32nd Annual Network and Distributed System Security (NDSS) Symposium

Exploring User Perceptions of Security Auditing in the Web3 Ecosystem

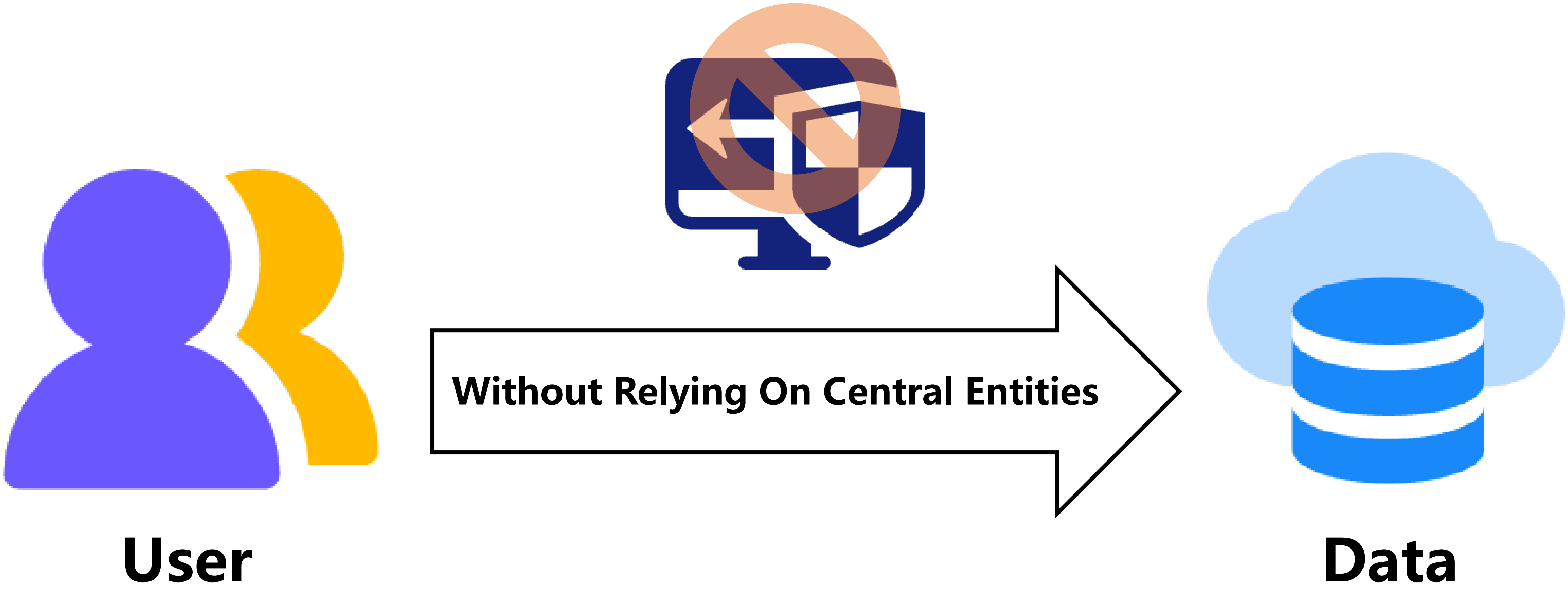
Molly Zhuangtong Huang[1], Rui Jiang[1], Tanusree Sharma[2] , and Kanye Ye Wang[1]

[1] University of Macau [2] Pennsylvania State University

San Diego, CA Tuesday, 25 February 2025

Web3

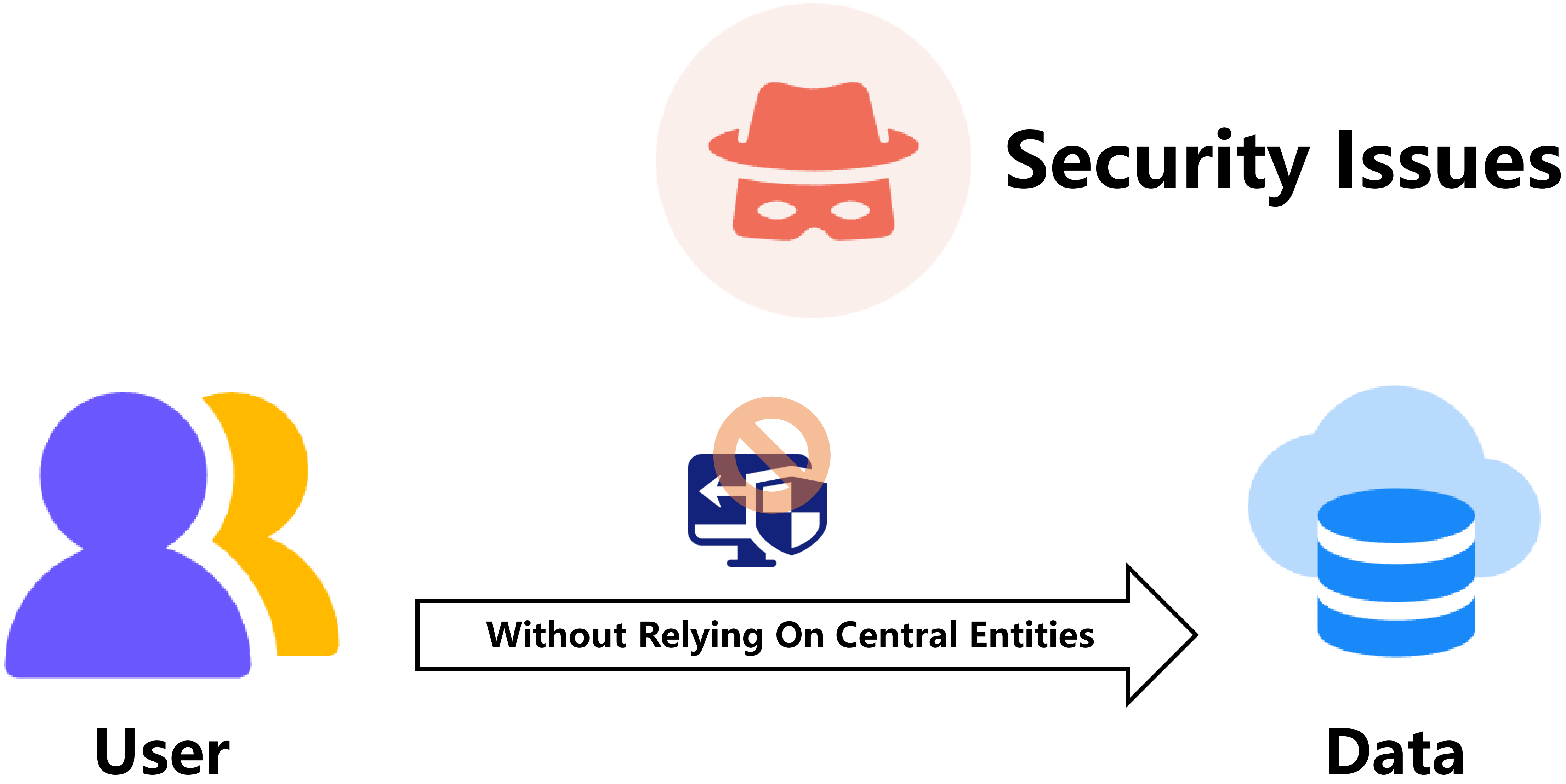
Blockchain



Without Relying On Central Entities

User

Data



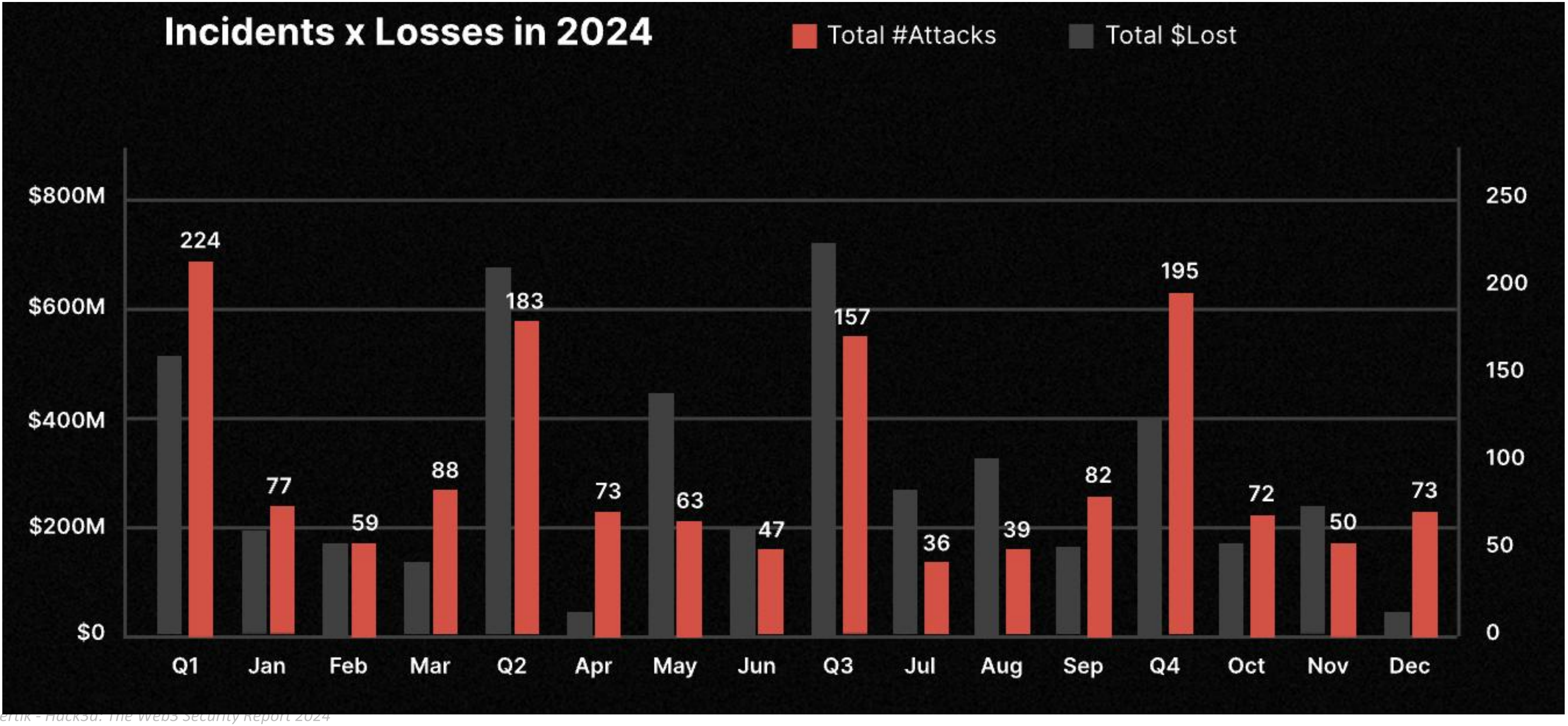
Security Issues

Without Relying On Central Entities

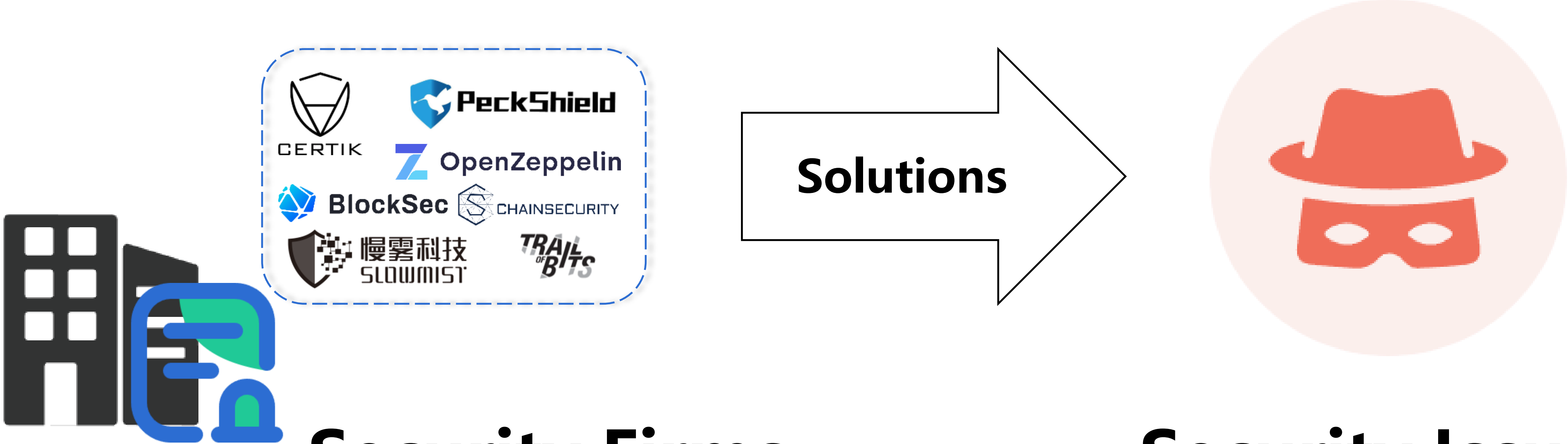
User

Data

Frequent Security Incidents And Significant Financial Losses



Source: Certik - Hack3d: The Web3 Security Report 2024

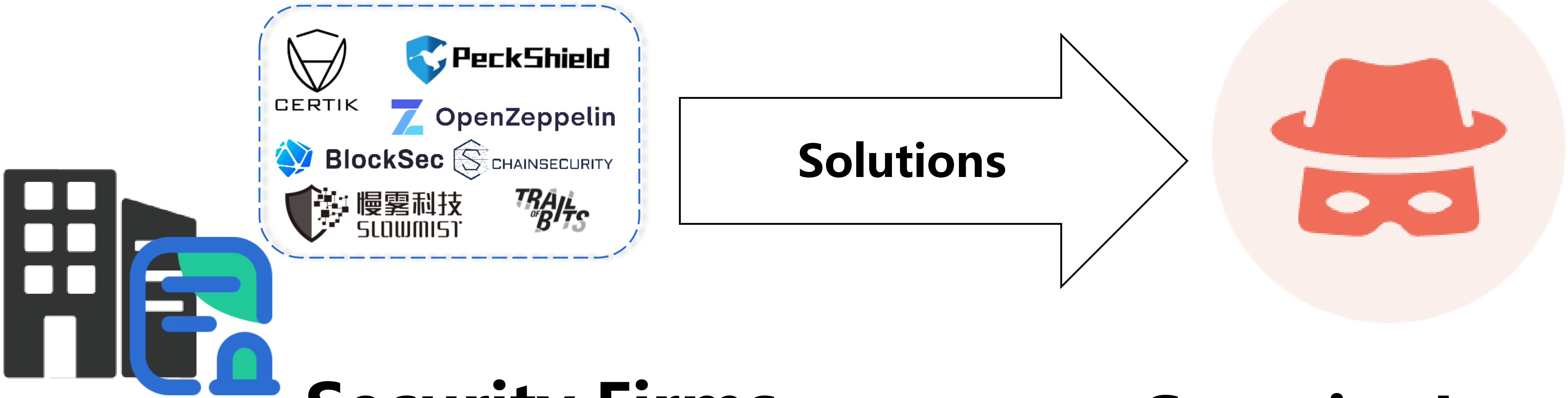


Solutions

Security Firms

Security Issues

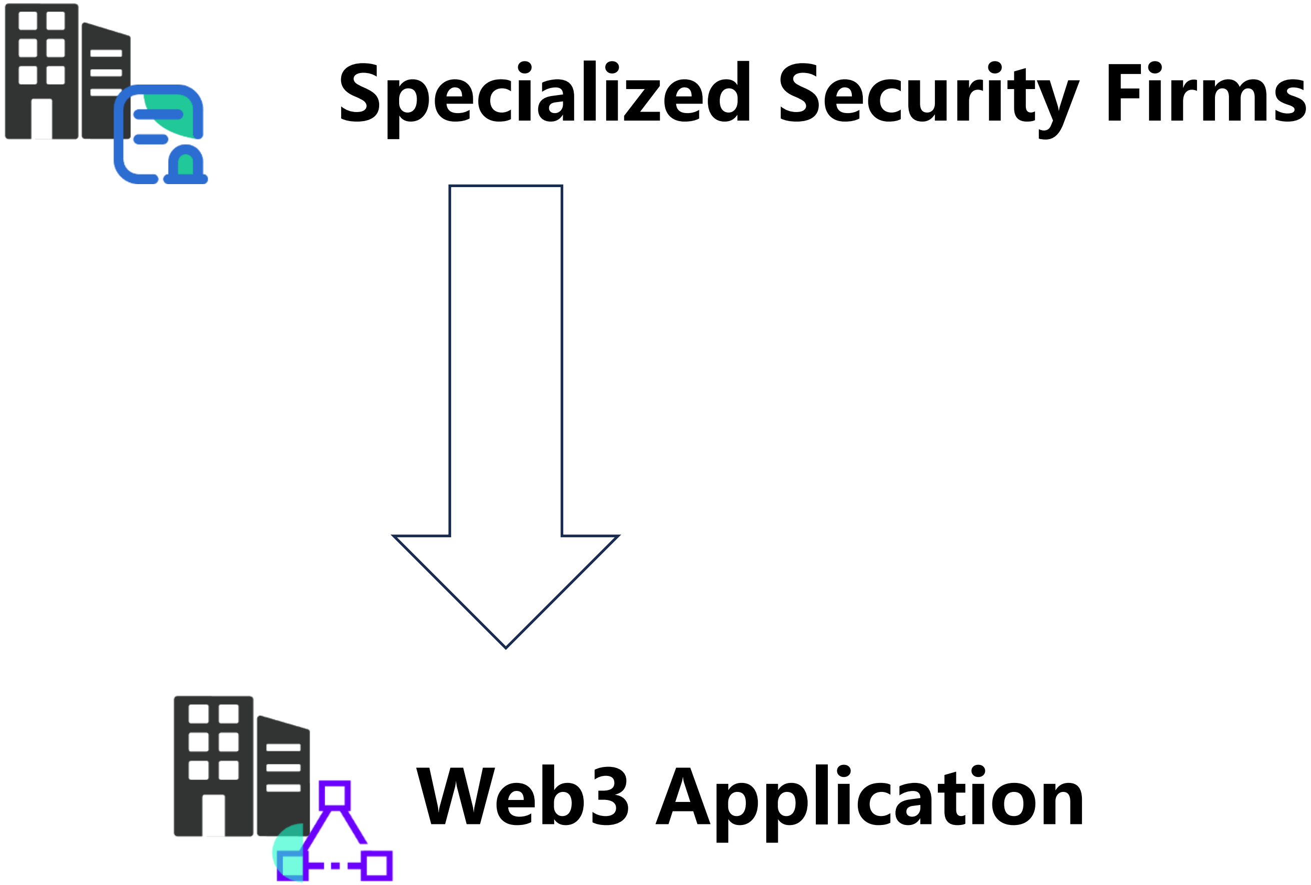
Security Auditing



Solutions

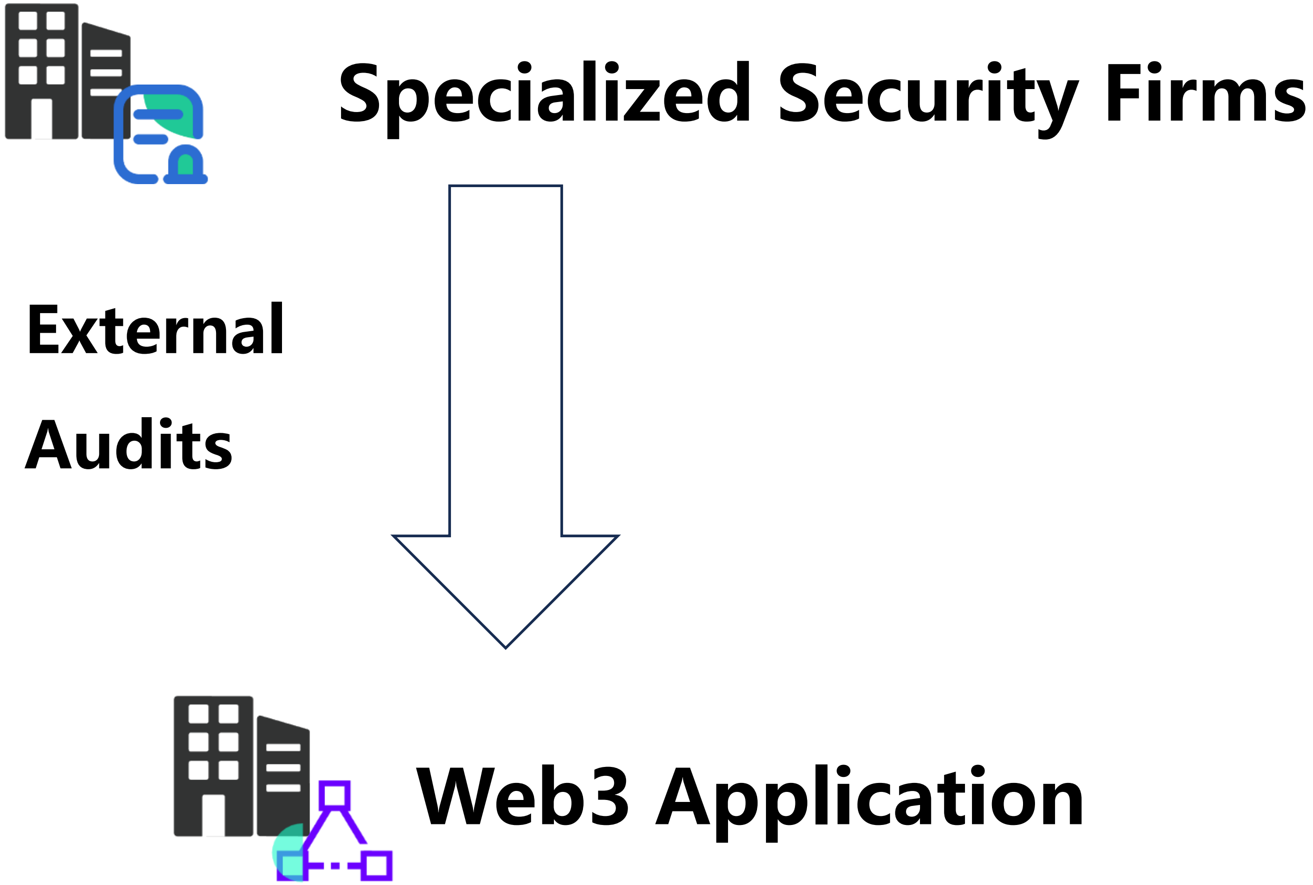
Security Firms

Security Issues



Specialized Security Firms

Web3 Application

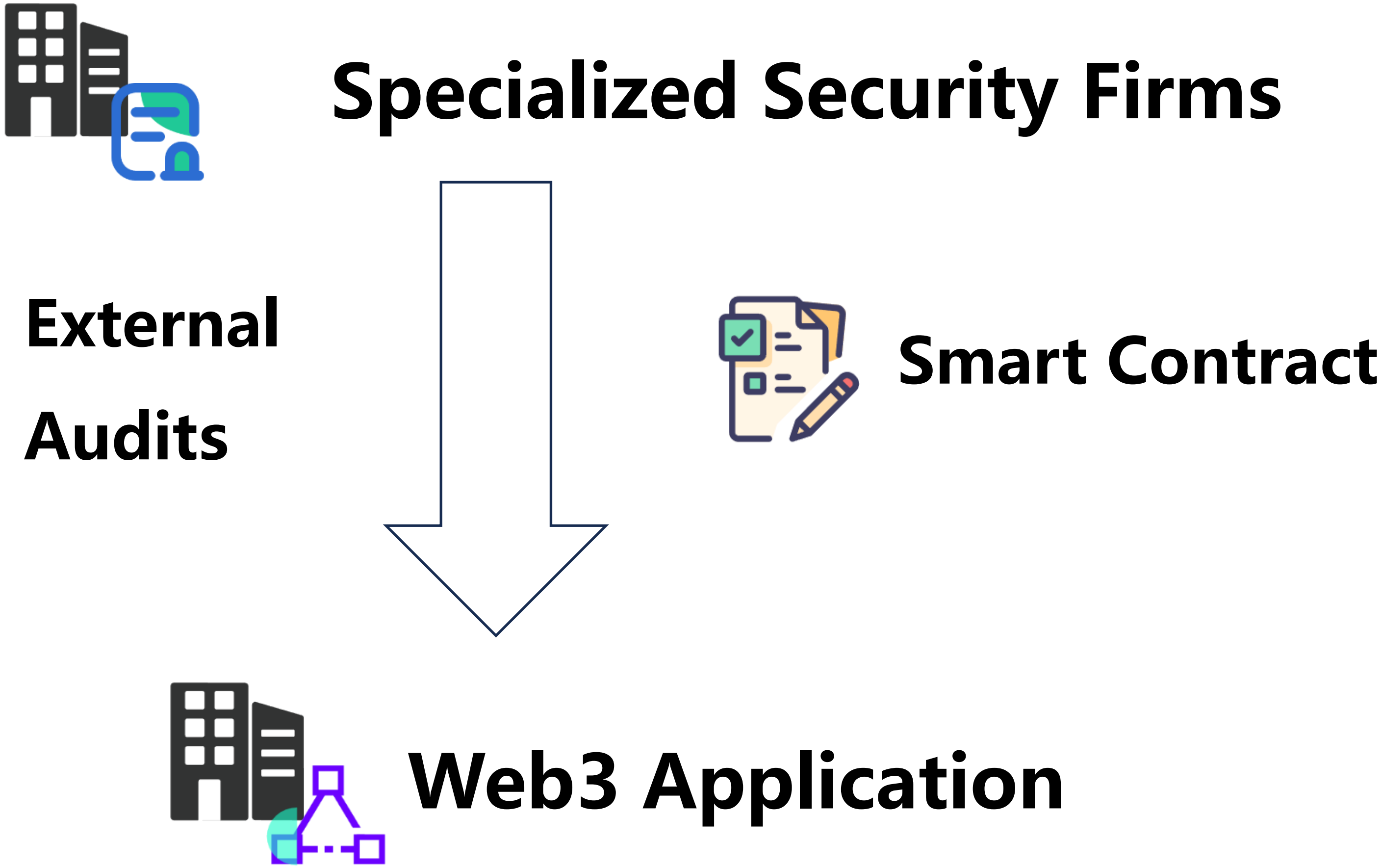


Specialized Security Firms

External

Audits

Web3 Application



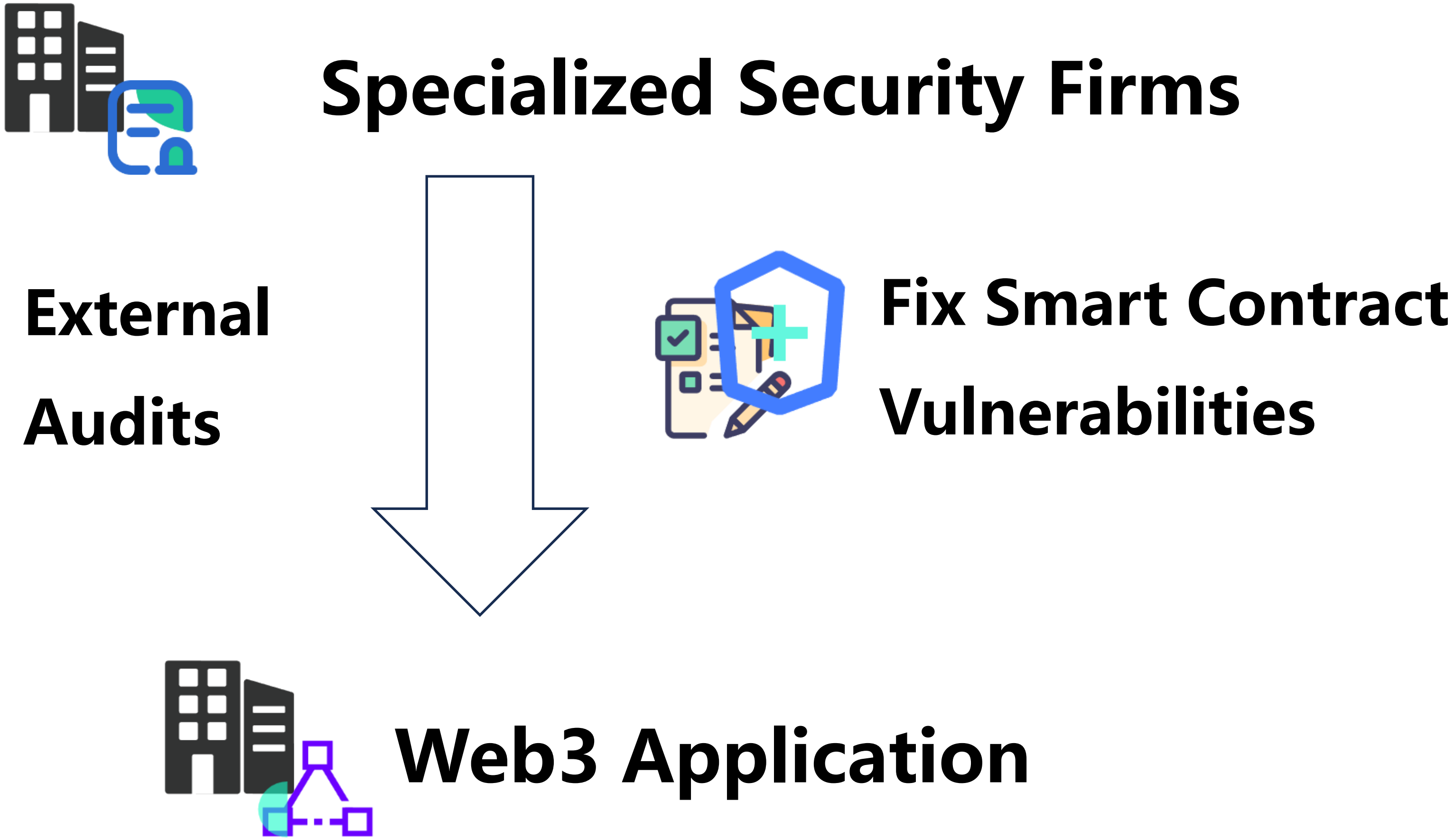
Specialized Security Firms

External

Audits

Smart Contract

Web3 Application

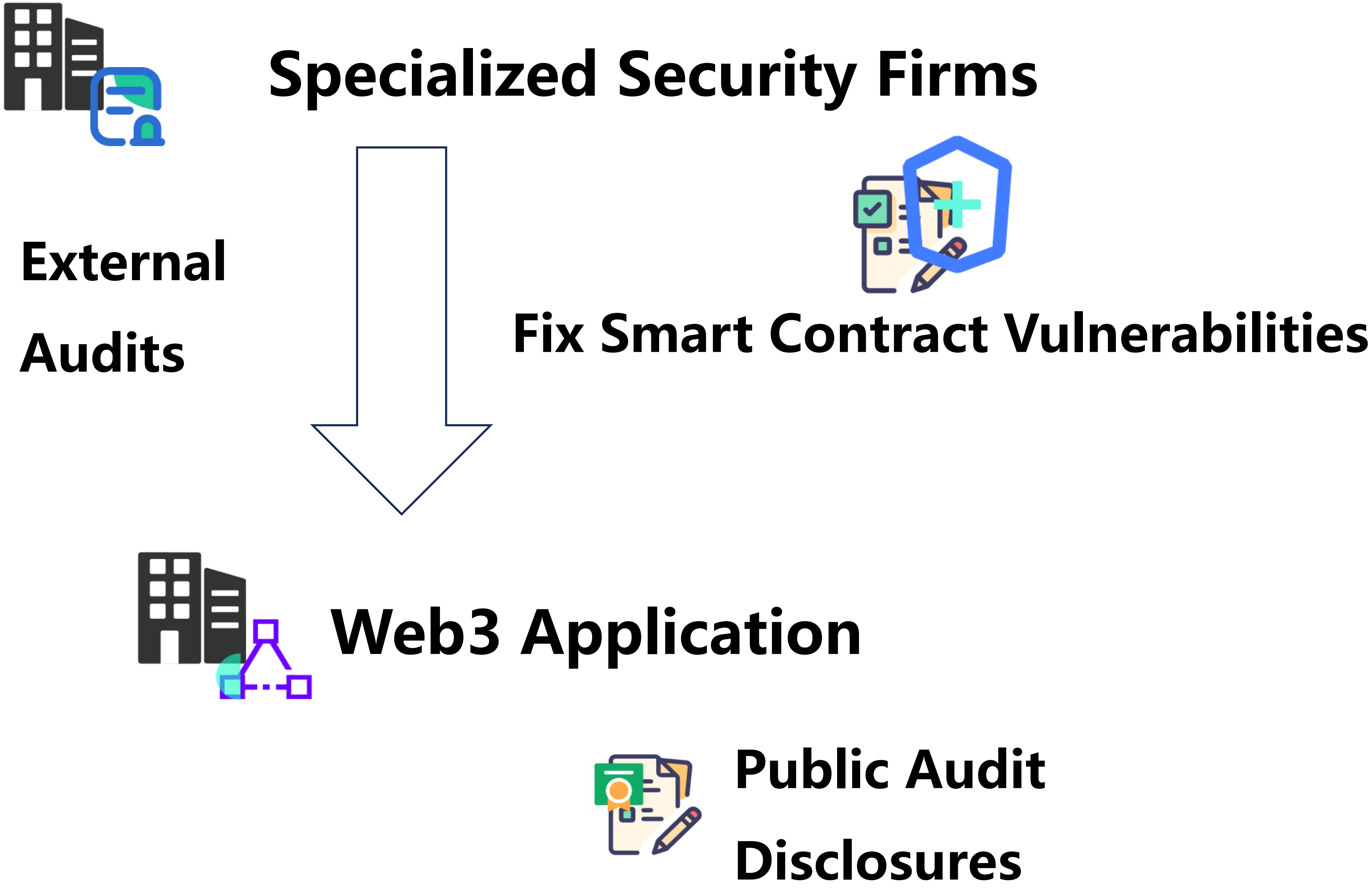


Specialized Security Firms

External Audits

Fix Smart Contract Vulnerabilities

Web3 Application



Specialized Security Firms

External Audits

Fix Smart Contract Vulnerabilities

Web3 Application

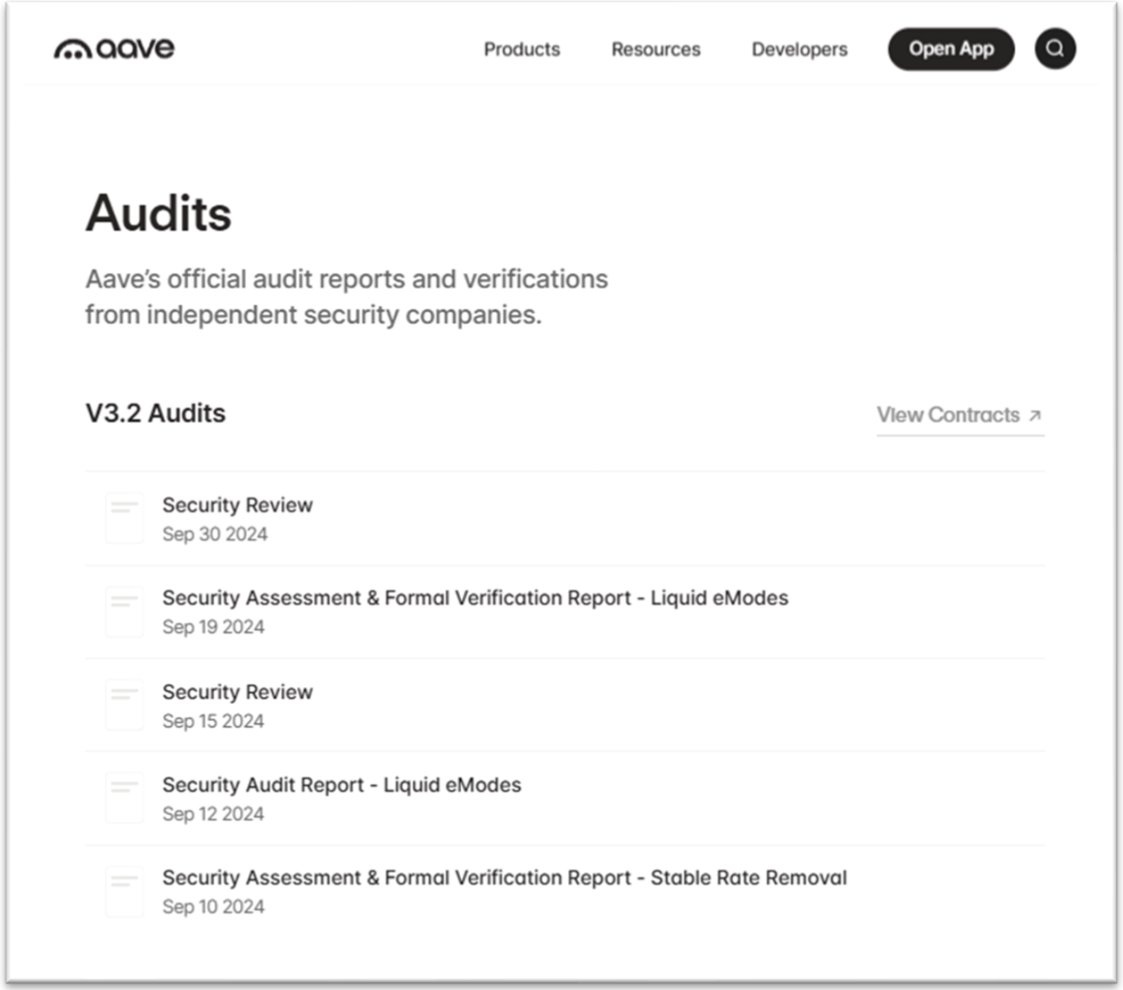
Public Audit Disclosures

CYBER AND CRYPTO LAB

NDSS SYMPOSIUM/2025 Internet Society 澳門大學 UNIVERSIDADE DE MACAU UNIVERSITY OF MACAU

Public Audit Disclosures

Application Website



Audits

Aave's official audit reports and verifications from independent security companies.

V3.2 Audits

View Contracts ↗

Security Review
Sep 30 2024

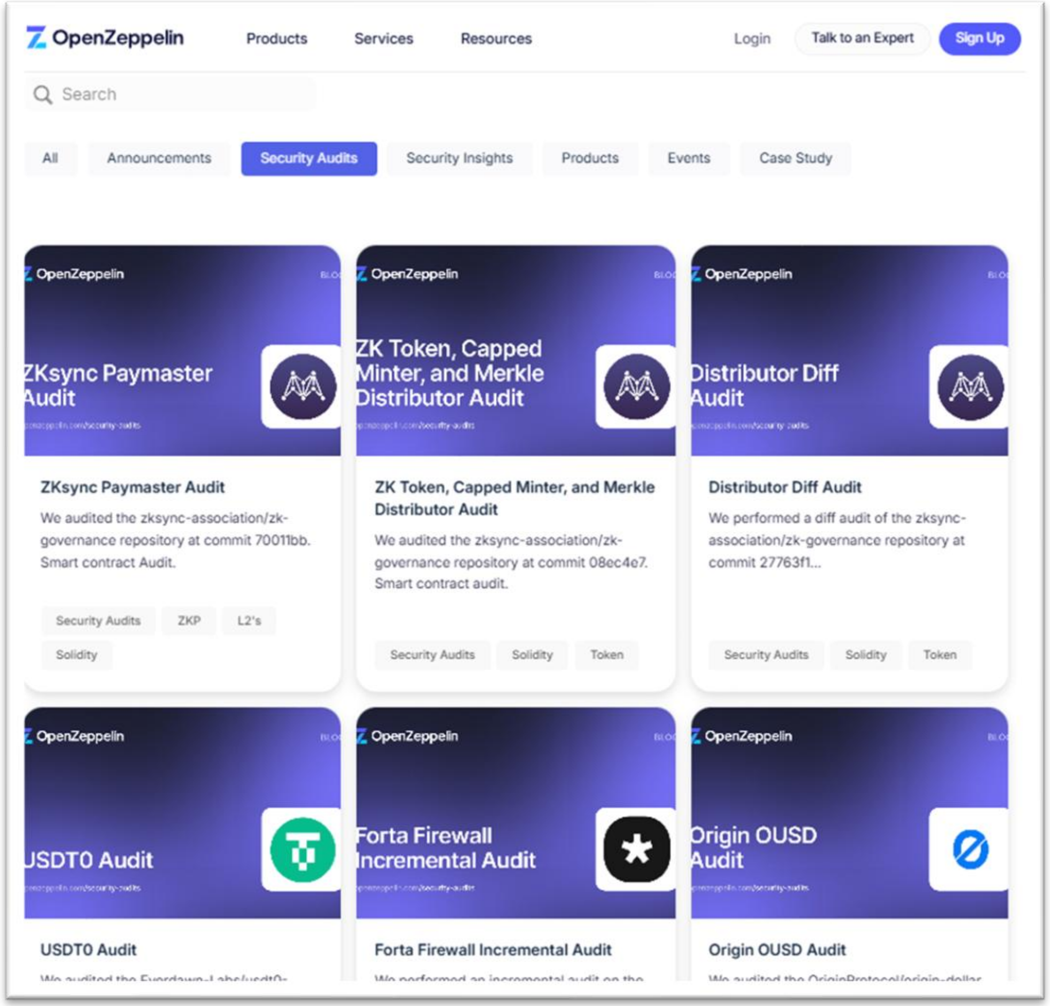
Security Assessment & Formal Verification Report - Liquid eModes
Sep 19 2024

Security Review
Sep 15 2024

Security Audit Report - Liquid eModes
Sep 12 2024

Security Assessment & Formal Verification Report - Stable Rate Removal
Sep 10 2024

Audit Firm Homepage



ZKsync Paymaster Audit

We audited the zksync-association/zk-governance repository at commit 70011bb. Smart contract Audit.

Security Audits · ZKP · L2's · Solidity

ZK Token, Capped Minter, and Merkle Distributor Audit

We audited the zksync-association/zk-governance repository at commit 08ec4e7. Smart contract audit.

Security Audits · Solidity · Token

Distributor Diff Audit

We performed a diff audit of the zksync-association/zk-governance repository at commit 27763f1...

Security Audits · Solidity · Token

USDT0 Audit

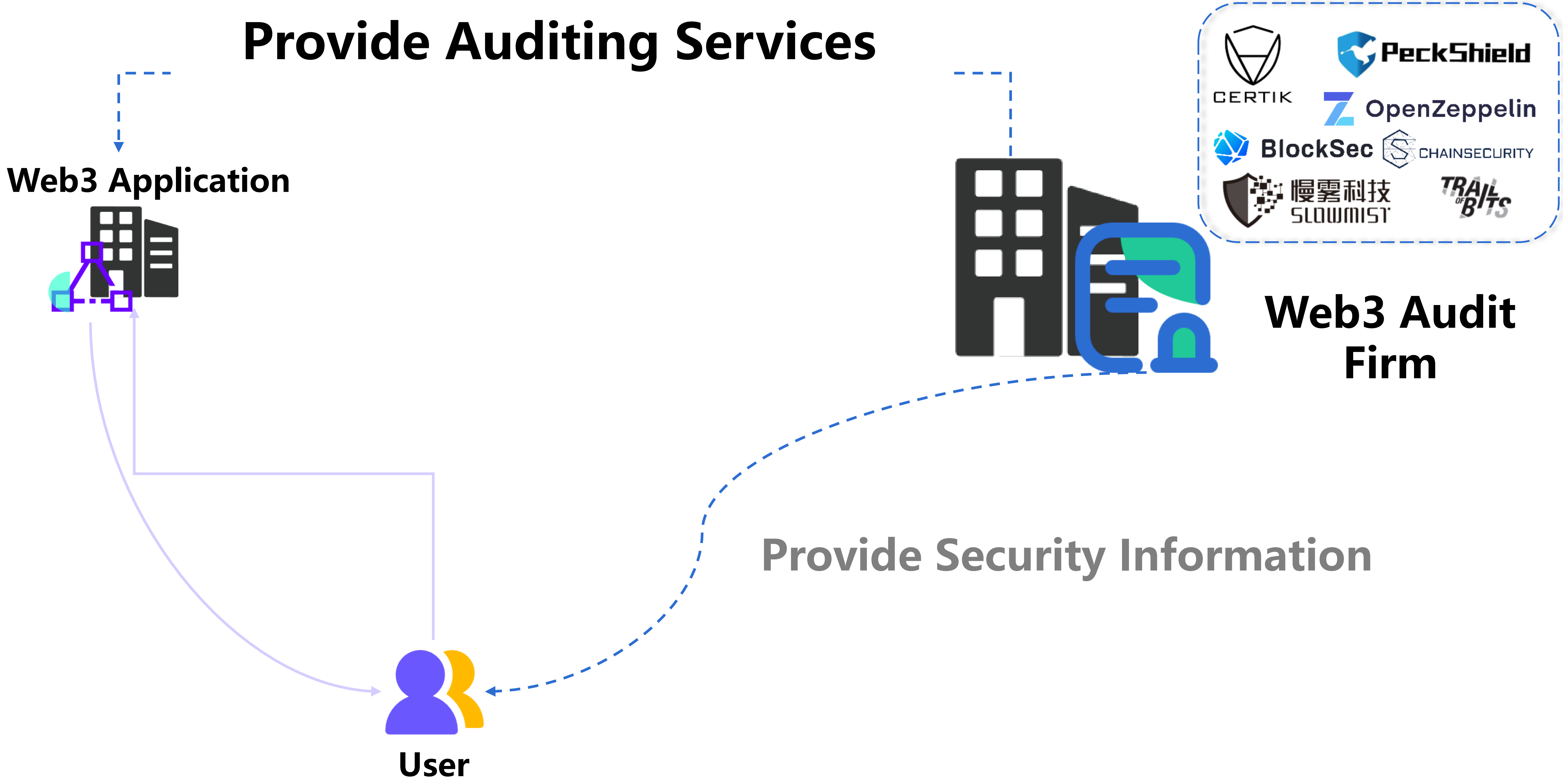
We audited the Everdawn-Labs/usdt0-

Forta Firewall Incremental Audit

We performed an incremental audit on the

Origin OUSD Audit

We audited the OriginProtocol/origin-dollar



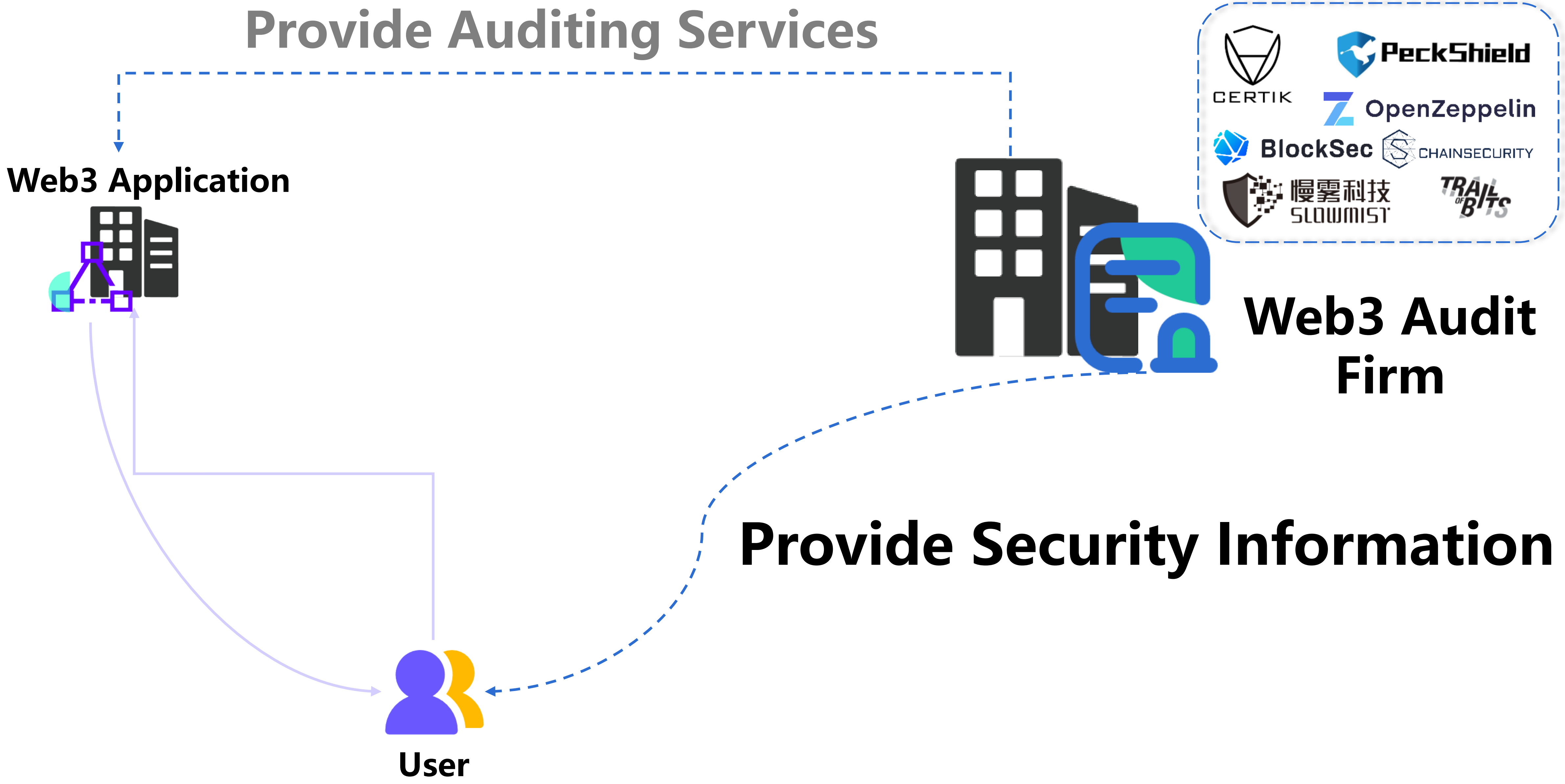
Provide Auditing Services

Web3 Application

Web3 Audit Firm

Provide Security Information

User



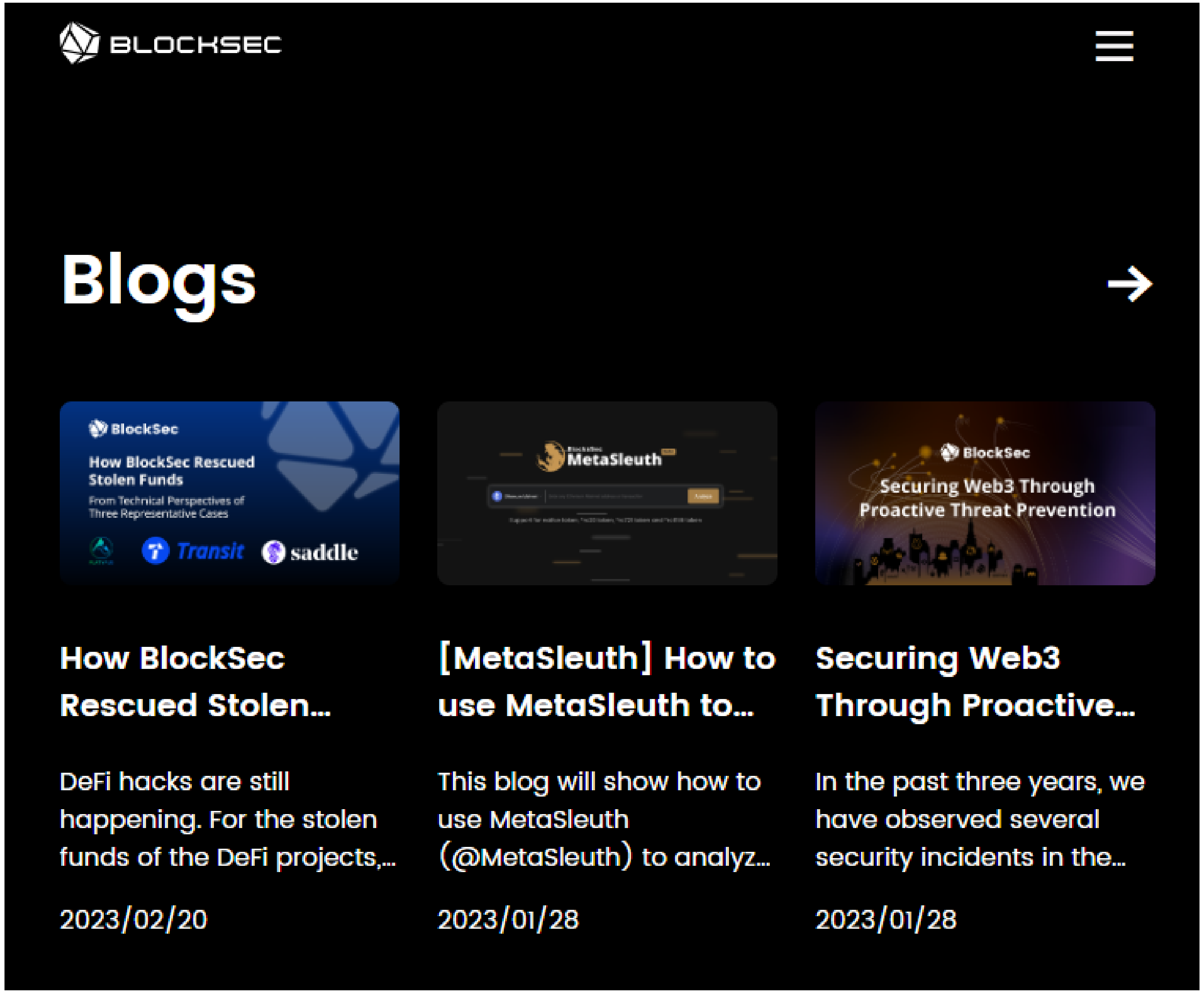
Provide Auditing Services

Web3 Application

Web3 Audit Firm

Provide Security Information

User



Blogs

BlockSec
How BlockSec Rescued Stolen Funds
From Technical Perspectives of Three Representative Cases
Transit
saddle

How BlockSec Rescued Stolen...

DeFi hacks are still happening. For the stolen funds of the DeFi projects,...

2023/02/20

[MetaSleuth] How to use MetaSleuth to...

This blog will show how to use MetaSleuth (@MetaSleuth) to analyz...

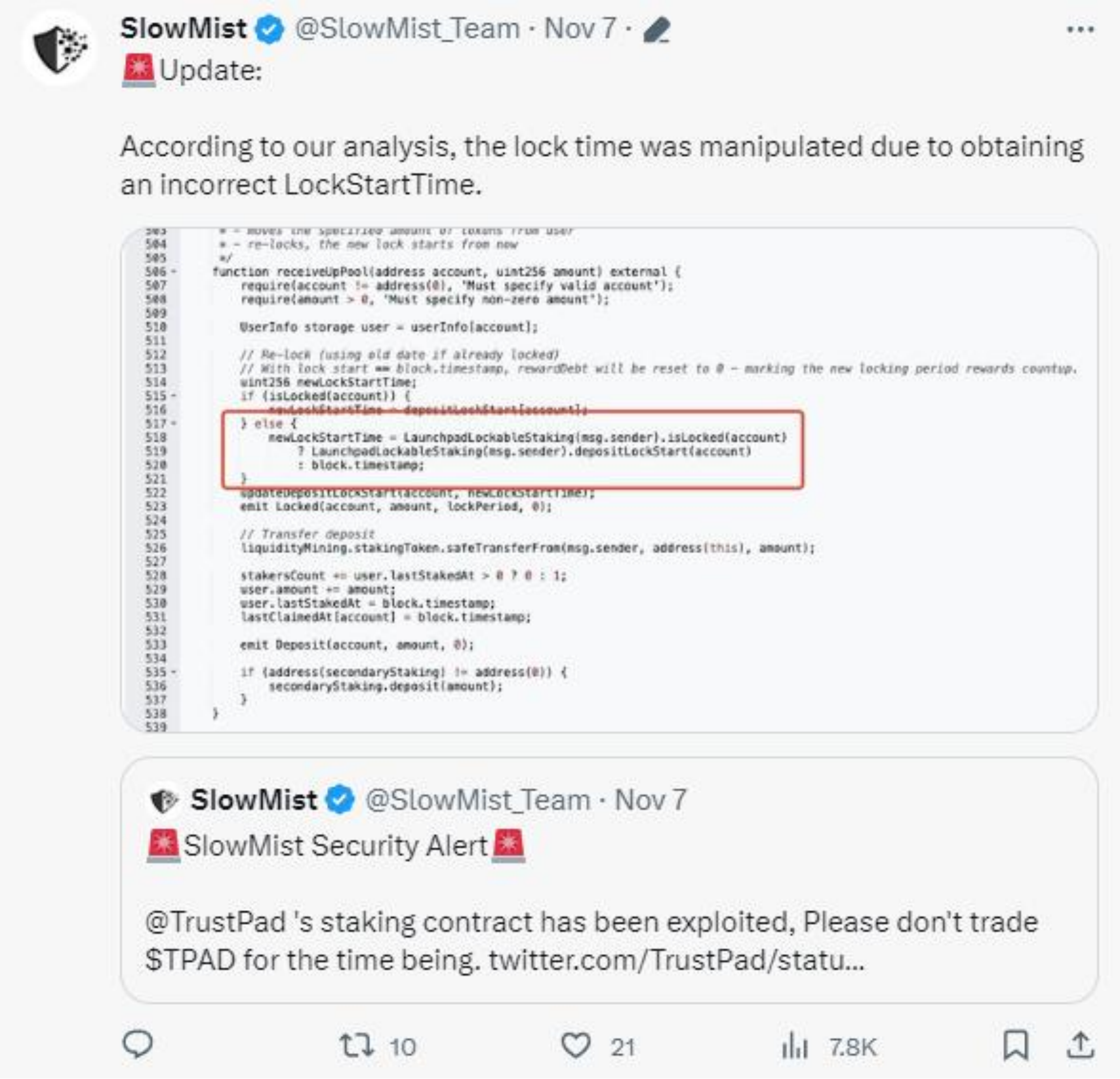
2023/01/28

BlockSec
Securing Web3 Through Proactive Threat Prevention

Securing Web3 Through Proactive...

In the past three years, we have observed several security incidents in the...

2023/01/28



SlowMist @SlowMist_Team · Nov 7 ·

🚨Update:

According to our analysis, the lock time was manipulated due to obtaining an incorrect LockStartTime.

```
     * - moves the specified amount of tokens from user
     * - re-locks, the new lock starts from now
     */
    function receiveUpPool(address account, uint256 amount) external {
        require(account != address(0), 'Must specify valid account');
        require(amount > 0, 'Must specify non-zero amount');

        UserInfo storage user = userInfo[account];

        // Re-lock (using old date if already locked)
        // With lock start == block.timestamp, rewardDebt will be reset to 0 - marking the new locking period rewards countup.
        uint256 newLockStartTime;
        if (isLocked(account)) {
            newLockStartTime = depositLockStart[account];
        } else {
            newLockStartTime = LaunchpadLockableStaking(msg.sender).isLocked(account)
                ? LaunchpadLockableStaking(msg.sender).depositLockStart(account)
                : block.timestamp;
        }
        updateDepositLockStart(account, newLockStartTime);
        emit Locked(account, amount, lockPeriod, 0);

        // Transfer deposit
        liquidityMining.stakingToken.safeTransferFrom(msg.sender, address(this), amount);

        stakersCount += user.lastStakedAt > 0 ? 0 : 1;
        user.amount += amount;
        user.lastStakedAt = block.timestamp;
        lastClaimedAt[account] = block.timestamp;

        emit Deposit(account, amount, 0);

        if (address(secondaryStaking) != address(0)) {
            secondaryStaking.deposit(amount);
        }
    }
```

SlowMist @SlowMist_Team · Nov 7

🚨SlowMist Security Alert🚨

@TrustPad 's staking contract has been exploited, Please don't trade $TPAD for the time being. twitter.com/TrustPad/statu...

Is This Security Auditing Enough To Secure Web3?

Technical Security

Usable Security

Technical Security

Usable Security

Exploring User Perceptions of Security Auditing in the Web3 Ecosystem

User

Perceive

Web3 Auditing Security Information

User

Perceive

Role of Web3 Auditing In Enhancing Security

User

Impact

Interaction With Web3 Application

Case Study

Information disclosure review
on 21 audit firm websites

Interview

Perceptions of 20
Web3 users

Data Analysis

905 related discussions
on Reddit

How Do Users Perceive Security Information Obtained From Web3 Auditing?

Insufficient Information Comprehensiveness

84%

Unclear Team Member

87%

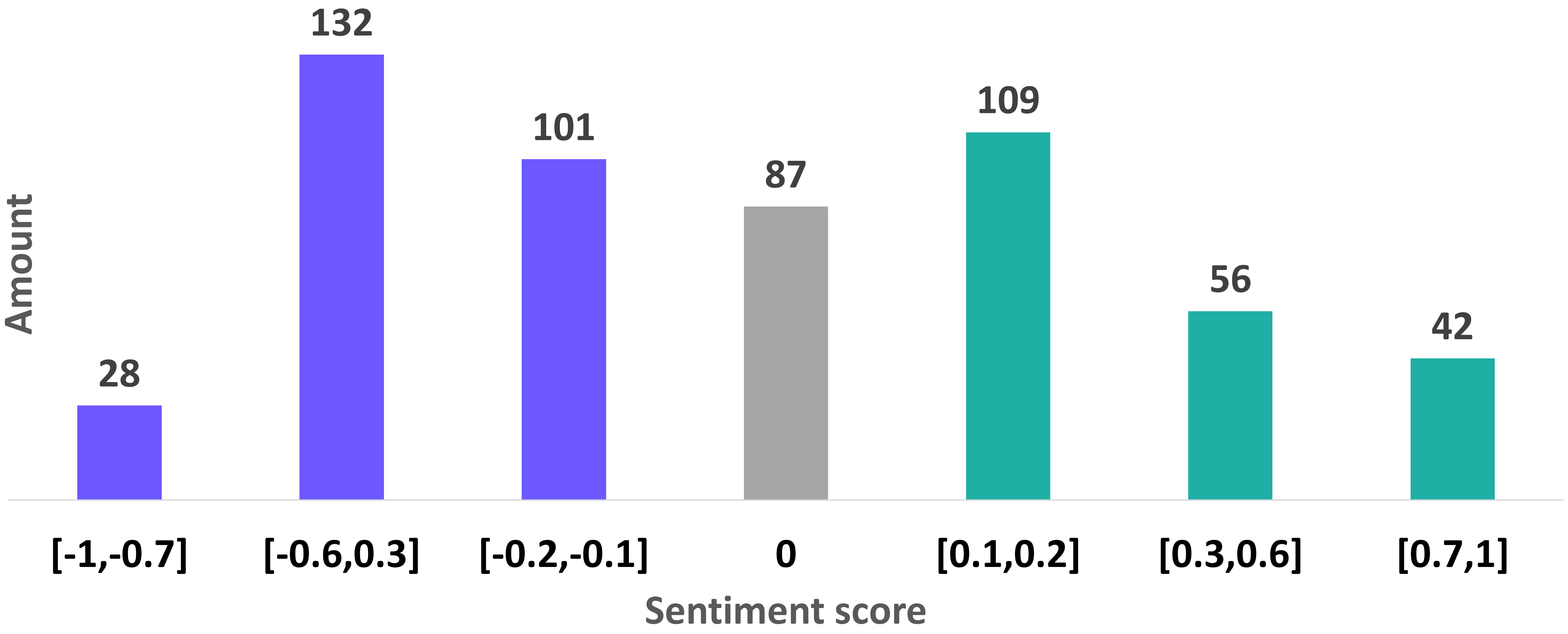
No History Record

Insufficient Information Depth

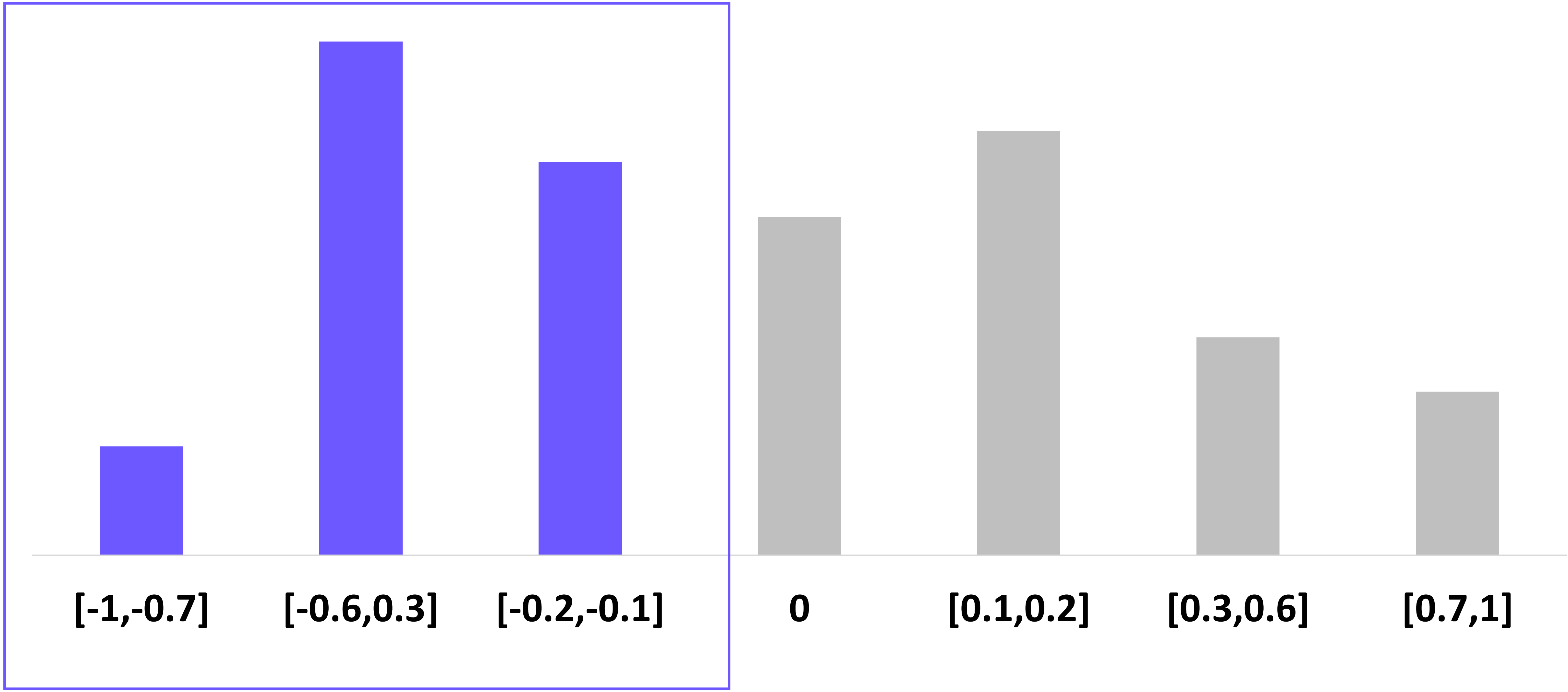
"I feel many of them are overly simplified. Many audits adopt a mass-production method to endorse applications and gather funds merely. The resulting report is concise, just a few pages, and the content lacks depth" (P01)

How Do Users **Perceive** the **Role** of Web3 Auditing in **Enhancing Security** within the Web3 Ecosystem?

Distribution of Sentiment Analysis on Online Web3 Community Discussion



Negative Attitudes



Questioning the Effectiveness

“Do Web3 audits hold any value? On a single day, two Web3 applications verified by [Audit Firm] suffered breaches, with losses summing up to 14 million USD” (Post189).

Questioning the Effectiveness

“Do Web3 audits hold any value? On a single day, two Web3 applications verified by [Audit Firm] suffered **attacks**, with **losses** summing up to 14 million USD” (Post189).

Questioning the Auditing Firms

“Slip a bribe to the audit team.” (Post266: Comment13).

Independence?

“The brief three-page report, scarcely filled with a hundred words about an ’ Accumulated Error from Integer Division’ . . . it lacks any solid proof . . . This is both disappointing and disturbing” (Post65).

Impartiality?

Questioning the Auditing Firms

“Slip a **bribe** to the audit team.” (Post266: Comment13).

Independence?

“The brief three-page report, scarcely filled with a hundred words about an ’ Accumulated Error from Integer Division’ . . . **it lacks any solid proof** . . . This is both disappointing and disturbing” (Post65).

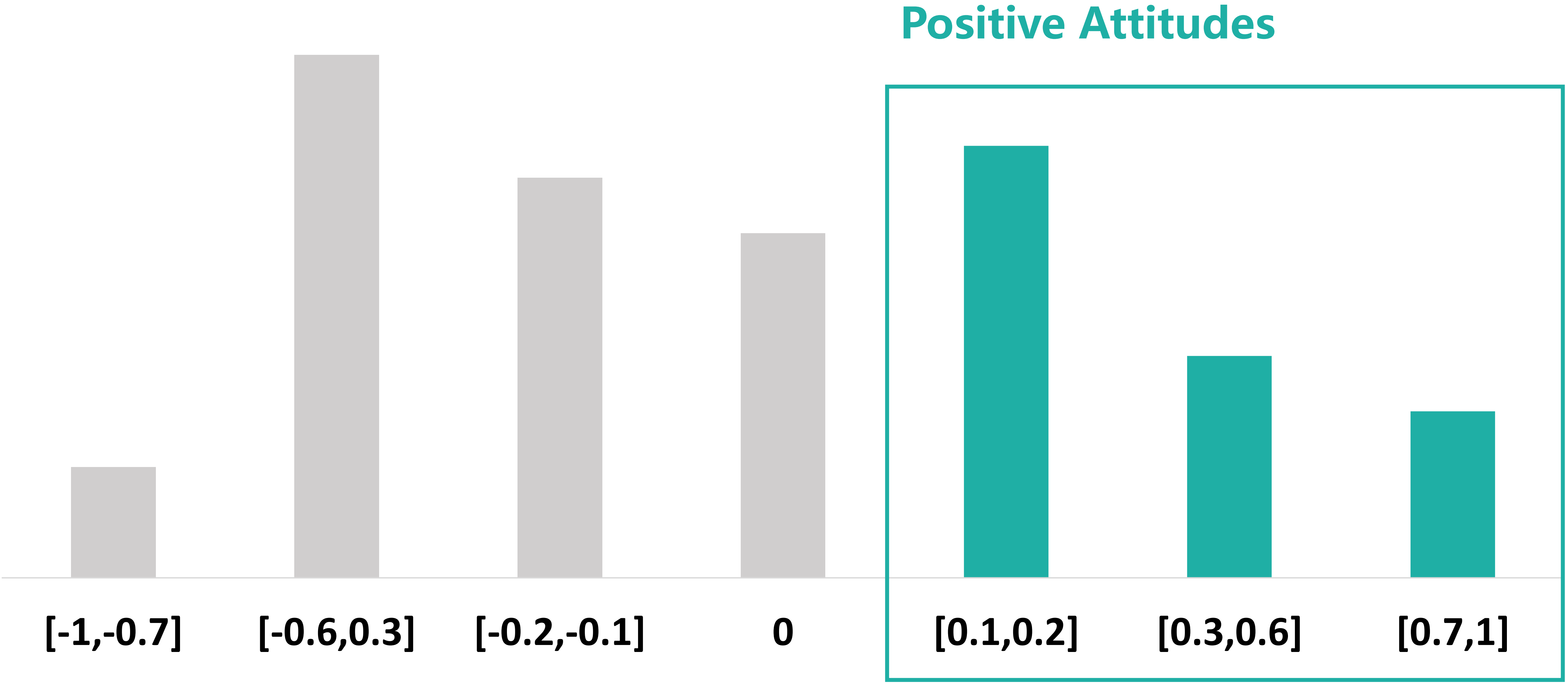
Impartiality?

Auditing Firms Lack Reputation

90%

Can’t name a

trustworty audit firm


Positive Attitudes
[-1,-0.7]
[-0.6,0.3]
[-0.2,-0.1]
0
[0.1,0.2]
[0.3,0.6]
[0.7,1]

Catalyst for Enhanced Security

"I think that auditing can reduce the likelihood of such attacks to some extent" (P03)

"Mandating that [application] be backed and audited would be a commendable regulatory measure" (Post57:Comment2).

Proof for Security Efforts

“Contract security itself cannot achieve 100% protection. . . the greatest value of an audit is to give ordinary users confidence, showing that the application is serious about its security and at least willing to invest in an audit.” (P14)

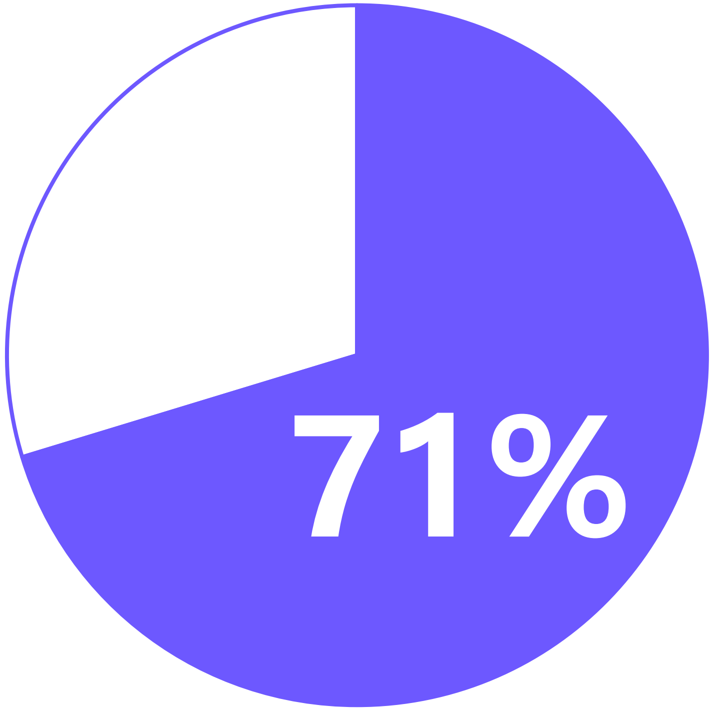
Financial Cost

Proof for Security Efforts

> “Contract security itself cannot achieve 100% protection. . . the greatest value of an audit is to give ordinary users confidence, showing that the application is serious about its security and at least willing to invest in an audit.” (P14)

Financial Cost ← Lack of Strong Backing

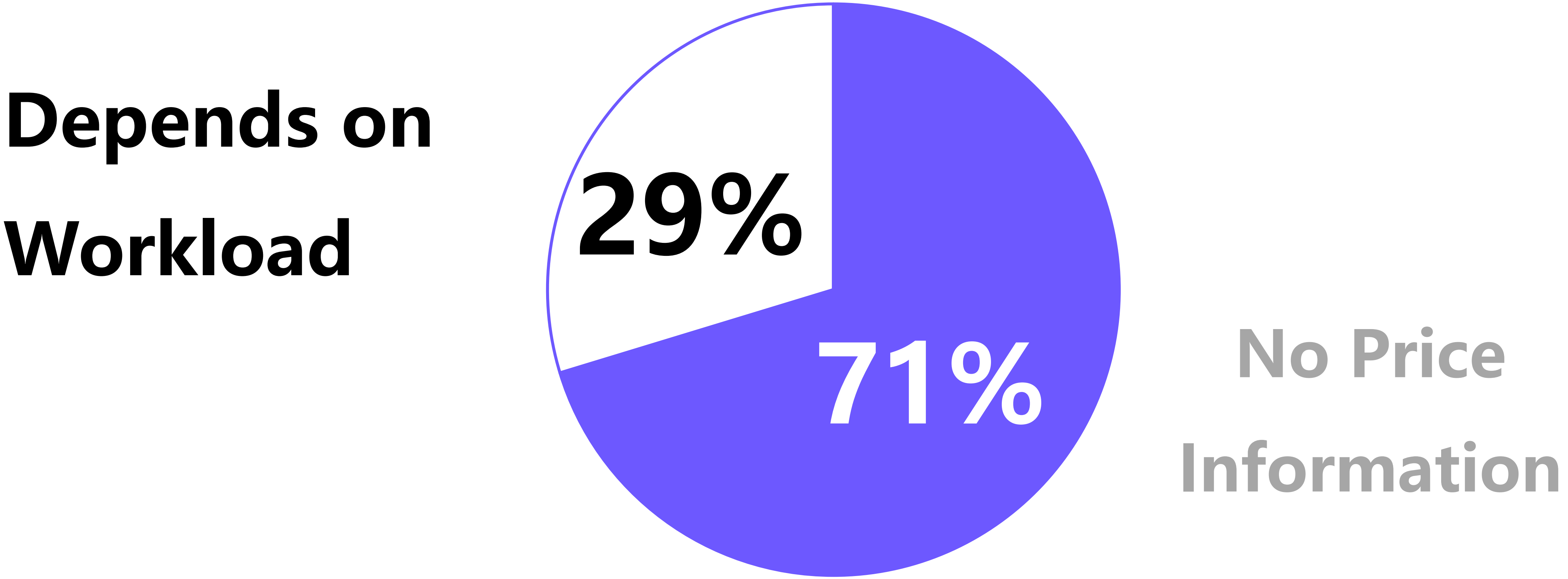
Hard to Know Proof for Security Efforts



No Price

Information

Hard to Know Proof for Security Efforts



CYBER AND CRYPTO LAB

NDSS SYMPOSIUM/2025 Internet Society 澳門大學 UNIVERSIDADE DE MACAU UNIVERSITY OF MACAU

How Do Users Perceive The Impact of Web3 Auditing on Their Interactions With Audited Applications?

Limited Impact on Security Decisions

“I don’ t think it is necessary to read the audit report. . . I at least know that this application has been **audited**” (P15).

“I just browsed it briefly and didn’ t look at it seriously” (P08)

Limited Impact on Security Decisions

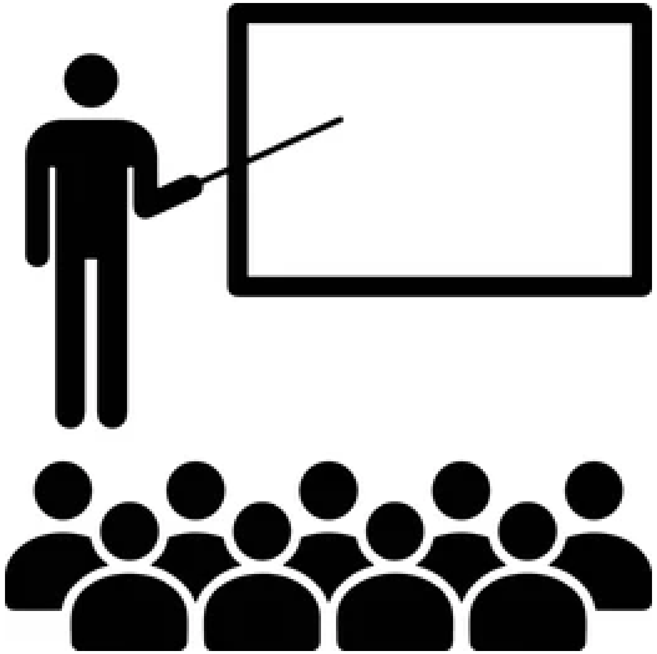
“I don’ t think it is necessary to read the audit report. . . I at least know that this application has been **audited**” (P15).

“I just browsed it briefly and **didn’ t look at it seriously**” (P08)

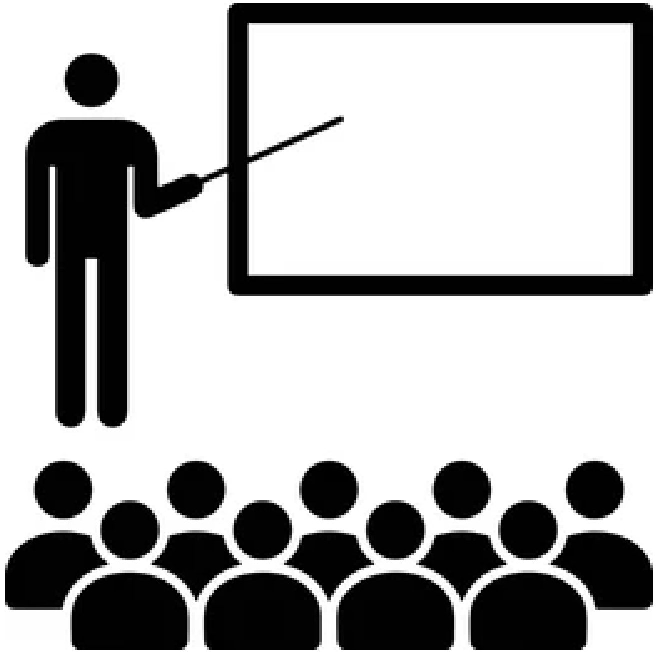
CYBER AND CRYPTO LAB

NDSS SYMPOSIUM/2025 Internet Society 澳門大學 UNIVERSIDADE DE MACAU UNIVERSITY OF MACAU

Security Education

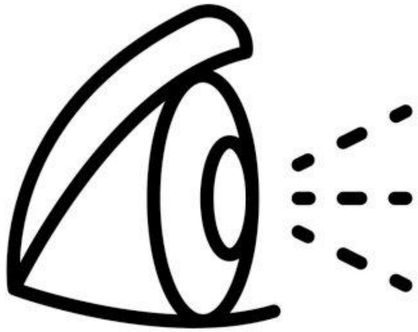


Security Education



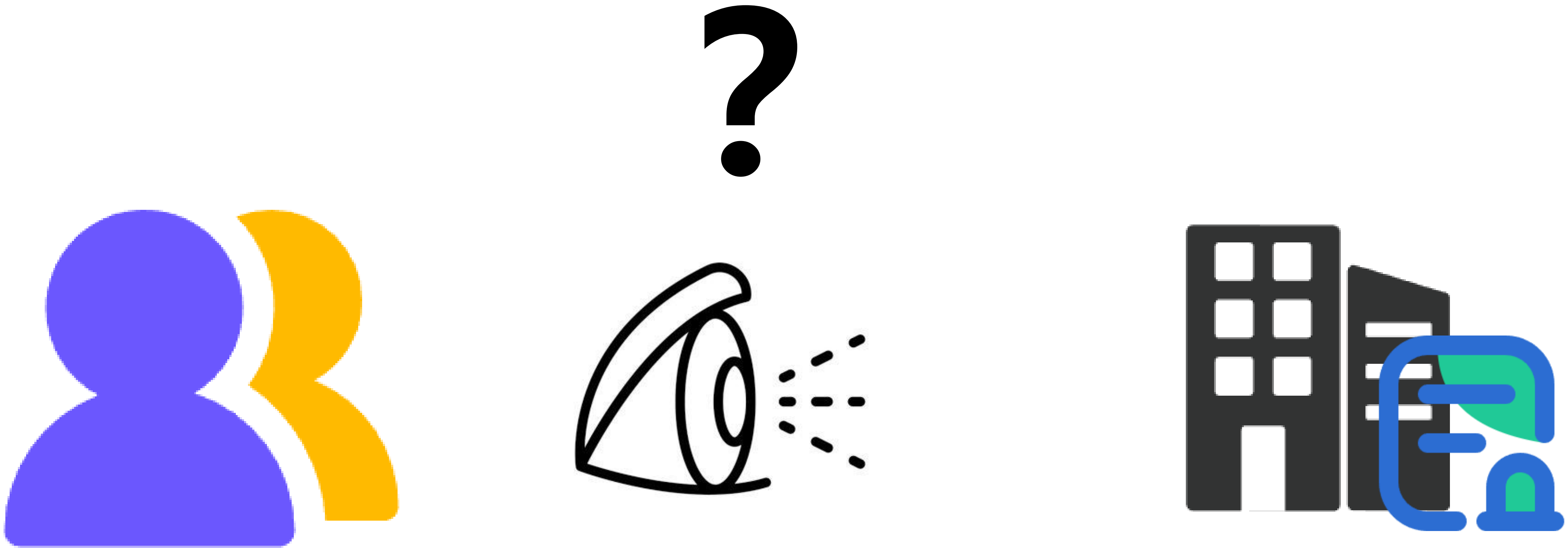
Security Awareness

User



Perceive

Web3 Auditing



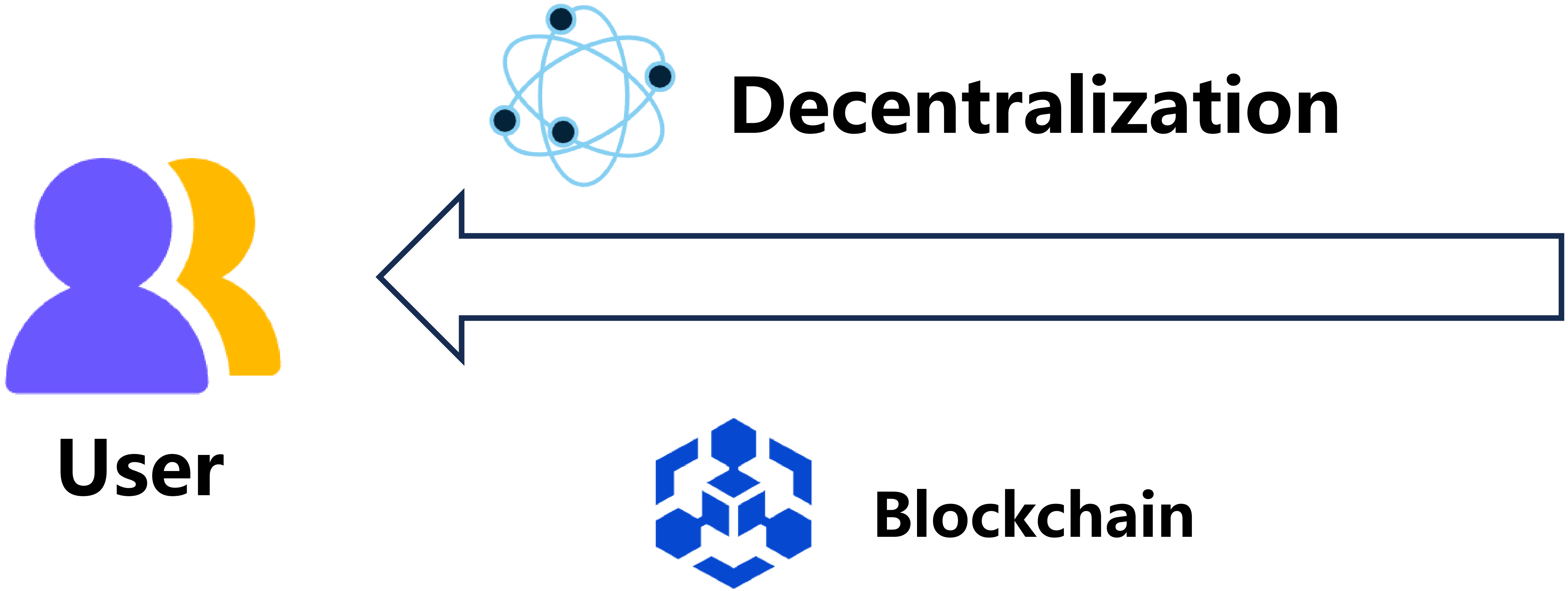
?

User

Perceive

Web3 Auditing

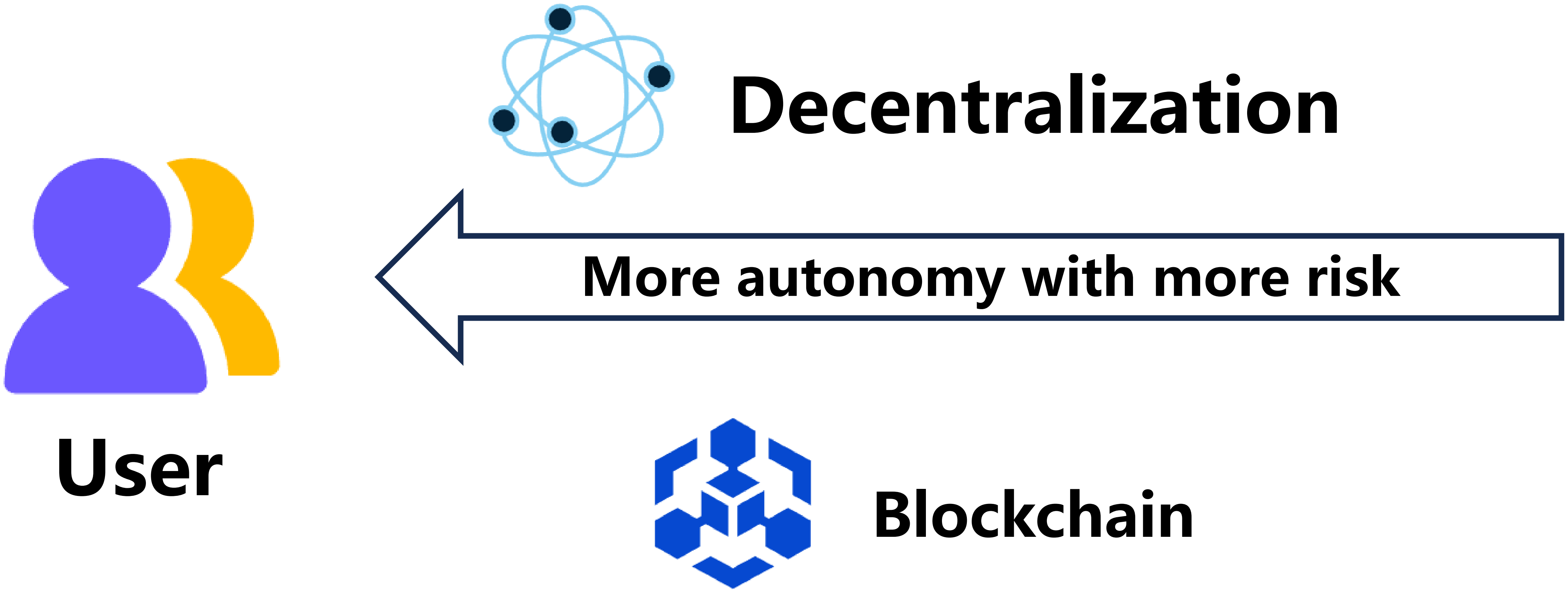
The Unique Characteristics of Web3 and Challenge in Security Auditing



Decentralization

User

Blockchain



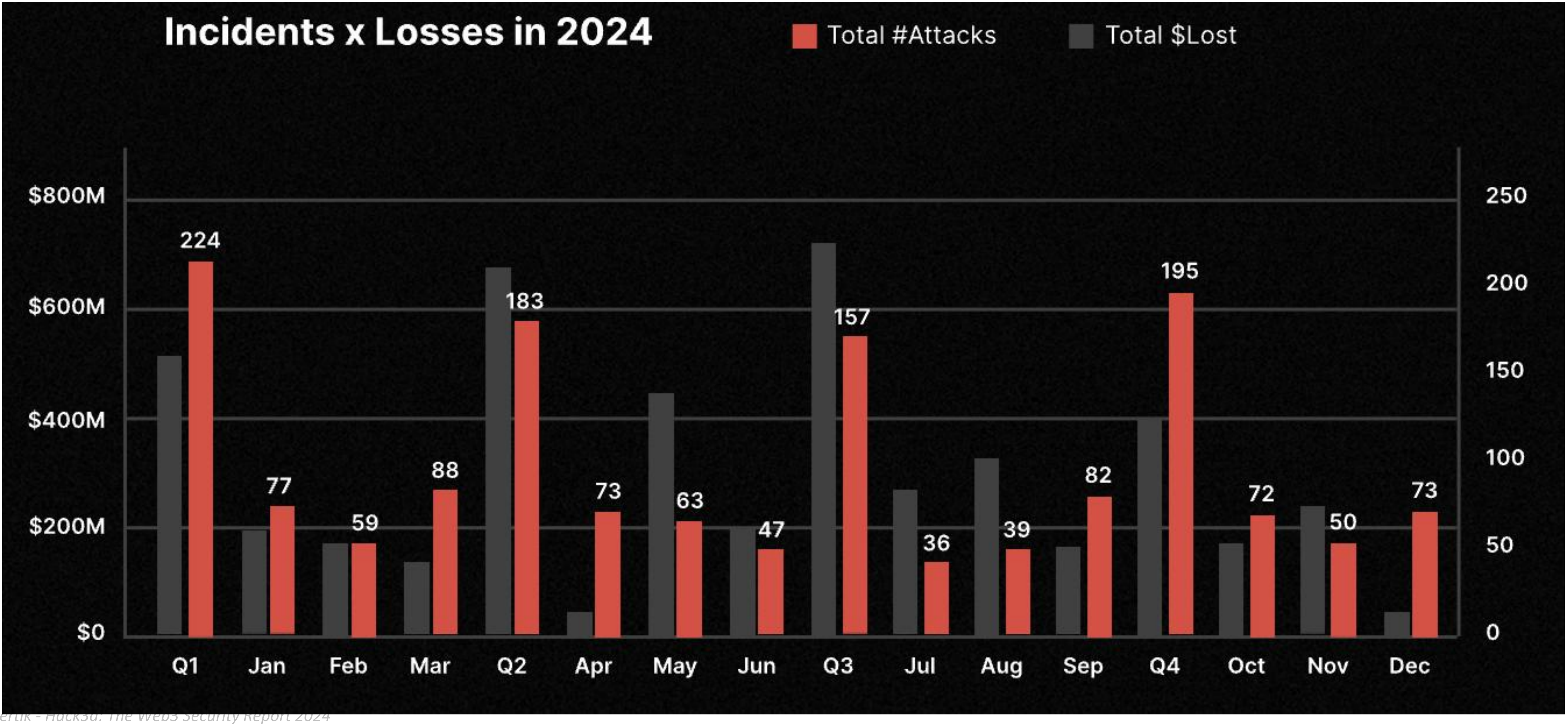
Decentralization

More autonomy with more risk

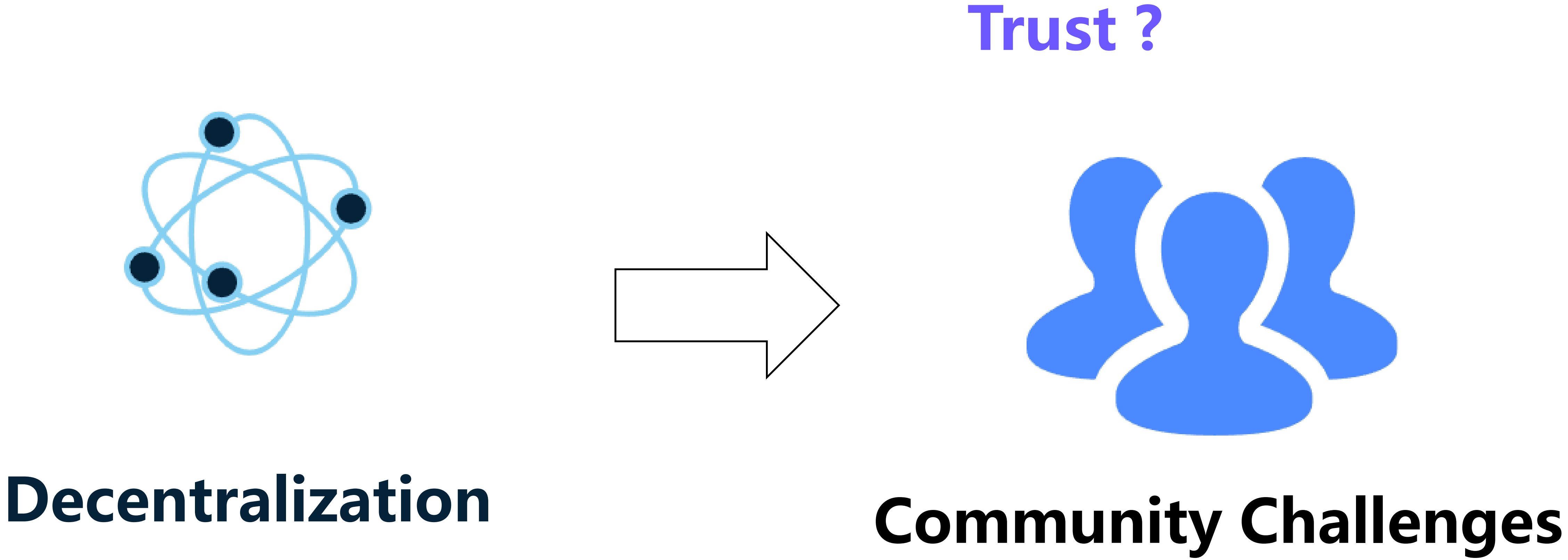
User

Blockchain

Frequent Security Incidents And Significant Financial Losses



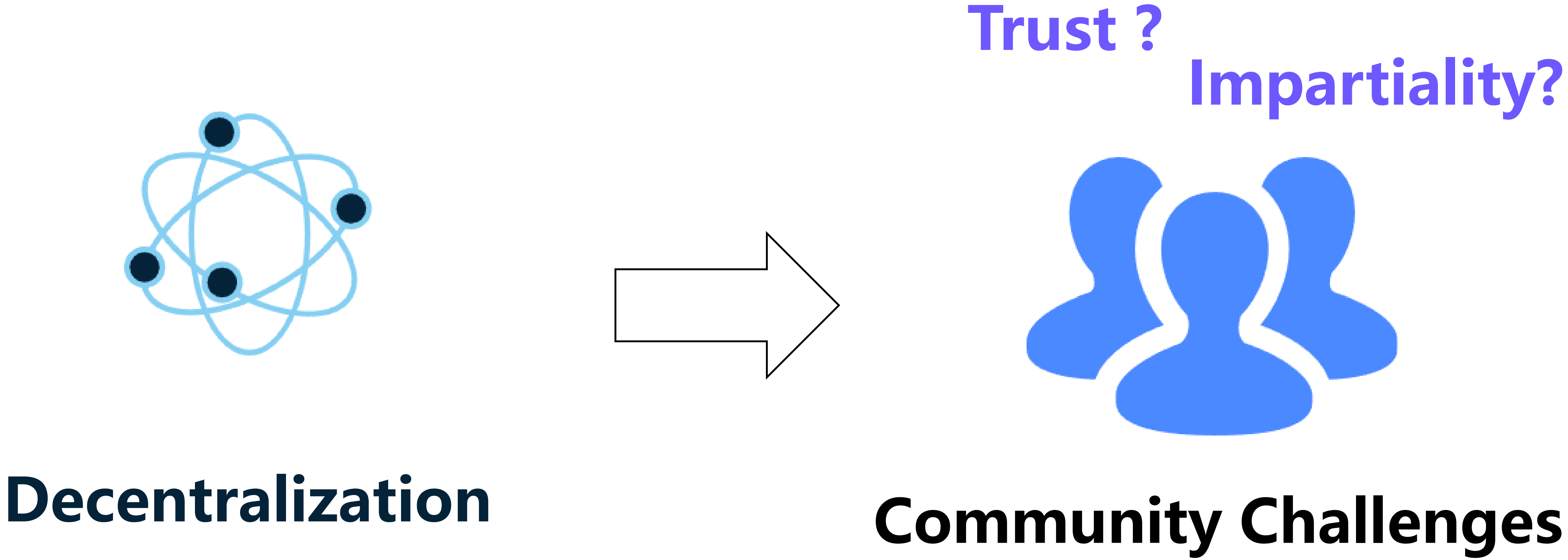
Source: Certik - Hack3d: The Web3 Security Report 2024



Trust ?

Decentralization

Community Challenges

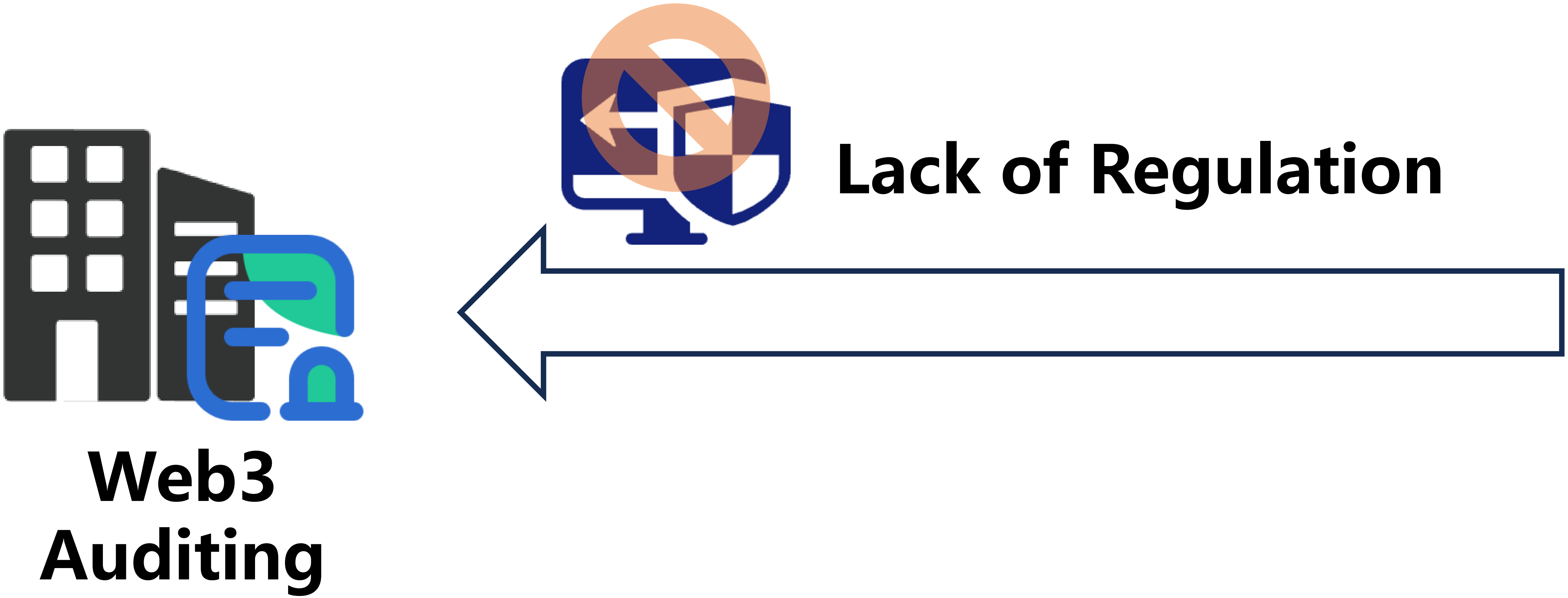


Trust ?

Impartiality?

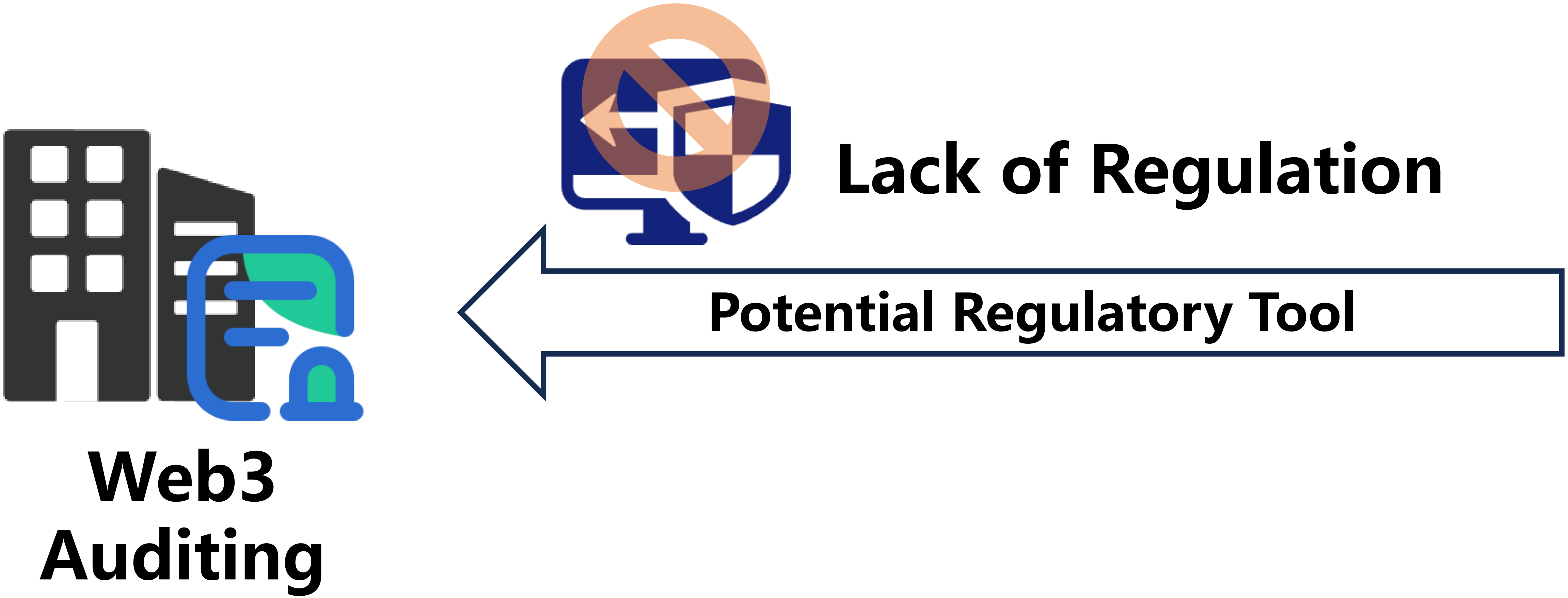
Decentralization

Community Challenges



Lack of Regulation

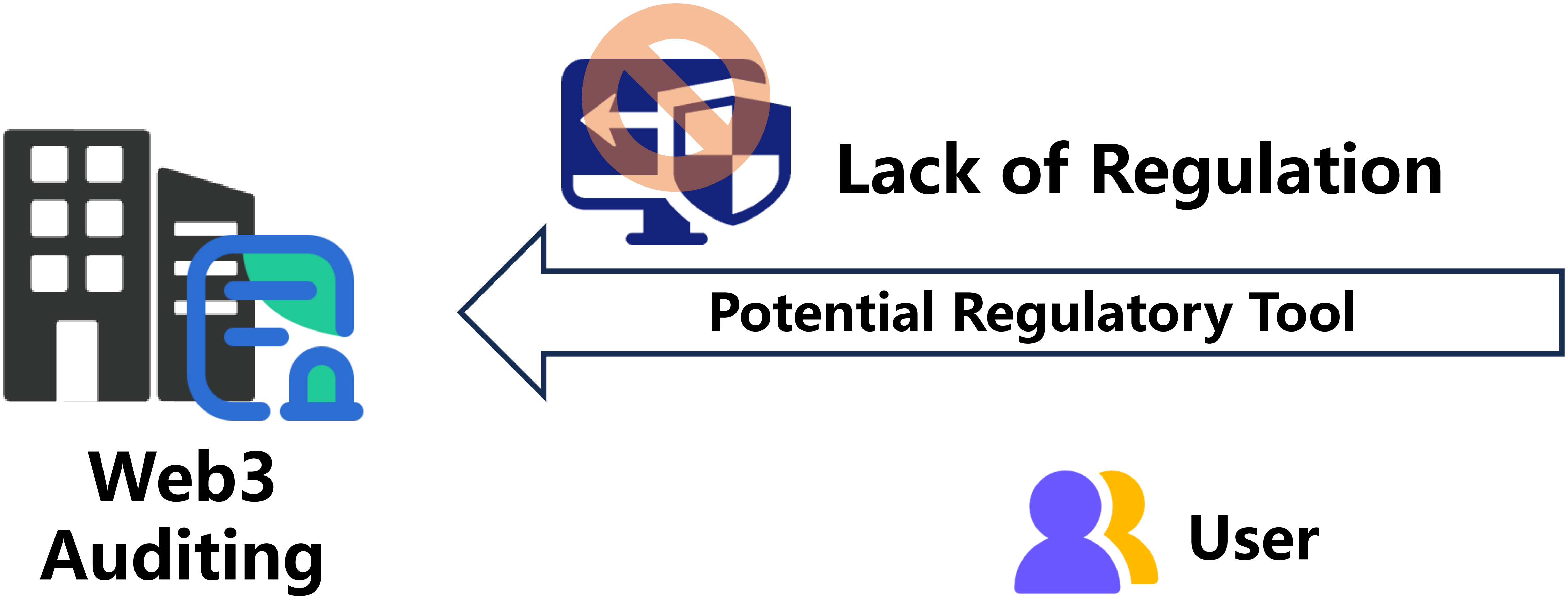
Web3 Auditing



Lack of Regulation

Potential Regulatory Tool

Web3
Auditing

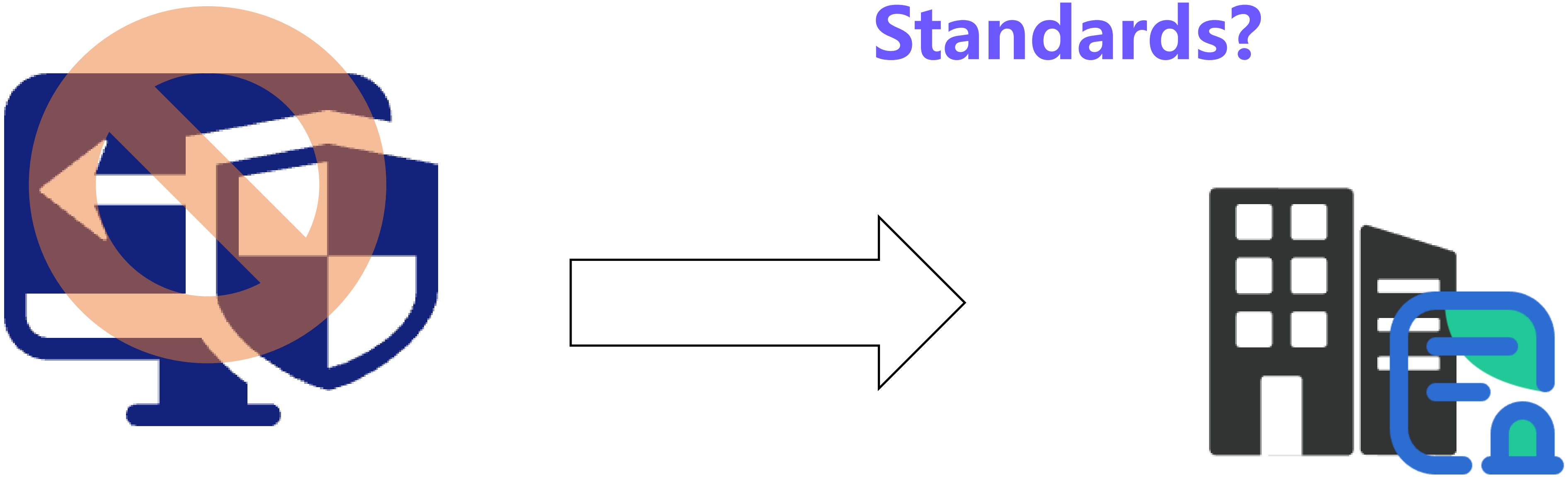


Lack of Regulation

Potential Regulatory Tool

Web3 Auditing

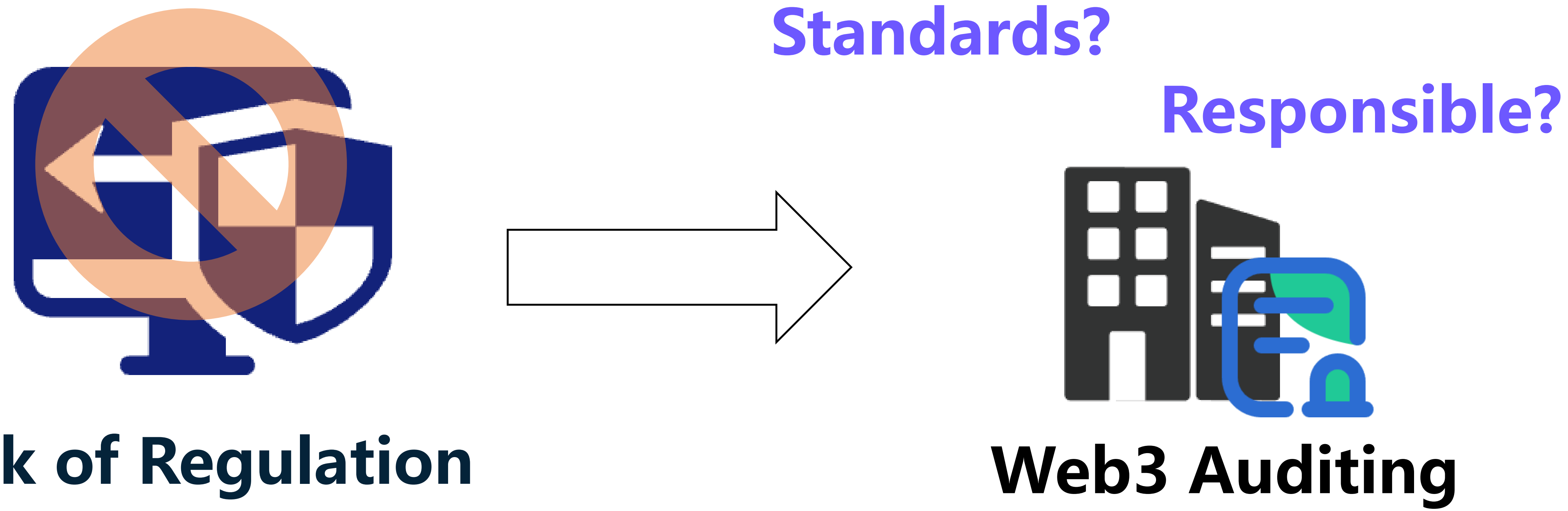
User



Standards?

Lack of Regulation

Web3 Auditing



Lack of Regulation

Standards?

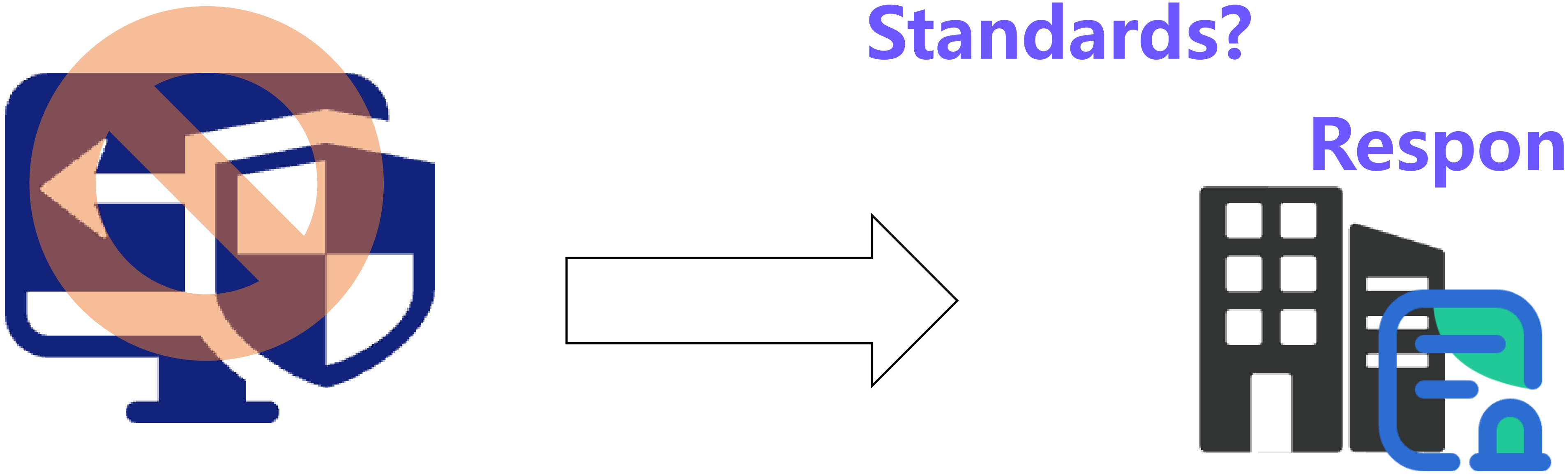
Responsible?

Web3 Auditing

Reputations?

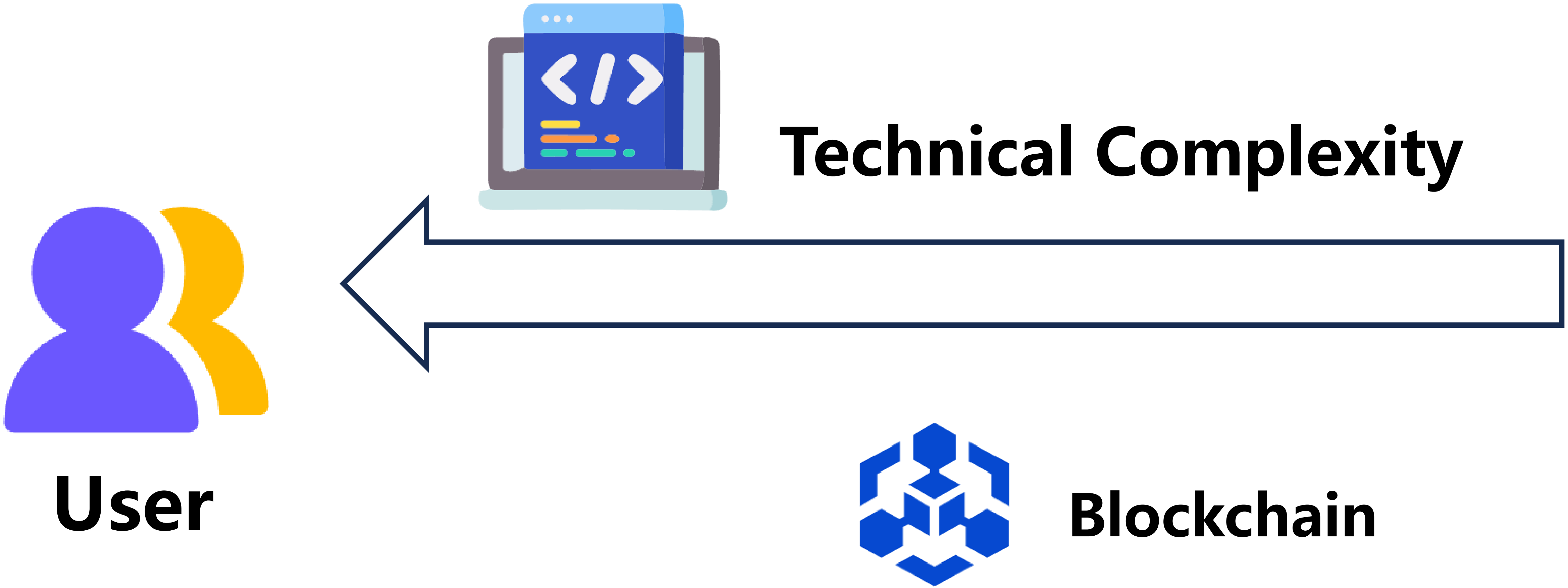
Standards?

Responsible?



Lack of Regulation

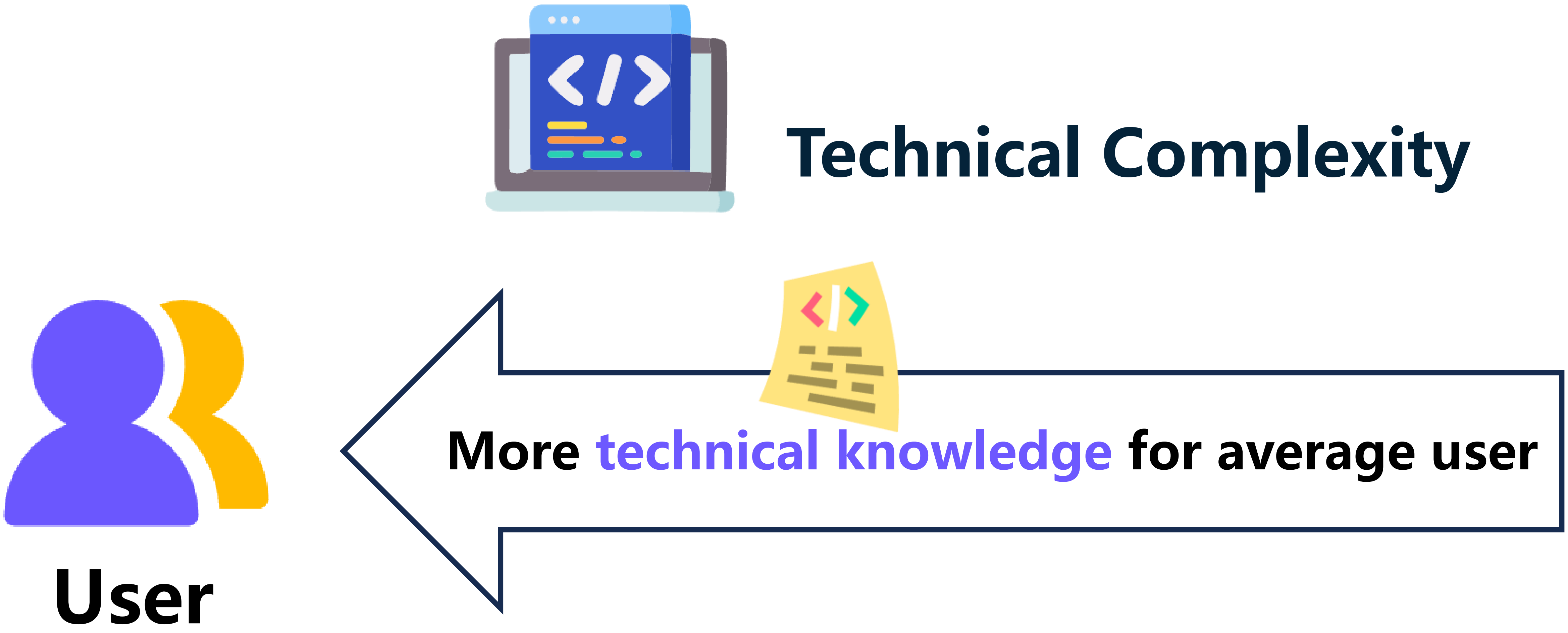
Web3 Auditing



Technical Complexity

User

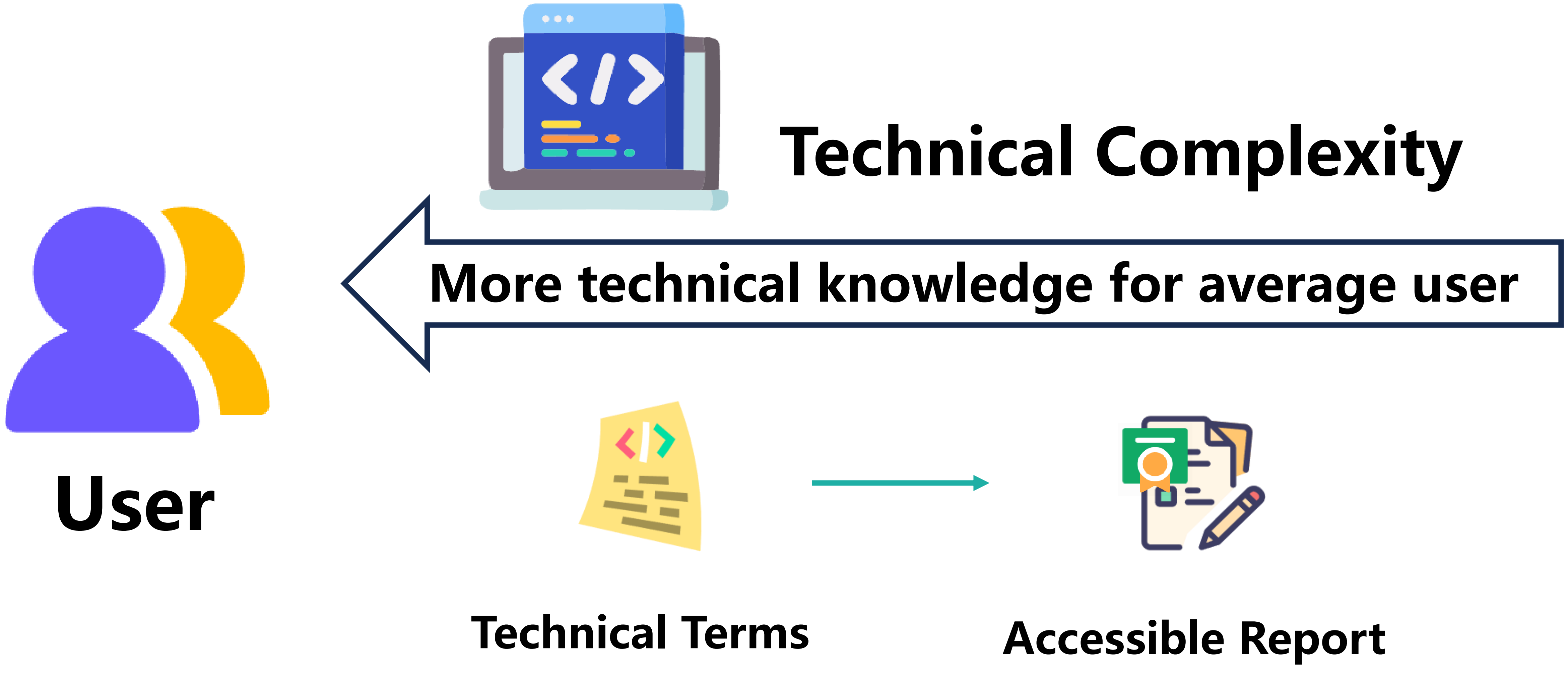
Blockchain



Technical Complexity

More technical knowledge for average user

User



Technical Complexity

More technical knowledge for average user

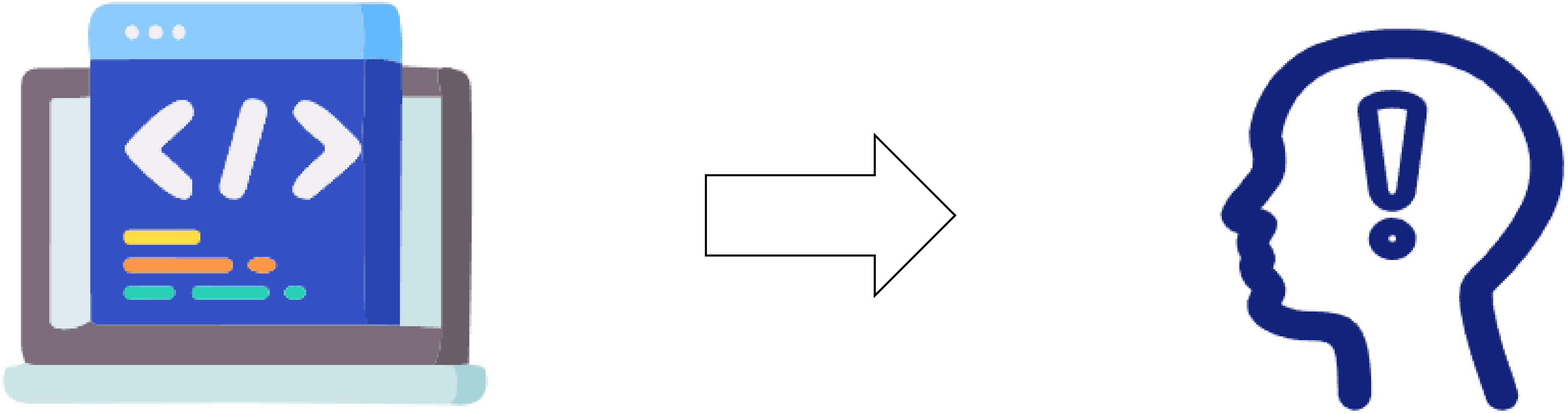
User

Technical Terms

Accessible Report

Readability?

Professionalism?



Technical Complexity

Diverse Users Backgrounds

Design Implication

User：Leveraging Communities for Technical Understanding

Audit Firms: Information Balance and Trust-built Measures

CYBER AND CRYPTO LAB

NDSS SYMPOSIUM/2025

Internet Society

32nd Annual Network and Distributed System Security (NDSS) Symposium

Exploring User Perceptions of Security Auditing in the Web3 Ecosystem

Molly Zhuangtong Huang, Rui Jiang, Tanusree Sharma , and Kanye Ye Wang

San Diego, CA

Tuesday, 25 February 2025

THANK YOU!

Any questions?

✉ Email us at: yc37496@umac.mo

X: @ZhuangtongH

Visit University of Macau

澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU