Secured Off-Chain Data for Smart Contracts

Data Empowering the Full Potential of Blockchain Technology

BLOCKSIZE

June 2023

00

Agenda

00 Agenda

01 Introduction (Why bring off-chain data on chain at all?)

02 Smart contracts and hybrid smart contracts

03 The Oracle Problem (How to secure off-chain data?)

04 Decentralized oracle networks

05 Summary and References

BLOCKSIZE

01

Introduction

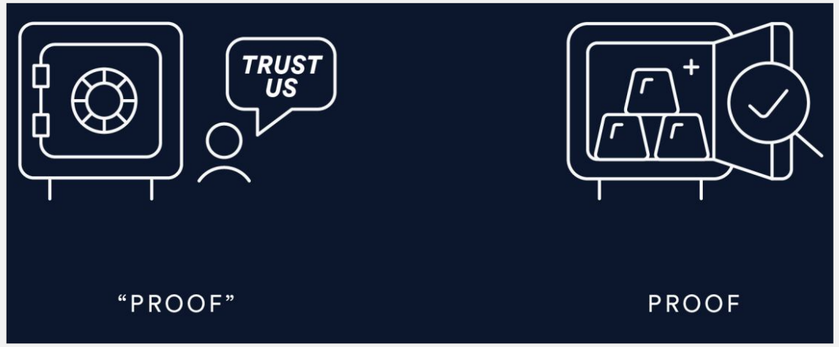


Image by Chainlink

01 Introduction (Why bring off-chain data on chain at all?)

- Synopsis:
  secured off-chain data is what helps smart contracts to unfold the true potential of blockchain technology applications, e.g., in the fields of finance, sustainability, and insurance.

- Why?
  Data on most blockchains is public and immutable:
  everyone can audit and verify it (at least in principle)

- How?
  Data origination needs to comply to the security and integrity standards of the blockchain in use

BLOCKSIZE

01 Introduction (Why bring off-chain data on chain at all?)

Example use case I/III: tracking of carbon offset or sustainability

Key idea: use sensor data to track sustainability of farming and mint carbon-offset tokens for farmers (smart contract users)

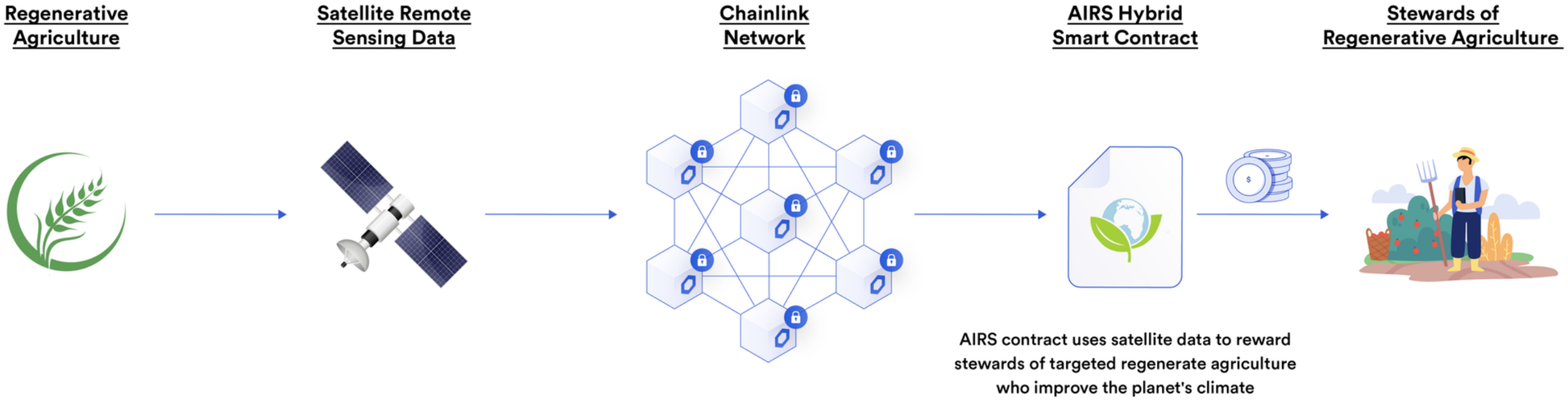


Image by Chainlink

BLOCKSIZE

01 Introduction (Why bring off-chain data on chain at all?)

Example use case II/III: monitoring reserves of stablecoins or tokenized assets like gold (works also for exchanges!)

Key idea: use custodian data to track reserves backing stablecoins or tokenized assets

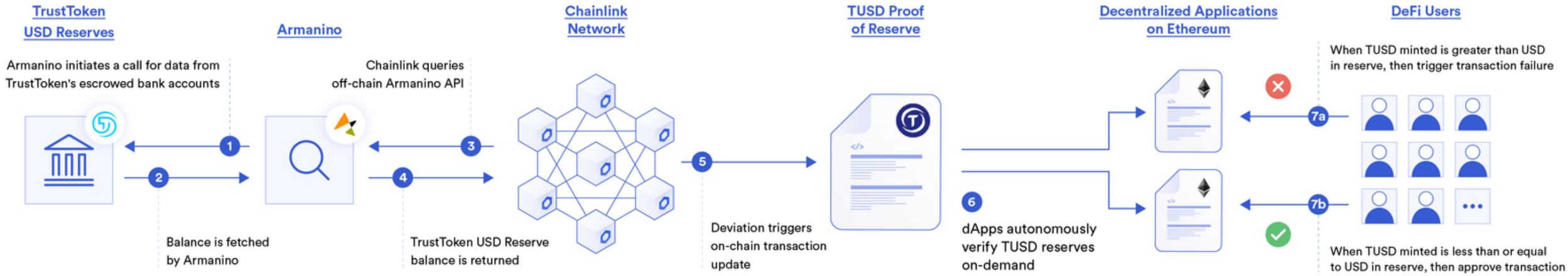
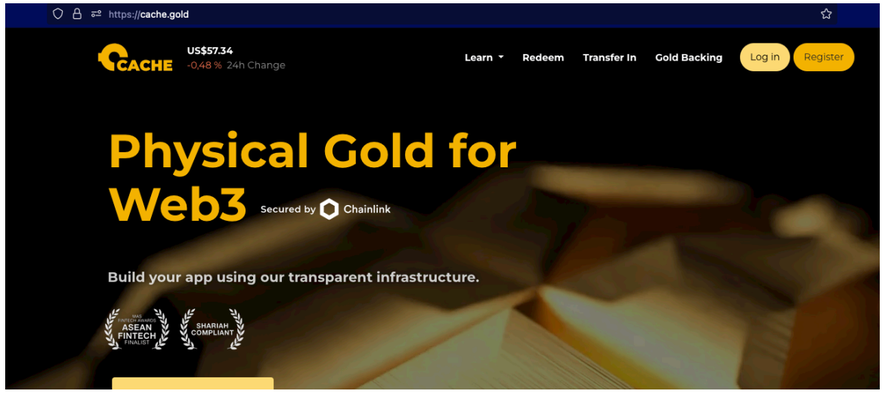


Image by Chainlink



BLOCKSIZE

01 Introduction (Why bring off-chain data on chain at all?)

Example use case III/III: parametric insurance

Key idea: Use sensor data to track the presence or intensity of the insured risk (e.g. natural disaster)

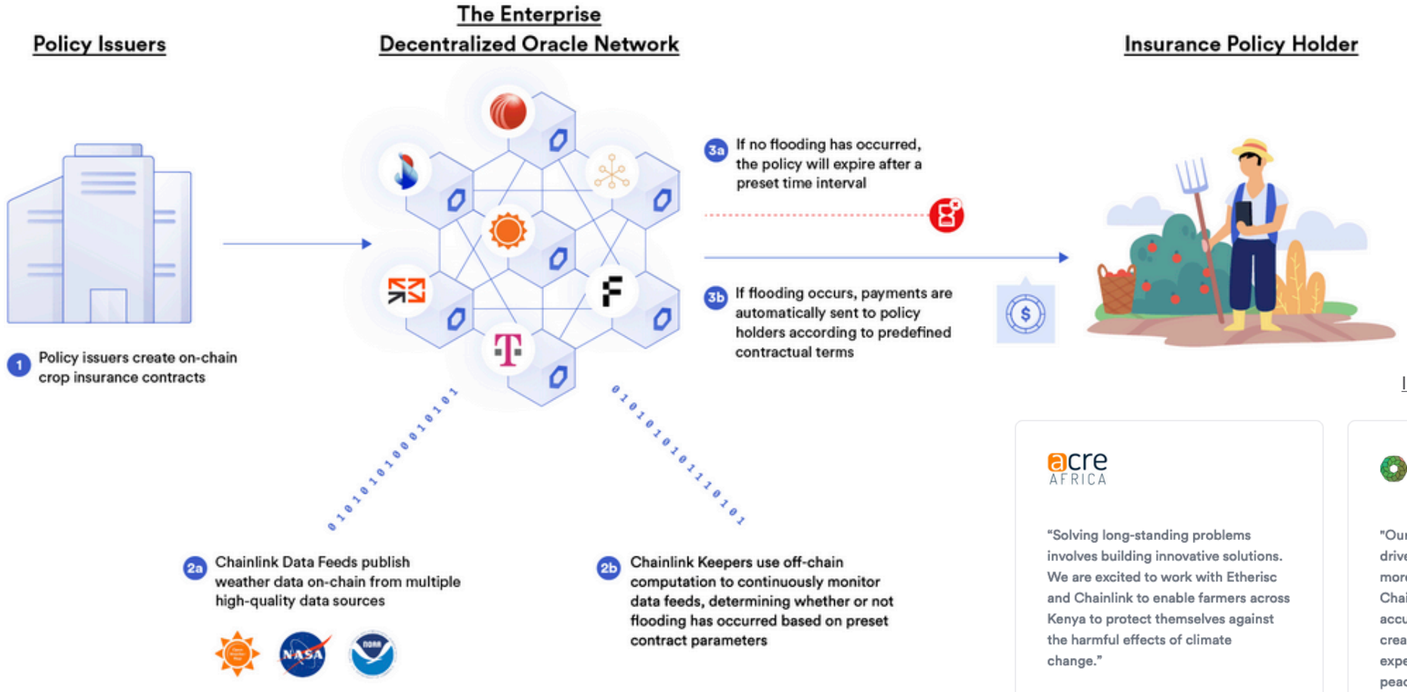


Image by Chainlink

acre AFRICA

"Solving long-standing problems involves building innovative solutions. We are excited to work with Etherisc and Chainlink to enable farmers across Kenya to protect themselves against the harmful effects of climate change."

George Kuria
CEO

ARBOL

"Our core mandate is to make data-driven parametric coverage products more accessible and affordable. Chainlink is integral for providing accurate data to our smart contracts, creating a more transparent coverage experience that gives our clients peace of mind."

Siddhartha Jha
Founder and CEO

ensuro

"Chainlink provides time-tested oracle infrastructure that enhances Ensuro's reliability and flexibility by enabling the seamless addition of more data sources that underwriters can use to create novel parametric insurance products."

Marco Mirabella
CEO

ETHERISC

"Accessible and affordable crop insurance is crucial for smallholder farmers to increase their resilience to climate change. With the aid of Chainlink's decentralized oracle network, Etherisc has the potential to help improve the economic livelihoods of hundreds of thousands of farmers in East Africa."

Michiel Berende
Chief Inclusive Officer

02

Smart contracts and hybrid smart contracts

Smart contracts …

- are compiled programs on a blockchain
- implement functions that can be called via transactions
- can trigger many transactions or state changes in one call
- are executed inside of a virtual machine (by all validators)
- call data (TXs, data) is validated via blockchain consensus mechanism and included in blocks

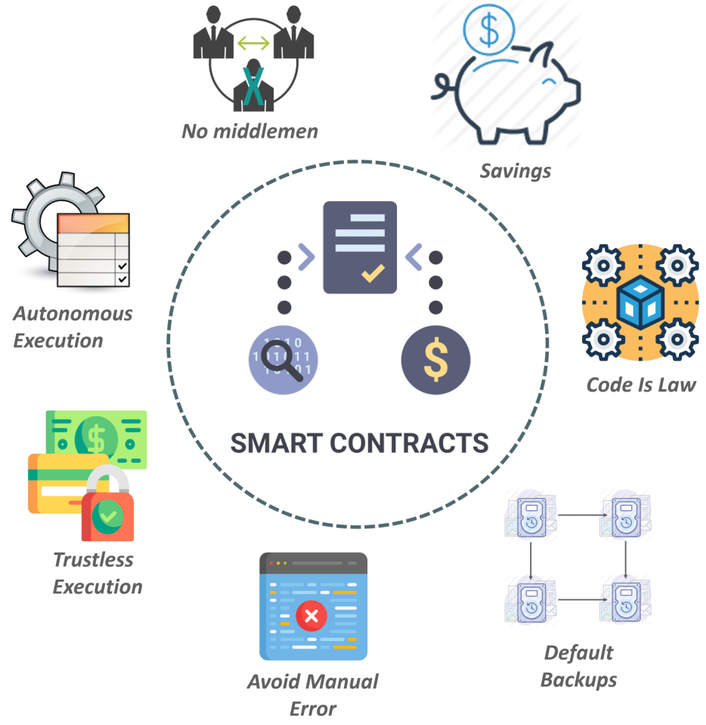


Image by MEXC

BLOCKSIZE

02

Smart contracts and hybrid smart contracts

Hybrid smart contracts …

- are normal smart contracts that need off-chain data for their function
- enable an exciting amount of applications in DeFi:
  - insurance
  - proof-of-reserves
  - carbon tracing and many more
- are at the origin of The Oracle Problem:
  - a single-origin data input could manipulate the outcome of the hybrid smart contract's functions

Image by Chainlink

BLOCKSIZE

03

The Oracle Problem

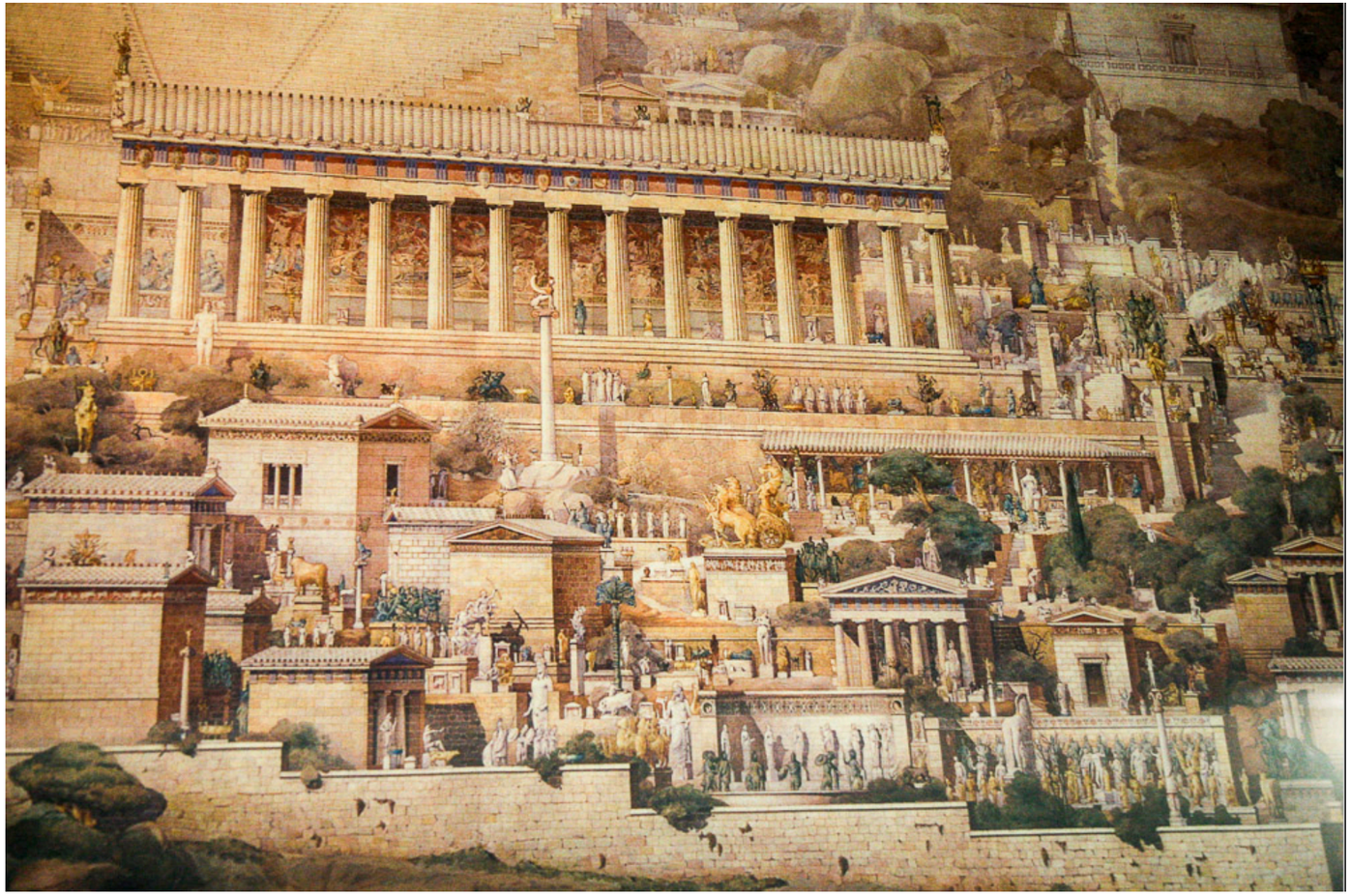


Image by Ancient-Greece.org

BLOCKSIZE

03 The Oracle Problem (How to secure off-chain data?)

On the Oracle Problem and its resolution via data decentralization

- Data from a single origin defeats the purpose of the decentralization of the blockchain in use
- That's the Oracle Problem:
  tampered (centralized) data could manipulate smart contracts while their execution would still be (decentrally) validated
- much like Pythia in ancient Delphi could have manipulated the pilgrims listening to her forecasts delivered by priests (intermediaries)

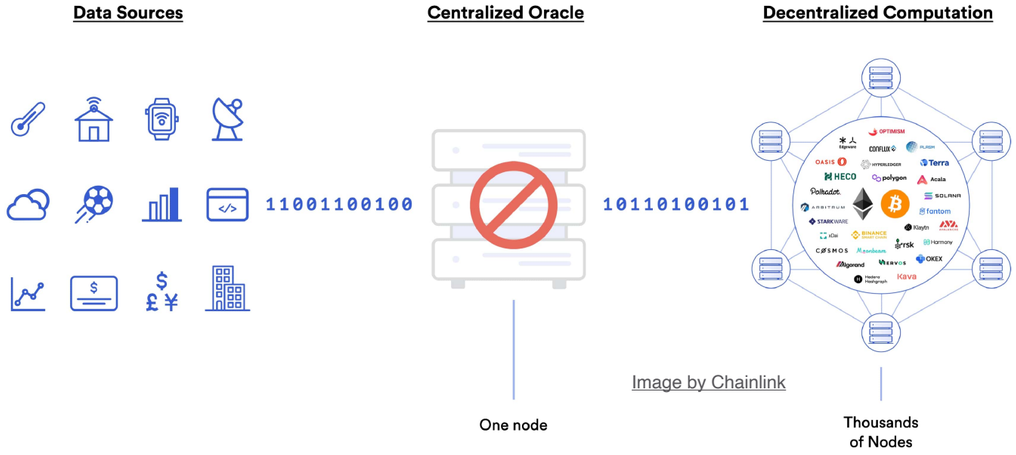


Image by Chainlink

BLOCKSIZE

03 The Oracle Problem (How to secure off-chain data?)

On the Oracle Problem and its resolution via data decentralization

How to resolve the Oracle Problem?

- decentralized oracle networks: introduce decentralization to data origination
  - data from different independent origins
  - consensus mechanism between data origins
  - validated, decentralized data is forwarded to hybrid smart contracts

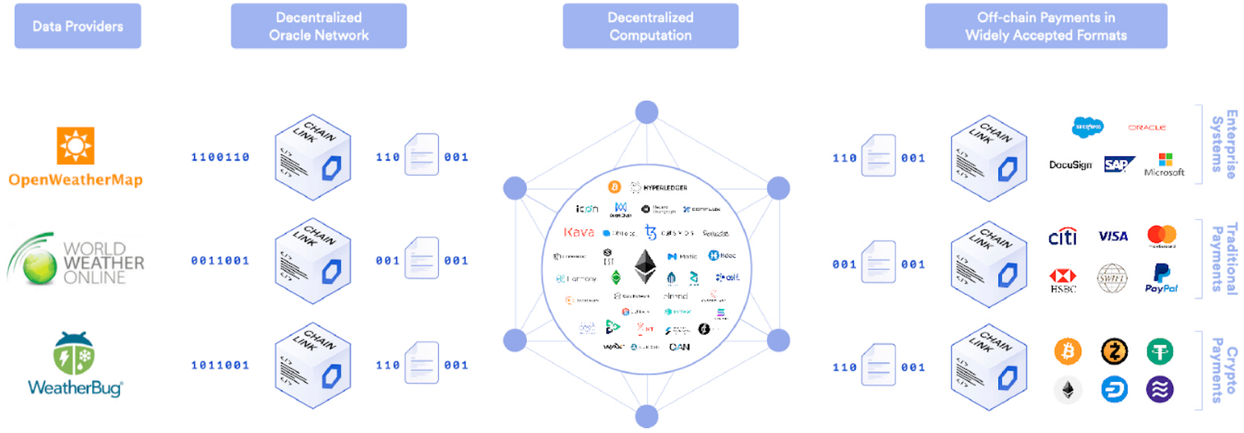


Image by Chainlink

Chainlink

BLOCKSIZE

04

Decentralized oracle networks

DONs enable a tremendous amount of blockchain technology applications

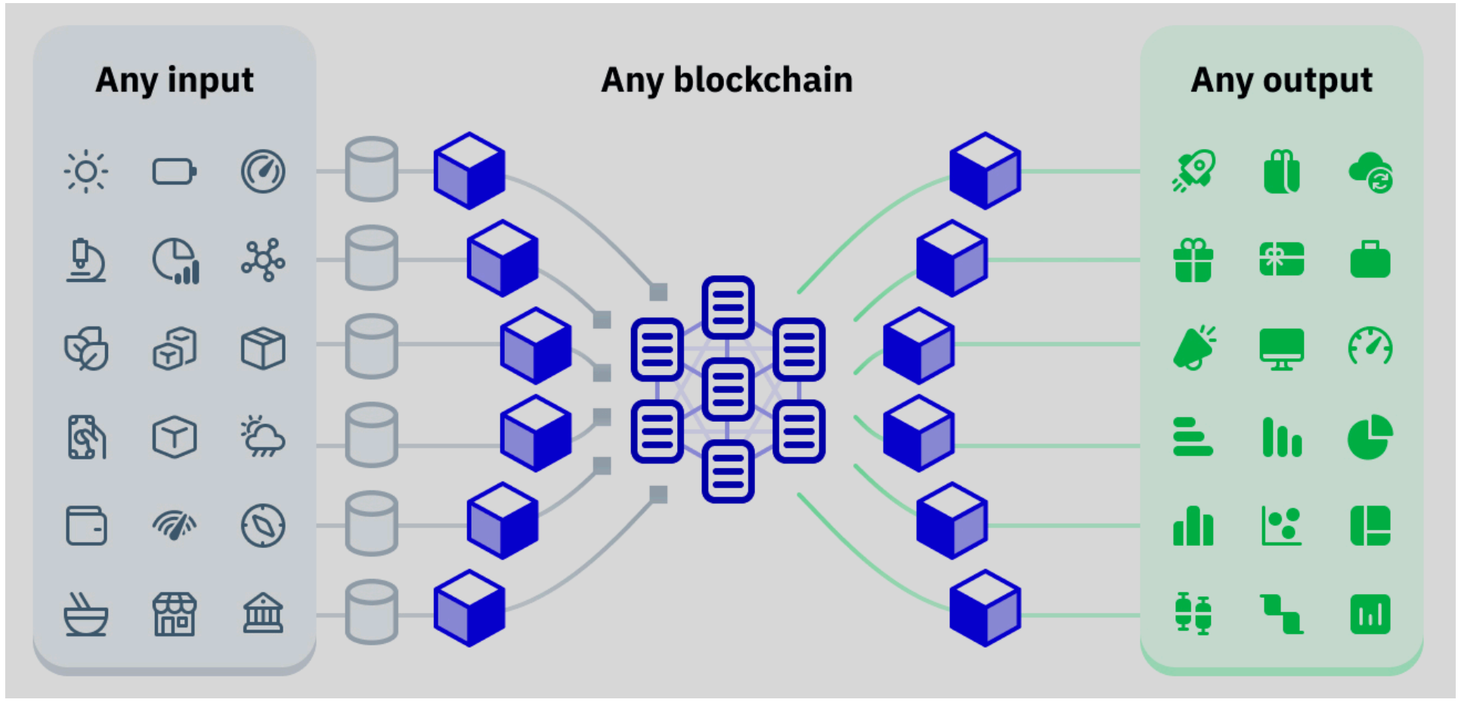


Image by Chainlink

BLOCKSIZE

04 Decentralized oracle networks (DONs)

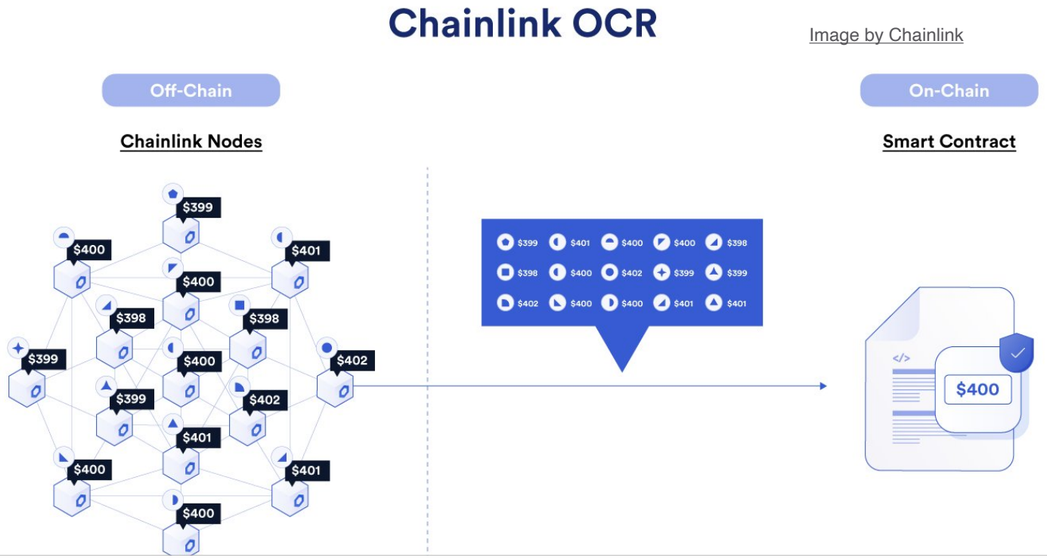
Existing DON implementations

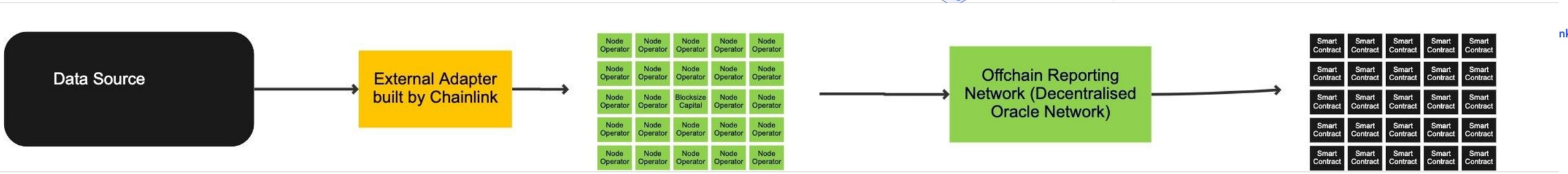
- Chainlink
    - Started on Ethereum, now on many chains
    - Decentralization via the so-called off-chain-reporting network (OCR)
    - OCR is a peer-to-peer network
    - OCR node operators transact data to the blockchain (they need to also operate nodes in the blockchain network)
    - OCR implements anomaly detection and consensus on data, incentives for oracle accuracy and reliability
- BAND
    - BAND has its own blockchain (BANDchain) with a proof-of-stake consensus, but is connected to many chains via cosmos' IBC
    - Validators on BANDchain make a consenus on data provided by Oracles
    - Accuracy of Oracles is incentivized by fees, i.e., if their data is validated in the consensus
- PYTH
    - Started on Solana, now on many blockchains
    - Incentive alignment via staking: oracles stake tokens on the accuracy of their data
    - Stake is slashed if consensus finds oracle data to be inaccurate

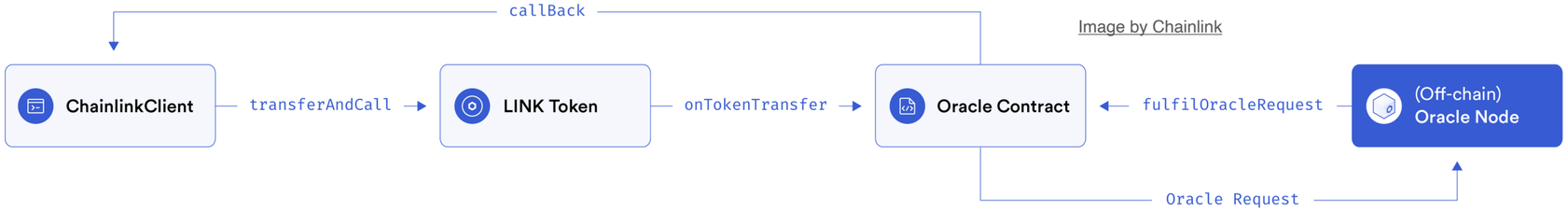
04 Decentralized oracle networks (DONs)

DON implementation of Chainlink in more detail

How do Chainlink DONs work?







BLOCKSIZE

04 Decentralized oracle networks (DONs)

DON implementation of Chainlink for cross-chain oracles

- OCR network can be used as a relay between different blockchains
- OCR nodes may publish data to several blockchains
- OCR nodes can read data from one chain and publish to another or several others

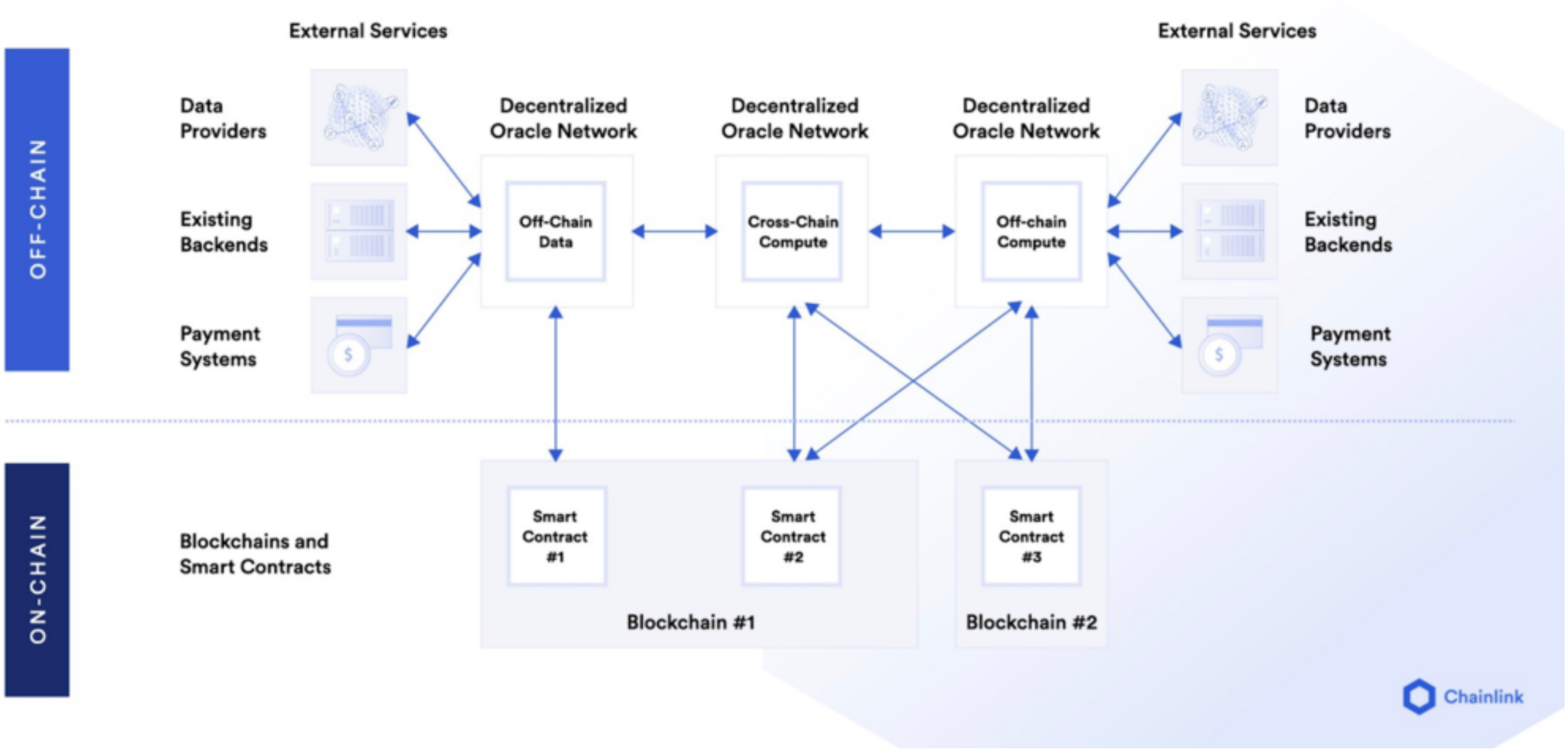


Image by Chainlink

BLOCKSIZE

05

Summary and References

Secured off-chain data is what helps smart contracts to unfold the true potential of blockchain technology applications, e.g., in the fields of finance, sustainability, and insurance.

BLOCKSIZE

Summary:

- Secured off-chain data unleashes the true power of blockchain technology applications
- Hybrid smart contracts and decentralized oracle networks are awesome and exciting technological concepts
- Example use cases: data-driven incentive alignment (carbon tracking), trustless risk transfer (parametric insurance), automated auditing (proof-of-reserves)

Further reading:

Chainlink's off-chain reporting: https://blog.chain.link/off-chain-data-and-computation/

Other DONs: https://bandprotocol.com/ https://pyth.network/

Sustainability: https://blog.chain.link/hyphen-receives-grant-to-build-oracle-framework-for-tracking-greenhouse-gases/

http://greenworld.org/ https://chain.link/use-cases/climate-markets

Insurance: https://www.weforum.org/agenda/2021/06/blockchain-can-help-us-beat-climate-change-heres-how/
https://www.coindesk.com/tech/2020/08/19/chainlink-to-provide-data-for-farming-insurance-startup-arbol/

Proof-of-Reserve: https://chain.link/proof-of-reserve https://cache.gold/proof-of-reserve-transparency
https://blog.chain.link/stablecoins-and-proof-of-reserve/

BLOCKSIZE

Passion to enable

www.blocksize-capital.com

Dr. Axel U. J. Lode
Head of Decentralized Finance
Email: al@blocksize-capital.com