**Project Background**

**Candidate Names: Discuss the marketing aspect with MINA experts.**

**ZK Proof Engine for Tokenization (ZK – PET)**

**ZK Composition Engine for Tokenization (ZK – CET)**

**ZK Proof Engine for Tokenization (ZK – PET)** —The platform ZKPET is a provable business process composition engine for real-world asset tokenization. SCF-RWA-Reimagined is a reference implementation of ZK-PET for supply chain finance, including international trade finance and insurance. It involves layers of proof composition to reduce the validation risk for financiers.

The platform reference implementation addresses MSMEs' lack of financial access, lack of privacy-protection methods for business-sensitive data, and lack of appropriate counter-party decision aggregation. This is an area where Western banks, other institutions, and increasingly institutional Defi want to participate in meeting global demand, particularly from the developing economies, but it is heavily under-penetrated due to a lack of transparency. Blockchain adoption has been limited, and the capabilities of this platform are a key enabler for RWA / Institutional Defi.

**Problem Statement:**

Centralized solutions have not been able to reach a global scale in to developing economies. These systems are fragmented with excessive delays and a high degree of inefficiencies. Beyond the technical aspects of provenance, audibility, and non-reputability needed for validations, Blockchain opens a new era of financial access networks, particularly for developing economies in all topologies, private, public, and hybrid.

**So, What is the problem in Finance, and particularly in Supply Chain Finance?**

The lack of wider financial access for borrowers, particularly in developing economies, is well documented. Even, traditional finance wants to get into this area earlier. Still, both the origination and the fulfillment have been in narrow quarters marred by a lack of access infrastructure, closely held exclusive networks, predominantly local. With the first wave of blockchains, the connectivity is improving, with a lot of promise, but there is a lot more ground to cover. Defi sounded good, but most credit in Defi has been predominantly overcollateralized lending, based on on-chain native crypto assets and only seemed to have helped native traders. origination and fulfillment.

The predominant issue has been validation risk for financiers. Even with the DLT based systems so far, there is very little in way of current solutions they do NOT go beyond a simple hash of a current process documents, which only marginally improves the situation, and does NOT include the deep data integrity of the underlying systems of proofs. For the borrowers, the issue is that they are having to do excessive documentation , without knowing anything about the process on which any decisioning is made on. Specifically, there are no capabilities to model dynamic possibilities arising out of DLT/AI-based transformation of the supply chain finance process, as these can shrink the time of efficiencies that allow for many dynamic ways of negotiating and re-negotiating payment terms in the delivery-versus-promise cycle.

Institutional Defi / and RWA, and tokenization in general, have spurred interest with increasing regulatory movements and awareness of real-world blockchain use cases possible with the underlying technology.

**IMPACT/ ECOSYSTEM:**

**Tokenization efforts are poised to grow exponentially, BUT if we must bring the next one billion people into Web 3, the use cases that are going to be helpful are the ones that are inter-twined with the lives of most people day-to-day, which is precisely the opportunity that Supply chain Finance brings.** Supply chain finance is the lifeblood of working capital for SMEs and MSMEs in most economies. In the MSME sector, financial access is still under-penetrated in all areas. For example, in India, a huge number of people are on the thin borderline of GST payments based on their revenues and are classified as proprietary business owners.

**Just how important are MSMEs ( Micro Small and Medium Enterprises)?**

In the International trade area alone, this is a 2-3 trillion financing deficit, and in general supply chain finance, it is estimated at 16 T.

**MSMEs are important globally (**[**Davies, Narayanan and Balasubramanian 2021**](https://armgpublishing.com/wp-content/uploads/2021/04/6-1-2021.pdf)**):**

* + **Over 95% of all companies are UK & US are MSMEs**
  + **90% of all businesses globally are MSMEs, they employ over 50% of all workers**
  + **88% of EU companies exporting to USA are MSMEs**
  + **They are even more important in developing countries like India, particularly in the context of exports/imports (**[**Chakravarthy, Bharathi, Khire, and Narayanan, 2023**](https://armgpublishing.com/wp-content/uploads/2023/04/9_SEC_1_2023-1.pdf)**): 30% of GDP (40% of emerging economies income globally).**
  + **Roughly the total addressable market is about 16 trillion USD – that’s the income generated SMEs globally!**

**Please refer to About ChainAim section for more details about the publications. ( in attachments ) .**

In general tokenization efforts, are expected to increase after the eBL law ( Sep 2023 ), MicA ( 2024 ), and anticipated regulatrory movement in 2025 in the USA. In all this, the English law leads the way with respect to the trade finance digitization, that works along side MLETR, and other regulations in different parts of the world.

**Why ZK ? Why MINA ?**

MSMEs' business sensitives need privacy-protected solutions, and Zero-Knowledge proofs allow for wider adoption by MSMEs to confidently share minimally required information on the blockchain with a wide variety of financiers. MINA allows for the balance of the on-off-chain and on-chain topologies and granularity aggregations for these kinds of enterprise data-heavy use cases for counterparty consumption. MINA is one of the few protocols that checks our requirement to fill the wide gap between the Web 2.0 and Web 3.0 systems to be able to conceive and build deep layers of aggregation and disaggregation of enterprise data as proofs.

**Proposal Overview:**

The proposal builds on the work from the ZK Montreal Hackathon win, and the tokenization data integrity win from XDC, another EVM chain., to address the privacy and scalability aspects of the solution using a combination of effective off-chain and on-chain design with MINA blockchain.

The MINA navigators proposal is to build the following components of the **ZK-PET Engine For Supply Chain Finance Tokenization**

**ZK PET DEEP COMPOSITION ENGINE FOR SUPPLY CHAIN FINANCE**

**ZK PET DOMAIN ORACLE REGISTRY**

**ZK PET BUSINESS PROCESS PROVER**

**ZK PET RISK MODEL PROVER**

**ZK PET DEEP COMPOSITION ENGINE FOR SUPPLY CHAIN FINANCE** consists of producing proofs for

1. layered identity (including local jurisdictional identity, domain-specific identity, and emerging global legal entity standards like GLEIF )

Is the candidate borrower a registered entity? in the local jurisdiction

Is the candidate borrower a global legal entity?

1. verification of the key title documents based on the **Model law for electronic transmission of records (MLETR) specifications. Key instruments** like the Bill of Lading, and other collateral documents like the consumer invoice, and other substantiative documents for the jurisdictions involved are critical for real world tokenization in the supply chain finance space. Verifications are needed not just for integrity of the source identification, but in supply chain finance in goes deep, and also includes

Is the instrument / document truly complying to the standards schema ? like ( digital container shipping association schema for bill of lading )?

counter-party sensitive data integrity – (for example, Purchase Order to Consumer Invoice)

Is the Bill of Lading in sync with the customer invoice,and is the customer invoice in sync with the PO in a privacy – protected proof.

1. layered compliance,

Are the borrowers and the associated entities compliant with export-import agencies.

Configurations for sanctions can be checked as well.

1. operational excellence indicators, including history
2. financial health proofs about the cash / asset balances and other financial metrics
3. proofs of association (being part of a deep supply chain network)

the financiers are inclined to support a supplier that participates in the global supply chain of well-known brands for running efficient supply chains

**ZK PET DOMAIN STANDARDS ORACLE REGISTRY**

This component is a registry of standardized digital negotiable instruments based on evolving regulations in the supply chain finance RWA tokenization space.

The primary’s business relationships have been with many industry standards groups, which are emerging the standards. The primary has working relationships with these industry standard groups in multiple jurisdictions. Since the start of the shaping of this proposal, initial conversations have happened with most of them, and they are showing interest, to onboard those APIs to ChainAim’s ZK PET These include APIs for standards and data providers in digital trade instruments, algorithmic contract types, risk model apis, and access paths to corporate registration, legal entity identifiers. Initially we will be working in jurisdictions with known apis, and emerging standards for income tax, and GST.

This registry provides validation of the data and the models from the source , which ZK-PET in turn attests and further composes aggregated proofs on them to meet the demands of the verifiers.

We expect this to extend in to other sources based on some of the MINA ecosystem partners, and other external partners, which we will cover in the ecosystems section (also having discussions with the MINA team on some of the ecosystem details).

**ZK PET BUSINESS PROCESS PROVER**

As the standards-based trade instruments are provided, these tokenization workflows need the deep content analysis based on global schema compliance, and attestations on top of them for the execution completeness and the order sequence based on the process definition ( including parallelism ) for start to end state of the process.

Per the industry practices, and for financier risk management, the specific templates for types of engagement and payments are modelled, for “negotiable”, non-negotiable types of interactions and any delivery-versus payments contract / guarantees.

For a given template , the expected flow is matched against the execution trace – the “witness” trace . The solution uses a standard for modelling these templates and mapping them to convert them into circuits and state-transition checks for producing proofs of execution of expected business processes.

**ZK PET RISK MODEL PROVER (a basic implementation )**

This module asserts and produces proofs based on the standards evolving in the space of next generation standards management that central banks are starting to use to model financial data and flows, based on credit risk, behavioral risk and market risk.

ChainAim has proprietary relationships with many of the work groups, and will produce the configurable service layer implementation serving as an oracle , based on these underlying evolving standards.

The proofs of the simulated cash flows will be modelled against desired risk tolerance.

These proofs address the critical Trade finance flows for Bill of Lading acceptance, which is a guarantee under English law ( which is the global trade law ), for the tokenization of the instruments and the value transfer.

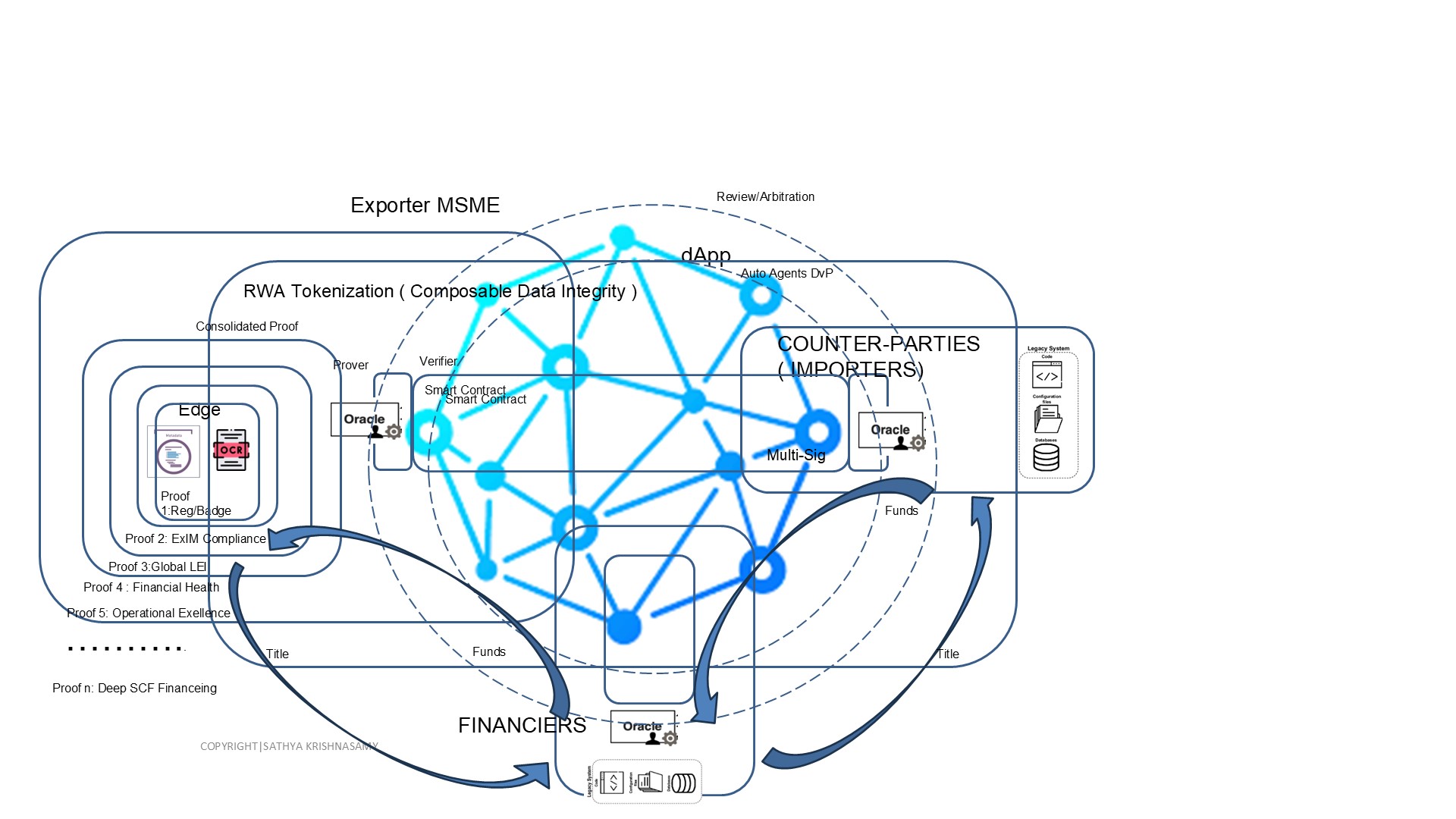
The same concepts equally apply to other kinds of insurance for business process flows, in insurance including primacy ( primary / secondary ) evaluations and agreements at the business levels, for primary/secondary.

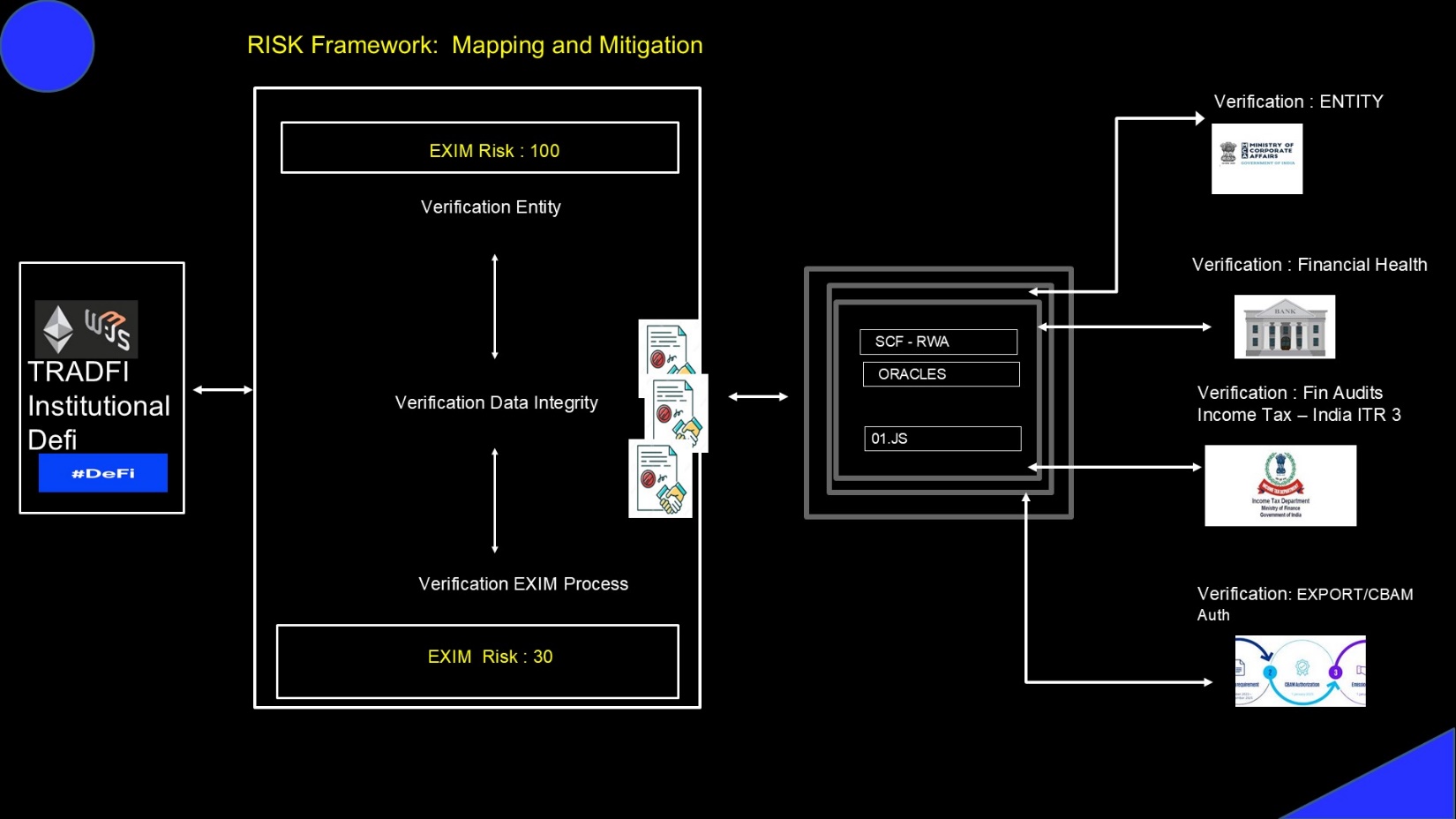
**Audience**

This is a multi-sided network platform that includes MSMEs( Both Buyers and Sellers ) and financiers, and many other web 2 platforms, brick-and-mortar factoring companies, which need an on-ramp into web3 tokenization. Over time, the regulatory bodies could participate in the network.

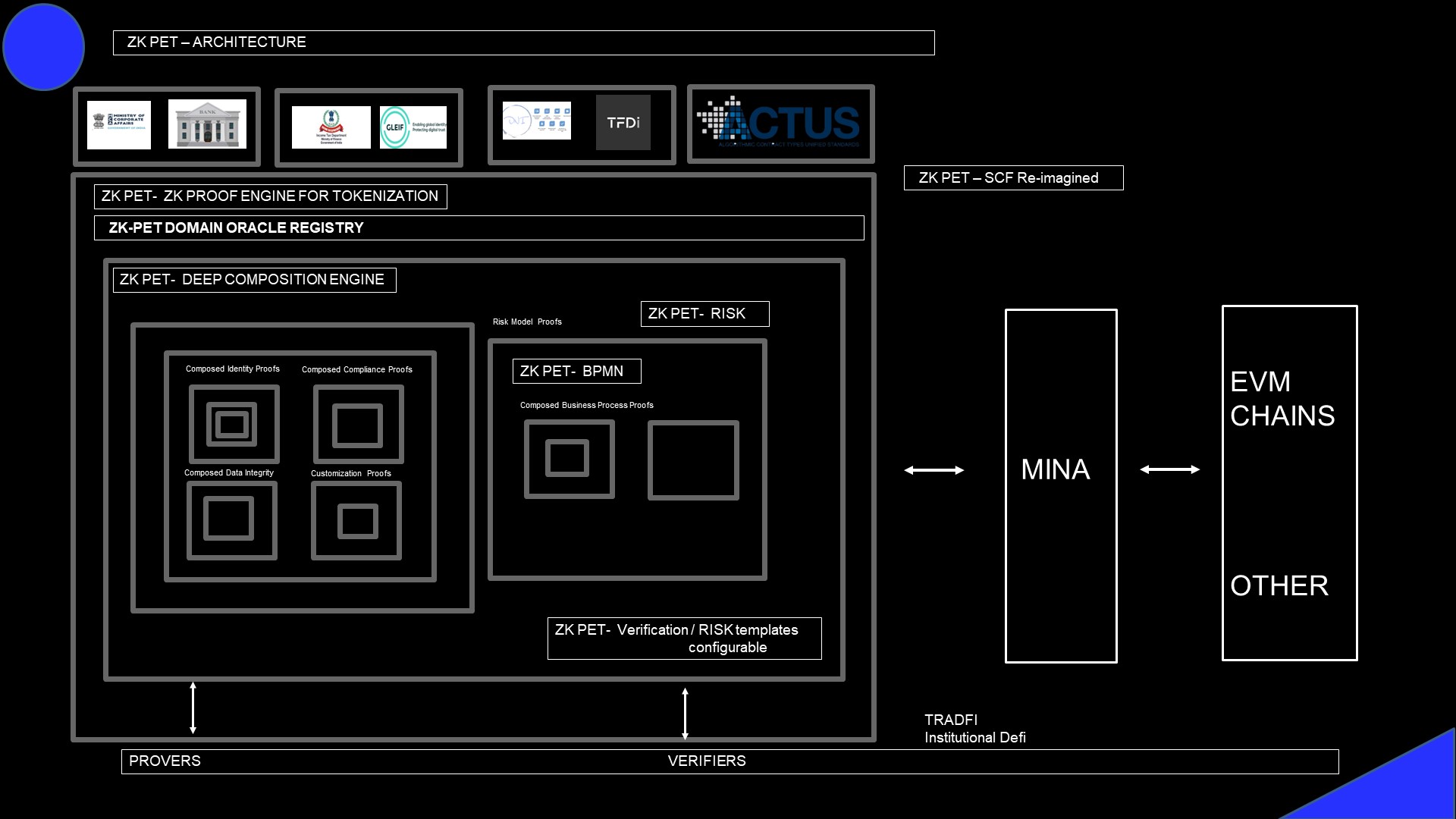
This is where the scale comes in, as this includes single-owner proprietary companies, and their accountants who are motivated to get their GSTN credits on time, for both domestic and international operations. ChainAim is already in talks with SMEs / MSMEs looking for better options than their current options which even in developed countries take significant amount of time, and cuts in to 20-40 % on rotational velocity, and in developing economies, we have seen rates as high as 60 percent for even a 2 week advance of working capital.

**The Schematic:**





**Architecture:**

****

**Unique Aspects of the Solution:** The tokenization space is still evolving, and the institutional interest is starting, but there are no detailed solutions. The few that have surfaced are very trivial and shallow that simply hashes the documents on which a token is likely associated (or) a simple band-aid on existing inefficient processes.

However, in reality, the trade finance area needs a detailed integrity analysis. Also, the structures needed for effective tokenization and institutional defi need a range of capabilities between the Web 2.0 and Web 3.0 layers. These need to aggregate and disaggregate information in a privacy-centric way in a B2B2C environment that assembles the needed information for the needs of the financiers in the institutional defi space.

ChainAim has been working with multiple industry standards groups to identify and formulate the standards in this area including Trade Finance distribution initiative ( TFDi ), Algorithmic standards for systemic risk modeling ( ACTUS ), Global Trade Analysis Protocol ( GTAP ) and many others including operational supply chain. Also, we have been in talks through our strategy consulting advisory Infisum Modeling, to many governmental agencies, ministries and trade organizations and EXIM banks in many jurisdictions. We are also following the regulations very closely and mapping them meticulously for the details that are needed for high fidelity.

**Please refer to the deck, and the details in the Annexure on the Principals, and their publications on topics of payment integrity, emerging technologies, and strategy consulting.**

We are uniquely positioned to bring in the technical and the domain expertise needed to build a ZK Co-processer / Attestor for this tokenization. Though the reference implementation is targeted towards the supply chain finance, as we expect that to be in first waves of payment innovation, the architecture is designed to be super flexible for other types of enterprise data integrity for domains including payments, and delivery-versus-payments in many domains, but not at a superficial level, but truly answering the questions of actionable, provable privacy protected enterprise integrity at the right level of aggregation for multi-party computing. Another important distinction is the concept and the multiple level of proofs we have built during and since ZK-Montreal in Aug 2024, to show these concepts in multiple-levels of aggregation. This we believe strongly paves way for producing minimal data availability proofs for the maximum level of utility from a overall consumption and scalability point of view.

**Ecosystem:**

As indicated in the architecture schematic, our solution is designed as a collection of pluggable components that we expect will help us participate in and work with the overall MINA and emerging blockchain ecosystems.

First, we expect some components of our solution to be fully open-sourced. We expect some aspects of generic identity, compliance, and data integrity proofs to be fully open-sourced. At this point we expect that some service components will be in the areas of generic and basic standards of financial instruments (DSCA) and contract types for risk analysis like Principal At Maturity, FOREX, Loans etc.

We expect some domain-specific services to be initially run as a service and, with sophistication, open up for development sandboxes but a paid model for production services.

We have examined the ecosystem MINA protocol has developed, working, and continuously intend to use, and work closely with the following.

1. **MINA protocol:** Firstly, we intend to give a good view of layered composition that is needed for deep composition flows for real-world tokenization to

further advance MINA protocol for the off-chain / on-chain design constructs and give an indication of depth and layers that would be needed and practical ways to achieve them by adequately combining and balancing on-chain / off-chain designs and further developing the core protocol capabilities.

1. **Aligned Layer**: As our designs evolve and capabilities are built, we expect the proofs in MINA to be available to multi-EVM chains. We are developing our understanding of the MINA-aligned layer integration, and we think we would be able to build a capability for minimal data availability butsufficient sample sizes and the right type of data availability for the intended tokenization requirement utility while achieving modularity and scalability amidst the current landscape, constraints, and capacity roadmaps.
2. **ZK ON:** We have read through some of the ongoing work from ZK ON, and we intend to be an important player in this space as a predominant Attestor and Aggregator for the collaborative ZK. Our architecture is set up with pluggable Composition—Recurrsion modularity and Proof DA that can work with other Proof Providers and other Proof Consumers.

ChainAim is also familiar with Threshold cryptography, along with some work we did for encrypted data on off-chain / next-gen wallet designs for privacy-protected data and threshold-based security for reassembly sharding. With a deeper understanding of the MINA foundation and ecosystem, we intend and expect to add capabilities and participation.

1. **Reclaim:** We could possibly look into Reclaim protocol for the UI layer for the user interactions for Web content related flows, as needed, as a provider and an overall demand generator for the MINA protocol.
2. **ZK RegEx:** We expect to reuse some libraries developed in earlier efforts from the MINA protocol, like ZK-RegEx, and enhance them where needed.
3. **ZK OK:** We would like to get support for our marketing activities from the ecosystem ZK OK

From our efforts, we will be more than happy to extend the leverage we have with ChainAim’s partnerships to contribute to the overall ecosystem with MINA including systemic risk modeling

frameworks that central banks are starting to use( ACTUS), and other standards advancing tokenization in supply chain, payment integrity and insurance verticals( TFDi, DCSA, DNI etc. )

**QUESTIONS: We would like to work closely with MINA foundation to understand ZKAPP off-chain roadmap and MINA to other blockchain implementations ( particularly EVM based).**

**DESIGN:**

The ZK PET Tokenization Proof Engine provides the Proofs needed for the tokenization process for data and process integrity.

These programs are primarily designed as ZK Programs that can be composed and recurrsive, from self and different sources.

**ZK PET DEEP COMPOSITION ENGINE**

The ZK PET composition Engine produces different categories of proofs for business processes. The reference implementation for RWA Supply Chain Finance includes Identity, Compliance, Instrument Integrity for the data Integrity of the SCF data instruments that are the underlying data sources for tokenization, Business Process Correctness, and Risk Alignment proofs based on standards evolving in trade finance instruments and finance, and other custom proofs. Each classification of proofs uses composition and recursion for composing lower-level proofs that are based on data assimilated from different sources that the financiers need, that the engine sources work with minimally needed information, and produce the ZK proofs. For the entity the Proof Tree is constructed leveraging off-chain storage and the desired aggregation of proofs are submitted on-chain to MINA protocol, and other tokenization definitions that require the proofs in a data availability layer.

The following figure shows the summary structure of the ZKPET Proof Tree as a MINA o1.js Typescript composition/recurrsion implementation. The details of every kind of poof needed for the tokenization will be explained in the later section with a detailed view.

‘

**ZK PET Deep Composition Engine: Proof Tree**

A diagram of a diagram

Description automatically generated with medium confidence

These type of composition is used for entity identities and compliance, and other potential structural elements.

The following design diagram shows an example that was built during the ZK Montreal Hackathon., which has been continuously expanded for more layers of compliance.

A diagram of a basketball game

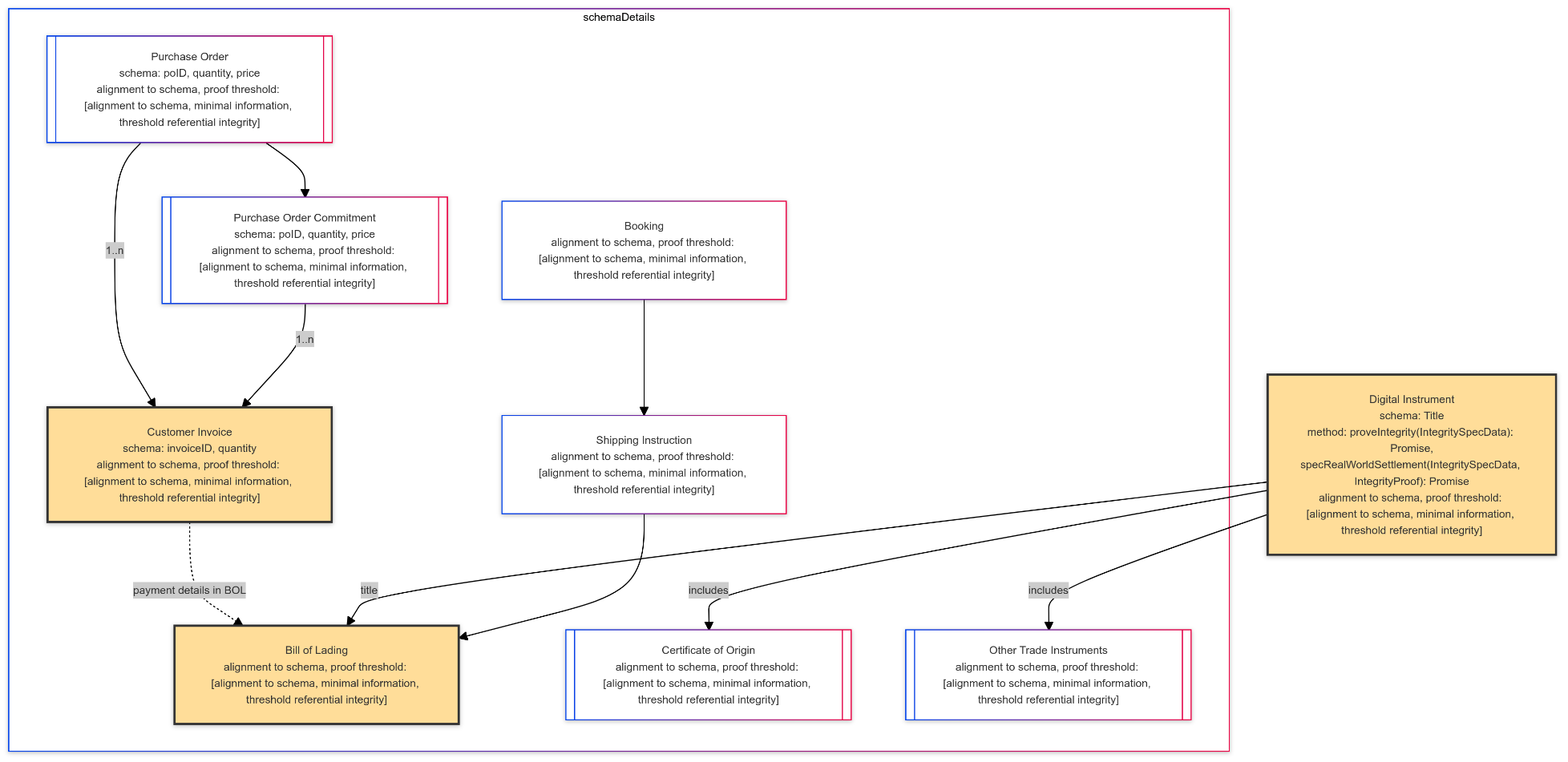
Description automatically generated

**ZK Deep Composition Engine: ZK PET Data Integrity Prover**

This capability proves the reliability of not just the content hash but the deep understanding of the contents themselves of the instruments behind the tokenization. In supply chain finance, the predominant Digital Instrument that is behind the title transfer and the settlement is typically the Invoice and the Bill of Lading( shown in brown color below), and could include trade instruments. The true efficiencies of DLT and AI transformation can be achieved by fulfilling the key decisioning requirements which are minimally needed, not much and not less. Hence this module has capabilities to define the global standards schemas behind these documents, for example DCSA for the key title document, Bill of Lading, and PEPPOL standards for e-invoicing, and other evolving standards for risk management, and trade finance initiation and distribution. The protocol schema definition, proof of alignment to schema, and identification of minimal data needed based on these global standards. The diagrams below highlight these tokenization critical instruments, defines the thresholds for proof, that takes in to account the alignment to the schema, the availably of critical data in the document, and identifying and disseminating the minimal required information and their metadata, that includes source validity, alignment to schema, and critical referential integrity between these structures.

**Why is this so critical?**

The absence of this rigor simply erodes confidence in the tokens that represent these real world enterprise data structures, which in the Web3 economy is a B2B2C flow, where the data owners are MSMEs. We have heard the need and noticed the void, and that led to the simpler implementation in the XDC EVM Chain. However, for full fledged high scale implementation the implementation needs a privacy protected and closer to Web2 connectivity, and hence these designs model them as MINA protocol typescript 01.js data structures for ZK proof generations and verifications.

****

**A diagram of a diagram

Description automatically generated**

**ZK PET DOMAIN STANDARDS ORACLE REGISTRY:**

The standards needed for the deep composition and the source of instruments needs for the deeper referential integrity for tokenization reliability is defined in the ZK PET Domain Registry. This registry will initially focus on the standards and sources needed for supply chain finance based on what is evolving in specific jurisdictions and the sources of information, including jurisdictions like India, Saudi Arabia, UK, Japan and the US. The ZK application will be configurable for jurisdictional compliance, by corridors. The corridors in immediate consideration is India-Saudi, India- UK ,and India-Japan, followed by India-US and other combinations.

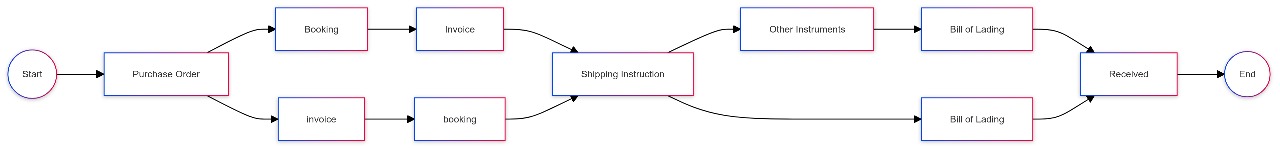
The standards include the any core standards for SCF including the digital container shipping association( DCSA), the e-invoicing standard( PEPPOL), Global Trade Analysis Protocol GTAP, ITFA digital negotiable instruments initiative, TFDi Trade Finance Distribution Initiative, ACTUS – standard framework for finance contract types.

The identity layers include personal and business identity primitives, registration proofs (ministry of corporate affairs-India(MCA), Director general of foreign trade-India(DGFT), Export Development Authority-India), Global Legal Entity Identifier Foundation ( GLEIF). The compliance layers include MCA, DGFT, LEI India, GLEIF, KYCAML registries, Sanctions Registries. GSTN Setu sandbox for GSTN and Income Tax data. This registry will expand into other jurisdictions, and we also expect this area to extend and collaborate with other global initiatives with different governments and identity solutions evolving, that we expect to leverage, contribute towards a wider registry ecosystem with MINA blockchain and overall blockchain ecosystem partners.

We are starting the registry with the above-mentioned end points Following is the initial schema and the sandbox details for the implementation to start for the needed functionality. We also expect some of the proprietary relationships that ChainAim has cultivated to on-board more participants along with their signature details for the source validation. We expect to also grow this with other MINA and other blockchain ecosystem partners. This is not intended to be a complete registry but a definition registry that refers this work and other work in the ecosystem that can be brought in through the ecosystem.

**ZK PET DOMAIN BUSINESS PROCESS PROVER:**

The following is a standards Modeling standards notation for a sample business process expected is shown in the BPMN 2.0 Modelling language in Figure below. This module will have an UI component that hosts templated such files for specified business processes the financiers, and other tokenization products would need to have proved. These templates can be fine-tuned and approved states are saved in the standards XML or JSON files. This engine understands the expected paths including all parallel flows, and fork and joins. The implementation of the BPMN circuit in o1.js for this sample is included in our github, and additional material for the model.

****

**Expected sequence of process:** a(cb|bc)d(ef|f)g extracted from the BPMN model

The actual execution trace is deducted from the instruments complying to the standards and uploaded or fed from the sources in the registry. The expected is compared against the trace witness executions which can be private input, and the ZK Proofs are generated based on specific states being available or not available, and the timeseries proofs check compliance to the state transitions. This component is so critical because it helps to make sure anything the financiers need to be checked for the integrity of the process before the tokenization can be checked, and gives a live monitor for any deviations much before the current status quo, with fragmented systems with no traceability. We intend to further advance other projects in the MINA ecosystem like o1.js , and ZKON for the steps and the compositions involved. We expect this to further enhance the concepts of Collaborative ZK that we see emerge in the MINA ecosystem. Please note that the basic instruments can be in any off-chain source or potentially another blockchain, but the proof systems can be generated and hosted in a succinct and privacy protected manner, including sampling models for data availability in MINA protocol , and through aligned layer in the Ethereum Ecosystem.

The following are an illustration of some samples of the accepted and rejected scenarios for the proof generation.

**Legend**

a = Purchase Order b = Booking c = Invoice d = Shipping Instruction e = Other Instruments F = Bill of Lading G = Received

**Trace accepted scenario:** abcdefg (accepted)

A diagram of a diagram

Description automatically generated

**Trace rejected scenario :** abfcdg (rejected)

**A diagram of a diagram

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

The sample shown will be expanded to different segments of the process, and composed in to and full end2end process, We expect to handle a set of templates for different processes in the securitization frameworks as they develop for the underlying assets, and the tokenization process based on whether they are security or commodity / utility tokens, and the proof of the business processes behind the tokenization.

**ZK PET RISK MODEL PPOVER:** The increasing complexity of financial markets and the growing need for risk management have necessitated the development of robust financial risk models. Also, slowly the Tradfi and defi systems are starting to show some signs of blending, and Institutional Defi is emerging as a concept With the advent of tokenization, there is increasing realization that are wide gaps between the Web 3 and Web 2 current day systems. The ZK PET Risk Model Prover provides capabilities to fill these gaps by running risk validation services for financiers for both TradFi, a frameworks that promote unified standards and financial contract types that can be common between transactional and analytical needs to simulate cash flows on time epochs for contract types, and provide proofs for financiers that the base scenario, and the risk events scenario. In the basic implementation, we expect to cover basic scenarios related to supply chain finance, leveraging ChainAim’s strategic working relationship with ACTUS framework simulations, and other risk datasets for supply chain finance.

The Key components include

**Contract Types**: Defines various financial instruments, such as loans, fixed or floating rate notes. forex, etc with specific attributes and behaviors.

**State Variables**: Captures essential characteristics of contracts, including loan amount, payment schedules, interest rates, and maturity dates, reference rate, and reset frequencies.

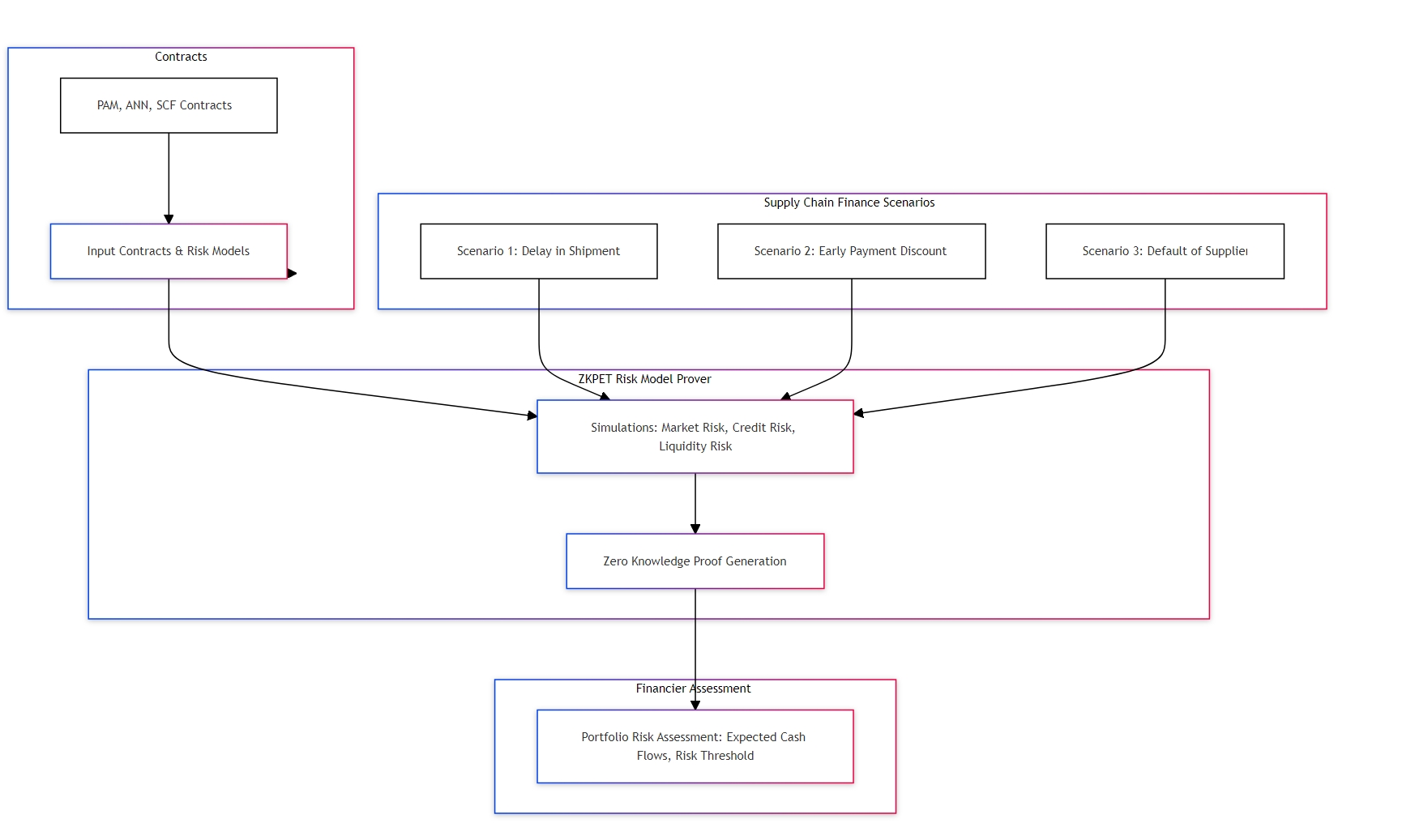
**Events**: Represents occurrences that affect the contract, such as payment events or defaults.

The ZKPET Risk Model Prover stores templated risk models, and can respond to financier risk models, and produce proofs for risk metrics validation and potential compliance proofs, without revealing granular characteristics or individual borrower data.

In a typical supply chain financing arrangement, a supplier (Importer in Trade Finance) provides goods to a buyer (Exporter in Trade Finance) on credit. The buyer, in turn, obtains financing from a financial institution to pay the supplier. ZKPET Risk Model Prover, models a receivable financing contract modeled using frameworks like ACTUS, detailing payment schedules, interest rates, and terms of repayment. The platform can generate, validate, and attest ZKPs for the financial institution to prove the validity of its credit risk models, demonstrating that the expected default rate of suppliers is within acceptable limits without revealing extraneous supplier details. We are also engaged in research of dynamic models these tokenization models produce like dynamic discounting, for working capital optimization for each of the entities. The dynamic discounting agreements will be analyzed to produce ZKPs that confirm the accuracy of expected cash flows from the receivables without disclosing the identities or amounts of the invoices involved

This is vast area for tokenization, depending on the underlying structure that is tokenized (securities and commodities), and we expect to design this in a much more extensible manner, but the first basic implementation will be in sync with the other aspects of the engine, to make it a compelling suite of capabilities that can be extended as a service.

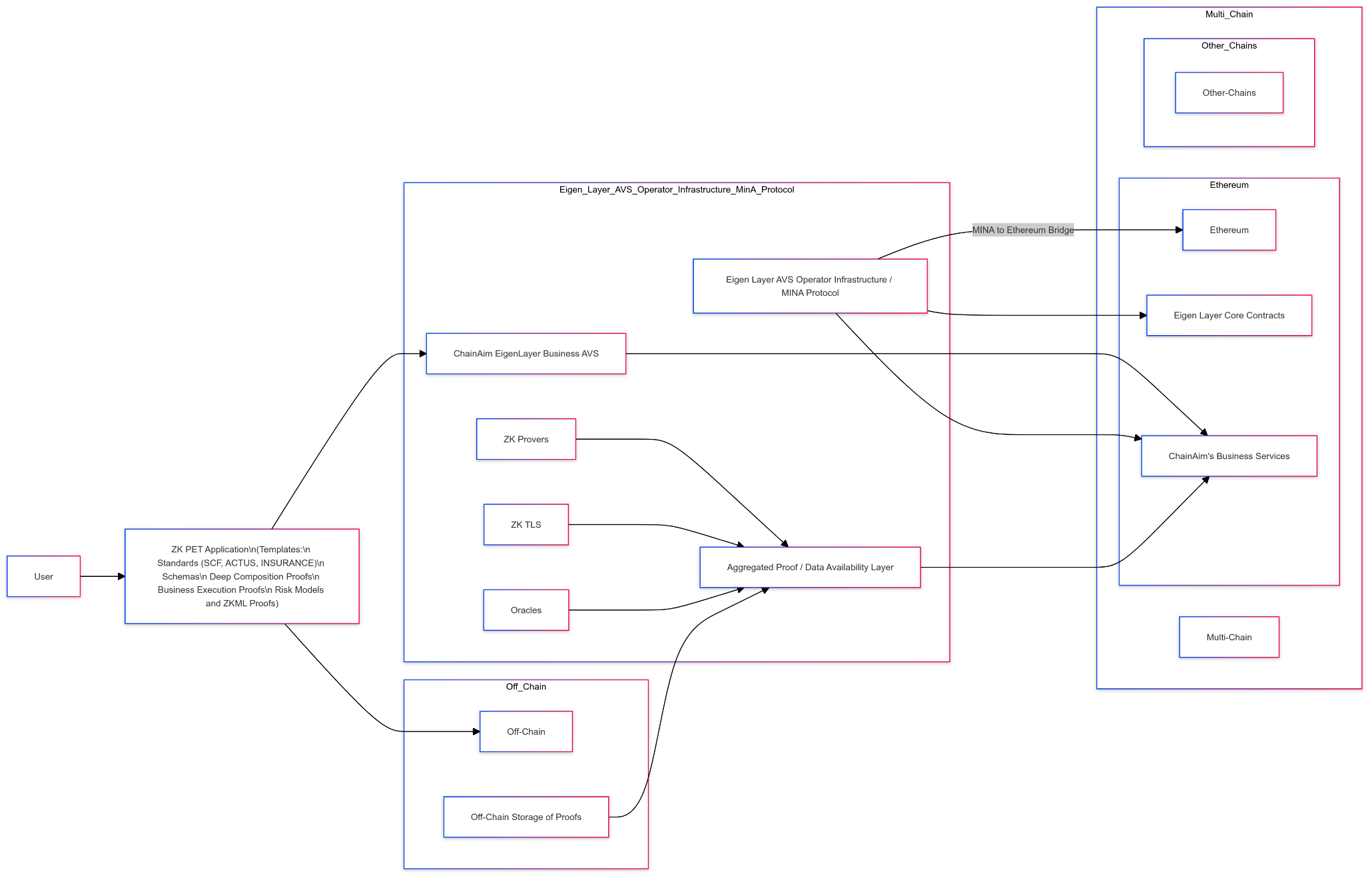
As explained earlier, the reason we are focused on supply chain finance is that we expect this area to be the next after cash and treasury bills in the line of tokenization that is practical in the tokenization spectrum based on the regulatory and legal movements we have been following and gaining a deep understanding of since 2023, and the regulations we expect to fall in place in the next 18 months. Given this is a very bread-and-butter for B2B2C flow, for advancing credit and needs risk analysis for simple things like cash advances and working capital credit analysis, we see the relevance for the gaps to be filled for tokenization in this area, and we think the off-chain and on-chain composition mechanisms with MINA / o1.js , and working with the ecosystem and the data availability for succinct proofs in a minimal data availability layer with substations that can be further indirected will be a huge demand generator.



**VISION FOR FUTURE**

The futuristic vision for ChainAim’s ZKPET ( Proof Engine for Tokenization ) is to be a key Tokenization enabler in multiple financial markets at the business source of truth layer, and be a connectivity hub between Web2 and Web 3 systems onboarding B2B2C users and enabling Institutional Defi, by running key components of a modular decentralized architecture. Most systems today are able to verify that the transactions were signed by a private key, but the content of those systems are not relatable to the notion of truth. As we move in to tokenization, and as the technical architecture layer emerges with ZKTLS, ZK Provers, Decentralized verifiers etc like Aligned Layer, we expect to play a role in the ecosystem, by being a multi-party attestation service, that can translate the tokenization demand side needs , by evaluating the standards driving tokenization and develop a layer of Business application level infrastructure leveraging MINA protocols off-chain / on-chain proving systems to store class of proofs and their applicability in the tokenization context, by making it available in a data availability and attestation layer from ChainAim’s ZK PET libraries. We also inspire to be a business source of truth layer for business standards, and alignment to standards service as a decentralized service leveraging re-staking and cryptoeconomic security layers such as Eigen Layer that helps accelerate the business layer components. Our Vision is to be the business source-of-truth and integrity layer. We are working on a provisional patent on this. This integrity layer can works with the ecosystem that builds on Proofs generated by us and other systems at the class of context-aware proofs for specific tokenization areas. Our Key focus is to put out source-of-truth attestations, minimal data definitions for the ecosystem based on schema and alignment to schema analysis ( these become extremely important in the context of regulatory mechanisms like HIPAA, BSA etc ), facilitating minimal data transfer between the ecosystem players including ChainAim, which can be re-attested for minimal data, and Zero Knowledge proofs for the decisioning context, and machine learning classification contexts for tokenization.

The following is an early-stage conceptualization schematic and we intend to review and enhance it working with the MINA team, and the ecosystem partners, as these newer concepts get flushed out, and the scalability parameters are tested out.



We expect to start with deterministic simulations for Proof of Risk Validation, with simple contract types, but extend them to comprehensive contract types, and advanced ZK ML models, and provide tiering of digital instruments for the client validation needs. As the tokenization aspects are proceeding in multiple blockchains in all combinations of Private / Public and hybrid ( Subnets), we intend to build an extensible system, that can use a ZK Proof system that payment entities / risk bearing entities ( financiers / insurers ) can bring their configurations to standards based risk validations.

**Work Already Done:**

Since the hackathon the following activities have been continued.

The Deep Composition Engine that was developed during the Aug 2024 hackathon, now is continuously getting extended for recursive identity and compliance circuits successfully.

Building on top of it, based on the O1.js tech stack, the wishlist we had during the hackathon to check for critical data content in a document, has been tested out. This gives us the ability to do Intra Instrument Integrity as well. The design for the deep composition using composition, recursion and off-chain structures have advanced.

The sources of data have been identified for jurisdictional and global identity and compliance for supply chain finance.

The Business Prover module has been charted out, including test proofs for expected and actuals using

Many standards have been already analyzed as part of detailed design including MLETR ( Model Law for Transmission of Electronic Records), DCSA for Bill of Lading, ITFA – DNI, Business Process Modeling Notation ( BPMN V2.0 )

Initial Conversations have happened leveraging ChainAim’s strategic positioning ACTUS framework for with Unified Financial Contract Risk Modelling, which we have received positive feedback. These concepts have been validated in many forums and with emerging networks such as Bulla Network who have started financing in the Ethereum Ecosystem, and had validated the need for such validation services as well, and have expresses initial interest in working with ChainAims ZK PET Engine.

**Proposal Timeline and Budget:**

Though there are many components to be developed, the design has proceeded far along, and we will be able to start development by Oct 1, or first week of October.

Deliverables can be planned in 4-week intervals.

End of Week 4 – Iteration 1 Complete - 25000 MINA

ZK Deep Composition Engine - Implementation of Identity, Compliance, Schema and Compliance to Schema. Finish complete specs on Inter Instrument Integrity

ZK Business Process Prover - Complete for Common templates in Supply Chain Finance / Trade Finance. UI Designs complete.

ZK Domain Oracle Registry - Design complete and connectivity with the different sources identified. Inter Ecosystem analysis complete.

ZK Risk Model Prover - Connectivity to the sandbox.

End of Week 8 – Iteration 2 Complete – 25000 MINA

ZK Deep Composition Engine – Complete and testing progressed.

ZK Business Process Prover - Complete including UI integration

ZK Domain Oracle Registry - Operational for identified data sources. Inter Ecosystem dependencies complete.

ZK Risk Model Prover - Connectivity to the sandbox, and basic contract types tested out.

End of Week 12 – Iteration 3 Complete – 30000 MINA

ZK Deep Composition Engine - Implementation of Identity, Compliance, Schema and Compliance to Schema. Finish complete specs on Inter Instrument Integrity

ZK Business Process Prover - Complete for Common templates in Supply Chain Finance / Trade Finance. UI Designs complete.

ZK Domain Oracle Registry - Implementation Complete and inter- ecosystem extensions planned for future.

ZK Risk Model Prover - Risk Models for basic SCF Done. Extension roadmap charted out for comprehensive tokenization of financial markets in priority order.

Documentation Complete.

We expect to deliver the, and Business Process Prover for basic templates as open source, ZK composition engine for templated SCF flows for open dev for other MINA ecosystem projects to use in test environments. Our focus is on the technical stack implementation, while we in parallel will work on the tokenomics aspects for further extensions as the regulations mature.

Given this is a full fledged capabilities for the platform, we expect the timeline to be roughly 3 months, and the budget at 80000 MINA.

Discuss further with MINA experts.

**Documents and Artifacts:**

**Current Github**

<https://github.com/chainaimlabs/ZK-SCF-RWA>

We are abstracting this in to a re-usable component architecture, around ZK-RWA-Engine for SupplyChainFinance, Insurance, Payment Integrity, DvP flows.

We will include the next version github, and a website soon as well.