MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Confusion Capital, Inc., Digital Securities Initiative, Ketsal, and Arktouros PLLC

On June 12, 2025, Crypto Task Force Staff met with representatives from Confusion Capital, Inc., Digital Securities Initiative, Ketsal, and Arktouros PLLC.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Confusion Capital, Inc., Digital Securities Initiative, Ketsal, and Arktouros PLLC representatives provided the attached document, which was discussed during the meeting.

The Digital Securities Initiative

SEC Crypto Task Force <> Digital Securities Initiative (DSI) Meeting Request
Dates: Week of June 9th, 2025
Topic: Tokenization of Securities

Agenda:

- Discussion of a proposed framework that DSI is developing to facilitate and support the secondary trading of tokenized securities in decentralized finance (DeFi).

Attendees:

- Nevin Freeman, President, Confusion Capital
- Michael Cameron, Chief of Staff, Confusion Capital
- William “Billy” Sanders, Research and Development Fellow, DSI
- Andrew Worth, Research and Development Fellow, DSI

The Digital Securities Initiative

May 15, 2025

Commissioner Hester M. Peirce
Chair, SEC Crypto Task Force
U.S. Securities and Exchange Commission
100 F Street NE
Washington, D.C. 20549

Re: Request for Meeting with SEC Crypto Task Force

Dear Commissioner Peirce and Members of the Crypto Task Force,

As the Commission explores avenues for the permissible tokenization of securities, it is important to preserve what makes DeFi great - the interoperability of assets and financial services, and the permissionless, open access for broad populations. While avoiding the many pitfalls will be challenging, it is possible to implement customer identification and market integrity controls without sacrificing what makes DeFi great.

Introduction

Herein, we present a conceptual proof of concept for how to get the best of both worlds. By making use of **(a) ZK proofs**, and **(b) clear technical standards for onchain compliance infrastructure**, we can give regulators the information and powers they require while still giving users and developers the simplicity, accessibility, and privacy necessary to enable **safe, thriving onchain capital markets**.

This system would be implemented and operated in a decentralized way by hundreds or thousands of companies, similar to how the blockchain ecosystem operates today, rather than picking any particular company or agency to sit at the center of the system as was the case with the creation of the DTC.

We are working to identify the precise laws and regulations that would need to change for decentralized compliance to be possible. We think an initial trial of such a system would be best approached through limited exemptive relief, and if proven effective, would concretely show the way for rulemaking and policy change.

We are not trying to clear a legal path for one specific company to build one specific product, since that's not how decentralized compliance would work. Rather, we are proposing a change to the division of responsibilities and the core types of regulated entities which would still leave it up to

the industry to technologically innovate and commercially compete to provide the best services, with a clear path to compliance.

The Banking and Securities Industry Committee thought deeply about how to structure digital clearing and settlement of securities in order to facilitate the transition from paper to digital in the 1970s, giving birth to the Depository Trust Company with its clever governance structure and special place in the industry.

We are aiming to do something similar, proposing an overall way things could work that would achieve regulator and industry objectives, but in a decentralized way.

The proposed system would enable the trading of tokenized securities within regulated zones built on top of a permissionless smart contract blockchains. It wouldn't require the creation of a permissioned chain or limiting node participation to a select group of participants, but could instead be built on popular blockchains like Ethereum or Solana.

The approach contains the following pieces:

- A method for identifying onchain users in a privacy preserving manner
- Onchain mechanisms for evaluating risk and compliance with various regulations
- Dynamic transaction filtering based on risk by users and smart contracts

Who are we?

The Digital Securities Initiative (DSI) is an open industry collaboration – essentially a think tank.

The work presented below was funded and carried out by Confusion Capital, Inc., the company that instigated DSI, and reviewed by several others in the industry. If a decentralized compliance approach like the following were to be adopted, Confusion Capital would stand to benefit from overall growth in the tokenized securities market, since it is closely affiliated with a DeFi project which aims to incorporate tokenized securities. Confusion Capital does not have or currently intend to build or invest in any product line that would be present in this system other than onchain DeFi applications.

Furthermore, I, Nevin Freeman, President of Confusion Capital and founder of DSI, have become convinced that onchain capital markets could be really awesome for the world if done right and really annoying and problematic if done wrong, so my entrepreneurial itch to make sure we "get it right" is a big driver behind this work.

Proposed Architecture for Decentralized Compliance

User Identification

Users start by going through a Customer Identification Program (CIP), but only need to do so once.

A user submits their government-issued ID to what we call an **Identity Keeper**, a private company operating a regulated role in the system, who stores it privately. The Identity Keeper issues the user a cryptographically signed verifiable credential which indicates that the Identity Keeper has verified the identity of the user and that they have stored the user's PII. The user keeps this credential to themselves in their wallet application, where they retain control of it: they back it up or port it to a new wallet. Should they lose the credential, the user can retrieve it from the Identity Keeper again.

The Identity Keeper checks for initial risks such as identity theft, if the user is on an applicable sanctions list, and other identity-based financial crimes. The Identity Keeper maintains a public record of encrypted information that reveals nothing about any of its customers, but can be used by customers at will to prove whether or not they are associated with various types of risk using a zero-knowledge ("ZK") proof.

Identity Keepers implement an open sibyl resistance system that prevents users from registering many identities. If a user's Identity Keeper goes out of business or loses its authority to perform the role in the system, the user can onboard with another one.

Centralized exchanges that already hold identity info for many crypto users would be natural entities to become Identity Keepers. The service providers that provide ID-checking services to financial companies may also choose to provide their services directly to users, although they would likely be taking on a more regulated role than they are used to. Users may pay for this service, or may receive it for free from companies and platforms who have an interest in onboarding them to their platform.

Transaction Filtering

When a user transacts with a regulated asset onchain, their wallet application submits a ZK proof as part of each transaction, which can be used to establish certain facts about the account that submitted the transaction.

Regulated tokens and DeFi applications have logic in their code that implements **Transaction Filtering** by checking that certain conditions are true before allowing the transaction to go through. For instance, they could check that the user has a certified digital identity held by a legitimate Identity Keeper, and that the user is not on any applicable sanctions lists or a citizen of a broadly sanctioned country.

Because of the nature of ZK proofs, these checks would not reveal any other information about the user or their identity. The Identity Keeper is still the only party with access to the user's identity.

In addition, users can configure their wallet to filter transactions, automatically restricting the use to low risk and regulated DeFi applications. Not only does this allow the user to be compliant, it protects them from scams and predatory applications.

DeFi Application Controls

Transaction filters would apply to DeFi applications as well as users; a regulated token would not allow transfers to a DeFi application's address unless the transaction contains a proof that the application itself implements appropriate transaction filters. This would be necessary so that the tokenized positions that DeFi applications so frequently generate, which give rise to the composability and convenience of DeFi, would not become backdoors to allow unmonitored, unidentifiable transactions of underlying regulated tokens.

For example, imagine someone deposits a regulated token into a simple wrapper app that gives them a new token which anyone can redeem for the regulated token. This would strip the controls and defeat the purpose.

Our solution prevents this by using a standardized definition of adequate controls for each relevant context, and DeFi developers must be able to receive an onchain certification or self-certify that their application is in compliance. We touch on standards more below.

Transaction Monitoring

In addition to Identity Keepers, we propose another role in the system: **Transaction Monitors**. While in the traditional system, financial institutions of all types are expected to hold customer identity information and monitor transactions for suspicious activity, in this new environment, the roles need not be played by the same party. We believe it would be best if they were separated by design, which we'll address below.

Each regulated token and DeFi application must hire a Transaction Monitor to monitor its transactions. When a Transaction Monitor accepts this role, they agree to monitor all relevant transactions, and evaluate the user behavior. They keep records of user behavior, and publish a subset of their records, though again, everything they publish is encrypted and does not reveal anything about users to the public.

For example, a Transaction Monitor may watch for signs of market manipulation, and if it detects a series of strong signs, will update the public encrypted record for the relevant user. This may impact that user's ability to transact on the relevant DeFi application, which can have as part of its transaction filter that users must not have a score above a certain threshold for signs of market manipulation.

This tracking and filtering is on the level of users, not individual blockchain addresses. When a user transacts with a regulated asset onchain, their wallet application also submits a unique pseudonym in connection with the transaction, encrypted for only the applicable Transaction Monitors to see. Thus, Transaction Monitors can tell that a series of transactions were all conducted by the same user even if the user uses many blockchain addresses. The public, however, cannot see this.

The Transaction Monitor does not know each user's real identity, only their unique pseudonym. However, in addition to their pseudonym, the user's wallet must always disclose who their Identity Keeper is to the Transaction Monitor. Thus, if a user commits a crime, the Transaction Monitor can report the transactions to law enforcement along with their pseudonym and Identity Keeper, and lay enforcement can, through due process, discover their identity from the Identity Keeper.

A user uses the same digital identity across blockchains, so their transactions can ultimately be connected by law enforcement even if they hop from one chain to another.

Risk Scoring

A central concept in the way Transaction Monitoring and Transaction Filtering are implemented is **Risk Scoring**. As is already ubiquitous in compliance technology today in both traditional finance and crypto, the system would effectively track risk of several different things at once, such as money laundering, market manipulation, insider trading, theft, and so on.

This same methodology can be turned in the other direction for the benefit of users: a Transaction Monitor could maintain risk scores for DeFi applications and tokens, including unregulated tokens, flagging potential scams and fraud and helping users avoid loss of funds.

Privacy

As you can see by now, this system is designed to provide information access in a very targeted way:

1. Regulated tokens and DeFi applications receive information about the user like whether they have gone through KYC, whether they are sanctioned, whether they have engaged in. market-manipulation-like transaction behavior, all via ZK proofs that only selectively reveal what is defined as necessary to enable the user to transact.
2. Law enforcement receives suspicious activity reports and criminal activity reports from Transaction Monitors, and can access user identity information from Identity Keepers.
3. Transaction Monitors do not receive user identity information, and Identity Keepers do not receive user address or transaction information.

The public receives none of this information; they merely see the same information they currently see for blockchain transactions. All additional information required for preventing access to suspected bad actors or sanctioned parties and seeking recourse for apparent criminal activity is stored and accessed by law enforcement offchain.

Because all of the information that the system needs for these regulatory functions is offchain, the need for any transaction information to be visible to the public, which is essential to present-day transaction monitoring and response to thefts, is no longer present. As a consequence, this opens the door to embracing privacy chains and privacy solutions that operate atop of existing chains.

Similar to how we value and rely on the privacy we enjoy with only our bank or broker seeing our balances and transactions rather than the whole world, there's a case to be made that if a good portion of capital markets and commercial transactions come onchain, we're going to need a lot more privacy than we have today. We believe this system would make full privacy on the blockchain layer a non-issue for regulators, and thus resolve the seemingly unresolvable tension between privacy and monitoring on blockchains.

Separation of Data-Rich Roles

In order to (a) offer users as much privacy as possible and (b) avoid a handful of companies gaining a privileged view of the entire financial system which they could end up abusing, we believe it's best to fully separate the roles of Transaction Monitor and Identity Keeper by disallowing companies from performing both functions.

Prevention and Recourse

The system is designed to address both:

1. Preventing suspected bad actors from accessing the system, even if it is not practical to prosecute each one.
2. Identifying and prosecuting suspected criminals when it is the priority of law enforcement to do so.

Clear Ontological and Technical Standards

A hidden challenge in making a system like this work is establishing clear standards. For example, if one Transaction Monitor tracks 17 illicit behavior categories they made up themselves and another one tracks 13 they made up themselves, a DeFi developer has to pick one and use custom Transaction Filter code that fits, whereas if there is a standardized set of risk categories and a standardized implementation on each chain for how to communicate about them, everyone can use it interchangeably. The same would apply to transaction efficiency – a user's wallet would have to construct a proof for many more categories if they are doing a muti-hop transaction in the case

where every token and DeFi app's Transaction Filter required different categories or different implementations of the same categories.

As an analogy, imagine a world where every computer company had their own proprietary type of plugs – that would be a lot more of a problem than a world where we all use USB.

We envision two levels of standard setting:

- **Ontological:** a system-wide set of categories and definitions that would apply on any blockchain.
- **Technical:** a blockchain-specific technical implementation of the system-wide categories.

These standards will have to strike a balance between specific enough to ensure interoperability and general enough to ensure that they are flexible and can adapt to new forms of illicit behaviours.

The ontological standardization would need to be done by some body with legitimacy early on. We're still researching precedents for standardization and noodling on how best to go about this.

The technical standards could be worked out by each blockchain's technical community through their existing process for setting standards, which has worked out well in defining standard token types and so on.

Cross-Asset and Cross-Jurisdiction Transactions

Cross-asset transactions work elegantly in this system; the user's wallet just includes all of the elements necessary to satisfy the Transaction Filter for each DeFi app and token involved in the transaction in a single ZK proof. Because of how ZK proofs work, the more that's involved, the more offchain computation is needed to construct the proof, but the amount of onchain computation to check the proof remains constant, avoiding an explosion in gas cost.

Cross-jurisdiction transactions become more complicated if we can't get regulators in different countries to agree to using the same system and ontology, but if sufficient coordination can be achieved (which there is precedent for, e.g. cross-border bank wire systems, global air traffic control, and so on), we can enable global transactability, while preserving each country's power in setting the specifics of its own rules.

Conclusion

This was a brief overview of the complex system which would empower the tokenization of securities on permissionless smart contract blockchains. DSI recognizes the importance of implementing a system of controls to ensure tokenized securities remain regulated. By creating

regulated zones within the wider DeFi ecosystem, we believe that the proposed system strikes the appropriate balance between innovation and investor protection.

We're continuing to seek input from regulators, builders and legal experts to determine the required regulatory changes to implement such a system.

We appreciate your consideration and welcome the opportunities to further discuss these matters with you.

Sincerely,

Nevin Freeman
President
Confusion Capital

Embedded Regulation on the Contract Level for Permissionless Blockchains

The Digital Securities Initiative

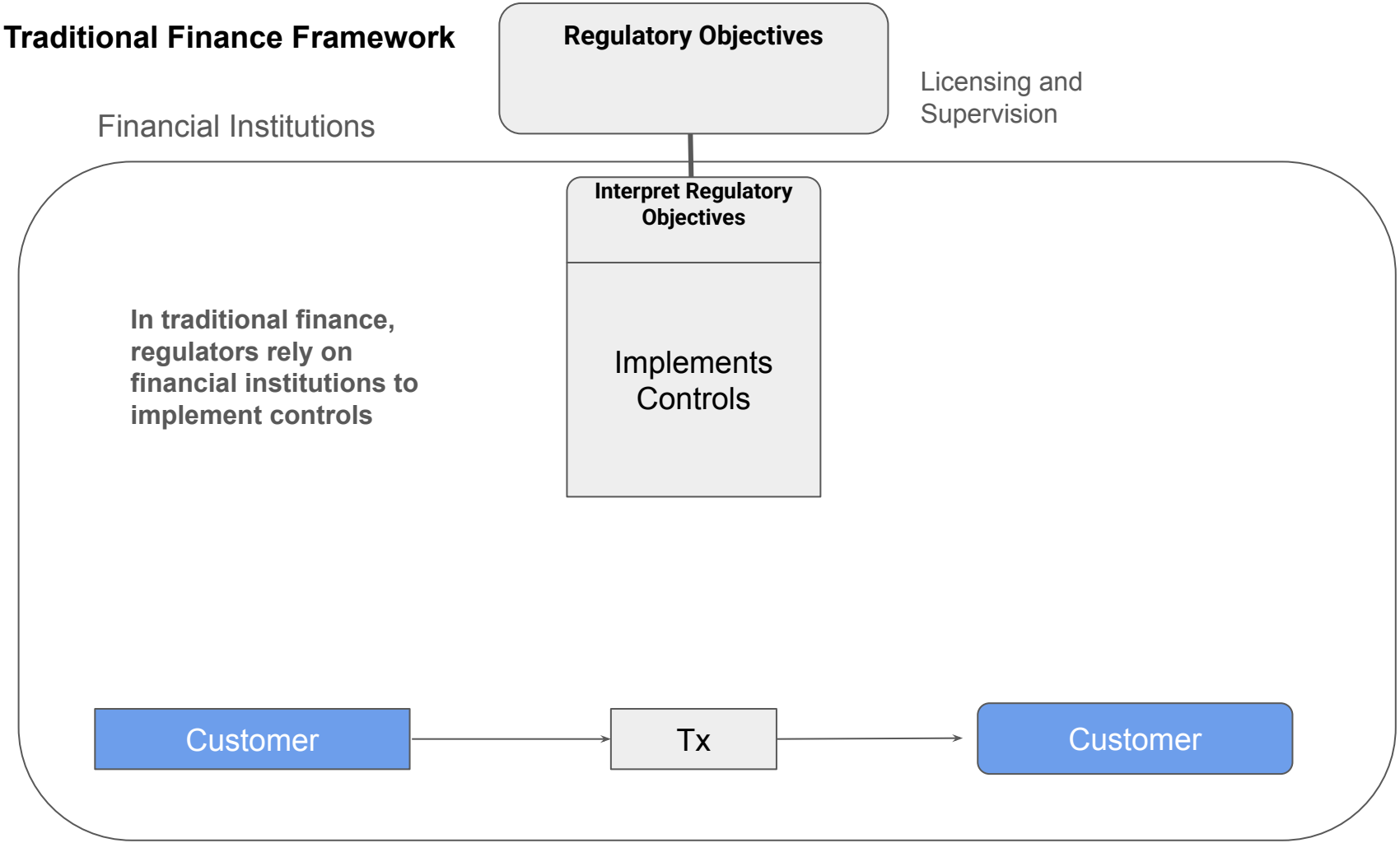
Table of Contents

The Digital Securities Initiative

Overview

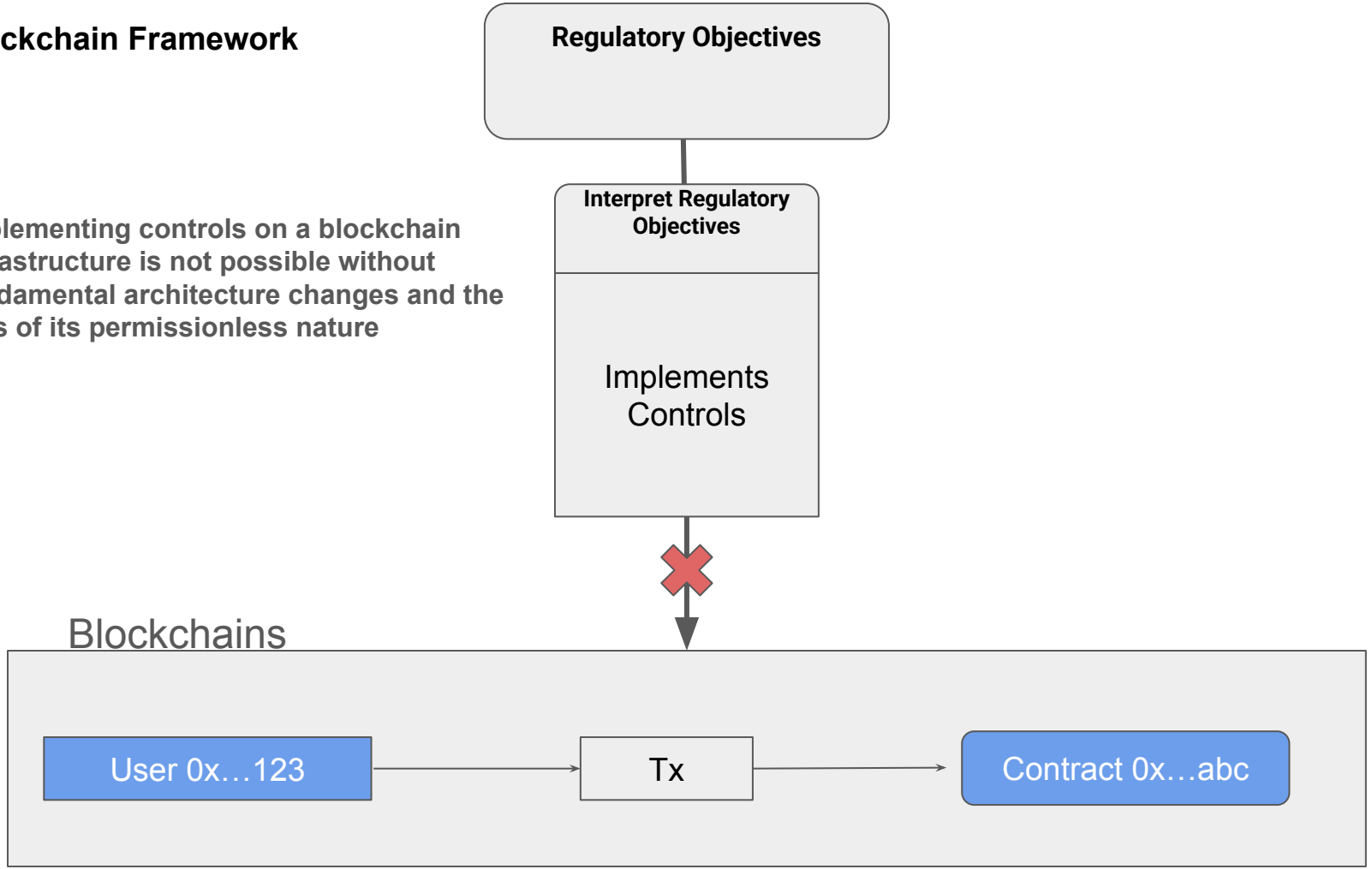
The Digital Securities Initiative

Traditional Finance Framework



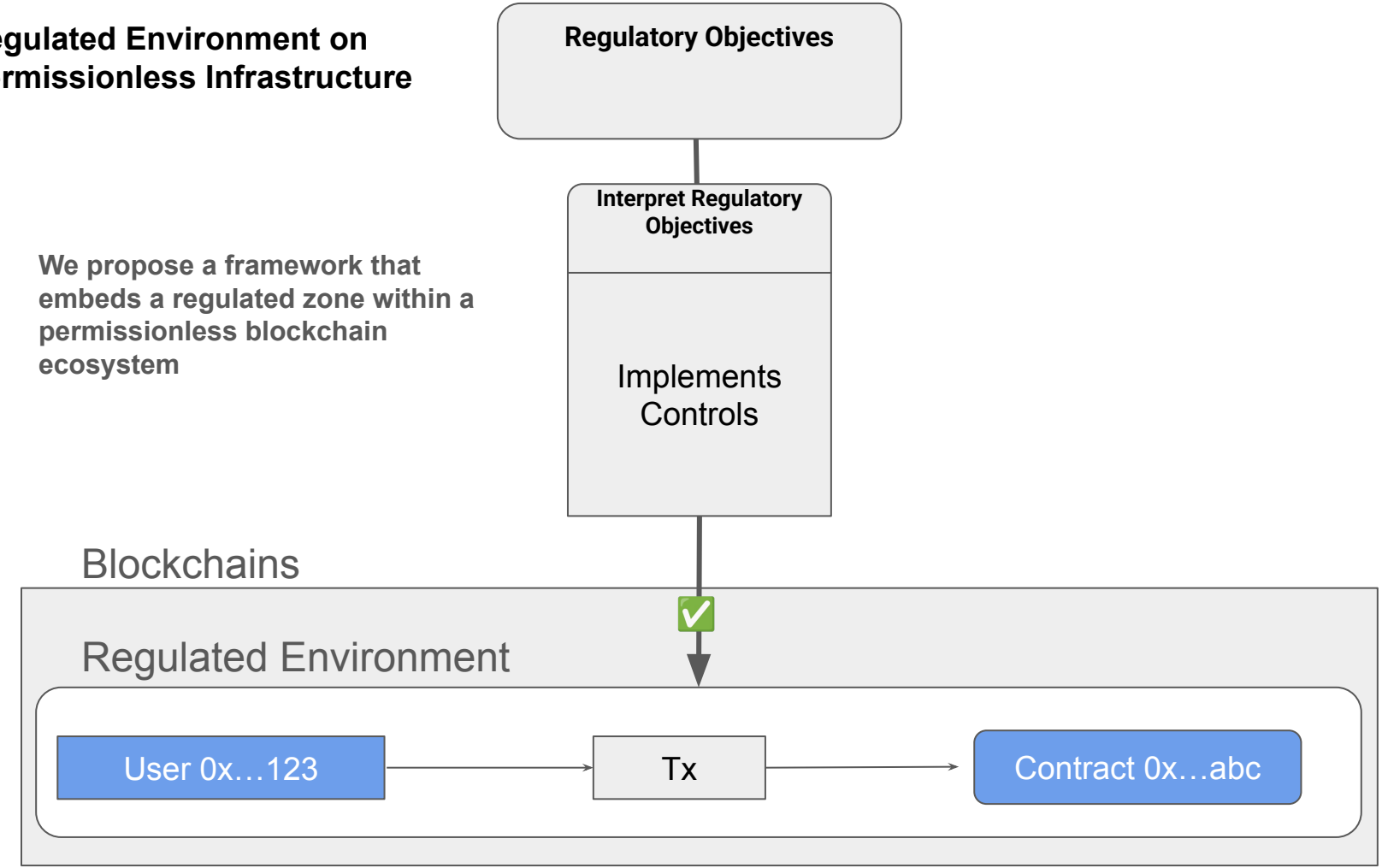
Blockchain Framework

Implementing controls on a blockchain infrastructure is not possible without fundamental architecture changes and the loss of its permissionless nature

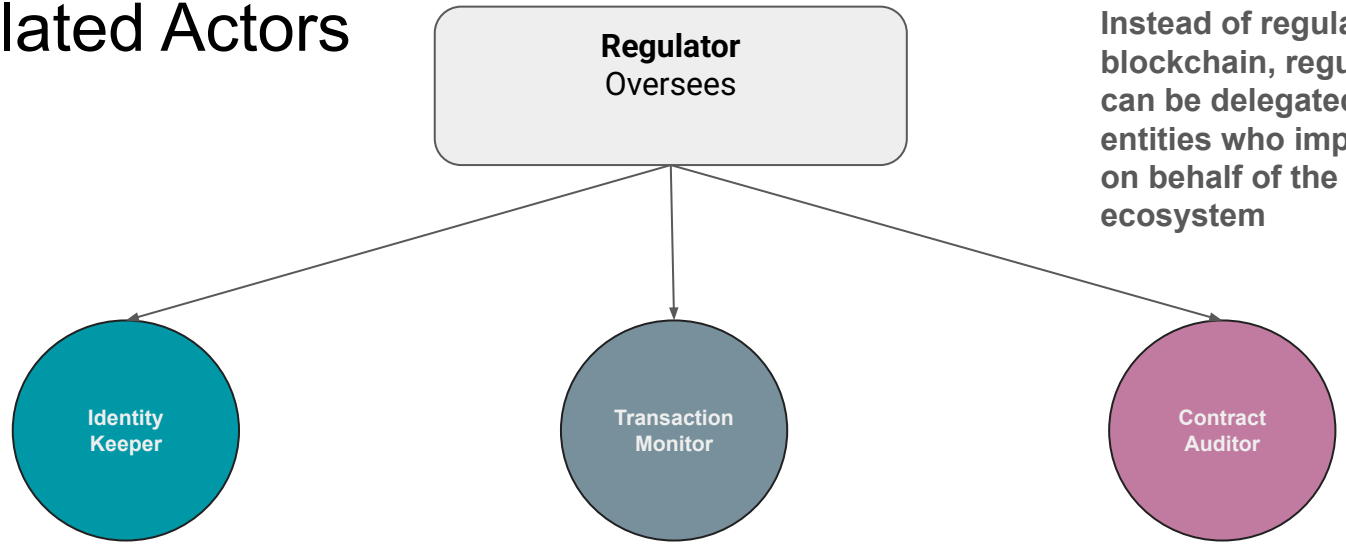


Regulated Environment on Permissionless Infrastructure

We propose a framework that embeds a regulated zone within a permissionless blockchain ecosystem



Regulated Actors



Instead of regulating the entire blockchain, regulatory processes can be delegated to various entities who implement controls on behalf of the broader ecosystem

Verifies personally identifying information (PII) of users

Users must:

- Register with a credentialed Identity Verifier

Observes and analyzes transaction patterns

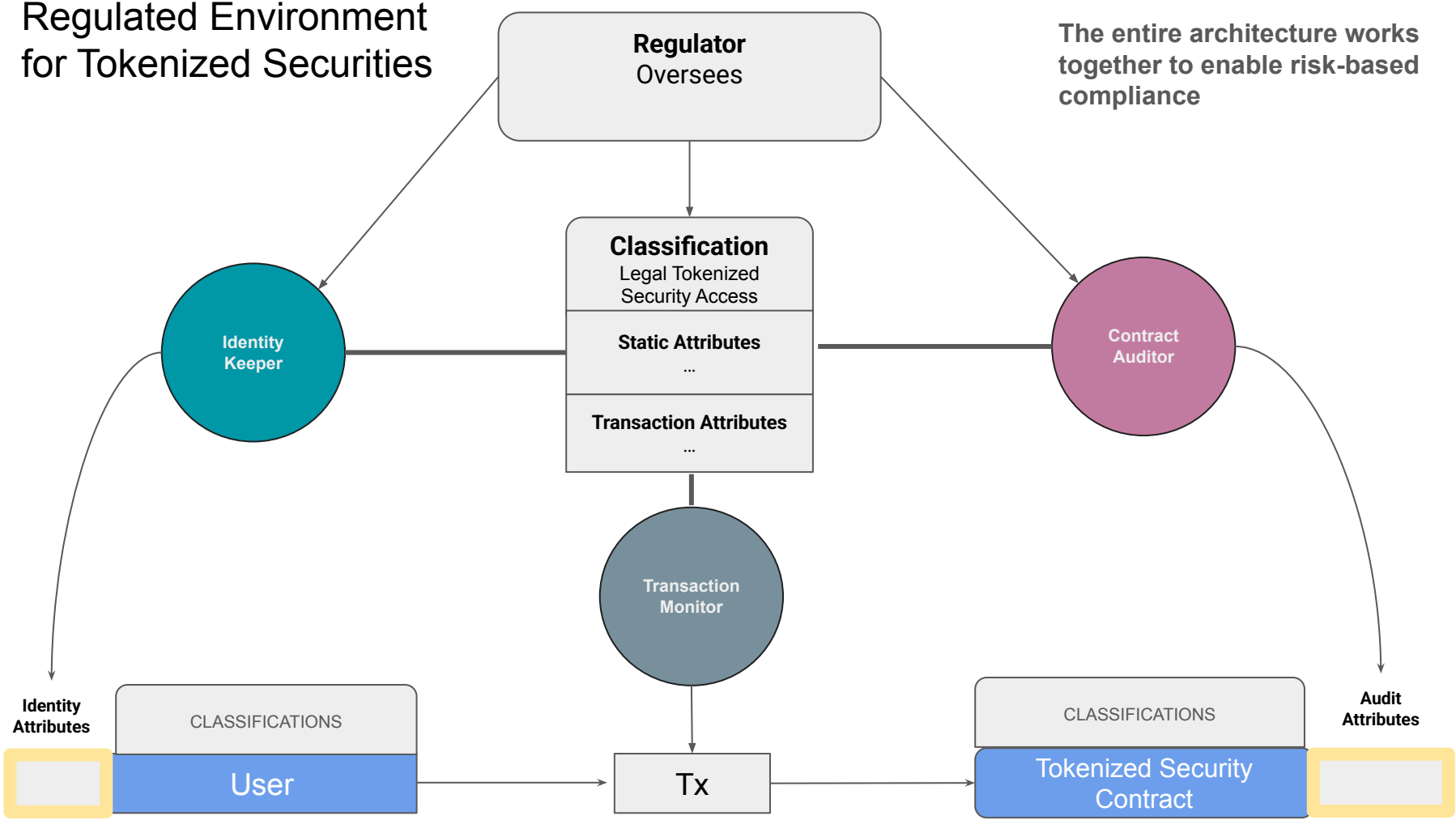
Confirms contracts comply with standards and security

Developers must:

- Receive an audit credential from a Contract Auditor

The Digital Securities Initiative

Regulated Environment for Tokenized Securities



Core Concepts

The Digital Securities Initiative

Zero Knowledge (ZK) Proofs

Cryptographic workhorse

ZK proofs allow users to prove relationships within hidden data

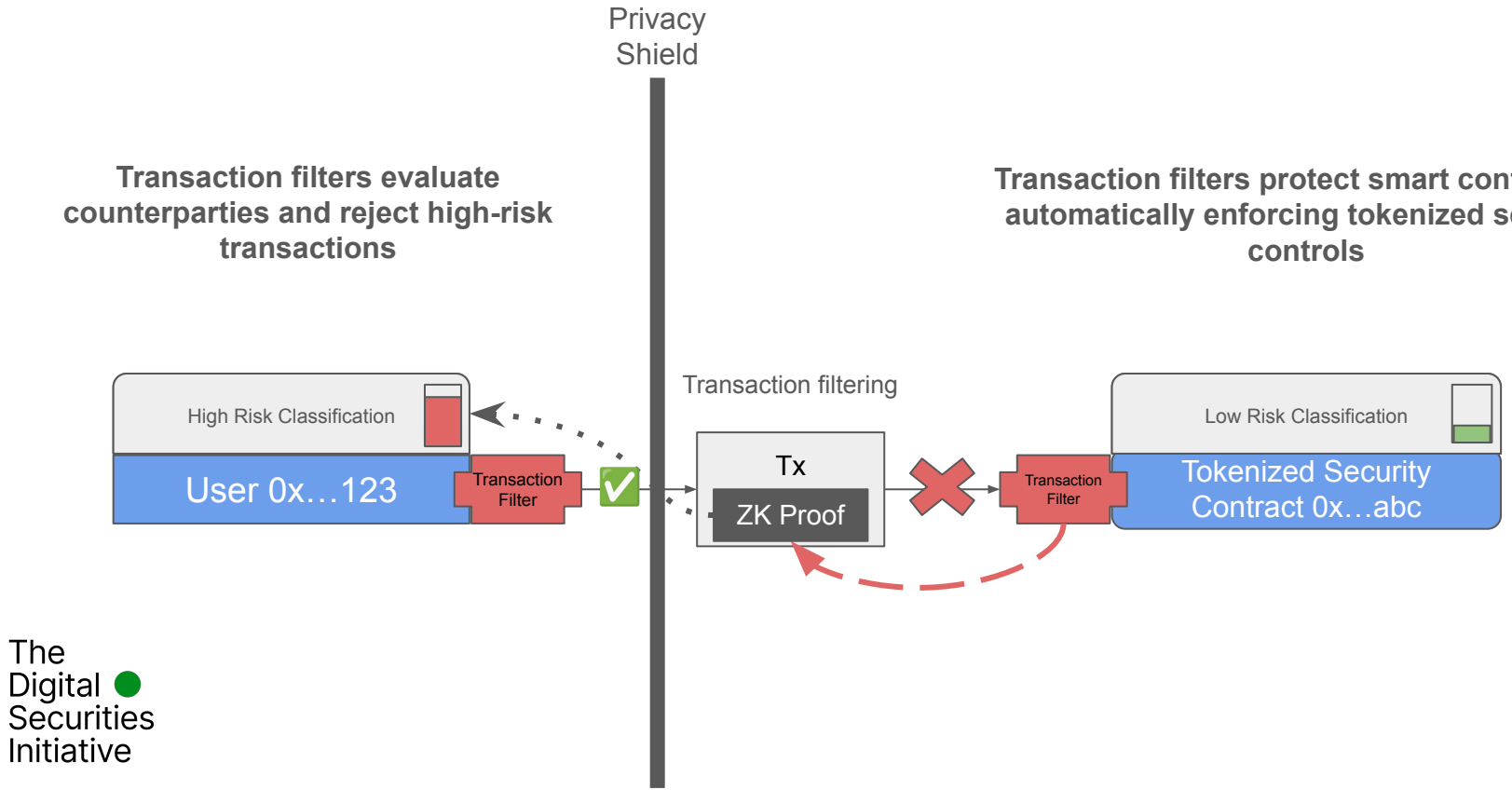
Good for privacy (reveal no information)

Efficient (compresses operations)

The Digital Securities Initiative

Transaction Filter (TF)

Controls of the Regulated Environment



The Digital Securities Initiative

Verifiable Credentials

Tech for certifications

Allows one digital identity to certify another digital identity

Credentials can be verified by a smart contract

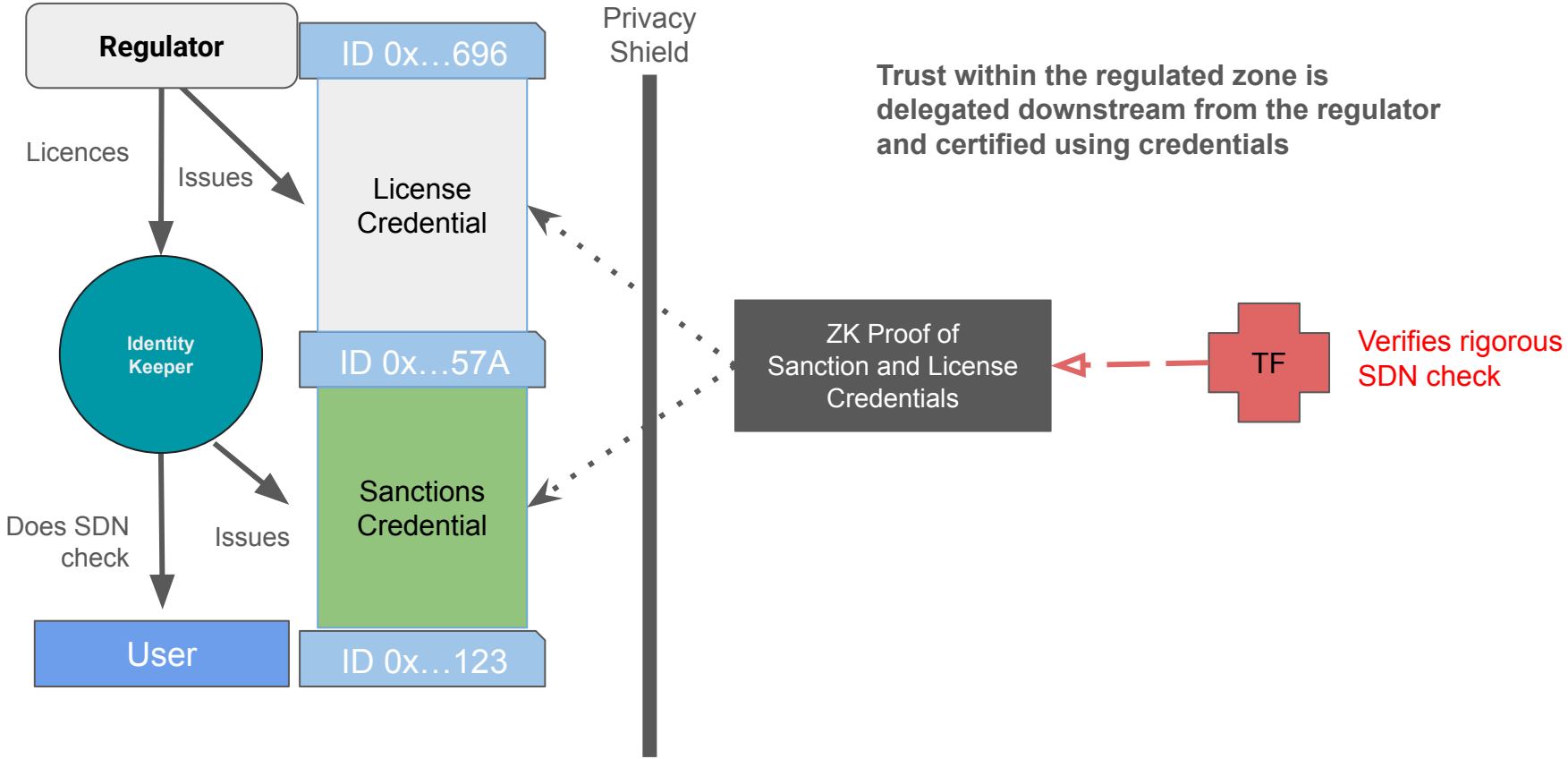
Enables real world assessments to be recorded onchain

The Digital Securities Initiative

Verifiable Credentials

Tech for certifications

Example: Sanctions Enforcement



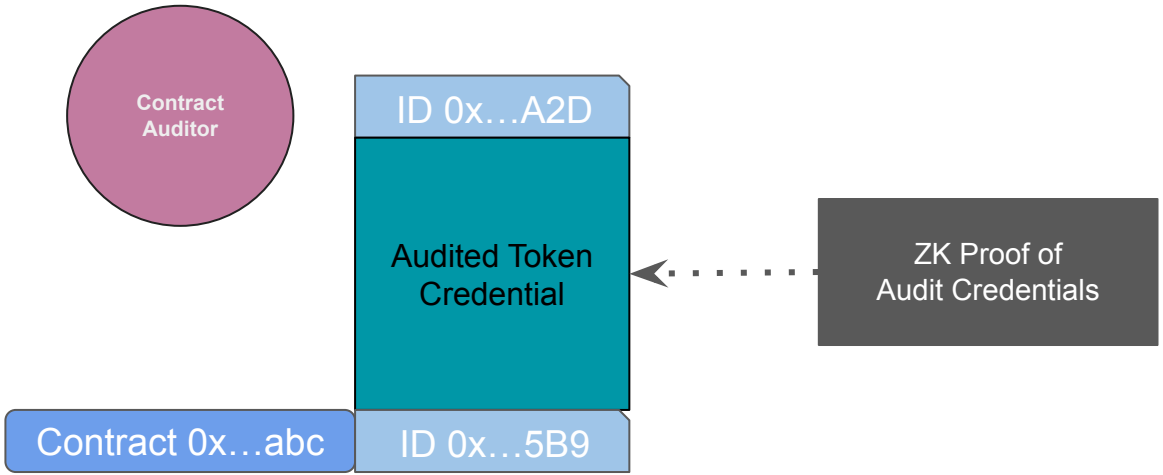
Trust within the regulated zone is delegated downstream from the regulator and certified using credentials

Verifiable Credentials

Tech for certifications

Example: Controls

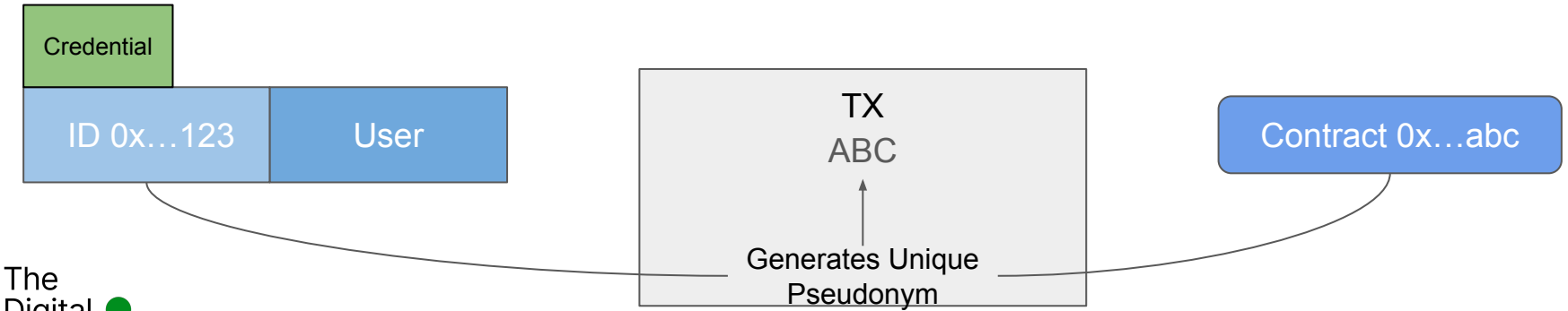
Contract Auditors certify that Smart Contracts have controls in place that ensure compliance



Pseudonyms

User Identification

Pseudonyms guard against criminals creating thousands of fake wallets

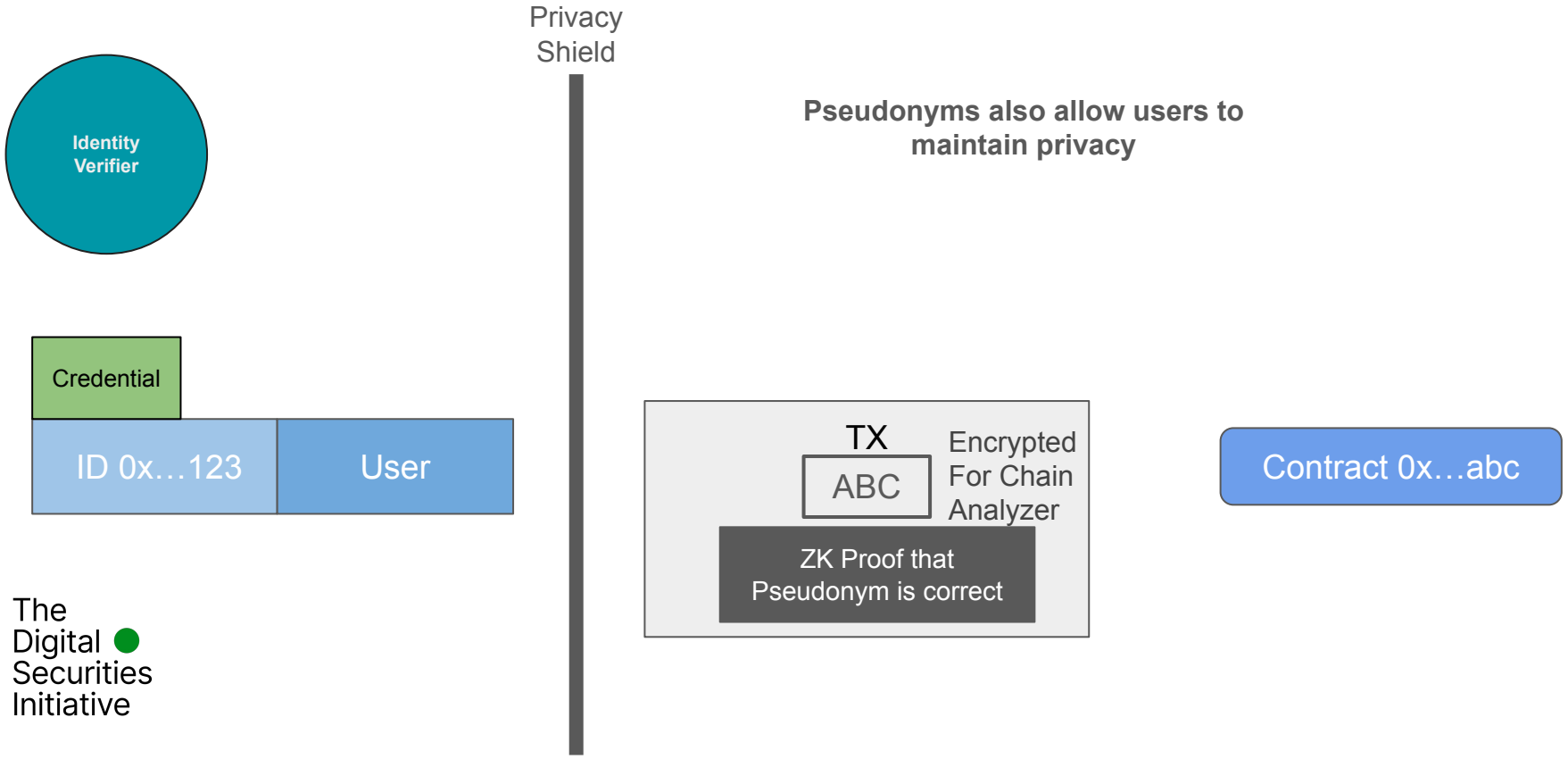


The Digital Securities Initiative

1 User +Credential+Smart Contract = 1 Unique Pseudonym

Pseudonyms

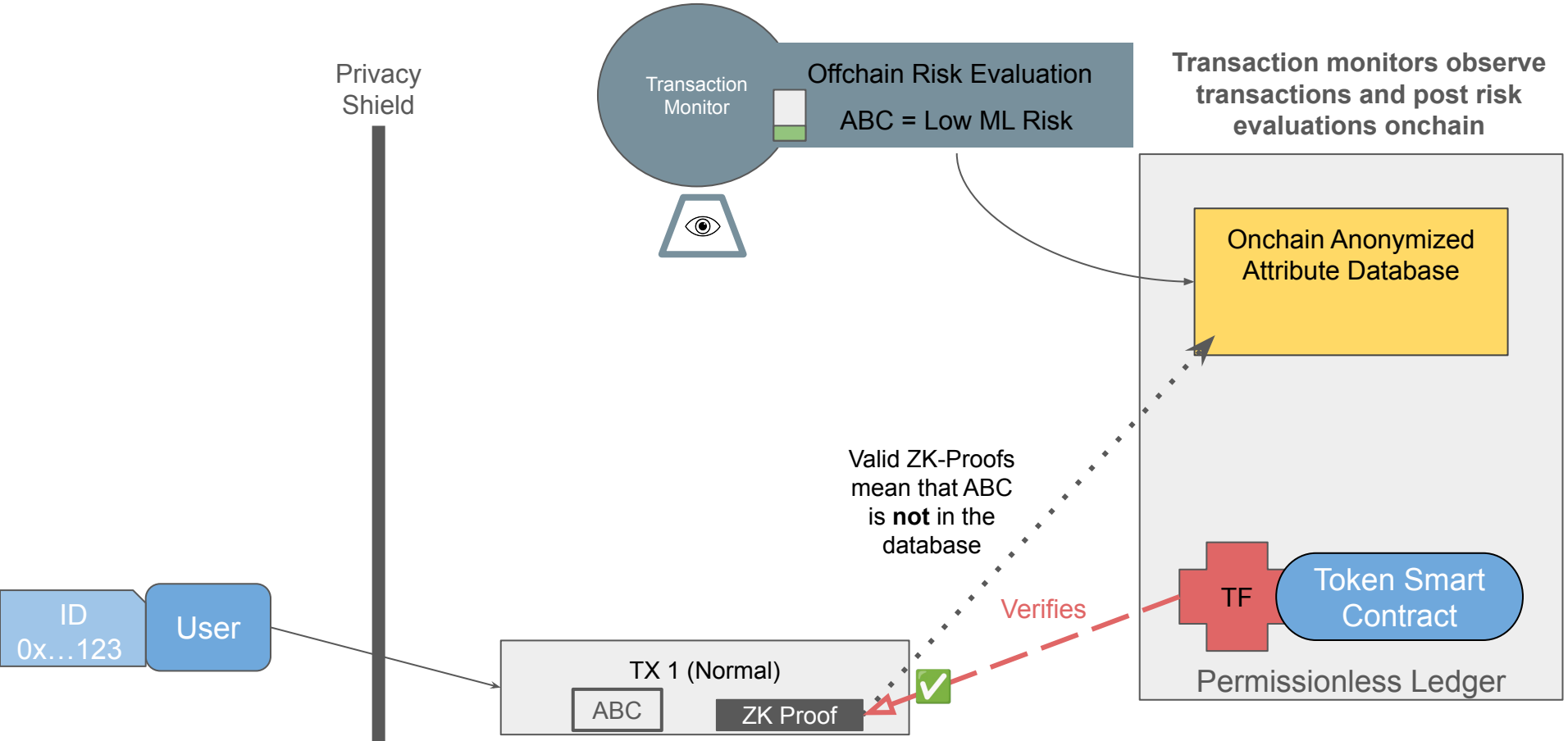
User Identification



The Digital Securities Initiative

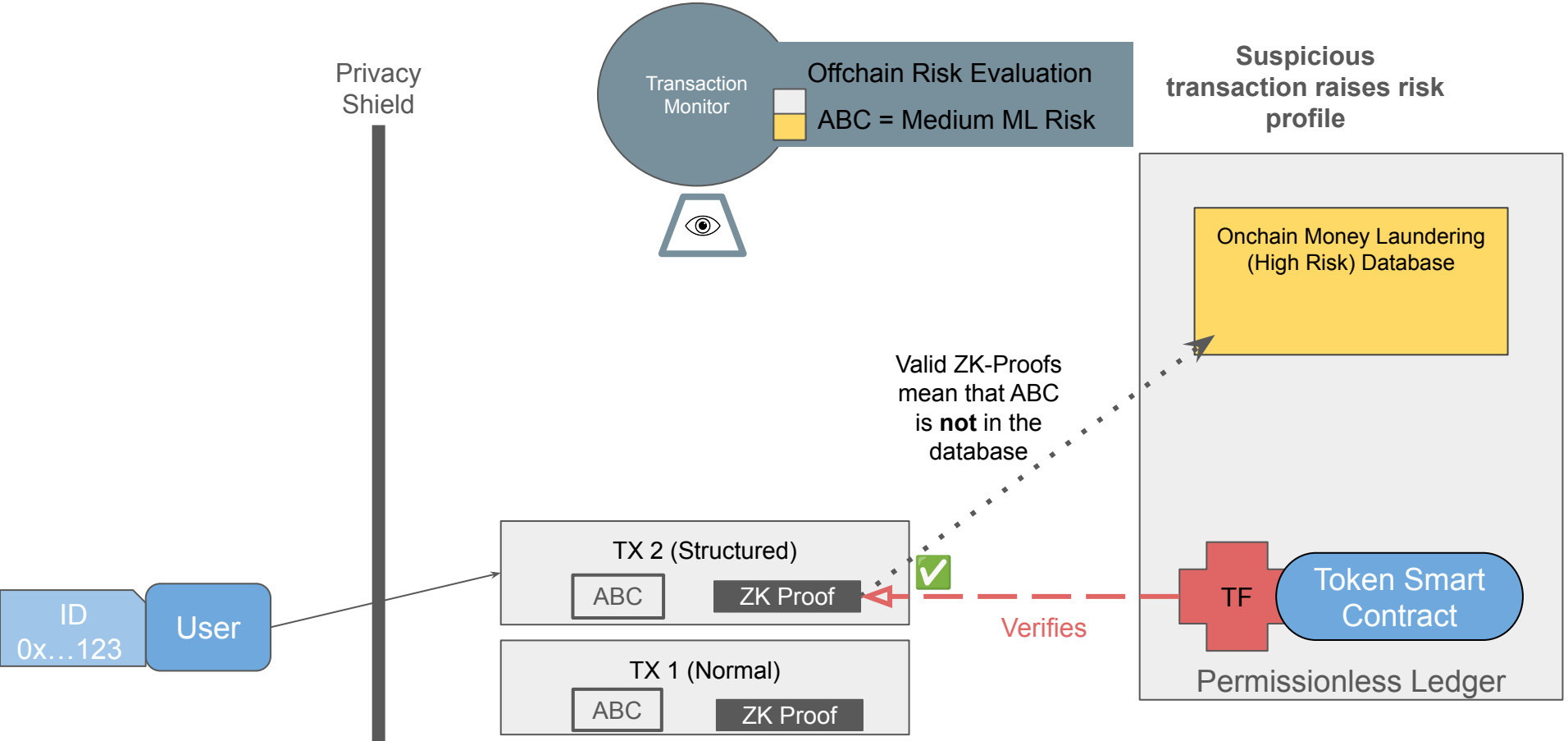
Transaction Monitor

Example: Revisit AML



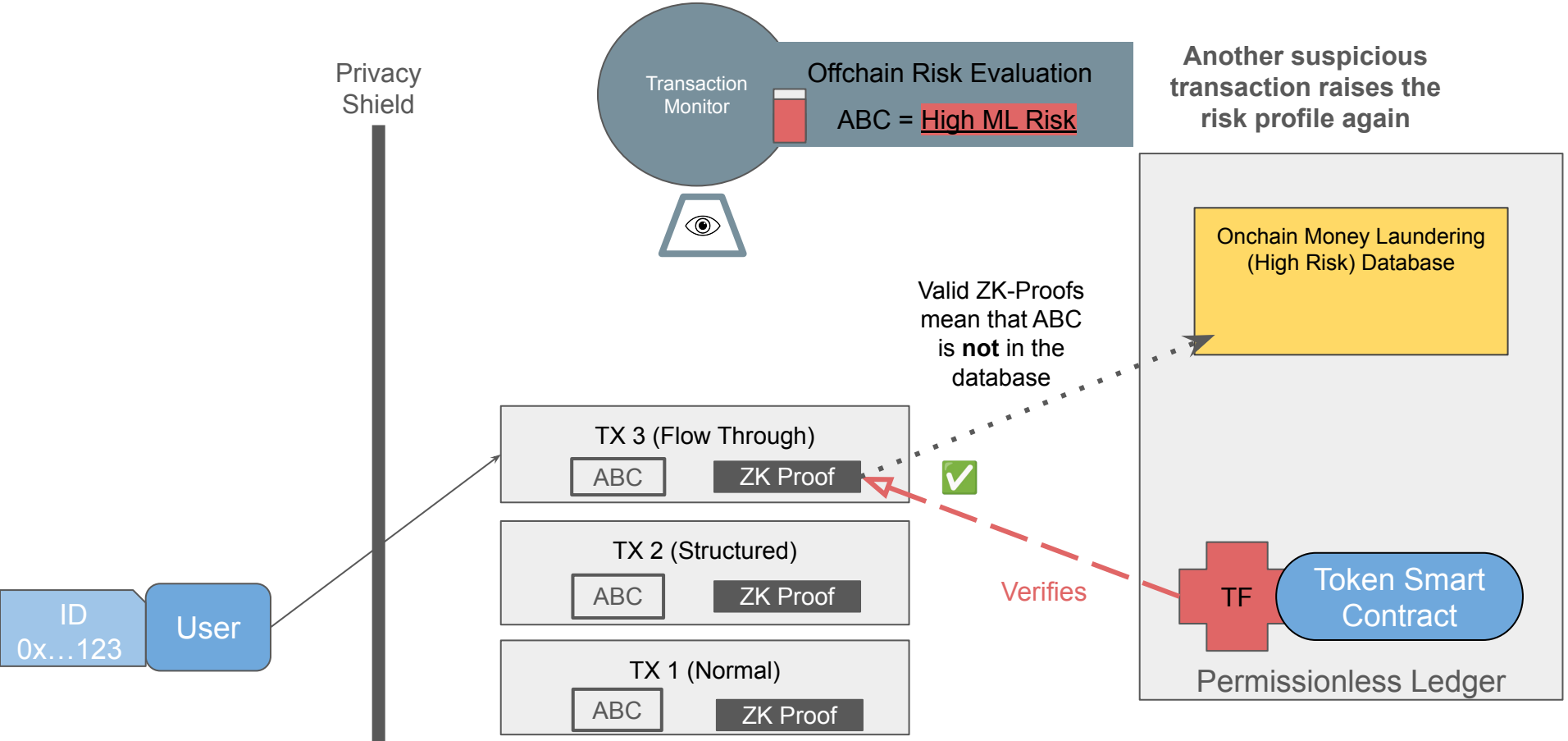
Transaction Monitor

Example: Revisit AML



Transaction Monitor

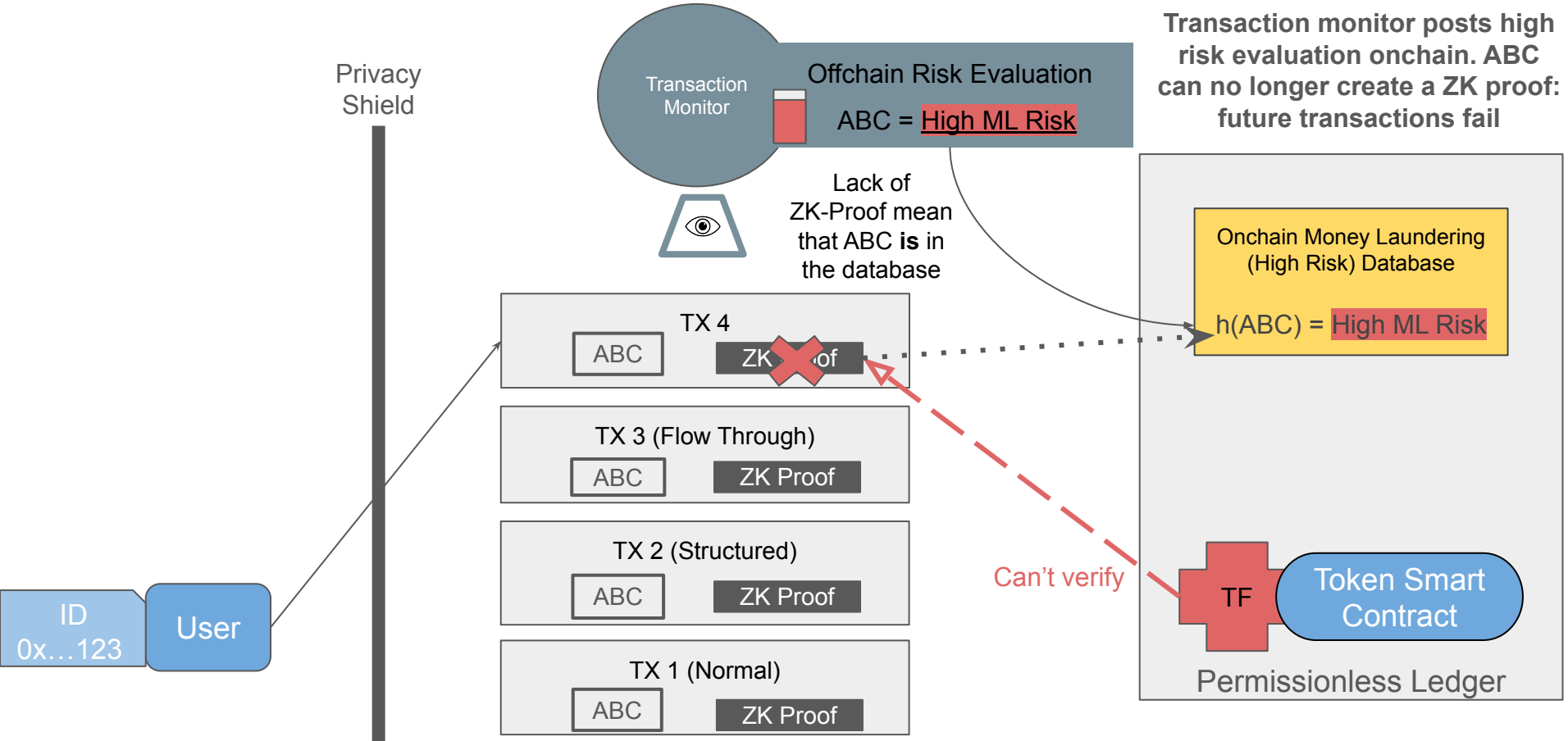
Example: Revisit AML



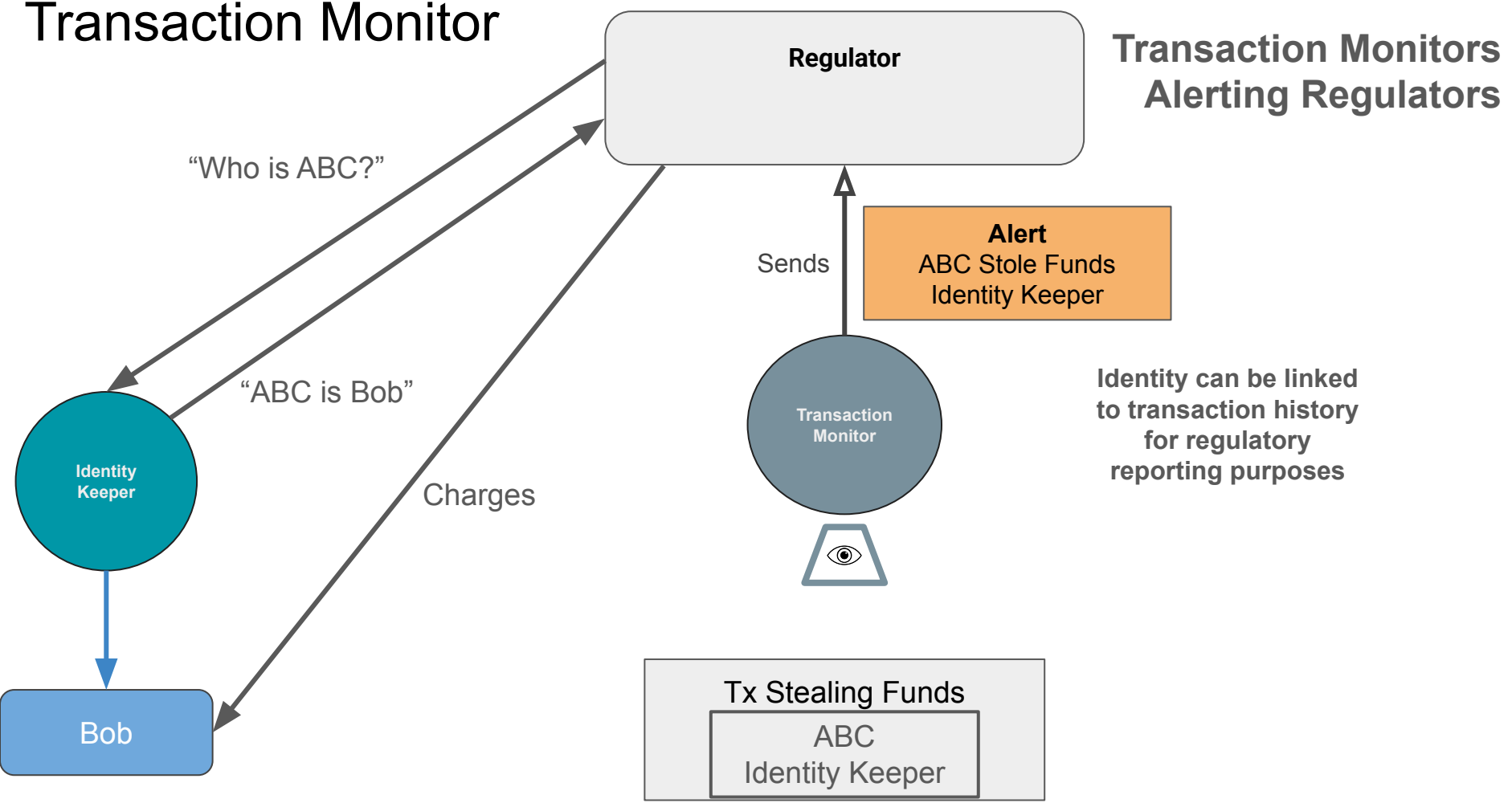
Transaction Monitor

Transaction Monitoring implementation

Example: Revisit AML

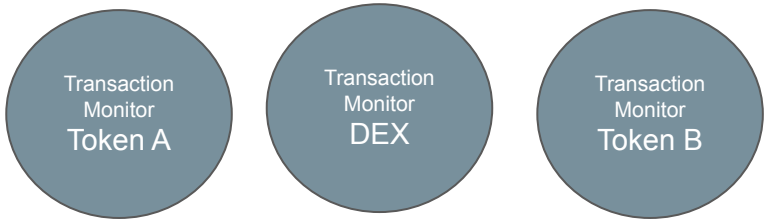


Transaction Monitor



Composing Smart Contracts

Everything x3



User swapping tokenized security A for tokenized security B using a DEX

Privacy Shield

TX
- ➔ Token A Transfer
- ➔ DEX Swap
- ➔ Token B Transfer

ABC | 3QF | X2Y

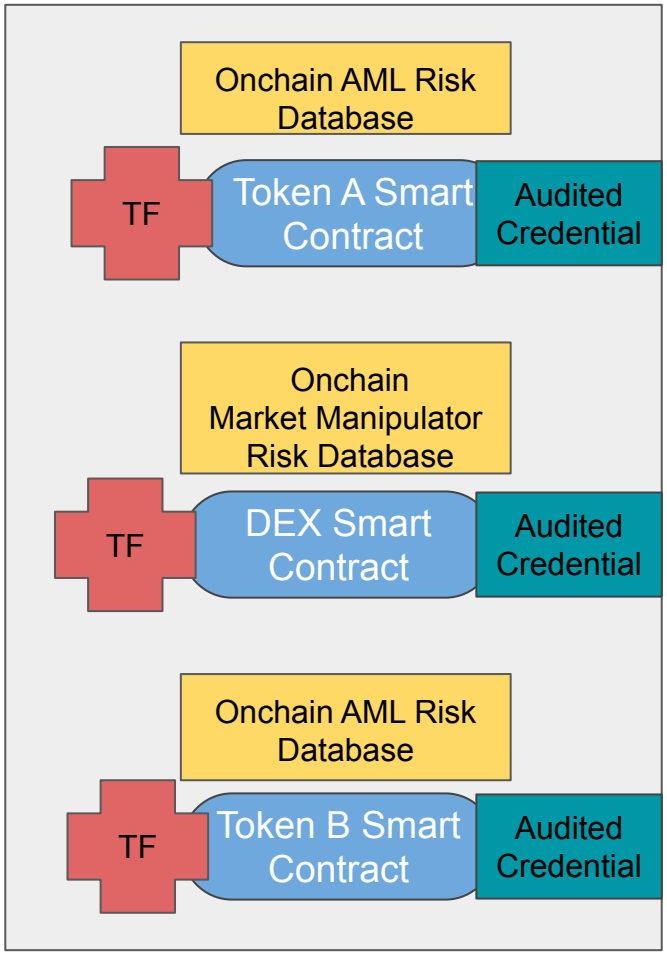
ZK Proof

Sanctions Credential

ID 0x…123

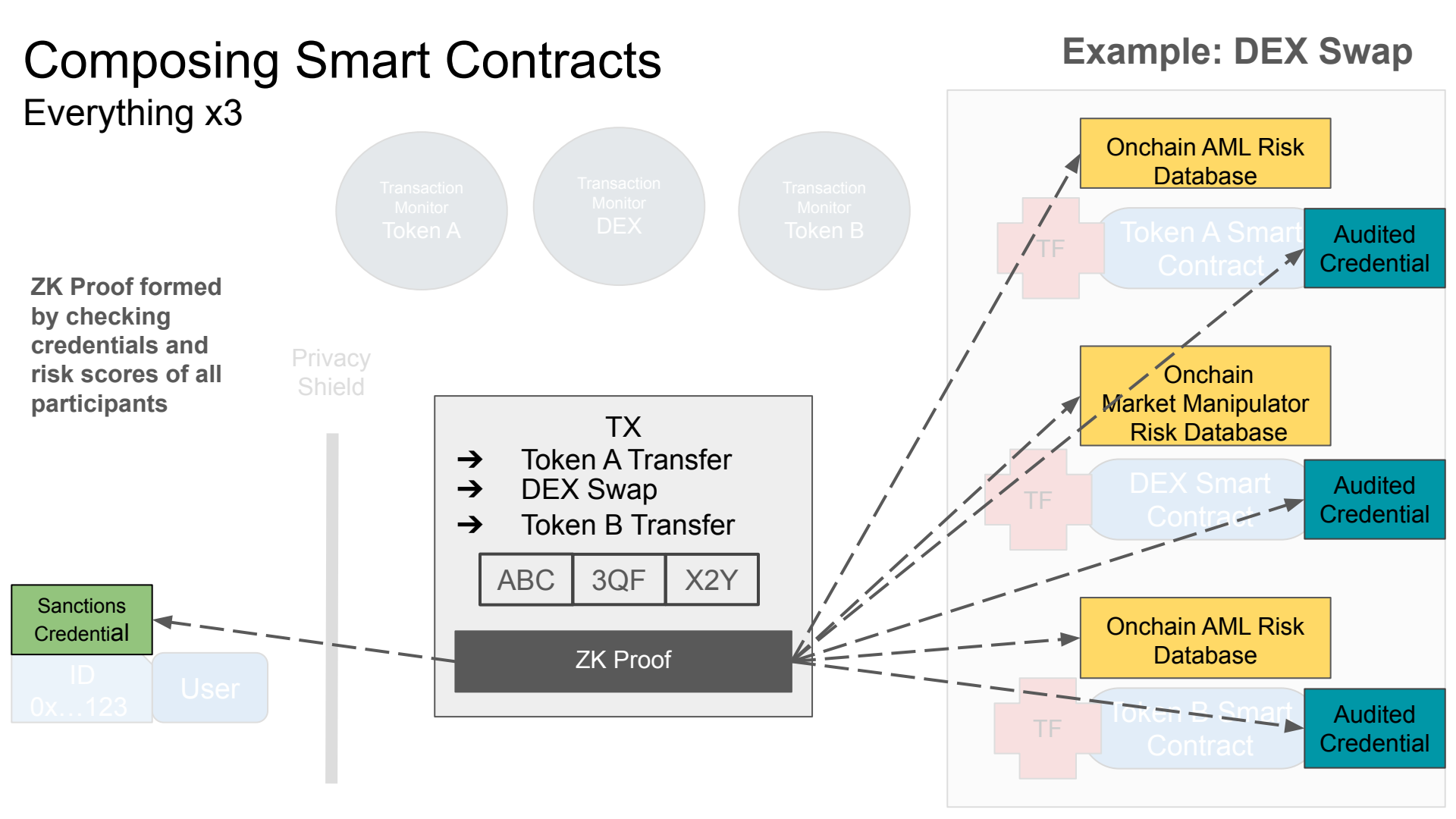
User

Example: DEX Swap



Composing Smart Contracts

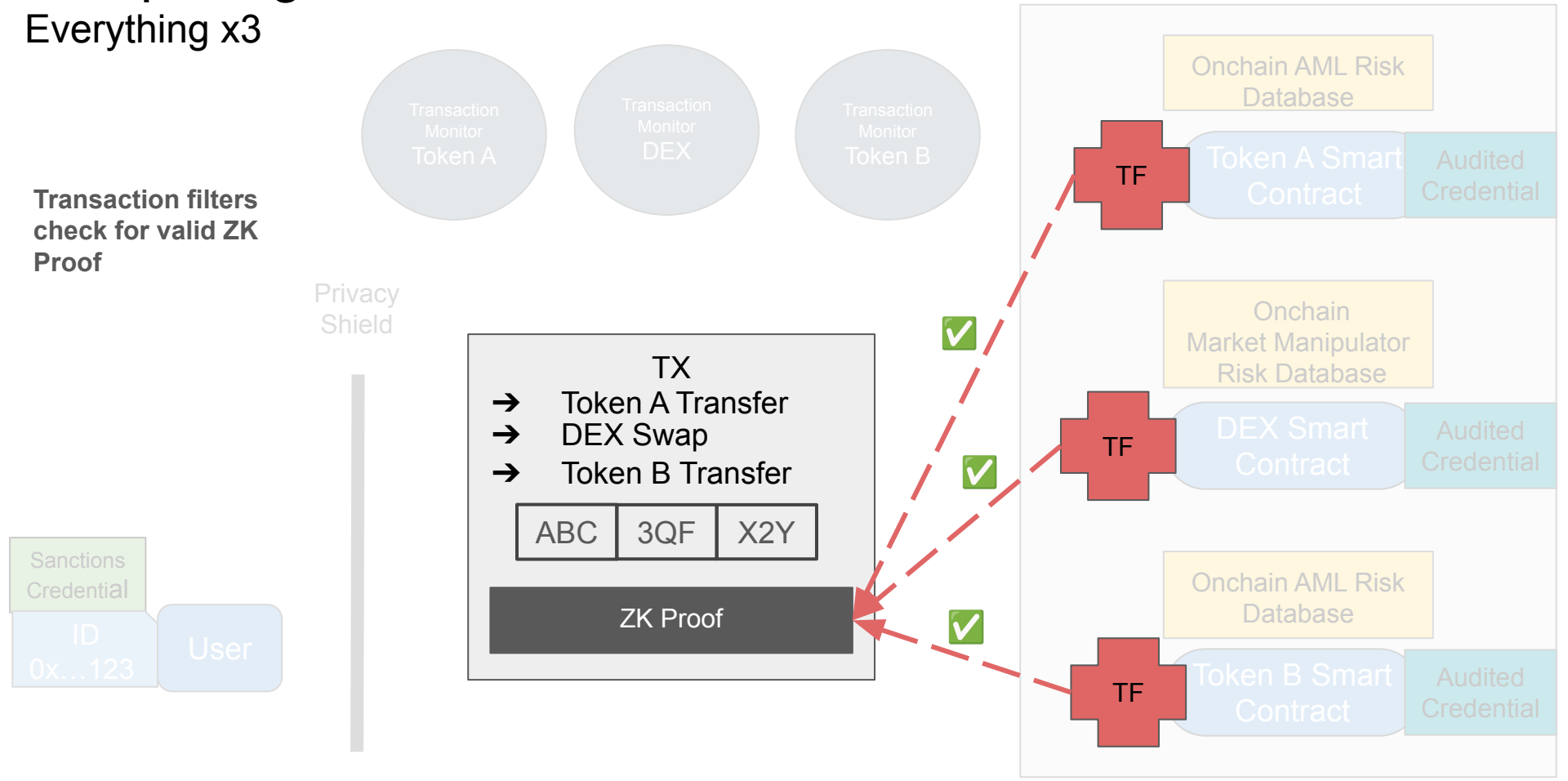
Everything x3



Composing Smart Contracts

Everything x3

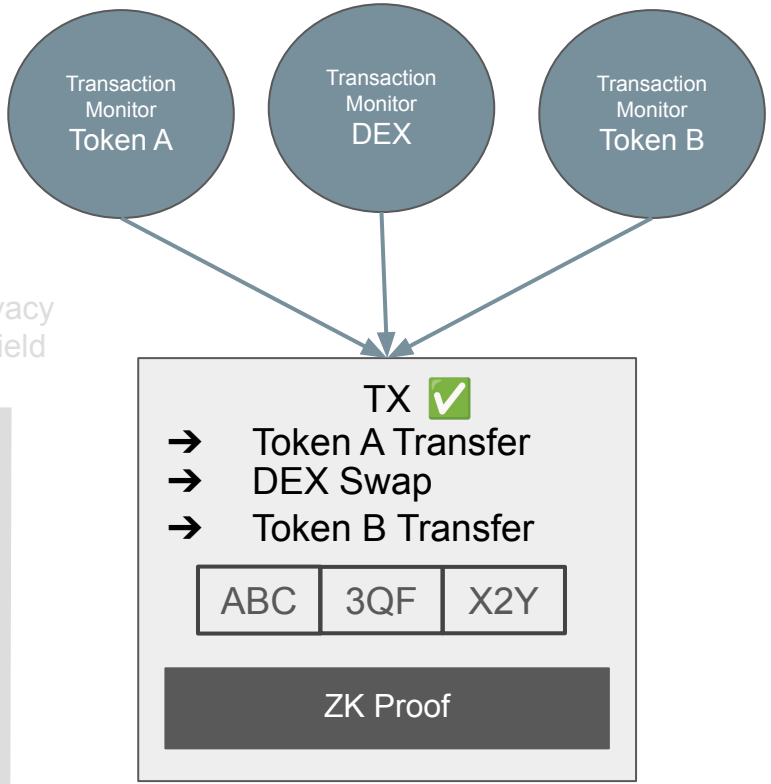
Example: DEX Swap



Composing Smart Contracts

Everything x3

Transaction is executed and is observed by Transaction Monitors. Risk databases are updated if needed



Example: DEX Swap

Privacy

If Chain Analyzers do the analysis…

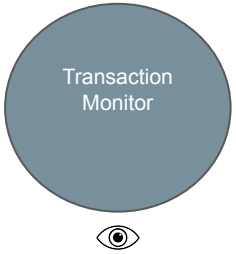
And Identity Verifiers do identification…

Privacy Pools and Privacy chains can be compliant!

The Digital Securities Initiative

Privacy

In a private token, the encrypted state and transactions can be read by the transaction monitor.

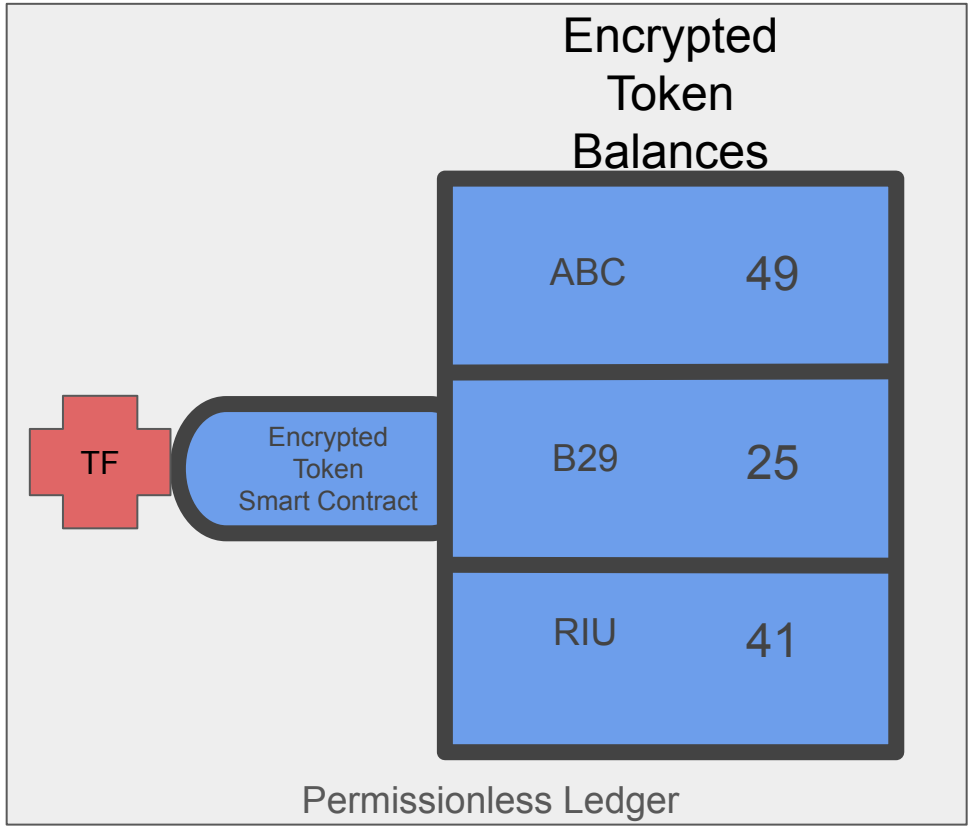


TX 3
Send 49 to B29
ABC

TX 2
Send 25 to ABC
5XL

TX 1
Send 41 to RIU
RIU

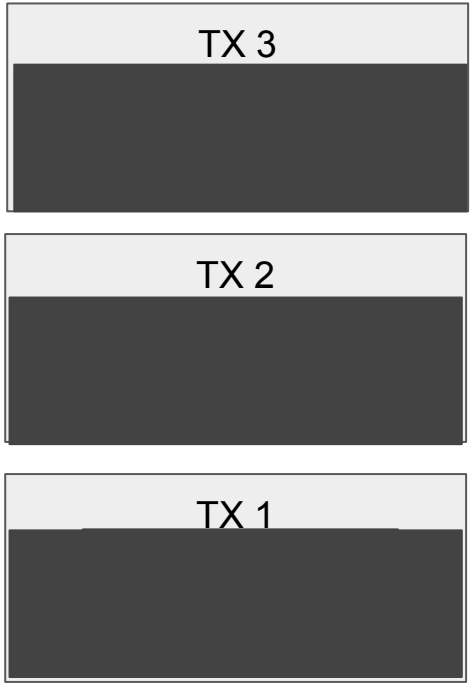
Example: Encrypted Token Transaction Monitor View



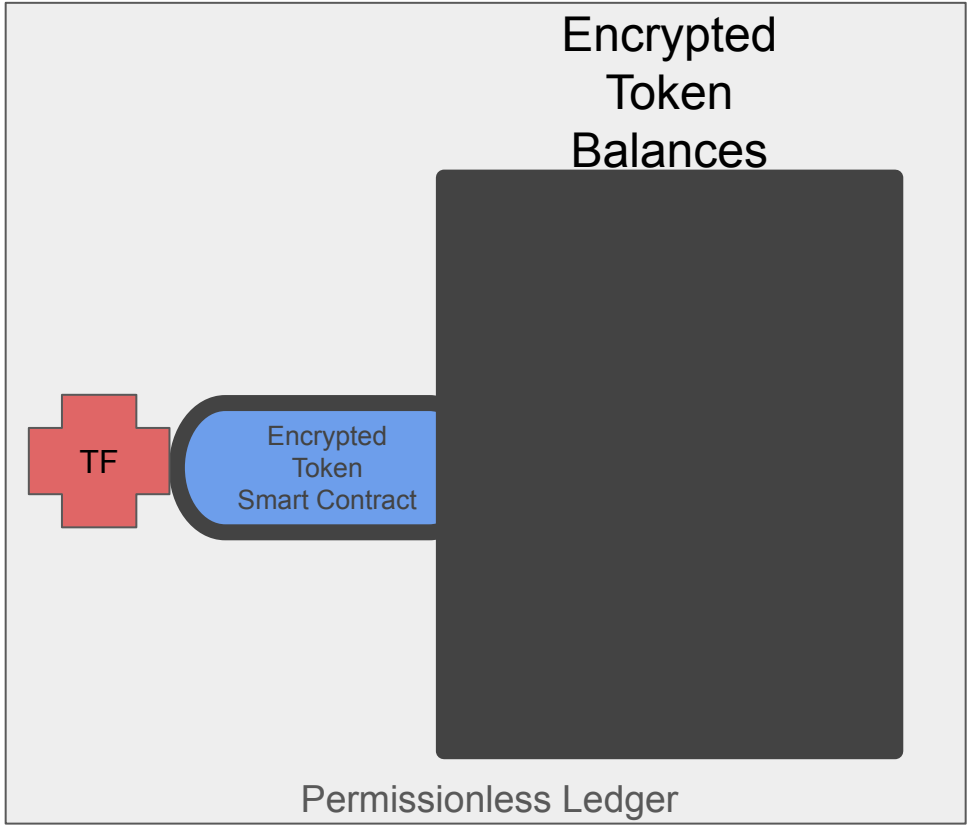
Privacy

General Public

But the general public cannot see anything



Example: Encrypted Token Transaction Monitor View



Regulated Zone for Tokenized Securities

The Digital Securities Initiative