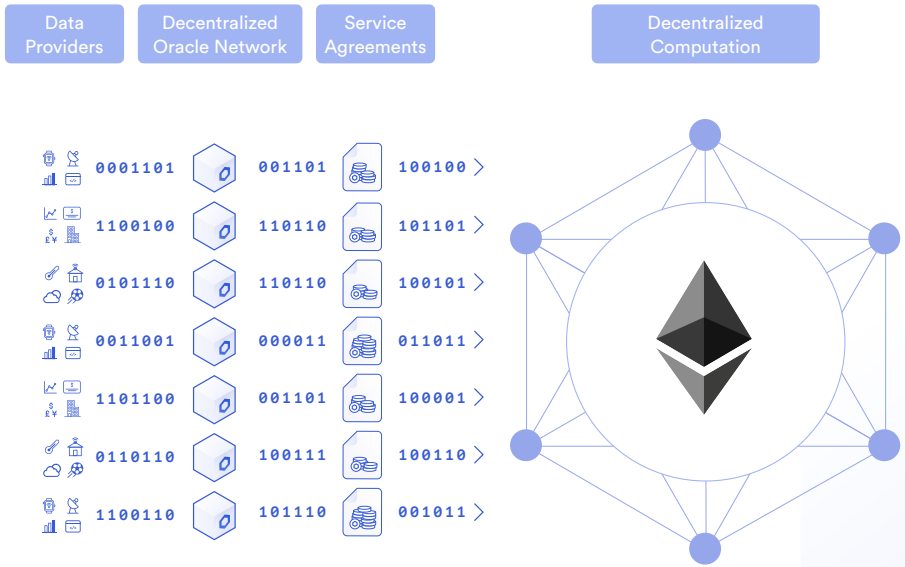
- Undefined Data Delivery Terms
- Undefined Data Quality Terms
- No Data Quality Guarantees

101011001 0 1 0 0

Smart Contract Broken by Bad Data

Chainlink

Decentralization at the Data Source Level

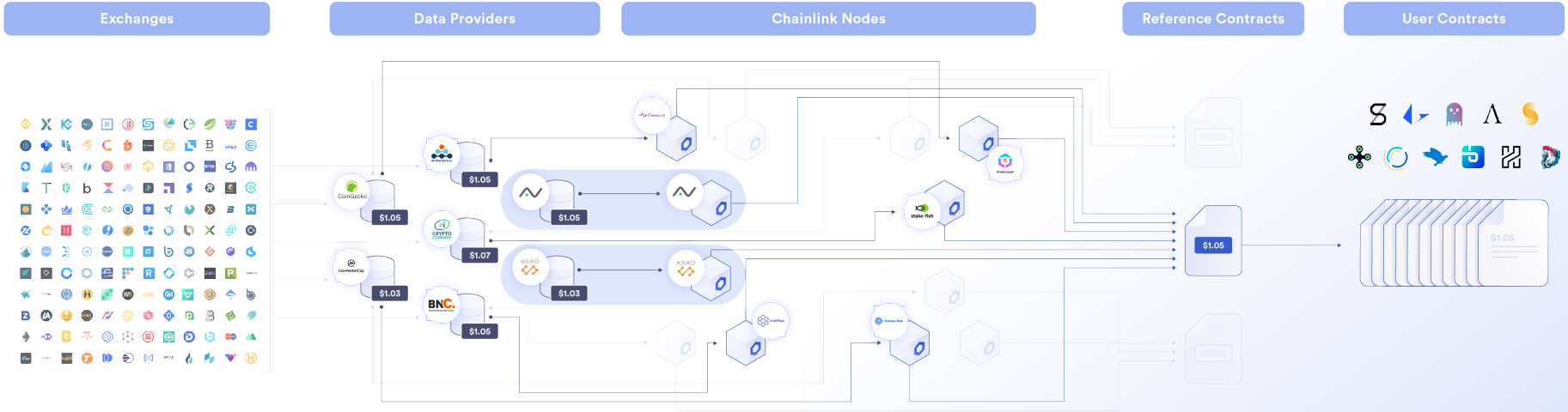


Highly Validated Data

Decentralization at the middleware layer enables the inclusion of multiple secured data sources

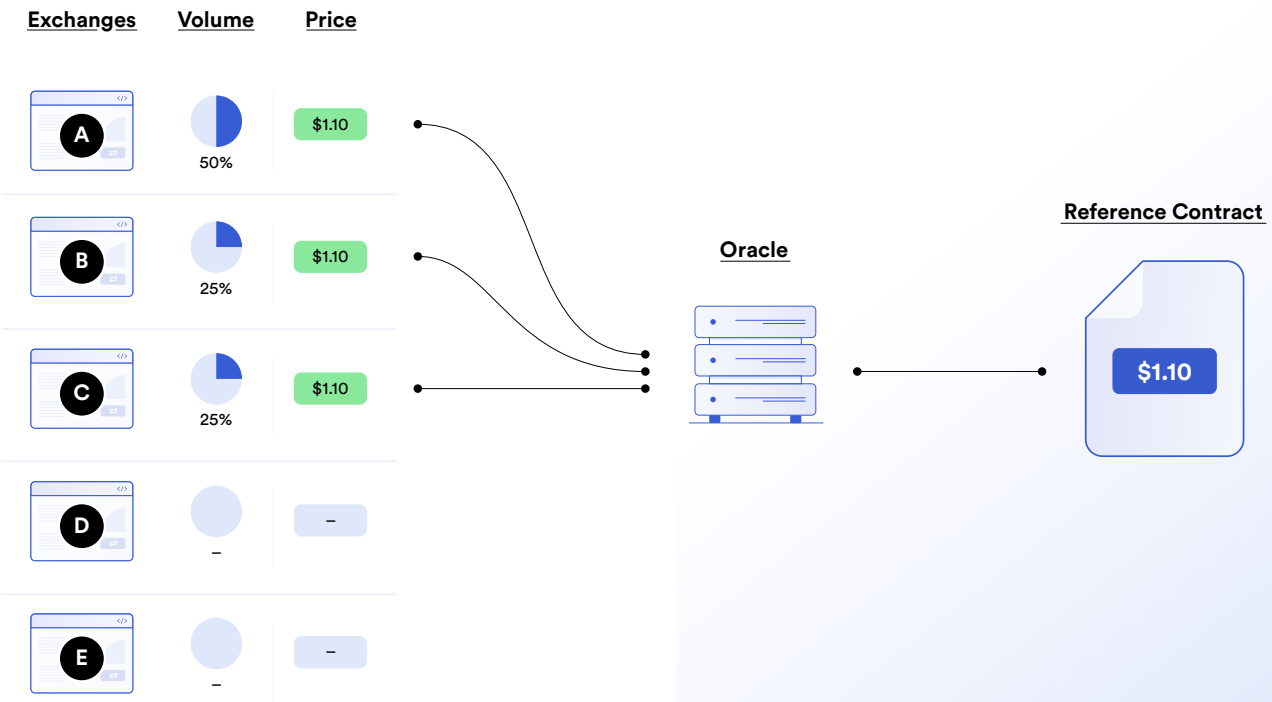
Pre-made Chainlinks make it easy to build multiple data sources into your smart contract, with data quality grantees and data delivery guarantees from node operators built in.

Truly Decentralized Finance via Decentralized Oracles



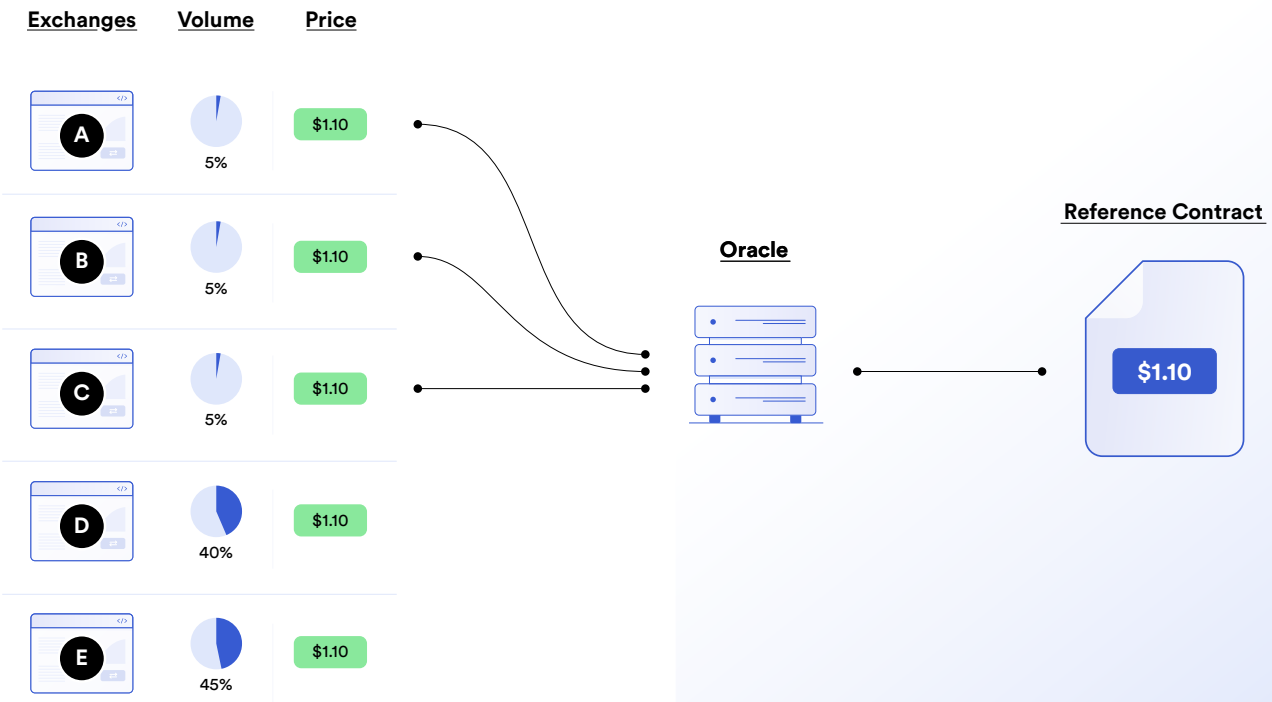
Chainlink

Proper Market Coverage is a Key Part of Data Quality



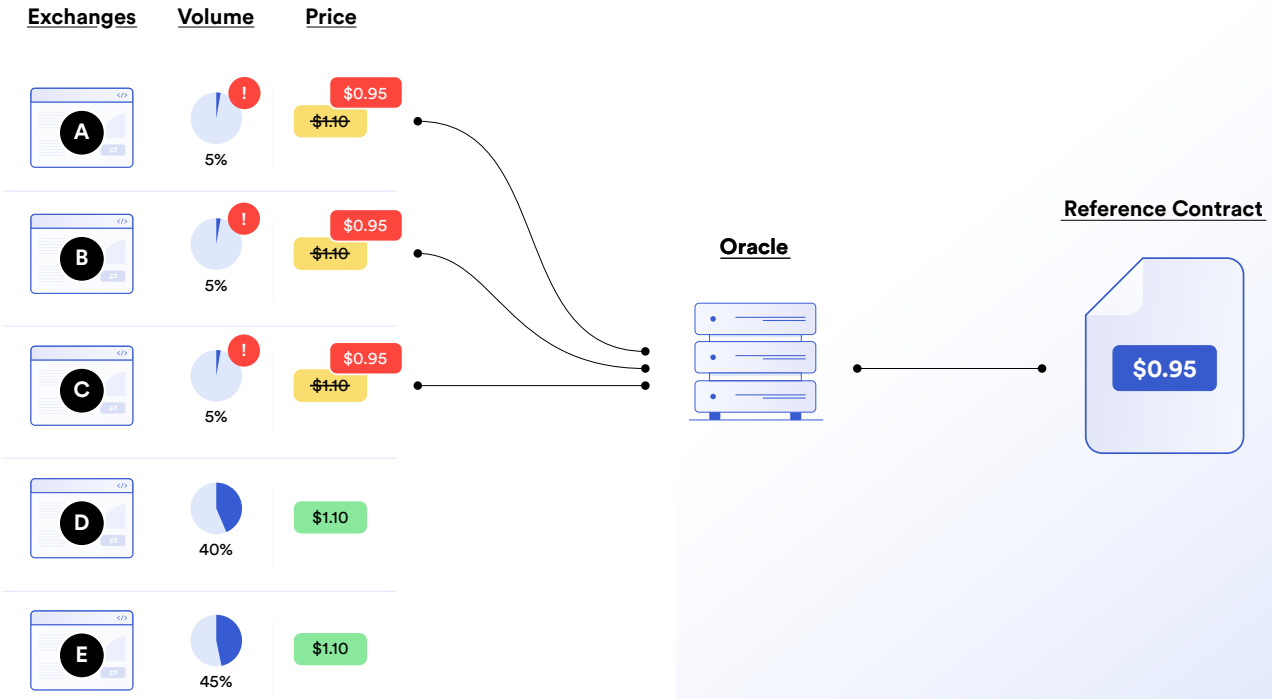
Chainlink

Proper Market Coverage is a Key Part of Data Quality



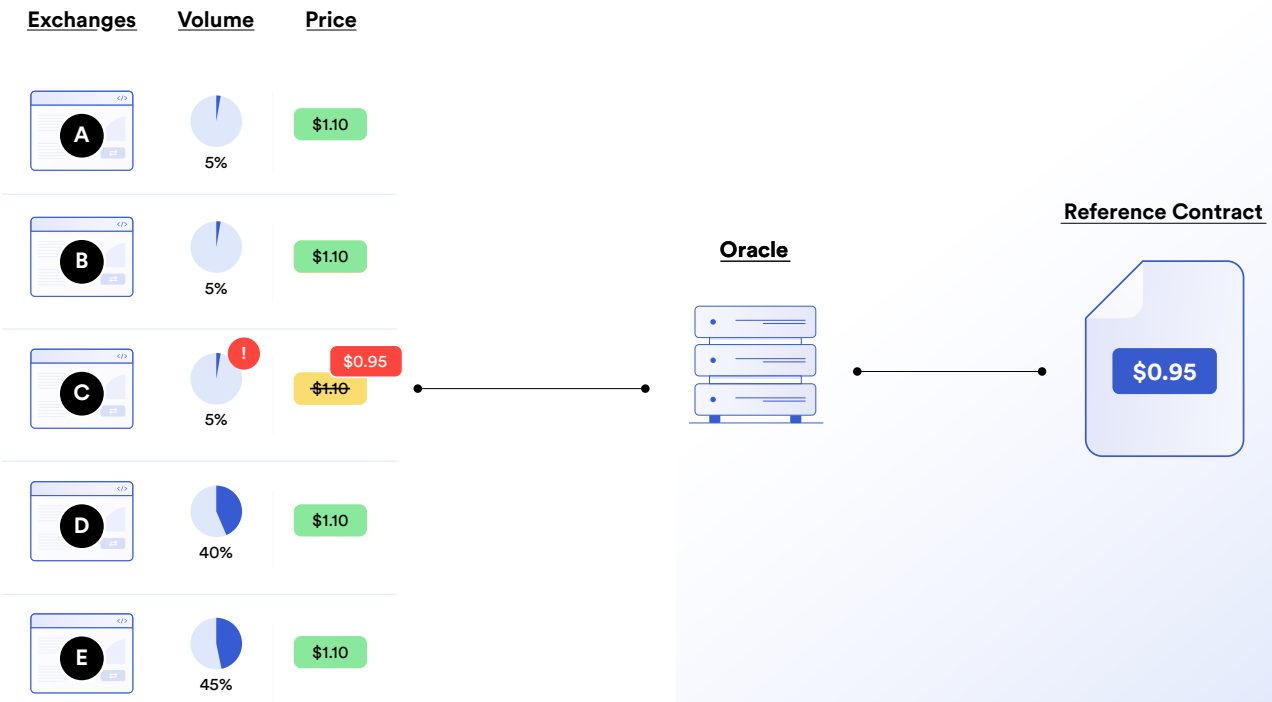
Chainlink

Proper Market Coverage is a Key Part of Data Quality



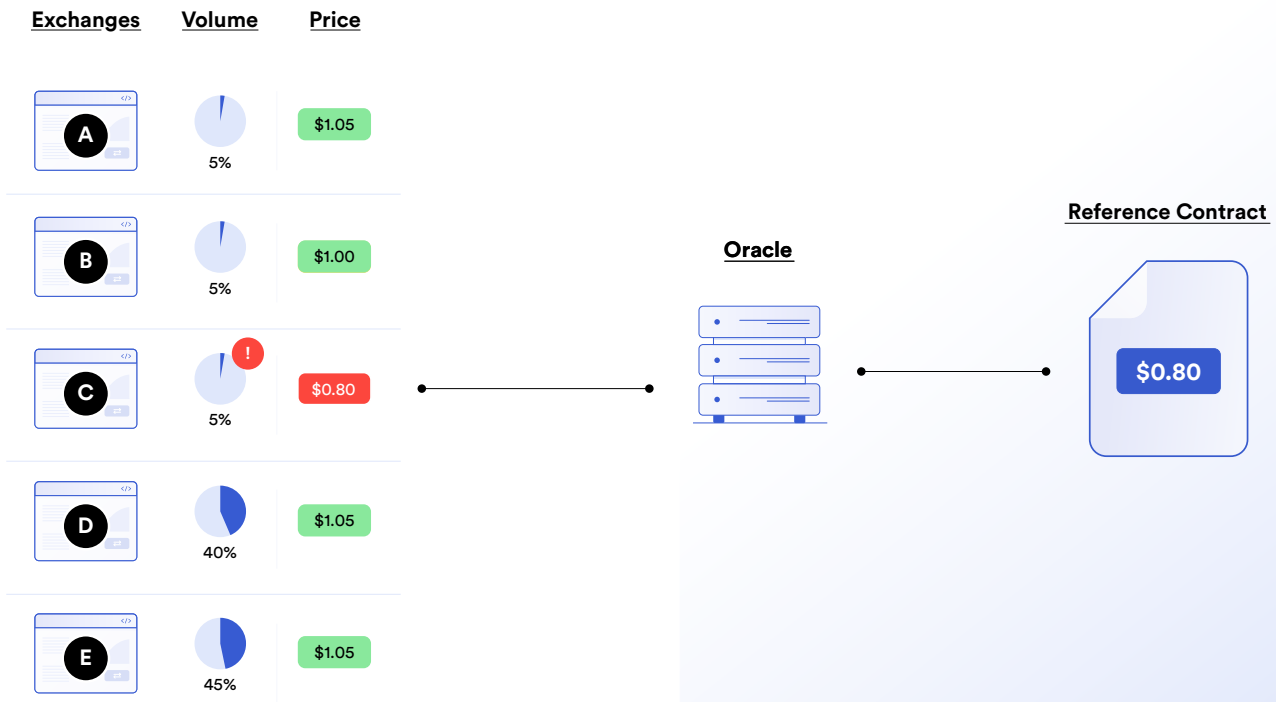
Chainlink

Proper Market Coverage is a Key Part of Data Quality



Chainlink

Using Any One Exchange for Price Data is a Large Risk



Chainlink

Price Data Calculation Methodologies Can Vary Greatly

Volume Weighted Average Price

$$P_{\mathrm{VWAP}} = \frac{\sum_j P_j \cdot Q_j}{\sum_j Q_j}$$

$79

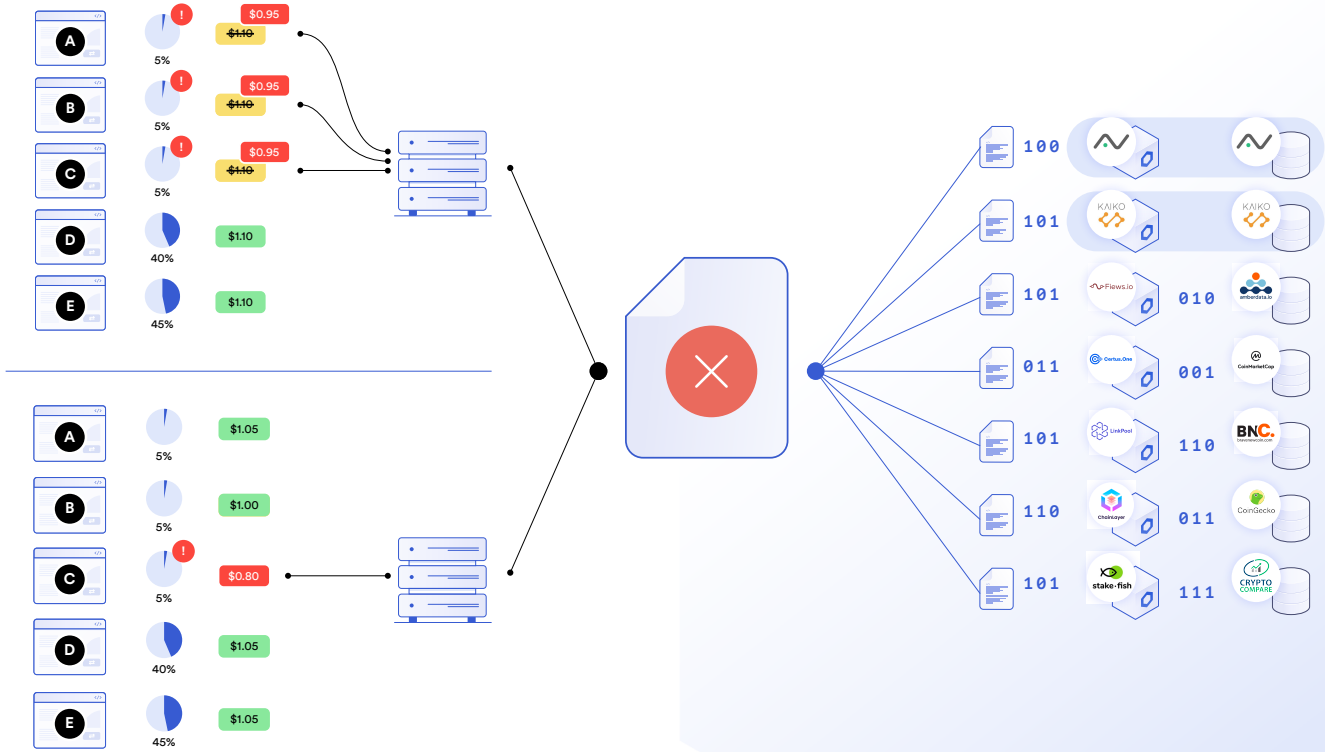
Time Weighted Average Price

$$p_{t_1,t_2} = \frac{\sum_{i=t_1}^{t_2} p_i}{t_2 - t_1}$$

$125

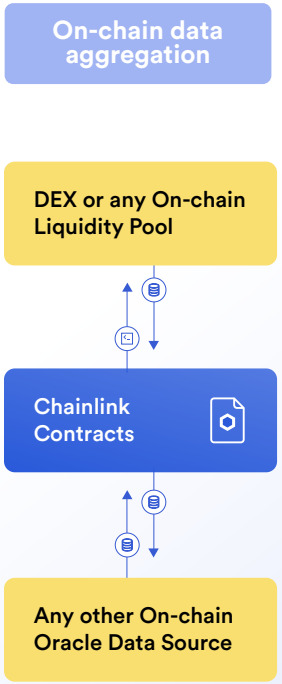
Chainlink

Low Quality Data + High Quality = Lower Data Quality



Chainlink

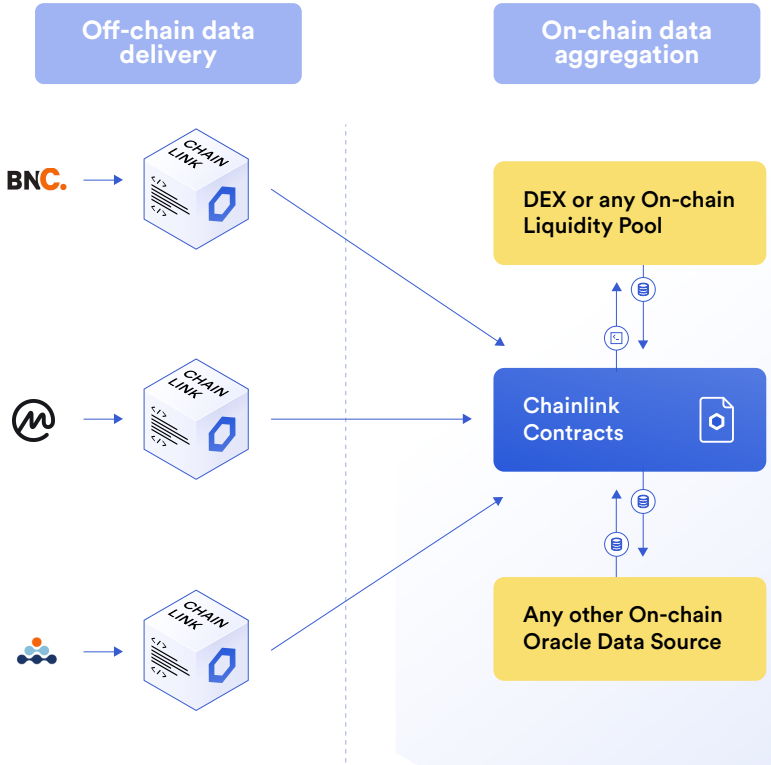
Chainlink's Meta Oracle Can Combine Data if Needed



https://blog.chain.link/introducing-chainlinks-meta-oracle-capabilities-for-defi/

Chainlink

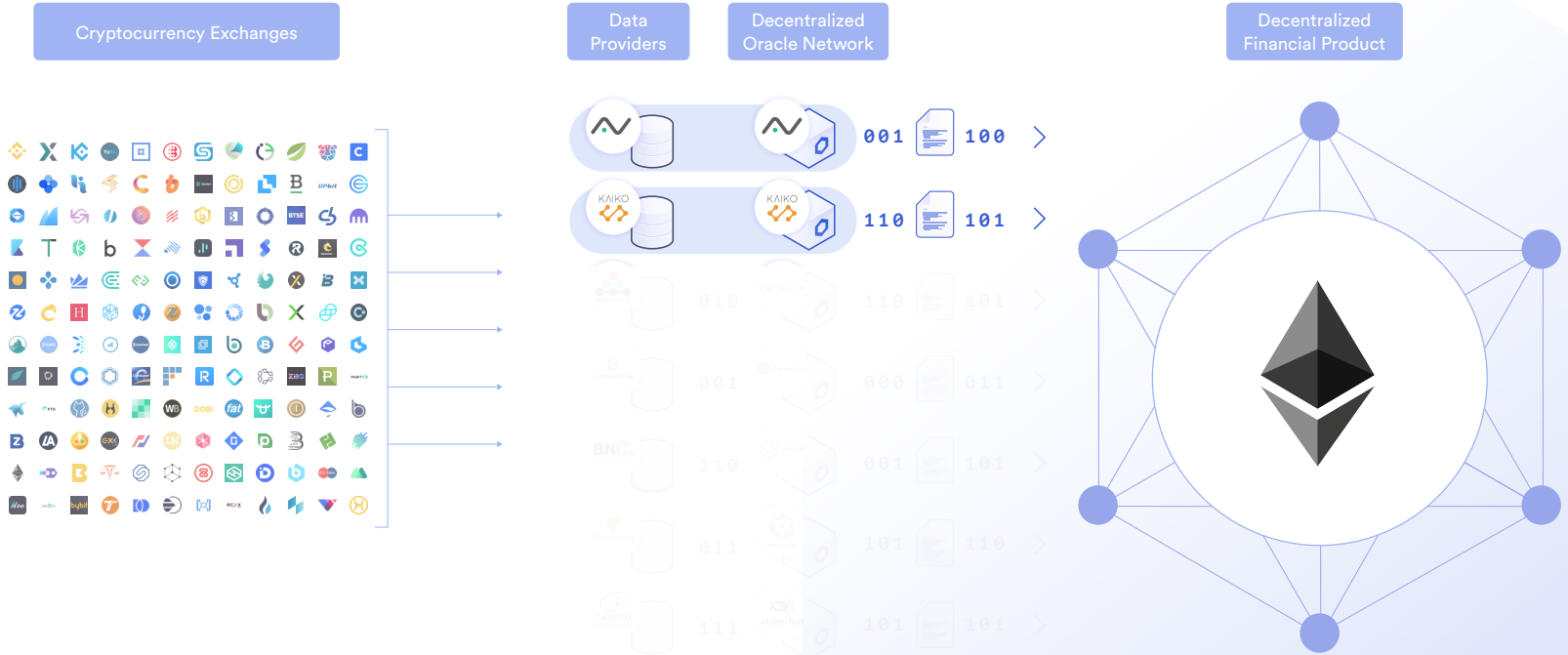
Chainlink's Meta Oracle Can Combine Data if Needed



https://blog.chain.link/introducing-chainlinks-meta-oracle-capabilities-for-defi/

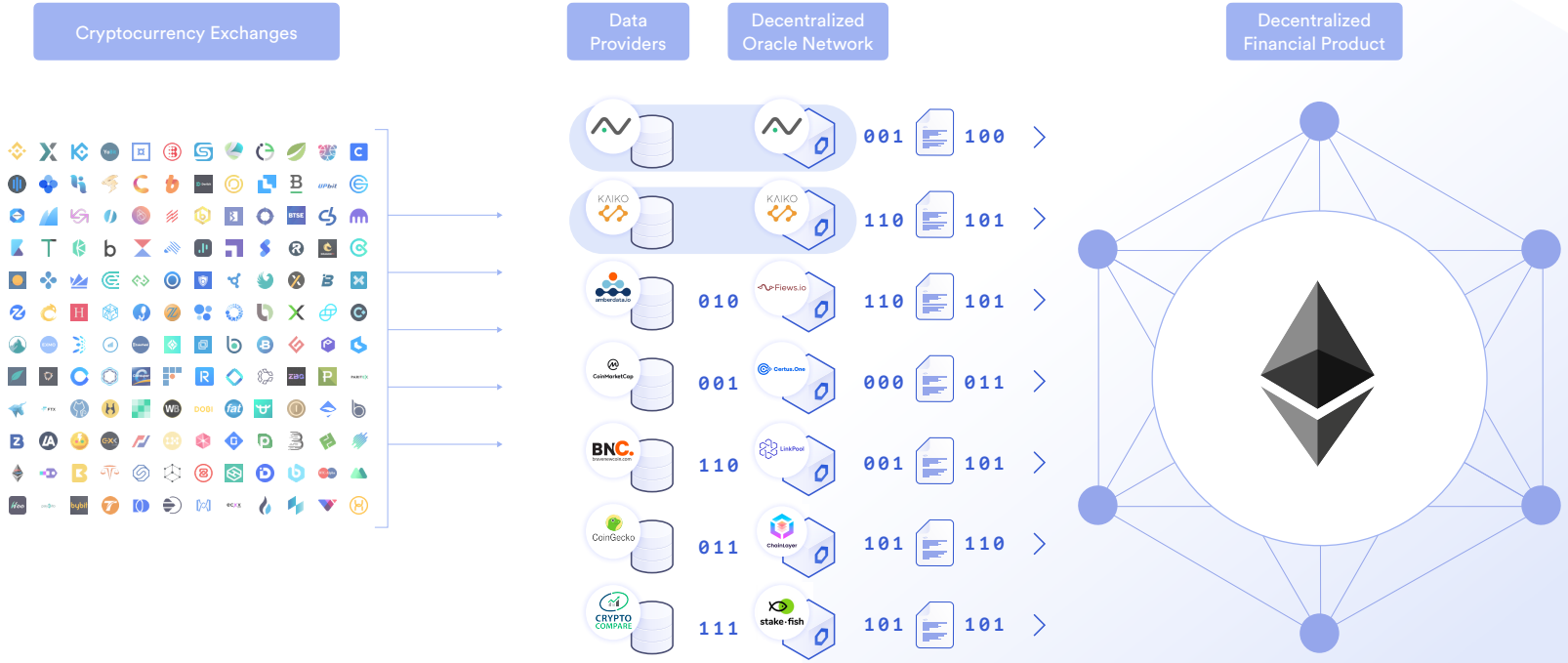
Chainlink

Truly Decentralized Finance via Decentralized Oracles

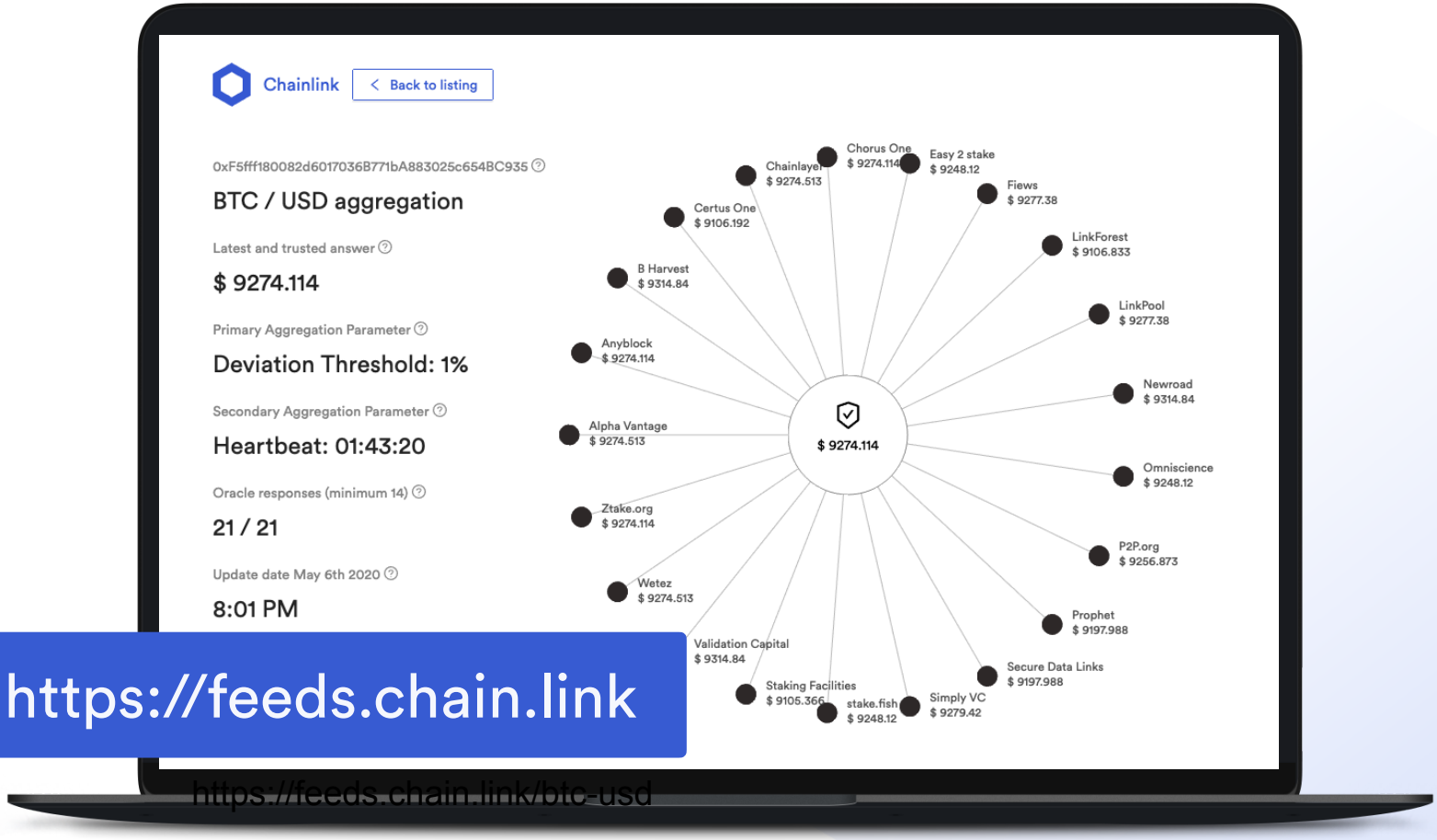


Chainlink

Truly Decentralized Finance via Decentralized Oracles



Chainlink

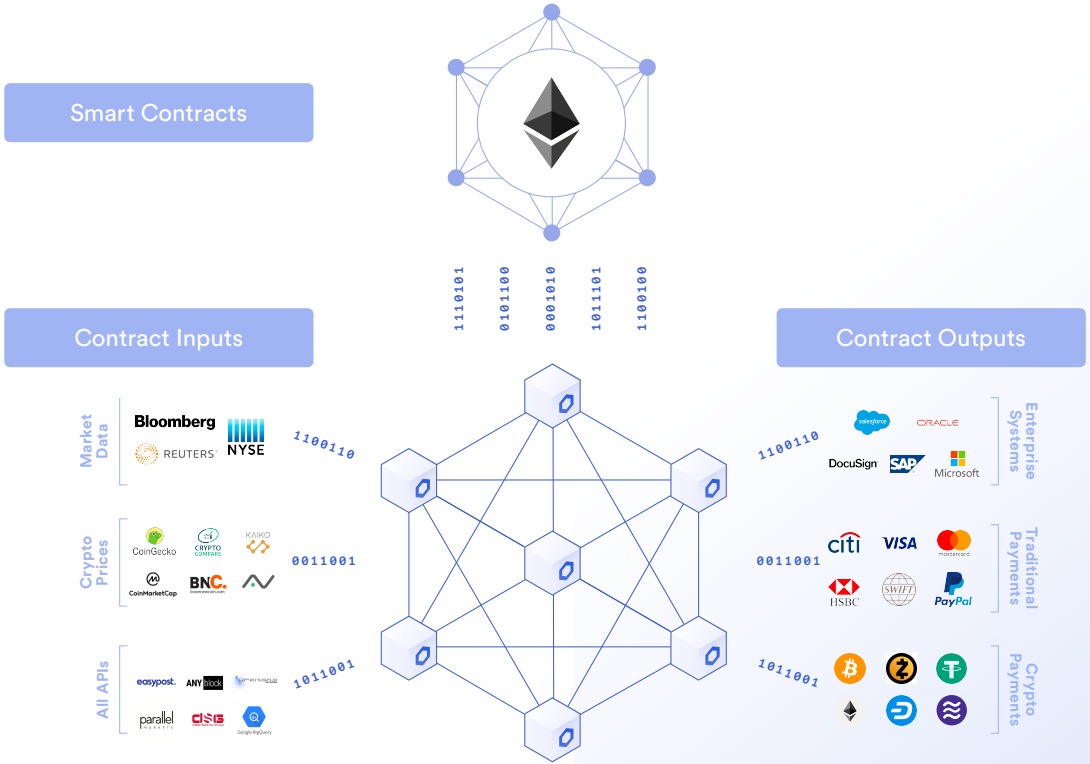


https://feeds.chain.link

https://feeds.chain.link/btc-usd

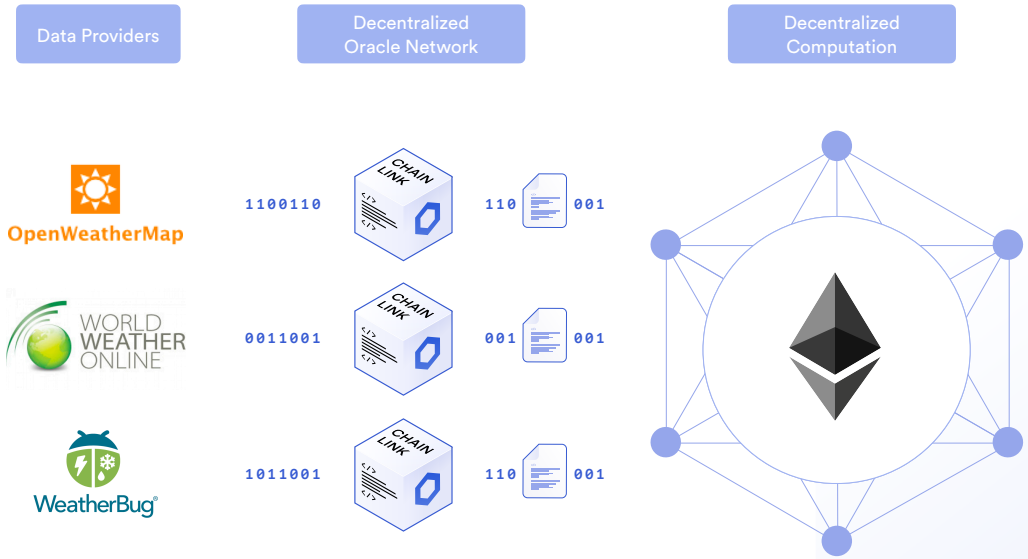
Chainlink

Connecting Any Blockchain to All Inputs and Outputs



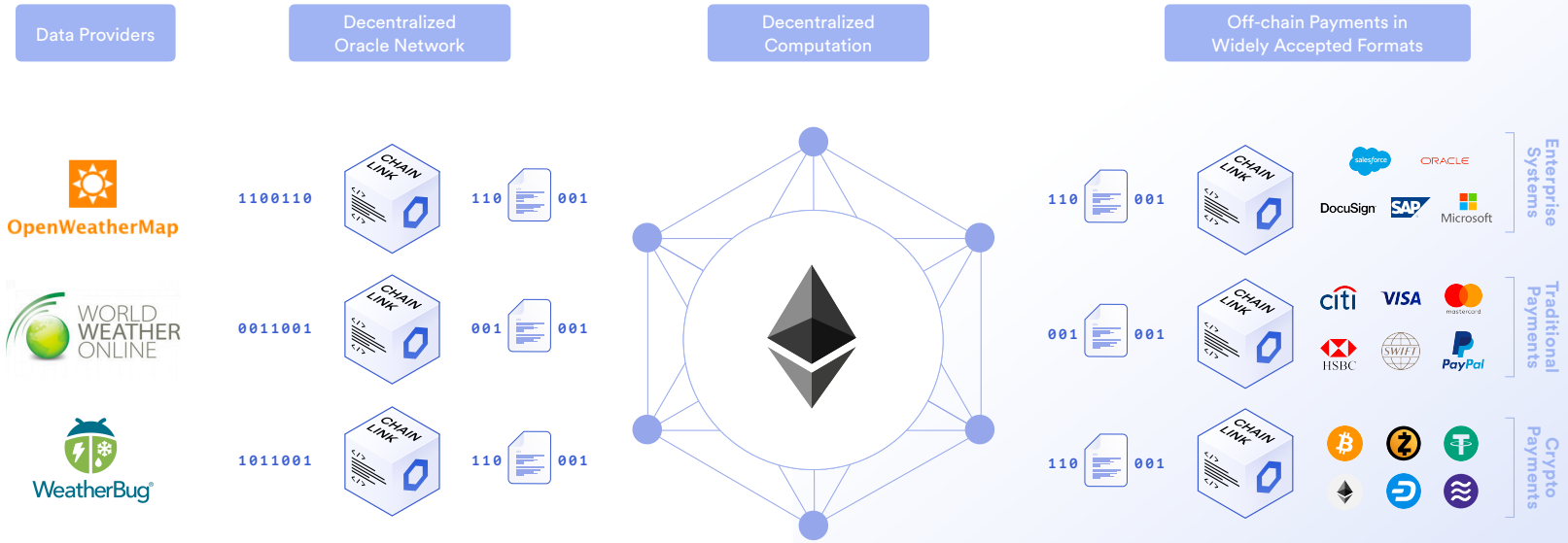
Chainlink

Smart Contract Crop Insurance with Decentralized Oracles



Chainlink

Smart Contract Crop Insurance with Decentralized Oracles



Chainlink

Join Our Team

Build great open source software that enables the next generation of DeFi and many other smart contract types.

We're an idea meritocracy where the best ideas win.

We're a remote team working with great people all over the world.

careers.chain.link

Chainlink

Thank You

Disclaimer: This presentation is for informational purposes only and contains statements about the future, including anticipated programs and features, developments, and timelines for the rollout of these programs and features. These statements are only predictions and reflect current beliefs and expectations with respect to future events; they are based on assumptions and are subject to risk, uncertainties, and change at any time. There can be no guarantee that any of the contemplated programs or features will be implemented as specified nor any assurance that actual results will not differ materially from those expressed in these statements, although we believe them to be based on reasonable assumptions. All statements are valid only as of the date first presented. The statements in this presentation also may not reflect future developments due to user feedback or later events and we may not update this presentation in response.

Chainlink