A Regulatory Model for Tokenized Securities on Permissionless Blockchains

(A draft paper)

The Digital Securities Initiative

This document proposes the DSI Regulatory Model, a novel regulatory framework for tokenized securities. Our model simultaneously addresses financial crime, improves market efficiency, and provides privacy to market participants. We propose a chain-agnostic "Regulated Zone" for onchain tokenized securities, using the Global Access Protocol to embed financial regulations into the smart contract layer of permissionless blockchains, reducing infrastructure interventions and preserving the benefits of blockchains. The integrity of each Regulated Zone is maintained by a competitive service provider layer administered by permissionless Trust Anchors.

Each Regulated Zone is an open, collaborative system with many on and off ramps. Anyone can create a Regulated Zone and implement this Regulatory Model, ensuring a fundamentally permissionless system. Moreover, the DSI Regulatory Model solves a fundamental fragmentation problem posed by traditional whitelists: all Regulatory Zones exist via a common protocol and are thus composable, allowing a user to access numerous markets with a single onboarding process. Lastly, Regulated Zones can be deployed on privacy chains, allowing users to compliantly trade securities on permissionless ledgers without revealing their transactions publicly.

The DSI Regulatory Model does not enable regulatory arbitrage, nor does it enable participants to profit off of regulatory capture. The DSI Regulatory Model builds public infrastructure that enforces the policy objectives regulations are meant to achieve—sanctions compliance, KYC, market integrity, investor protection—using technology instead of intermediaries.

1. Introduction

The tokenization of securities represents one of the most significant opportunities in modern finance. By representing stocks, bonds, funds, and other regulated instruments as tokens on blockchain networks, markets gain access to instant settlement, continuous trading, fractional ownership, and global accessibility. The potential scale is staggering. Global securities markets exceed $250 trillion in value, and even a fraction of this migrating onchain would transform how capital is formed and exchanged.

This shift is already underway. Leading financial institutions like BlackRock, JP Morgan, Franklin Templeton, Fidelity, Apollo and many more have launched products onchain. Regulatory frameworks are emerging across jurisdictions from the United States to Singapore to the European Union. Yet despite this momentum, tokenized securities remain largely confined to permissioned platforms or centralized exchanges and their aggregate onchain value is less than $20 billion.

Progress is slow because permissionless blockchain challenges many of the foundational assumptions of traditional financial regulation, that there are intermediaries like brokers, custodians and transfer agents that identify customers, monitor transactions, and enforce rules. Permissionless blockchains enforce rules via cryptography and consensus algorithms and thus do not need such gatekeepers . Anyone can deploy a smart contract, execute a transaction, or build an application without seeking approval as long as they follow the rules laid out in the code.

Current tokenization efforts fail to leverage the full power of blockchains to coordinate human behavior, and instead achieve compliance by sacrificing the fundamental openness that makes DeFi work. Consider an investor who holds a tokenized treasury bond on one platform and wants to use it as collateral to purchase a tokenized equity on another. Today, this simple transaction is nearly impossible. Each platform maintains its own whitelist. The investor must complete separate identity verification for both, wait for manual approval, and hope the platforms have established a bilateral integration. Even then, the assets likely cannot interact with DeFi protocols. This means no lending against the bond, no automated market making, and no composable strategies. The

investor faces the worst of both worlds: the operational friction of traditional finance without the liquidity and flexibility of decentralized markets. The problem is further compounded if the assets belong to two different regulatory jurisdictions.

Furthermore, current blockchain compliance programs are incompatible with privacy. Currently, projects must rely on blockchain analytic services that monitor all public blockchains. These analytics, which trace the history of funds, are at odds with privacy tools that necessarily obfuscate that history. Besides laying the framework for a financial panopticon, public blockchains prevent investors from hiding their trading strategies, positions, and their exposure. Thus in order for securities to be tokenized, blockchain participants need compliance programs that are compatible with privacy.

To facilitate the Tokenization of Securities, the *Digital Securities Initiative (DSI)* set out to solve these problems by designing a novel regulatory model that preserves the benefits of DeFi while providing regulators the necessary tools to do their job. DSI is a cross-disciplinary effort, with input from DeFi builders, tokenization platforms, regulatory agencies, and leading practitioners in securities law and financial compliance. The resulting *DSI Regulatory Model* is a blueprint for a new set of actors to replace current intermediaries in regulating markets. Although this model is designed for the tokenization of US Securities, it is generally applicable to other asset classes and jurisdictions.

The DSI Regulatory Model offers a fundamentally different approach from other compliance programs. It uses the *Global Access Protocol (GAP)*, a compliance aware protocol, to define and enforce regulatory standards, embedding compliance directly into the smart contract layer. In the DSI Regulatory Model, a competitive service provider layer uses these standards to create and maintain collaborative *Regulated Zones* with many gate keepers. Since these Regulated Zones are created with the same protocol, GAP, they are composable making them fundamentally different from simple whitelists.

Before entering a Regulated Zone, a user completes identity verification once with an *Identity Keeper*, who issues privacy-preserving credentials. The credential includes attestations like "not sanctioned" or "accredited investor" that can be proven without publicly revealing underlying personal data. When that user interacts with a tokenized security, *Transaction Filters* in the various smart contracts verify credentials using zero-knowledge proofs. The contracts themselves have been audited and classified by *Contract Certifiers* who attest that the code enforces required controls. *Transaction Monitors* observe activity within the zone, flagging suspicious patterns. Finally, governance bodies operating under regulatory oversight, called *Trust Anchors*, set standards, register service providers, and maintain accountability across the system. Each component is examined in detail in the sections that follow.

Our goal is a global financial system where a user completes identity verification once and gains access to regulated markets worldwide. Where developers build applications that route seamlessly across jurisdictions without bespoke integrations for each regime. Where investors transact

privately without exposing their positions, strategies, or personal information. And where regulators retain the tools they need to enforce sanctions, monitor for abuse, and identify bad actors through proper legal process. This is how tokenization reaches its full potential and trillions in securities finally migrate onchain.

2. System Overview

The DSI Regulatory Model consists of both people and technology: it outlines novel social institutions coordinated by the *Global Access Protocol (GAP)*, a new compliance aware protocol deployed on a permissionless blockchain. GAP embeds compliance directly on the smart contract layer, allowing other contracts to filter out users. However these filters require real world information about both users and other smart contracts, requiring people to record this real world information onchain. The effectiveness of the filters is limited by the accuracy of this information, and thus social institutions must be developed to ensure the integrity of these assessments. Thus the protocol and the institutions are necessary in the DSI Regulatory Model.

GAP is currently being developed by DSI and according to the requirements of the DSI Regulatory Model. However, since GAP is fundamentally permissionless, nothing prevents its use contrary to the DSI Regulatory Model, and hence GAP represents a distinct layer of the DSI Regulatory Model. This document primarily focuses on the roles and functions of social institutions that GAP is designed to facilitate[1]. However, we begin with an overview of GAP.

At its core, GAP is a tool to deploy a *Regulated Zone*, a group of contracts that are operating under a common set of standards that allow them to comply with regulatory obligations. Amongst other obligations, contracts within each Regulated Zone must have a module called a *Transaction Filter* which rejects transactions containing function calls not permitted under the rules of the Regulated Zone. Specifically, for each function call, the Transaction Filter checks the relevant addresses, whether they belong to a user or another smart contract, and it makes a determination based on:

1. The attributes of the users' Personally Identifiable Information (PII)
2. A users' risk for violating rules of the Regulated Zone with past transactions
3. The standards that the contract adheres to

In order for the Transaction Filter to work, GAP enables different *Service Providers* to record onchain each of the above three types of information:

1. *Identity Keepers* issue credentials containing hashes of PII based attributes
2. *Transaction Monitors* analyze contract calls and flag potential abuse
3. *Contract Certifiers* issue credentials that classify smart contracts under standards set in Regulated Zone

[1] For a technical description of GAP, we refer the reader here: GAP White Paper

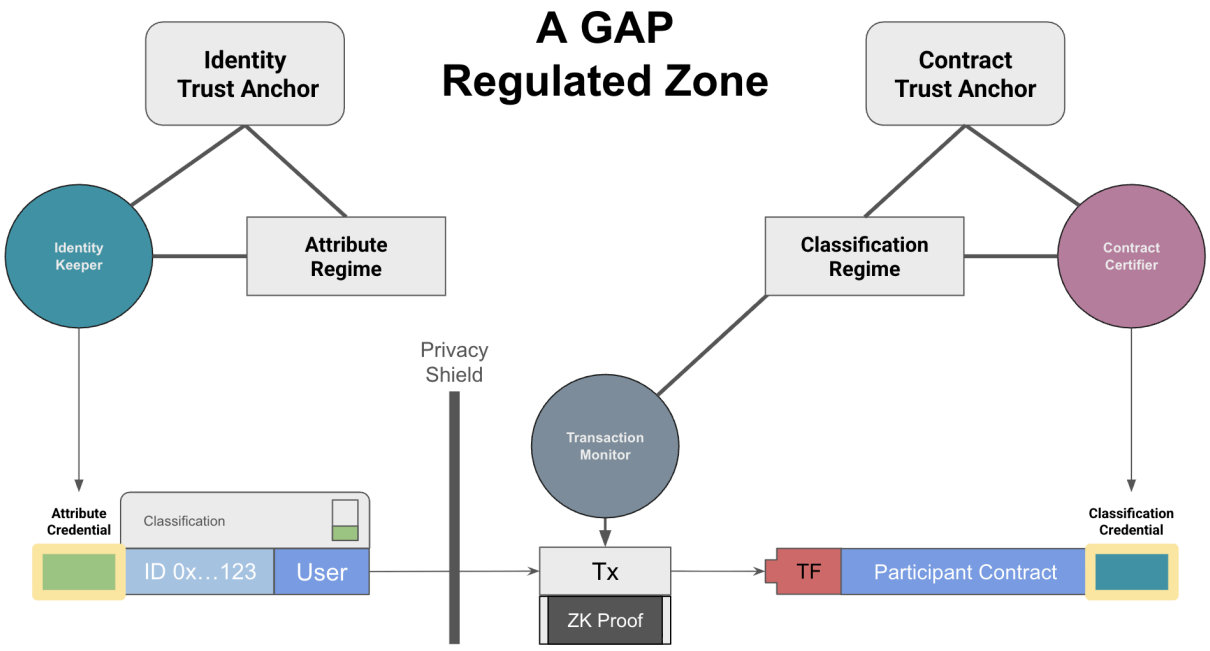

Figure 1: Visual overview of a Regulated Zone under the Global Access Protocol

To ensure quality of services, these Service Providers operate under the administration of entities we Trust Anchors. Specifically, the Identity Keepers must register with Identity Trust Anchors who set standards for how PII is collected and encoded. Contract Certifiers register with Contract Trust Anchors who adopt classification systems for contracts which determine requirements and obligations so each smart contract, including behaviours that a Transaction Monitor must flag. Although anyone can be a Trust Anchor, different Trust Anchors will be accepted or rejected based on their reputation and the quality of standards they maintain.

This architecture is designed to maximize privacy. Only the hash of PII based attributes are published onchain in credentials. Similarly, users interact with Transaction Monitors via a *Pseudonym*, a contract specific identifier that protects the user's identity. Users use ZK proofs to prove that they have the necessary PII attributes and that their Pseudonyms have not been flagged. This creates a fundamental barrier between user's information and their transaction data. Moreover, since each Transaction Monitor has a different user Pseudonym, their profiles on each user cannot be immediately aggregated. Thus, no actor has a honey pot of data that can be abused or compromised. Lastly, the local views of Transaction Monitors allows this protocol to be deployed on privacy chains without granting a single actor broad surveillance powers.

Although broadly applicable, the DSI Regulatory Model is designed to facilitate the tokenization of US Securities. In the design of this system, DSI took into consideration the primary regulatory objectives of the relevant regulatory agencies, such as the Security and Exchange Commission (SEC), Financial Crimes Enforcement Network (FinCEN), and Office of Foreign Assets Control

(OFAC). Specifically, the DSI Regulatory Model addresses sanctions enforcement, AML, market manipulation, best execution/MEV, and offering restrictions.

3. Identity Keepers

3.1 Attributes and Attribute Credentials

Under the DSI Regulatory Model, data standards called *Attribute Regimes* manage access to Regulated Zones for users by providing the semantics necessary for the automated modules in GAP to reason about users. Specifically, Attributes define *Attributes*, objects storing PII. Attribute Regimes also implicitly mandate the information collected during onboarding processes to allow them to access the smart contracts in Regulated Zones. Thus an Attribute Regime binds the Regulated Zone to the real world.

Using a permissionless neutral, permissionless contract in GAP, users will register a static identifier called a Digital Identity (DID) to which service providers called *Identity Keepers* can issue *Attribute Credentials*, attestations which contain the hash of an Attribute. This technology is an example of Verifiable Credential which is an established tool that allows one entity to digitally certify something about another entity.[2] A DID is useful because it is more permanent than a wallet address. Indeed a user can rotate their wallet addresses or use several simultaneous addresses for privacy reasons. However, a DID remains static.

Attribute Credentials are issued and stored onchain, however since the Attribute is obfuscated by a hash function[3], no personal information is revealed. GAP will provide the machinery necessary for a user to produce ZK proofs to prove claims based on these Attributes.

In GAP, Attribute Credentials are always issued under the auspices of an administrator called an *Identity Trust Anchor*. Specifically, GAP enables this Trust Anchor to grant and revoke Identity Keepers permissions to grant Attribute Credentials under an Attribute Regime. In order to issue Attribute Credentials under its auspices, an Identity Keeper must first register with the Identity Trust Anchor, undergoing a KYB process, and agreeing to the Identity Trust Anchor's Terms of Service. Under the DSI Regulatory model, the Identity Trust Anchor will periodically audit Identity Keepers to ensure that they are following the proper procedures.

Under the DSI Regulatory model, Identity Keepers have two main responsibilities. First, to receive Attribute Credentials, a user must go through a Customer Identification Process (CIP) with an Identity Keeper. This process involves presenting documentation which is verified by the Identity Keeper. The Identity Trust Anchor ensures that Identity Keepers' processes are robust and conform

[2] We note that DIDs is a technology well established outside of GAP that has many potential uses. https://www.w3.org/TR/did-1.1/

[3] Although a hash does not always fully obfuscate PII, GAP actually uses salted hashes.

to the relevant standards, such as FATF Recommendations.[4] Since customers only need to be onboarded once to receive all their credentials, a stringent CIP is quite reasonable.

Second, Identity Keepers must also also revoke credentials when appropriate. This can be done for instance if the user decides that they would rather use a different Identity Keeper. These entities will be tasked with monitoring any changes in status. For example, if the user is added to the Specifically Designated Nationals (SDN) list, the Identity Keeper will need to revoke the requisite credentials. Since revocation is done simply by issuing a transaction, this process will be very agile.

Lastly, Identity Keeper will be required to store the Attributes and also relevant PII. Since the Attributes are not revealed publicly onchain, they cannot be recovered if they are lost. Thus a user's wallet must be able to query and fetch them the Identity Keeper via an API. Also, a regulator, with appropriate due process[5] may at times request the PII under procedures established by the Identity Trust Anchor. Thus this storage is a critical task, and Identity Keepers will have an ongoing relationship with a user as long as their Attribute Credential is valid. Under the DSI Regulatory Model, Identity Keepers will maintain rigorous storage procedures in accordance with best practices, relevant law, and ethical treatment of data. For example, Identity Keepers will be contractually obligated to not abuse this data by selling it or performing analytics.

3.2 Attribute Regimes

Below we outline several example Attribute Regimes that would be needed to create a Tokenized Securities Regulated Zone. This list is not necessarily exhaustive nor are the descriptions complete. We envision that these Attribute Regimes will gain wider adoption into a variety of Regulated Zones adhering to the DSI Regulatory model, allowing users to access a wide variety of assets with a single onboarding experience.

Standard Verified Identity Attribute Regime - This Attribute Regime will consist of basic PII about a user that is normally collected during a CIP process: their name, date of birth, nationality, etc. It will also indicate if the individual is not listed on the United States Specially Designated Nationals and Blocked Persons List (SDN List) or other foreign sanctions list.

The idea is that this Standard Verified Identity Attribute Regime will be suitable to grant access to Regulated Zones for RWAs in many jurisdictions across the globe, not just Tokenized Securities. It will enable CIPs that are consistent with the relevant FATF Customer Due Diligence Recommendations.[6] In the DSI Regulatory model, this Attribute Regime of this sort can become the default identity standard used in most Regulated Zones. Indeed, the information present in the Standard Verified Identity Attribute Regime should not be very controversial and thus receive wide adoption.

---

[4]Such as the identity portions of FATF Recommendation 10.

[5] Identity Trust Anchor will set guidance on what constitutes sufficient due process along with the appropriate procedures and portals.

[6] The identity portions of FATF Recommendation 10.

Standard Verified Entity Attribute Regime - Similar to the Standard Verified Identity Attribute Regime, this Attribute Regime that will be used for organizations. As with other users, entities that wish to hold assets in the Tokenized Asset Regulated Zone must undergo a KYB process. We intend this Attribute Regime to become a widely adopted standard used in many Regulated Zones. This Attribute Regime will also record if the entity performs custodial services.

Investor Status Attribute Regime - This Attribute Regime will indicate classifications like "Accredited Investor" or "Qualified Purchaser". This Attribute Regime will be used to restrict ownership for Regulation D offerings or similar securities in the Tokenized Asset Regulated Zone.

3.3 Liability

- IKs and CCs have a ToS contractual agreement with the thrust anchor to perform the task they need to do.
    - This ToS would have an indemnification clause
    - IKs and CCs would have variety of liabilities if they wantonly violate the standards set forth
    - The Identity Trust Anchor would be liable for the standards and rules that are set
- If a bad actors are let into the system, who is liable?
    - Obviously all parties are potentially liable,
        - indemnifications only aligns incentives
    - In order for failure, two things need to happen, and these parties would be found liable
        - If an Identity Keepers flagrantly violating ToS
        - If the Identity Trust Anchor no ejecting such Identity Keepers
    - Individual projects must be reasonably sure that these things dont happen

The Standard Verified Identity Attribute Regime will also indicate whether or not the holder is agreeing to the Terms of Use agreement set forth by the Identity Trust Anchor. In short, users will agree to a myriad of reasonable conditions:

- The user is not misrepresenting themselves to the Identity Keeper
- The user does not currently have another Standard Verified Identity Attribute either from a different Identity Keeper or with a different DID
- The user will not commit fraud within any Regulated Zone using these credentials
- The user will not engage in financial crime or market manipulation
-

3.4 Economic Incentives

Identity Keepers are able to monetize their role of onboarding and maintaining users. Their role is closest to existing KYC service providers, making their business models relatively portable to the DSI Regulatory Model. Likely Identity Keepers could include centralized exchanges or other regulated trading venues, banks and traditional KYC vendors, or specialized identity verification or credentialing firms. These are entities that have experience in collecting user PII. It is important to note that unlike a purely static registry, an Identity Keeper is performing ongoing, active services such as running CIPs, maintaining and revoking credentials, and responding to relevant updates over time (for example, sanctions regimes).

One primary revenue stream can come from onboarding fees, which cover the costs associated with performing Customer Identification Programs and the subsequent issuing and active management. Management fees cover the costs of determining if any credentials should expire, if for example, a user is added to a sanctions list or a user needs to reassert their investor status. Similarly, Identity Keepers may implement a PII rental storage model, requiring a periodic fee from users to maintain their credentials, with revocation as a consequence of non-payment.

Additional fees can be generated on a per-credential and update basis. This includes charges for issuing new Attribute Regimes, which grant access to additional jurisdictions. Furthermore, fees are applied when credentials need to be refreshed or upgraded due to changes in the underlying user information. For institutional clients that require mass user management, such as exchanges or platforms with pre-vetted users, the Identity Keeper can offer subscription or membership models tailored for large-scale onboarding and ongoing maintenance.

Finally, Identity Keepers can participate in referral or revenue share agreements. These arrangements would be established with wallets, venues, or other integrators that encourage users to default to a specific Identity Keeper within the regulated zone. These agreements are subject to strict standards and rules specifically designed to maintain a competitive environment and prevent the formation of walled gardens or oligopolies among service providers.

4. Transaction Monitoring

4.1 Risk Flags

Some regulatory objectives can be achieved by knowing a user's identity information, for example sanctions enforcement. However, other regulatory concerns, such as market manipulation or money laundering, are dynamic and require monitoring transaction patterns. To that end, GAP enables Service Providers called *Transaction Monitors* to scan smart contract calls and issue *Risk Flags* when it detects possible abuse. Potentially, Risk Flags could indicate patterns including market manipulation or money laundering, however these flags can be much more nuanced.

For each contract monitored, a Transaction Monitor will maintain an *Onchain Risk Database* which lists the Risk Flags for that contract. Transaction Filters combine a user's Risk Flags along with their Attributes to assess whether or not the User may call the transaction. Although a Risk Flag can be a simple blacklisting function, these flags can be more versatile. First, Risk Flags can express degrees of risk, and a Transaction Filter can decide the appropriate threshold for action. Furthermore, the Transaction Filter also considers PII contained in Attributes: the Transaction Filter could tolerate more Risk Flags from users from low risk countries.

Occasionally, Transaction Monitors will make false positives, and flag users that should not be flagged. If this happens, a user will be able to appeal to a Transaction Monitor off chain to have their flag removed.

Certain smart contracts in a Regulated Zone will be required to have a Transaction Monitor to detect certain types of behaviour. Specifically, it will define a precise list of Risk Flags which the Transaction Monitor can use. Each Transaction Monitor will monitor and analyze calls to their smart contract in order determine if a user should be flagged. To perform this analysis, Transaction Monitors will maintain a private, offchain database of the risk profiles. Although the flags are set by the Classification Regime, the Transaction Monitor has flexibility and leeway in deciding the specific patterns they use in their analysis. This will serve to obfuscate the methods of the Transaction Monitor from attackers[7].

For example, in order to achieve a regulatory objective like AML screening, the Classification Regime might define the flag 0001 as "High Risk Structuring[8]." The Transaction Monitor then can define the patterns they look for that suggest high structuring risk. The Transaction Monitor then records the appearance of these patterns in their private risk database. If a user exhibits enough of these patterns, then the Transaction Monitor assigns them the 0001 flag on the Onchain Risk Database.

How does a Transaction Monitor record a user's flags on the Onchain Risk Database? Since ZK proofs obfuscate the relationship between user PII and their transactions, a Transaction Monitor does not know who issued each transaction. We address this issue in the following section.

4.2 Pseudonyms, Privacy, and Local Transaction Monitoring

Currently, automated address based blacklists are impossible with DeFI since a user can always simply create a new address. This problem also is more generally applicable to Risk Flags. GAP solves this problem using an identifier called a *Pseudonym*: a user generates a Pseudonym

[7] For example, if a criminal knew the exact patterns that were tracked to detect money laundering, then they would simply adjust their techniques to avoid these patterns.

[8] Structuring is a money laundering pattern where large transactions are broken into smaller, less suspicious transactions.

deterministically from their DID and a smart contract address. A Pseudonym cannot be forged, and every caller of a smart contract has a unique Pseudonym. Very importantly, no one can derive the original user DID from the Pseudonym[9].

When a user calls a smart contract in GAP, it includes the Pseudonym for that contract[10]. Thus, a Transaction Monitor can create a Pseudonymous log of contract calls based on these Pseudonyms, and this log is the primary object of their analysis. Furthermore, Risk Flags are assigned to user Pseudonyms, which solves the automated blacklist problem discussed earlier.

Pseudonyms allow a Transaction Monitor to reason about individual users without knowing anything about user PII. Thus, GAP not only effectively erects a wall between users' PII and their transaction patterns, a user's different contract specific transaction patterns are also fundamentally separated from each other. Even if one Transaction Monitor's pseudonymous data leaks, it will reveal very little since every other Transaction Monitor uses a different set of Pseudonyms.

Thus, Pseudonyms allow us to solve another problem in blockchains: the growing panopticon of blockchain analytics. Blockchain analytic companies leverage the current public nature of blockchains to analyze user behavior and source of funds. We call this *Global Transaction Monitoring*. This work has been extremely valuable to law enforcement and to combat financial crime onchain. However as blockchains receive greater adoption, Global Transaction Monitoring raises fundamental privacy questions.

Via Pseudonyms, GAP introduces the concept of *Local Transaction Monitoring*: the monitoring of all calls of a single smart contract and indexing behavior using Pseudonyms. Local monitoring is a revolutionary concept that enables privacy, because it allows the transactions and the smart contract state to be encrypted, as long as the Transaction Monitor has the ability to decrypt it. Local Transaction Monitoring also prevents honeypots of private transaction data from being collected and abused

Because of the privacy tools, Local Transaction Monitoring is quite different from Global Transaction Monitoring. For example, consider tracing the history of funds. To prevent money laundering, Global Transaction Monitoring traces the sources of wealth on public blockchains. In response, a criminal can attempt to obscure the history of the funds by moving them through complicated patterns. However, with Pseudonyms, such tricks do not work; the user will present the same Pseudonym for each transfer, making the history of the funds very clear. Moreover, in a Regulated Zone, if assets are subject to Local Transaction Monitoring and credential based

---

[9] The astute reader may notice that a user can simply create more DIDs. However, GAP allows each user to receive one Attribute Credential per Attribute Regime under each Identity Trust Anchor. So credentialed DIDs, and thus also their Pseudonyms, are Sybil resistant. See GAP White Paper, Appendix III.

[10] For privacy sake, the Pseudonym is encrypted so only the Transaction Monitor can see it. Otherwise, anyone could perform this analysis.

Transaction Filters, participants can be confident that all funds within that Regulated Zone are clean.

Note that Global Transaction Monitoring still has a place within the DSI Regulatory Model, since we do not expect our model to swallow all of DeFi. For example, a DEX between ETH and a tokenized security would need a global Transaction Monitor to ensure that only clean ETH is deposited into the DEX.

4.3 PII Referrals

The DSI Regulatory Model maintains a strict separation between user PII held by Identity Keepers, and the fragments of transaction data held by Transaction Monitors. This separation offers strong protections against abuse and theft. However, to enable a variety of regulatory objectives, a regulator or other relevant party may need to be able to know the identity of a user.

The DSI Regulatory Model resolves these conflicting mandates through the use of referrals. Along with their Pseudonym, every user will encrypt in their transaction the their Identity Keeper's unique identifier. Thus, a transaction monitor can record the Identity Keeper associated with each Pseudonym, this allows them to refer any identity request by a regulator to the appropriate Identity Keeper.

If necessary, the Identity Keeper can also furnish the requestor with the user's *private salt*, a secret key used to derive each contract Pseudonym. With this value, the regulator can go to any Transaction Monitor and query all transaction data for this Pseudonym. In short, a regulator can obtain via many requests all PII and all transaction data across all Regulated Zones for each individual single user. These requests strike a balance between a regulator's prerogative and an individual's protection from an over zealous regulator.

Under the DSI Regulatory Model, the process governing PII referrals will be strictly enforced, ensuring that the requestor has the appropriate authority and has undergone due process. There are instances under state law where other entities may need to periodically collect the names of shareholders of securities, for example before a governance vote. If granted access to the data, the requestor should only receive the data that they need. In particular, the private salt will be closely guarded by the Identity Keeper.

4.4 Transfer Agents

Under the DSI Regulatory Model, Transaction Monitors for Tokenized Security contracts will perform extra duties: specifically they will act as a Transfer Agent. Recall that Transaction Monitors have a pseudonymous log of all contract calls. For Tokenized Security contracts, this log can act as the source of truth from which they can build a Master Security Holder File. Thus, the blockchain will be a vehicle for sellers to register transfers of security ownership to purchasers.

Unlike in traditional finance, Transfer Agents in the DSI Regulatory Model will not hold any PII, and thus they maintain a pseudonymous Master Security Holder File. However, these pseudonymous records will still allow them to perform their traditional roles as Transfer Agent: furnish records necessary for owners to exercise their entitled rights. They can facilitate the distribution of dividends and enable voting. If necessary, the Transfer Agents can communicate with owners via either Identity Keepers or potentially messaging services hosted on blockchain infrastructure. Also, as discussed in the last section, Transfer Agents can relay any request for owner PII to the appropriate Identity Keeper.

Transfer Agents will also have the important role of arbitrating any consensus disputes. Although these events should be rare, forks and consensus failures can potentially create ambiguity of ownership. For example, consider the Ethereum Classic Ffrk after the DAO hack of 2016. In this instance, the Ethereum community decided to rollback the Ethereum blockchain to reverse the hack, and the Ethereum Classic fork continued without the rollback. In such an event, which fork would be the true record of ownership for a Tokenized Security? Under the DSI Regulatory model, the Transfer Agent can arbitrate ownership in such difficulties.

4.5 Economic Incentives

Transaction Monitors serve a crucial function by providing behavior-based risk intelligence and ensuring market integrity, which they can effectively monetize. Transaction Monitors must be profitable else the Regulatory Model will not be sustainable. The potential fee models for these monitoring services are diverse and flexible, accommodating various platform needs. These include venue-level monitoring agreements, where entities such as Decentralized Exchanges, issuance platforms, and lending protocols pay recurring fees for comprehensive Anti-Money Laundering and market integrity coverage over specified contracts or markets. Alternatively, a per-transaction or per-proof micro-fee model involves embedding small, transparent charges, typically a few cents or basis points, whenever a Transaction Filter queries an Onchain Risk Database to verify a Zero-Knowledge Proof (ZKP). This latter model is particularly well-suited for high-volume platform flows.

Alternatively, to lower transaction fees, projects can subsidize Transaction Monitors themselves via a subscription model, where projects pay a monthly or annual fee for continuous coverage across multiple contracts or Regulated Zones. This comprehensive subscription can include value-added services such as incident response. Further monetization streams include integration fees, which are flat payments made by projects to cover the initial setup of monitoring services, deployment of the Onchain Risk Database, and other necessary infrastructure. Projects maintain the flexibility to determine how much of the total cost they cover directly to minimize end-user fees and how much is passed on to the users themselves.

The providers likely to offer these monitoring services include specialized blockchain analytics and chain monitoring firms, compliance technology providers, and compliance consultants. Many of

these firms already offer risk intelligence and monitoring services off-chain, the DSI Regulatory Model is a vehicle to increase their market share. Furthermore, larger exchanges or Decentralized Finance (DeFi) teams may choose to vertically integrate monitoring capabilities.

It is conceivable for a DeFi project to be their own Transaction Monitor, assuming of course that they follow the appropriate procedures. Like the other roles in this protocol, the Transaction Monitor market should be accessible and competitive, ensuring good service for users, and thus allows for projects to vertically integrate service provider roles.

5. Contract Certifiers

5.1 Classification Regimes

GAP supports the creation of *Classification Regimes* that enumerate *Contract Classes*. Besides letting a wallet know which contracts belong to a Regulated Zone, these Classes allow a contract to dictate with which contracts it can be composed. For example, a Transaction Filter can require an asset to only be deposited into a Contract Class with the same Transaction Filter, preventing a user from bypassing a Transaction Filter by wrapping the token .

Classes can be based on the functionality of the underlying smart contract, and also by the real world obligations of the deployers of the smart contract. For example, the deployer of a tokenized security contract may need to file an S1. Classification Regimes can also reference Attribute Regimes to specify the categories of users that can perform specific function calls on different types of contracts.

The most important example of a functional requirement would be a filtering mechanism (revisiting in Transaction Filters) that requires the caller to possess particular attributes and which smart contracts it can be composed with. As an alternative example of a functional requirement, many[11] have argued for a clear distinction in regulations between contracts with and without centralized points of control. A Classification Regime can define classes that distinguish between such contracts

In the DSI Regulatory model, Classification Regimes effectively define a Regulated Zone, which is a collection of smart contracts that interoperate together to achieve unified regulatory objectives. The Classification Regimes allow contracts to be compliant in two ways. First, to belong to a certain compliant class of contracts, a contract must conform to the requisite requirements. Second,

---

[11] Reddig, Rebecca; Mosier, Michael; and Gilman, Katja. "Genuine DeFi as Critical Infrastructure: A Conceptual protocol for Combating Illicit Finance Activity in Decentralized Finance," available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4607332

Classification Regimes allow contracts and users to interact only with other compliant contracts. Thus regulatory objectives can be met via cooperation.

The Class, and hence boundaries of the regulated zone, are indicated by *Classification Credentials*, which are issued onchain to indicate the classification of a contract under a Classification Regime. Classification Credentials play a crucial role in maintaining a Regulated Zone. For example, without them, a Certified Asset in the AM/CFT Classification Regime could be deposited into a contract without a Transaction Filter. This would allow anyone to bypass the AML/CFT controls, in the same way that through banking can be sometimes used to violate sanctions law.

To maintain the integrity of its Regulated Zone, GAP enables an administrator called the *Contract Trust Anchor* to control who issues Classification Credentials under its auspices. Specifically, each Classification Credential lists a *Contract Trust Anchor* under whose authority the Credential was issued. The entities it gives permission to issue Classification Credentials are called *Contract Certifiers*.

Contract Certifiers are the gate keepers that allow smart contracts into the Regulated Zone. By issuing a Classification Credential, they certify that the contract meets all the requisite criteria. Furthermore, as a Service Provider, Contract Certifiers, like Identity Keepers, must Register with Contract Trust Anchor and agree to uphold their rules and standards. The Contract Trust Anchor will periodically audit Contract Certifiers to ensure that their standards are met. This ensures the entire Regulated Zone is effectively achieving the desired regulatory objectives.

What exactly must a Contract Certifier check? First, they will make sure any real world obligations are met. For example, for a contract to be certified as a Tokenized Security, the deployer may be required to file an S1 with the SEC. Similarly, if a smart contract has a centralized point of control, the regime may require the project developing it to register as an MSB. Contract Certifiers would also certify that the source code is publicly available and well documented, so that users can have transparency in their investments.

The Contract Certifier must certify that all functional requirements are met. In particular, they will also have to certify that the contract has no malicious back doors or ways to bypass any functional requirements such as the Transaction Filter. This includes looking for secret wrapping functions, or calls to unregulated smart contracts. This certification will require a smart contract audit for compliance (this is different from a typical smart contract audit for bugs and vulnerabilities). This audit does not have to be done by the Contract Certifier directly, but they must ensure that a reputable audit takes place.

Contract Certifiers, Classification Credentials, and Classification Regimes are analogous to Identity Keepers, Attribute Credentials, and Attribute Regimes. However, one notable difference is that we do not need the DIDs representing smart contracts, since a smart contract address is a suitable static identifier. Moreover, the machinery supporting Classification Credentials is simpler since no privacy preserving mechanisms are needed.

Also, under the DSI Regulatory Model, we assume that there will be many more Contract Trust Anchors than Identity Trust Anchors. Indeed, we envision standardized Attribute Credentials, such as outlined in the Standard Verified Identity Attribute Regime, to be widely in Regulated Zones in jurisdictions around the world. However, different jurisdictions, interpretations of the law, and risk appetite will cause greater fragmentation amongst Classification Regimes and Classification Thrush Anchors.

5.2 Example Classification Regimes

Below, we give two examples of model Classification Regimes that can be used to build a Regulated Zone for Tokenized Securities.

AML/CFT Classification Regime - This regime can be used to comply with AML/CFT laws for a wide variety of RWAs. This regime classifies contracts into three general categories

- Controlled Assets: These will be token contracts that have the appropriate AML/CFT controls. Specifically, they will have
    - A Transaction Monitor that is searching for money laundering or sanctions evasion
    - A Transaction Filter requiring:
        - Users have a Standard Verified Entity Attribute Credential and have not been flagged by the contract's Transaction Monitor
        - The token can only be deposited on other contracts certified under the AML/CFT Classification Regime.
- Genuine DeFi Protocols: These will be generic contracts with no independent control[12]. These contracts must have
    - No centralized point of control
    - A Transaction Filter requiring users have a Standard Verified Entity Attribute Credential
- CeFi Protocols: These are protocols that do have centralized points of control. These contracts must have
    - The controller must abide by the relevant laws such as registration as a Money Services Business (MSB)
    - A Transaction Filter requiring users have a Standard Verified Entity Attribute Credential

The actual specification for this regime would be far more specific than what is written above. It will be designed to effectively thwart money laundering and enforce sanctions. Moreover, it is consistent with the various participants' obligations.

[12] As defined by Rettig, Mosier, and Gilman https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4607332

Why would contracts opt into this Classification Regime? This is a subtle question. The authors do not envision forcing all of DeFi into its Regulatory Model, nor do they believe that software developers should be subject to the BSA.

First, many assets, such as US securities, require effective compliance programs in order to be tokenized, and thus it will be advantageous for their issuers to use a contract of the Controlled Asset Class. Other DeFi and CeFi contracts will join in order to service these tokens.

Second, this enables privacy friendly compliance. Under current guidance from FinCen, in order for a centralized exchange to allow a customer to liquidate a Convertible Virtual Currency on their platform, the exchange must be able to trace the history of the funds. This implies that the transactions must be monitored by a blockchain analytics service, precluding privacy. However, GAP is compatible with privacy technology. Since a Regulated Zone implementing the AML/CFT Classification Regime would be clean, any funds originating from there can also be considered clean.

Tokenized Securities Regime - This regime will allow participants to comply with securities law while tokenizing and trading US securities. This Classification Regime will be quite complex and may actually be instantiated as a collection of smaller more modular regimes. Generally, Classes will fall under the following general groups.

- Tokenized Securities Classes: These are issuer sponsored securities, where the security is issued onchain. Individual Classes of Tokenized Securities will be determined by their type and subsequent controls, e.g. a Reg D Contract Classfor Regulation D offerings. These contracts will need the following:
    - Certified as Controlled Asset Contract Classunder the AML/CFT Classification Regime
    - Issuer has appropriate registrations and disclosures
    - Must have a Transaction Monitor acting as a Transfer Agent
    - A Transaction Filter checking their Investor Status Attribute Credential if the security has certain restrictions
- Decentralized Exchange Classes: These DeFi contracts facilitate the trading of Tokenized Securities. They require the following:
    - Certified as Genuine DeFi Protocol: in particular, these contracts do not have centralized points of control
    - A Transaction Monitor and Transaction Filter performing Market Integrity screening: this includes checking for Sandwich Attacks, Wash Trading, or other manipulative patterns
- DeFi Lending Protocol Classes:
    - Certified as Genuine DeFi Protocol: in particular, these contracts do not have centralized points of control
    - Must have requisite functionality such as collateral requirements.

- General DeFi Class: An assortment of contracts that do not fall into the above categories. We envision potentially many different types of novel contracts deployed under this regime, and some of which may challenge classification. Their requirements are:
    - Certified as Genuine DeFi Protocol: in particular, these contracts do not have centralized points of control
    - Are not any of the above Classes
    - Is not a wrapper[13]
    - Other requirements may vary with the specific Class
- Centralized Contracts: these include contracts with centralized points of control. The controls on these contracts can vary wildly. However, registration requirements for regulated actors will be enforced.

This Classification Regime achieves many regulatory objectives and concerns, as demonstrated in the following table:

Risk	**Regulatory Concern**	**How GAP Addresses It**
Offering Restrictions	Ensuring compliance with exemption requirements (e.g., Reg D accredited investor limits, Reg S geographic restrictions, holding periods)	Transaction Filters automatically enforce investor eligibility and transfer restrictions at the smart contract level based on credentials issued by Identity Keepers.
Sandwich/MEV Attacks	Transaction ordering and onchain execution mechanics that adversely impact price fairness	Transaction Monitors detect MEV patterns; certified smart contracts implement execution fairness controls.
Market Manipulation	Flash loans, oracle manipulation, wash trading, and coordinated onchain abuse	Transaction Monitors flag abnormal patterns; integration with external oracle verification; Terms of Service remedies including ejection from TAC's Regulated Zone.
AML/Sanctions	Illicit finance and sanctions evasion through pseudonymous transactions	The AML/CFT Classification Regime offers robust protections: Identity Keeper credentials tied to identity verification and sanctions checks; automatic credential revocation for OFAC designations; Transaction Monitors detect laundering patterns.

[13] A wrapper of a tokenized security is itself, a security

Cybersecurity	Hacks, exploits, and unauthorized access to smart contracts or user assets	Contract Certifier audit requirements; formal security reviews for Software Publishers; immutable onchain logs for forensic analysis.
Liquidity / Volatility	Continuous 24/7 trading without circuit breakers amplifying price shocks	The ability to trade in DeFi doesn't replace one's ability to trade through a traditional exchange or a brokerage. GAP terms would make the risks of 24/7 trading clear for users of the system
Best Execution	Onchain execution mechanics versus traditional best execution obligations	The ability to trade in DeFi doesn't replace one's ability to trade through a traditional exchange or a brokerage. GAP terms would make the risks of AMM-based trading clear for users of the system
Pseudonymity	Enforcement visibility and ability to link transactions to real entities	Although they do not hold user PII, Transaction Monitors can refer law enforcement to the correct Identity Keeper to retrieve the PII under lawful request. Periodic audits and regulator access protocols will be provided for in Terms of Service.

5.3 Liabilities

DeFi projects may also choose to register themselves as a Contract Certifier so that they can certify their own smart contracts, and be under the direct supervision of Contract Trust Anchor, TAC. This would make sense for larger projects who do not wish to be reliant on some intermediary.

In the case where a contract is not self certified, the Contract Certifier will record the name of the Contract Sponsor: the entity that deployed the contract and with whom certain liabilities lie. Ultimately the certification process cannot be one hundred percent fool proof: even the most rigorous code audit can still miss a malicious back door. If such a back door is discovered, the rightful liability should lie with the Contract Sponsor who deployed the contract.

- IKs and CCs have a ToS contractual agreement with the thrust anchor to perform the task they need to do.
    - This ToS would have an indemnification clause

    - IKs and CCs would have variety of liabilities if they wantonly violate the standards set forth
    - Contract Trust Anchor would be liable for the standards and rules that are set
- Contract Sponsors (DeFi projects) are subject to ToS
    - Must satisfy the obligations in good faith set forth in classification regime
    - The Contract Sponsor is liable if they lie or misrepresent their code
        - If a Contract Certifier says that the code meets the terms of the classification, they are not liable if the code does not in fact meet classification. For example, if the code has a back door that is missed, then Sponsor has misrepresented the to Certifier
    - Trust Anchor is liable for classification itself
        - If Contract Trust Anchor not require a sanctions filter on tokenized securities, then it's their fault and they should be liable sanctions violations
        - This encourages projects to trust the classification system

5.4 Economic Incentives

Contract Certifiers play a crucial role in the regulated zone by classifying and certifying smart contracts that seek to operate within a specific Classification Regime. This function mirrors that of contemporary audit and compliance firms, but with the distinct feature of producing explicit onchain outputs, specifically Contract Classifications registered under the relevant regime.

The monetization potential for Contract Certifiers is diverse, encompassing several fee models. These include per-contract certification fees, which could be tiered based on the complexity, risk profile, or anticipated volume of usage—distinguishing, for instance, between simple wrapper contracts and complex, multi-asset venues supporting multi-hop routing compliance. Certifiers can also charge per-version recertification fees whenever a contract undergoes an upgrade that necessitates a review and attestation of the new code. Furthermore, offering retainer or support agreements allows for ongoing advisory services and continuous certification coverage for a set of contracts, including management of upgrades or incident response. Finally, Certifiers may offer bundled audit and certification packages through partnerships with traditional code auditors, legal/compliance firms, or cybersecurity vendors to deliver end-to-end solutions.

The pool of likely providers for this role is broad, including existing smart contract audit firms, compliance and regulatory advisory firms, and cybersecurity and risk management providers. Additionally, larger Decentralized Finance (DeFi) platforms or financial institutions with established in-house compliance teams may register as certifiers for specific regimes to manage their own needs. Within the GAP framework, certified contracts are the essential, composable components that form regulated venues and facilitate the secure movement of assets on and between them. As the demand for tokenized securities and other Real-World Assets (RWAs)

continues to increase, Contract Certifiers with high reputations will be positioned to compete effectively on factors such as speed, quality, and price.

7. Conclusion

Ive said what Ive said, and thats all Im gonna say. If you made it this far, you were probably obliged to read this document. If you need a recap, go reread the intro or ask your favorite LLM. In conclusion, conclusions are dumb.