**TRADEINS ORA : SOLUTION ARCHITECTURE AND DESIGN**

**Version 2 : Adding more details.**

**Problem Statement:** The EXPORT-IMPORT Cross-Border trade flow is a high regulation, low transparency, and high friction process flow, leading to barriers for capital markets to invest in cross-border supply chain finance hurting global MSMEs. All parties need a privacy-protected, yet integrity monitoring and front-loaded detection and resolution mechanism, which blockchains offer. However, the earlier versions of possibilities did not offer a complete solution.

**Design considerations:**

Public Blockchains without Privacy: Though it could timestamp provenance, entities were hesitant to put private data( PII, Business sensitivity data )

Private Blockchains: Though they gave private channels, the solution did not scale as the participants had many flavors of private data, that increased the number of channels, and these solutions could not get to the wider population.

Privacy enabled capabilities: are key requirements.

**Solution:** Our solution identity proofs, data discrepancy detection and resolution, and process checks to be proved to counterparties with ZK Oracles , Recursion and ZK process proofs.

Phase1

**ZK Oracles:**

1. **Identity:** Personal Identity Verification, Business Entity Verification, Business Badges Verification
2. **Compliance:** Financial Health Verification, Income Tax Verification, Compliance Verification – CBAM
3. **Inter Entity Data Integrity** : InterEntityData Integrity Verification and Reconciliation and visualizations.

**Phase 2**

**ZK Process/Standard contracts:**

1. The BPMN process definitions / ACTUS financial contracts : Proof of agreed definitions of workflow state and business financial settlement proofs calculated off-chain , checked for integrity and posted for on-chain state transitions if verified.

The implementation is targeting a discounting process flow.

**Considerations:**

In phase 1, the implementation focuses on the Zk oracles, where the TradeInsora will have a server component that performs the off-chain proofs/computations and compositions and signs the transactions onto the blockchain, focusing on the orchestration needed for the identity and reconciliation aspects., while we are researching the apis we need.

Even in this case, we will be leveraging other projects in MINA that have implemented things like ZK Email, ZK Authenticate, etc., to be able to preserve the root source of the documents.

In phase 2, we will be advancing to HTTPS-based implementations on the client side browser-based off-chain computations, directly working with the MINA blockchain where possible.

**Architecture:**

**Real World Data Sources / APIs / Portals**

TradeInsora Client

REACT WEB APP

BPMN.js 🡪 DFA

ZK AUTHENTICARE

SNARKY JS

TRADEINSORA SERVER (NODE JS) Email

Recursion

ZK ORACLES

ZK EMAIL

SNARKY JS

**MINA BLOCKCHAIN**

ZK SMART CONTRACTS EVENTS

We are working on the phase 1 items, while also researching on the phase 2 libraries we would need for BPMN graph alegrabraic and sequence defintions, and their regex extraction to convert them to DFA for integrity checks for ZK proofs.

**RECURSION EXAMPLES**

The proof of Business Badges ( Based on nativity certificates etc )

will be composed on top of the Business entity proof ( from the Ministry of corp affairs)

will be composed on top of proofs like personal identity verifiers.

Business Badge Proof

Business Entity Proof

Personal Identity Proof

Further composition is possible, for state transitions ( even across smart contracts )

CBAM Export Lic Proof

Income Tax Proof

Financial Health Proof

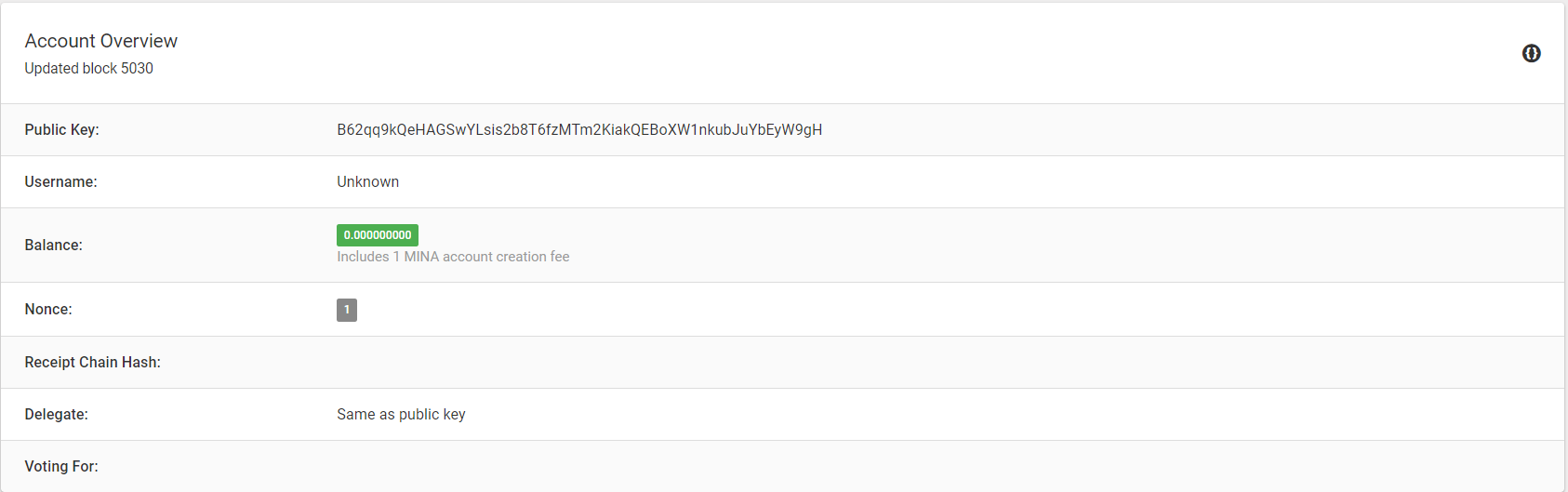
**VERSION 1 : Preliminary Check**

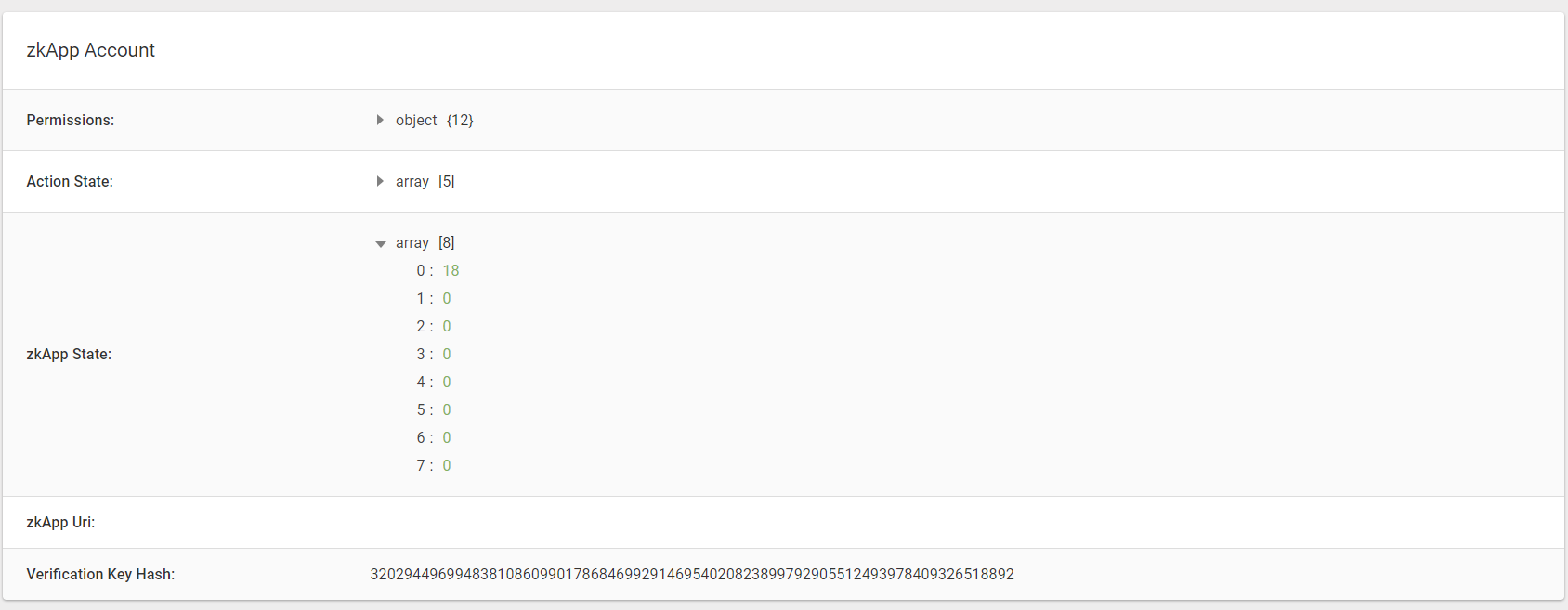
(Zkapp is deployed):

Verification hash: 3202944969948381086099017868469929146954020823899792905512493978409326518892

Two-level state transition

18 is the minimum age required for business registration, and that proof helps us to toggle the taxpayer state





(A transaction has been established):

The age of the business owner is appropriate and hence the taxpayer state is toggled to one

