Chainlink

The Evolution of Smart Contracts and Cryptoeconomic Security

What is a Contract and What is its Purpose?

Contract:

A binding agreement between two or more persons or parties.

Merriam-Webster

Contract:

A legal document that states and explains a formal agreement between two different people or groups.

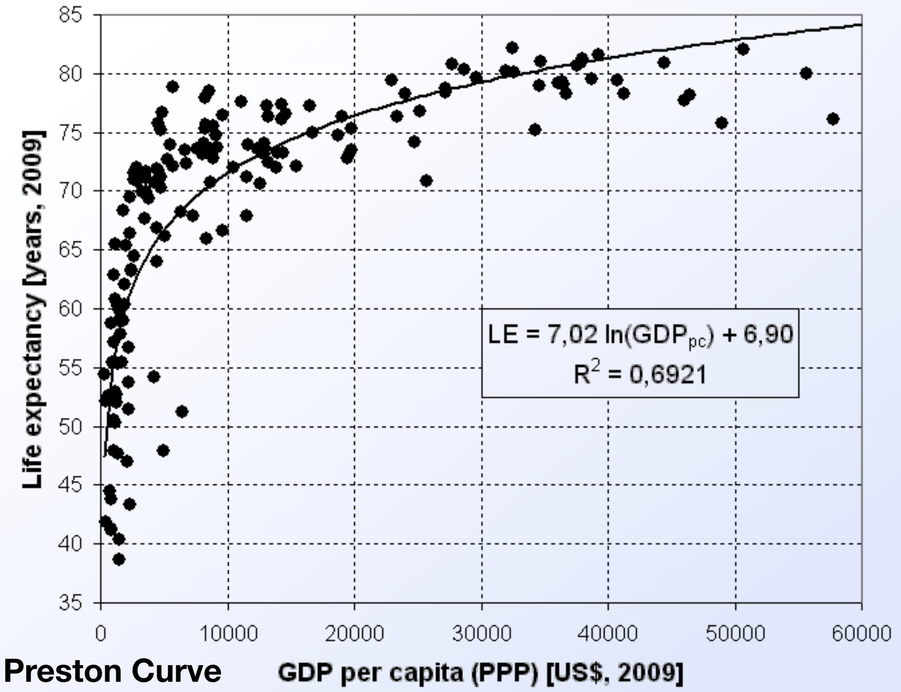
Cambridge Dictionary

Chainlink

The Social Contract: The Foundation of Our Society

Signing the Mayflower Compact 1620, by Jean Leon Gerome Ferris, 1899

"Where no law ... the life of man, solitary, poor, nasty, brutish and short." ~ *Thomas Hobbes*

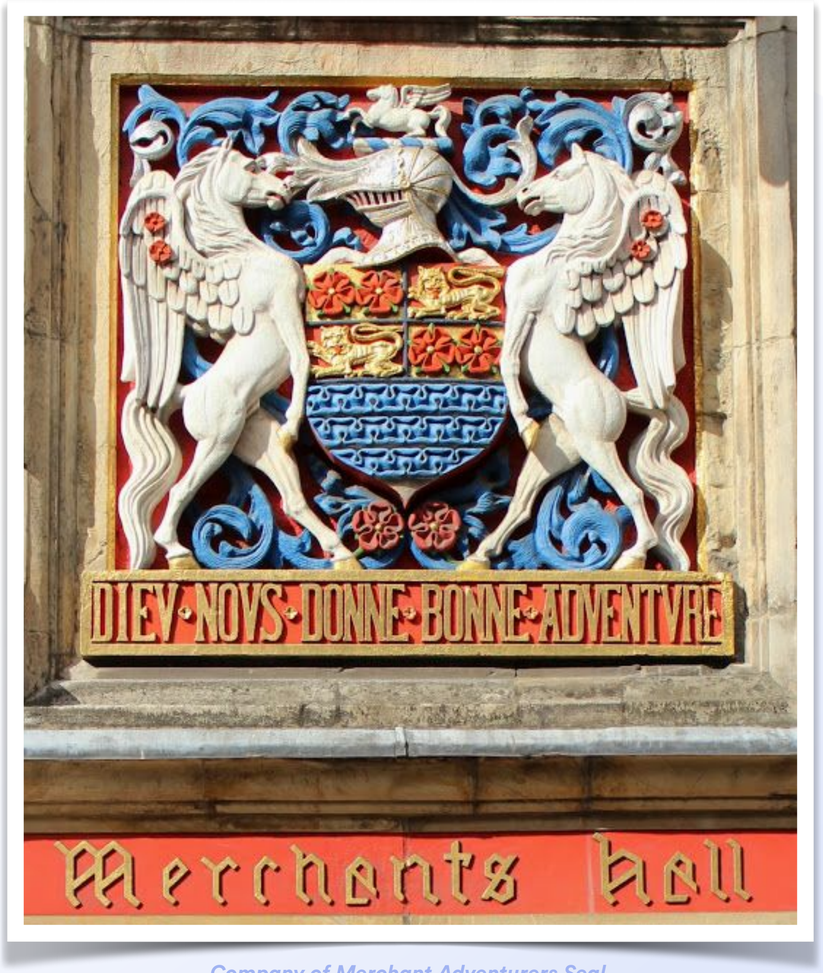


Preston Curve

Chainlink

Commercial Agreements: The Foundation of Progress

Edward Lloyd's Coffee house, by William Holland, 1789

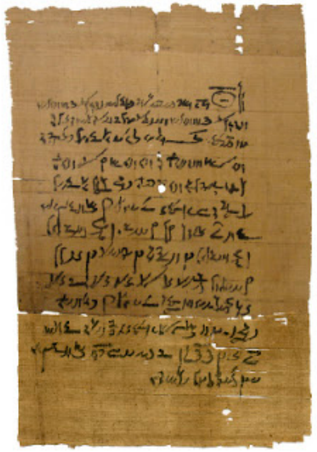


Company of Merchant Adventurers Seal

Chainlink

A Brief History of Commercial Contracts

Bill of Sale
(Ownership)
2600 BC



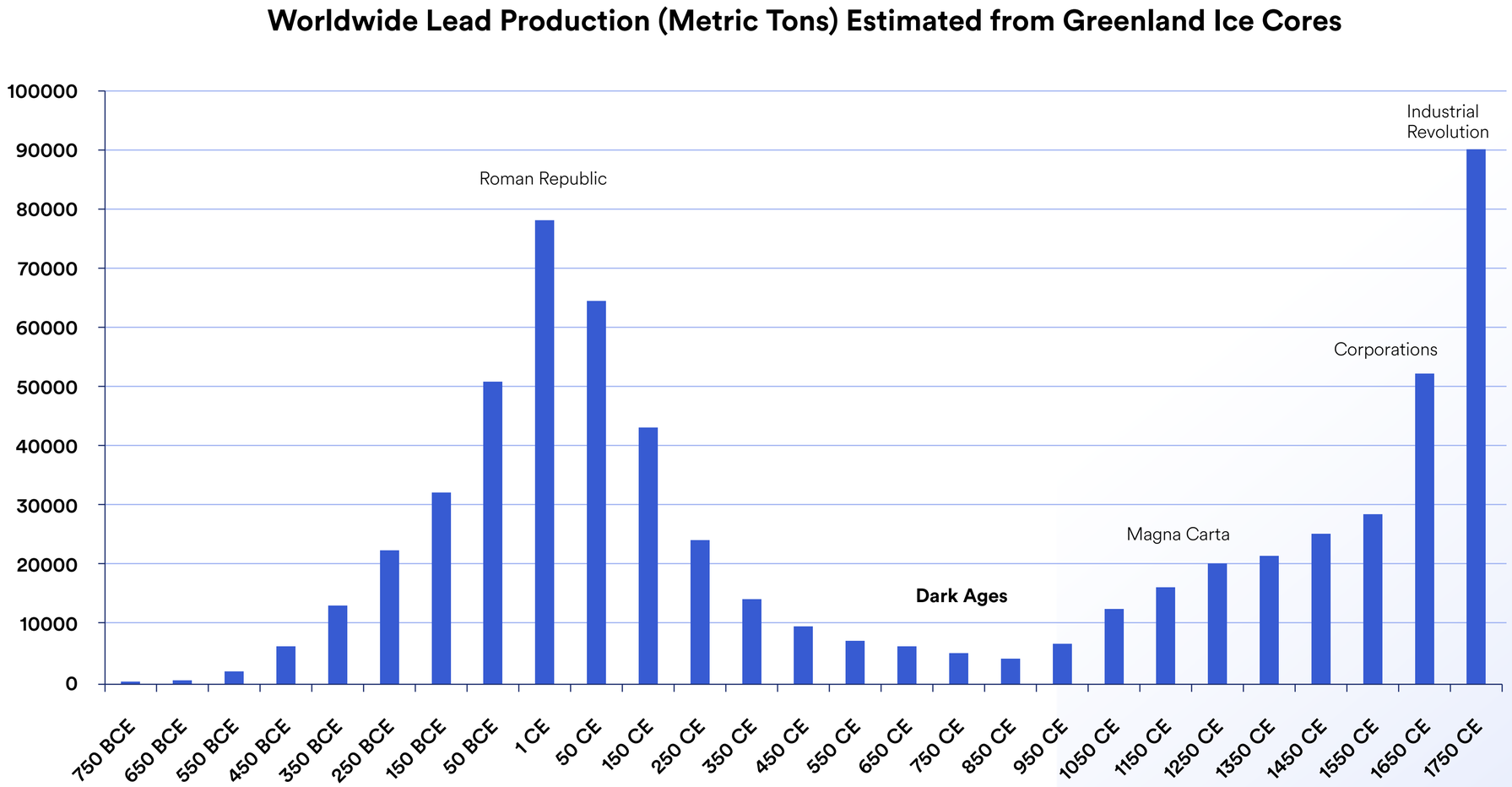
Employment Contract
(Income)
190BC

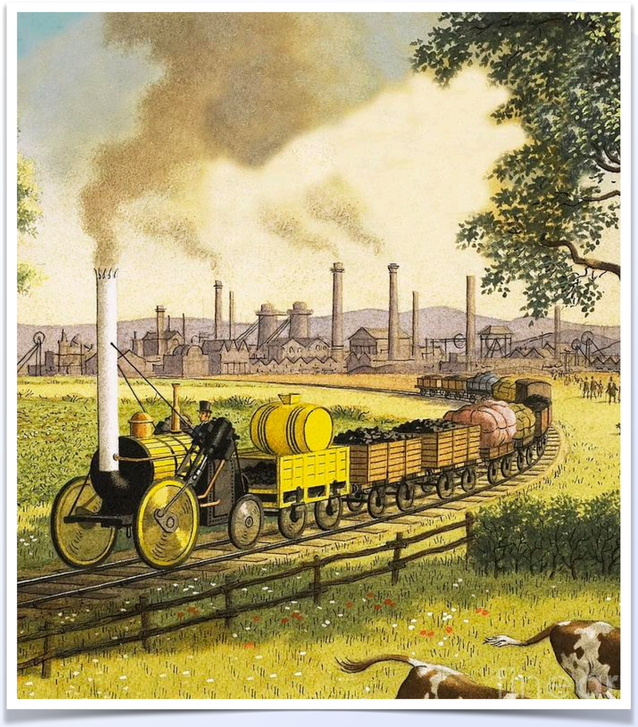
Roman Debt Contract
(Debt Obligations)
43AD

East India Company
(Corporations)
1600 AD

Chainlink

The Ability to Create Contracts Determines Progress

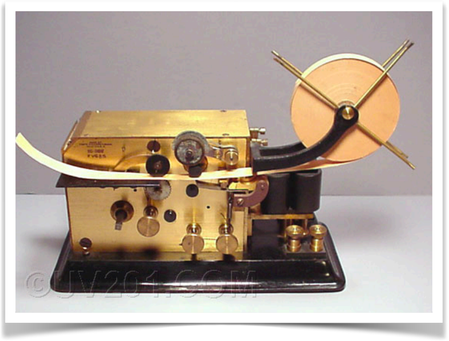


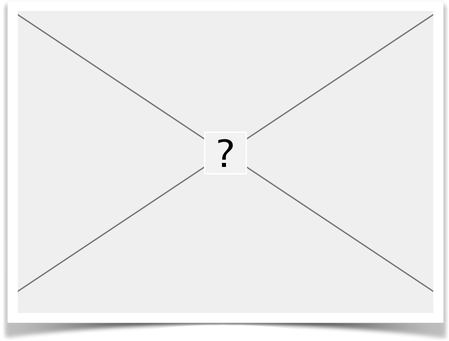


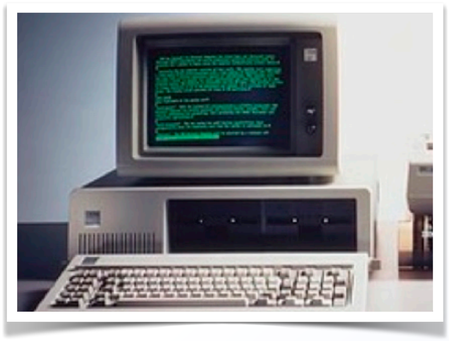
https://science.sciencemag.org/content/265/5180/1841

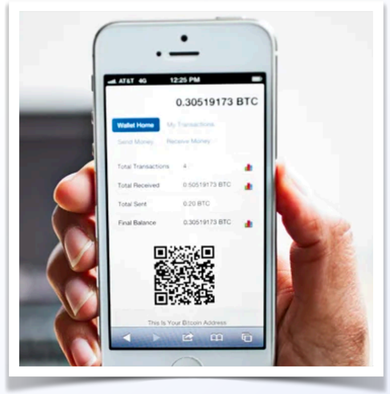
Chainlink

The Next Stage: Technologically Enforced Contracts









Telegraph Agreements (Electronically Signed) 1869

Telex Machines (Telecom Based) 1930s

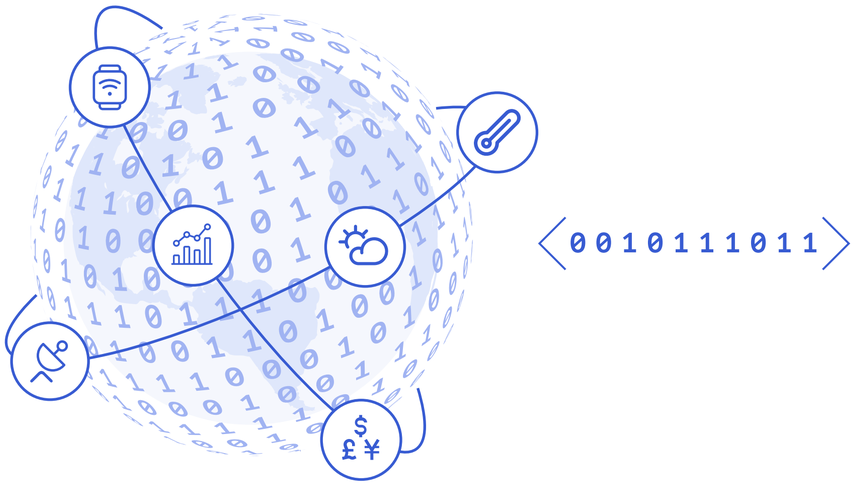
Digital Agreements (Internet Based) 1980s to Present

Smart Contracts (Blockchain Based) 2009 to Present

Chainlink

Digital Agreements

Performance Data



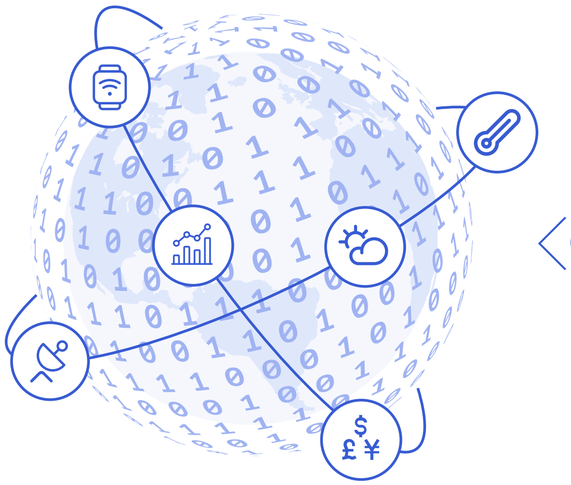
Contract Terms

Participants

Chainlink

Web/Internet Agreements are Centralized & Unreliable

Performance Data

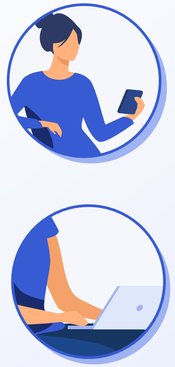


0010111011

Contract Terms

1100100101

0110010010

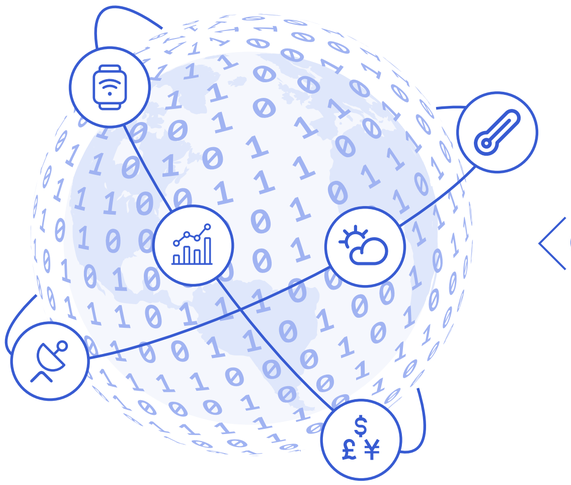


Contract Operator Conflicts of Interest (Pricing Monopolies)

Chainlink

Smart Contracts are Decentralized & Highly Reliable

Performance Data



0010111011

Contract Terms

1100100101

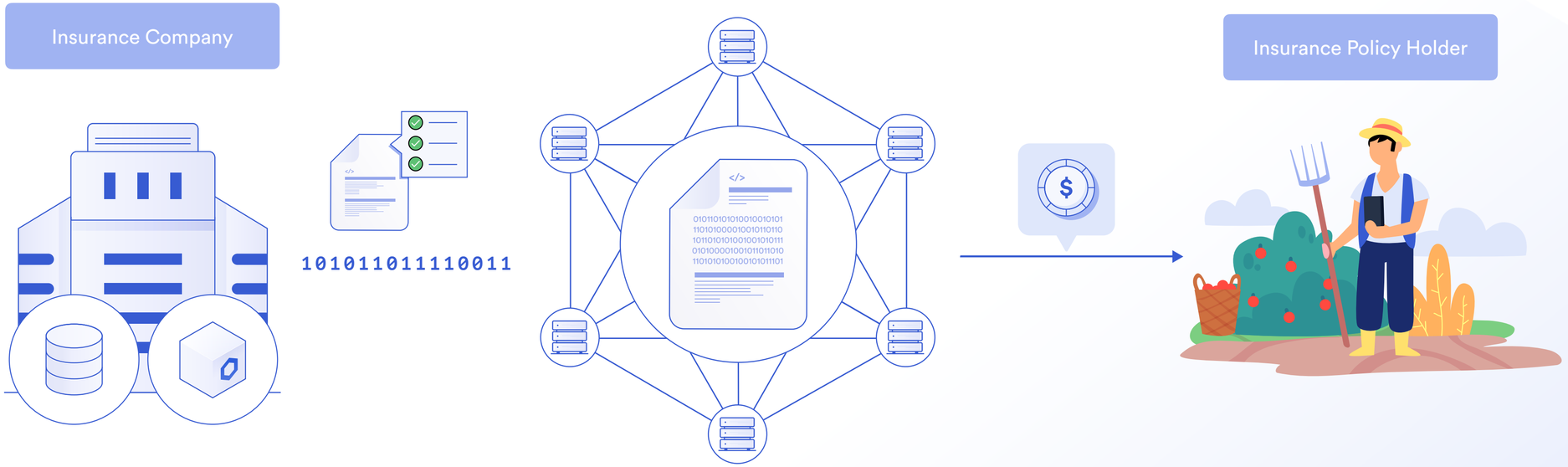
0110010010

Participants

Tamper Proof
(Open Source Standards)

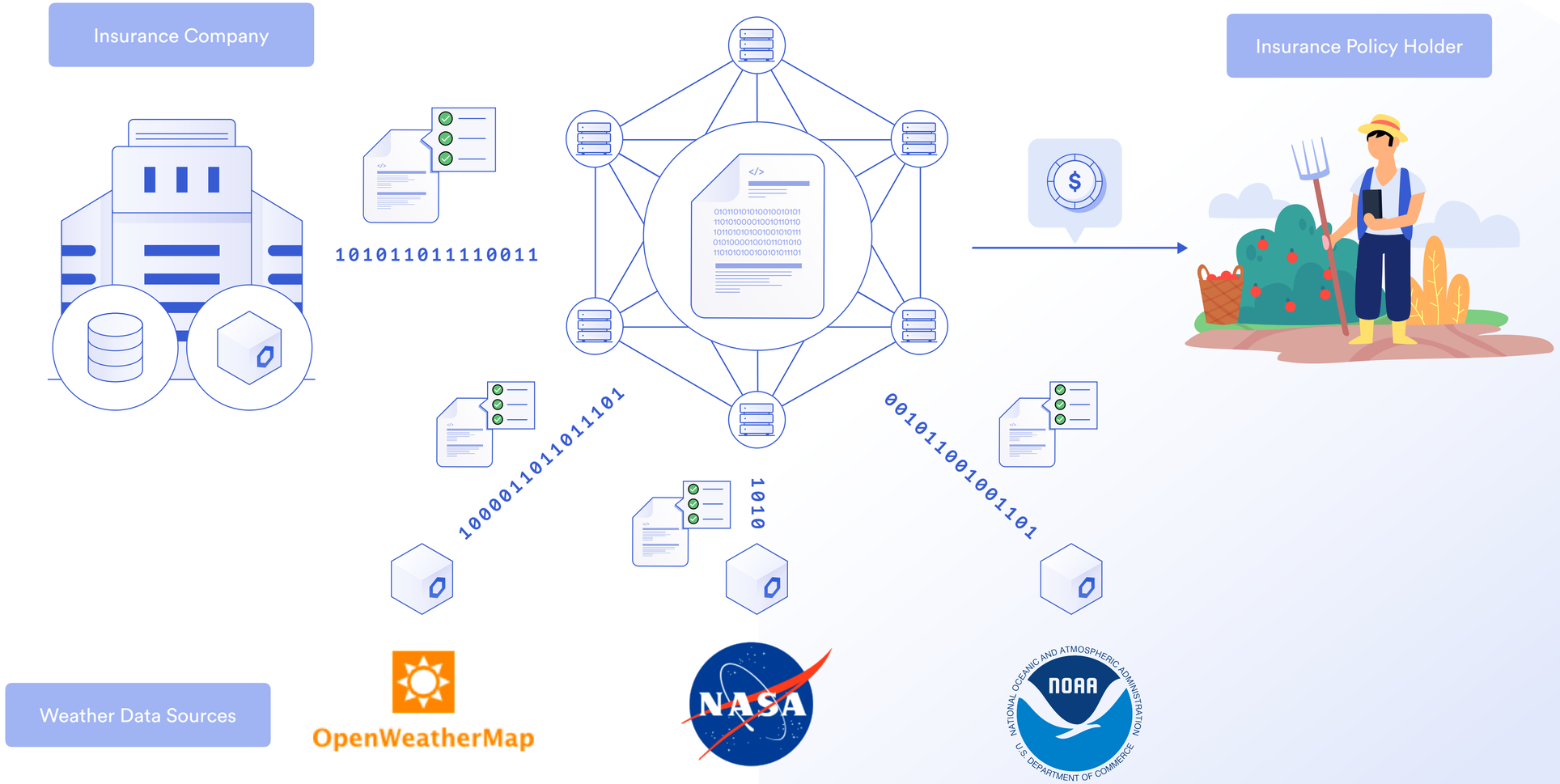
Chainlink

A Parallel Legal System for Emerging Market Growth



Chainlink

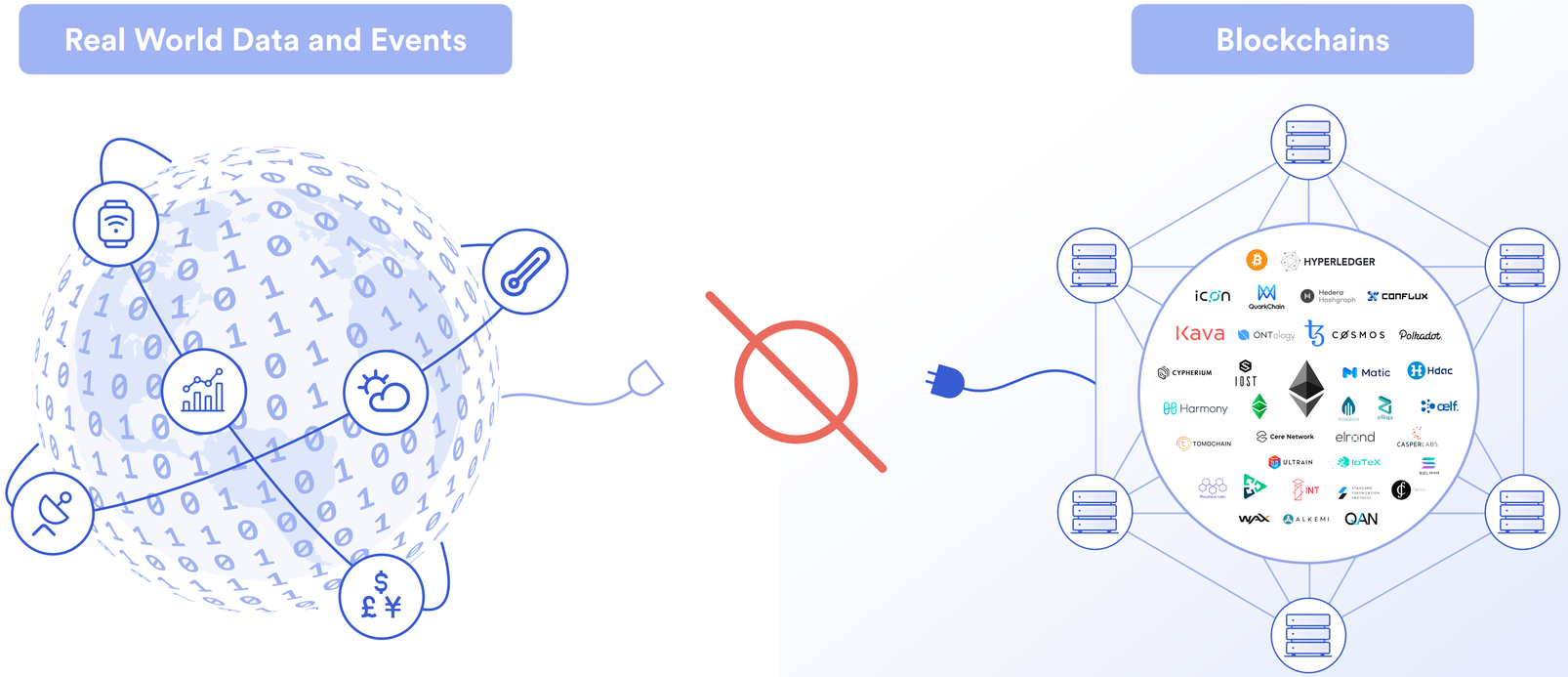
A Parallel Legal System for Emerging Market Growth



Chainlink

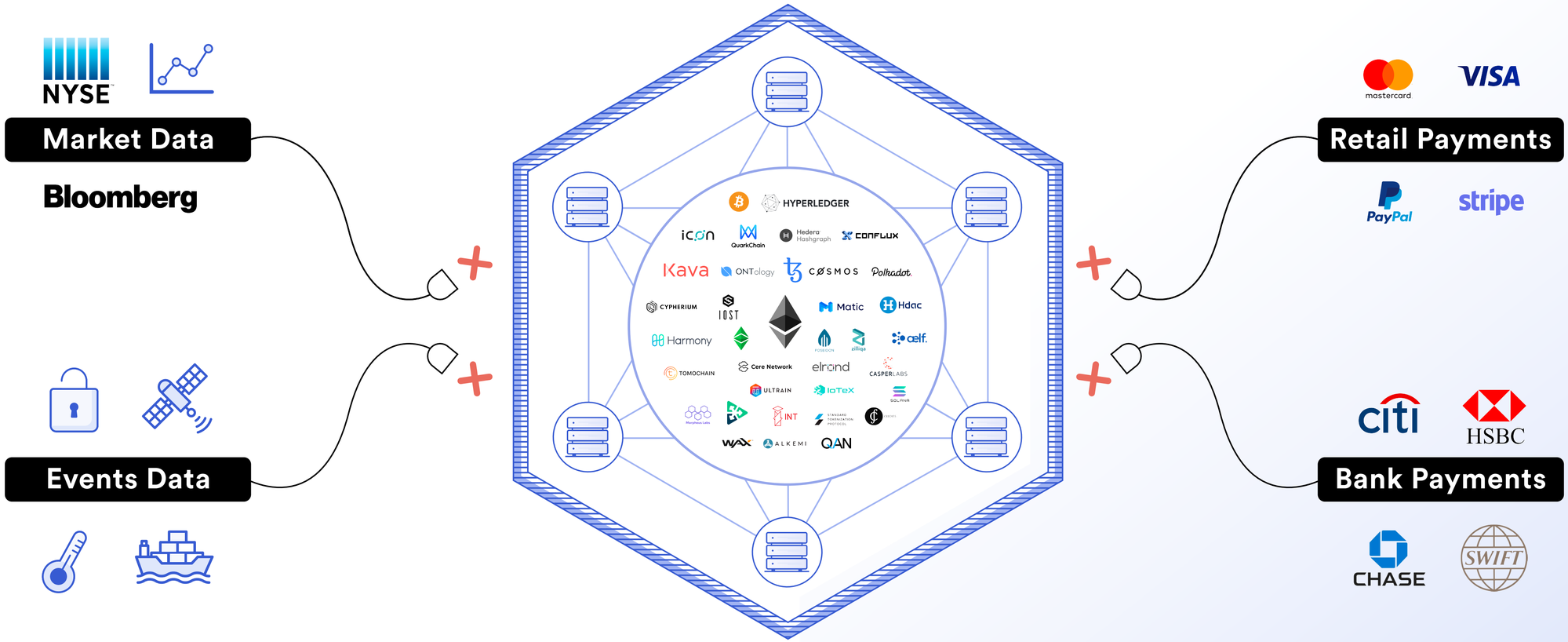
The “Oracle Problem” for Smart Contracts

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



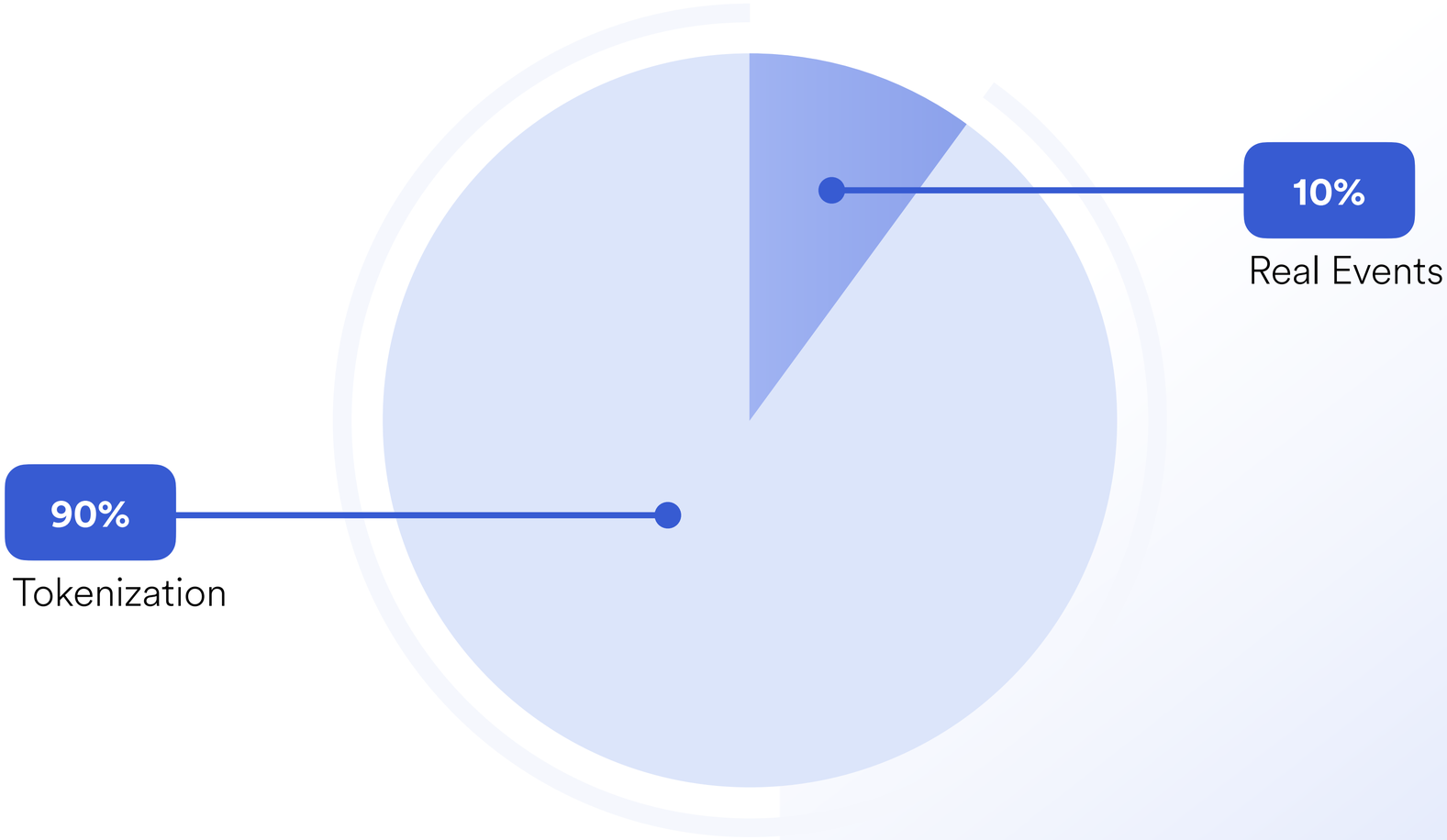
Chainlink

The “Oracle Problem” for Smart Contracts



Chainlink

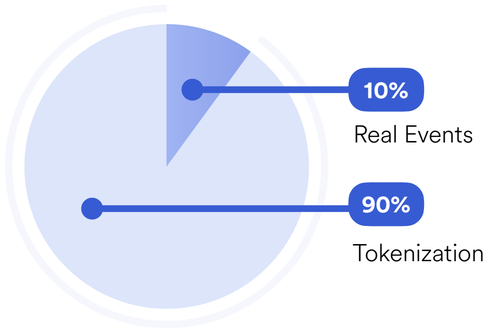
Smart Contracts are Currently Used for Tokenization



Chainlink

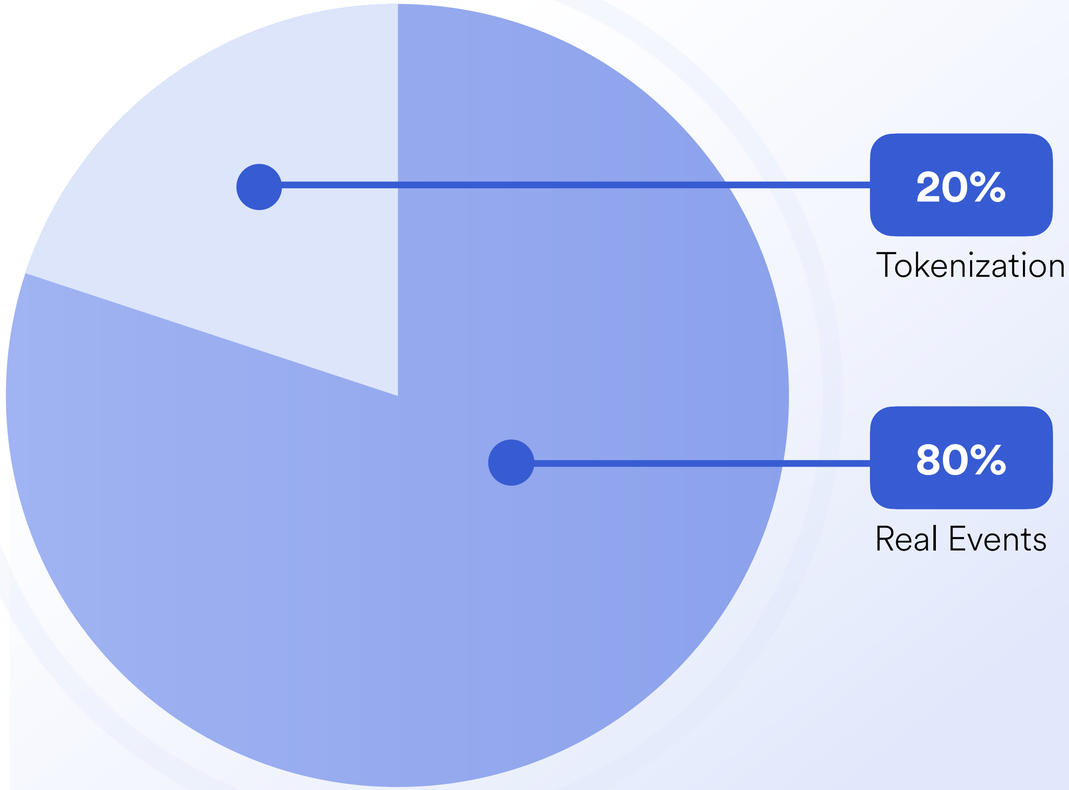
Redefining Smart Contracts With External Events

Current Distribution of Smart Contract Transaction Volume and Value Secured



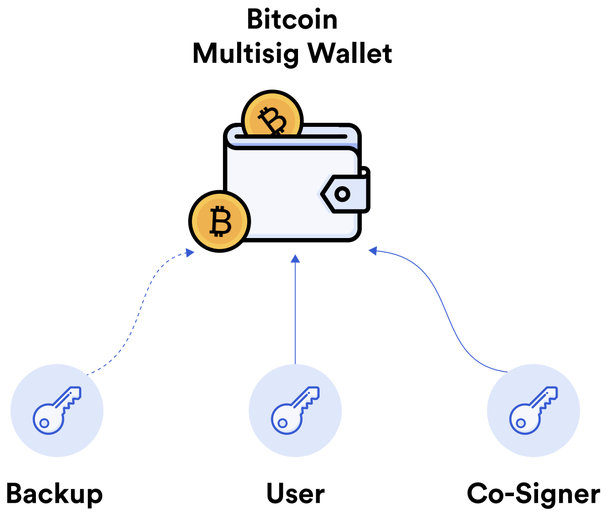
Externally Connected Contracts

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

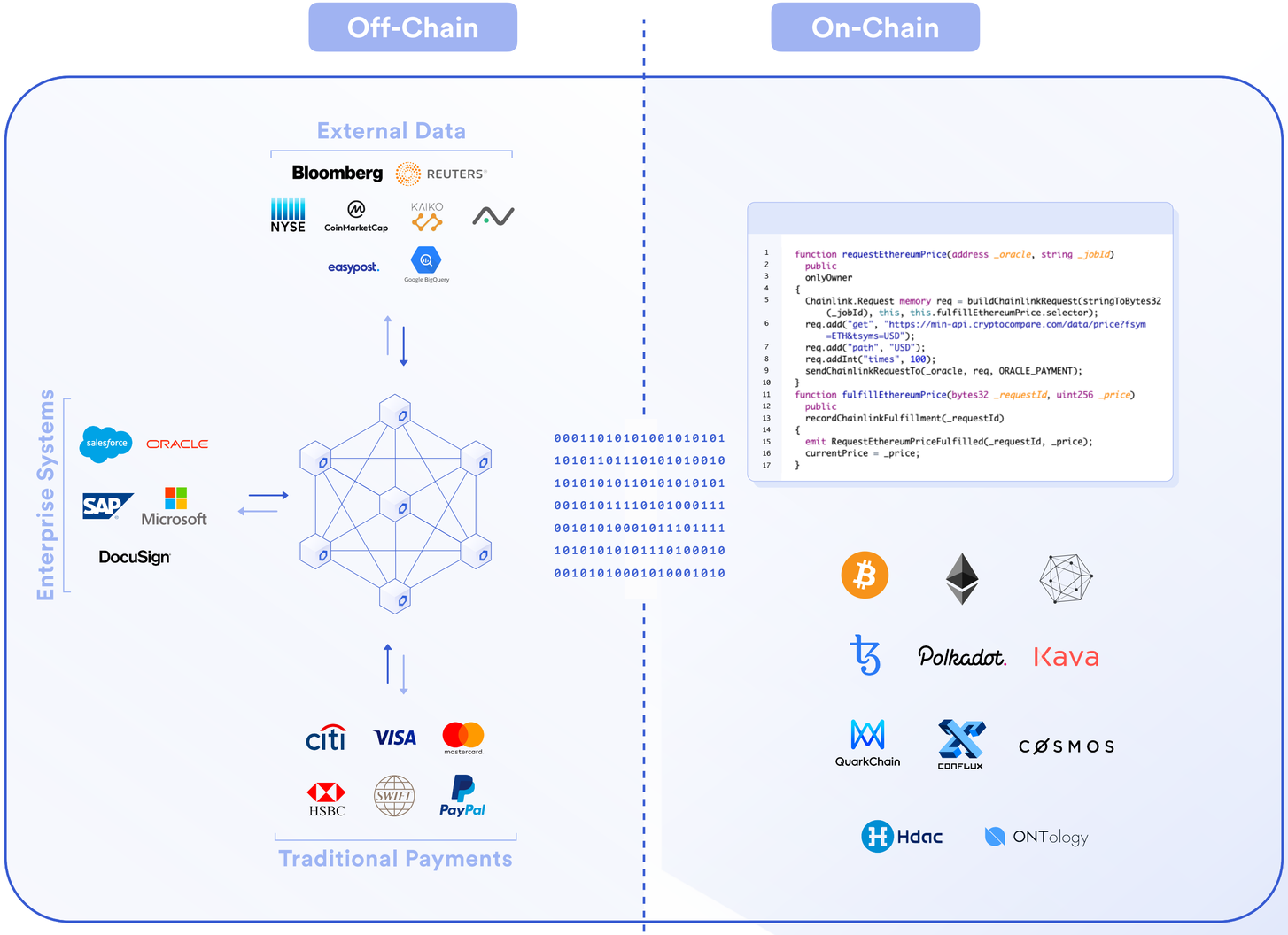
AAVE

bZx

Nexus Mutual

Chainlink

DeFi Smart Contracts Have Two Important Parts



Chainlink

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

Chainlink

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

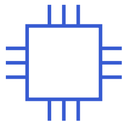
Our Approach to Reliable & Secure Oracles for Web3

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

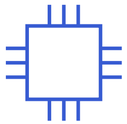
Our Approach to Reliable & Secure Oracles for Web3

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

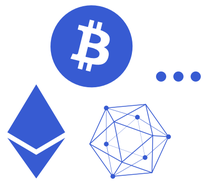
Provably Secure Nodes that provide cryptographic proof of their overall security

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)

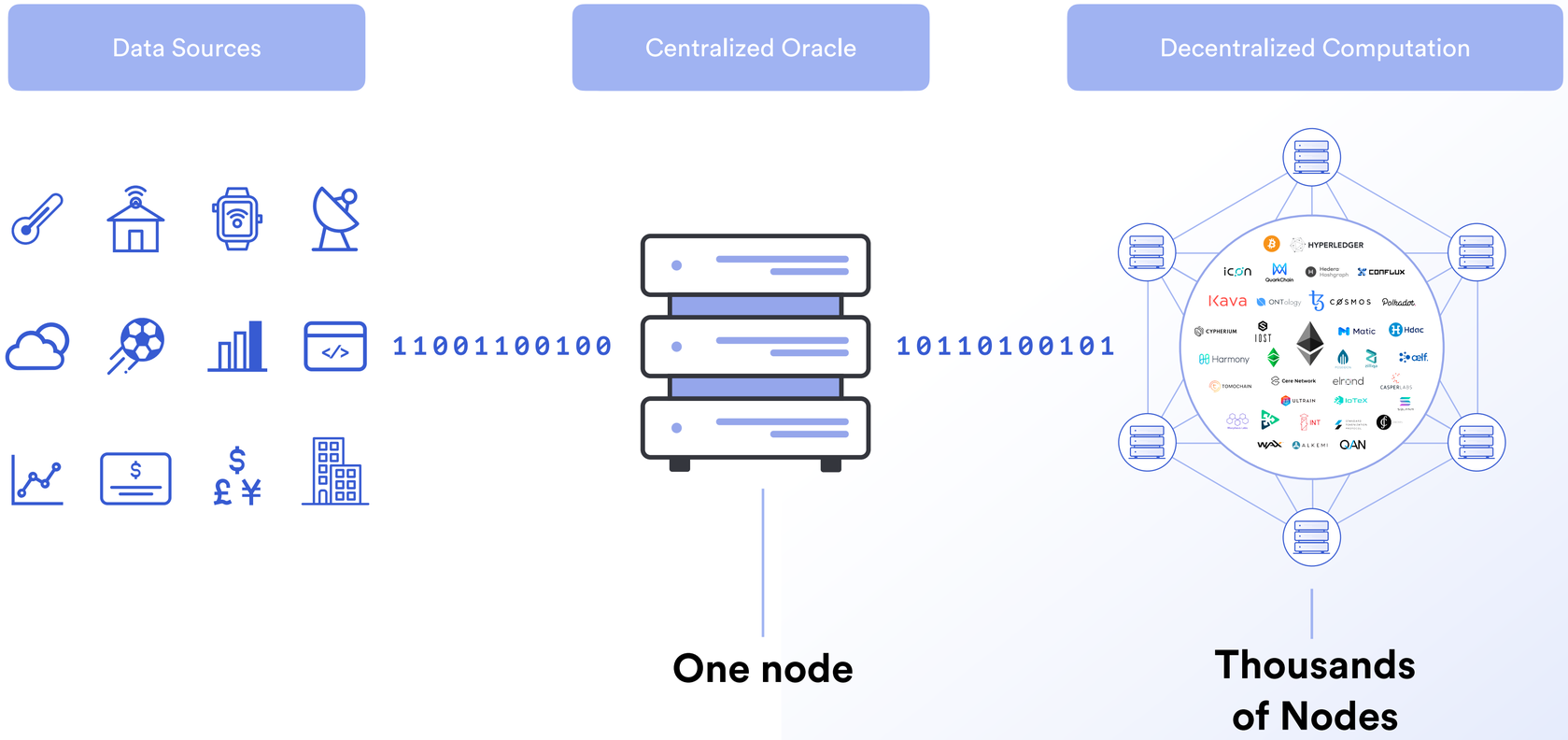
A Large Open Source Community of Node Operators, Developers, Researchers and Security Auditors



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.

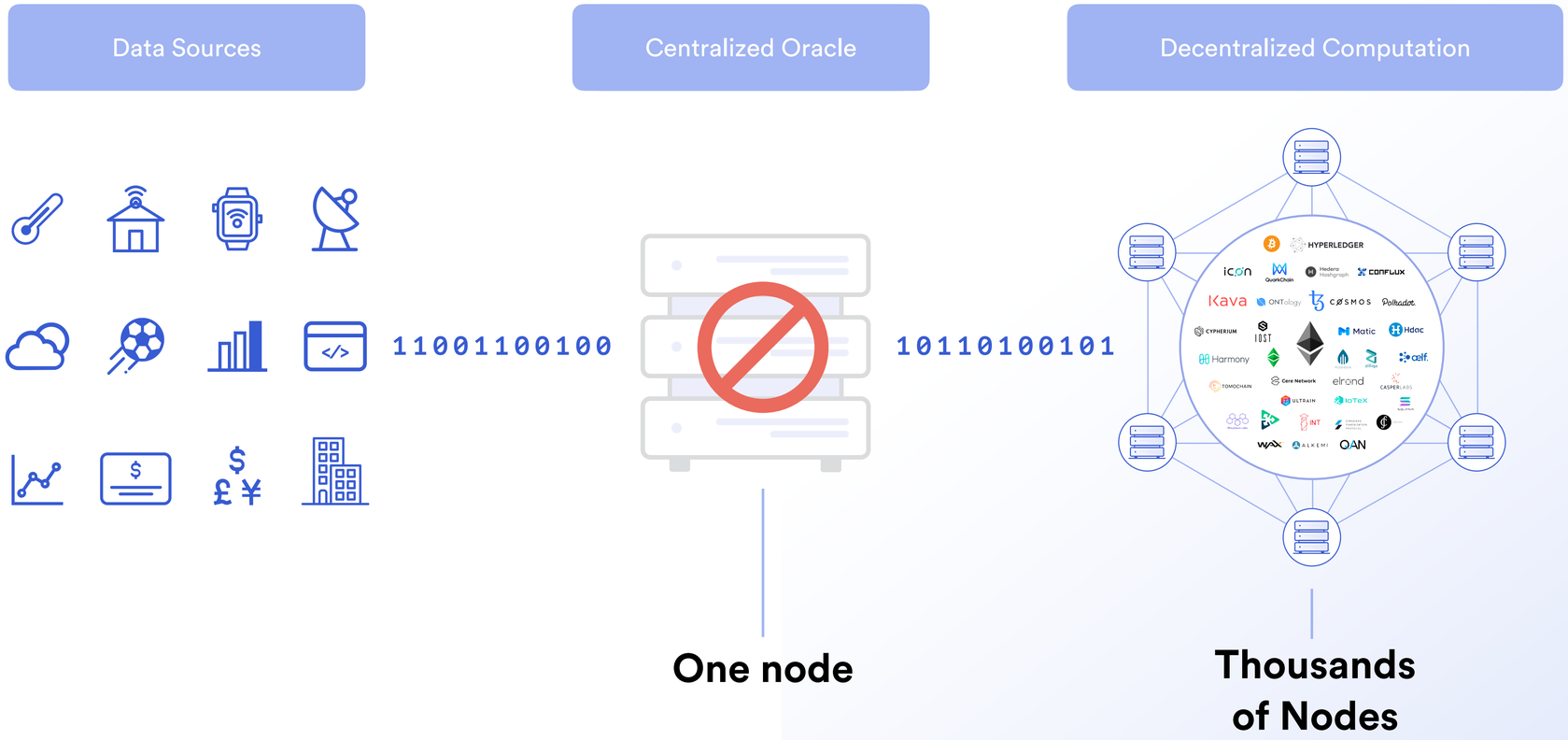
Chainlink

Centralized Oracles are a Point of Failure



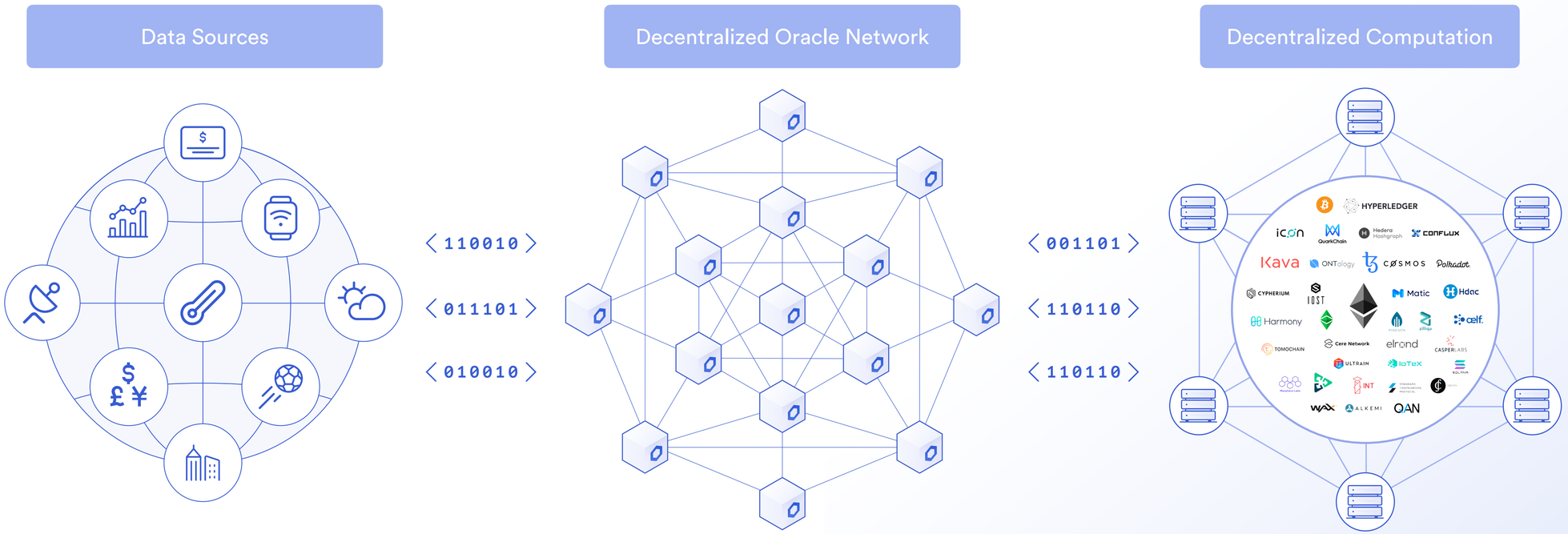
Chainlink

Centralized Oracles are a Point of Failure



Chainlink

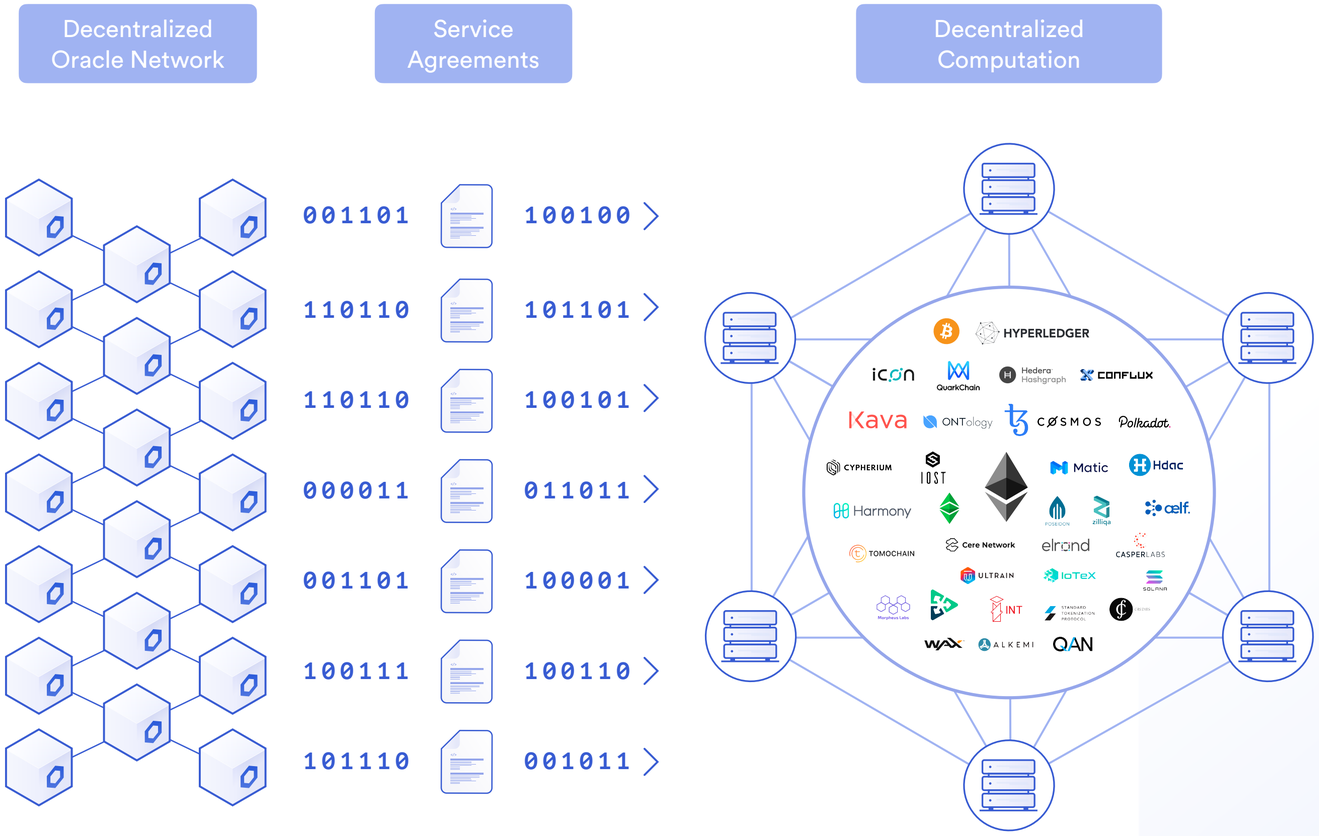
A Decentralized Oracle Network



Decentralized Oracles: A form of decentralized computation that validates data about real world events, making data reliable enough to trigger other forms of decentralized computation, e.g. smart contracts.

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.

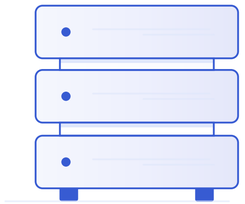
Chainlink

On-chain Service Agreements Provide Guarantees

Unpaid/Free OpenAPI

- Low Quality Data
- Unreliable Responses
- No Quality Guarantees

A Node Without Credential Management



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

Smart Contract With Low Quality Data

Chainlink

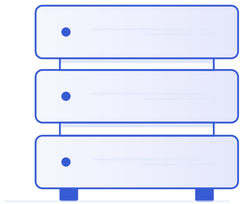
On-chain Service Agreements Provide Guarantees

Unpaid/Free OpenAPI

- Low Quality Data
- Unreliable Responses
- No Quality Guarantees

10101110101011110

A Node Without Credential Management



10101110101011110100101001

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

Smart Contract With Low Quality Data

Data Providers

ALPHA VANTAGE · KAIKO · amberdata.io · CoinMarketCap · CoinGecko · Google BigQuery · CRYPTO COMPARE · BNC. bravenewcoin.com · JSECOIN · BINANCE · ANYblock · easypost. · parallel MARKETS · CONSTELLATION · DSG Data Sports Group · coti · FLCA · streamr · RTRADE · OPENSEA · RANDOM.ORG · fabr(x)

- High Quality Data
- Highly Responsive
- Quality Guarantees

10101110101011110

Chainlink Node

11011

On- chain Service Agreement

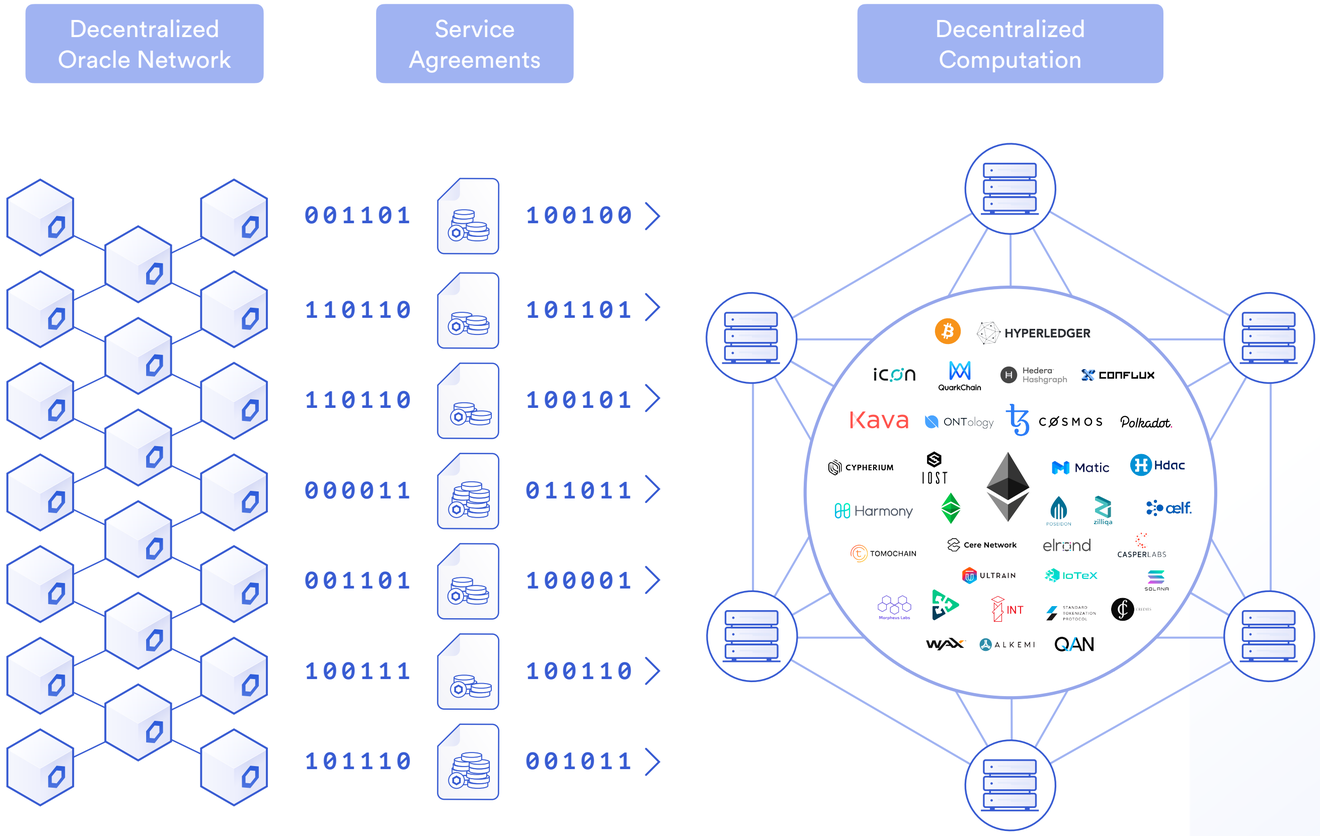
10010100101001010010

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

Smart Contract with High Quality Data

Chainlink

Crypto-economic Security from Staking



Cryptoeconomic Security from Staking

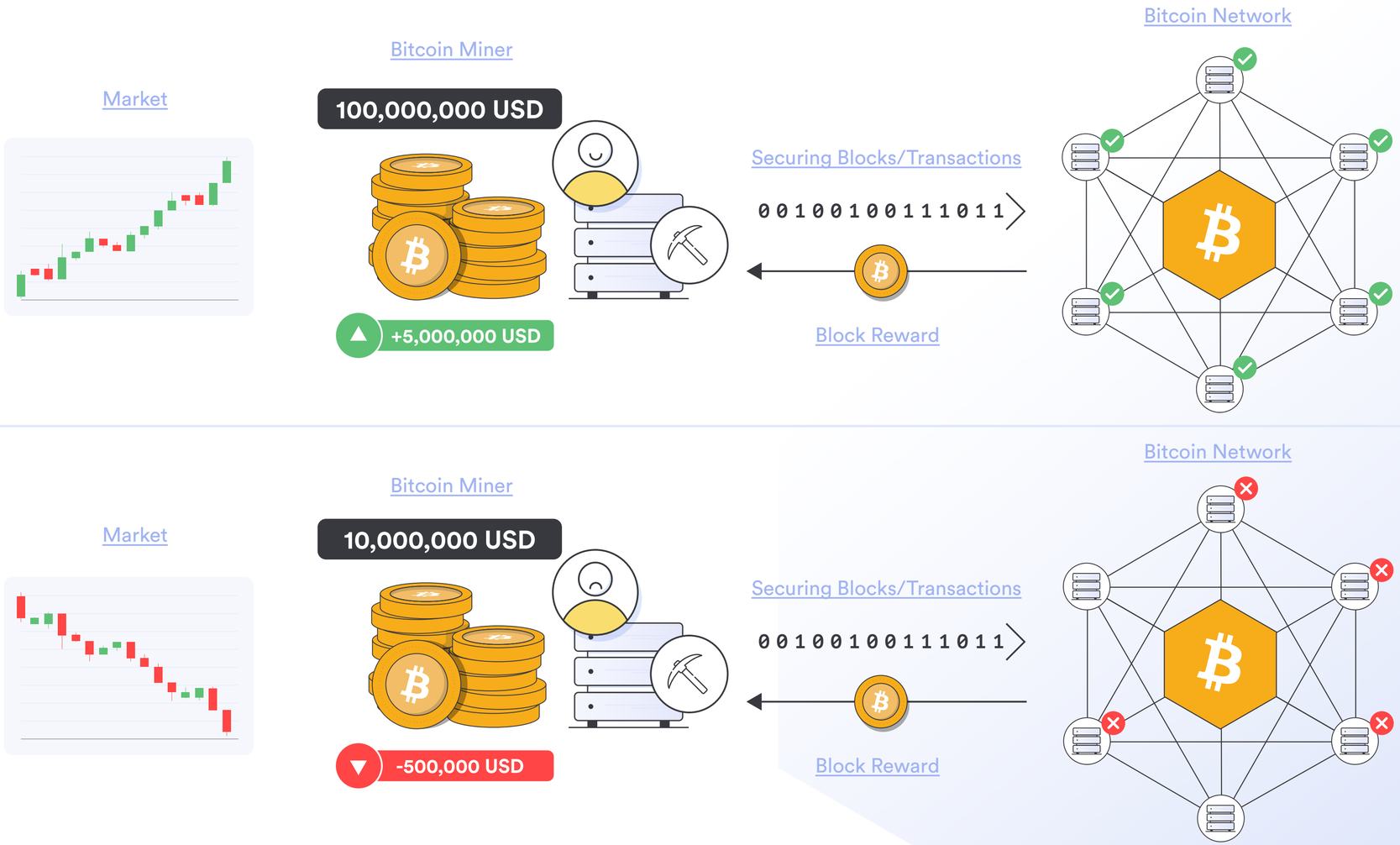
Using the commitments from binding service agreements, we can define clear parameters for the penalties for misbehaving nodes, bad data providers and any other point in the data origination and/or data transfer process.

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.

Chainlink

Forms of Staking Already Support Network Security

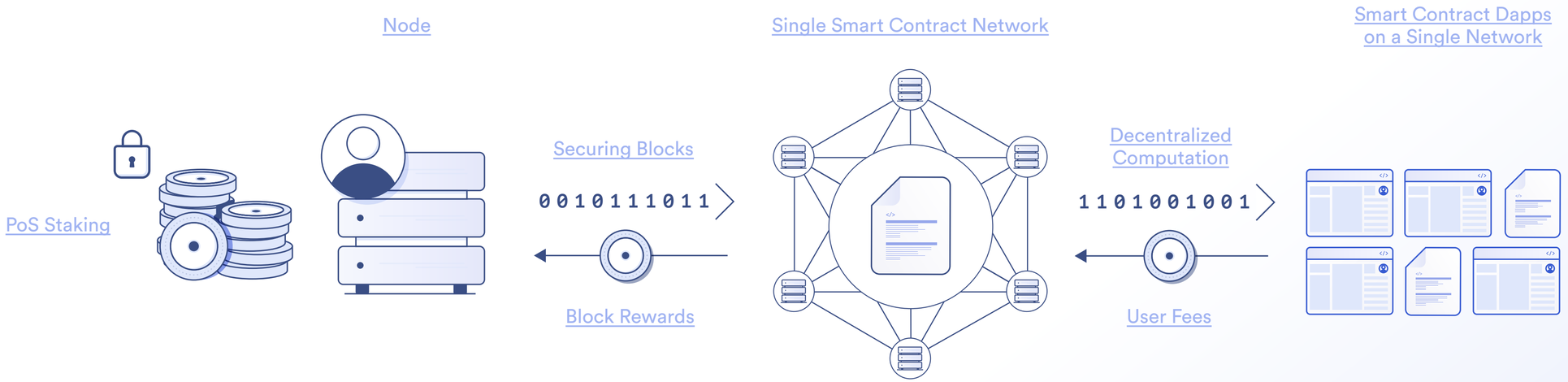
Implicit Staking: Holding an asset whose value can decrease based on deviations from a protocol run by you and others.



Chainlink

Crypto-economic Security from Staking for Blocks

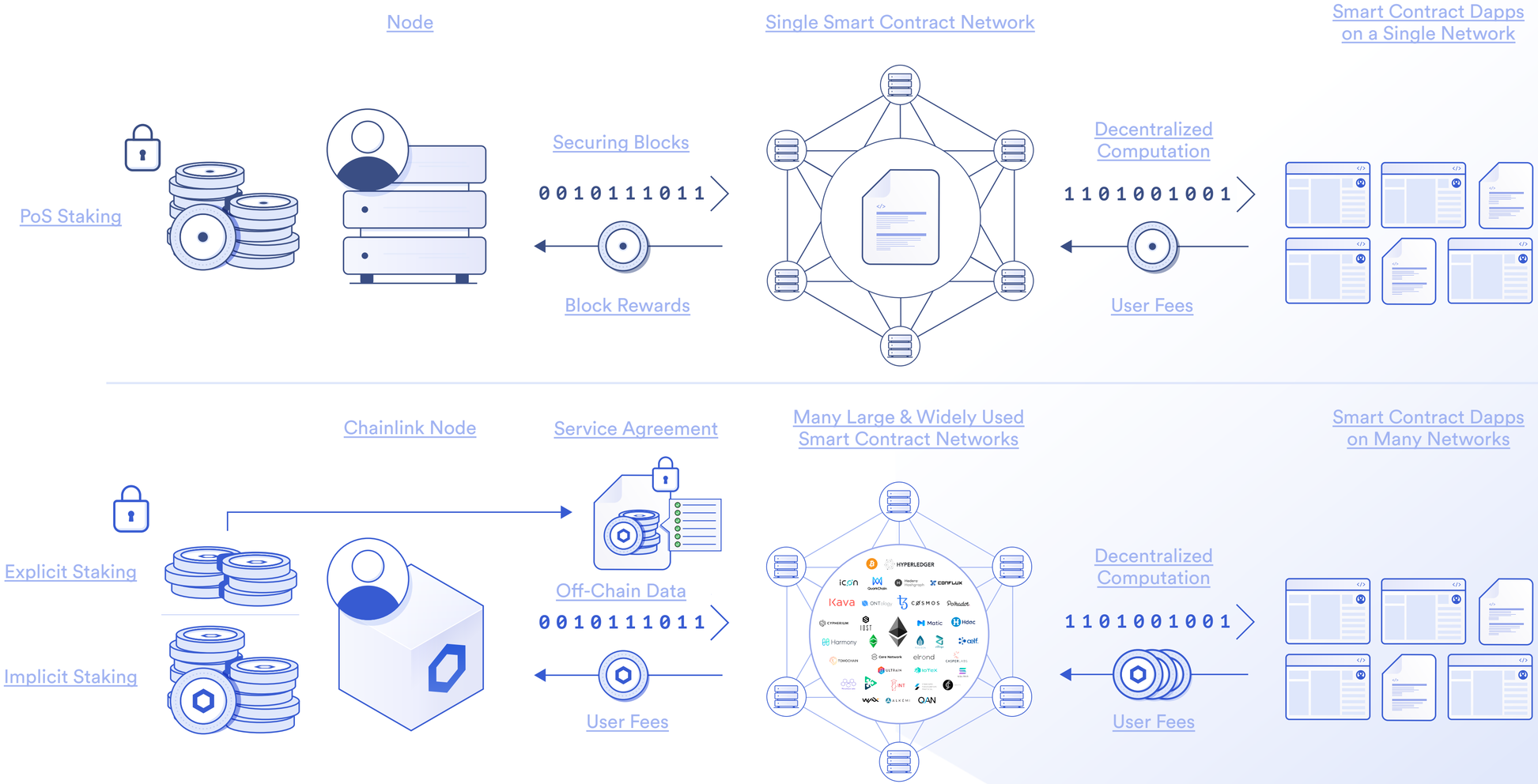
Explicit Staking: Putting down a deposit, that may be lost if only you deviate from a protocol.



Chainlink

Crypto-economic Security from Staking for Data Delivery

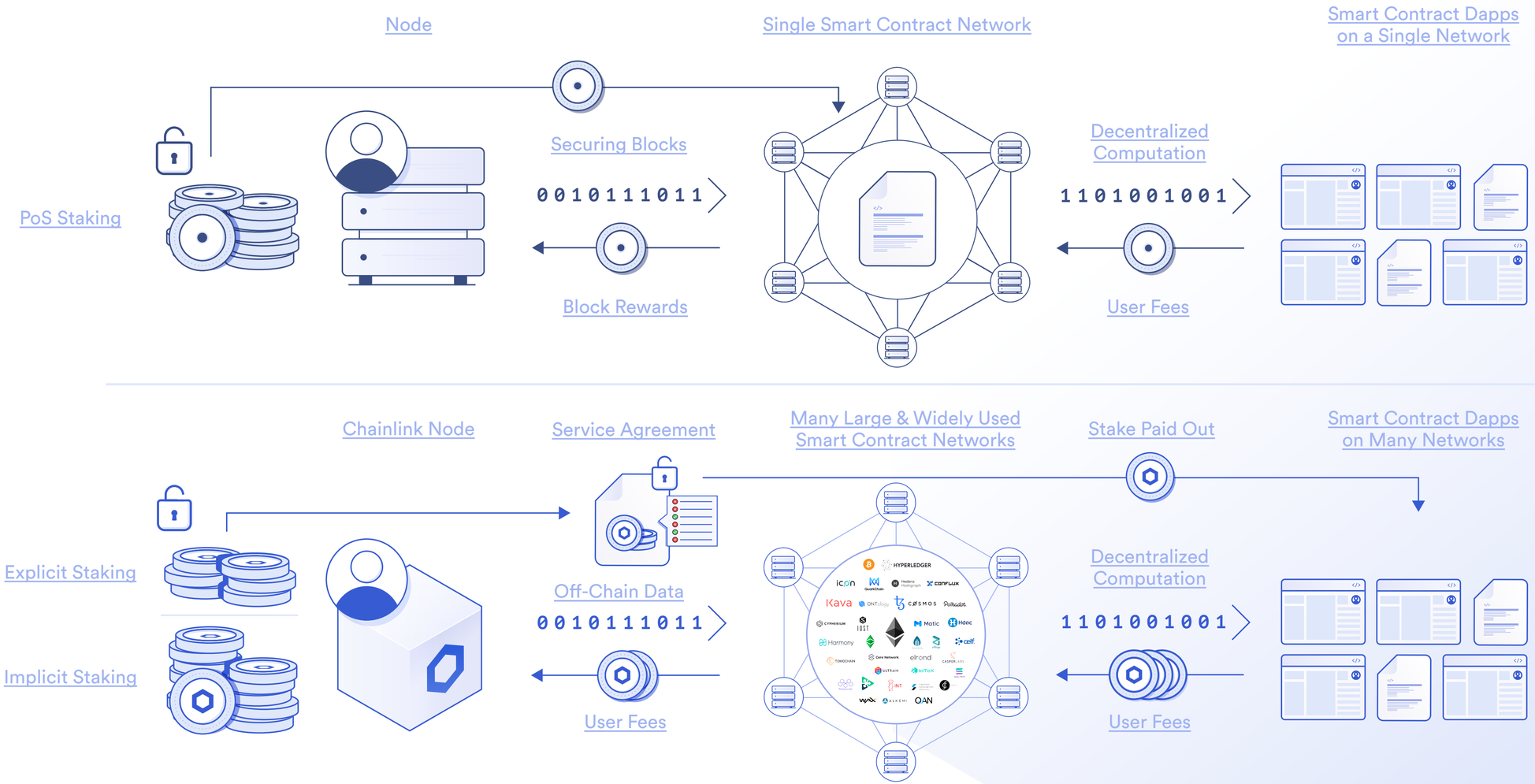
Explicit Staking: Putting down a deposit, that may be lost if only you deviate from a protocol.



Chainlink

Crypto-economic Security from Staking for Data Delivery

Explicit Staking: Putting down a deposit, that may be lost if only you deviate from a protocol.



Chainlink

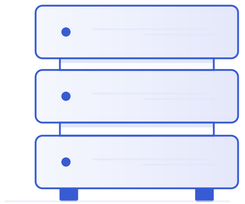
On-chain Service Agreements Enforce Data Delivery

Unpaid/Free OpenAPI

- Low Quality Data
- Unreliable Responses
- No Quality Guarantees

10101110101011110

A Node Without Credential Management



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

10101110101011110100

Smart Contract Broken by Bad Data

Data Providers

ALPHA VANTAGE · KAIKO · amberdata.io · CoinMarketCap · CoinGecko · Google BigQuery · CRYPTO COMPARE · BNC. bravenewcoin.com · JSECOIN · BINANCE · ANYblock · easypost. · parallel MARKETS · CONSTELLATION · DSG Data Sports Group · coti · FLCA · streamr · RTRADE · OPENSEA · RANDOM.ORG · fabr(x)

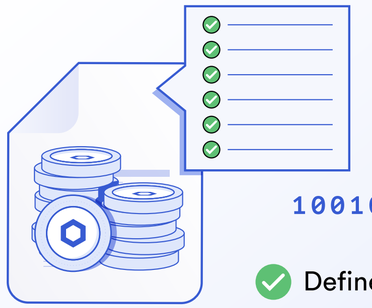
- High Quality Data
- Highly Responsive
- Quality Guarantees

10101110101011110

Chainlink Node

11011

On- chain Service Agreement



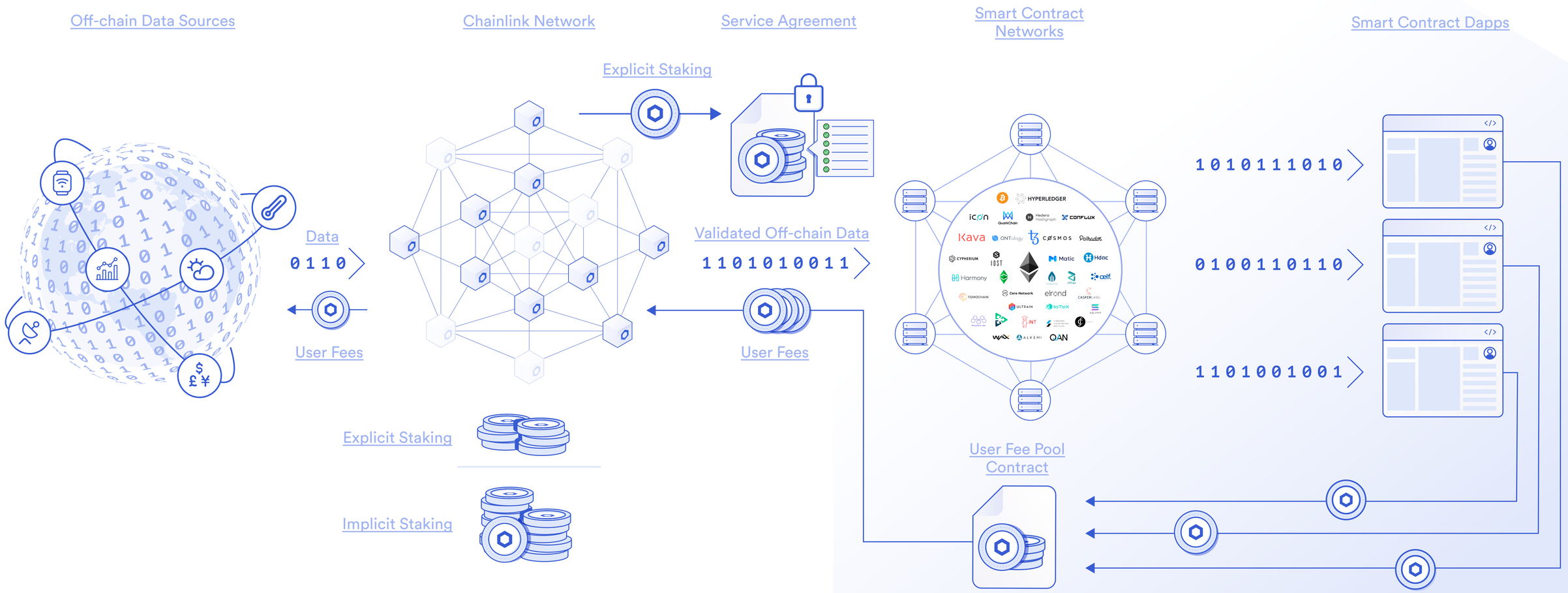
10010100101001010010

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

Smart Contract with High Quality Data

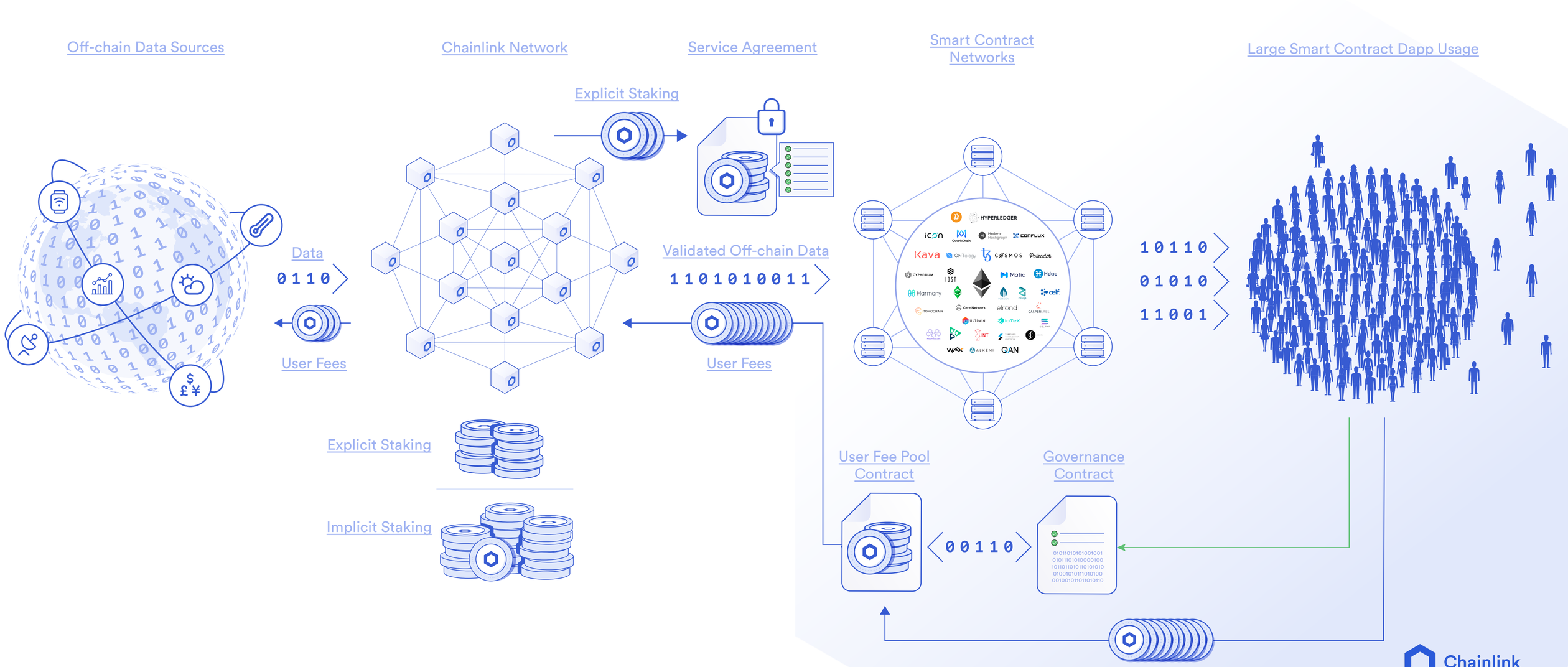
Chainlink

User Fees Go to Node Operators For Data Delivery

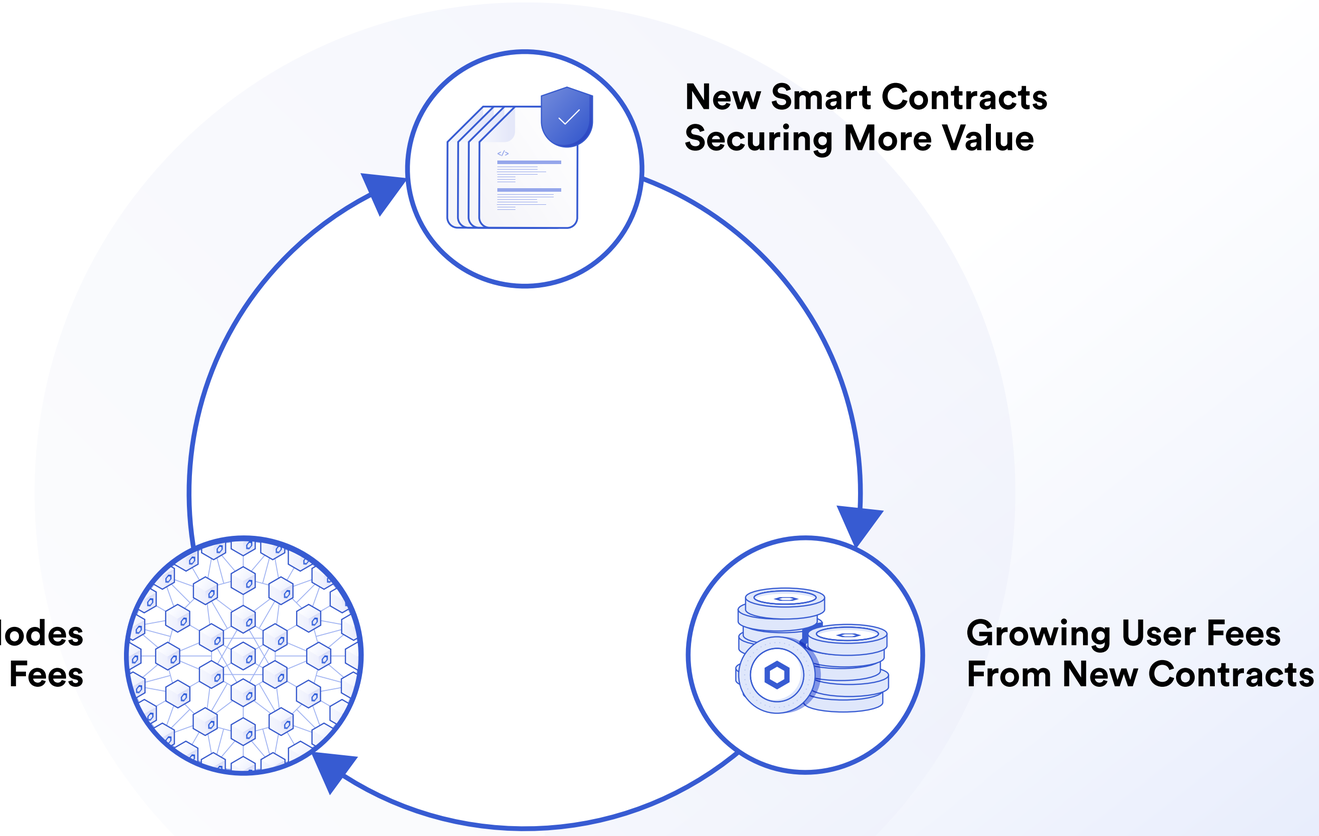


Chainlink

Fees and Staking Grow With Smart Contract Usage

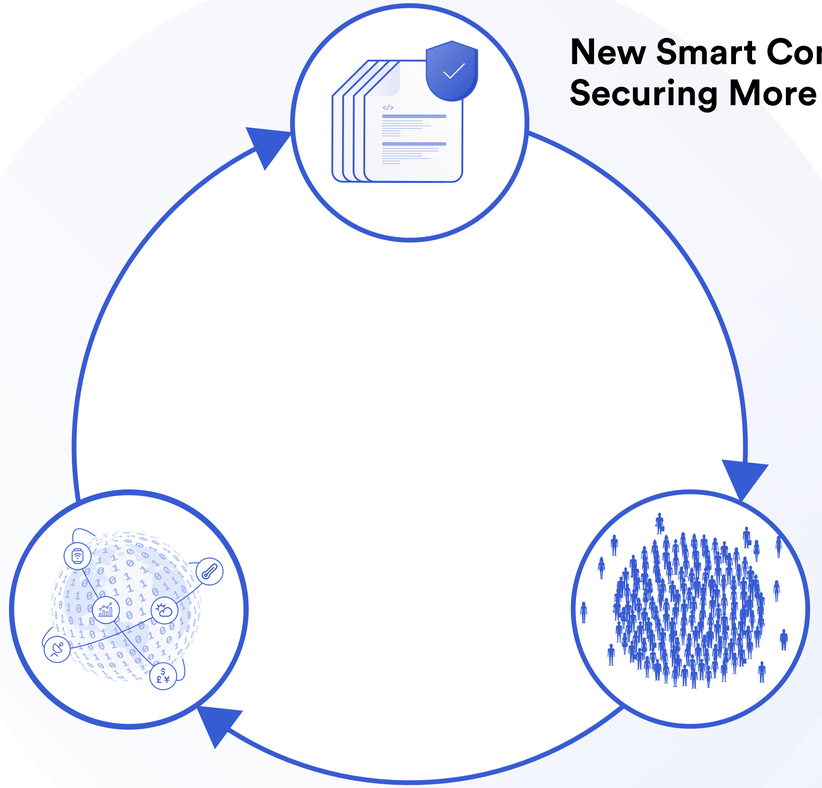


Greater User Fees Drive Greater Security Guarantees



Chainlink

Greater Usage of Data Drives More Data On-chain



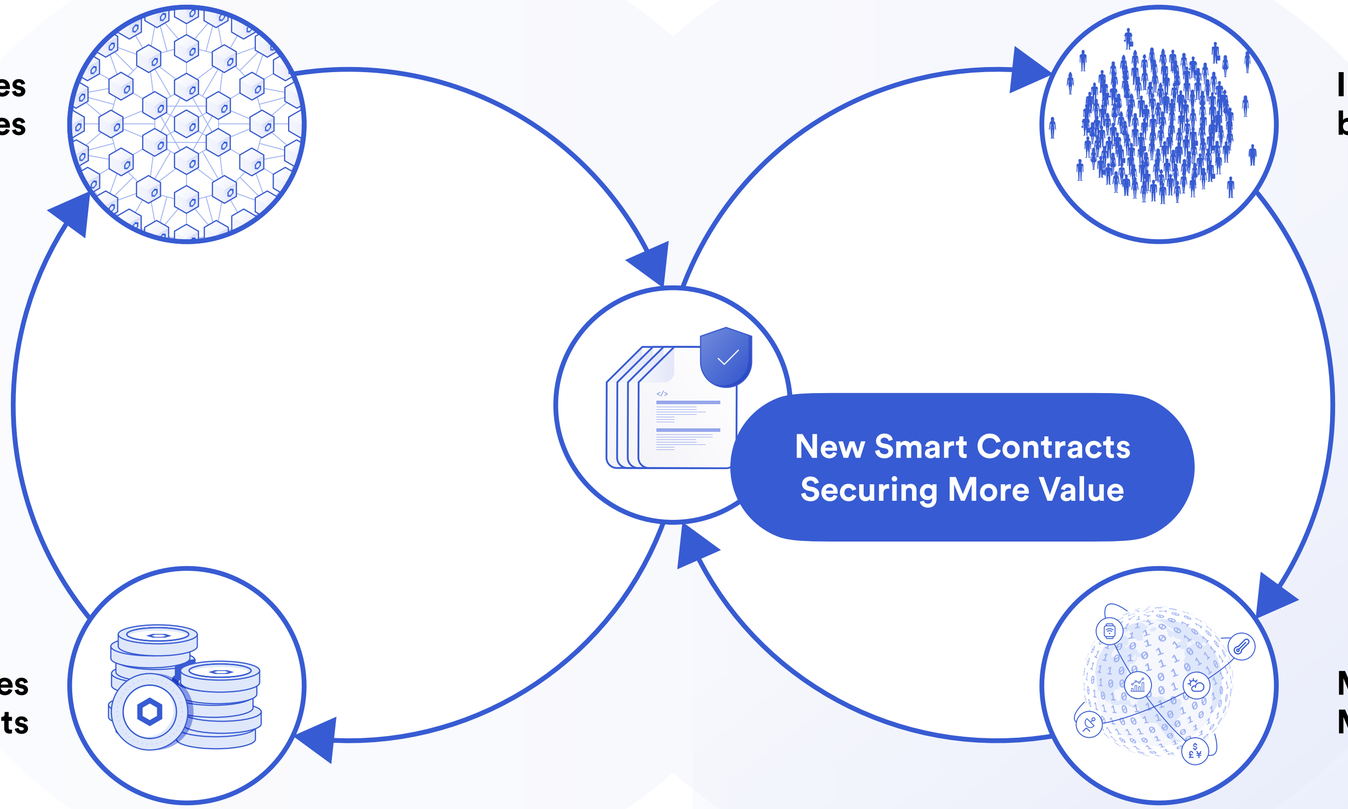
New Smart Contracts
Securing More Value

Increased Usage of Data
by Smart Contracts/Users

More APIs and Data
Sources Made Available

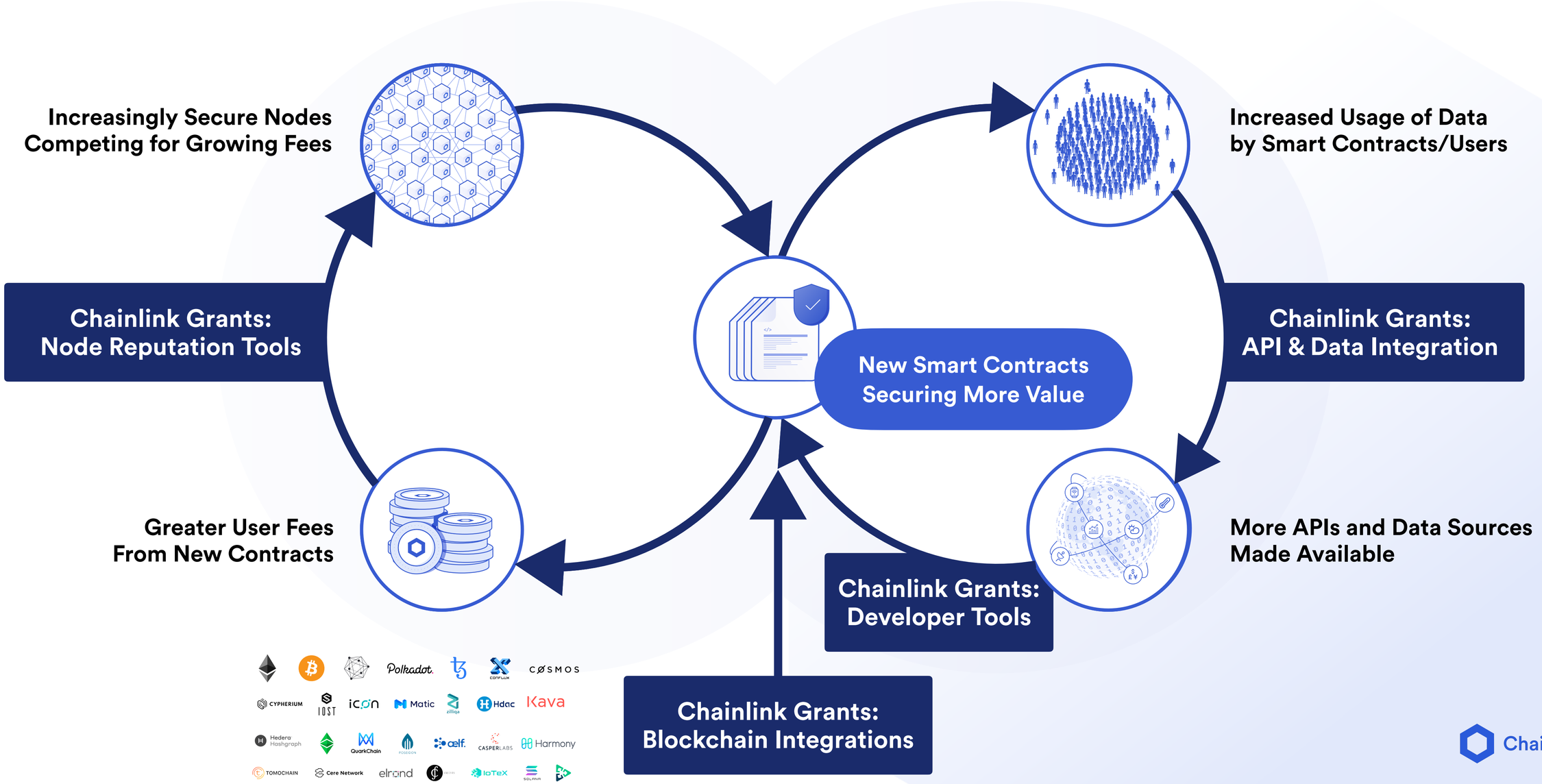
Chainlink

Smart Contracts as The Dominant Digital Agreement



Chainlink

Accelerating the Creation of Various Smart Contracts



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.smartcontract.com

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