The role of RegTech & SupTech in Crypto-DeFi

Pouya Pourazam

Jan9 event

2025

TABLE OF CONTENTS

01 What is RegTech & SupTech

02 Crypto & DeFi Regulation Concerns

03 Self-Regulation and Embedded Supervision

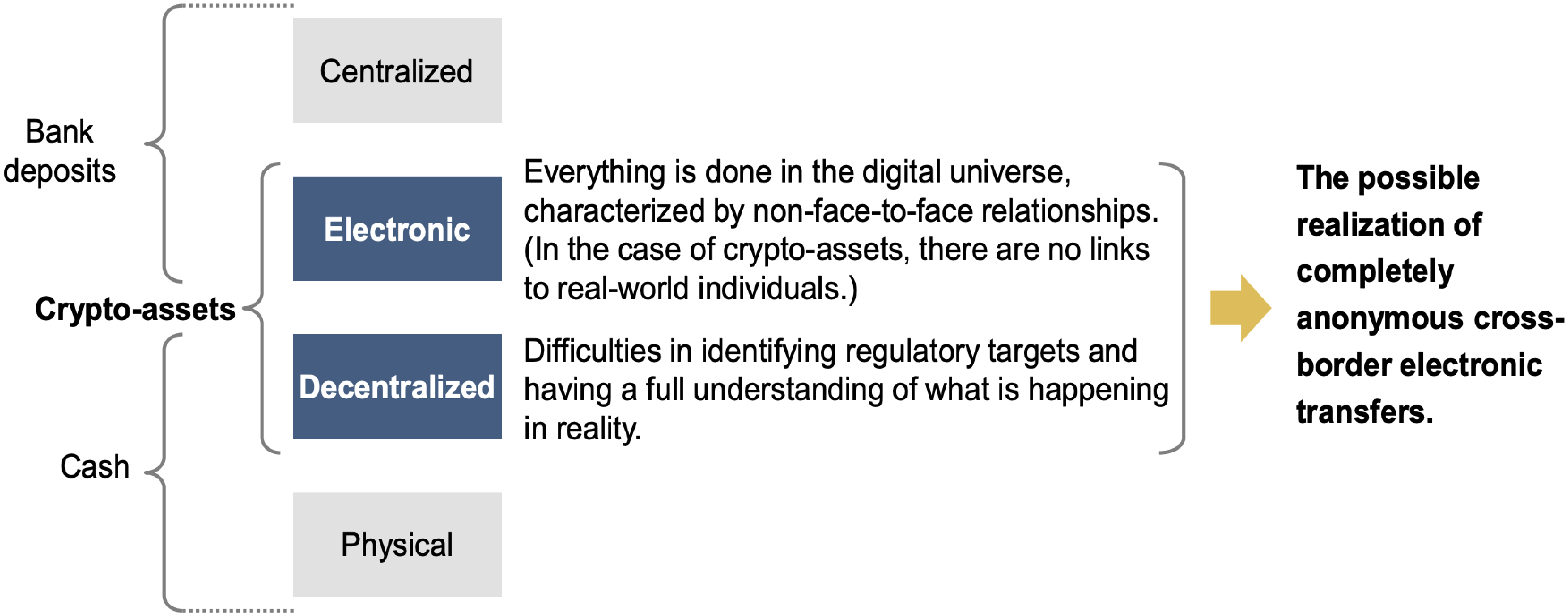
04 Financial-Crypto Blockchain Infra Security

05 Compliance ,AML, Fraud, KYT, DID

06 Crypto Investigation & Forensics

تغییر ماهیت پول و خدمات مالی = تغییر ماهیت
نهادهای قانون گذاری و نظارت

Characteristics of crypto-assets compared to fiat currencies



Bank deposits

Crypto-assets

Cash

Centralized

Electronic

Decentralized

Physical

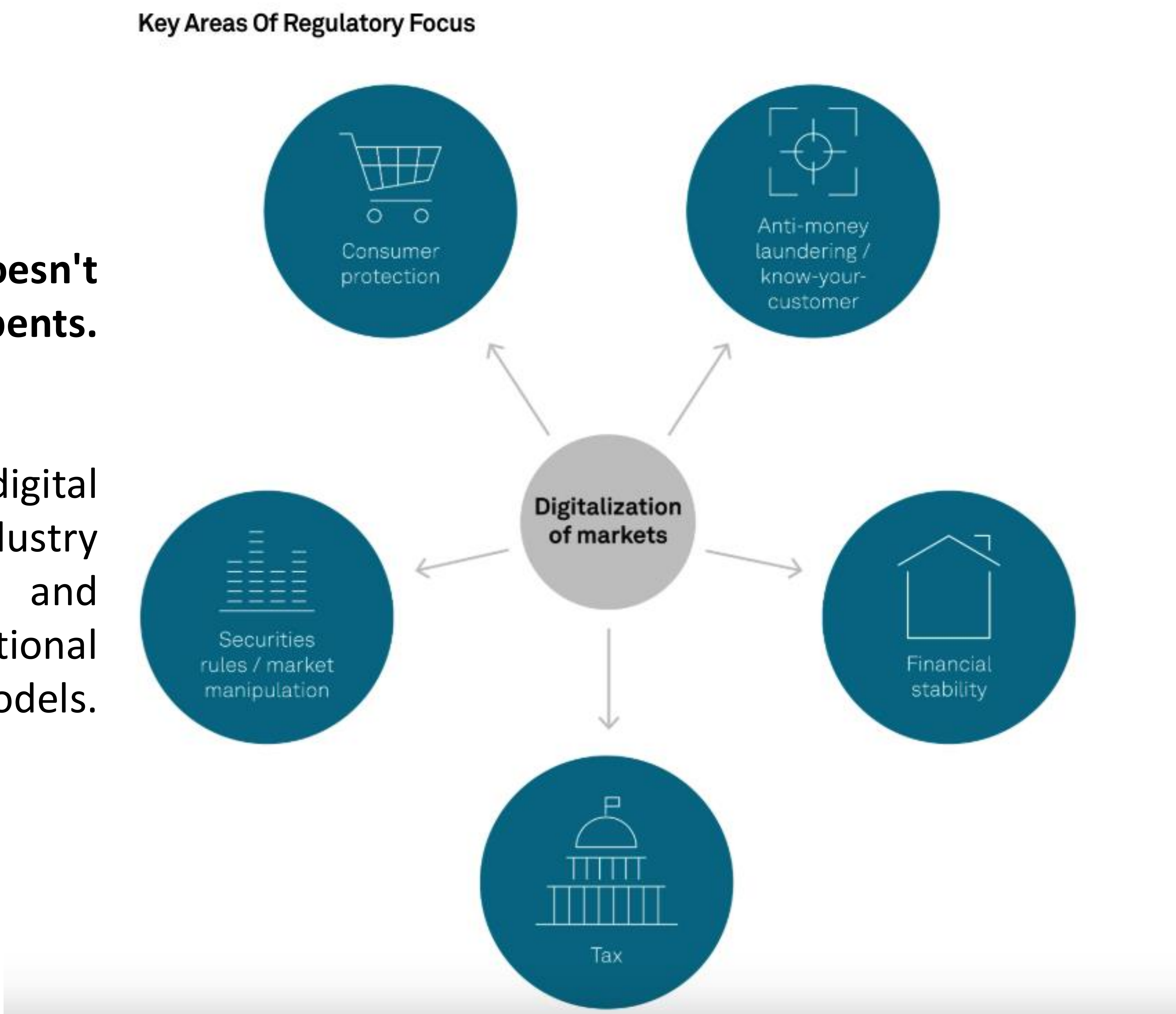
Everything is done in the digital universe, characterized by non-face-to-face relationships. (In the case of crypto-assets, there are no links to real-world individuals.)

Difficulties in identifying regulatory targets and having a full understanding of what is happening in reality.

The possible realization of completely anonymous cross-border electronic transfers.

An acceleration in regulatory initiatives doesn't necessarily protect traditional finance incumbents.

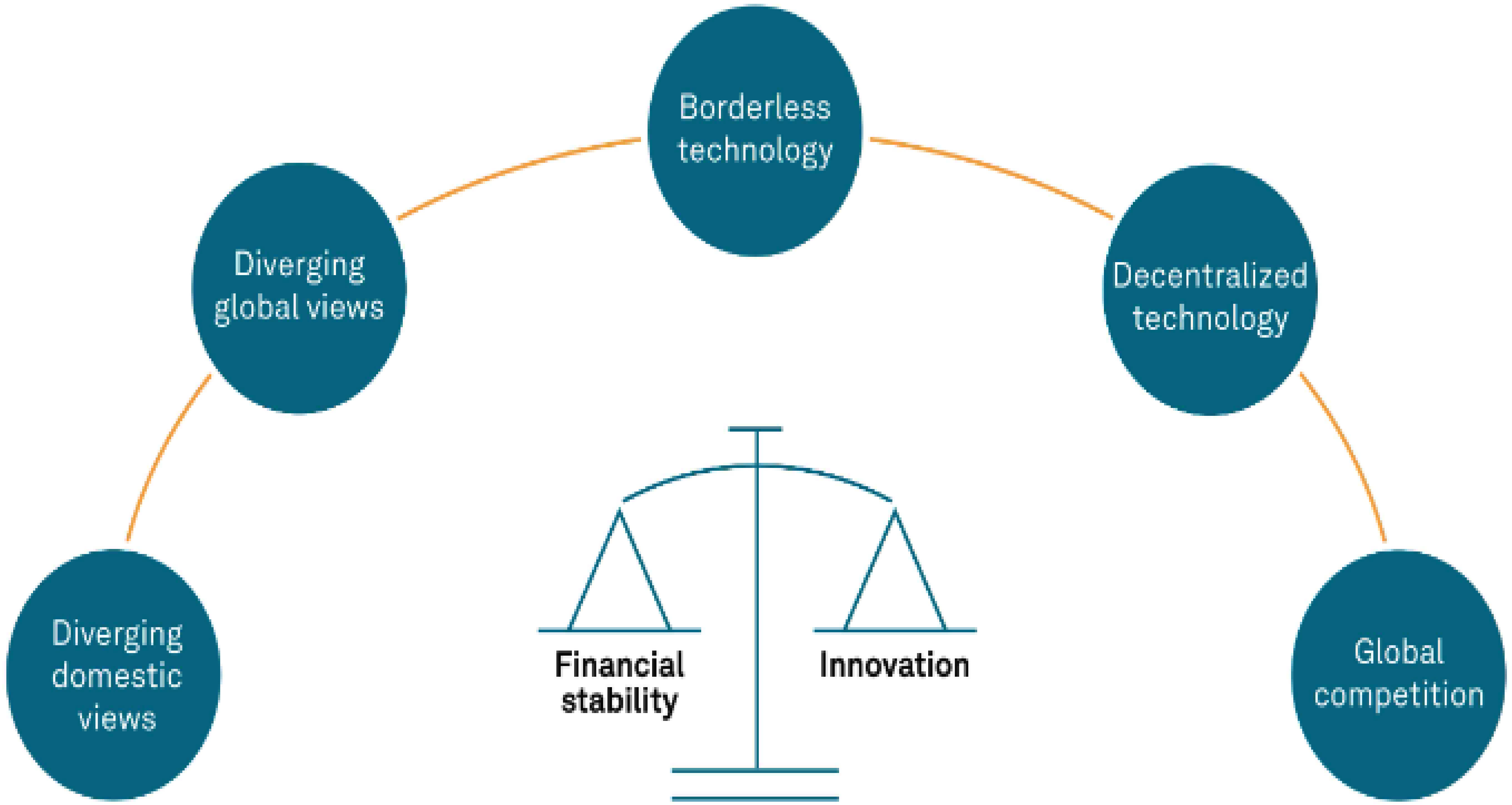
Building a coherent regulatory framework around digital assets and DeFi may legitimize and accelerate industry development, by attracting new customers and incentivizing entrants that pose a risk to traditional finance incumbents' operating models.


Key Areas Of Regulatory Focus
Consumer protection
Anti-money laundering / know-your-customer
Digitalization of markets
Securities rules / market manipulation
Financial stability
Tax

The statement released by the Financial Stability Board on July 11, 2022, highlights that this ecosystem "must be subject to effective regulation and oversight commensurate to the risks they pose, both at the domestic and international level".

Yet, in terms of regulating this new world of crypto and DeFi, the market adage that past performance is not indicative of future results could hold true. Standard setters and supervisors across regions will have to contend with several complicating factors

The Challenges Of Regulating Crypto



Source: S&P Global Ratings.
Copyright @ 2022 by Standard & Poor's Financial Services LLC. All rights reserved.

THE REGULATORY CHALLENGES

True decentralization makes it tough to identify persons or businesses that can be held accountable through regulations.

One key task is to determine which individuals or entities fall within regulatory perimeters

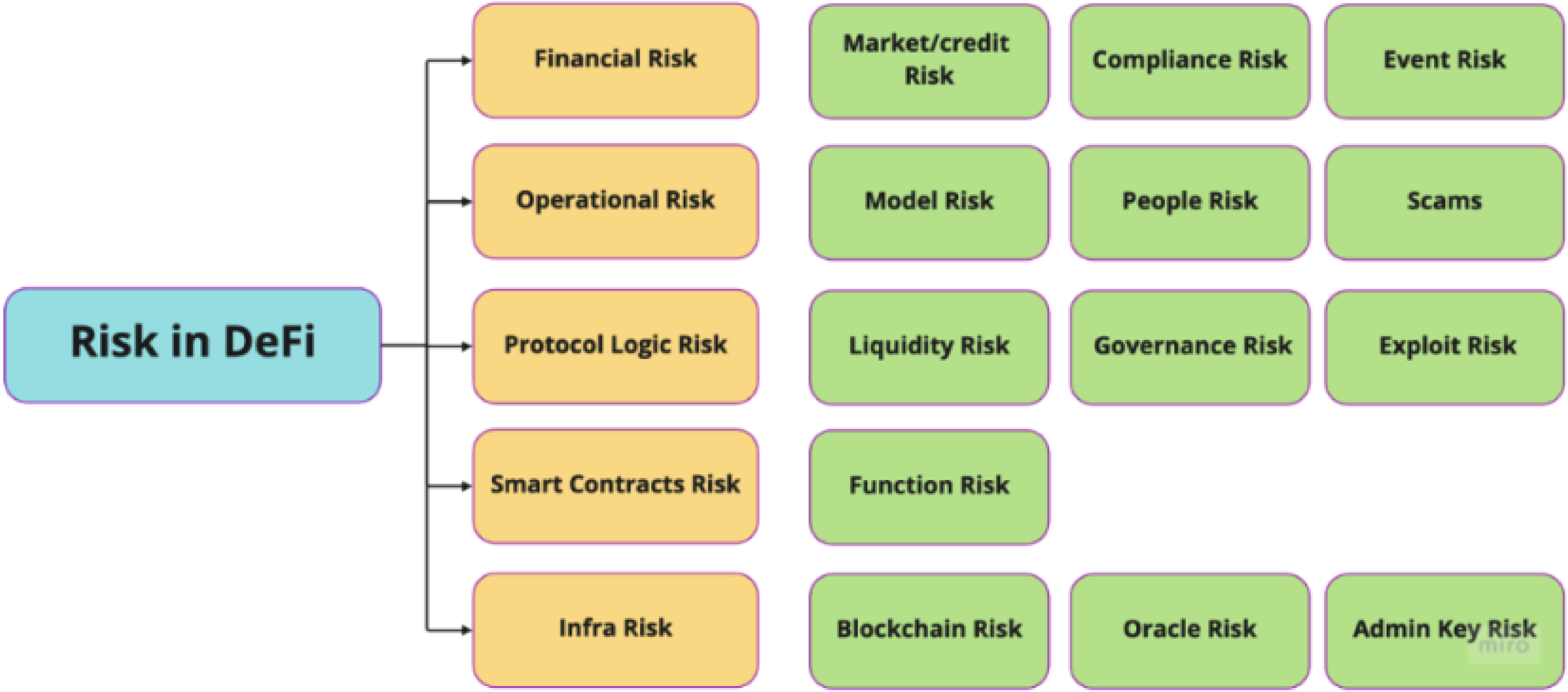
Because DeFi gives the financial responsibility--including asset custody and investments--back to users, we think some understanding of smart contracts is needed.

What is RegTech & SupTech

Regtech is critical in tackling compliance concerns in the DeFi age. Because of the decentralized nature of DeFi systems, creative solutions are required to assure regulatory compliance. Regtech is providing effective KYC and AML compliance, transaction monitoring, smart contract compliance, data privacy, regulatory reporting, and engagement with regulators through advanced technologies.

As the DeFi environment evolves, Regtech will continue to play an important role in managing compliance issues and promoting the expansion of decentralized finance in a secure and regulated manner

SCHOLZE (Co-founder and CEO of fija finance) noted that 88% of crypto holders in Europe want to earn yields on their assets, but only 4% do so. The problem? DeFi's complexity and perceived risks create a steep barrier to entry.



Risk in DeFi

Financial Risk

Operational Risk

Protocol Logic Risk

Smart Contracts Risk

Infra Risk

Market/credit Risk

Compliance Risk

Event Risk

Model Risk

People Risk

Scams

Liquidity Risk

Governance Risk

Exploit Risk

Function Risk

Blockchain Risk

Oracle Risk

Admin Key Risk

Balancing Transparency and Privacy

One of the key value propositions of blockchain and DeFi is transparency. Balancing the need for transparency with the need for privacy is a significant challenge.

Traceability and Privacy

Privacy in DeFi also faces regulatory challenges. Regulatory bodies around the world are concerned about the potential for cryptocurrencies and DeFi to be used for illegal activities such as money laundering or terrorist financing. As a result, there is a push for more transparency, not less, which may limit the development of privacy features in DeFi.

What is the role of SupTech?!

Policy Making
Supervision Toolkit
Licensing
Sandbox
Compliance data insight

Crypto and DeFi RegTech

Secure regulatory compliance in the decentralized context

Decentralized Finance (DeFi) has emerged as a game-changing force in the financial industry, providing novel loan, trading, and investing alternatives.

- ❖ DeFi, on the other hand, provides major compliance issues due to its rapid expansion and complexity. This is where Regulatory Technology, or Regtech, enters the picture

- ❖ Regtech solutions are employing technology to assist in addressing compliance concerns in the DeFi & Crypto age

- ❖ Financial transactions are conducted directly between peers with no centralized monitoring, it is critical to identify solutions to assure compliance with existing legislation and norms.

- ❖ Regtech, which is powered by artificial intelligence, machine learning, and blockchain, provides solutions to these compliance issues.

Here are some main areas where Regtech is making a difference in the DeFi era:

1

KYC & AML

KYC and AML standards are essential in the prevention of financial crimes such as money laundering. it is critical to authenticate participant identity and detect suspect activity

2

Data Security and Privacy

Regtech solutions solve these issues by introducing strong data privacy protocols and secure data storage solutions.

Regtech protects sensitive user information and assures compliance with data protection standards.

3

Risk management and transaction monitoring

Transaction monitoring is critical for detecting and preventing financial crimes, as well as guaranteeing regulatory compliance.

The balance between compliance and decentralization

Other RegTech key era

Compliance audits and regulatory reporting

Compliance with Smart Contracts

Collaboration and Regulatory Sandboxes

Transparency and auditing

Decentralized governance

Smart contract standards and security

SELF REGULATION

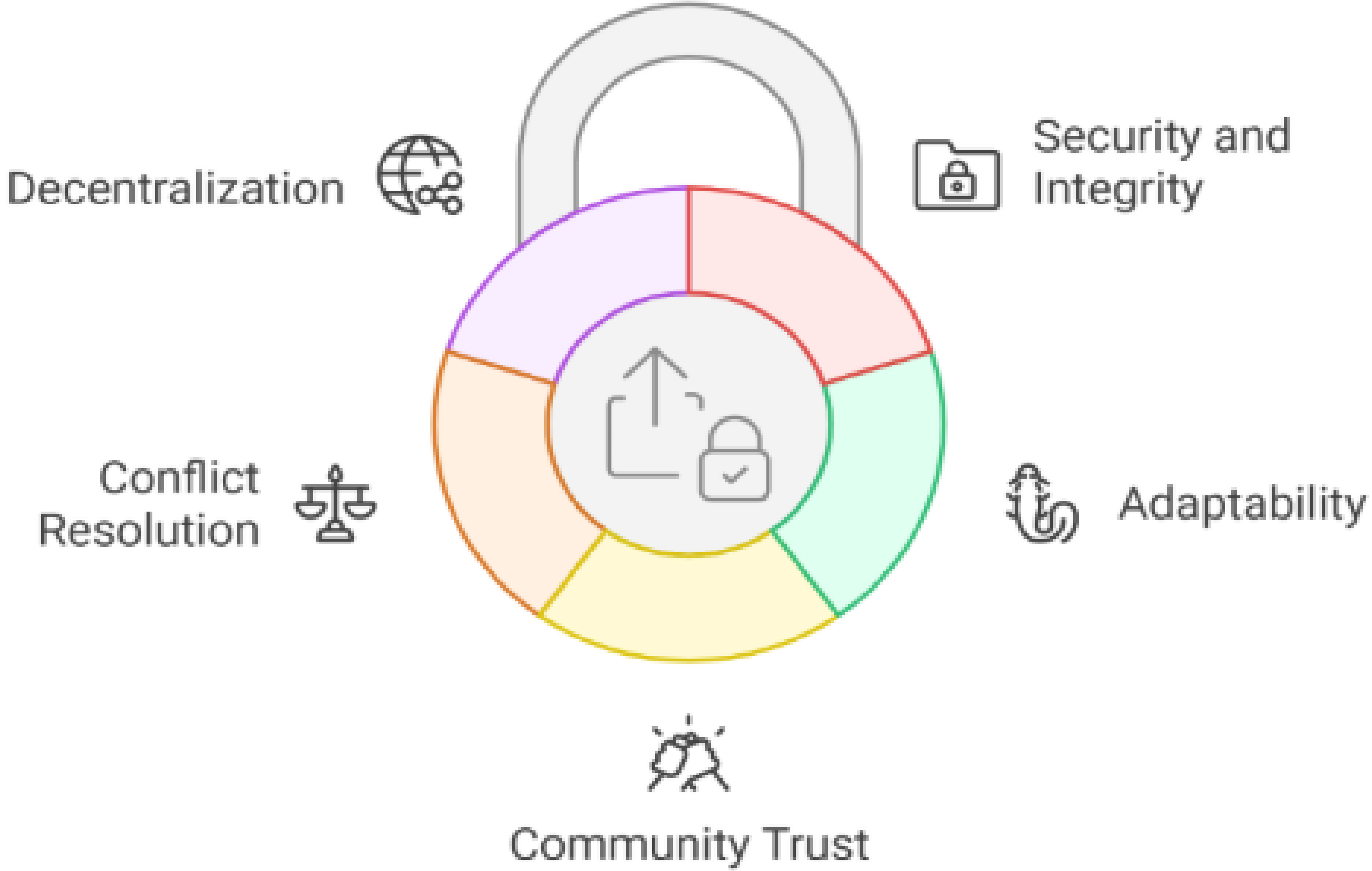
Can Regtech help DeFi Self-Regulate?

While DeFi promises a paradigm shift away from centralized control, the absence of regulatory oversight raises concerns regarding potential risks and challenges.

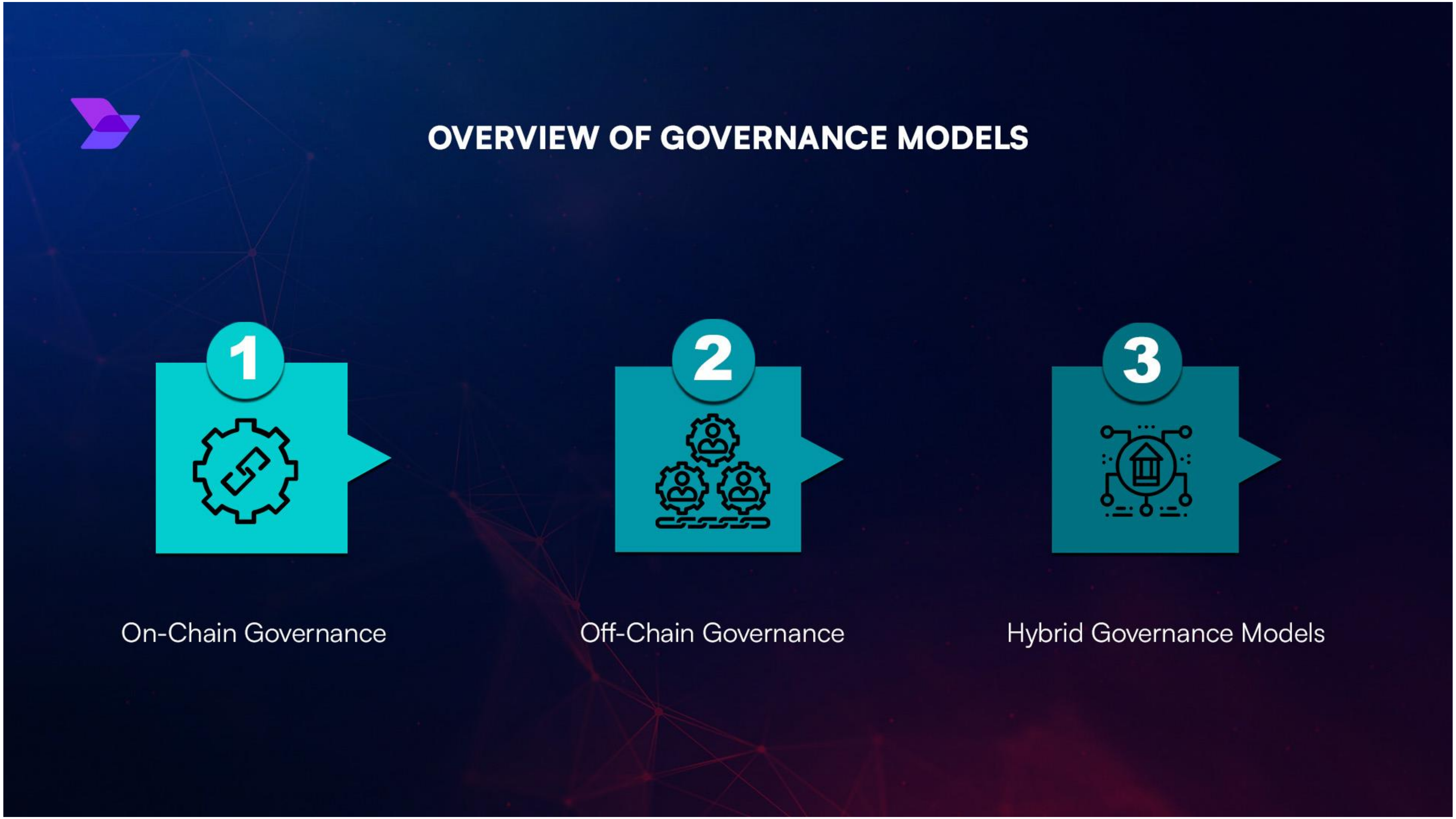
Self-regulation in DeFi refers to the establishment of rules, protocols, and mechanisms within the ecosystem to ensure fairness, security, and stability.

However, achieving effective self-regulation in a decentralized environment is a complex task, requiring collaboration, innovation, and community-driven governance.

The Importance Of Governance In Blockchain Networks



The Importance of Governance in Blockchain Networks



OVERVIEW OF GOVERNANCE MODELS

1

On-Chain Governance

2

Off-Chain Governance

3

Hybrid Governance Models

DECENTRALIZED GOVERNANCE

Decentralization and Democratic Governance: In Crypto & DeFi, power resides with the community or network participants, fostering security and democratizing decision-making through smart contracts and token-based governance.

Founder Control: The founders control the majority of Defi initiatives and set the direction for all the activities carried out by the users in the protocols. As choices are made completely by one individual, there is clear and faster decision making which helps the organizations to grow quickly.

Council Control: Here, the core developers serve as the council. The selected members of the community are appointed to help drive the governance and the future of these protocols. The authority is concentrated in a group of individuals who formulate plans and put out road plans. Bitcoin and Ethereum are two well-known examples of this model of governance.

Since users with more liquidity can access more governance tokens, the entire governance paradigm may progressively shift from decentralized to centralized, with power concentrated in the hands of a few. The existing Defi governance paradigm needs some significant improvements and options to fully address all these issues

What is the role of RegTech and SupTech?

EMBEDDED SUPERVISION: HOW TO BUILD REGULATION INTO DECENTRALIZED FINANCE

The emergence of so-called “decentralized finance” (DeFi) and a shadow financial system of cryptocurrency exchanges and stablecoin issuers raises the challenge of how to apply technology-neutral regulation so that similar risks are subject to the same rules.

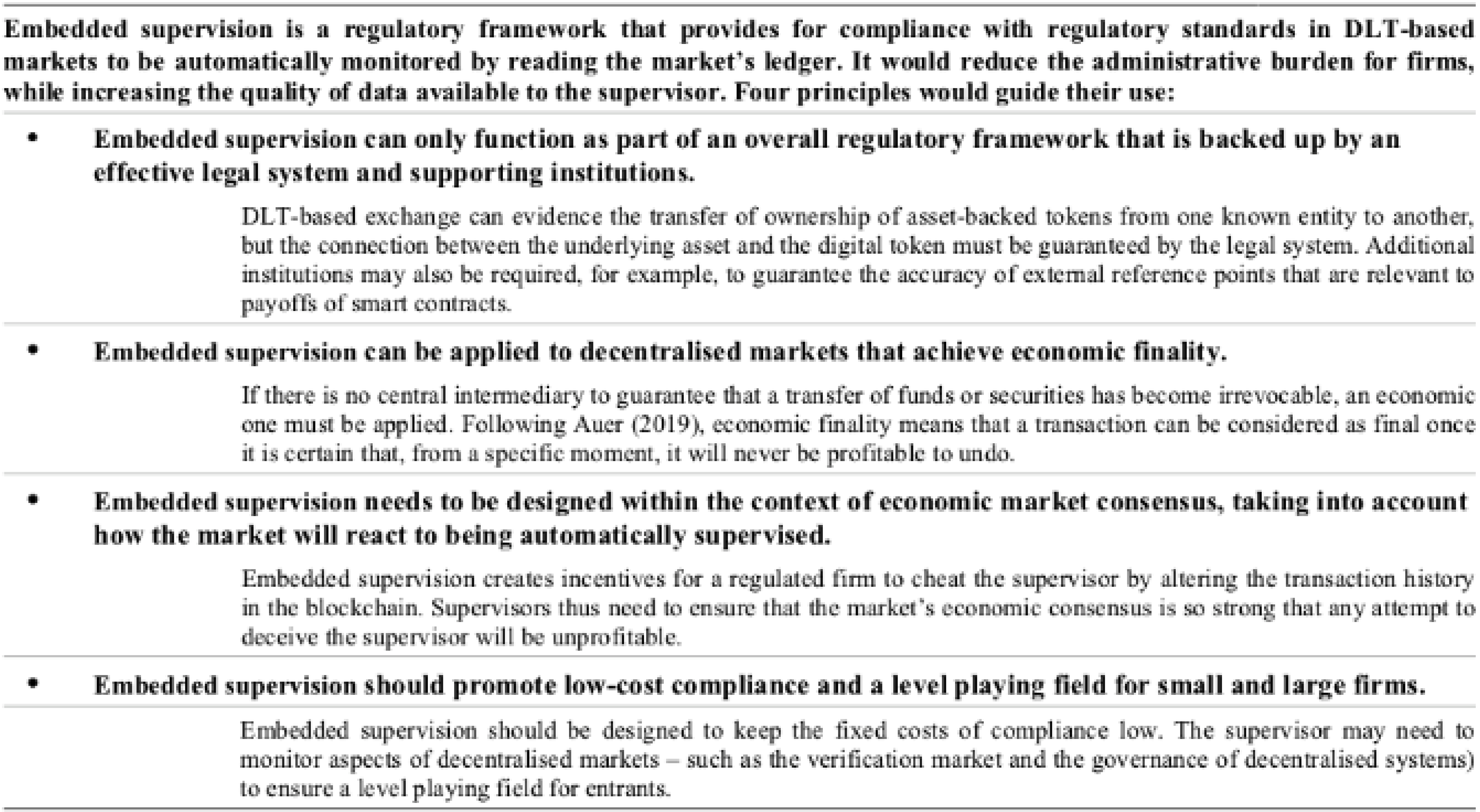
regulatory framework that provides for compliance in decentralized markets to be automatically monitored by reading the market’s ledger. This reduces the need for firms to actively collect, verify and deliver data

so that supervisors can trust the distributed ledger’s data

Active Supervision

Passive Supervision

Embedded supervision could further help maintain the confidentiality of firms and their customers, since cryptographic tools can be used to report an institution’s aggregated financial exposures to the supervisor without disclosing the underlying individual transactions.



Embedded supervision is a regulatory framework that provides for compliance with regulatory standards in DLT-based markets to be automatically monitored by reading the market's ledger. It would reduce the administrative burden for firms, while increasing the quality of data available to the supervisor. Four principles would guide their use:

- **Embedded supervision can only function as part of an overall regulatory framework that is backed up by an effective legal system and supporting institutions.**

  DLT-based exchange can evidence the transfer of ownership of asset-backed tokens from one known entity to another, but the connection between the underlying asset and the digital token must be guaranteed by the legal system. Additional institutions may also be required, for example, to guarantee the accuracy of external reference points that are relevant to payoffs of smart contracts.

- **Embedded supervision can be applied to decentralised markets that achieve economic finality.**

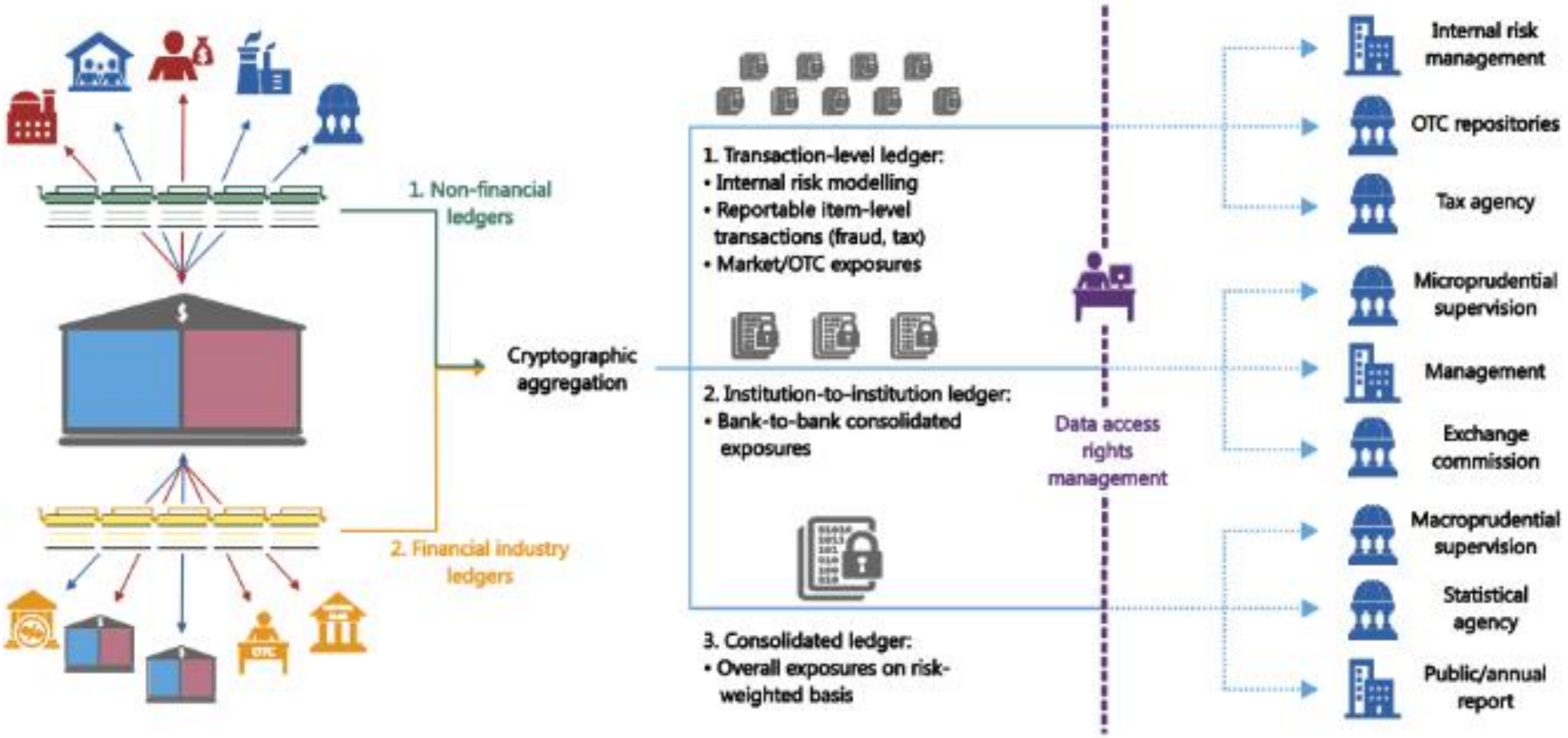
  If there is no central intermediary to guarantee that a transfer of funds or securities has become irrevocable, an economic one must be applied. Following Auer (2019), economic finality means that a transaction can be considered as final once it is certain that, from a specific moment, it will never be profitable to undo.

- **Embedded supervision needs to be designed within the context of economic market consensus, taking into account how the market will react to being automatically supervised.**

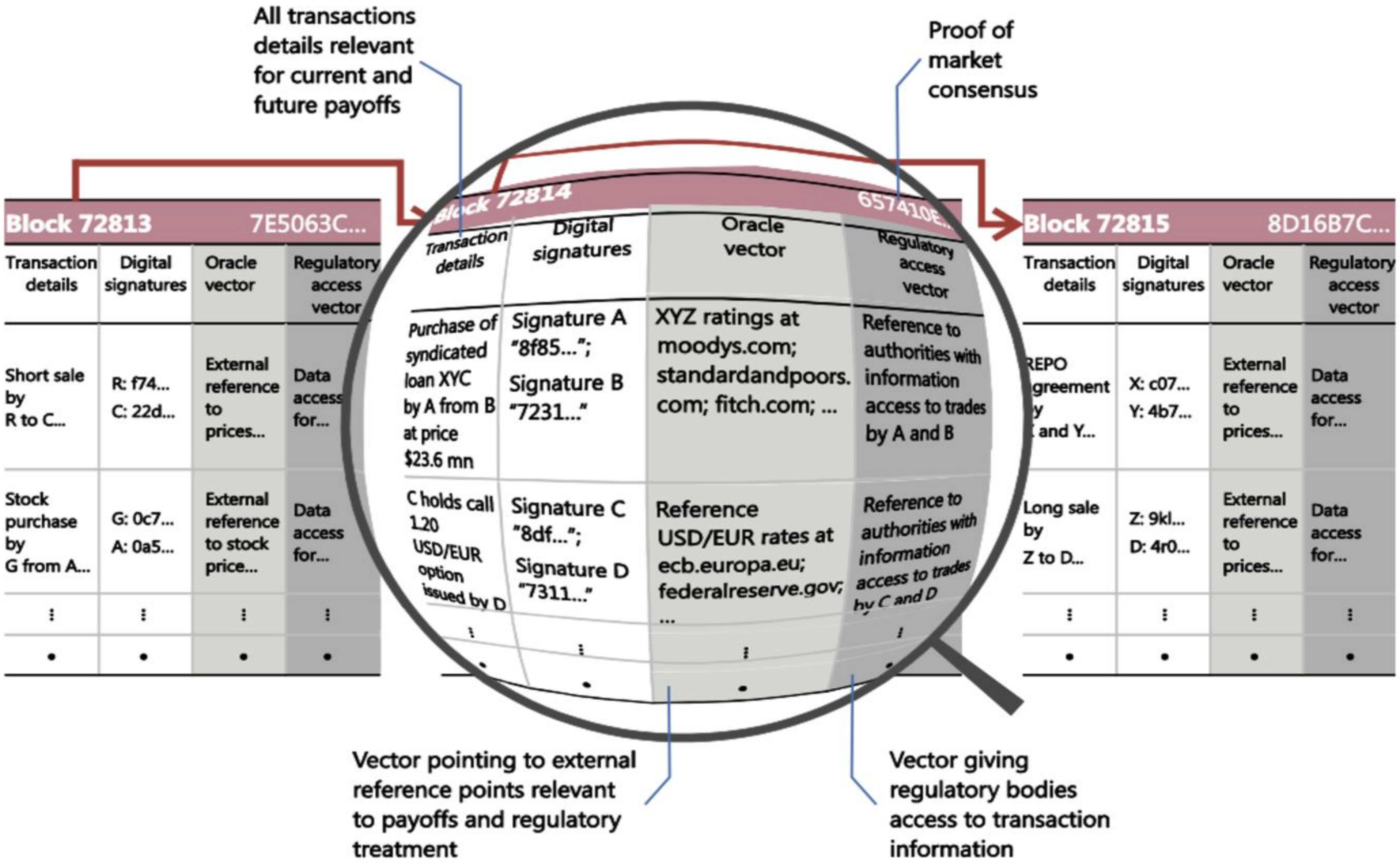
  Embedded supervision creates incentives for a regulated firm to cheat the supervisor by altering the transaction history in the blockchain. Supervisors thus need to ensure that the market's economic consensus is so strong that any attempt to deceive the supervisor will be unprofitable.

- **Embedded supervision should promote low-cost compliance and a level playing field for small and large firms.**

  Embedded supervision should be designed to keep the fixed costs of compliance low. The supervisor may need to monitor aspects of decentralised markets – such as the verification market and the governance of decentralised systems) to ensure a level playing field for entrants.


1. Non-financial ledgers
2. Financial industry ledgers
Cryptographic aggregation
1. Transaction-level ledger:
• Internal risk modelling
• Reportable item-level transactions (fraud, tax)
• Market/OTC exposures
2. Institution-to-institution ledger:
• Bank-to-bank consolidated exposures
3. Consolidated ledger:
• Overall exposures on risk-weighted basis
Data access rights management
OTC
Internal risk management
OTC repositories
Tax agency
Microprudential supervision
Management
Exchange commission
Macroprudential supervision
Statistical agency
Public/annual report

Embedded supervision can verify compliance with regulations by reading the distributed ledgers in both wholesale (symbolised by the green blockchain) and retail banking markets (symbolised by the yellow blockchain). Supervisors could access all transaction-level data. Alternatively, the use of smart contracts, Merkle trees, homomorphic encryption and other cryptographic tools might give supervisors verifiable access just to selected parts of such micro data, or relevant consolidated positions such as to institution-to-institution or sectoral exposures. Firms would only need to define the relevant access rights, obviating the need for them to collect, compile and deliver data.



All transactions details relevant for current and future payoffs

Proof of market consensus

Block 72813			7E5063C...
Transaction details	Digital signatures	Oracle vector	Regulatory access vector
Short sale by R to C...	R: f74... C: 22d...	External reference to prices...	Data access for...
Stock purchase by G from A...	G: 0c7... A: 0a5...	External reference to stock price...	Data access for...
⋮	⋮	⋮	⋮
•	•	•	•

Block 72814			657410E...
Transaction details	Digital signatures	Oracle vector	Regulatory access vector
Purchase of syndicated loan XYC by A from B at price $23.6 mn	Signature A "8f85..."; Signature B "7231..."	XYZ ratings at moodys.com; standardandpoors.com; fitch.com; ...	Reference to authorities with information access to trades by A and B
C holds call 1.20 USD/EUR option issued by D	Signature C "8df..."; Signature D "7311..."	Reference USD/EUR rates at ecb.europa.eu; federalreserve.gov; ...	Reference to authorities with information access to trades by C and D
⋮	⋮	⋮	⋮
•	•	•	•

Block 72815			8D16B7C...
Transaction details	Digital signatures	Oracle vector	Regulatory access vector
REPO greement y and Y...	X: c07... Y: 4b7...	External reference to prices...	Data access for...
Long sale by Z to D...	Z: 9kl... D: 4r0...	External reference to prices...	Data access for...
⋮	⋮	⋮	⋮
•	•	•	•

Vector pointing to external reference points relevant to payoffs and regulatory treatment

Vector giving regulatory bodies access to transaction information

The blockchain records the history of transactions and contractual obligations, as well as links to relevant external information sources (oracles) and a vector giving regulatory bodies access to the information. Market participants transact on the blockchain, which records their transactions and obligations in the form of smart contracts. Payoffs of structured financial products, etc may depend on oracles, which are external reference points such as official interest rates, exchange rates, or market rates elsewhere. Supervisors in various jurisdictions have access to the (non-public) information in the ledger, can apply their regulatory model and may also specify circuit-breaker rules for the resultant payoffs.

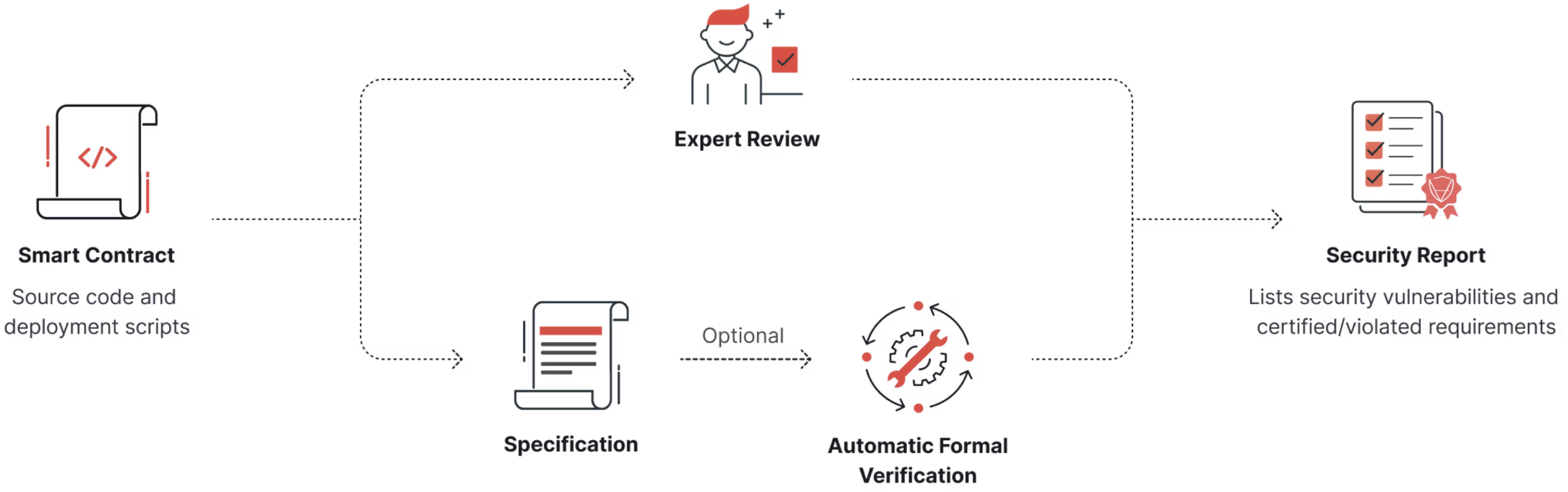
RegTech 2.0

Regtech solutions can automate compliance processes, reduce compliance costs, and enhance regulatory reporting, monitoring, and analysis

Some examples of RegTech applications include AML and KYC verification, risk management software, cybersecurity tools, end-to-end transaction monitoring, and regulatory reporting systems.

Blockchain technology as a game changer is leading to a new breed of RegTech 2.0. Addressing interoperable smart contracts will automate regulatory reporting, and make it more transparent, improving consistency, efficiency, and data quality

Crypto and DeFi Infrastrcture-Core Cyber Security



Smart Contract

Source code and deployment scripts

Expert Review

Specification

Optional

Automatic Formal Verification

Security Report

Lists security vulnerabilities and certified/violated requirements

Blockchain Infra Security

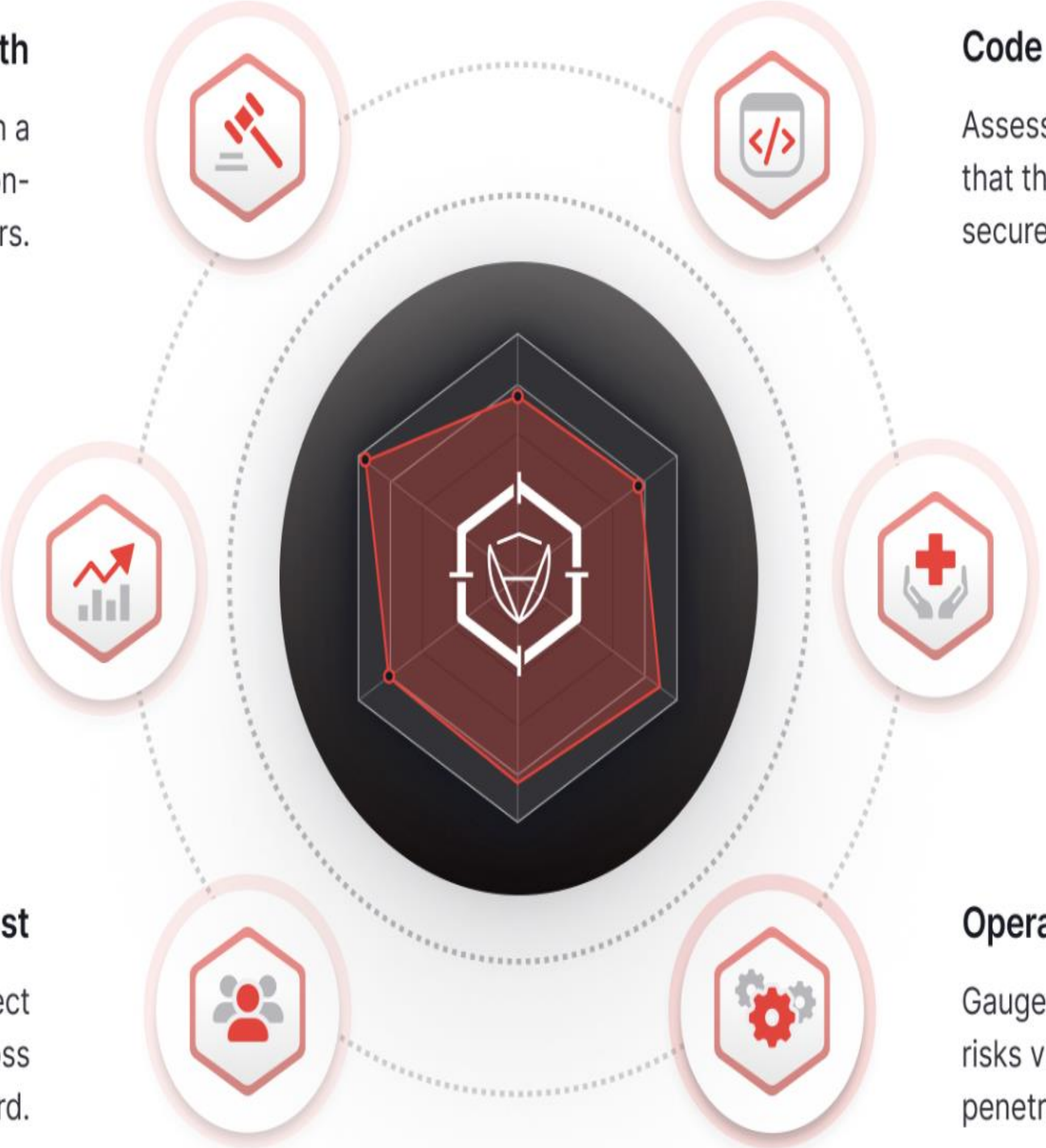
Secure smart contract development and auditing (Smart Contract PenTest)

Web3 and DeFi projects Evaluation

Digital assets Secure Transfer and management

Policy Engine, which secures transactions against internal collusion, human error, and external attacks.

Wallet Secure Key management (MPC + Multi Signature) leveraging MPC, Secure Enclave or HSM for key management



Governance Strength

Measures a project's ability to operate in a decentralized manner in terms of decision-making and distribution of token holders.

Code Security

Assesses the steps taken by teams to guarantee that the project's code and development are secure and reviewed.

Market Stability

Considers a project's ability to maintain a stable and predictable value over time without significant volatility fluctuations.

Fundamental Health

Measures team and project transparency, structure, quality of documentation, and related indicators.

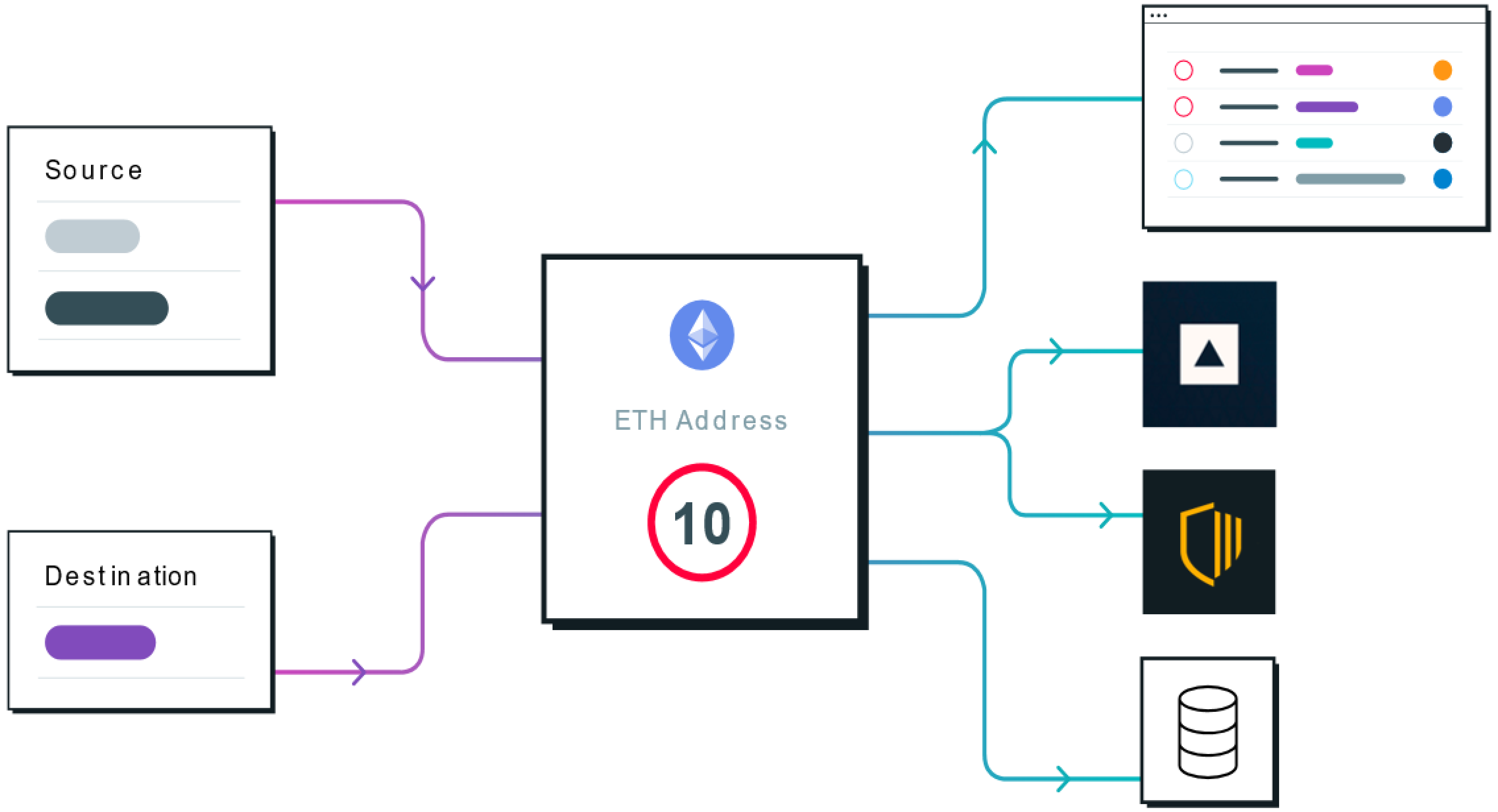
Community Trust

Measures the social engagement of the project by evaluating its overall social health across platforms like Twitter, Telegram, and Discord.

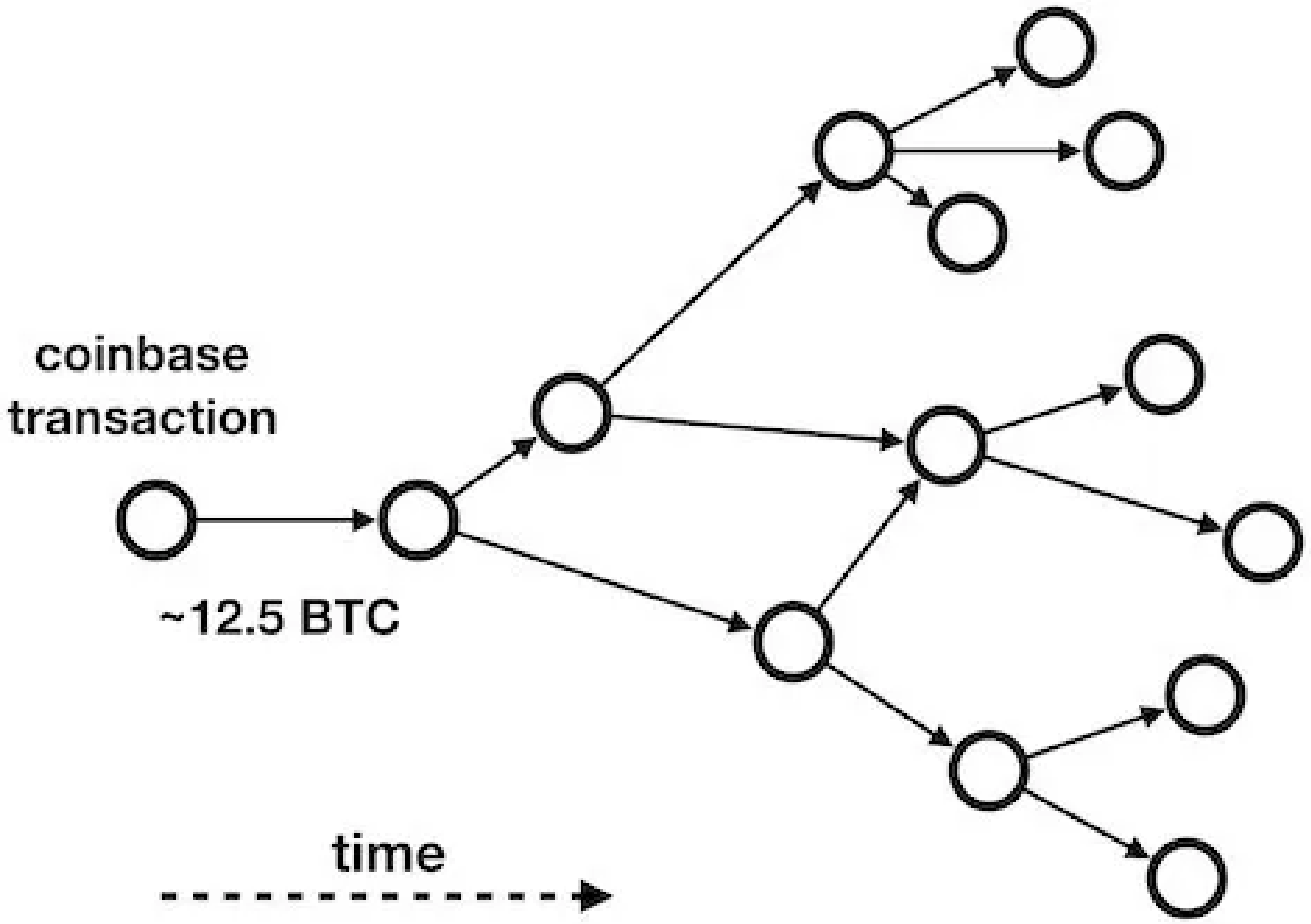
Operational Resilience

Gauges a project's ability to handle operational risks via security measures like bug bounties and penetration tests.

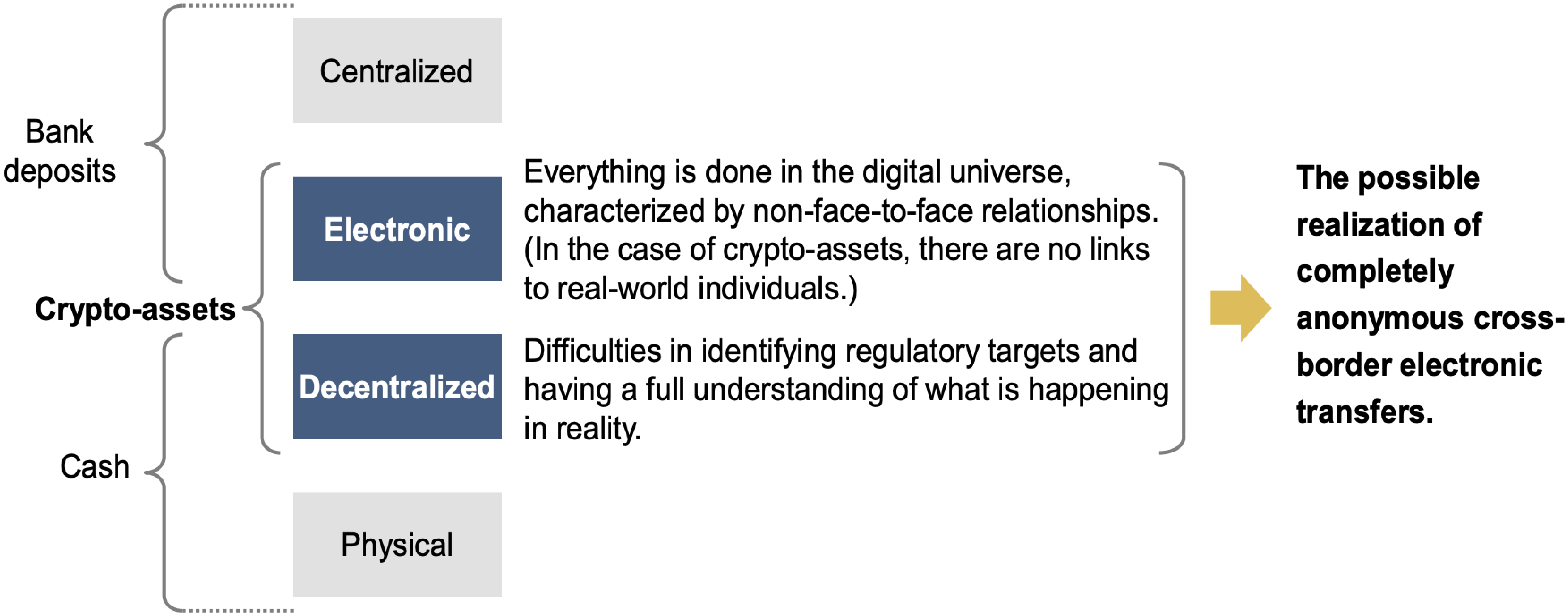
AML, Fraud, KYT and DID KYC



This is different to conventional crypto anti-money laundering (AML) solutions, which rely on tracing funds from known illicit wallets, or pattern-matching with known money laundering practices uncover unlawful activity and money laundering patterns by taking advantage of blockchain's pseudonymity and combining it with knowledge about the presence of licit (e.g., exchange, wallet provider, miner, etc.) and illicit services (e.g., darknet market, malware, terrorist organizations, Ponzi scheme, etc.) on the network.



Characteristics of crypto-assets compared to fiat currencies



Bank deposits

Crypto-assets

Cash

Centralized

Electronic

Decentralized

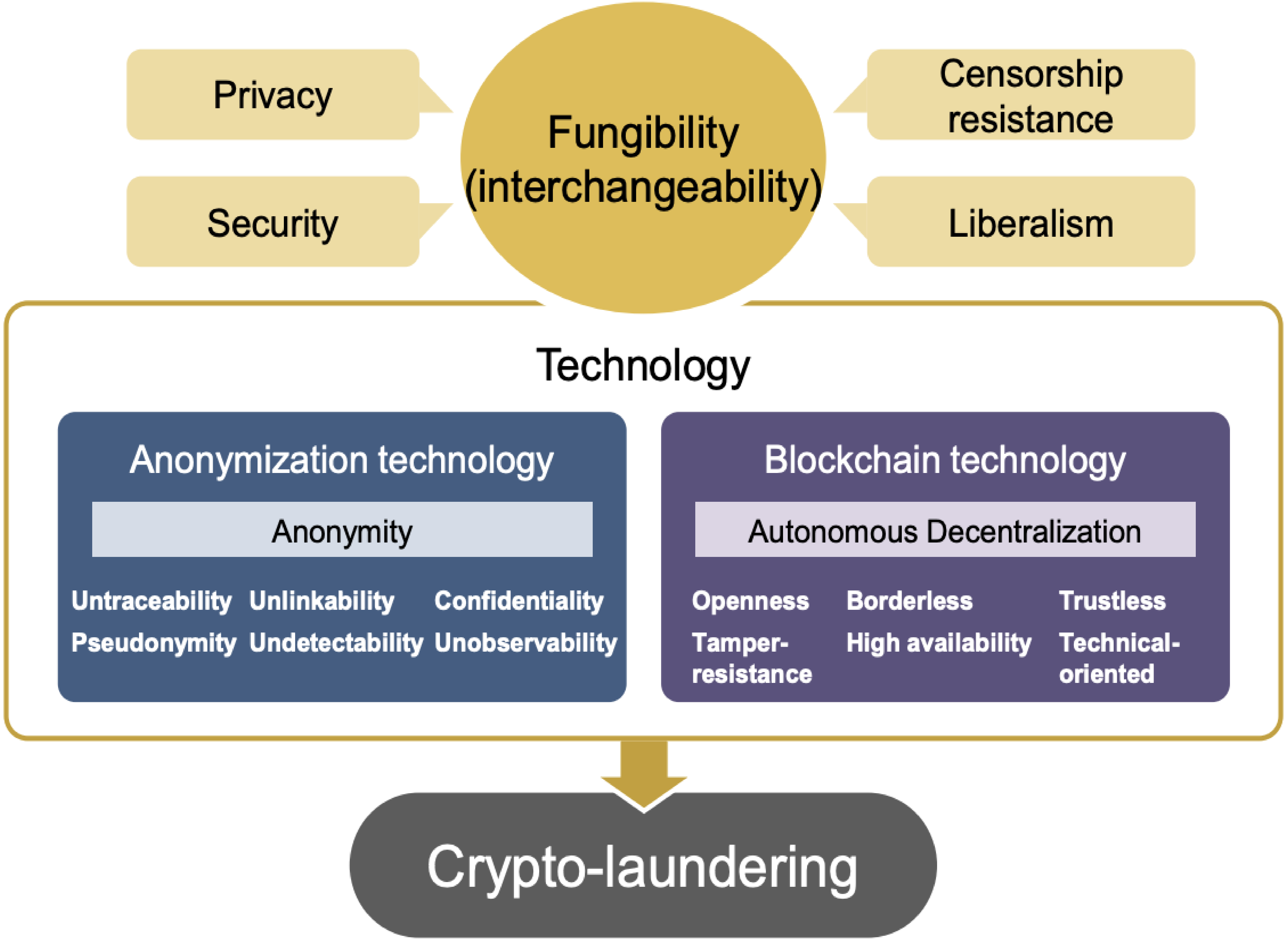
Physical

Everything is done in the digital universe, characterized by non-face-to-face relationships. (In the case of crypto-assets, there are no links to real-world individuals.)

Difficulties in identifying regulatory targets and having a full understanding of what is happening in reality.

The possible realization of completely anonymous cross-border electronic transfers.

Relationship between fungibility of crypto-assets and crypto-laundering

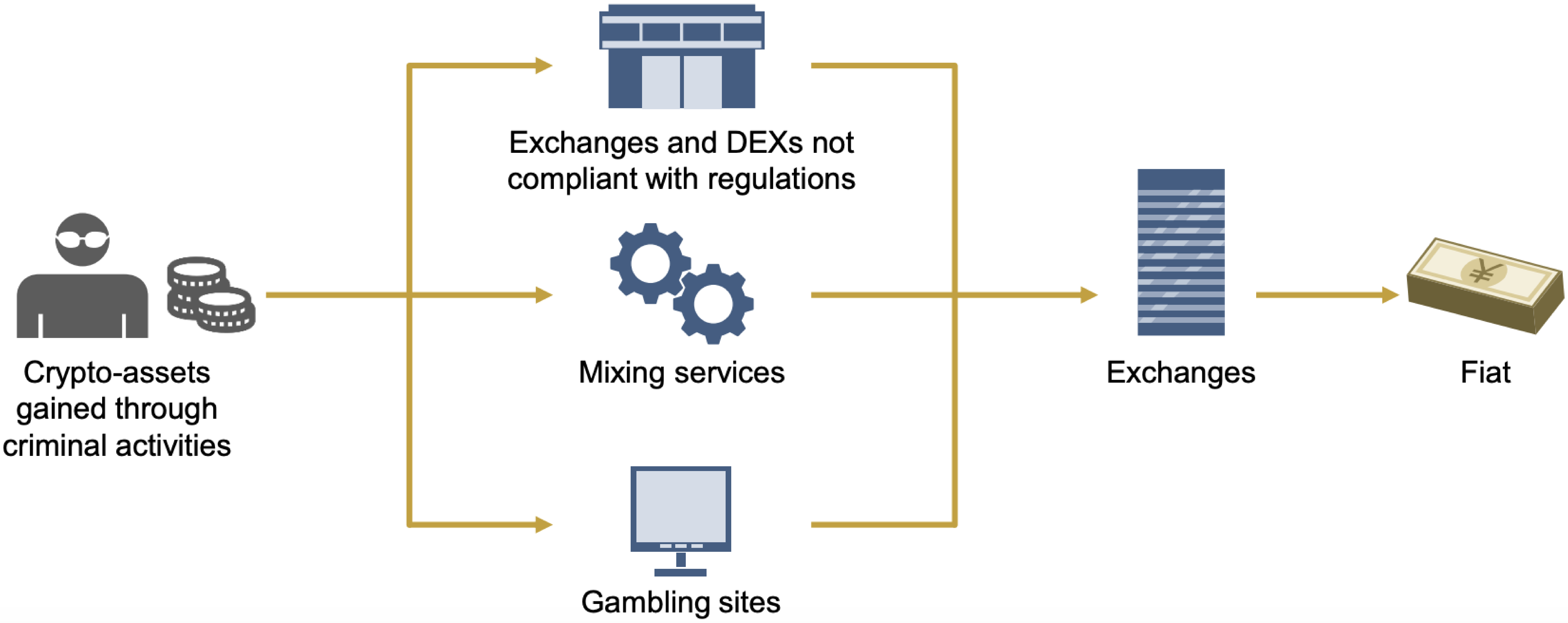


Fungibility is an important asset as a currency, and there is a lot of effort being put into ensure that it exists in crypto-assets.

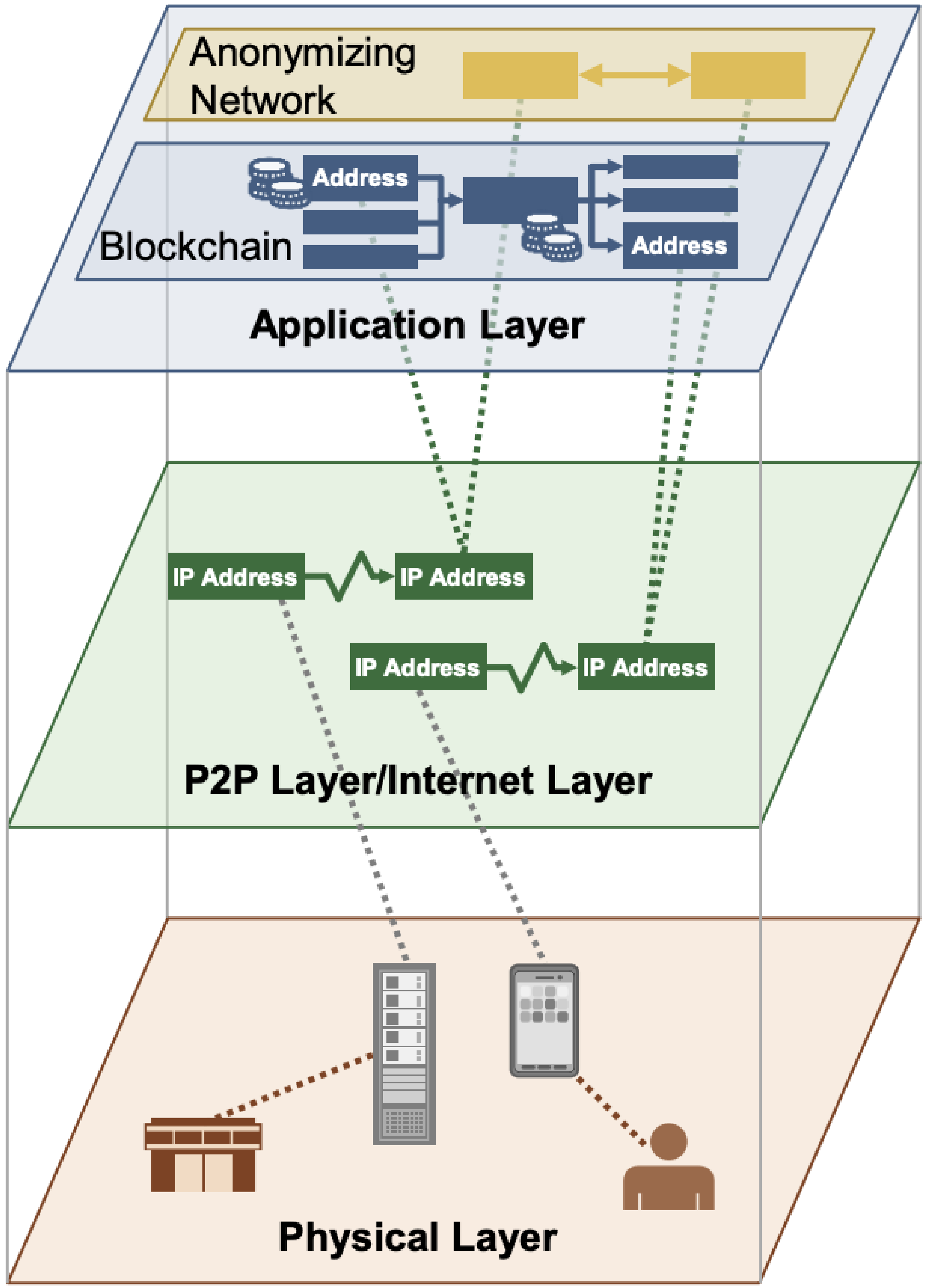
Since transfer routes could be made irrelevant by making transactions private, fungibility is being discussed within the crypto-asset technology community which in turn relates to other ideas such as privacy and security, as well as liberalism and censorship resistance.

On the other hand, there is a risk that a combination of anonymization technology and blockchain technology which will bring about fungibility could be used for crypto-crime and crypto-laundering.

Illustration representing the flow of crypto-laundering


Crypto-assets gained through criminal activities
Exchanges and DEXs not compliant with regulations
Mixing services
Gambling sites
Exchanges
Fiat

Overview of technologies
classified anonymization/de-anonymization technologies into three layers: the “Application Layer”, “P2P Layer/Internet Layer”, and “Physical Layer”.



Application Layer

Application Addresses* exist.
(e.g. Bitcoin address, Dark web address)

P2P Layer/Internet Layer

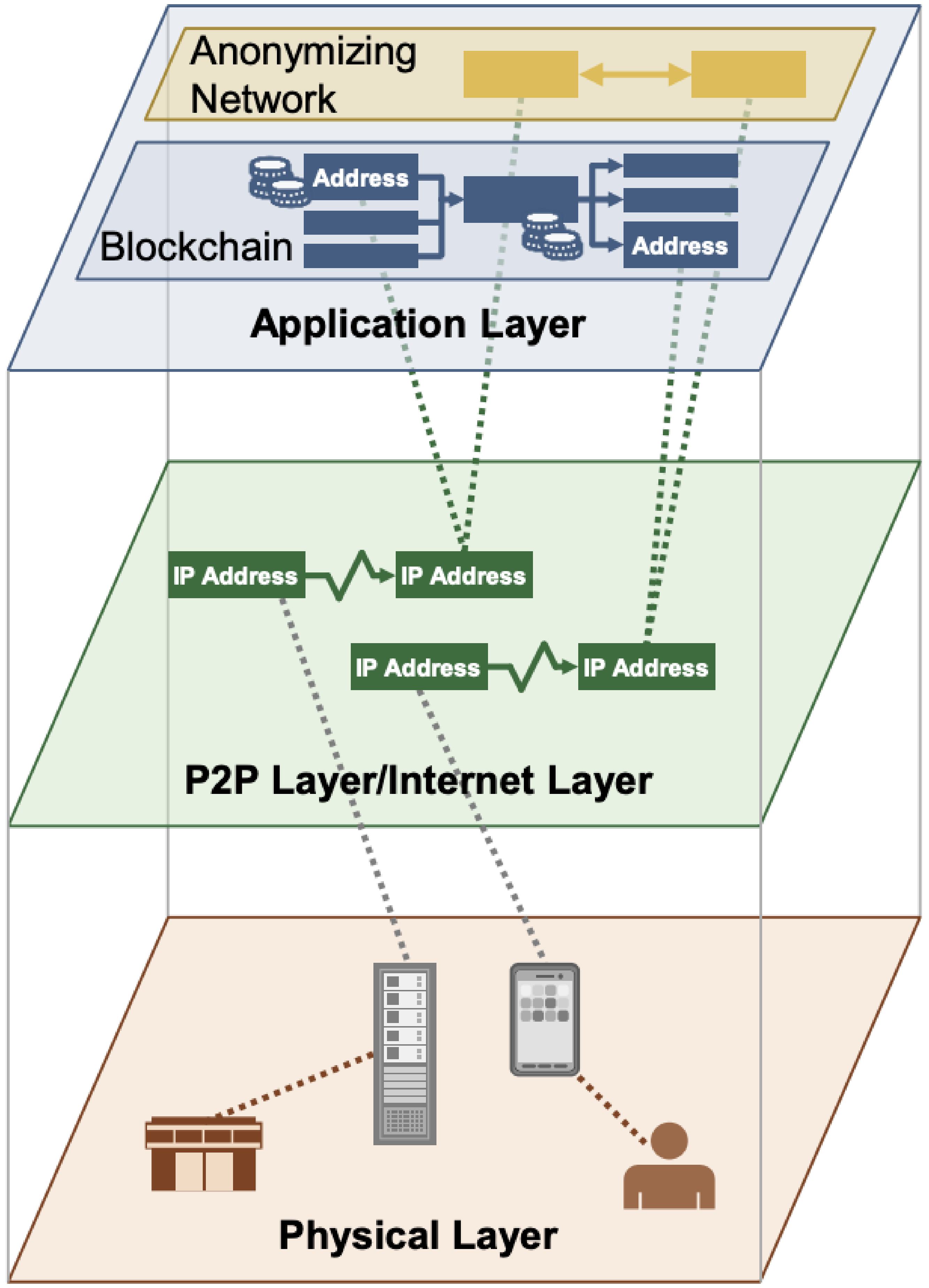
IP Addresses exist.

Physical Layer

Physical entities such as devices and users exist.

* “Address” is an identifier relating to a user’s location on a network or an application. (e.g., e-mail address)

Anonymization technologies are available for each layer, and it is not particularly difficult technologically or mentally to use them.



Application Layer

Blockchain -- Mixing services, anonymous altcoins etc.
Anonymizing Networks -- Tor hidden services,
secure chat tools etc.

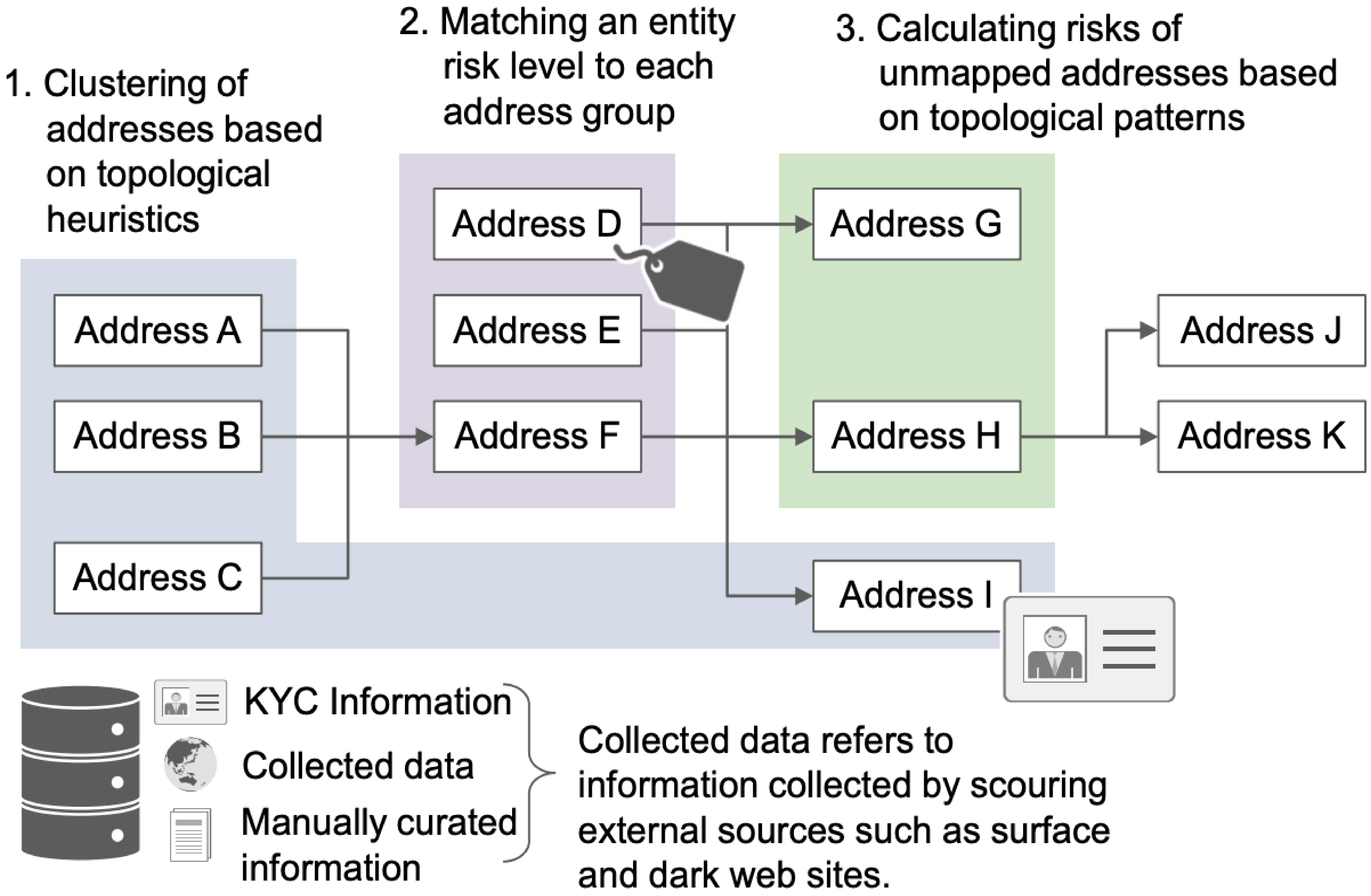
P2P Layer/Internet Layer

Tor onion-routing, I2P, Freenet etc.

Physical Layer

Free Wifi, secondhand devices, prepaid SIM,
Bitcoin ATM etc.

Illustration of blockchain data de-anonymization


1. Clustering of addresses based on topological heuristics
2. Matching an entity risk level to each address group
3. Calculating risks of unmapped addresses based on topological patterns
Address A
Address B
Address C
Address D
Address E
Address F
Address G
Address H
Address I
Address J
Address K
KYC Information
Collected data
Manually curated information

Collected data refers to information collected by scouring external sources such as surface and dark web sites.

1. Cluster addresses into multiple groups based on topological heuristics.
2. Match an entity risk level to each address group. Address-entity associations are collected from external sources such as the dark web and each entity is assigned a risk level based on its category (exchanges, mixers etc.).
3. Calculate risk levels of unmapped addresses based on topological patterns between mapped and unmapped addresses.

However, there is no consensus on the validity of the heuristics used in the first clustering process.

Track & Monitor crypto transactions KYT

Blockchain DLT Data Insight , Data Intelligence and analyzing

Real-Time On-Chain Transaction and digital assets Monitoring

Real-time updates to sanctions lists, exploits, hacks, and security incident
Transaction Risk Scoring

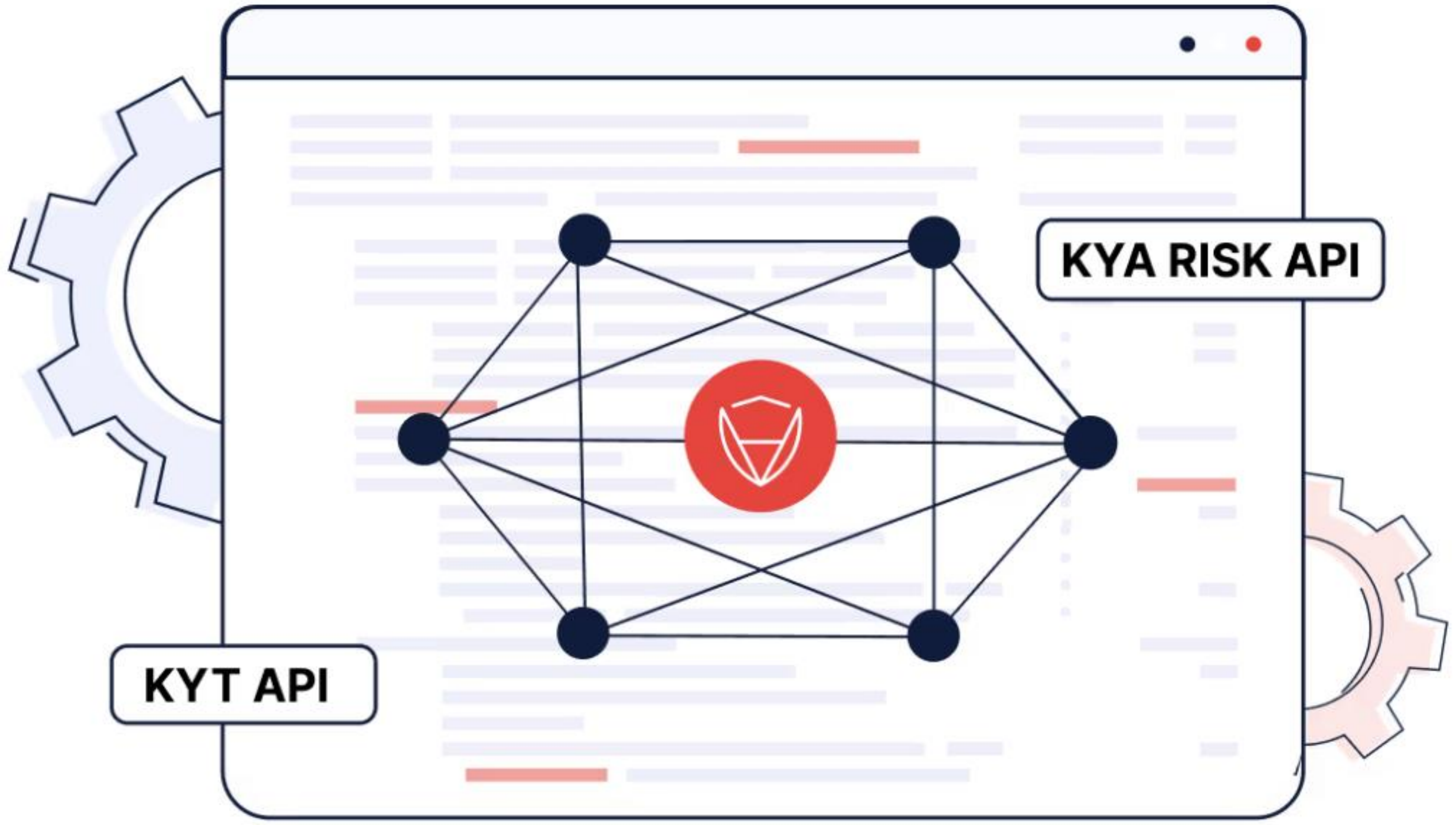
Wallet and Address Screening

Multi-chain and cross-chain risk evaluations and scores.

Comprehensive risk analysis, both on-chain and off-chain.

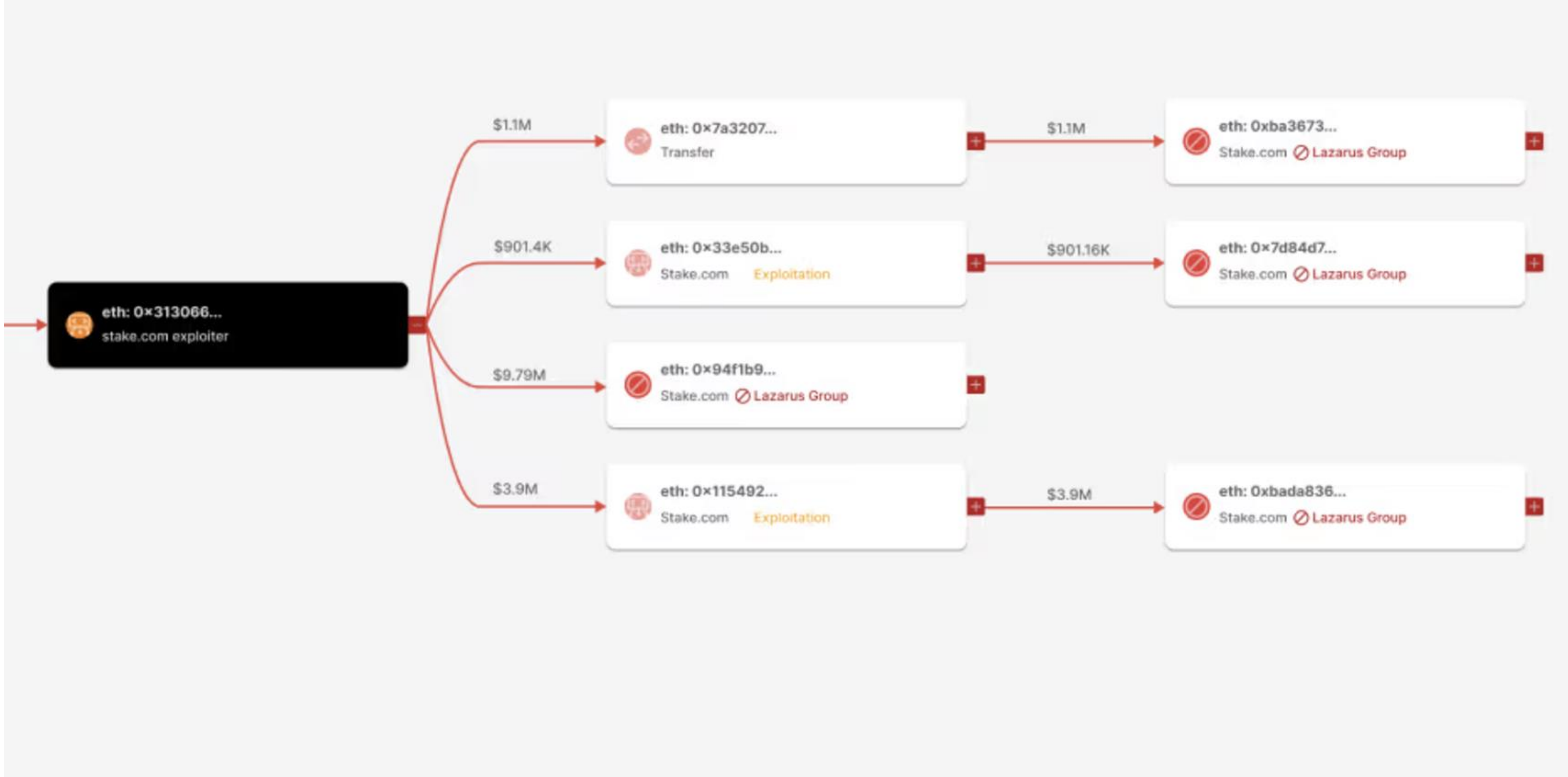
Detailed tracing of cryptocurrency transactions across chains, including bridges and mixers.

Data exports to enhance reports for compliance and investigation teams.



AI + ML

Transaction Graph and Flow Analyzer



Decentralized Identification (DID) KYC

The Problem with Traditional KYC:

Compromising User Privacy

Inefficiencies in Centralized Data Storage

Heightened Risks and Non-Compliance

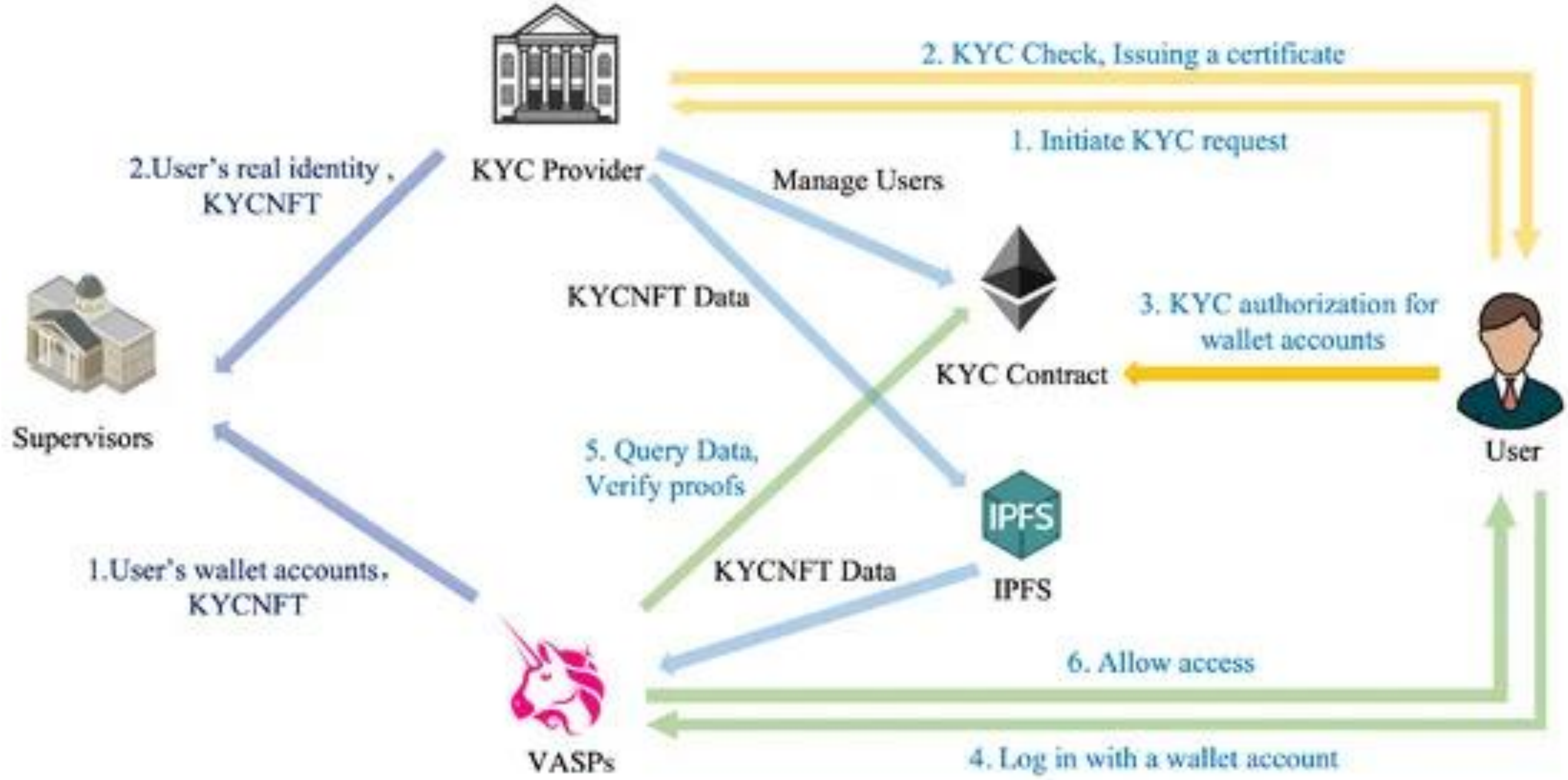
Centralized KYC processes are prone to cyberattacks

ZKP-Based Solution

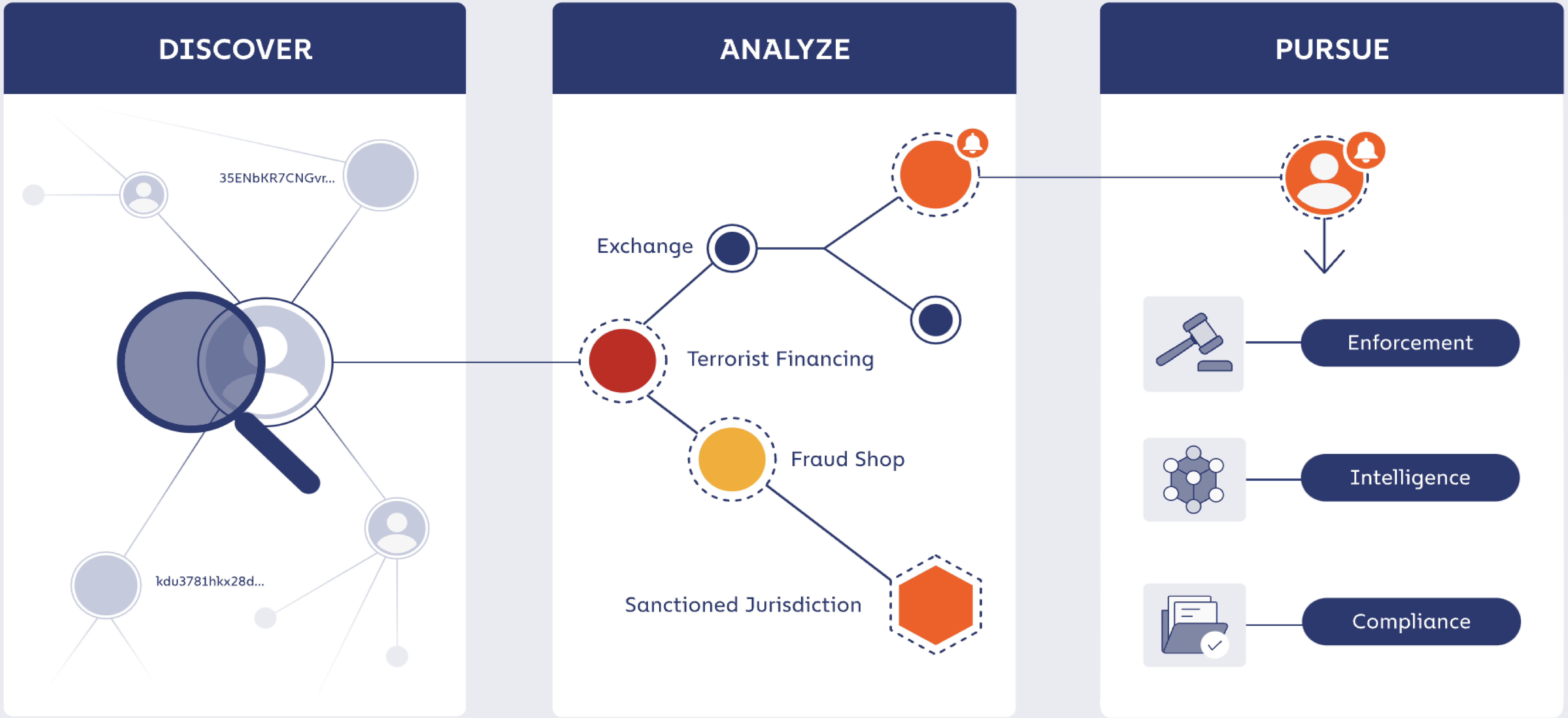
Zero-Knowledge Proof (ZKP) technology
ZKPs allow one party to prove to another that they possess certain information without revealing the information itself. For instance, in the context of KYC, This method ensures regulatory compliance while preserving user privacy

Decentralized Identity (DID)

A Web standard that identifies participants in the Self-Sovereign Identity (SSI) ecosystem. DIDs can be stored in a decentralized identity wallet.


2. KYC Check, Issuing a certificate
1. Initiate KYC request
2.User's real identity ,
KYCNFT
KYC Provider
Manage Users
KYCNFT Data
3. KYC authorization for
wallet accounts
KYC Contract
Supervisors
User
5. Query Data,
Verify proofs
IPFS
IPFS
1.User's wallet accounts,
KYCNFT
KYCNFT Data
6. Allow access
VASPs
4. Log in with a wallet account

Crypto Investigations



Crypto Investigation and Forensics
Crypto Crimes Investigation

Financial fraud detection

Identifying local and international fraud schemes

AI + ML

Monitoring illicit crypto activities

Safeguarding customer assets from crypto-related threats

THANKS!