AMERICAN SUBSTITUTE DOLLAR

(A S D)

Master Investor Proposal

Part II — Infrastructure, Security, Custody & Compliance

How ASD Is Built to Be Safe, Secure, Compliant, and Durable — by Design

[ASD LOGO PLACEHOLDER]

SECURITY PHILOSOPHY

Trust is not asserted; it is engineered, verified, and disclosed. This part of the proposal describes the architecture, controls, and legal framework designed to protect the system — and is candid about the risks that no design can erase, because honesty about risk is itself a security control.

Part II of IV • Version 1.0 • June 1, 2026
www.asdcoins.us • support@asdcoins.us

Contents — Part II

SECTION 4 — BLOCKCHAIN ARCHITECTURE & TECHNOLOGY

15. Blockchain Core Infrastructure

ASD is engineered as a digital asset on a high-performance, EVM-compatible, Proof-of-Stake (PoS) blockchain environment — a foundation chosen because it offers the combination institutional users require: cryptographic security, fast and deterministic settlement finality, high transaction throughput, low fees, and a mature developer and tooling ecosystem. The specific production network is being finalised from among the leading high-throughput PoS layer-1 and layer-2 networks; the architecture, however, is defined by the design requirements set out below rather than by any single vendor, and is portable across compatible chains.

The decentralised ledger

At its base, ASD relies on a distributed, append-only ledger replicated across an independent validator set. Every issuance, redemption, transfer, and reward distribution is recorded immutably and is publicly verifiable. This removes reliance on a single trusted operator: state is agreed by consensus, history cannot be silently rewritten, and any participant can independently audit the chain of transactions. Immutability and public verifiability are not features bolted onto ASD — they are the substrate on which its transparency commitments rest.

Consensus mechanism

ASD's environment uses a modern Proof-of-Stake consensus with Byzantine-fault-tolerant finality. Validators commit economic stake to participate in block production and are penalised (slashed) for malicious or negligent behaviour, aligning their incentives with the integrity of the network. Compared with Proof-of-Work, PoS delivers comparable or superior security with a fraction of the energy cost and with rapid, deterministic finality — meaning a settled transaction is mathematically final within seconds rather than probabilistically final after many confirmations. A sufficiently large and well-distributed validator set is prioritised to resist collusion and centralisation.

Throughput and ultra-low fees

The architecture is designed to sustain high transaction throughput — on the order of thousands of transactions per second at the base and scaling further through layer-2 execution — with finality measured in seconds and transaction (gas) costs of a fraction of a cent. These are design targets reflecting the demonstrated capabilities of the network class ASD is built on, not promises of a fixed figure; real throughput depends on network conditions. The objective is unambiguous: ASD must remain practical and cheap for everyday transfers, remittances, and merchant settlement, where high or volatile fees would defeat the purpose of the system.

SECTION 4 — BLOCKCHAIN ARCHITECTURE & TECHNOLOGY

16. Smart-Contract Automation & Framework

The operational logic of the ASD ecosystem — issuance against reserves, redemption, reserve accounting, fee handling, and the distribution of participation rewards — is governed by audited smart contracts: deterministic, self-executing programs that run exactly as written, identically for every participant, with their behaviour recorded on-chain. By moving rule-bound processes into code, ASD reduces dependence on manual intervention and discretionary control, which in turn reduces the scope for human error and limits the opportunity for unilateral manipulation.

It is important to state this precisely rather than to overclaim. Smart contracts remove discretion from defined processes, but they are still software, and software can contain defects. ASD therefore does not claim that automation makes manipulation or error impossible; it claims, accurately, that a disciplined contract framework — combined with the audit and control regime described in Section 5 — substantially narrows those risks.

Architectural principles

- **Modularity and least privilege.** Functions are separated into focused, independently reviewable modules, each granted only the permissions it strictly requires.
- **Administrative controls under multi-signature and timelocks.** Privileged actions are not held by a single key; they require multiple authorised approvals and, for sensitive changes, a mandatory time delay during which the community can react.
- **Governed, transparent upgradeability.** Upgrades follow a transparent governance process with timelocks, so changes are visible and contestable before they take effect — never silent.
- **Formal verification and exhaustive testing.** Critical components are subjected to formal methods where feasible and to comprehensive unit, integration, and adversarial testing before deployment.
- **Emergency safeguards.** Defined, governance-controlled pause and circuit-breaker mechanisms allow the protocol to halt specific functions in the event of a detected anomaly, limiting potential damage while a fix is prepared.

The result is an ecosystem whose core rules execute predictably and verifiably, whose privileged powers are constrained and observable, and whose failure modes are anticipated and bounded rather than ignored.

SECTION 4 — BLOCKCHAIN ARCHITECTURE & TECHNOLOGY

17. Ecosystem Interoperability & Cross-Chain Bridging

Value that cannot move freely is value trapped. ASD is therefore designed for interoperability: because it is EVM-compatible, it can be deployed across multiple leading blockchain networks, allowing holders to use ASD wherever the liquidity, applications, and users they need already exist. The goal is a single, coherent unit of gold-anchored value with a presence across the chains that matter, rather than an asset stranded on one island of liquidity.

Secure cross-chain movement

Cross-chain functionality is delivered through audited bridging and cross-chain messaging, designed conservatively. This caution is deliberate and informed: bridges have historically been among the most heavily exploited components in the entire industry, responsible for some of its largest losses. ASD's approach therefore favours rigorously audited mechanisms, validated message-passing, conservative limits, and monitoring over aggressive, speed-first expansion. Where a bridging model introduces risk that cannot be adequately controlled, ASD will not adopt it; security takes precedence over reach.

Real-world and e-commerce integration

Beyond chain-to-chain movement, ASD is built to connect with real-world commerce through documented application programming interfaces (APIs) and software development kits (SDKs). Merchants, payment processors, and e-commerce platforms can integrate ASD for pricing, checkout, and settlement using clear, well-supported interfaces — with settlement APIs, webhooks for confirmation, and reference integrations. This is how a gold-anchored unit becomes usable at the point of sale and in business settlement, not merely held in a wallet, extending the network's utility into the economy it is meant to serve.

SECTION 4 — BLOCKCHAIN ARCHITECTURE & TECHNOLOGY

18. The Native ASD Digital Wallet Architecture

The wallet is where most users will experience ASD, so it is designed to make security effortless and global utility intuitive. Its guiding philosophy is that the safest behaviour must also be the easiest — protection should be the default, not an expert option.

UI / UX philosophy

The interface is built to be approachable for newcomers and efficient for advanced users: clean flows for sending, receiving, redeeming, and staking; plain-language confirmations; contextual safety prompts before irreversible actions; and clear visibility of reserve-attestation status, so holders can see the backing behind what they hold. Complexity is hidden by default and available on demand.

Keys and account security

Security is layered. The wallet supports non-custodial key ownership, where users hold their own keys, as well as advanced protections designed to reduce the catastrophic risk of a single lost key: optional multi-party computation (MPC) and social-recovery schemes that remove single points of failure, support for hardware wallets, device-level biometric and PIN protection, and encrypted local storage with no plaintext key material. Sensitive operations are confirmed explicitly, and recovery options are designed to balance self-custody with resilience. Users are clearly informed of their responsibilities in non-custodial mode, because honest guidance is part of keeping them safe.

Cross-border utility

Functionally, the wallet is a global instrument: it enables fast, low-cost transfer and settlement across borders at any hour, integrates with partner on- and off-ramps for conversion to and from local currency where available and compliant, exposes redemption against reserves, and provides access to participation programmes. The aim is a single application through which a holder anywhere can store, verify, move, and use gold-anchored value.

SECTION 5 — ADVANCED CYBERSECURITY & SAFETY

19. Institutional-Grade Security Protocols

ASD's security model is built on the principle of defense-in-depth: no single control is trusted to be sufficient, so protections are layered such that the failure of one does not compromise the whole. The objective is to make a successful attack require defeating many independent safeguards at once — while accepting, honestly, that no system can be declared unbreakable.

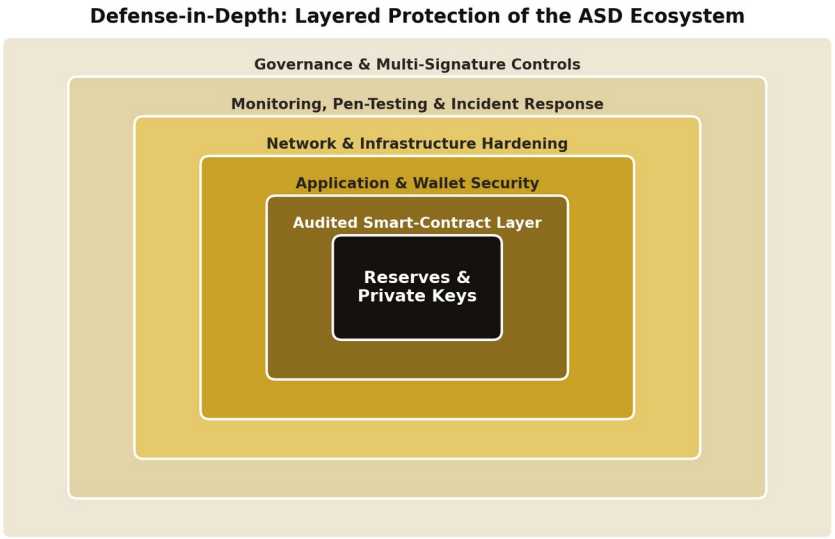

Figure 1 — Layered protection. Each layer is independent; the failure of one does not defeat the rest.

Encryption and key protection

Data is protected with strong, industry-standard cryptography — AES-256 for data at rest and TLS 1.3 for data in transit — and the most sensitive operations are performed inside hardware security modules (HSMs) so that private keys are never exposed in plaintext. Access follows a zero-trust, least-privilege model with strict segregation of duties, so that no individual and no single compromised credential can unilaterally move value or alter critical systems.

Anti-intrusion and resilience

The infrastructure employs web-application firewalls, distributed-denial-of-service protection, network segmentation, rate limiting, and hardened configurations to resist intrusion and disruption. These measures are designed to raise the cost of attack dramatically and to contain any breach that does occur.

Continuous testing and monitoring

Security is treated as an ongoing process, not a one-time event. ASD's programme provides for regular independent penetration testing and red-team exercises, continuous vulnerability scanning, around-the-clock security monitoring with anomaly detection, a documented incident-response plan with defined escalation, and a public bug-bounty programme that rewards researchers for responsibly disclosing issues before adversaries can exploit them.

AN HONEST SECURITY POSTURE

These controls are designed to reduce the likelihood and limit the impact of attacks to the greatest extent practicable. They do not make the system invulnerable — no system is. ASD's commitment is to defend rigorously, to monitor continuously, and, if an incident occurs, to disclose and remediate transparently. A project that claims it cannot be hacked is telling you something untrue; a project that tells you how it would respond is telling you something useful.

SECTION 5 — ADVANCED CYBERSECURITY & SAFETY

20. Asset Custody & Multi-Signature Vaults

The integrity of ASD ultimately rests on the safekeeping of two things: the physical gold that backs it, and the cryptographic keys that control issuance and the protocol treasury. Both are protected by a custody model designed to eliminate single points of failure and to require distributed, deliberate authorisation for any significant action.

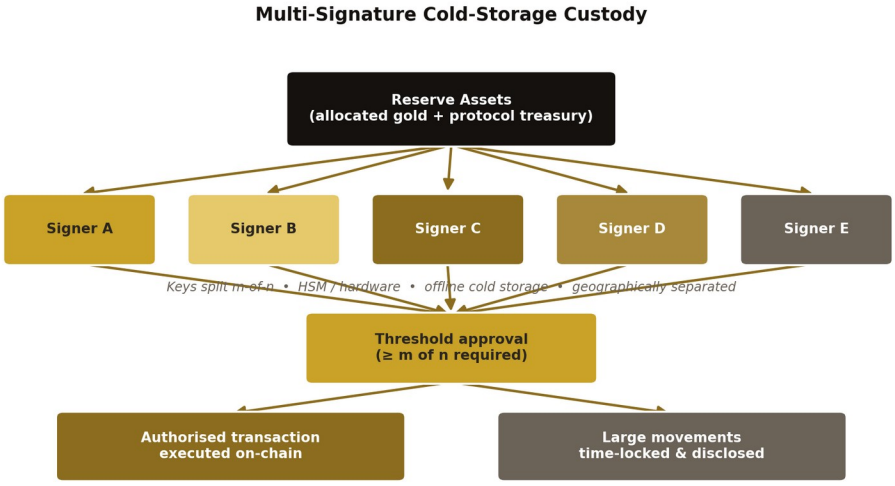

Figure 2 — Reserve assets are controlled by keys split across geographically separated, offline signers; movement requires threshold approval.

Reserve gold custody

Physical gold reserves are intended to be held with professional, qualified custodians on an allocated and segregated basis — distinct from operating funds — under arrangements designed for security, insurance coverage, and independent verification. The reserve exists to back ASD, and the custody model is structured so that it cannot be quietly diverted to other uses.

Multi-signature cold storage for keys

Cryptographic control of protocol assets uses multi-signature (multi-sig) vaults: authority over reserves and the treasury is split among multiple independent signers under an m-of-n threshold, so that no single person can move funds and the compromise of any one key is insufficient to cause loss. Keys are generated and held within hardware security modules or hardware wallets, the bulk of assets are kept in offline cold storage isolated from the internet, and signers are geographically distributed to resist localised compromise or coercion. The minimal balances required for day-to-day operations are tightly limited.

Controls on movement

Beyond the threshold requirement, large movements are subject to time-locks and disclosure, giving the organisation and its community a window to detect and respond to any anomalous or unauthorised request before it can settle. Custody arrangements, and the attestation of reserves, are designed to be independently verified rather than self-certified.

SECTION 5 — ADVANCED CYBERSECURITY & SAFETY

21. Third-Party Smart-Contract Audits

Independent security auditing is mandatory in ASD's development lifecycle, not optional. No smart contract that handles reserves or user funds is intended to reach production without having undergone independent third-party security review, with findings remediated and the results published for the community to inspect.

Audit programme and cadence

The programme provides for a comprehensive audit prior to mainnet deployment and for re-audits whenever contracts are materially upgraded, supplemented by continuous monitoring between formal reviews. ASD intends to engage tier-one blockchain security firms — the calibre represented by firms such as CertiK, Hacken, Trail of Bits, OpenZeppelin, and Quantstamp — for these reviews. These names are cited to indicate the standard of independent scrutiny the project intends to meet; the firm or firms actually engaged, together with the dated audit reports, will be published once the engagement is complete, and this document should not be read as asserting a current relationship with any specific firm.

Beyond a single audit

Auditing is necessary but not, on its own, sufficient. For critical components, formal verification is used to mathematically check defined properties; a standing bug-bounty programme incentivises continuous external scrutiny; and the defense-in-depth, multi-sig, monitoring, and emergency-pause controls described above exist precisely to contain any issue that all of the foregoing might still miss.

> **ON 'ZERO VULNERABILITIES'**
>
> No audit — from any firm, however eminent — can guarantee that code is free of all vulnerabilities; serious auditors say so themselves. Any project promising 'absolute' or 'guaranteed' elimination of all bugs is misrepresenting how security works. ASD's commitment is stronger because it is truthful: rigorous, repeated, independent auditing, published in full, backed by formal verification, bug bounties, monitoring, and layered containment for the residual risk that always remains.

SECTION 5 — ADVANCED CYBERSECURITY & SAFETY

22. Capital-Protection & Risk-Mitigation Framework

Serious investors do not want to be told that risk has been abolished; they want to see that it has been understood, structured, and managed. This section sets out how ASD is designed to protect capital and to withstand market crashes and extreme 'black swan' events — and it is equally clear about the limits of what any such framework can achieve.

The layers of protection

1. **Full reserve backing.** The primary protection is structural: circulating ASD is designed to be backed at or above 100% by allocated physical gold, so the unit's value is tied to a tangible asset rather than to market sentiment that can evaporate in a panic.
2. **An over-collateralisation buffer.** The reserve mandate targets coverage above the 100% floor, creating a buffer intended to absorb operational costs and short-term market movement without breaching backing.
3. **A conservative reserve mandate.** Reserves are concentrated in physical gold and highly liquid assets, governed by strict limits that prioritise the integrity and redeemability of backing over the pursuit of yield.
4. **Risk management and hedging — stated accurately.** Gold itself functions as a hedge against fiat debasement and inflation, which is central to ASD's design. Within its mandate, the project may employ defined risk-management measures to manage specific operational exposures. What hedging cannot do — and what ASD will never claim it does — is remove market risk: the price of gold can fall, and with it the value referenced by ASD.
5. **Emergency procedures and circuit breakers.** Governance-controlled pause mechanisms, multi-signature authorisation, and defined incident-response playbooks allow the protocol to react to extreme events in a controlled, transparent manner.
6. **Insurance and transparency.** The project intends to pursue appropriate custody insurance, and periodic independent attestation is designed to surface problems early — the most valuable protection of all, because risks detected early are risks that can be managed.

Black-swan events

By definition, black-swan events exceed historical models and cannot be fully anticipated. ASD's resilience against them rests not on a claim of prediction but on robustness: tangible backing rather than reflexive leverage, conservative reserves rather than fragile yield-chasing, distributed custody rather than single points of failure, and the ability to pause and respond rather than to freeze. These properties are designed to help the system endure shocks — not to make it immune to them.

Risk	How ASD is designed to mitigate it
Gold-price decline	Backing in a tangible asset; over-collateralisation buffer; long-horizon, value-preservation framing. Residual market risk remains.

Risk	How ASD is designed to mitigate it
Market crash / panic	Value anchored to reserves rather than sentiment; circuit breakers; transparent attestation to maintain confidence.
Smart-contract failure	Audits, formal verification, bug bounty, emergency pause, multi-sig containment.
Custody / theft	Allocated, segregated custody; multi-sig cold storage; geographic key distribution; target insurance.
Liquidity stress	Liquidity provisioning; conservative, liquid reserves; defined redemption framework.
Regulatory shock	Jurisdiction-by-jurisdiction authorisation; qualified counsel; compliance-first design.

THE STATEMENT WE WILL NOT MAKE — AND WHY

We will not tell you that this framework guarantees your principal remains 100% safe, because that statement would be false, and a false guarantee is the single most reliable warning sign of investment fraud. No reserve fund, hedge, or control can guarantee principal in an asset whose value moves with the gold market and which carries technology, custody, and regulatory risk. Capital invested in ASD is genuinely at risk, and you could lose value, potentially all of it.

What we offer instead is a rigorously engineered framework to reduce, contain, and survive risk — and the honesty to tell you where its limits are. That honesty is not a weakness in this pitch. It is the strongest evidence that the people behind ASD intend to be trustworthy stewards of your capital.

SECTION 6 — COMPLIANCE, ROADMAP & CLOSING

23. Global Regulatory Compliance Framework

ASD's strategy is to grow within the law, market by market, building compliance into the product rather than treating it as an obstacle. The summary below describes the principal regimes that bear on a gold-backed digital asset and the project's intended posture toward them. It is a general framework, not a legal opinion; classification and licensing are matters for qualified counsel in each jurisdiction, and the project commits to obtaining that advice before offering ASD in any given market.

European Union — MiCA

Under the EU's Markets in Crypto-Assets Regulation (MiCA), a token that references the value of a commodity such as gold is treated as an asset-referenced token (ART).[1] An ART issuer must be established in the EU and authorised by a national competent authority, must maintain full, segregated reserves in highly liquid form, must publish a compliant white paper disclosing technology, risks, and reserve policy, must afford holders redemption rights, and must undergo regular audits, with enhanced supervision for tokens deemed 'significant.' ASD's gold-referenced design places it squarely within this ART regime, and the project's reserve, transparency, and audit commitments are aligned to those requirements.

United States — a nuanced picture

In the United States, the GENIUS Act of 2025 created the first comprehensive federal framework for payment stablecoins, and provides that compliant payment stablecoins are treated as neither securities nor commodities.[2] Crucially, that regime is built around stablecoins that reference the US dollar. A gold-backed token is not a USD payment stablecoin, and therefore cannot simply assume the GENIUS Act's favourable classification. Its US treatment requires separate, careful analysis — potentially engaging commodity regulation, the securities-law 'investment contract' analysis, and state money-transmitter licensing — and is precisely the kind of question on which the project will rely on specialist US counsel rather than on assumption.

Digital-asset taxonomy and global posture

Correct classification is the foundation of compliance: ASD must be characterised accurately — as an asset-referenced or commodity-backed instrument — under the taxonomy of each jurisdiction, because that characterisation determines which authorisations, disclosures, and protections apply. Across markets, the project's posture is consistent: obtain jurisdiction-specific legal opinions, secure the required authorisations or licences before launch in a market, implement the Travel Rule and applicable transfer-of-funds requirements, and decline to operate where it cannot do so compliantly. ASD does not claim to be 'already compliant everywhere'; it commits to doing the work, jurisdiction by jurisdiction, that genuine compliance requires.

[1] EU MiCA: tokens referencing commodities such as gold are asset-referenced tokens (ARTs); ART issuers require EU authorisation, full segregated reserves, a published white paper, redemption rights, and regular audits. MiCA stablecoin rules applied from 30 June 2024; transitional period ends 1 July 2026 (ESMA/EBA). Verify current requirements with counsel.

[2] US GENIUS Act, signed 18 July 2025: first federal framework for USD payment stablecoins; compliant payment stablecoins treated as neither securities nor commodities; implementing rules in progress (OCC/FDIC/Fed/Treasury, ~2026). A gold-backed token is not a USD payment stablecoin and requires separate analysis. Not legal advice.

SECTION 6 — COMPLIANCE, ROADMAP & CLOSING

24. KYC & AML: The Compliance Engine

A clean ecosystem is a prerequisite for institutional trust and regulatory good standing. ASD is designed around a robust, risk-based Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) programme, substantially automated so that compliance is consistent, auditable, and scalable rather than dependent on manual discretion.

Identity verification

Onboarding incorporates identity verification using government-issued documents combined with biometric liveness checks to confirm that a user is genuine and present, calibrated to the risk and to local regulatory requirements. Business and institutional onboarding extends to beneficial-ownership and enhanced due-diligence checks.

Screening and ongoing monitoring

Users and counterparties are screened against sanctions lists, politically-exposed-person (PEP) databases, and adverse-media sources at onboarding and on an ongoing basis. Automated transaction monitoring applies risk-based rules and behavioural analytics to detect patterns associated with money laundering, fraud, or sanctions evasion, generating alerts for review by a qualified compliance team.

Reporting, recordkeeping, and the Travel Rule

Where activity warrants, the programme provides for the filing of suspicious-activity reports to the relevant authorities, for compliant collection and transmission of originator and beneficiary information under the Travel Rule, and for the retention of records consistent with applicable law. The programme is overseen by a designated compliance function, subject to independent testing and periodic review, with staff training and clearly restricted or geofenced jurisdictions where ASD does not operate. The objective is unambiguous: to keep the ecosystem clean, to protect honest users, and to give regulators confidence that ASD is run responsibly.

SECTION 6 — COMPLIANCE, ROADMAP & CLOSING

25. Roadmap — Phase 1: Foundation & Token Genesis (Next 6–12 Months)

Phase 1 is deliberately weighted toward the unglamorous work that earns trust: legal structuring, reserves, audits, and compliance must precede scale. Timeframes are indicative and subject to regulatory and operational sequencing.

Workstream	Phase 1 objectives
Legal & structuring	Establish entity and governance; engage qualified counsel; select launch jurisdictions and begin authorisation pathways.
Reserves & custody	Engage qualified custodians; begin allocated gold acquisition; establish segregation and attestation arrangements.
Technology	Complete smart-contract development; testnet; independent security audits with published reports; deploy mainnet.
Compliance	Stand up KYC/AML engine, sanctions screening, and Travel-Rule capability.
Product	Launch the native ASD wallet with issuance, redemption, and reserve-verification visibility.
Genesis & liquidity	Token genesis and public distribution; initial liquidity provisioning; first published reserve attestation.

The defining milestone of Phase 1 is not the token sale; it is the first independently published reserve attestation alongside completed, published audits. That is the moment ASD asks the market to trust it — and arrives with the evidence to justify the request.

SECTION 6 — COMPLIANCE, ROADMAP & CLOSING

26. Roadmap — Phase 2: Global Integration & Utility Expansion (Years 1–2)

Phase 2 turns a credible asset into a widely used one, expanding utility, liquidity, and reach while deepening compliance.

- Secure listings on reputable exchanges and deepen liquidity and redemption access across venues.
- Open remittance and cross-border settlement corridors in priority markets, targeting the high-fee flows where ASD's advantage is sharpest.
- Onboard merchants and e-commerce platforms via settlement APIs and reference integrations.
- Deploy audited cross-chain interoperability and broaden wallet compatibility.
- Launch revenue-funded staking and participation programmes with transparent, published rules.
- Pursue MiCA asset-referenced-token authorisation in the EU and expand licensing into additional jurisdictions.
- Move toward more frequent — progressing to near-real-time — proof-of-reserves.

Throughout Phase 2, growth is gated by compliance and security: ASD will expand into a market when it can do so lawfully and safely, and not before.

SECTION 6 — COMPLIANCE, ROADMAP & CLOSING

27. Roadmap — Phase 3: Toward a Global Standard & Institutional Integration (Year 3+)

Phase 3 sets out ASD's long-term ambition: to become a widely trusted standard for asset-backed digital value, integrated into commerce and treasury operations at scale. This is stated honestly as a direction of travel, not a guaranteed destination — each milestone is contingent on execution, adoption, regulation, and market conditions.

- Pursue institutional and treasury-grade adoption with the controls, reporting, and tooling such users require.
- Extend global market coverage and settlement corridors, and deepen liquidity toward reference-asset reliability.
- Advance reserve verification to continuous, on-demand transparency.
- Mature decentralised governance and community ownership of the protocol.
- Explore integration with broader financial and institutional infrastructure where compliant and beneficial.

> **ON 'SOVEREIGN RESERVE INTEGRATION'**
>
> The prospect of asset-backed digital instruments being held at institutional or sovereign scale is a legitimate long-term theme in global finance — but it would depend on regulatory acceptance, scale, and trust that must be earned over many years, and it is entirely outside any single project's control. We therefore present it as a long-horizon aspiration that informs our direction, not as a planned or promised milestone. Describing it as anything more certain would mislead, and ASD's credibility depends on never doing that.

SECTION 6 — COMPLIANCE, ROADMAP & CLOSING

28. The Investor Call to Action

Every section of this document has argued a single, deliberate case: that the next generation of trusted digital value will be built by the projects with the strongest foundations, not the loudest promises. ASD has been engineered, from the reserve outward, to be one of them — anchored to physical gold, secured in depth, custodied across distributed and offline controls, independently audited, and built to grow within the law.

The opportunity is structural rather than fleeting. Gold is the most valuable asset class on earth; demand for stable, digitally-native value is already vast and rising; and the category that unites them — transparent, gold-backed digital assets — remains remarkably small relative to both. An investor who recognises that asymmetry, and who values disciplined execution over spectacle, has a genuine reason to engage with ASD at its foundation stage, when conviction and contribution count for the most.

We make our case with confidence, and without the pressure tactics this industry has too often relied upon. We will not tell you that you must act this instant or miss the chance of a lifetime; manufactured urgency is the language of schemes, not of sound investments, and the asymmetry described here does not evaporate overnight. What we will tell you is this: the opportunity is real, the foundation is being built with unusual rigour, and the right investors for ASD are those who do their own diligence and arrive with their eyes open. Foundation-stage participation carries the greatest potential and, candidly, the greatest risk; it suits conviction capital that can hold through cycles, not money that cannot afford to wait or to lose.

> **AN INVITATION, ON HONEST TERMS**
>
> If you want exposure to a transparently gold-backed digital asset built by people who tell you the risks as plainly as the rewards — examine our verified data room, scrutinise our audits and attestations, take independent advice, and decide on the evidence. We would welcome that conversation, and we are confident in what your diligence will find. Reach us at support@asdcoins.us.

SECTION 6 — COMPLIANCE, ROADMAP & CLOSING

29. Glossary, Legal Disclaimers & Risk Disclosures

Institutional Glossary of Terms

Term	Meaning
Allocated gold	Physical gold specifically assigned and segregated to back reserves, rather than a general unsecured claim.
AML / KYC	Anti-Money-Laundering / Know-Your-Customer compliance procedures.
ART (Asset-Referenced Token)	Under EU MiCA, a token referencing the value of assets such as commodities (e.g., gold); ASD's likely classification.
Attestation / Proof-of-Reserves	Independent verification that reserves exist and cover circulating units, published for holders.
BFT finality	Byzantine-fault-tolerant consensus producing rapid, deterministic settlement finality.
Cold storage	Holding cryptographic keys offline, isolated from the internet, to resist remote compromise.
EVM-compatible	Able to run on the Ethereum Virtual Machine standard, enabling multi-chain portability.
HSM	Hardware security module — tamper-resistant hardware for secure key generation and storage.
MiCA	The EU's Markets in Crypto-Assets Regulation governing crypto-assets and stablecoins.
MPC	Multi-party computation — splitting key control across parties so no single party holds a complete key.
Multi-signature (multi-sig)	A control requiring m-of-n independent approvals to authorise an action.
Proof-of-Stake (PoS)	A consensus mechanism securing the network through staked economic value rather than computational work.
Slashing	Penalising validators by confiscating staked value for malicious or negligent behaviour.
Travel Rule	Requirement to transmit originator and beneficiary information with qualifying transfers.

Legal Disclaimers

This document is provided for general information only. It is not, and must not be construed as, an offer to sell or a solicitation of an offer to buy any security, token, or financial instrument, nor as investment, legal, tax, or accounting advice, in any jurisdiction where such an offer, solicitation, or advice would be unlawful. The regulatory discussion is a general description of frameworks and intended posture; it is not a legal

opinion and may not be relied upon as one. Classification and licensing depend on facts and on the law of each jurisdiction and are matters for qualified counsel.

Forward-looking statements, roadmaps, targets, and illustrative figures involve assumptions, risks, and uncertainties and are not guarantees of future performance; actual results and timelines may differ materially. References to third-party firms or standards are illustrative of intended quality and do not assert any existing engagement, endorsement, or affiliation unless expressly stated and substantiated.

Risk Disclosures

An investment in or holding of ASD involves significant risk, including the possible loss of some or all of the value committed. Risks include, without limitation:

- **Market & gold-price risk:** the price of gold can fall; the value referenced by ASD can fall with it.
- **Technology & smart-contract risk:** software may contain vulnerabilities despite audits; exploits can cause loss.
- **Custody & key risk:** failure, theft, or compromise of custody or keys, despite controls, could result in loss.
- **Bridge & interoperability risk:** cross-chain mechanisms are a known attack surface.
- **Regulatory & legal risk:** laws may change or restrict ASD in some jurisdictions; classification is uncertain and consequential.
- **Liquidity & redemption risk:** liquidity and the ability to redeem depend on market conditions.
- **Counterparty risk:** reliance on custodians, auditors, exchanges, and partners.
- **Black-swan & execution risk:** extreme events exceed models; an early-stage project may fail to meet its objectives.

No return, yield, redemption value, or preservation of capital is guaranteed. Prospective participants should conduct independent due diligence and obtain independent legal, tax, and financial advice, and should rely on verified data — audited attestations, security-audit reports, legal opinions, and validated models — rather than on any illustrative content in this document.