Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

22-23 MAGGIO 2025

POLITECNICO DI TORINO

Auditorium Energy Center
Via P. Borsellino, 38 int.16
10138 Torino

Oracles for the Blockchain

Speaker: Giulio Caldarelli
Affiliation: University of Turin

About Me

- Assistant Professor in Accounting, Department of Management Walter Cantino (University of Turin)
- Lecturer in Financial Accounting, SAA School of Management
- Lecturer in Blockchain and DeFi Fundamentals, Czech-US Summer School (Prague)"
- My research activities focus on oracle design and integration in real-world blockchains.

Research products

Giulio Caldarelli

FOLLOW

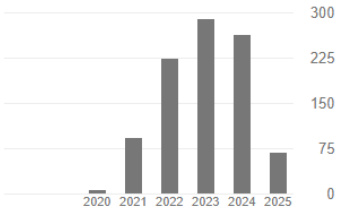
University of Turin
Verified email at unito.it - Homepage

Blockchain Oracles Real World Assets (RWAs) Decentralized Finance

TITLE	CITED BY	YEAR
Understanding the blockchain oracle problem: A call for action G Caldarelli Information 11 (11), 509	234	2020
The blockchain oracle problem in decentralized finance—a multivocal approach G Caldarelli, J Ellul Applied Sciences 11 (16), 7572	180	2021
Blockchain adoption in the fashion sustainable supply chain: Pragmatically addressing barriers G Caldarelli, A Zardini, C Rossignoli Journal of Organizational Change Management 34 (2), 507-524	153	2021
Trusted academic transcripts on the blockchain: A systematic literature review G Caldarelli, J Ellul Applied Sciences 11 (4), 1842	100	2021
Overcoming the blockchain oracle problem in the traceability of non-fungible products G Caldarelli, C Rossignoli, A Zardini Sustainability 12 (6), 2391	89	2020
Wrapping trust for interoperability. A study of wrapped tokens	61 *	2021

Cited by

	All	Since 2020
Citations	960	958
h-index	10	10
i10-index	10	10



Co-authors EDIT

cecilia rossignoli
University of Verona

Joshua Ellul
Associate Professor in the Depar...

Alessandro Zardini
University of Pavia - Department ...

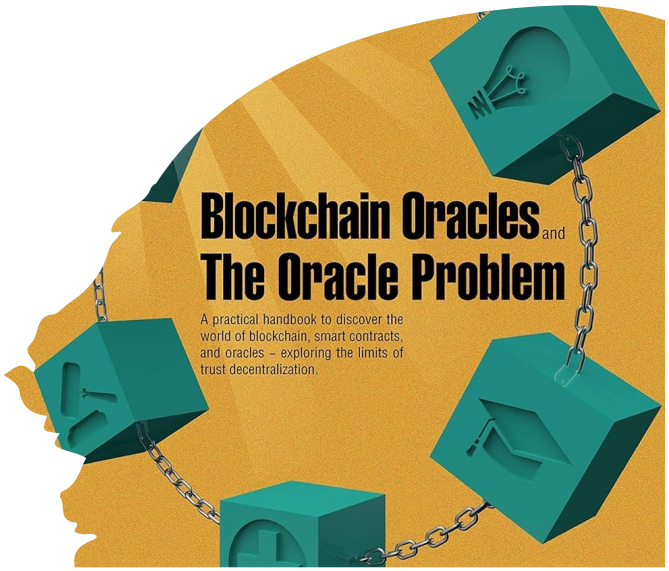
RESEARCH ARTICLE

Before Ethereum. The Origin and Evolutio of Blockchain Oracles

GIULIO CALDARELLI
Department of Management, University of Turin, 10124 Turin, Italy
e-mail: giulio.caldarelli@unito.it

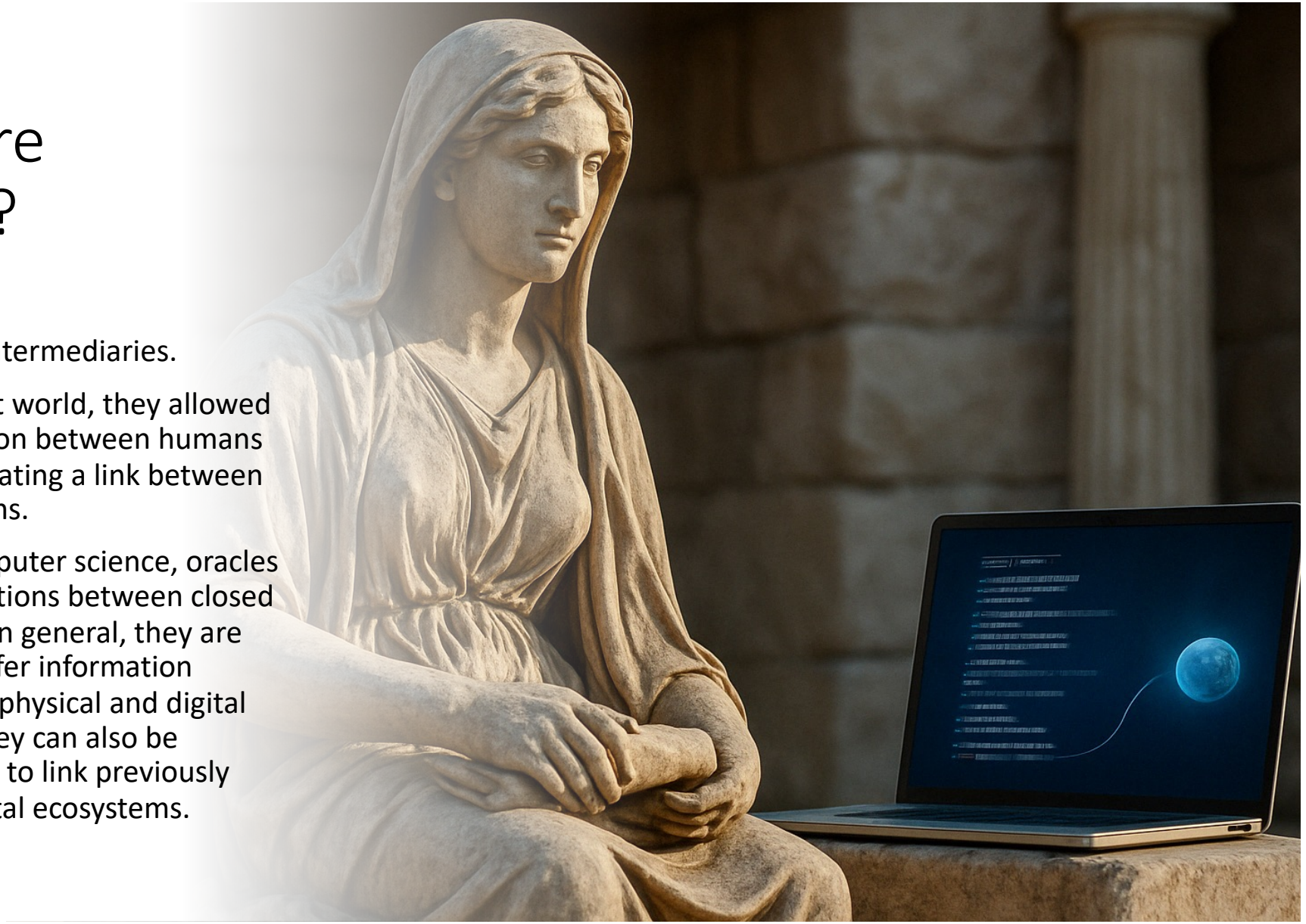
ABSTRACT Before the advent of alternative blockchains such as Ethereum, the future as all in the hands of Bitcoin. Together with Nakamoto itself, early developers were coin's potential to decentralize traditionally centralized applications. However, bec tralized machine, the available non-trustless oracles were considered unsuitable. T elaborated to solve the so-called "oracle problem" in the newborn scenario. By and crawling early forums and repositories, this paper aims to retrace and re contributions that gave birth to oracles on Bitcoin. The evolution of early pr countered in their development, are also outlined. Analyzing technical Bitcoin, the transition to Ethereum will also be discussed.

tracts, oracles, extrinsic dat



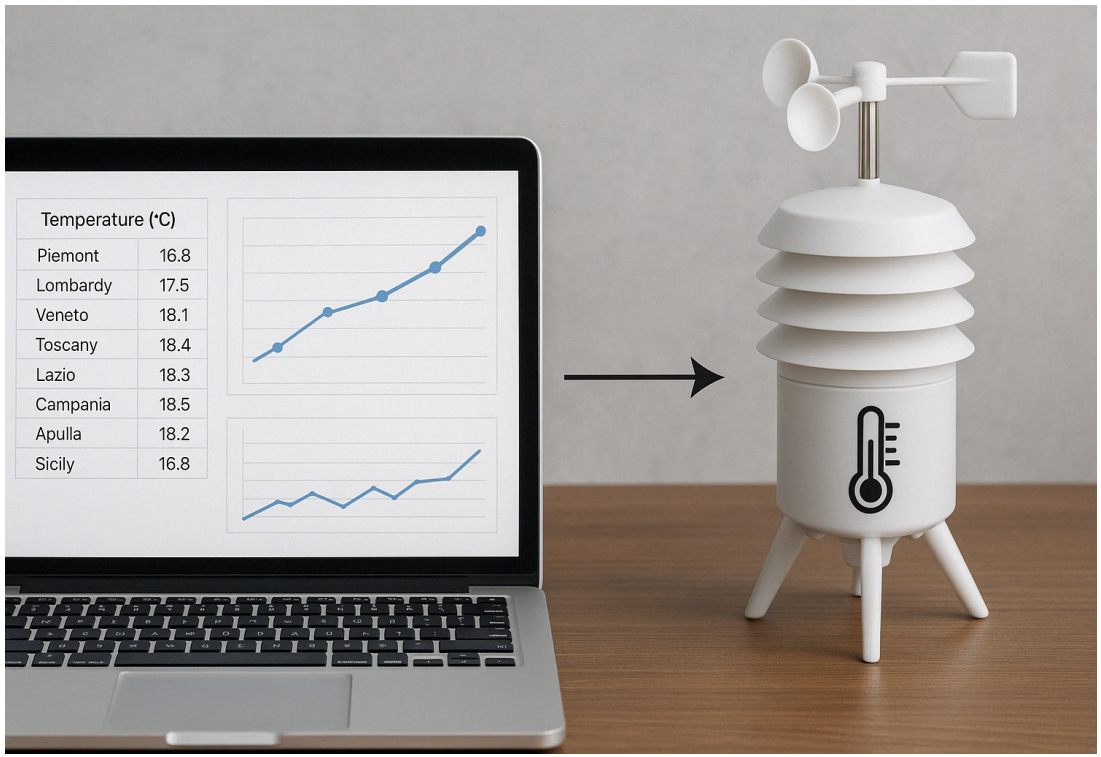
What are oracles?

- Oracles are intermediaries.
- In the ancient world, they allowed communication between humans and gods, creating a link between the two realms.
- Today in computer science, oracles allow connections between closed ecosystems. In general, they are used to transfer information between the physical and digital world, but they can also be implemented to link previously separate digital ecosystems.



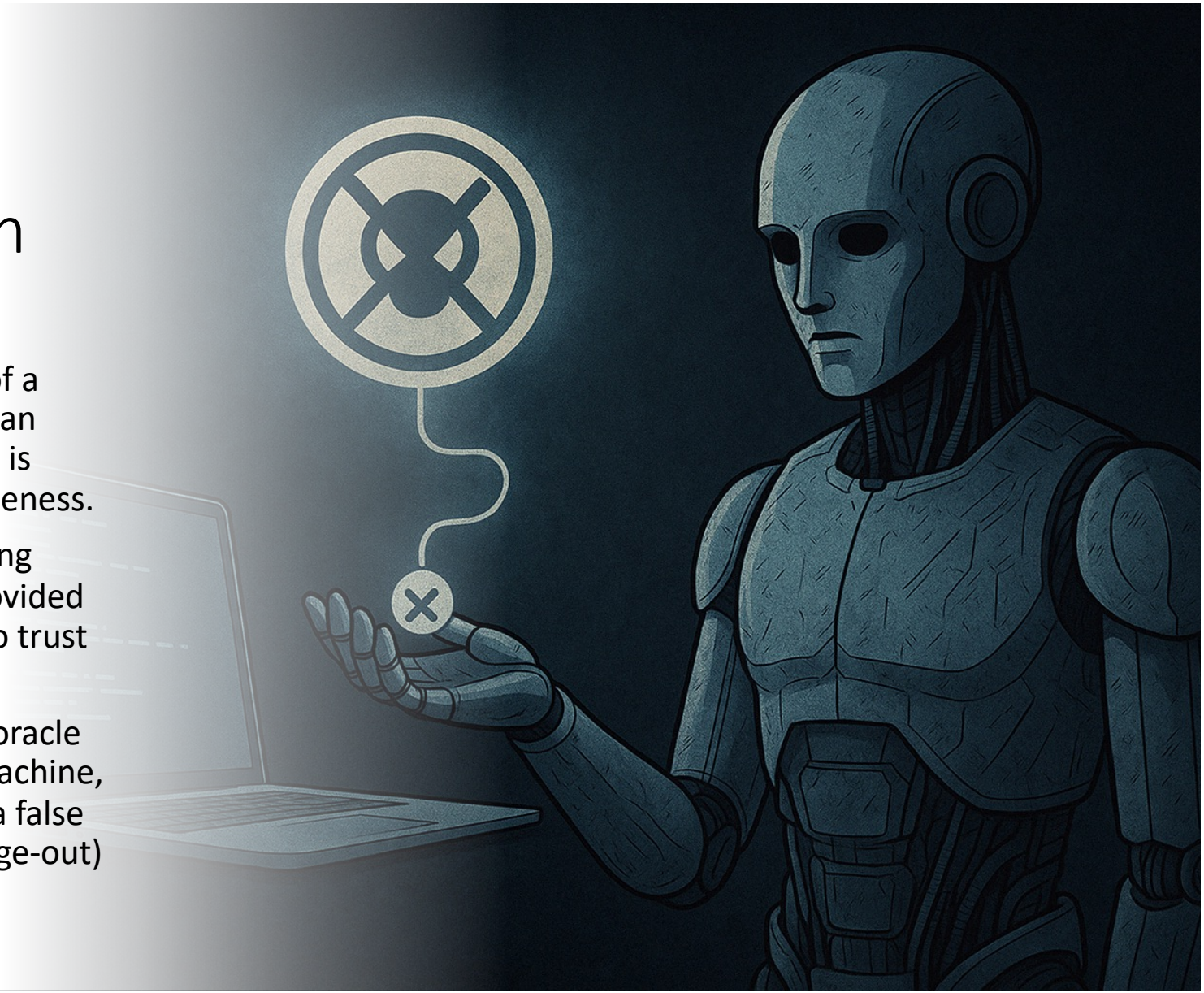
When machines needs oracles

- If we ask a machine to calculate the average temperature across Italian regions, it can certainly average numbers, but it lacks the actual temperature data.
- Sensors or APIs (oracles) provide the necessary external data.



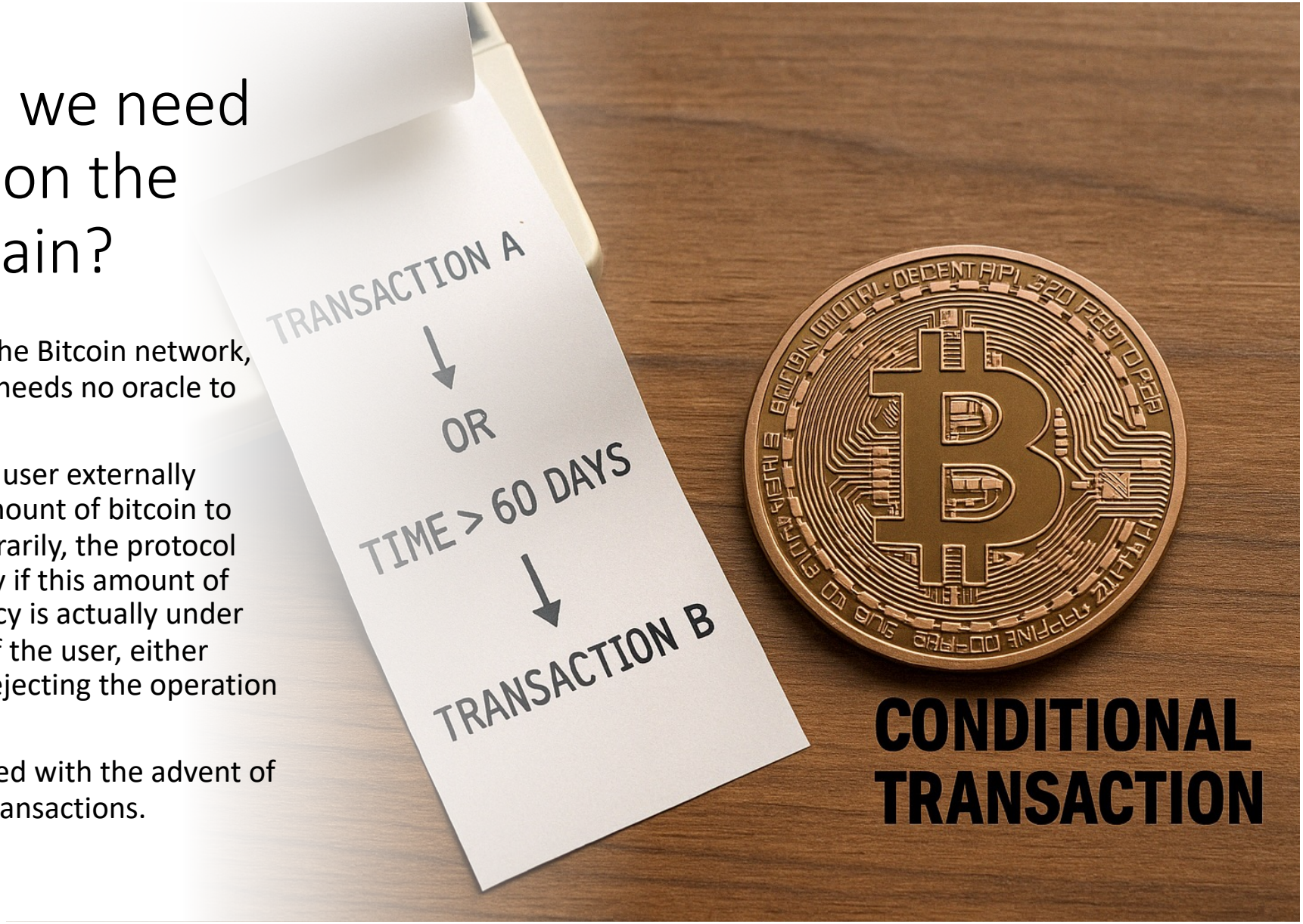
The so-called oracle problem

- The fundamental aspect of a piece of data provided by an oracle is that the machine is unable to verify its genuineness.
- The machine knows nothing about the information provided by the oracle and needs to trust it.
- As you can imagine, if an oracle provides false data to a machine, the machine will provide a false output (garbage-in, garbage-out)



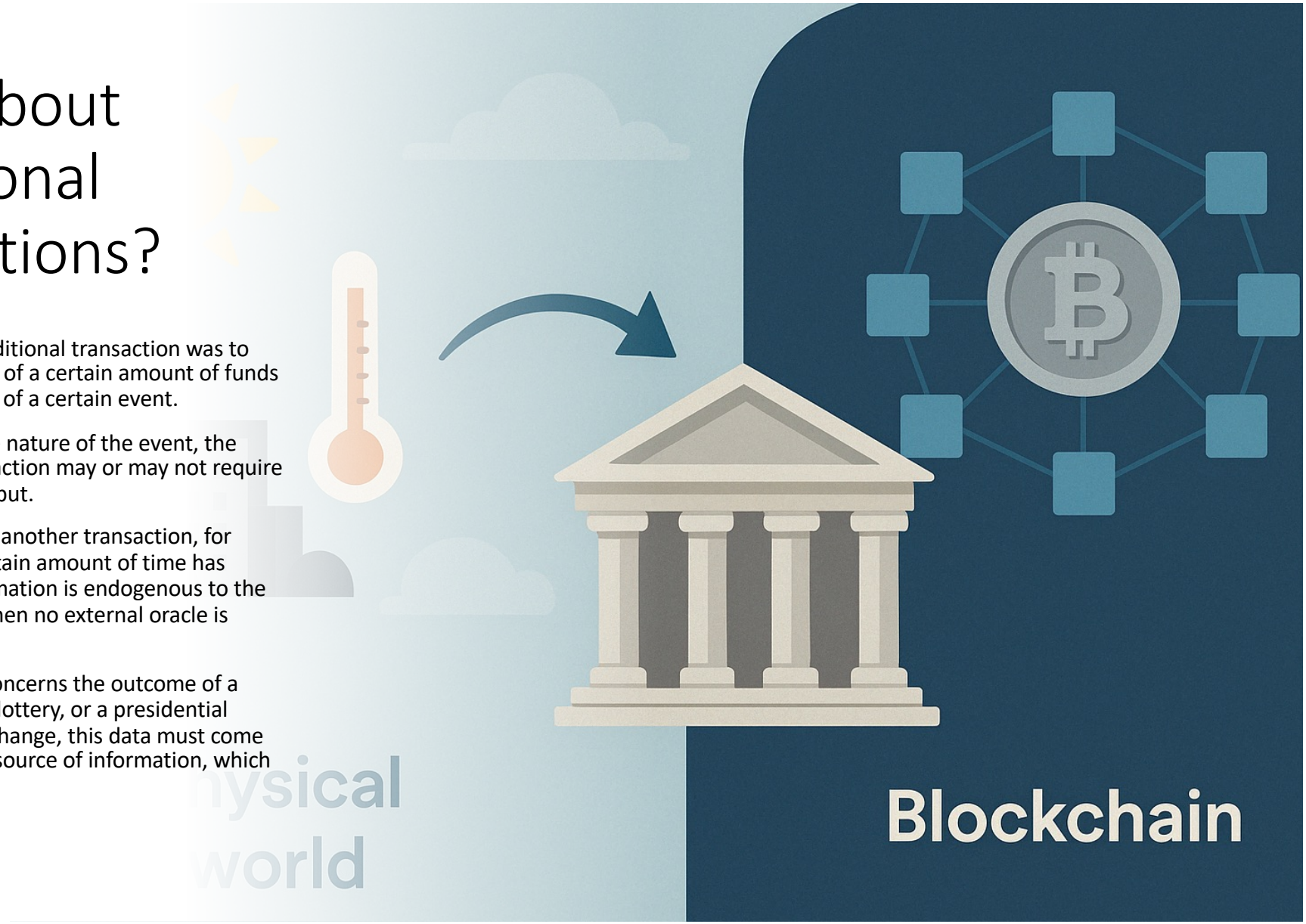
Why do we need oracles on the blockchain?

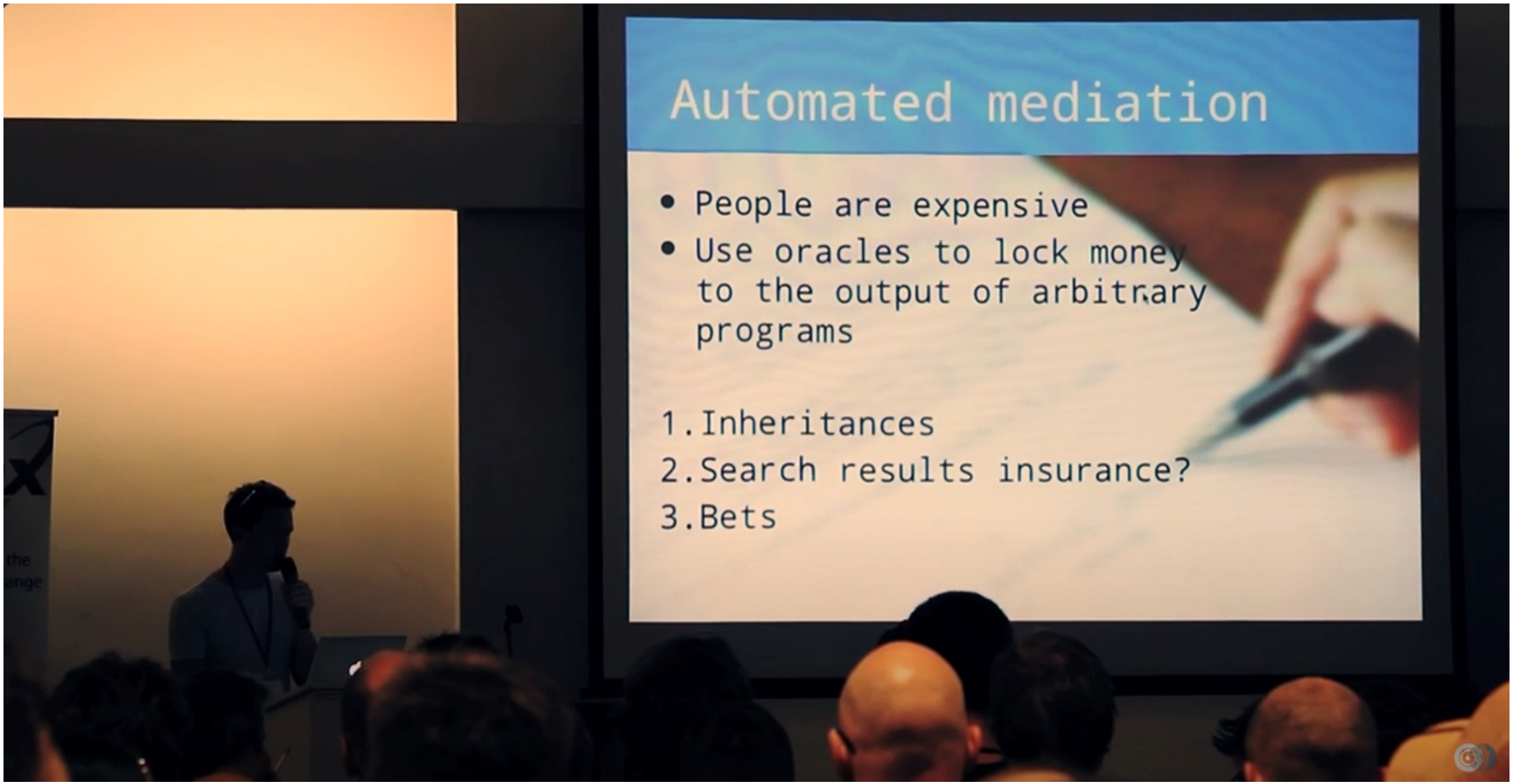
- In principle, the Bitcoin network, for example, needs no oracle to operate.
- Although the user externally inputs the amount of bitcoin to transfer arbitrarily, the protocol knows exactly if this amount of cryptocurrency is actually under the control of the user, either allowing or rejecting the operation trustlessly.
- Things changed with the advent of conditional transactions.



What about conditional transactions?

- The idea of a conditional transaction was to allow the transfer of a certain amount of funds as a consequence of a certain event.
- Depending on the nature of the event, the conditional transaction may or may not require external oracle input.
- If the condition is another transaction, for example, or a certain amount of time has passed, the information is endogenous to the blockchain, and then no external oracle is required.
- If the condition concerns the outcome of a football match, a lottery, or a presidential election, a price change, this data must come from an external source of information, which is our “oracle”.




Automated mediation
• People are expensive
• Use oracles to lock money to the output of arbitrary programs
1. Inheritances
2. Search results insurance?
3. Bets

Re: Holding coins in an unspendable state for a rolling time window

From: Satoshi Nakamoto <satoshin@gmx.com>
Date: Wed, Apr 20, 2011 at 11:39 AM
To: Mike Hearn <mike@plan99.net>
Subject: Re: Holding coins in an unspendable state for a rolling time window

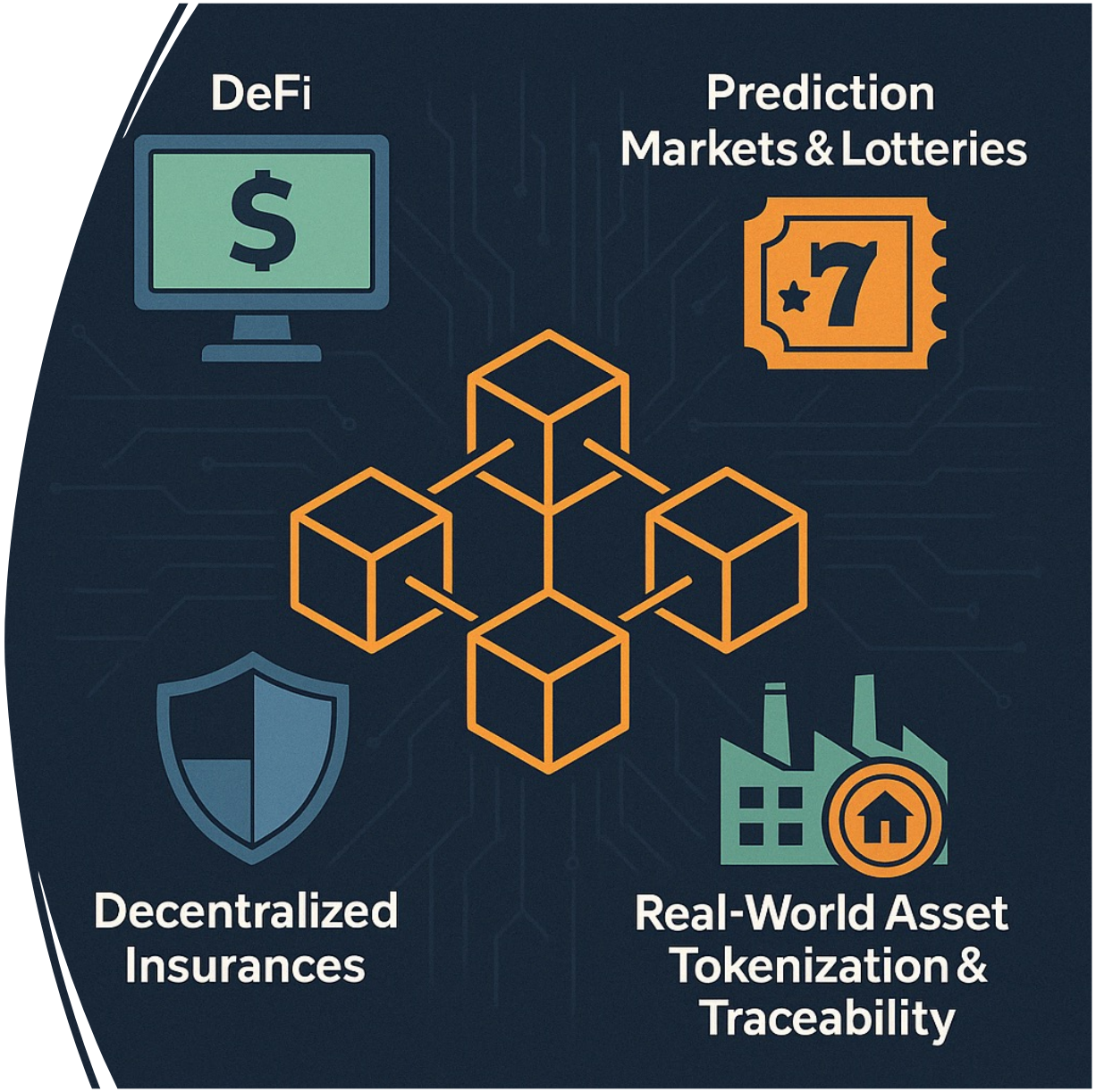
If the script language is not stateless, if it has access to any outside information that changes or varies between nodes, attackers can use it to fork the chain. The only exception is if it is always false before a certain time and permanently true after, which is implemented with nLockTime.

What Applications Rely on Blockchain Oracles?

Web3 applications such as:

- DeFi
- Prediction Markets and Gaming
- Decentralized Insurances
- Real-world Assets tokenization and Traceability

These applications are as trustless and reliable as the oracle that is implemented to fetch the data.



What Types of oracles we have?

- We mostly have two types of oracles

1) Oracles ensuring the transmitted information matches exactly the source data.

2) Oracles using voting-based systems to ensure provided data aligns with user expectations.

Therefore, no oracle is really capable of telling the “Truth”, nor can it represent a trustless data reporting.

What can go wrong?

- Programming an oracle is highly complex, and ensuring it is bug-free is extremely challenging.
- In DeFi, oracles often manage vast amounts of capital, sometimes hundreds of millions of dollars. As a result, they represent an attractive honeypot for hackers.
- By manipulating asset prices, malicious actors can exploit protocols and drain them entirely.
- To date, over $9.28 billion has been stolen due to oracle-related exploits, including direct manipulation and bridge hacks.

What Are Price Oracle Manipulatio
Attacks in DeFi?

Jaypalsinh Jadeja
Content Strategist for Web3 & AI Brands | Following Curiosity | Content Creator & Crypto Research | DEX | DeFi

October 7, 2024

Products Industries

CRIME

Oracle Manipulation Attack
Rising, Creating a Unique Co
for DeFi

MARCH 7, 2023 | BY CHAINALYSIS TEAM

HACKEN Audits Services Solutions Community Blog Company

cken → Blog → Insights → The BonqDAO Price Oracle Hack Explained (February 2023)

The BonqDAO Price Oracle Ha
Explained (February 2023)

Feb 3, 2023 / Upd: Dec 2, 2024 4 minutes By Malanii Oleh

On February 2nd, 2023, the Polygon DeFi protocol BonqDAO fell victim to a price oracle hack due to a
error in a smart contract code. The attacker stole 100 million $BEUR stablecoins and 120 million
Wrapped AllianceBlock Token ($WALBT).

Conclusions

- Oracles are necessary to develop Web3 applications based on real-world assets/events.
- Its use somehow contradicts the disintermediation role of blockchain and constitutes an additional layer of centralization.
- Many oracles have been proposed, but to date, none has proven to be infallible.
- With complex game-theoretical designs, however, carefully balancing risks and rewards, oracles can sufficiently support integrations required by Web3.
- Mistakes in oracle programming can, however, result in highly damaging consequences.