Table of Contents

Solidus: A Decentralized Identity Protocol for Permissionless Verification

Version: 1.0.0 **Date:** March 2026 **Authors:** Solidus Core Team **Contact:** research@solidus.network

---

Abstract

Identity verification on the internet is structurally centralized: a small number of corporations maintain databases of personal data, charge rent for access, and create single points of failure and surveillance. We propose Solidus, a blockchain protocol that replaces centralized identity providers with an open, decentralized infrastructure. Solidus enables users to complete identity verification once, receive a cryptographic credential, and present that credential to any relying party without re-verification, without exposing raw personal data, and without depending on any central service.

The protocol combines W3C Decentralized Identifiers (DIDs), W3C Verifiable Credentials (VCs), BBS+ signatures for selective disclosure, and a Sybil-resistant consensus mechanism called Proof of Identity (PoI) — an extension of Byzantine Fault Tolerant (BFT) consensus that requires validators to be verified human entities. The result is a verification network that achieves 1-2 second finality, 50,000+ TPS per subnet, and a cost structure approximately 95% below centralized alternatives.

This paper describes the protocol architecture, the PoI consensus mechanism, the credential system with its privacy guarantees, the economic model, and provides a security analysis against known attack vectors on decentralized identity systems.

Table of Contents

---

1. Introduction

1.1 The Problem

Authentication and identity verification are fundamental operations of the digital economy. Every login, every compliance check, and every credential presentation relies on infrastructure that is concentrated in a handful of corporations. This concentration produces three systemic problems:

Cost. Auth0 charges $23,000 per million logins [1]. Okta charges $30,000+ [2], with gross margins of 73-75% (Okta FY2024 SEC filing [2]). The underlying computational cost of verifying a signature and checking a credential is negligible — approximately $0.001 per verification at current commodity compute prices. The remainder is organizational overhead: sales teams, marketing budgets, offices, executives, and shareholder returns.

Redundancy. A user who maintains accounts on five exchanges has been KYC-verified five times. Five copies of their passport exist in five databases, each a breach target. Each verification cost the exchange $5-50. The aggregate cost of duplicated verification in the global crypto industry alone exceeds $1 billion annually [3].

Surveillance. Every login to an Auth0 or Okta-powered service is recorded. The identity provider accumulates a comprehensive graph of where users authenticate, when, and with what credentials. This data is sold, subpoenaed, or breached. The user consented only to use the application — not to have their authentication behavior profiled by a third party.

These are not product-level problems solvable by better software. They are structural consequences of authentication being a product rather than a protocol. Email eliminated paid message delivery. HTTP eliminated paid content distribution. TCP/IP eliminated paid network access beyond the physical connection. Authentication is next.

1.2 The Solidus Approach

Solidus addresses these problems through three architectural choices:

First, decentralized identifiers. Users create DIDs that are anchored to the Solidus blockchain. DIDs are controlled by the user’s private key. No corporation can revoke a DID. No terms of service change can sever the user’s identity [4].

Second, verifiable credentials. When a user completes identity verification, the result is encoded as a W3C Verifiable Credential — a cryptographically signed, tamper- evident data structure stored in the user’s wallet. The credential is presented to relying parties directly,

without querying the issuer [5]. Revocation is checked on-chain in real time, not through the issuer's API.

Third, a verification network. Validators on the Solidus network process credential issuance, revocation, and verification queries. Validators earn fees for their work. No single validator controls the network. The network is secured by both economic stake and identity verification — the Proof of Identity consensus mechanism.

The economic result: verification at approximately $1,000 per million operations versus $23,000 for Auth0 — a 95% cost reduction achieved through the elimination of organizational rent, not through subsidy or cost-shifting.

1.3 Contributions

This paper makes the following contributions:

1. The Proof of Identity (PoI) consensus mechanism, extending BFT consensus with identity-based Sybil resistance (§4.3)
2. A credential revocation scheme that provides real-time revocation without a central revocation server (§4.5)
3. A selective disclosure system using BBS+ signatures and Groth16 ZK-SNARKs with W3C Verifiable Credentials (§4.4)
4. A subnet architecture for jurisdiction-compliant identity processing with cross-subnet credential portability (§3.2)
5. An economic model that aligns validator incentives with network reliability and user privacy (§7)
6. A security analysis against known attacks on decentralized identity systems (§5)

1.4 The Name

The protocol takes its name from the *solidus*, the gold coin introduced by Roman Emperor Constantine I around 312 AD. The solidus remained in circulation for over a thousand years — an unmatched record of monetary longevity. It succeeded for structural reasons: standardized weight and purity across mints (merchants trusted the coin without trusting the emperor), wide acceptance across jurisdictions, and decentralized production where no single mint was a point of failure. These properties describe what a digital identity protocol must be: standardized, widely accepted, decentralized in operation, and durable beyond any single organization.

---

2. Background and Related Work

2.1 Decentralized Identifiers

The W3C DID specification [4] defines a standard format for decentralized identifiers and a resolution mechanism (DID documents). Numerous DID methods exist, each anchoring identities to different ledgers or systems (did:eth, did:ion, did:key, etc.). Solidus defines a new DID method (did:solidus) optimized for high-throughput credential operations and identity-specific consensus.

2.2 Verifiable Credentials

W3C Verifiable Credentials [5] provide a standard data model for credential issuance and presentation. Prior work (Jolocom [7], uPort [8], Bloom [9]) demonstrated the feasibility of blockchain-anchored VCs but suffered from scalability limitations and poor developer experience. Solidus inherits the VC data model while replacing Ethereum-based anchoring with a purpose-built identity blockchain.

2.3 Zero-Knowledge Proofs in Identity

Anonymous credentials [10, 11] provide cryptographic unlinkability between credential issuance and presentation. Idemix [12] and BBS+ signatures [13] enable efficient multi-message selective disclosure. Solidus uses BBS+ signatures as the primary selective disclosure mechanism (efficient, no trusted setup) and Groth16 ZK-SNARKs [14] for complex predicate proofs (e.g., age range checks), accepting the trusted setup requirement in exchange for proof efficiency (< 10ms verification time).

2.4 Sybil-Resistant Consensus

Bitcoin's Proof of Work [15] achieves Sybil resistance through energy expenditure. Ethereum's Proof of Stake [16] achieves it through economic stake. Both allow one entity to control many identities by accumulating sufficient resources. Proof of Humanity [17] and Worldcoin [18] attempt to add biometric personhood to identity systems. Solidus's Proof of Identity requires validators to be verified unique humans (KYC Level 2) while also staking economic collateral, creating dual Sybil resistance.

2.5 Existing KYC Solutions

Jumio [19], Onfido [20], and Sumsub [21] provide centralized KYC-as-a-Service with document verification and liveness detection. These systems achieve reasonable accuracy but store biometric data, charge per-verification fees, and create the data redundancy problem described in §1.1. They are the incumbents Solidus replaces. Civic [22] and Veriff [23] attempted blockchain-based KYC but without the credential portability or privacy model that makes reusable KYC economically compelling.

2.6 Competitive Landscape

Several projects address aspects of the decentralized identity problem:

Project	Approach	Limitation
World (Worldcoin) [18]	Iris-scanning biometric uniqueness, 17.9M+ users	Biometric centralization, privacy concerns, no credential portability
Polygon ID	ZK-based credentials on Polygon PoS	Tied to Polygon's chain economics, no identity-specific consensus
SpruceID	Sign-in with Ethereum (SIWE)	Ethereum-native only, no KYC/verification layer
Ceramic Network	Decentralized data streams	Data layer only, no consensus or

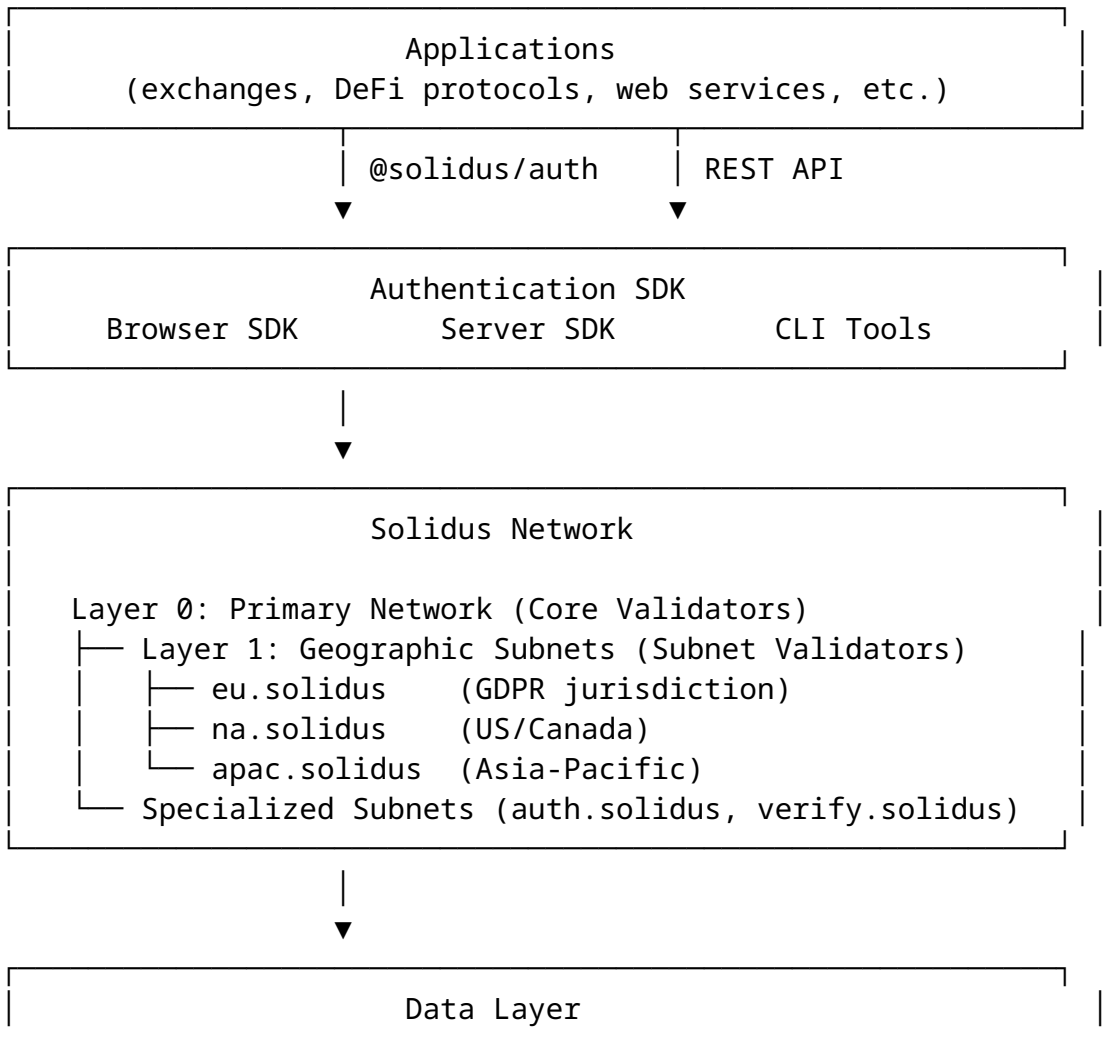
Project	Approach	Limitation
	for identity	verification
Dock.io	Verifiable Credentials platform	Centralized issuer model, limited network effects
ION (Microsoft)	Bitcoin-anchored DIDs	Read-only anchoring, no credential operations, limited throughput

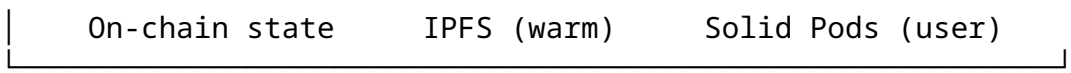
Solidus differs from all of these in combining a purpose-built identity blockchain (not piggy-backing on a financial chain), a verification-specific consensus mechanism, reusable W3C-standard credentials with selective disclosure, and an economic model that makes each subsequent verification of an already-verified user nearly free.

---

3. Architecture

3.1 Protocol Overview





The architecture follows a three-layer model. The **Application Layer** provides SDKs in JavaScript/TypeScript, Python, Go, and Rust, plus a REST API for direct integration. The **Network Layer** is a purpose-built blockchain organized into subnets for horizontal scaling and jurisdictional compliance. The **Data Layer** separates on-chain state (DID documents, revocation lists, schema registries) from user-controlled storage (Solid pods for personal data, IPFS for warm caching).

3.2 Subnet Architecture

The Solidus network operates as a hierarchical system of subnets, each optimized for specific operational requirements:

Primary Network (Layer 0). The root chain maintained by Core Validators. It stores the canonical DID registry, cross-subnet credential anchors, validator stake records, and governance state. It does not process individual verification queries.

Geographic Subnets (Layer 1). Jurisdiction-specific subnets that process verification operations for users and relying parties within their geographic region. EU subnet validators operate under GDPR constraints; no personal data leaves the EU subnet boundary. Geographic subnets contain their own validator committees (21-100 validators per subnet) and maintain independent state, with Merkle root anchoring to the Primary Network every 100 blocks.

Specialized Subnets. Purpose-specific subnets for high-volume operations: `auth.solidus` handles authentication queries, `verify.solidus` handles KYC credential issuance, `token.solidus` handles SLDS token operations. These can be independently scaled without affecting other subnets.

Cross-subnet communication. A credential issued on `eu.solidus` is presentable on `na.solidus` through a cross-subnet verification protocol: the verifier queries the issuing subnet's state via a Merkle proof anchored to the Primary Network. Cross-subnet latency: < 6 seconds.

Subnet creation. New subnets require either 100,000 SLDS stake + government partnership, or 1,000,000 SLDS via community governance vote. Each subnet requires a minimum of 21 validators.

3.3 Data Layer

On-chain state includes DID documents (public keys and service endpoints — no personal data), credential schema definitions, issuer registries, revocation bitmaps, and validator records. The chain is a trust anchor, not a data store.

What does not go on-chain: personal data, credential contents, biometric information, document images, or any sensitive user data.

User-controlled storage follows the Solid protocol specification [27]: user-controlled data pods using linked data formats, Web Access Control for authorization, application-level data requests

with user-granted permissions, and portability between pod providers. If the pod provider ceases to exist, the user's identity persists — anchored to their DID on the ledger.

Warm storage uses IPFS for historical credential snapshots, revocation list archives, and public credential schemas. Content-addressed storage ensures immutability without on-chain storage costs.

---

4. Protocol Specification

4.1 Decentralized Identifier Method

The `did:solidus` method defines identifiers of the form:

```
did:solidus:<network>:<identifier>

where:
  <network>    := "1" (mainnet) | "testnet" | <custom-network-id>
  <identifier> := Base58(BLAKE3(Ed25519_public_key)[0:20])
```

Key properties: - Deterministically derivable from the public key - 160-bit collision resistance from BLAKE3 truncation - No on-chain lookup required to verify key ownership (key is derivable from DID) - Compact representation (34 characters Base58-encoded)

DID Document structure:

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ],
  "id": "did:solidus:1:8Qx9kJ2mBnVrPqEw3sLd",
  "verificationMethod": [{
    "id":                 "did:solidus:1:8Qx9kJ2mBnVrPqEw3sLd#key-1",
    "type":               "Ed25519VerificationKey2020",
    "controller":         "did:solidus:1:8Qx9kJ2mBnVrPqEw3sLd",
    "publicKeyMultibase":
"z6MkhaXgBZDvotDkL5257faiztiGiC2QtKLGpbnnEGta2doK"
  }],
  "authentication":
["did:solidus:1:8Qx9kJ2mBnVrPqEw3sLd#key-1"],
  "assertionMethod":
["did:solidus:1:8Qx9kJ2mBnVrPqEw3sLd#key-1"],
  "keyAgreement":
["did:solidus:1:8Qx9kJ2mBnVrPqEw3sLd#key-1"]
}
```

Key rotation. DID documents support multiple verification methods with versioned key identifiers (`#key-1`, `#key-2`, etc.). Key rotation is a single on-chain transaction that adds the new key and optionally deactivates the old one. Credentials signed with a deactivated key remain valid if they were signed before the deactivation timestamp. This enables key compromise recovery without identity loss.

Social recovery. Users may designate 3-5 trusted recovery contacts. Each contact holds an encrypted key fragment (Shamir's Secret Sharing). Recovery requires m-of-n contacts to approve (default: 3-of-5), reconstructing the master seed without any single contact having access. Recovery contacts are recorded in the DID document as recovery service endpoints.

4.2 Verifiable Credential Schema

Solidus credentials conform to the W3C Verifiable Credentials Data Model 2.0 [5]. The credential envelope uses Ed25519Signature2020 as the proof type, with BBS+ signatures used for credentials that require selective disclosure.

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/solidus/credentials/v1"
  ],
  "id":     "vc:solidus:1:Af7eP2mRqKs9nLv0wXtY",
  "type":   ["VerifiableCredential", "KYCLevel2Credential"],
  "issuer": "did:solidus:1:IssuerOracleDID",
  "issuanceDate": "2026-03-14T14:00:01Z",
  "expirationDate": "2027-03-14T00:00:00Z",
  "credentialSubject": {
    "id":                "did:solidus:1:8Qx9kJ2mBnVrPqEw3sLd",
    "kyc_level":         2,
    "human":             true,
    "document_country":  "DE",
    "age_over_18":       true
  },
  "credentialStatus": {
    "id":
"https://api.solidus.network/v1/credentials/Af7eP2mRqKs9nLv0wXtY/statu
s",
    "type": "SolidusRevocationList2026"
  },
  "proof": {
    "type":               "Ed25519Signature2020",
    "created":            "2026-03-14T14:00:01Z",
    "verificationMethod": "did:solidus:1:SolidusVerifyIssuer#key-1",
    "proofPurpose":       "assertionMethod",
```

```
    "proofValue":          "z3FXQjeczkB7..."
  }
}
```

Credential minimality enforcement: The Solidus credential schema registry defines the exact claim set for each credential type. Issuers cannot add claims outside the schema definition. This prevents credential over-scoping at the protocol level, not just by convention.

Credential types: The protocol defines a hierarchy of verification levels:

Type	Verification	Claims	Use Case
Email (L0)	Confirmation link	Email address, ownership proof	Basic authentication
Phone (L0)	SMS OTP	Phone number, carrier verification	Two-factor authentication
KYC Level 1	Automated	Name, DOB, address	Basic compliance
KYC Level 2	Document + liveness	L1 + document country, document hash, liveness proof	Full compliance
KYC Level 3	Enhanced due diligence	L2 + sanctions screening, PEP check, address proof	High-value financial

4.3 Proof of Identity Consensus

Proof of Identity (PoI) extends Snowman++, the BFT consensus protocol used by Avalanche [24], with two additional validator requirements beyond economic stake:

Requirement 1: Verified human identity. Validators must hold a KYC Level 2 credential issued by the Solidus verification engine. This establishes that each validator is a unique, verified human. An adversary acquiring 33% of validators by stake must also acquire 33% of verified human identities — a qualitatively harder attack than pure economic accumulation.

Requirement 2: Reputation score ≥ 800. Validators accumulate a reputation score through sustained honest participation. New validators start at 800 (the minimum). The score approaches 1000 through consistent uptime, correct consensus votes, and governance participation. Slashing events reduce the score. This creates a graduation cost for new validators and a progressive track record requirement.

Validator selection per round:

```
For each consensus round:
  1. Compute VRF(round_seed, validator_id) for all eligible validators
  2. Sort by VRF output (deterministic, unpredictable)
```

```
  3. Select top 21 validators weighted by:
     effective_weight = stake × (uptime_30d) × (reputation / 1000)
  4. Selected committee proposes and votes on the next block
```

The VRF ensures that committee membership is unpredictable before the round begins (preventing targeted DoS attacks on known committee members) while remaining verifiable after the fact (anyone can confirm the correct validators were selected).

Finality: A block is finalized when 2/3 of the committee's weighted stake has voted for it (the BFT safety threshold). Finality is irreversible and typically achieved within 1-2 seconds.

Validator staking tiers:

Tier	Minimum Stake	Role
Light Node	10,000 SLDS	Read-only relay, storage provision
Subnet Validator	100,000 SLDS	Subnet-level consensus participation
Core Validator	1,000,000 SLDS	Primary Network consensus, cross-subnet coordination

4.4 Selective Disclosure

Solidus supports two complementary selective disclosure mechanisms, chosen per credential type based on the privacy requirements:

BBS+ Signatures (primary). Credentials signed with BBS+ [13] support efficient multi-message selective disclosure without ZK circuits. A holder can derive a presentation that reveals a subset of credential claims while proving that the unrevealed claims exist and were signed by the issuer. BBS+ requires no trusted setup and produces compact proofs (< 400 bytes).

The holder generates a derived proof for a subset of claims:

```
DeriveProof(credential, disclosed_indices, nonce) → presentation
VerifyDerived(presentation, issuer_pk, disclosed_claims, nonce) → bool
```

Groth16 ZK-SNARKs (for predicate proofs). For complex predicate claims — "prove age ≥ 18 without revealing birthdate" — the protocol uses Groth16 [14] over the BN254 curve. The statement proved is:

```
∃ credential C such that:
  1. C is signed by a valid Solidus issuer DID
  2. C has not been revoked (membership proof in the non-revoked set)
  3. C.credentialSubject.birth_year ≤ current_year - 18
```

Trusted setup: Groth16 requires a one-time trusted setup per circuit. Solidus conducts a multi-party computation (MPC) ceremony for each circuit type, following the structure of the Zcash Powers of Tau [25]. At least 100 independent participants must contribute, with the ceremony output being secure as long as at least one participant discarded their secret.

Three disclosure modes per credential field:

Mode	Recipient Sees	Cryptographic Mechanism
Reveal	Full field value	Standard VC presentation
Hide	Nothing (proven to exist)	BBS+ derived proof
Derive	Predicate result only ("Age ≥ 18: true")	Groth16 ZK-SNARK

4.5 Credential Revocation

The SolidusRevocationList2026 scheme provides real-time revocation status without a central revocation server:

1. Each issuer maintains a bitmap revocation list on-chain. Bit position $i = 1$ means the i-th credential issued by this issuer is revoked.
2. The revocation list is compressed and stored in the subnet state. IPFS stores historical snapshots. Light clients can verify membership proofs against the on-chain list root.
3. Revocation takes effect at the next block after the revocation transaction is finalized (1-2 seconds).
4. Credential presentations include a non-revocation proof — a zero-knowledge membership proof that the credential is NOT in the revocation list. This allows offline verification against a recent snapshot without a live network query.

Privacy-preserving revocation: The issuer revokes a credential by index, not by DID. Observers of the revocation transaction cannot determine which user's credential was revoked without the issuer's internal mapping.

4.6 Cross-Subnet Communication

Credentials issued on one subnet must be verifiable on any other subnet without requiring the verifier to query the issuing subnet in real time.

Mechanism: Each subnet publishes its state root to the Primary Network every 100 blocks (anchoring). A cross-subnet verification constructs a Merkle inclusion proof from the credential's revocation status in the issuing subnet, through the subnet's state root, to the Primary Network's latest checkpoint.

Latency: Cross-subnet verification adds at most one checkpoint interval (< 6 seconds) to the verification latency. For time-critical use cases, relying parties can subscribe to the issuing subnet's block stream directly.

Atomicity: Cross-subnet credential operations (e.g., revoking a credential on `eu.solidus` that was presented on `na.solidus`) use optimistic rollups with fraud proofs: the operation is accepted provisionally and finalized after a challenge period (5 minutes).

---

5. Security Analysis

5.1 Adversary Model

We consider a computationally bounded adversary with the following capabilities: - Controls up to 1/3 of staked SLDS in any subnet - Controls a corresponding fraction of verified human identities (bounded by 1/3) - Controls a subset of network links (partial network control) - Cannot break BLAKE3, Ed25519, BBS+, or Groth16 in the security parameter range

We do not consider: - Quantum adversaries (post-quantum migration is future work; see §14) - Nation-state adversaries who can coerce all KYC oracles simultaneously - Social engineering attacks against individual validators

5.2 Consensus Safety

Theorem: If at most f < n/3 of validators (by stake weight) are Byzantine, the PoI consensus protocol cannot finalize two conflicting blocks at the same height.

Proof sketch: Finalization requires 2/3 supermajority. If two conflicting blocks both achieved 2/3 supermajority, at least 1/3 of validators voted for both, implying they are Byzantine — contradicting our assumption of f < n/3 Byzantine validators. □

Liveness: If at most f < n/3 validators are faulty (Byzantine or crashed), the protocol continues to finalize blocks. This follows directly from Snowman++'s liveness proof [24] plus the observation that validator rotation (via VRF, every 7 days) prevents indefinite collusion among a fixed coalition.

5.3 Sybil Attacks

Economic Sybil attack: An adversary creates multiple validator identities using accumulated economic stake. *Mitigation:* identity binding requires a unique verified human identity per validator. A single human cannot hold two KYC Level 2 credentials (the oracle checks for biometric uniqueness across its records). The attack cost is therefore: (economic stake for 1/3 of validators) × (acquisition of 1/3 unique human identities) — multiplicative, not additive.

Oracle collusion attack: A malicious oracle issues multiple KYC credentials to the same human. *Mitigation:* Solidus uses multiple independent oracles. A credential from a colluding oracle is only valid within subnets that accept that oracle. Colluding oracles are removed from the approved oracle set through governance.

Identity farming attack: An adversary acquires valid identities of other humans (purchased, coerced, or stolen) to register multiple validators. *Mitigation:* (1) validator reputation requires sustained uptime — identities cannot be acquired and registered passively; (2) governance allows flagging of suspicious validator clusters; (3) the minimum stake per validator makes this attack economically costly.

5.4 Eclipse Attacks

An eclipse attack isolates a target node by surrounding it with adversarial peers, presenting a false view of the network state.

Mitigations: - Peer diversity requirements (no more than 20% of peers from a single /24 subnet) - Validators publish signed attestations of their view; divergent views are detectable - Clients verify against multiple independent validators, not a single peer - Light clients query at least 3 validators and require agreement before accepting state

5.5 Long-Range Attacks

In Proof of Stake systems, an adversary who held stake in the past can rewrite history from a fork point without current stake.

Mitigation: Solidus uses weak subjectivity checkpoints — signed state roots that validators publish every 100 blocks and that clients embed in software releases. A client syncing from genesis accepts the published checkpoints and cannot be fed a chain that diverges before the most recent checkpoint.

5.6 Credential Forgery

Forging a credential requires either: (a) Compromising the issuer’s private key, or (b) Breaking Ed25519 (requiring a quantum adversary at 256-bit key sizes)

Issuer key compromise mitigation: HSM key storage for the Solidus verification engine; mandatory key rotation every 90 days; revocation of all credentials signed by a compromised key and automated re-issuance.

5.7 Revocation Bypassing

An adversary presents a revoked credential before the revocation is finalized. The attack window is at most 1-2 seconds (the finality time). For most use cases this is acceptable. For high-stakes use cases (large financial transactions), relying parties may require a freshness proof with a maximum age of one block.

5.8 Privacy Attacks

Correlation attack: A verifier attempts to correlate presentations from the same user across sessions. *Mitigation:* each BBS+ derived proof uses a fresh nonce, producing an unlinkable presentation. Without the holder’s cooperation, the same credential presented twice is cryptographically indistinguishable from two different credentials.

Issuer tracking: An issuer attempts to track where and when its credentials are presented. *Mitigation:* derived presentations replace the original credential ID with a per-presentation commitment. The issuer cannot distinguish its credential from another issuer's credential in the presentation flow.

---

6. Privacy Analysis

6.1 Unlinkability

Issuer-holder-verifier unlinkability: Standard VC presentations allow issuers to track presentations if they observe the network (a presentation contains a credential ID visible to the issuer). Solidus uses BBS+ derived presentations that replace the original credential ID with a per-presentation commitment, preventing issuer tracking.

Cross-verifier unlinkability: Each presentation to a different verifier uses a fresh ephemeral commitment. Without the holder's cooperation, two verifiers cannot determine they served the same user.

Network-level unlinkability: Requests to the Solidus network are not linked to real-world IP addresses by default. Validators do not log client IPs for standard verification queries. Enterprise clients operating their own nodes gain full network-level unlinkability for their users.

6.2 Data Minimization

The selective disclosure system enables relying parties to receive binary answers to specific questions without the underlying credential data:

Use Case	Data Shared	Data NOT Shared
Age verification	"Over 18: true"	Birth date, name, document number
Jurisdiction check	"EU resident: true"	City, address, exact country
FATF compliance	"FATF member country: true"	Specific nationality
Professional license	"Licensed physician: true"	License number, issuing authority
Sanctions screening	"Not sanctioned: true"	Identity, citizenship, addresses

6.3 GDPR Compliance by Design

The Solidus architecture implements the principles that data protection law attempts to enforce, at the infrastructure level:

Data minimization (Art. 5(1)(c)). Zero-knowledge proofs ensure that only the minimum data required for a specific purpose is disclosed. The protocol enforces this — an application cannot extract more data than the user approved.

Right to erasure (Art. 17). User data resides in user-controlled Solid pods. The user can delete their data at any time. On-chain state contains only public keys and cryptographic commitments — no personal data.

Data portability (Art. 20). Credentials are W3C-standard data structures stored in user-controlled pods. They are portable by design to any compliant system.

Purpose limitation (Art. 5(1)(b)). Selective disclosure enforces purpose limitation at the cryptographic level. A credential shared for age verification cannot be repurposed for identity extraction.

Privacy by design (Art. 25). All identity claims support zero-knowledge proof presentation. Privacy is the default state, not an opt-in feature. Users can choose to disclose more; they cannot accidentally disclose more than they intend.

---

7. Economic Model

7.1 Token Supply and Distribution

The SLDS token has a fixed supply of 1,000,000,000 (1 billion). No new tokens can be minted after genesis. This supply was chosen for utility-first economics: whole-number fees (5 SLDS for KYC L2, not 0.00005), accessible staking tiers for validators worldwide, and clean denomination for micro-transactions across the protocol.

Category	Allocation	Vesting	Purpose
Community rewards	15%	Various program-based	Bootstrap user adoption
Core team	15%	1-year cliff, 3-year linear vest	Align founders with long-term success
Private round	12%	6-month cliff, 2-year linear vest	Seed and strategic funding
Ecosystem fund	10%	5-year linear unlock	Developer grants, partnerships
Seed investors	8%	6-month cliff, 2-year linear vest	Early-stage funding
Development fund	7%	5-year linear unlock	Protocol development
Airdrops	5%	Event-based	Community distribution
Liquidity mining	5%	Program-based	DEX liquidity
Marketing	5%	3-year linear unlock	Awareness and adoption
Public sale	5%	25% at TGE, 75% over 6 months	Broad distribution
Strategic partnerships	5%	Deal-based	Ecosystem expansion

Category	Allocation	Vesting	Purpose
Advisors	5%	6-month cliff, 2-year linear vest	Strategic guidance
Operations	3%	3-year linear unlock	Foundation operations

Deflationary mechanism: 10% of all transaction fees are burned permanently. As the network grows and fee volume increases, the circulating supply decreases. At scale (100M+ verifications/day), the burn rate exceeds the staking inflation rate, making the network net deflationary.

7.2 Fee Structure

All network operations require fees paid in SLDS tokens. Fees are denominated in SLDS but pegged to USD price targets via an on-chain price oracle (Chainlink). The SLDS denomination adjusts quarterly to maintain stable USD pricing, preventing fee volatility from disrupting business use cases.

Operation	Fee	Distribution
DID creation	0.001 SLDS (~$0.001)	70% validators / 20% treasury / 10% burn
DID update	0.0001 SLDS	70% / 20% / 10%
Email verification	0.01 SLDS (~$0.01)	70% / 20% / 10%
Phone verification	0.02 SLDS (~$0.02)	70% / 20% / 10%
KYC Level 1	1.0 SLDS (~$1.00)	70% / 20% / 10%
KYC Level 2	5.0 SLDS (~$5.00)	70% / 20% / 10%
KYC Level 3	20.0 SLDS (~$20.00)	70% / 20% / 10%
Credential issuance	0.01 SLDS	70% / 20% / 10%
Verification query	0.001 SLDS (~$0.001)	70% / 20% / 10%

The cost advantage at scale: at $0.001 per verification query, 1 million re-verification checks cost $1,000. Auth0 charges $23,000 for the equivalent volume [1]. The 95% savings come from re-use — the expensive initial KYC verification happens once; every subsequent check is a cheap credential query.

7.3 Validator Economics

A validator’s revenue per epoch (7 days) is:

```
revenue = fee_pool_7days × 0.70 × (effective_stake /
total_effective_stake)

effective_stake = staked_SOLID × uptime_score × (reputation / 1000)
```

Break-even analysis for a Light Node (10,000 SLDS minimum stake):

At 1,000,000 verifications per day across the network: - Network daily fee revenue: ~$100,000 (mixed Level 1 and Level 2 checks) - Validator reward pool: $70,000/day - Light Node share (1/10,000 of effective stake): ~$7/day = $210/month - Light Node operating cost: $10-50/month (VPS hosting) - Net profit: $160-200/month

At scale (10,000,000 verifications per day): - Validator reward pool: $700,000/day - Light Node share: ~$70/day = $2,100/month

These projections are illustrative. Actual earnings depend on network adoption, fee mix, and the number of validators competing for the reward pool.

Slashing. Validators lose stake for dishonest or negligent behavior:

Violation	Penalty
Double-signing	10% of stake
Extended downtime	0.1% per hour offline
Invalid verification attestation	5% of stake
Censorship (provable)	1% of stake
Collusion (provable)	100% of stake + permanent ban

Slashed funds: 50% burned, 50% distributed to reporting validators.

7.4 Anti-Extractive Design

The fee distribution is explicitly designed to prevent rent extraction:

1. **No company receives fees.** There is no “Solidus Inc.” that takes a cut. The Solidus Foundation is a non-profit entity that bootstraps protocol development — analogous to the Ethereum Foundation’s relationship with Ethereum. Validators (infrastructure operators) and the community-governed protocol treasury receive all fees.

2. **The treasury is community-governed.** Treasury funds can only be spent through governance votes. There is no executive team that controls the treasury.

3. **Fees decrease as the network scales.** As more validators join, competition for the reward pool increases. Validators optimize infrastructure to lower costs. Fee rates are adjusted through governance to remain competitive with centralized alternatives.

7.5 Supply Dynamics

Staking rewards create 3% annual inflation (distributed to validators proportional to stake). The 10% fee burn creates deflationary pressure proportional to network usage. The crossover point

— where the network becomes net deflationary — occurs at approximately 82 million daily verifications.

Year	Daily Verifications	Annual Burn	Staking Inflation (3%)	Net Supply Change
1	1M	365,000 SLDS	+30,000,000	+2.96%
3	10M	3,650,000 SLDS	+30,000,000	+2.64%
5	50M	18,250,000 SLDS	+30,000,000	+1.18%
10	100M	36,500,000 SLDS	+30,000,000	-0.65%

8. Performance Analysis

8.1 Throughput

Configuration	TPS
Single geographic subnet	50,000
Single specialized subnet	100,000
Multi-subnet aggregate (Phase 3)	100,000+

These targets are based on: - 32 parallel execution shards per subnet - 16 validation lanes with batched signature verification (256 sigs/batch) - 500ms block time with pipelined block proposals

Comparison: Auth0 processes approximately 15 billion authentications per month [1], or roughly 5,800 per second globally. The Solidus Phase 3 aggregate target of 100,000 TPS represents 17× Auth0’s current global throughput, on a single instance.

8.2 Latency

Operation	Target Latency
Block time	500 ms
Finality	1-2 seconds
Auth fast path (cached)	< 200 ms
Auth slow path (full verify)	< 500 ms
Cross-subnet transaction	< 6 seconds
KYC Level 1 (automated)	< 2 minutes
KYC Level 2 (automated)	< 5 minutes

The auth fast path uses a per-subnet LRU cache of recent verification results (1,000,000 entries, configurable TTL). Under steady-state load, 80-90% of authentication requests are served from cache without a consensus round, dramatically reducing per-authentication cost and latency.

8.3 Scalability

The subnet model provides horizontal scalability. Additional subnets are created to accommodate load without degrading existing subnet performance. Geographic subnets provide an additional scaling dimension — GDPR-compliant EU users are processed by EU validators, with no cross-region data transfer required.

The 32-shard execution model within each subnet ensures intra-subnet horizontal scaling. Cross-shard atomicity is handled through two-phase locking with a deadlock-free ordering guarantee.

---

9. Governance

The protocol is governed by validators and token holders, not by a foundation, corporation, or core team.

9.1 Protocol Upgrades

Upgrades require supermajority validator consensus through a structured process:

1. **Proposal.** Any token holder meeting the governance threshold submits a Solidus Improvement Proposal (SIP) with a full technical specification.
2. **Review period.** Minimum 30 days for public review and discussion. The minimum duration is enforced by the protocol — no fast track.
3. **Validator signaling.** Validators signal support or opposition, weighted by stake.
4. **Activation.** If 67% of weighted stake signals support, the upgrade activates at a predetermined block height.

There is no emergency override. Identity infrastructure must be stable. A protocol that can be changed quickly by a small group is merely trusted — a weaker property than trustworthy.

9.2 Issuer Accreditation

Credential issuers for regulated types (KYC, professional licensing) must pass an accreditation process:

- Demonstrate regulatory standing in at least one jurisdiction
- Complete a technical capability assessment (key management, infrastructure security)
- Post a bond (in SLDS) that is slashed for fraudulent credential issuance
- Undergo periodic re-accreditation

The accreditation registry is on-chain and publicly auditable. Accreditation can be revoked through governance vote.

9.3 Credible Neutrality

The founding team has no special governance privileges, no outsized voting power, and no ability to unilaterally modify the protocol. The team’s tokens vest on the same schedule as any

other participant. After vesting, the team participates in governance with the same weight-per-token as any other holder.

This is a deliberate rejection of the “progressively decentralized” model, in which a project launches centralized and promises to distribute power later. That promise is rarely kept.

---

10. Regulatory Position

Identity is a regulated domain. Solidus does not circumvent regulation — it provides better tools for meeting regulatory requirements.

KYC/AML compliance. Accredited issuers are regulated entities. Their credentials carry the same legal weight as existing attestations, delivered through a different mechanism. Regulation requires verification, not centralization.

Data protection. Solidus is architecturally aligned with GDPR (see §6.3), CCPA, and equivalents: data minimization through zero-knowledge proofs, right to erasure via user-controlled pods, explicit consent for every disclosure, and portability by design.

Jurisdictional neutrality. The validator network operates across jurisdictions. Geographic subnets ensure data residency compliance. Applications built on Solidus remain subject to the laws of their jurisdiction. The protocol provides the tools; applications bear the compliance obligations.

Credential legal standing. The eIDAS 2.0 regulation in the EU recognizes verifiable credentials as legally valid for electronic identification [28]. MiCA (Markets in Crypto-Assets Regulation) requires exchanges to perform customer identification — Solidus credentials satisfy this requirement while keeping personal data under user control rather than in exchange databases.

---

11. Interoperability

11.1 W3C Standards Compliance

- **DID Core.** Solidus DIDs conform to the W3C DID Core specification [4]. The `did:solidus` method will be registered per W3C requirements.
- **Verifiable Credentials Data Model 2.0.** All credentials conform to the VC Data Model [5] and interoperate with any compliant system.
- **DID Resolution.** The resolver implements the DID Resolution specification.
- **Solid Protocol.** User data pods follow the Solid specification [27] for user-controlled storage.

11.2 Legacy Bridges

OAuth/OIDC bridge. Translates Solidus credential presentations into standard OAuth 2.0 tokens. Applications that accept “Sign in with Google” can accept “Sign in with Solidus” with a single library import. No application rewrite required.

SAML bridge. Enterprise integration through a translation layer for legacy identity federation systems.

Credential import. Existing identity attestations from traditional KYC providers can be wrapped as Verifiable Credentials by accredited bridge issuers, allowing gradual migration without requiring users to re-verify.

These bridges are transitional infrastructure designed to remove adoption friction. As native Solidus integration becomes standard, bridge usage will decrease.

11.3 Cross-Chain Anchoring

Solidus DIDs can be anchored to other blockchains for cross-ecosystem portability:

- **Ethereum.** DID anchoring via smart contract for DeFi integrations
- **Bitcoin.** Periodic checkpoint anchoring for maximum tamper resistance
- **IPFS.** Content-addressed storage for credential schemas and revocation archives

Cross-chain anchoring provides redundancy — if the Solidus network experiences temporary partitioning, DID state can be verified against external anchors.

---

12. Roadmap

These are targets, not guarantees. Pace depends on technical progress, regulatory engagement, and ecosystem growth.

Year 1 — Foundation (Months 1-12)

- Launch testnet with functional validator network (Month 3)
- Release production Verify product (KYC credential system) (Month 6)
- Onboard 100-1,000 active validators across multiple regions (Month 9)
- Launch public mainnet (Months 10-12)
- Publish SDKs for JavaScript/TypeScript and Python
- Complete first independent security audit
- Establish OAuth/OIDC bridge for legacy integration
- Target: 1,000 beta users, $10K MRR

Year 2 — Growth

- 100+ applications building on the protocol
- 100,000 users with Solidus-based identity (realistic target)
- Credential types beyond KYC: age verification, professional licensing, educational credentials
- SDKs for Go, Rust, and Java
- Formal regulatory engagement in major jurisdictions (EU eIDAS, US state-level)
- Additional geographic subnets (EU, APAC)

- Target: $200K MRR

Year 3 — Default

- Solidus becomes a standard authentication option for new applications
- Major frameworks (Next.js, Rails, Django, Spring) include Solidus as a first-class auth option
- Credential interoperability with other decentralized identity networks
- Enterprise adoption for internal identity management
- Multiple competing wallet implementations with mature UX
- 1,000-5,000 active validators

Year 5 — Maturity

- Centralized providers economically obsolete for new applications
- Credential issuance at scale across finance, healthcare, education, government
- Protocol governance fully decentralized, no residual influence from founding team
- 5,000-11,000+ validators across 50+ geographic subnets
- The protocol is infrastructure — invisible, reliable, taken for granted

---

13. Risks

A credible protocol acknowledges what can go wrong.

Cold start. The network is useful only if applications integrate it, applications integrate only if users exist, and users appear only if applications support them. The KYC wedge (businesses with acute cost pain) and the OAuth/OIDC bridge (no application rewrite required) are designed to break this cycle, but there is no guarantee of sufficient initial traction. *Mitigation:* focus on 3-5 early-adopter crypto exchanges with explicit cost savings commitment.

Regulatory uncertainty. Some jurisdictions may view decentralized identity infrastructure with suspicion, particularly regarding KYC/AML obligations. *Mitigation:* proactive regulatory engagement; use of accredited (regulated) issuers; geographic subnets for jurisdictional compliance; legal opinions in target markets before launch.

Cryptographic risk. Zero-knowledge proof systems are mathematically complex. Bugs in ZKP implementations have caused real-world failures in other protocols [29]. *Mitigation:* formal verification of critical circuits; multiple independent security audits; conservative cryptographic choices (established curves, well-studied constructions); BBS+ as the primary mechanism (simpler, no trusted setup) with Groth16 reserved for complex predicates.

Verification engine trust. The Solidus verification engine is the credential issuer. If the verification engine is compromised, Sybil resistance degrades to pure PoS. *Mitigation:* HSM key storage for signing keys; multi-party approval for credential issuance; governance mechanism for emergency revocation; audit log of all issued credentials.

Usability. Decentralized identity is harder to use than “Sign in with Google.” Key management and credential storage are concepts most users should not need to understand. The protocol

succeeds only if wallet implementations make the experience as simple as existing alternatives. *This is the most likely failure mode.* The quality of the consumer experience will determine adoption more than any technical or economic advantage.

Scope. The Solidus ecosystem encompasses 16 products across identity, wallet, social, and governance domains. Building all of them simultaneously would be fatal. *Mitigation:* Verify (KYC) is the only product that matters for Year 1. The remaining 15 products are deferred until the protocol has traction, revenue, and a proven validator network. The protocol is general; the product focus is narrow.

Competition. World (Worldcoin) has 17.9M users and substantial funding. Polygon ID, SpruceID, and Ceramic address adjacent problems. Centralized providers may respond with lower prices or improved features. *Mitigation:* structural cost advantage (95% lower) is not matchable by centralized providers without destroying their business model. Execution speed and developer experience must outweigh incumbents' distribution advantages.

---

14. Conclusion and Future Work

Solidus demonstrates that decentralized identity verification can be economically viable, privacy-preserving, and performant at scale. The Proof of Identity consensus mechanism extends BFT consensus with human-identity Sybil resistance without sacrificing finality speed or throughput. The verifiable credential system provides portability and selective disclosure without a central credential store. The economic model makes verification approximately 95% cheaper than centralized alternatives while compensating validators for real infrastructure work rather than extracting rent from a proprietary system.

The fundamental argument is economic, not ideological. When infrastructure becomes a protocol, the rent-seeking intermediaries disappear. Email eliminated paid message delivery. HTTP eliminated paid content distribution. TCP/IP eliminated paid network access beyond the physical connection. Authentication is next.

The question is not whether decentralized identity will replace centralized authentication. The question is when, and whether the transition will be led by an open protocol or captured by another set of intermediaries.

Known limitations: - Post-quantum cryptography not yet integrated; migration requires a hard fork - ZK circuit trusted setup requires broad participation to ensure soundness - Biometric-based Sybil resistance depends on the quality of the KYC oracle ecosystem - Cross-jurisdiction regulatory compliance requires ongoing legal work per market

Future work: - ML-KEM and ML-DSA integration for post-quantum signatures and key exchange [26] - Decentralized oracle network for KYC to eliminate oracle trust assumptions - Formal verification of the PoI consensus safety and liveness properties - W3C DID method registration and standardization of Solidus credential schemas - State channel protocol for off-chain high-frequency authentication (unlimited TPS) - Cross-chain DID resolution for Ethereum, Bitcoin, and Cosmos ecosystems - AI agent identity — extending DIDs to autonomous software agents operating on behalf of verified humans

References

[1] Auth0. “Pricing.” https://auth0.com/pricing. Accessed March 2026.

[2] Okta. “Annual Report FY2024.” SEC EDGAR. Gross margin: 73-75%. Accessed March 2026.

[3] Chainalysis. “Crypto Crime Report 2025.” Chainalysis, 2025.

[4] Sporny, M., et al. “Decentralized Identifiers (DIDs) v1.0.” W3C Recommendation, July 2022. https://www.w3.org/TR/did-core/

[5] Sporny, M., et al. “Verifiable Credentials Data Model 2.0.” W3C Recommendation, 2024. https://www.w3.org/TR/vc-data-model-2.0/

[6] Berners-Lee, T. “Solid: A Platform for Decentralized Social Applications.” MIT, 2016. https://solidproject.org

[7] Jolocom. “Jolocom SmartWallet: Decentralized Identity.” https://jolocom.io. 2019.

[8] Lundkvist, C., et al. “uPort: A Platform for Self-Sovereign Identity.” arXiv:1607.01427. 2017.

[9] Bloom. “Bloom Protocol: A Decentralized Credit System.” https://bloom.co. 2018.

[10] Camenisch, J., Lysyanskaya, A. “Signature Schemes and Anonymous Credentials from Bilinear Maps.” CRYPTO 2004.

[11] Camenisch, J., Lysyanskaya, A. “A Signature Scheme with Efficient Protocols.” SCN 2002.

[12] IBM Research. “Identity Mixer.” https://idemix.wordpress.com. 2018.

[13] Tessaro, S., Zhu, C. “Short Pairing-Free Blind Signatures with Exponential Security.” EUROCRYPT 2022. (BBS+ reference implementation)

[14] Groth, J. “On the Size of Pairing-Based Non-Interactive Arguments.” EUROCRYPT 2016.

[15] Nakamoto, S. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 2008.

[16] Buterin, V., et al. “Combining GHOST and Casper.” arXiv:2003.03052. 2020.

[17] Kleros. “Proof of Humanity: A Protocol for Human Verification.” https://proofofhumanity.id. 2021.

[18] Worldcoin. “World ID: The Privacy-Preserving Proof-of-Personhood Protocol.” Worldcoin whitepaper, 2023.

[19] Jumio. “AI-Powered Identity Verification.” https://jumio.com. Accessed March 2026.

[20] Onfido. “Identity Verification Platform.” https://onfido.com. Accessed March 2026.

[21] Sumsub. “Full-Cycle Verification Platform.” https://sumsub.com. Accessed March 2026.

[22] Civic. “Civic Reusable KYC.” https://civic.com. 2022.

[23] Veriff. “Identity Verification.” https://veriff.com. Accessed March 2026.

[24] Rocket, T., et al. “Scalable and Probabilistic Leaderless BFT Consensus through Metastability.” arXiv:1906.08936. 2019.

[25] Bowe, S., et al. “Scalable Multi-party Computation for zk-SNARK Parameters in the Random Beacon Model.” Cryptology ePrint Archive, 2017.

[26] NIST. “Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203).” NIST, 2024.

[27] Solid Project. “Solid Protocol Specification.” https://solidproject.org/TR/protocol. 2022.

[28] European Commission. “eIDAS 2.0 — European Digital Identity Regulation.” Regulation (EU) 2024/1183. 2024.

[29] Zcash. “Zcash Counterfeiting Vulnerability CVE-2019-7167.” Disclosure report, 2019.

Appendix A: Comparison Matrix

Feature	Google Login	Auth0	Okta	World (Worldcoin)	Solidus
Cost per 1M auths	Free (data is the product)	$23,000	$30,000+	Free (VC token model)	~$1,000
User data ownership	Google	Auth0 tenant	Okta tenant	World Foundation	User (Solid pod)
Credential portability	No	No	No	Limited	Full (W3C VC)
Selective disclosure	No	No	No	Limited ZK	Full (BBS+ / Groth16)
KYC reusability	No	No	No	No (identity only)	Yes
Single point of failure	Google	Auth0	Okta	World orb network	None (decentralized)
Open protocol	No	No	No	Partial	Yes
Vendor lock-in	High	High	High	Medium	None
On-chain privacy	N/A	N/A	N/A	Iris hash on-chain	No personal data on-chain
Regulatory	Platform-	Platform	Platfor	Uncertain	Issuer-level

Feature	Google Login	Auth0	Okta	World (Worldcoin)	Solidus
compliance	dependent	-dependent	m-dependent		(regulated KYC providers)

Appendix B: Glossary

Term	Definition
BBS+	A pairing-based signature scheme that supports efficient multi-message selective disclosure
BFT	Byzantine Fault Tolerant — consensus protocols that function correctly with up to 1/3 malicious participants
Credential	A cryptographically signed data structure attesting to claims about a subject (W3C Verifiable Credential)
DID	Decentralized Identifier — a globally unique, user-controlled identifier (W3C standard)
Groth16	A ZK-SNARK construction with constant-size proofs and fast verification
Issuer	An entity authorized to create and sign Verifiable Credentials
KYC	Know Your Customer — regulatory requirement for identity verification
Liveness check	Biometric verification that the person presenting a document is physically present
MPC	Multi-Party Computation — protocol where multiple parties jointly compute a function without revealing inputs
Verification engine	The Solidus-native system that performs document checks, liveness detection, and issues credentials on the network
PoI	Proof of Identity — Solidus's consensus mechanism combining BFT with identity-verified validators
Presentation	A derived proof from a credential shared with a verifier (may include selective disclosure)
Relying party	An application or service that verifies a user's credential
Selective disclosure	Revealing only specific claims from a credential while proving the unrevealed claims exist
Slashing	Economic penalty (loss of staked SLDS) for validator misbehavior
Solid	Tim Berners-Lee's protocol for user-controlled data pods (solidproject.org)
SLDS	The native utility token of the Solidus Protocol
Subnet	An independent validator committee within the Solidus network, specialized by geography or function

Term	Definition
VRF	Verifiable Random Function — produces unpredictable but verifiable pseudorandom outputs
ZK-SNARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge — a compact proof that a statement is true without revealing why

This document is version 1.0.0. It has not been independently peer reviewed. Claims about security properties are design descriptions, not formal proofs. A full formal security analysis will be conducted as part of the Phase 1 protocol audit. This document will be updated to reflect audit findings.