



Decentralized Oracle Networks

Zsófia Tasnádi-Tulogdi
University of Bern
11.12.2024

Agenda

1. Oracle Problem

2. What is an Oracle?

3. Decentralized Oracle Network (DON)

4. About ChainLink

5. Chainlink Network

6. CCIP (Cross-Chain Interoperability Protocol)

7. My project

Oracle problem

Real World Data and Events



Blockchains



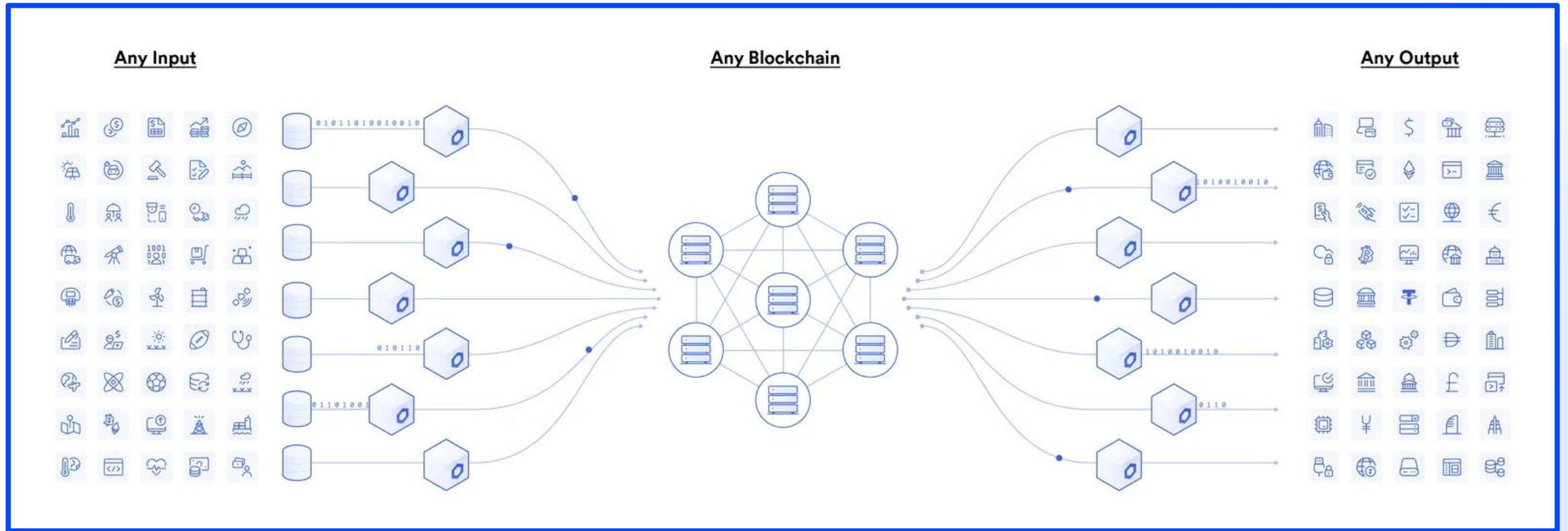
Blockchain Oracles

A blockchain oracle is any system that services a smart contract by providing it with data from an offchain source or connecting it with an offchain system.

Oracles enable connectivity between blockchains and real-world data by interfacing with external APIs and data feeds, allowing them to pull data for or push data from a smart contract.

**Internet connects computers to the outside world → oracles connects
blockchains to offchain data**

Blockchain Oracles



Types of Oracles

Input Oracles

Fetches data
offchain

Delivers data
onto a blockchain
network

Most recognized

Output Oracles

Opposite of input

Smart contracts
send commands to
offchain systems

Triggers them to
execute certain
actions

Cross-chain Oracles

Read and write
information
between different
blockchains

Moving data,
assets between
blockchains

Centralized Oracles

Data Sources



Centralized Oracle



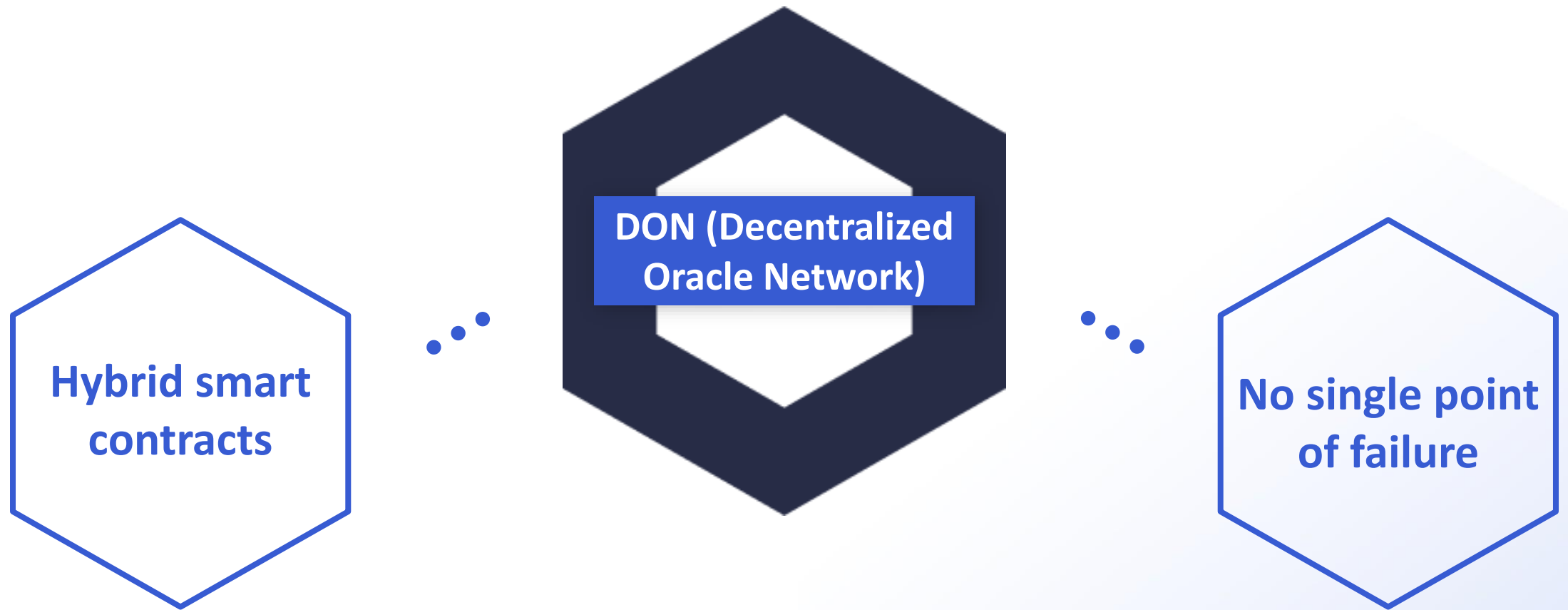
One node

10110100101

Decentralized Computation



Thousands
of Nodes



Combines multiple independent oracle node operators and multiple reliable data sources to establish end-to-end decentralization.

About Chainlink

Blockchain-agnostic

DONs (Decentralized Oracle Networks)

2017

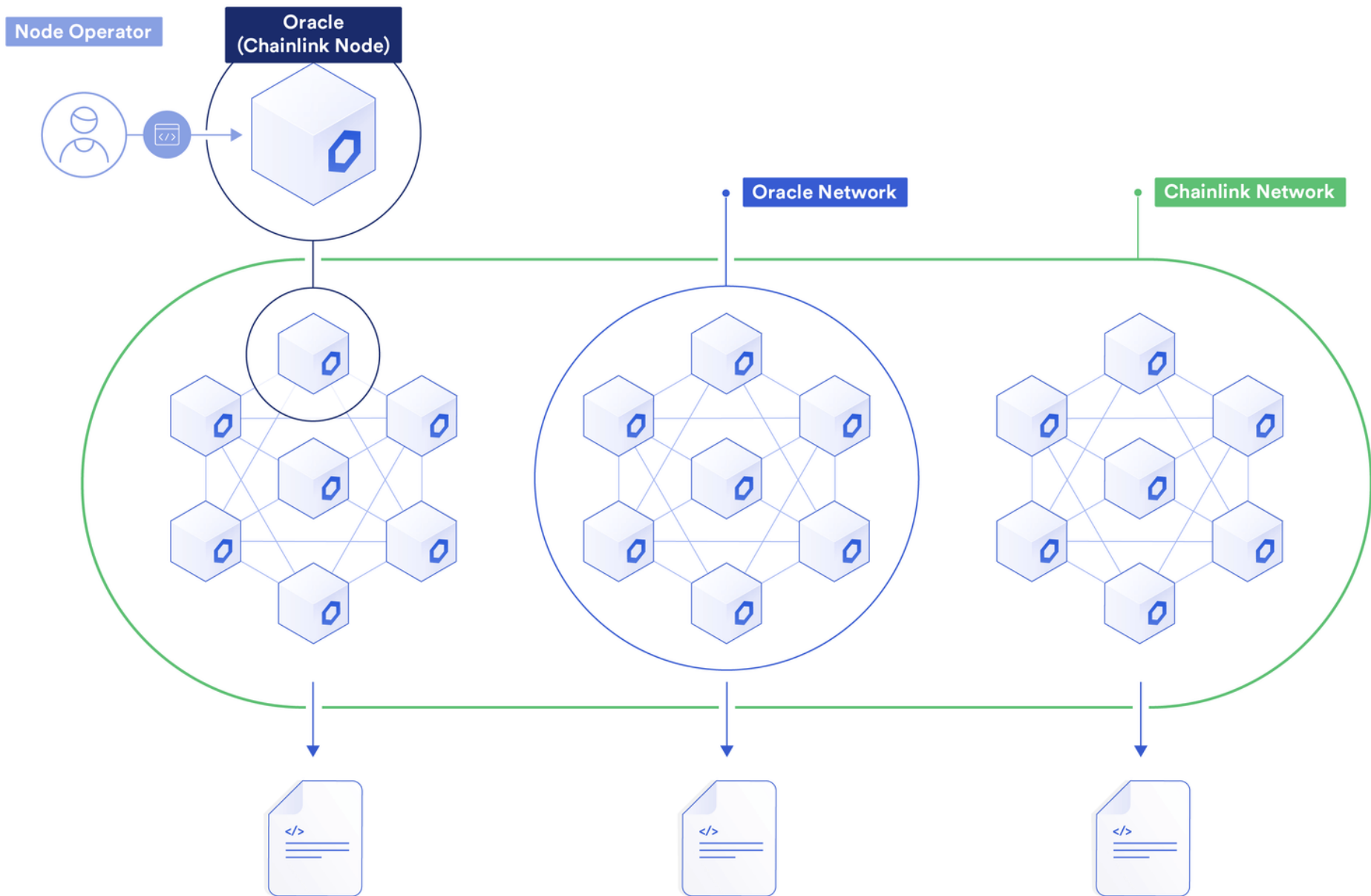
Initially built on Ethereum

Oracle services

LINK

Chainlink Network

- Infinitely scalable
- Independent oracles and oracle networks
- Each oracle runs the Core Chainlink software
- Able to simultaneously be a part of different oracle networks and/or operate independently
- Node operators: entities running the oracle infrastructure
- DONs: maintained by a committee of Chainlink nodes
- Blockchain abstraction layer



Interoperability protocols

Foundation for building blockchain abstraction layers, allowing traditional backends and dApps to interact with any blockchain network through a single middleware.

Capabilities:

- Transfer assets and information across multiple blockchains
- Application developers can leverage the strengths and benefits of different chains
- Building of cross-chain applications → serve more users + provide additional features or products

Chainlink CCIP

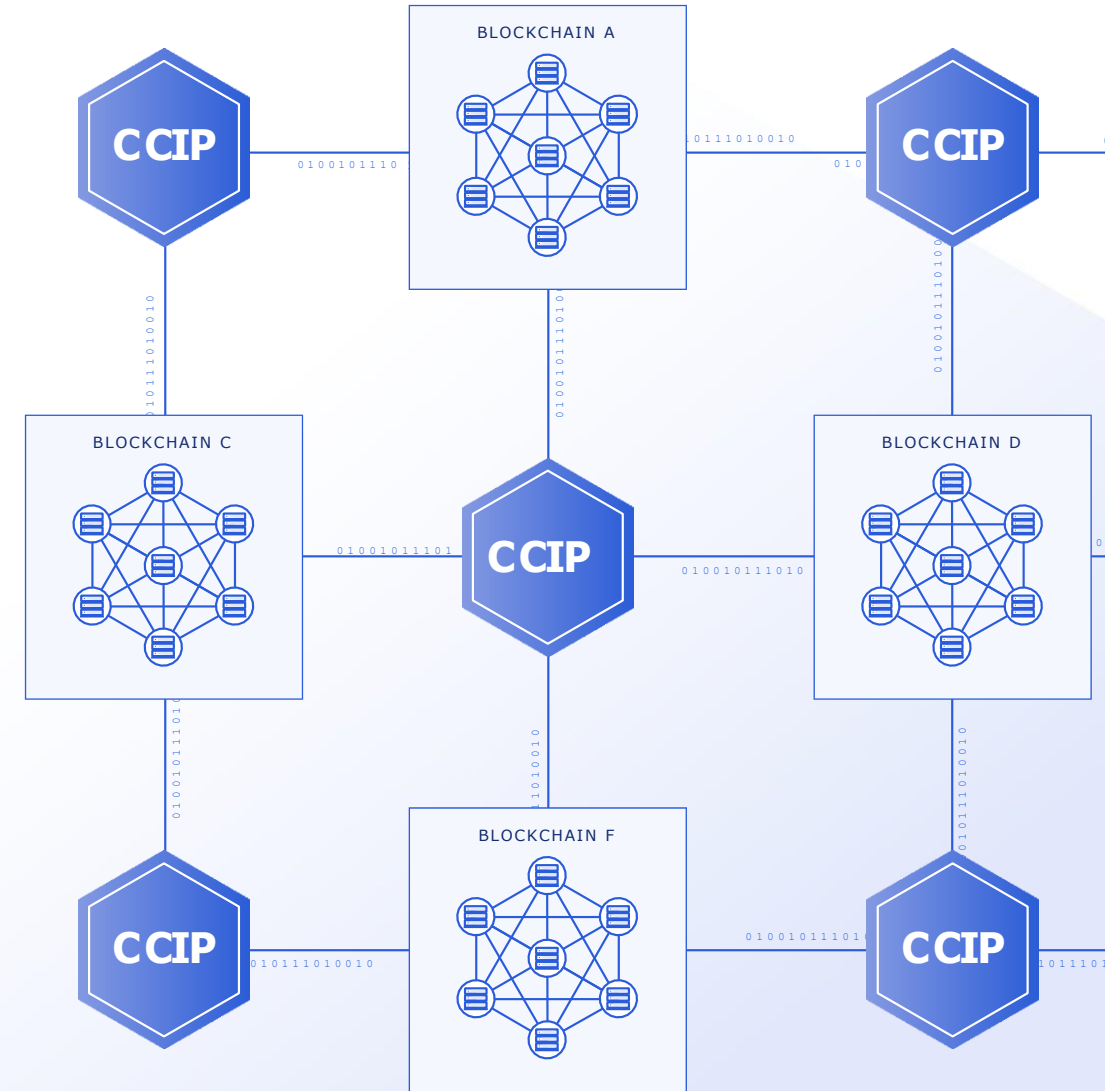
Blockchain Interoperability Protocol

Building secure applications

Transfer tokens, data or both across chains

Defense-in-depth security

Powered by Chainlink's oracle networks



Three main capabilities

Arbitrary Messaging

The ability to send arbitrary data (encoded as bytes) to a receiving smart contract on a different blockchain.

Token Transfer

The ability to transfer tokens to a smart contract or directly to an Externally Owned Account (EOA) on a different blockchain.

Programmable Token Transfer

The ability to simultaneously transfer tokens and arbitrary data (encoded as bytes) within a single transaction.

Chainlink CCIP



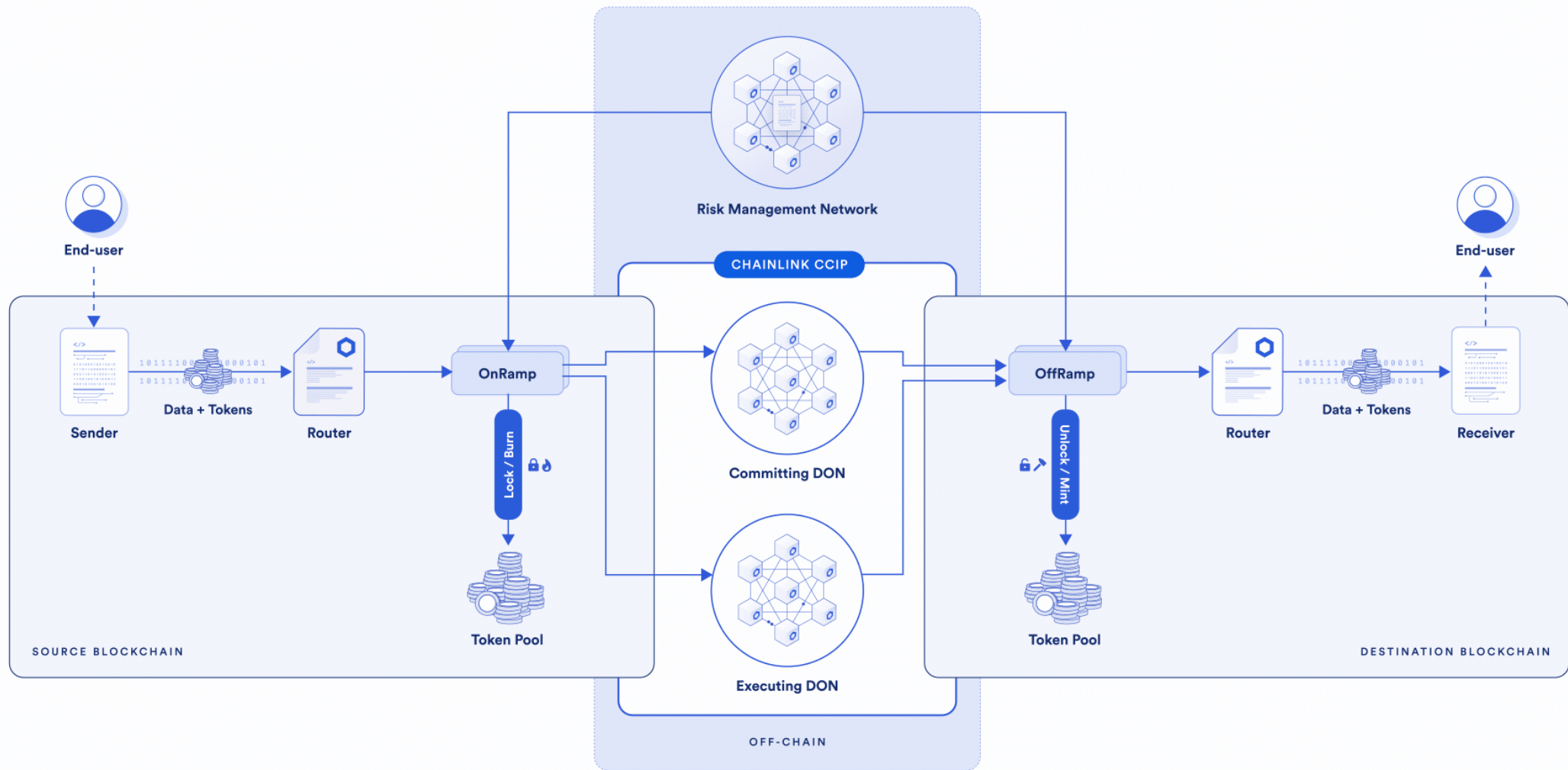
Receiving account types:

- Smart contracts: *data and tokens*
- Externally owned account (EOA): *only tokens*



Use cases:

- Cross-chain lending
- Low-cost transaction computation
- Optimizing cross-chain yield
- Creating new kinds of dApps





Total Value Hacked:

\$2.6B+

1 in 150 chance

Key security benefits

Independent nodes

Three decentralized networks

Separation of responsibilities

Two separate code bases across two different implementations

A trusted computing base of only about 10,000 lines of code

Never-before-seen level of risk management

Three defenses

Rate Limiting

Cap on Value Flow

Blessing

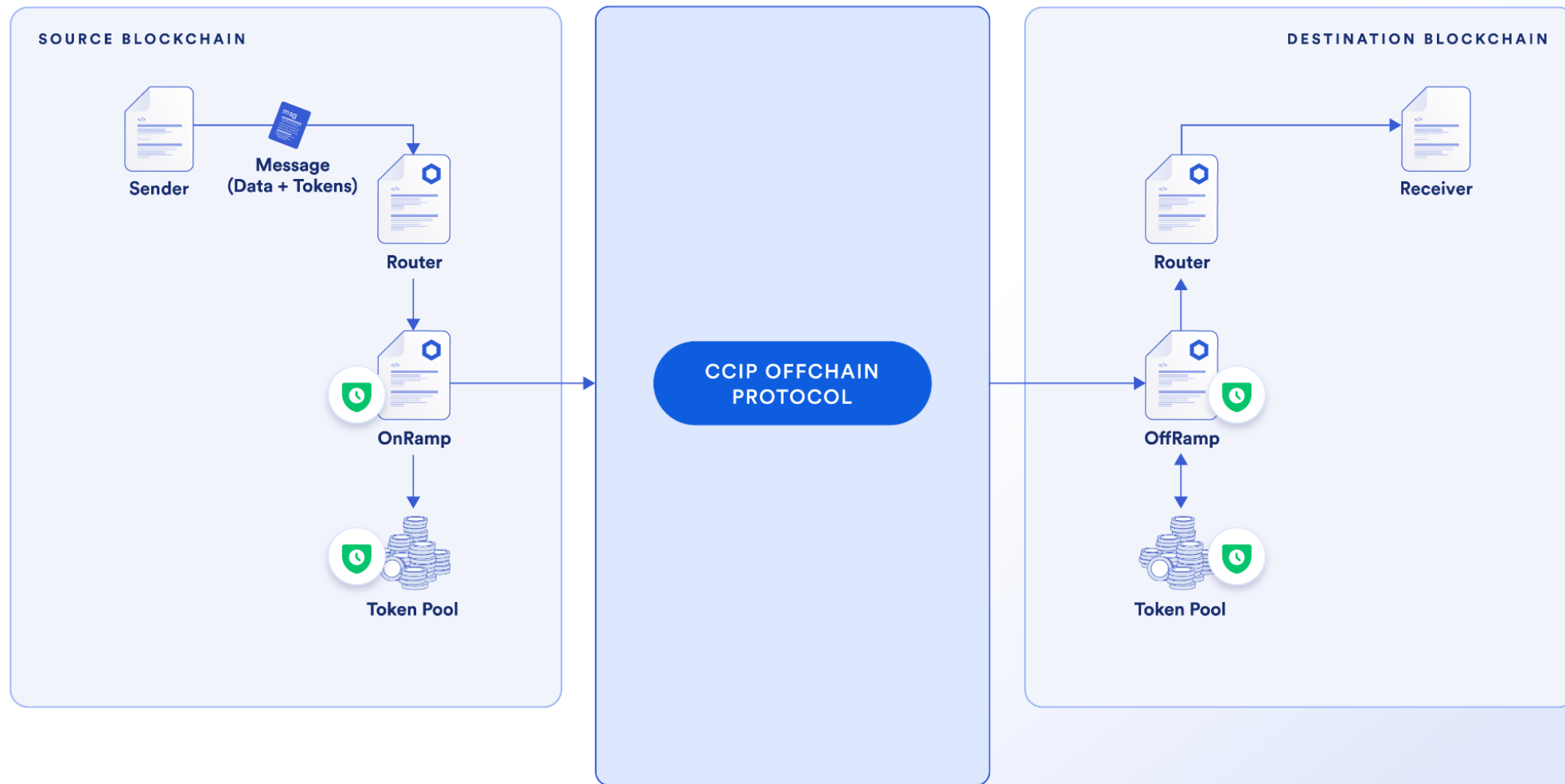
Secondary Approval

Cursing

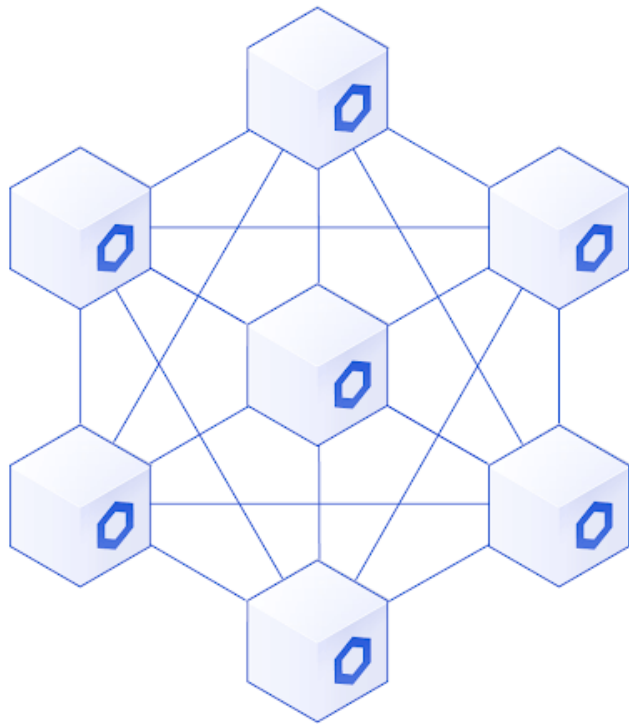
Anomaly Detection

Risk Management Network

Rate Limiting

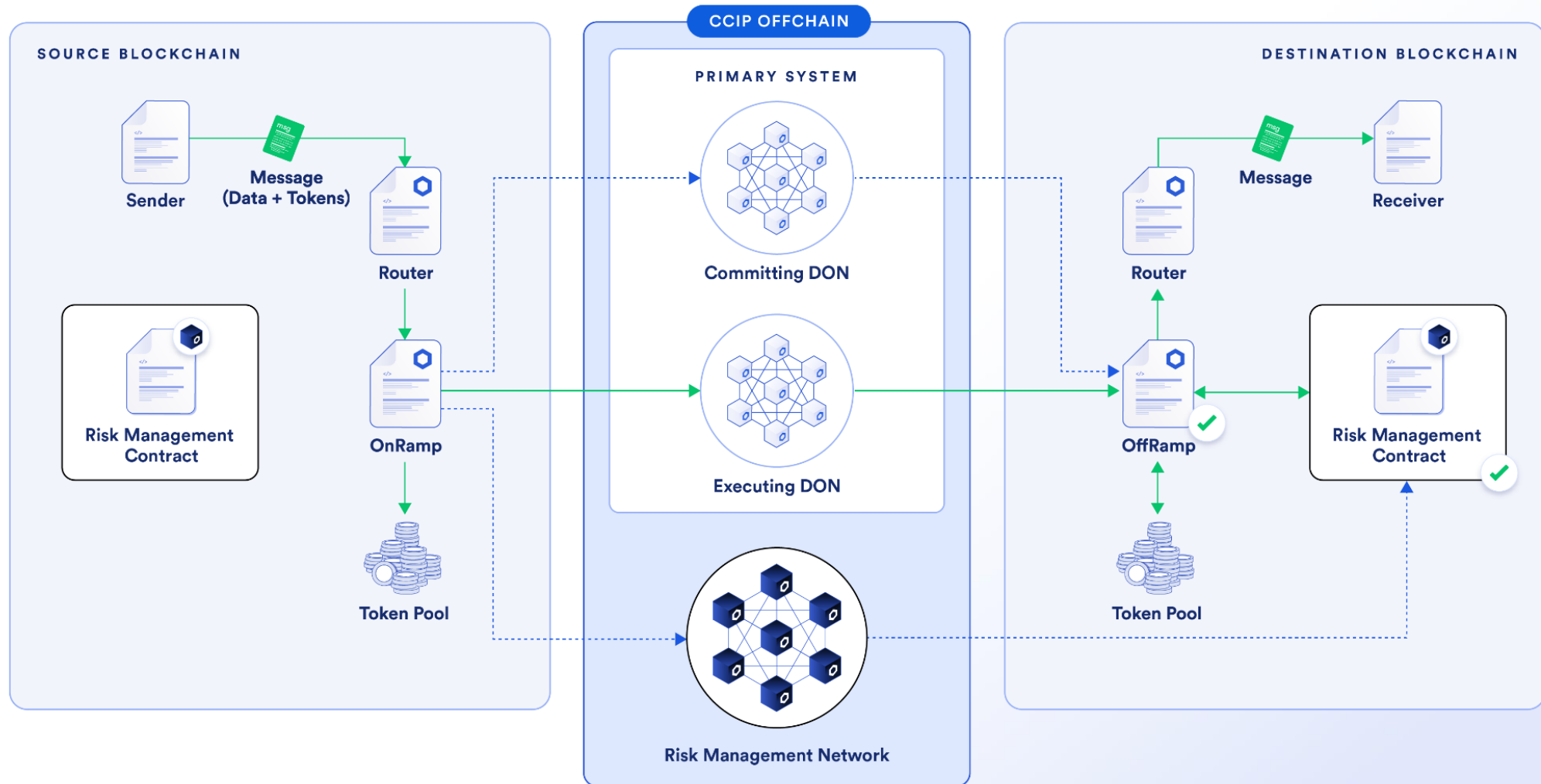


Risk Management Network

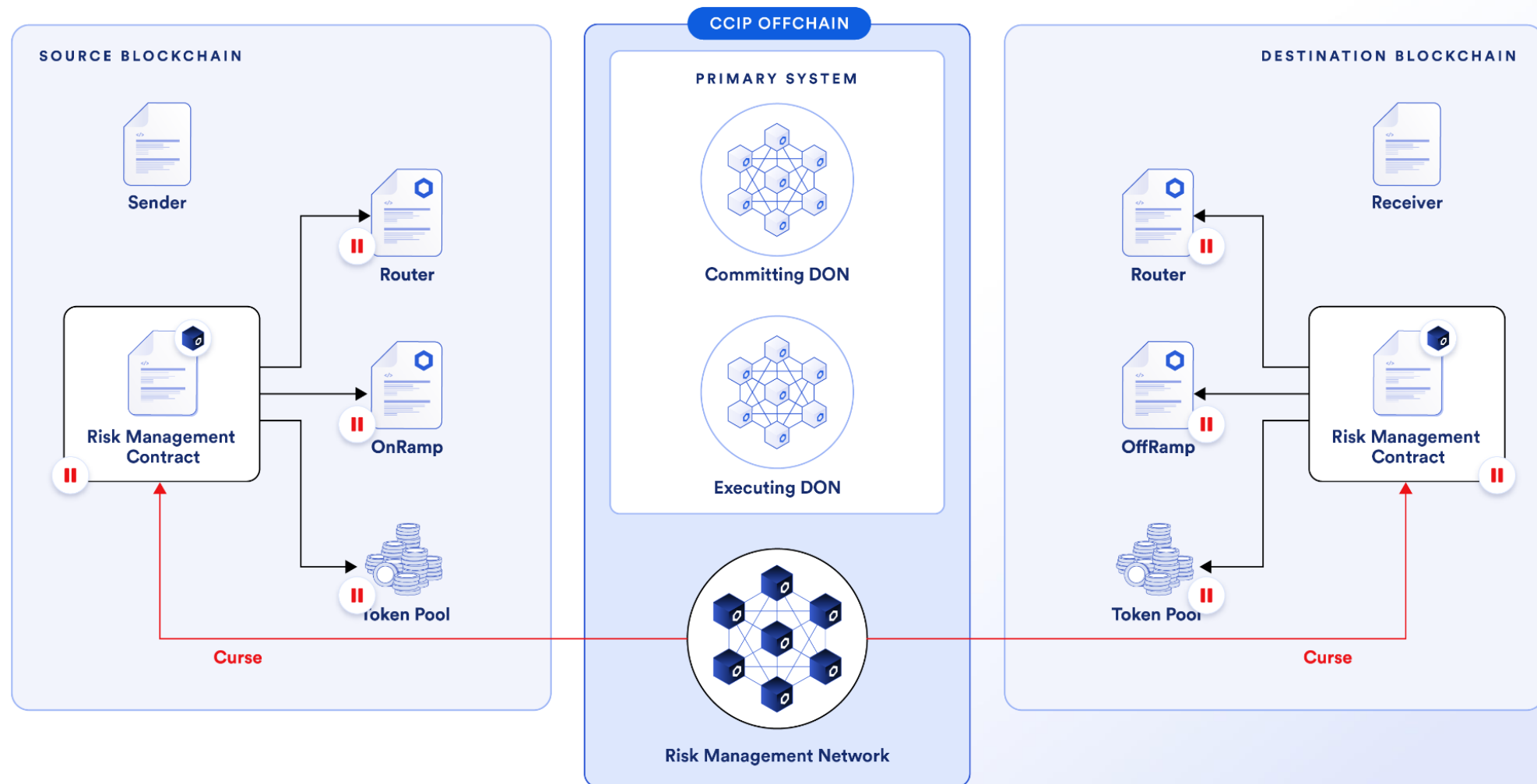


- Separate, independent network
 - Different programming language (Rust)
 - Different development team
- N-version programming (NVP)

Blessing (secondary approval)



Cursing (Anomaly Detection)



My project

Amazing starter kits

Chainlink Local

Limitation: real testing requires having 1 LINK on the Ethereum mainnet

Two smart contract: MessageSender and MessageReceiver

Testing it locally

My project

```
PS C:\Users\zsofi\Documents\BernUni\Blockchain\Chainlink_project> |
```



The background features several light blue hexagons of varying sizes and opacities, creating a geometric pattern. The word "Questions" is centered in a bold, blue, sans-serif font.

Questions