QUANTUM SHIELD

Evidence before trust.

White Paper

Web3 security for people, companies, and AI agents.

VERSION 1.1 / PUBLIC BETA

4 October 2026

QUS Planned service-payment token
1,000,000,000 Planned total supply
x402 Planned agent micropayments

Live capabilities, limits, and the roadmap are distinguished throughout.
Token deployment and payments are not active.

Inside this paper

1. Executive summary 3

2. The problem and the users 3

3. Product portfolio and current availability 4

4. Website security methodology 5

5. Wallet intelligence and destination attribution 6

6. Post-quantum readiness 6

7. Architecture and trust boundaries 7

8. QUS service-payment token 7

9. x402 and agent micropayments 8

10. Service model and sustainable revenue 8

11. Security, privacy, and responsible reporting 9

12. Delivery roadmap and release gates 10

13. Research basis and project boundaries 10

14. References and version record 11

Read the current status and coverage before relying on a report. This document specifies service-payment utility only; no tokenomics or allocation schedule is included.

1. Executive summary

Quantum Shield is building an accessible security intelligence service that helps people examine websites and public blockchain activity before making decisions. Its central principle is simple: show the evidence, explain the uncertainty, and never turn missing information into a promise of safety.

The public beta brings together domain reputation, AI-assisted website source review, wallet snapshots, token metadata, wallet comparison, recent Ethereum and Base activity, and a limited local image-format check. Users can explore these tools without an owner account or payment. The service does not hold assets, request recovery phrases, or sign transactions on the user's behalf.

The longer-term product is a layered service for individuals, company security teams, and software agents. Planned improvements include isolated website interaction testing, transaction and signature analysis, broader historical indexing, better destination attribution, company reporting, and cryptographic-readiness workflows. Each capability must pass a defined validation gate before it is described as operational protection.

QUS is the planned Quantum Shield service-payment token, with a planned total supply of **1,000,000,000 QUS**. Its intended utility is payment for selected services that become paid in the future. Quantum Shield also plans to integrate **x402** so compatible AI agents can purchase individual results through small, transparent payments. Neither QUS payments nor x402 settlement is active in the beta. This paper does not specify token allocations, distribution, vesting, or other tokenomics.

2. The problem and the users

A convincing website, familiar logo, or unlisted domain is not evidence that connecting a wallet is safe. Harmful behavior may appear only after a click, after a wallet connects, or when a user signs a message or spending approval. An attack may use ordinary wallet APIs, while an innocent site may contain the same APIs inside a legitimate library. A useful security report must distinguish a code reference, an observed request, and a demonstrated effect.

Blockchain investigation presents a different problem. People need an understandable record of transfers, timing, amounts, and destinations. Data is spread across networks and providers; address labels may be absent, outdated, or incomplete. A public address does not establish a person's identity, and a transfer to an unlabeled address does not establish an exchange deposit.

Quantum Shield serves three groups. Individuals need understandable checks before interacting with a link, wallet, or token. Companies need repeatable evidence, ownership of review tasks, history, and integration into existing workflows. AI agents need bounded machine-readable results and, eventually, a way to pay small amounts for specific services within a spending policy.

The commercial focus is companies, with a free entry point for individual users. The product should earn repeat use through useful evidence and clear workflows. It should not depend on frightening scores, promises of guaranteed protection, or token price expectations.

3. Product portfolio and current availability

Product	Public beta capability	Important boundary
Website Code + AI Review	Reads a public HTTPS page and limited same-origin scripts; combines rules with AI-selected evidence	Static review only; no wallet interaction or transaction simulation
Domain Reputation Check	Looks up reported threats and checks visible URL patterns	An unlisted domain is not a safe domain
Wallet Scanner	Reads account code, nonce, native balance, and block evidence on Ethereum, Base, BNB Chain, Arbitrum, or Polygon	No ownership verification, contract audit, or theft prediction
Token Check	Reads available name, symbol, decimals, and reported supply	Metadata can be misleading; no endorsement or complete token-risk assessment
Wallet Compare	Compares two addresses on one supported network at a common block	Not a cross-chain asset portfolio or identity match
Wallet Activity	Combines recent Ethereum and Base transaction and token-event pages	Not complete history, 20-chain coverage, or complete exchange attribution
Image File Check	Locally compares a supported image header with its filename	Not antivirus, image-exploit detection, or QR analysis
Team Treasury	Wallet sign-in, team policies, invitations and saved transfer drafts	Workspace preview only; no deposits, on-chain wallet or execution
Company workspace	Owner-only pilot for saved reports and manual watch checks	Not open company onboarding; external keys and invitations are disabled on the main domain

Quantum Vault, automatic asset protection, post-quantum account migration, real-time attack prevention, and a public paid agent API are roadmap capabilities. Marketing illustrations, animated network maps, and example security scores are demonstrations, not live security measurements.

Team Treasury: multisignature custody roadmap

Team Treasury has a live workspace preview for wallet sign-in, team access, saved signer configurations and transfer drafts. It does not yet deploy an on-chain wallet, receive deposits or execute transactions. Email delivery is pending. Initial configurations cover Base Sepolia, Ethereum Sepolia and Solana Devnet, not all chains.

The required custody architecture is non-custodial, with team-controlled keys and on-chain threshold enforcement through separately verified Safe and Squads integrations. Quantum Shield must have no privileged spending or signer-replacement key. Each network needs its own wallet and token verification. Users must retain a tested independent protocol interface or direct-contract recovery path when our service is unavailable. Ordinary multisig is not post-quantum protection.

The current website, authentication and draft storage are centralized Cloudflare services; this release must not be called completely decentralized. Future funds and approval authority must be independent of that off-chain workspace. Protocol upgrade authority, modules, external RPC services and token issuer controls remain dependencies that must be evaluated and disclosed.

No treasury platform fee or recipient wallet is configured. The project owner will provide the recipient and fee schedule later. Network gas is distinct from a Quantum Shield service fee. Future fee amount, asset, network and recipient must be displayed before signing and bound to the approved transaction; no hidden deductions, unlimited approvals, automatic fee collection or platform-controlled custody are permitted. Users must retain an independent access route without a Quantum Shield exit fee. See the Team Treasury specification for current status and release gates.

4. Website security methodology

Domain reputation

The domain check identifies the actual destination hostname, checks patterns such as misleading credentials before an @ symbol and shortened links, and consults PhishDestroy. Only the hostname is sent for that reputation lookup. A threat report is attributed to its source. An unavailable provider produces an incomplete result, not a clean report.

Static page and script review

The deeper scan requests one public HTTPS page and up to three same-origin scripts referenced in its HTML. Each source is capped at 200 KB. Redirects are bounded and checked; non-public destinations and credential-bearing or custom-port URLs are rejected. The scanner does not execute downloaded code, connect a wallet, or submit a transaction. Cross-origin scripts, dynamically loaded imports, server-side code, authenticated views, and code beyond the limits remain uninspected.

Rules identify possible recovery-secret requests, token approvals, NFT operator approvals, Permit or typed-signature references, wallet transaction calls, and selected encoded-code execution patterns. A match is evidence for review, not automatic proof of a wallet drainer. Reports identify the source and show the relevant excerpt.

AI-assisted evidence review

Cloudflare Workers AI reviews selected public source excerpts. The current adapter uses GLM-4.7-Flash and limits input to the first 10,000 characters of each inspected source. Model choices may change with availability and evaluation. The model is instructed to treat website content as untrusted data. A proposed finding is accepted only when its quote exists in the submitted source. Free-form model instructions are not shown as user advice, and AI cannot erase a rule-based warning.

These controls constrain the review; they do not prove the model is correct or immune to manipulation. AI can miss an attack, misunderstand context, or flag legitimate code. Provider failure and invalid model output are shown explicitly. The interface uses findings that need review, red flags, or unverified status. It does not issue a certificate that a website is safe to connect to.

Protection still to be built

A stronger wallet-drainer defense requires an isolated browser environment, controlled test accounts, capture of requested wallet methods, signature interpretation, contract and spender checks, and transaction-effect simulation. It also needs representative attack samples and legitimate applications for evaluation. These components are planned, not implemented in the current scanner. Even simulated results would apply to a particular request and state, not every future action a website could perform.

5. Wallet intelligence and destination attribution

Account snapshots validate the provider's network identity and inspect state at a recorded block. The analysis preserves large blockchain quantities as strings and checks block consistency rather than converting financial amounts to imprecise floating-point numbers. Account code can indicate a contract or an EIP-7702 delegation marker; it does not establish that the policy is secure. A nonce is an activity signal, not a complete public-key exposure assessment.

Wallet Activity combines recent transaction and token-event pages from the Ethereum and Base Blockscout explorers. Results show UTC time, direction, amount where available, network, counterparty, source status, and any supplied public label. Failed transactions are identified as attempts. Transaction hashes are not displayed in the activity interface. That display choice does not remove the underlying need for traceable evidence during professional investigation.

An exchange name is shown only when supported by the source's public labeling. A contract's name alone is not proof of exchange ownership. Internal exchange transfers are generally outside public-chain visibility. Bridges require separate attribution and correlation; the same address on different networks does not by itself prove common ownership. Unknown destinations remain unknown.

The roadmap adds pagination, validated network adapters, internal transfer coverage, bridge-event interpretation, and licensed or independently verified labels. Expanded coverage must disclose which networks, block ranges, transfer types, and attribution sources were actually queried. Reports may help a project prepare evidence requested by an exchange, but cannot guarantee listing approval or replace that exchange's diligence.

6. Post-quantum readiness

Quantum Shield's name expresses a long-term research direction as well as the need for present-day security. The public beta does not make Ethereum, Base, a wallet, or QUS quantum-resistant. Website fraud checks and post-quantum cryptography address different problems.

NIST's finalized ML-KEM, ML-DSA, and SLH-DSA standards provide foundations for key establishment and digital signatures. They are not interchangeable building blocks. Integrating an algorithm into one component does not secure an entire signing, recovery, consensus, or custody system. [1]

The proposed readiness service will inventory signing mechanisms and dependencies, identify evidence gaps, document migration options, and support test-environment evaluation. Any future Quantum Vault or migration product needs a defined threat model, reviewed cryptographic implementation, recovery design, independent assessment, and deployment-specific testing. This roadmap does not predict a date when quantum computers will compromise existing networks.

7. Architecture and trust boundaries

The main deployment runs on Cloudflare Workers, with static web assets, public read-only service endpoints, Workers AI for source review, and D1 for private workspace records and rate-limit counters. Namecheap remains the domain registrar; registrar ownership is distinct from application hosting. Local development uses Node.js and SQLite. No proprietary blockchain or decentralized validator network is required for the current product.

Public browser tools use bounded application endpoints and, where disclosed, direct public RPC or explorer reads. The domain checker can use a browser reputation lookup if the server lookup is unavailable. Each external provider is a separate trust and availability dependency. A successful HTTP response is not automatically complete or trustworthy evidence.

The company workspace on the main domain is owner-only and uses a secure signed session. Public tools do not require that session. Private records remain behind server-side access controls; public tools do not expose company records. External API-key issuance and company invitations are disabled in this deployment. The existing workspace SDK is a development reference, not a currently available paid customer integration.

The future architecture separates collection, evidence normalization, analysis, report delivery, and payment authorization. Collection failures must remain visible through every layer. The payment service must decide access independently of the security verdict: paying for a scan must never buy a favorable result.

8. QUS service-payment token

Attribute	Project specification
Token ticker	**QUS**
Planned total supply	**1,000,000,000 QUS (one billion)**
Intended utility	Payment for selected Quantum Shield services when paid access launches
Current status	Planned; token payments are not enabled
Network and contract	Not finalized or published in this release

A future customer or agent will be able to choose QUS where a service explicitly lists it as an accepted payment asset. The checkout or API quote must identify the service, exact amount, network, asset contract, recipient, and expiry. Holding QUS does not currently unlock a product, and no payment should be sent to an address claimed to represent QUS before the official deployment details are published and verified.

The supply above is the project's planned specification, not a claim that one billion tokens have already been minted or that a deployed contract enforces it. Network selection, contract implementation, security review, and payment compatibility remain release gates. This document grants no ownership, dividend, guaranteed return, or governance entitlement and makes no exchange-listing promise. It contains no tokenomics or allocation schedule.

9. x402 and agent micropayments

Quantum Shield plans to integrate x402 for usage-based services. The protocol uses HTTP 402 to communicate payment requirements and allows a compatible client to submit payment authorization for a requested resource. This is a payment mechanism; it does not establish the quality of the purchased result. [2]

The proposed flow is: an agent requests a paid report; the service quotes an exact price and supported payment details; the agent checks its allowed recipient, asset, network, per-request ceiling, and daily budget; the payment is verified and settled through a supported integration; and the service returns a result and receipt. The x402 v2 specification defines payment request, authorization, and response headers that the implementation will follow and test. [3]

The pricing objective is small, predictable charges. **US$0.01-equivalent for a selected lightweight lookup is an illustrative target, not an active price or a promise for every service.** AI, licensed intelligence, historical indexing, and simulation may have different costs. The user or agent must see the price before authorizing it. Network and facilitator fees, minimum charges, and any conversion costs must be disclosed rather than described as universally free.

QUS support is not automatic merely because x402 is integrated. It depends on the chosen chain, token contract, transfer authorization method, and facilitator support. The current x402 documentation distinguishes token transfer mechanisms, including EIP-3009 and Permit2-based flows on EVM networks. Any QUS integration must validate its actual compatibility; a compatible stablecoin may be an additional quoted payment option if needed. [4]

XPay at x-pay.llc is the project's intended integration candidate from earlier planning, not a confirmed production partner. Its availability, supported networks and assets, API contract, custody model, settlement behavior, and operating terms must be verified before activation. No XPay connection, x402 settlement, or QUS checkout is represented as live in this release.

The payment implementation must handle the case where settlement succeeds but report delivery fails. A payment identifier and stored result should support recovery without duplicate charging; quote expiry and authorization nonces must prevent replay. These are engineering requirements for the planned integration, not capabilities the current free endpoints provide. Expired, invalid, unsupported, or underfunded payments must fail explicitly. Agent access will require its own production API contract rather than treating today's browser-only POST routes as a finished agent service.

10. Service model and sustainable revenue

The current public beta is free within capacity limits. Basic individual checks are intended to remain an entry point. Future paid services should charge for additional work and operational value: deeper website investigation, transaction-request analysis, broader history, bulk queries, scheduled monitoring, exportable company reports, licensed data, API usage, and support.

Companies may prefer recurring plans with clear quotas and support terms. Agents may prefer per-result micropayments. Human users may choose an individual paid report without a recurring subscription. QUS is intended as a payment option for eligible services, rather than a prerequisite for trying the present free tools. Prices and service commitments will be published before billing is enabled.

Commercial validation should measure repeated use, useful findings, review time saved, false-positive burden, delivery reliability, and cost per result. The business must account for inference, data licensing, RPC/indexing, storage, support, and settlement costs. This paper does not forecast revenue, token value, or customer returns.

11. Security, privacy, and responsible reporting

The public checks do not require seed phrases, private keys, asset transfers, or transaction signatures. Connecting a browser wallet for read-only account selection is different from granting token spending authority. Future payments will be a separate, explicit authorization flow and must never be disguised as a free security check.

The domain lookup sends a hostname to a reputation provider. Deep scanning sends the requested URL to the target website and selected returned source text to Workers AI. Wallet tools disclose their RPC or explorer providers. Image-format inspection reads the local file header without uploading or previewing the picture. Users should never submit secret-bearing invitation, password-reset, or private-access URLs for public scanning.

Private workspace records, labels, and relationships require restricted access even when the underlying addresses are public. Before company onboarding expands, the service needs a published retention/deletion policy, tested backup and recovery, incident contacts, provider review, and independent application security assessment. Existing tests and input controls are not substitutes for an audit.

Reports can contain false positives and false negatives. A correction process should preserve the original observation, record the correction and its reason, and show source freshness. The project will not claim verified detection accuracy until a representative, labeled evaluation and review process supports the claim.

12. Delivery roadmap and release gates

Stage	Deliverable	Gate before expansion
A. Public evidence beta	Free tools, source review, AI assistance, coverage disclosures	Provider failures remain explicit; permissions and evidence behavior pass tests
B. Detection validation	Labeled test corpus, adversarial source cases, correction workflow, richer collection	Measured false positives/negatives, independent review, and documented coverage
C. Wallet-action analysis	Isolated interactions, signature interpretation, spender analysis, transaction simulation	No real customer funds in testing; replayable evidence and evaluated failure behavior
D. Company and data services	Broader indexed history, verified labels, scheduling, onboarding, exports	Provider rights, tenant isolation, recovery tests, operational ownership
E. Paid access and QUS	Reviewed token deployment and supported service-payment flows	Published contract/network details, security review, tested quote and receipt lifecycle
F. x402 agent access	Bounded per-call payments and machine-readable results	Supported facilitator/assets, replay protection, duplicate-charge recovery, spending controls
G. Readiness research	Cryptographic inventory and test-environment migration work	Qualified cryptographic review before any protection or migration claim

These stages are dependency-based, not calendar promises. Token and payment planning can proceed in parallel with product validation, but paid protection claims must not precede demonstrated capability. Broad chain support is released network by network after adapter and data-quality checks.

13. Research basis and project boundaries

QRL's original white paper provides an example of grounding a post-quantum system in explicit cryptographic mechanisms and assumptions. Its historical network design is not Quantum Shield's architecture. Forta's historical litepaper illustrates the importance of runtime observation and distinct detection components; its authors also distinguish that paper from current implementation details. These references inform document structure and engineering questions, not claims that Quantum Shield operates their infrastructure or has their capabilities. [5][6]

This white paper describes Quantum Shield's current software and intended direction. It does not announce partnerships with referenced projects, a new blockchain, a completed security audit, an active token sale, or guaranteed protection from fraud. The live interface and published release notes should take precedence when a future version changes coverage. Material changes to scope, token deployment, or payment availability will require a new document version.

14. References and version record

[1] NIST: first finalized post-quantum standards. Cryptographic context; not a certification of Quantum Shield.

[2] x402: introduction. Payment-protocol overview.

[3] x402 Foundation: version 2 specification. Technical reference for the planned payment integration.

[4] x402: network and token support. Compatibility depends on the implemented network, transfer method, and facilitator.

[5] QRL: original white paper repository. October 2016 revised paper; historical design reference, not a current Quantum Shield capability.

[6] Forta: historical litepaper. Updated December 2021, published July 2022; historical design reference.

[7] Cloudflare Workers AI: GLM-4.7-Flash. Current beta model adapter reference; availability can change.

Version 1.1 adds the Team Treasury workspace, decentralized custody requirements and inactive fee policy to the public-beta paper. Version 1.0 superseded the private-pilot paper. Updated 4 October 2026 to document public tools, source-code review, actual deployment boundaries, the planned QUS supply and service utility, and future x402 payments. External sources were reviewed for this release. No tokenomics section is included.