

P4 Technology Build and Pilot Plan

A requested AI analysis of how the P4 / Wardtrac concepts should be built, staged, staffed, and technically validated.

Prepared for: Joel Ward

Purpose: To define a practical technology backbone and pilot build plan for presentation to a potential startup funder.

Date: September 2026

Executive Recommendation

P4 should be built as an evidence-grade asset record platform, not as a blockchain company. The product's credibility will come from disciplined identity controls, immutable document storage, cryptographic file hashes, professional attestations, audit logs, and exportable evidence packets. Blockchain may later be useful as an external timestamping or proof-anchoring layer, but it should not drive the pilot.

The pilot should prove that affluent households and professionals will use and pay for a trusted system that organizes valuable personal property records for estate planning, insurance, appraisal, succession, transfer, and loss documentation.

The Core Product to Build

The first P4 software product should create an Asset Evidence Passport for high-value personal property. That passport should not merely list items. It should preserve the evidence around them: photos, descriptions, receipts, appraisals, serial numbers, ownership history, insurance records, storage location, professional review, access history, and transfer instructions.

- A guided intake workflow for valuable personal property.
- Secure storage of original photos, receipts, appraisals, insurance documents, and provenance files.
- A timeline showing when each asset record was created, updated, reviewed, shared, transferred, or exported.
- Professional attestation by appraisers, estate attorneys, insurance professionals, fiduciaries, or approved inventory specialists.
- Exportable evidence packets in PDF and structured data form for estate files, insurance claims, appraisals, and family transfer.
- Role-based sharing so owners can invite the right professional without giving everyone the keys to the whole vault.

Recommended Technology Backbone

Layer	Pilot Recommendation	Reason
User experience	Responsive web app / progressive web app	Fastest path to desktop, tablet, and phone use without building separate native apps.
Front end	React / Next.js with TypeScript	Modern, maintainable, strong hiring market, good for secure workflows and dashboards.
Back end	TypeScript API, preferably NestJS, or Python FastAPI	A compact team can move quickly while preserving disciplined architecture.
Database	Managed PostgreSQL	Reliable relational model for assets, users, permissions, events, attestations, and workflows.
File storage	AWS S3 with versioning and Object Lock	Supports immutable, WORM-style preservation of uploaded files and helps prevent deletion or overwrite.
Identity	Auth0, AWS Cognito, Clerk, or similar	MFA, role-based access, password recovery, and audit-friendly identity management.
Evidence layer	Hashes, append-only event log, timestamps, signatures, evidence exports	Creates the proof structure that makes P4 more than an inventory app.
AI assistance	OCR, receipt parsing, serial-number capture, image quality checks	Reduces friction, but AI output must remain draft metadata until confirmed by a human.

AWS states that S3 Object Lock uses a write-once-read-many model and can help prevent objects from being deleted or overwritten for a fixed time or indefinitely. That is directly relevant to P4 because original evidence files should not silently change after upload.[1]

How the Evidence System Should Work

1. The owner or professional creates an asset record.
2. Photos, receipts, appraisals, certificates, insurance schedules, and related documents are uploaded.
3. The system stores original files in immutable storage where practical, with versioning enabled.

4. Each file receives a cryptographic hash, such as SHA-256, so later copies can be compared against the original digital fingerprint.
5. Every meaningful action is written to an append-only event log: creation, upload, edit, review, attestation, sharing, export, and transfer.
6. A professional reviewer can attest to exactly what was reviewed, when it was reviewed, and the scope of the attestation.
7. The system generates an Asset Evidence Passport containing the asset summary, evidence list, review history, file hashes, attestations, and verification instructions.

Blockchain Position

Blockchain should not be the pilot backbone. A blockchain can prove that a digital fingerprint existed at a certain time. It cannot prove the Rolex, painting, handbag, coin collection, jewelry, wine, antique, or aircraft part was genuine when photographed. The actual truth comes from source documents, identity, custody, expert review, and professional attestation.

The right later use is narrow: P4 could periodically create a batch hash, or Merkle root, from many asset evidence records and anchor that hash to a public blockchain or trusted timestamp service. Only the hash should be anchored. Private names, addresses, photos, values, estate details, insurance details, and ownership data should never be placed directly on-chain.

A more important future standard may be W3C Verifiable Credentials. W3C describes verifiable credentials as a way to express claims made by an issuer and secure them from tampering in an issuer-holder-verifier ecosystem.[2] That maps well to P4 if appraisers, attorneys, insurers, or fiduciaries eventually issue portable attestations that other parties can verify.

Build Stages

Stage	Duration	What Gets Built	Success Test
0. Founder validation	3-6 weeks	Interviews, sample evidence packet, professional feedback, pricing hypotheses	Professionals and households confirm a painful enough problem and willingness to pilot.
1. Concierge pilot	4-8 weeks	Manual or semi-manual Asset Evidence Passports using secure storage and structured templates	5-10 households or collections produce real packets reviewed by professionals.
2. Software pilot	12-16 weeks	Web app, asset records, uploads, permissions, hashes, event log, attestations, exports	75-150 asset records, multiple professional users, at least two paid or

			committed pilots.
3. Partner workflow	3-6 months	Professional dashboards, firm accounts, templates, reporting, improved verification	Appraiser, attorney, fiduciary, or insurance workflows become repeatable.
4. Scaled platform	6-18 months	APIs, integrations, portable credentials, optional blockchain anchoring, mass-market version	Evidence records can move across firms, households, and transfer events.

Pilot Staffing

For a real pilot, P4 needs a small, senior team. The pilot is not a marketing website. It will handle sensitive property, estate, insurance, family, and valuation information. That means the first build has to be modest in feature count but serious in security and data design.

Role	Level	Responsibility
Lead full-stack / architect	Senior, roughly 10+ years or equivalent	Responsible for architecture, security model, database, permissions, file integrity, cloud deployment, and code review.
Product full-stack engineer	Strong mid-to-senior, roughly 5+ years	Builds owner workflows, mobile-responsive intake, uploads, dashboards, evidence packet generation, and tests.
UX / product designer	Fractional	Designs the capture flow so wealthy households and professionals can use it without needing a training manual the size of a toaster oven.
Security / cloud reviewer	Fractional, 40-80 hours	Reviews identity, access control, logging, storage, encryption, backup, and operational risk before live pilot use.
QA / test support	Fractional near pilot start	Tests real workflows, permissions, exports, edge cases, and regression risk.

Minimum credible team: two strong programmers plus fractional design, security, and QA support for 12-16 weeks. Better team: three programmers if the goal is a more polished professional-facing pilot with cleaner dashboards, more robust permissions, and faster iteration.

Programmer Level Required

The lead technical hire cannot be a junior programmer, generic website developer, or blockchain enthusiast looking for a use case. P4 needs a senior product-minded architect who has built secure multi-user SaaS systems, understands cloud deployment, and respects audit trails, permissions, and data integrity.

- Must have prior experience with authentication, MFA, role-based permissions, and secure file handling.
- Should understand relational database design, event logs, backups, monitoring, and operational security.
- Should be comfortable building a narrow but production-grade pilot rather than an overbuilt platform.
- Does not need to be a blockchain specialist during the pilot.

Estimated Build Cost

These are planning ranges, not bids. Actual cost depends heavily on whether the team is U.S.-based, blended, offshore, agency-based, or founder-led with a technical cofounder.

Build Option	Likely Cost Range	Comment
Clickable prototype only	\$25,000-\$60,000	Good for demos and interviews, but not sufficient for live sensitive records.
Concierge pilot with light tooling	\$50,000-\$100,000	Useful if P4 first proves demand through a guided service and semi-manual evidence packets.
Two-programmer software pilot	\$140,000-\$300,000	Most realistic path for a credible 12-16 week pilot with security review.
Three-programmer professional pilot	\$250,000-\$450,000	Better if partner dashboards, attestation workflows, and polished demos matter from day one.

Data and Security Principles

- Use least-privilege permissions: each invited party should see only what they need.

- Require MFA for professional and administrator accounts.
- Encrypt files and database records at rest and in transit.
- Keep audit logs protected from ordinary user alteration.
- Separate private asset contents from public verification methods.
- Design export packets so they remain useful outside P4.
- Avoid placing private ownership data, valuations, or family transfer information on public ledgers.

NIST describes identity and access management as ensuring the right people and things have the right access to the right resources at the right time.[3] That is exactly the problem P4 must solve as records move among owners, attorneys, appraisers, insurers, fiduciaries, beneficiaries, and buyers.

What Not to Build First

The first version should avoid native mobile apps, token economics, NFTs, smart contracts, consumer crypto wallets, public ownership registries, broad marketplace features, broad appraisals automation, and integrations with every possible partner system. Those may sound exciting, but in a pilot they would distract from the central proof: will people pay for trustworthy asset evidence records?

Recommended Immediate Next Steps

8. Finalize a one-page P4 pilot definition: target users, asset categories, professional partners, and success metrics.
9. Create a manual Asset Evidence Passport template that mirrors what the software will eventually produce.
10. Interview 20-25 professionals and high-net-worth household decision makers.
11. Secure three design partners, ideally one estate attorney or fiduciary, one appraiser, and one insurance-facing professional.
12. Run 5-10 concierge evidence packets before funding the full software pilot.
13. Hire or contract a senior product-minded technical architect to write the technical specification and supervise the pilot build.

Bottom Line

P4 should be built in stages. The first stage proves the business problem. The second proves the evidence workflow. The third automates that workflow in a secure pilot. Blockchain, if used at all, belongs after those steps as a narrow verification enhancement.

The strategic technology thesis is simple: P4 is not a crypto project. It is a trust, evidence, and transfer infrastructure project for valuable personal property. That is a stronger position, a more fundable position, and a much more useful product.

Sources

- [1] Amazon Web Services, "Locking objects with Object Lock," Amazon S3 User Guide, accessed September 2026. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>
- [2] World Wide Web Consortium, "Verifiable Credentials Data Model v2.0," W3C Recommendation, May 15, 2025. <https://www.w3.org/TR/vc-data-model-2.0/>
- [3] National Institute of Standards and Technology, "Identity and Access Management," accessed September 2026. <https://www.nist.gov/identity-and-access-management>