Chainlink

The Ultimate Guide to Blockchain Oracle Security

MARCH 2022

Why Oracle Security Matters

Most Web3 developers know that security should be their top priority. However, many are unaware that the process of securing a smart contract extends to include a critical component for any use case that requires data or computation outside of a blockchain—the oracle.

Integrating off-chain data inputs within a smart contract greatly expands the realm of possibility for dApp developers but also adds security concerns; your smart contract now has to rely on data provided by an oracle to execute its functions. Even when the other components of your smart contract meet the most rigorous standards of security, if an entity can tamper with the data input or the data isn't delivered in a secure and timely manner, you can run into serious problems—and your entire contract might be at risk. Your smart contract is only as strong as its weakest link, and any breach can have serious negative consequences.

Poor oracle security can expose your smart contract to a wide range of potential exploits and hacks. That's why the quality of data inputs and the security of the oracle mechanism delivering them on-chain are integral to the security of any decentralized application.

> *"Many people overlook the importance of oracles in their smart contract application. The reality that we see time and time again is that a smart contract application's security is only as strong as its oracle."*

Trader Joe

0xMurloc
CO-FOUNDER OF AVALANCHE DEFI PROTOCOL TRADER JOE

With this in mind, it's clear that choosing the right blockchain oracle is crucial to the security of your project. In this guide, we lay out five key security risks to look out for when choosing a blockchain oracle—and the right oracle infrastructure that can help mitigate these risks.

Data, Oracle Nodes, and Oracle Mechanisms: A Three-Part Solution

In order to make an informed decision when choosing a blockchain oracle, it's important to understand the security layers of blockchain oracles.

In general, there are three domains of concern when it comes to blockchain oracle security. Every component plays a critical role and comes with its own sets of risks and best practices.

Data sources
Accuracy, reliability, and timeliness are of paramount importance when sourcing data. A single inaccurate data point, even if it registers for only a few seconds, has the potential to cause irreparable harm to your project.

Oracle nodes
Entities that deliver the requested data directly to smart contracts. Much like data sources, oracle nodes must be timely, reliable, and secure, as they are the stewards of your smart contract's connection to external information.

Oracle mechanisms
The mechanisms that are responsible for blockchain oracles and oracle network design. They decide how much control any individual node has over the delivery of data and its contents, the range of data sources available, and the level of decentralization within each network component.

5 Oracle Risks—And Solutions

1 Low-Quality Data Inputs Result in Low-Quality Outputs

Not all data sources are created equal. Consistently generating high-quality and accurate data often requires time, money, and a dedicated team of people. This is why many data providers require paid subscriptions or charge fees for access to their premium data sets.

In order to access these premium data sets on-chain, developers must find an oracle solution that has the ability to manage account logins and securely store API credentials. Without this ability, your access is limited to only free and openly available data sources.

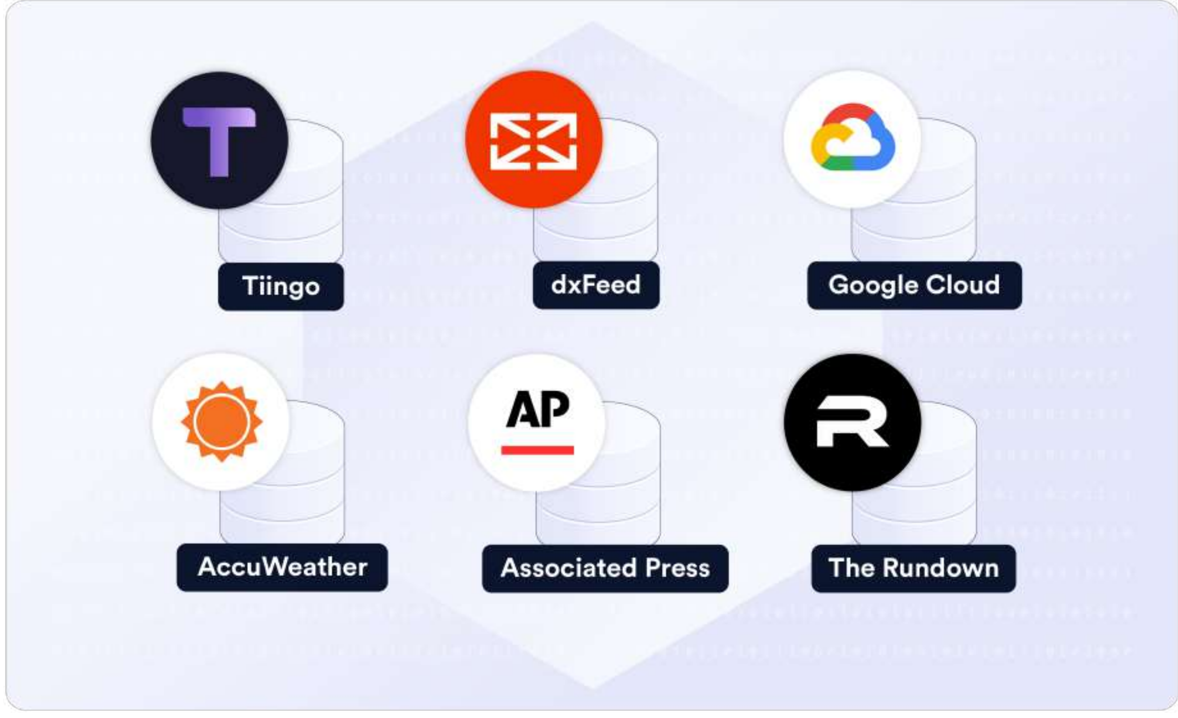
Problem: Unreliable free-tier APIs

Why are free-tier APIs a problem? Put simply, they can be unreliable.

While pulling data from free APIs or crowdsourced user submissions is relatively easy and cost-effective, free APIs often lack legally binding availability or service quality guarantees. Thus, the tradeoff is that these feeds can lack the accuracy and uptime guarantees needed to build a truly reliable protocol. An inaccurate data input, even for a short period of time, can lead to compromised user funds.

Takeaway: Use premium data providers

Look for oracle mechanisms that have built-in credential management capabilities for oracle nodes through modular adapters. Some blockchain oracles might use only free APIs, while others exclusively source data from premium data providers—go for premium data offerings that offer standardized, high-quality data, advanced aggregation methodologies, quicker response times, and service guarantees to better ensure your smart contract won't be compromised.



Chainlink is adopted by leading data providers.

> *"Chainlink is the undisputed leader in the oracle space — it has a proven track record of solving the oracle problem and providing high-quality data to live DeFi applications."*
>
> DODO Lei Mingda
> FOUNDER OF DODO

2 Single Data Sources Create Single Points of Failure

In addition to a high-quality data source, some data types require data redundancy in order to safely be used within decentralized applications.

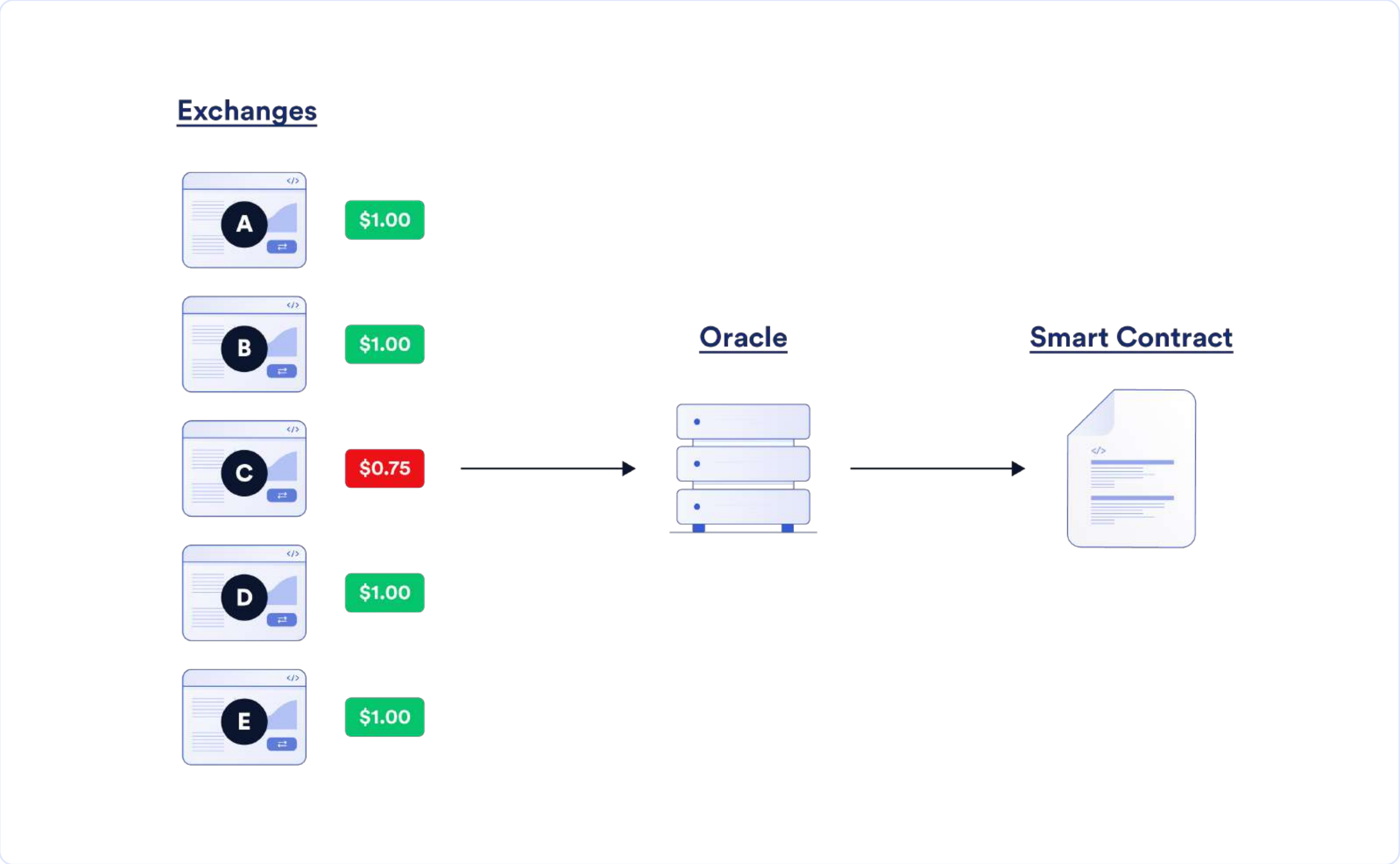
Applications that need price data on cryptocurrencies and tokens should be particularly wary of using a single data source or just a few data sources. Because these assets are so liquid and common, and trading activity takes place across a multitude of centralized and decentralized exchanges, it's possible for any single exchange to have a significantly different price from the larger market. Volume can also shift rapidly between exchanges, leaving oracle mechanisms with low market coverage exposed to data manipulation.

That's why it's important to think about the particular data type your smart contract needs and avoid single points of failure with redundant data.

Problem: Inaccurate prices and flash loan attacks

If your oracle mechanism relies on a single data source, it is vulnerable to price manipulation by well-capitalized malicious actors.

For example, if your oracle mechanism only feeds in a single data source from a decentralized exchange, your protocol is susceptible to price manipulation by flash loan-funded attacks. Flash loans enable users to briefly access a large amount of funds to make a quick, profitable trade. While flash loans in themselves are unproblematic, savvy hackers can use them to manipulate a single exchange's price for a short period of time. This leaves a window for hackers to exploit smart contract functions that are dependent on the exchange's price data.

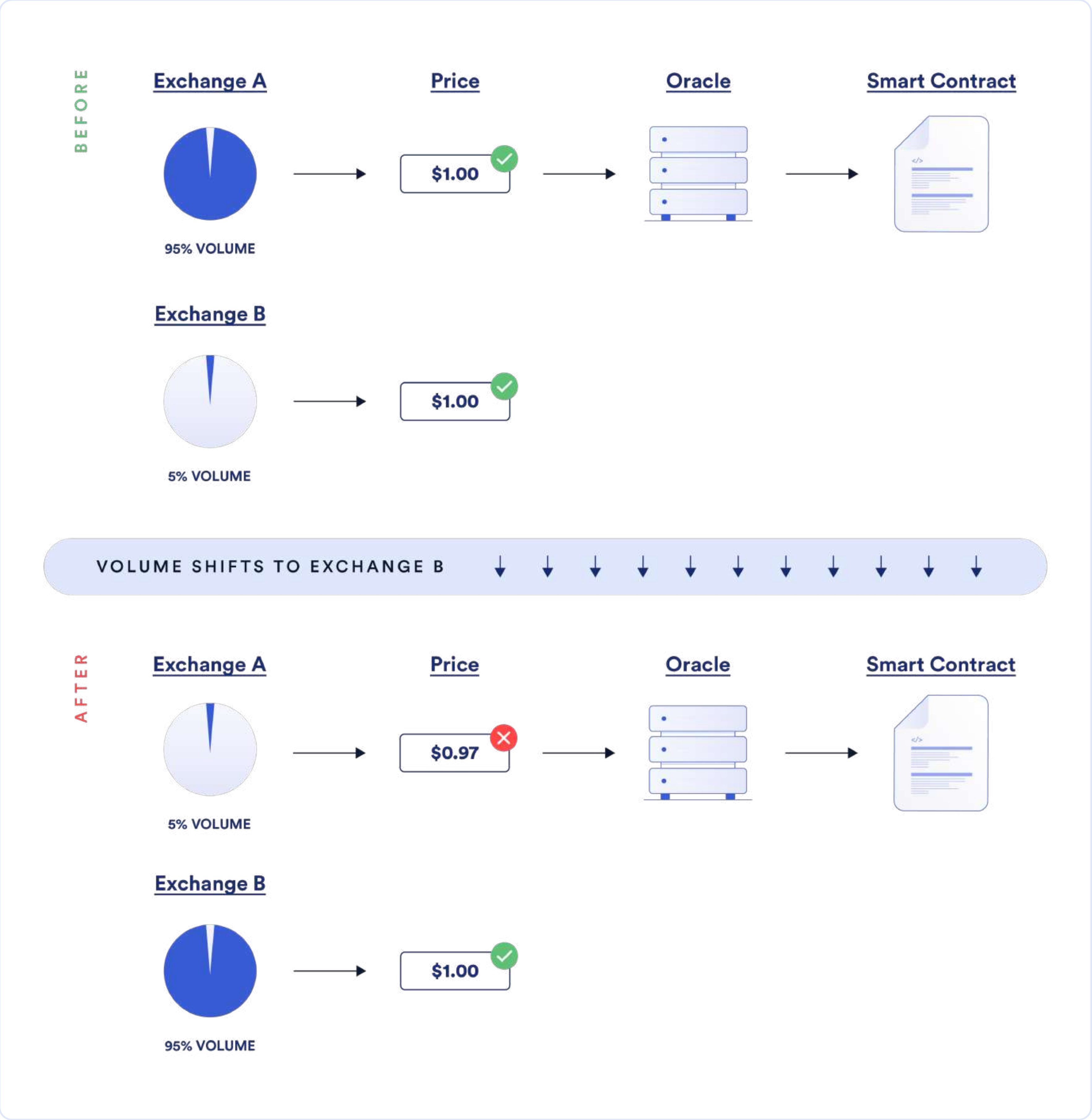


Single data sources can be manipulated by savvy attackers, leading to inaccurate data reporting.

Problem: Exchange volume shifts

Oracles that aggregate data from a select few predefined exchanges do not account for volume shifts to new exchanges not covered by the oracle mechanism.

This inherently makes the price data less reliable and secure. A sudden and unexpected decrease in volume means it's much easier for the price to move up or down, making it that much more likely the data isn't representing the fair market value.



Exchanges with little to no volume can unexpectedly deviate from the fair-market average price, making them unsuitable for dApps.

Takeaway: Integrate oracle networks that use a volume-weighted average price

Look for oracle networks that source data from professional data aggregators to maintain a volume-weighted average price across all trading environments.

Because they have deep liquidity pools, exchanges with higher volume tend to have better price discovery. Oracle networks using a volume-weighted average price account for both the extra reliability of pricing from high-volume exchanges and the potential unreliability of pricing from low-volume exchanges to deliver an accurate market price to your smart contract. Ideally, an oracle provider should also exclude outliers and fake exchange volume for further accuracy.

3 Individual Oracle Reliance Leads to Centralization Risks

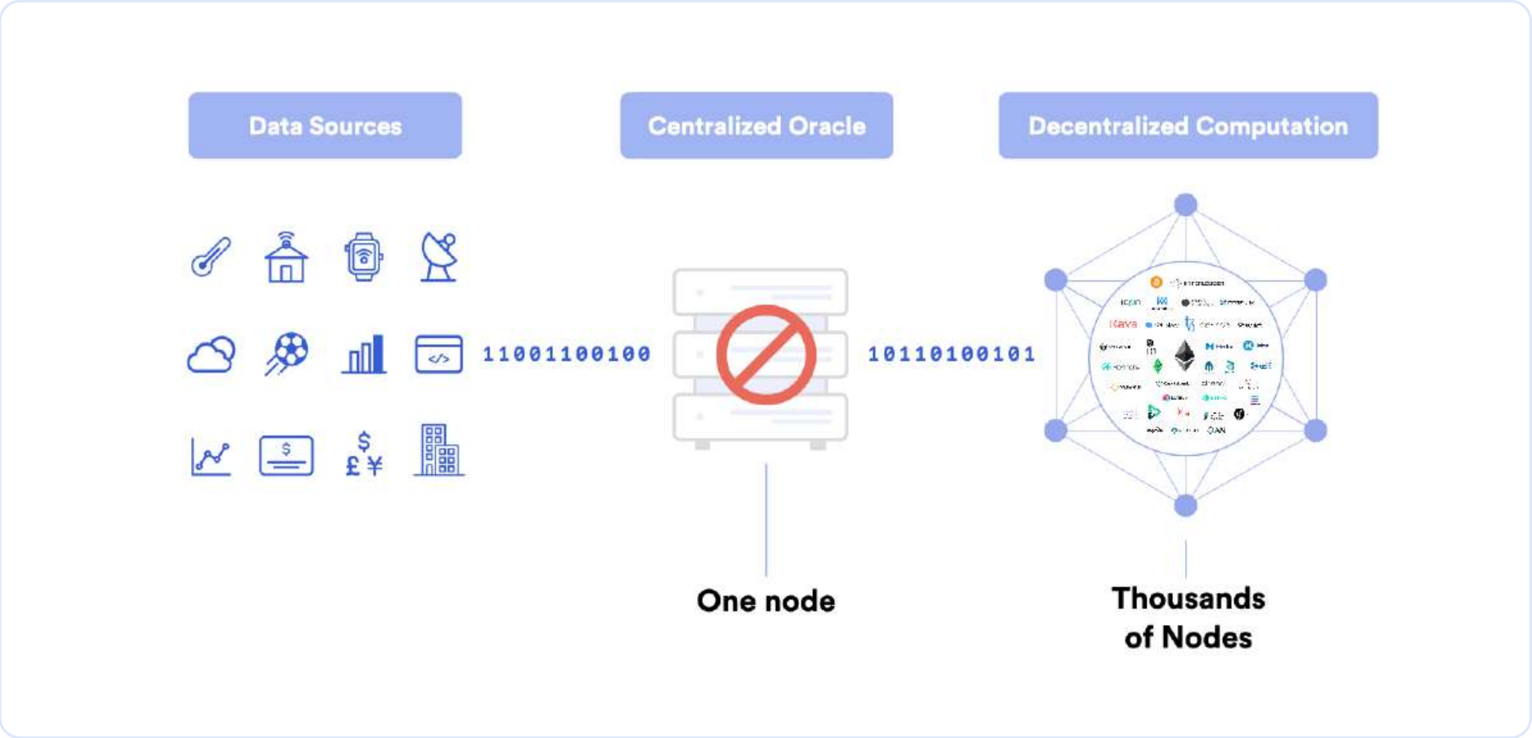
Even with the most reliable and accurate price data in the world, if there's only one oracle node delivering the data on-chain, your smart contract is vulnerable to a centralized point of failure.

Smart contracts need to be triggered by high-quality, tamper-proof data as they are irreversible and execute automatically. Oracles need multiple redundancies in the data delivery process through a decentralized network of independent oracle nodes.

Problem: Centralized data delivery

Reliance on a single oracle creates:

- Downtime risk—with only one centralized node operator, your smart contract relies on one entity operating 100% of the time, with no room for error.
- Avenues for manipulation—a centralized node means a single point of control over the entire data delivery mechanism and input, leading to the possibility of data manipulation for nefarious purposes.



Centralized oracles are a single point of failure.

Takeaway: Use decentralized oracle networks that aggregate multiple node responses

Chainlink decentralized oracle networks aggregate responses from numerous individual oracle nodes within an oracle network. For price data points, each individual node inputs a specific data point, which is then aggregated on the network level to remove the risk of downtime or data manipulation from any one oracle node.

> *"Integrating Chainlink price reference contracts as the basis for rebalancing our capital pool brings tremendous security to our members, who know that our most important assets are deeply insulated against any known or unexpected attack vectors."*

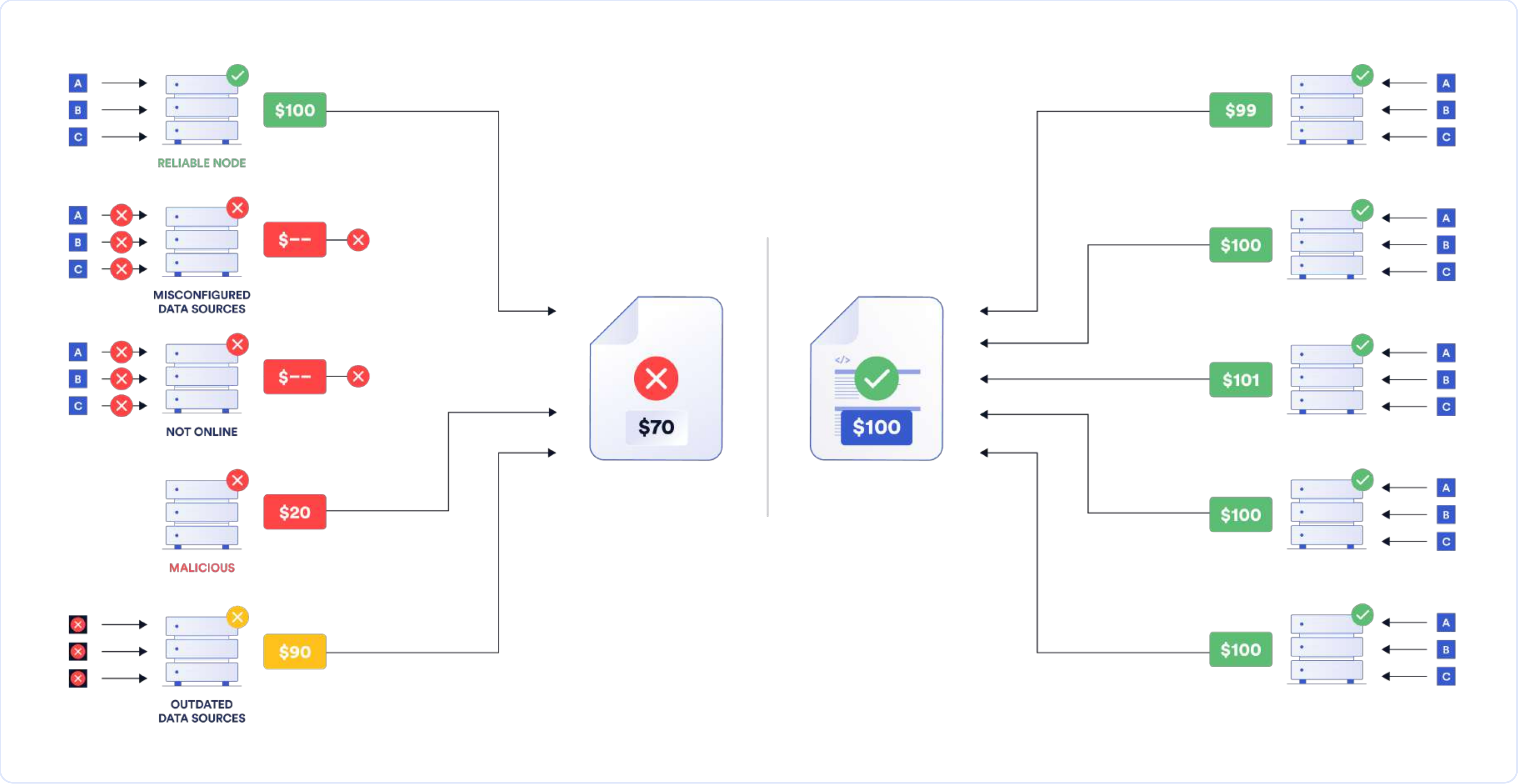
Nexus Mutual

Hugh Karp
FOUNDER OF NEXUS MUTUAL

4 Unreliable Node Operators Diminish Overall Network Quality

Oracle nodes are only as good as the teams running them. Delivering data to smart contracts with constant accuracy and reliability is a difficult task that requires years of experience in development operations (DevOps).

Though oracle networks present less risk than relying on any single node, every node of a well-functioning blockchain oracle network should be run by a world-class node operation team. An unreliable node operator can compromise the ability for an oracle network to function securely.



Unreliable or malicious oracle nodes can lead to the deterioration of the performance of the entire oracle network, resulting in inaccurate data.

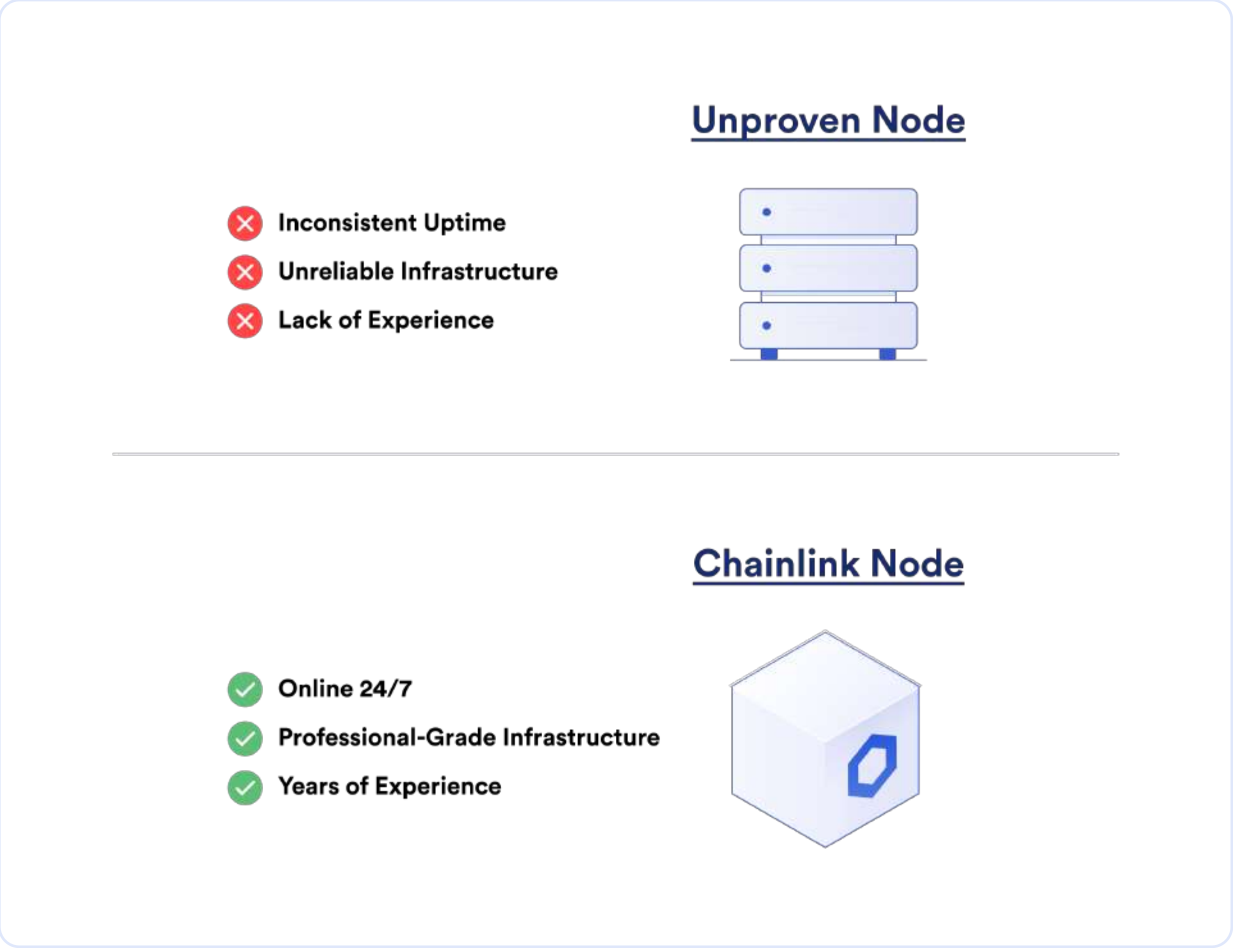
Problem: Unproven oracles

Oracle networks without proper oracle node standards expose contracts to larger attack surfaces, often leading to the diminished security of the oracle solution.

Takeaway: Identify oracle solutions with time-tested node operators

Find an oracle solution that exclusively uses security-reviewed oracle nodes run by DevOps teams with known identities and proven industry experience.

Node operation is a high-skill task, and identifying oracle networks with provably reliable nodes helps ensure constant uptime and secure delivery.



Chainlink oracle nodes are operated by professional DevOps teams with a proven track record of performance.

5 Opaque Oracle Mechanisms Invite Unknown Risks

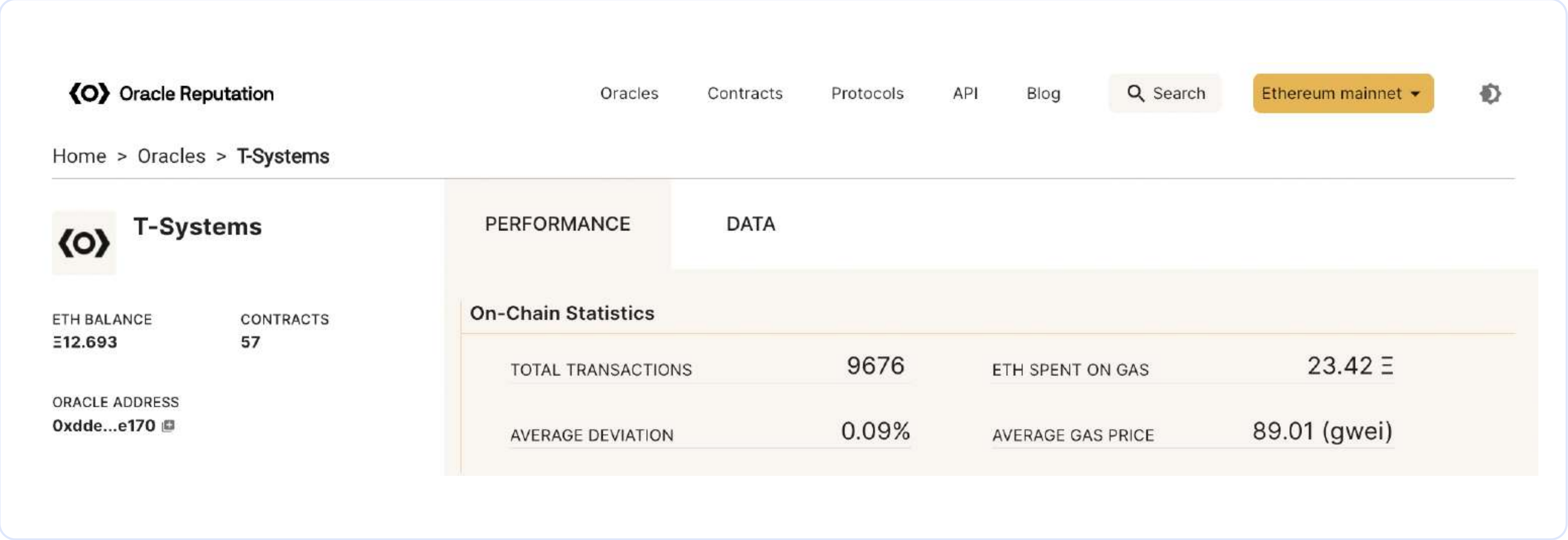
Transparency into the current and historical performance of an oracle network, as well as its software, is essential to making an informed decision.

Only after looking at network design, as well as data on uptime, reliability, and performance, can developers make a truly informed decision. In order to accomplish that, developers need on-chain and/or off-chain insights into the performance of each node and the decentralized oracle network as a whole.

Though compelling, a security-through-obscurity approach exposes users to hidden risks and reduces the ability for an open-source community to fix problems early.

Problem: Unknown vulnerabilities

Without transparency around oracle node performance, security, and operation, users are left exposed to unknown vulnerabilities with no mechanism for holding nodes accountable for their performance.



T-Systems

ETH BALANCE
Ξ12.693

CONTRACTS
57

ORACLE ADDRESS
0xdde...e170

On-Chain Statistics

TOTAL TRANSACTIONS	9676	ETH SPENT ON GAS	23.42 Ξ
AVERAGE DEVIATION	0.09%	AVERAGE GAS PRICE	89.01 (gwei)

Anyone can verify Chainlink oracle node and network statistics through independent services such as reputation.link.

Takeaway: Choose a transparent oracle solutions with robust monitoring systems

Open-source blockchain oracle solutions give developers insight into the entire oracle design —a critical feature that supports better network security while also allowing developers to do their due diligence.

Furthermore, robust monitoring systems can help developers better understand the performance of individual nodes and the larger oracle network. For example, Chainlink oracle nodes can cryptographically sign their data responses and post them on-chain as an immutable record of their performance.

This gives insight into the real-time and historical performance of both oracle nodes (listing service) and oracle networks (reputation system) to help you understand exactly what you're getting when using an oracle service to source off-chain data.

Conclusion

When it comes to smart contract and blockchain oracle security, it pays to spend time and effort finding the right solution.

A secure blockchain oracle decentralizes individual dependencies at all levels, from data sources to oracle nodes, with the goal of ever-reliable data delivery. Transparency into oracle mechanisms, design, and node/network performance gives developers a way to verify an oracle's security firsthand—a core tenet of blockchain technology and smart contracts.

Key takeaways:

- Choose oracle nodes and networks that leverage high-quality data sources and give assurances of high uptime, speed, and accuracy.
- Redundantly sourced data is more secure than using a single data source or a low number of data sources—and especially important for certain data types.
- Look for any single point of failure when considering oracle solutions, whether at the data source, oracle node, or oracle network level.
- Opt for oracle networks where all nodes have a proven history. No outliers—one weak pillar can compromise the safety of the entire building.
- Prioritize visibility into blockchain oracle solutions and oracle nodes' performances so you can monitor the oracle's security every step of the way.

About Chainlink

Chainlink is the industry standard for building, accessing, and selling oracle services needed to power hybrid smart contracts on any blockchain. Chainlink oracle networks provide smart contracts with a way to reliably connect to any external API and leverage secure off-chain computations for enabling feature-rich applications. Chainlink currently secures tens of billions of dollars across DeFi, insurance, gaming, and other major industries, and offers global enterprises and leading data providers a universal gateway to all blockchains.

Learn more about Chainlink by visiting chain.link or reading the developer documentation at docs.chain.link.

To discuss an integration, reach out to an expert.

Chainlink