

P4

ASSET EVIDENCE PASSPORT

BUSINESS PLAN

Produce. Preserve. Protect. Provenance.

The company in one sentence. P4 is a private, cross-brand evidence platform that helps households and trusted professionals create, preserve, verify, share, and transfer the records surrounding valuable movable property.

COMPANY STAGE Validation planning

DATE September 11, 2026

STATUS Confidential discussion draft - planning document, not an offering memorandum

Contents

Executive Summary

1. Identity, Mission, and the Four P's
2. The Problem
3. The P4 Solution
4. Market Opportunity
5. Customers and Use Cases
6. Competitive Position
7. Business Model and Pricing
8. Go-to-Market Strategy
9. Product and Technology Plan
10. Development Roadmap and Funding Gates
11. Operations, Team, and Governance
12. Legal, Security, and Intellectual Property
13. Financial Plan
14. Risks and Mitigation
15. Milestones and Investment Proposal

Appendix A. MVP Requirements

Appendix B. Base-Case Financial Assumptions

Appendix C. Plain-English Glossary

Addendum. P4 Stewardship Foundation Development Plan

Addendum. P4 Competitor and Partnership Landscape

Sources and Notes

Planning discipline. This plan integrates the prior strategic recommendation, market-acceptance analysis, and technology build plan. The financial model is a management hypothesis to be tested through stage gates; it is not a valuation or promise of results.

Executive Summary

P4 should proceed as a focused asset-evidence company, not as the universal registry, lending platform, public-safety system, or blockchain venture imagined across the broader historical portfolio. Its first product should be the P4 Asset Evidence Passport: a secure, private, cross-brand record for high-value movable personal property such as watches, jewelry, handbags, fine art, antiques, and selected collectibles.

The commercial wedge is practical rather than futuristic. Valuable objects are routinely separated from receipts, appraisals, certificates, service records, insurance schedules, provenance correspondence, ownership instructions, and family knowledge. Those gaps create friction and loss in insurance, estate planning, appraisal, transfer, consignment, sale, and post-loss claims. They also give counterfeiters room to pair fake articles with copied, altered, or ambiguous documentation. P4 organizes the evidence, identifies who supplied each claim, preserves changes over time, and produces selective reports that can be used by households and professionals.

P4 does not authenticate an object merely because someone records it. Its anti-counterfeit value is to preserve tamper-evident proof that a particular owner, expert, brand, manufacturer, laboratory, or authorized dealer made a particular claim at a particular time. When a trusted manufacturer or authorized issuer creates an origin credential and securely binds it to the physical article, later buyers and transferees can verify the issuer, inspect the evidence chain, and detect gaps, alterations, revocations, duplicate identities, or suspicious transfers more reliably than with loose paper alone.

The recommended distribution model is B2B2C. Estate-planning attorneys, fiduciaries, appraisers, insurance professionals, dealers, service specialists, auction houses, and collection managers become trusted introduction and workflow channels. Households retain the long-term dossier. P4 earns subscription revenue from households and professional firms, service revenue from concierge onboarding, transaction or attestation fees, and later enterprise/API revenue.

The technology uses established components where possible. PostgreSQL is a widely used database that stores structured records and the relationships among them. Encrypted object storage protects uploaded photographs and documents. A cryptographic hash is a digital fingerprint that reveals whether a file has changed. An append-only event history adds later actions without silently erasing earlier ones. A digital attestation is a signed, limited statement identifying who made a claim, what was reviewed, and when. Exportable evidence packets let an owner preserve or share useful records outside P4. Blockchain is optional later as a narrow way to prove that a fingerprint or batch of fingerprints existed by a certain time. It is not the product and should not be the pilot backbone.

P4's highest-value proprietary technology should be the **P4 Evidence Integrity Engine**. It would evaluate the reliability of each claim by combining issuer identity and authority, supporting evidence, physical-item binding, credential status, custody and service history, disputes, corrections, duplicate identifiers, and contradictory events. The customer sees an Asset Evidence Passport. The proprietary engine determines what the passport can responsibly prove, what remains uncertain, and what requires further inspection.

The market has developed many of the pieces P4 anticipated. Brand consortia and digital-product-passport platforms can issue origin credentials. Authentication and grading companies can provide specialized opinions. Registries can report theft or loss. Marketplaces can document a transaction. Inventory and estate platforms can organize household records. What the review did not identify is one cohesive, owner-controlled system that connects those sources across brands and asset categories; preserves authenticity assessments, ownership evidence, title and custody provenance, lifecycle events, disputes, and transfers; evaluates how much confidence each claim deserves; and keeps the resulting record portable through institutional change. **P4 can therefore use or integrate proven components while owning the connective and evaluative layer that makes the evidence useful as a whole.**

The principal strategic risk is not one named competitor. It is that a better-funded brand consortium, marketplace, authentication specialist, software vendor, or new horizontal entrant recognizes the opportunity and moves faster. P4 should respond with a layered defense: file narrowly focused patent applications before public disclosure; protect non-public methods and data as trade secrets; own all code and inventions contractually; conduct controlled pilots; accumulate longitudinal evidence and category knowledge; embed with trusted professional channels; interoperate with credible issuers; and build a reputation for precise claims, privacy, and dependable execution.

P4 should begin as a for-profit operating company because the early work requires concentrated product decisions, private capital, rapid testing, and commercial discipline. At the same time, the records are intended to remain useful beyond the life of any one company. The initial architecture and contracts should therefore include data portability, documented formats, redundant backups, recovery procedures, source-code and documentation escrow, and a plan for a later independent stewardship foundation. The foundation would protect continuity assets and emergency rights; it would not manage ordinary product development or take the operating company's commercial intellectual property without agreed triggers. The attached addendum describes how that structure could develop as outside reliance grows.

Decision	Recommendation
Launch scope	Luxury and collectible movable property across estate, insurance, appraisal, loss, and transfer workflows.
First market	One regional concierge pilot with 5-10 households, 75-150 assets, and 3-5 trusted professional partners.
First funding gate	\$25,000-\$50,000 for a fixed 90-day validation and concierge prototype.
Minimum proof required before building the MVP	Advance only after completed records, real professional use, paid commitments, and repeat household behavior.

Decision	Recommendation
Technology	Secure SaaS evidence platform; no public ownership ledger, crypto wallet, token, or native mobile app in the MVP.
Brand	Use P4 as the working identity, subject to formal trademark, domain, and naming clearance.

1. Identity, Mission, and the Four P's

The original name

The 2007 P4 archive identifies the four P's as Produce, Preserve, Protect, and Provenance. They still apply to the revised project - arguably more clearly than they applied to the broader original ecosystem.

The historical importance of the archive is its early recognition that valuable property needs more than an inventory entry or ownership assertion. The records anticipated a continuing evidence system that connects an article, the people and organizations making claims about it, the documents supporting those claims, and later events affecting ownership or reliability. The preliminary search found products and patents covering portions of that concept, but it did not identify a commercial platform delivering the entire P4 combination described in this plan. That conclusion remains subject to counsel's formal patent and market review.

P	Modern meaning for the company	Visible customer result
Produce	Create a structured, source-labeled asset record or issuer credential from photographs, documents, identifiers, user statements, and professional input.	A usable passport whose claims can be traced to their maker.
Preserve	Retain originals, file fingerprints, signatures, attestations, and a history in which corrections supersede rather than erase.	Copied or altered records are easier to detect; genuine history remains defensible.
Protect	Reduce piracy, counterfeit, insurance, estate, transfer, loss, and documentation risk through controlled access and verification.	A buyer, heir, or other recipient can receive only the evidence needed for that purpose, while unrelated assets, values, locations, and family information remain private.
Provenance	Show where each claim came from and how identity, custody, condition, service, appraisal, and transfer evolved.	A source-attributed chain that reduces gaps and makes unexplained gaps and substitutions visible.

Mission

Make valuable personal property easier to document, protect, understand, and transfer by preserving the evidence around each object and making that evidence useful in real professional workflows.

Vision

Become the owner-controlled evidence layer for valuable movable property across categories, institutions, and generations.

Positioning statement

For households and professionals responsible for valuable personal property, P4 creates a private Asset Evidence Passport that shows what is claimed, what supports each claim, who supplied or reviewed it, what changed over time, and what can safely be shared. **Unlike a generic inventory app or single-brand certificate, P4 preserves cross-brand evidence and professional workflows throughout the asset life cycle.**

Name recommendation

Keep P4 as the internal and investor-facing placeholder because the history is authentic and the four-part meaning remains strong. Do not commit substantial branding expense until counsel completes trademark clearance, relevant domains are investigated, and pilot users confirm that the name is memorable and credible. “P4 Asset Evidence Passport” should be treated as a descriptive working product name, not yet as a cleared mark.

2. The Problem

High-value movable property has a documentation problem disguised as an organization problem. The evidence exists, but it is fragmented across paper files, email, phones, appraiser PDFs, insurance portals, brand accounts, service centers, marketplace certificates, family memory, and storage locations.

- **Identity is uncertain:** serials, reference numbers, hallmarks, dimensions, condition photographs, and category fields are incomplete or inconsistent.
- **Claims are flattened:** a user statement, a receipt, a professional opinion, and a brand-issued certificate are often displayed as if they carry equal authority.
- **History is overwritten:** updated appraisals or corrected descriptions replace earlier information without preserving what changed and why.
- **Rights are collapsed:** owner, beneficial owner, custodian, trustee, agent, lienholder, creator, intellectual-property holder, beneficiary, and verifier may be different people.
- **Privacy controls are crude:** sharing an entire folder exposes more property, value, location, or family information than the recipient needs.
- **Records fail at the moment of use:** executors, heirs, insurers, appraisers, buyers, and law enforcement receive incomplete or stale packages.

The actual job to be done. P4 is not hired merely to store photographs. It is hired to create better evidence before an insurance review, appraisal, loss, estate event, gift, inheritance, consignment, or sale. Imagine evidence chain of custody protocols in criminal cases and apply the analogy to P4.

Counterfeits, product piracy, and unreliable paperwork

Counterfeit and pirated goods are a material global problem: the OECD and EUIPO estimated that counterfeit goods represented approximately \$467 billion, or 2.3% of global imports, in 2021. [15] For a buyer, insurer, heir, or reseller, the practical problem is not only the fake object. Certificates, receipts, serial labels, QR codes, photographs, service histories, and ownership stories may also be copied, altered, separated from the genuine item, or attached to a substitute.

Current records often prove too little about who made a claim, when it was made, whether the record changed, and whether the presented article is the same physical item. A plain QR code or uploaded certificate can be duplicated. A database entry can preserve a false assertion perfectly. The missing capability is a trustworthy chain linking an identified issuer, a signed and status-checkable claim, a sufficiently distinctive physical article, and subsequent custody or transfer events.

3. The P4 Solution

Core product: the Asset Evidence Passport

Each passport is a durable digital dossier for one object or collection. It contains a current summary and an append-only history, while keeping every claim tied to its source and evidence strength.

1. Capture and identify the object through guided photographs, serials, reference numbers, hallmarks, measurements, certificates, invoices, or QR and NFC identifiers. A QR code is a printed square code read by a camera. NFC, or near-field communication, is a short-range chip that a compatible phone or reader can scan.
2. Upload and preserve original evidence such as receipts, appraisals, grading reports, insurance schedules, service records, bills of sale, estate documents, and provenance correspondence.
3. Classify each claim by source and evidence grade. AI may suggest fields, but a human confirms them.
4. Invite a qualified professional to attest only to facts or opinions within that professional's competence.
5. Append events for appraisal, service, storage, custody, insurance, loss, dispute, gift, inheritance, sale, and transfer.
6. Generate selective, time-limited views and signed export packets for a specific purpose.
7. Transfer the dossier with controlled acceptance and without automatically disclosing private documents.

Evidence grades

Grade	Meaning	Illustrative support
A - Self-recorded	The owner created an identified record; no independent support yet.	Owner photographs, description, approximate acquisition date.
B - Document-supported	A claim is supported by a contemporaneous document.	Receipt, invoice, warranty card, service record, insurance schedule.
C - Professional-attested	A qualified third party signed a limited observation or opinion.	Credentialed appraisal, dealer inspection, watchmaker statement.
D - Issuer-confirmed	A brand, laboratory, creator, or authorized network issued or confirmed the record.	GIA report, brand passport, authorized-retailer certificate.
E - Authoritative link	The claim links to an appropriate external registry, custody, or legal record.	Lost/stolen check, court or custody record, registry receipt.

Grades describe the strength of support for a particular claim. They do not guarantee authenticity, market value, ownership, or legal title. Different claims within the same passport may carry different grades.

How P4 reduces counterfeit and product-piracy risk

1. An owner can create a time-stamped, tamper-evident record of possession and supporting documents. This proves what was recorded and when; it does not by itself prove authenticity.
2. A manufacturer, brand, laboratory, creator, authorized dealer, or qualified expert can issue a digitally signed credential limited to the facts or opinion it is competent to assert.
3. The credential is bound to the article using category-specific identifiers and images and, where justified, a tamper-evident label, NFC secure element, or other challenge-response device. A QR code alone is treated as a pointer, not proof.
4. P4 preserves the signed credential, its status, supporting evidence, cryptographic fingerprints, and an append-only history of service, inspection, custody, disputes, and transfer.
5. At purchase or transfer, the recipient verifies the issuer and signature, checks revocation or dispute status, compares the physical item with its binding evidence, and reviews gaps, duplicates, or inconsistent events.
6. Suspicious credentials or cloned tags can be flagged without deleting the earlier record, improving detection, investigation, and marketplace response.

The promise P4 can responsibly make. P4 can prove that an identified issuer made a particular claim and that the preserved record has not been silently altered. It cannot prove that the underlying claim is true unless the issuer and the connection between the digital record and the physical article are trustworthy. The World Wide Web Consortium, usually called W3C, develops open technical standards for the web.

Its Verifiable Credentials standard makes the same distinction: confirming a credential and its issuer does not, by itself, establish that every claim in the credential is true. [10]

Initial product family

Offer	Customer	Purpose
P4 Household	Affluent and collector households	Private vault, guided capture, life-cycle history, reports, sharing, and family continuity.
P4 Pro	Attorneys, fiduciaries, appraisers, insurers, dealers, and collection professionals	Client workspaces, evidence requests, narrow attestations, reports, collaboration, and renewal triggers.
P4 Concierge	Households or professional clients needing help	Photograph, organize, digitize, and structure initial records without making unsupported claims.
P4 Protect	Households and insurance-facing partners	Schedules, appraisal reminders, coverage-review inputs, and claim-ready exports.
P4 Transfer	Owners, fiduciaries, heirs, dealers, auction houses, and buyers	Controlled gift, inheritance, consignment, custody, and sale handoff.
P4 Origin / Verify	Manufacturers, brands, authorized dealers, laboratories, and resale partners	Signed origin and later-event credentials, physical binding, status checks, and buyer verification.
P4 Embedded/API	Enterprise partners after proof	White-label workflows, credential ingestion, exports, and integration with systems customers already trust.

4. Market Opportunity

No authoritative database counts households that would buy an evidence passport. A credible plan therefore uses several independent signals and refuses to turn them into a cartoonishly precise total addressable market.

Signal	Current evidence	Meaning for P4
Affluent U.S. base	UBS estimated more than 23.6 million U.S. dollar millionaires at year-end 2025, nearly 9% of U.S. adults. [1]	A large premium population exists before counting valuable-asset owners below the millionaire threshold.

Signal	Current evidence	Meaning for P4
Aging households	More than one in four U.S. householders were age 65 or older in 2025. [3]	Estate, incapacity, downsizing, executor, heir, and transfer events are structural demand triggers.
Younger collectors	A 2026 Chubb study of 1,000 affluent younger collectors found 78% considered future value important and fewer than half insured their collections. [4]	The need includes active digital collectors, not only older estate-planning clients.
Luxury asset flow	Personal luxury-goods spending was approximately EUR 358 billion in 2025; Bain projected recovery in 2026. [5]	Valuable objects move through service, insurance, resale, and transfer workflows.
Art ecosystem	Art Basel and UBS estimated global art-market sales at \$59.6 billion in 2025. [6]	One P4 category alone supports a substantial professional ecosystem.
Generational transfer	Cerulli projects \$124 trillion of U.S. wealth transfers through 2048, with more than half originating from high-net-worth and ultra-high-net-worth households. [7]	Movable-property evidence can become part of a multidecade succession workflow.
Collection succession	In Chubb's 2025 affluent survey, 68% planned to pass collections to heirs and 36% worried about legacy continuation. [8]	Family continuity creates urgency and a trusted-professional entry point.
Counterfeit exposure	OECD and EUIPO estimated \$467 billion in global counterfeit trade in 2021, equal to 2.3% of global imports. [15]	Trusted origin and life-cycle credentials create a second enterprise market alongside household evidence.

Initial serviceable market

The first serviceable market is U.S. households with at least one movable item above approximately \$5,000 or an aggregate valuable-property collection above approximately \$25,000, together with the professional firms serving those households in estate, insurance, appraisal, collection, loss, and transfer workflows. These dollar thresholds are pilot hypotheses, not published market facts.

Market entry categories

- Watches: identifiable references and serials, active service and resale markets, theft exposure, and brand certificates.
- Jewelry and gems: reports, appraisals, hallmarks, insurance scheduling, gifting, and inheritance.
- Designer bags and leather goods: authentication, condition, provenance, resale, and theft risk.
- Fine art and antiques: provenance, condition, title claims, appraisals, insurance, custody, and estate administration.

- Selected collectibles: coins, memorabilia, wine, or other categories only when a pilot partner supplies expertise and a repeatable evidence template.

Vehicles, boats, real estate, regulated financial assets, and broad household inventory should remain outside the first commercial release. They either have separate title systems or would dilute the high-value evidence workflow.

Comparable adoption signals — validation, not proof

The original plan identified adjacent companies but did not claim that their commercial results validated P4. The evidence below is stronger: it shows that customers, brands, collectors, and strategic investors already support important parts of the proposed behavior. None of these examples proves P4 pricing, conversion, retention, or profitability; the paid pilot must do that.

Comparable	Reported evidence	What it validates / limitation
Aura Blockchain Consortium	More than 70 million products registered across more than 50 brands as reported in 2025. [16]	Manufacturer demand for durable digital product records at scale. It is a luxury-brand consortium, not an owner-controlled cross-brand service.
Chrono24	More than 1.6 million watches sold since 2003, over 500,000 listings, and users in 150 countries. [17]	Trust and evidence matter in high-value secondary transfers. Marketplace economics differ from P4 subscriptions.
PSA	More than 80 million collectibles authenticated and graded. [18]	Collectors pay for credible, durable third-party evidence. PSA is an expert issuer in selected categories; P4 initially is not.
Trust & Will	Raised more than \$25 million in a 2025 Series C led by and including major strategic financial and insurance investors. [19]	Digital estate workflows can attract customers, channel partners, and strategic capital. It is a document platform, not an asset-provenance system.
Entrupy	Its authentication system was reported to use a reference database exceeding 20 million images and to support TikTok Shop authentication. [20]	Proprietary data and workflow integration can become defensible assets. Entrupy makes authentication judgments that P4 will not initially make.

5. Customers and Use Cases

Customer	Pain	First paid use
Collector or affluent household	Fragmented records; spouse or heirs cannot locate, understand, or use evidence.	Create and maintain an evidence-ready inventory with selective estate and insurance outputs.
Estate-planning attorney / fiduciary	Asset schedules are incomplete; ownership, custody, and beneficiary context are unclear.	Structured client intake, estate schedule, fiduciary access, and incapacity/death handoff.
Appraiser / category specialist	Repeated document chasing; unclear source history; version control is weak.	Client intake, evidence requests, appraisal history, and narrowly scoped attestations.
Insurance broker / valuable-articles specialist	Poor schedules, missing supporting documents, stale values, and weak claim readiness.	Coverage-review packet, appraisal reminders, and loss documentation.
Dealer / auction / service provider	Condition, custody, service, authentication, and transfer history break across transactions.	Inspection or service event, consignment packet, and controlled dossier transfer.
Manufacturer / brand / authorized issuer	Paper certificates, serials, and basic QR codes can be copied or detached from the genuine article.	Issue signed origin credentials, manage status, bind them to items, and support buyer verification.
Trust company / wealth manager	Movable property sits outside core financial reporting but creates family and fiduciary risk.	Embedded client benefit and professional oversight workflow after P4 proves repeatable use.

Pilot customer profile

Recruit 5-10 households with approximately 10-40 qualifying items each, introduced by 3-5 professionals in one manageable region. The pilot should document 75-150 assets across several categories and generate actual estate, insurance, appraisal, or transfer outputs. A successful pilot requires completed records, professional reliance, payment, and repeat behavior - not compliments about the demo.

6. Competitive Position

The market is validated but fragmented. During roughly the last decade, companies have commercialized important portions of the broader P4 concept, including digital product passports, authentication, grading, provenance certificates, theft registries, marketplace inspection, household

inventory, and estate workflows. That development reduces the amount P4 must invent, but the review did not identify one public offering that combines P4’s cross-brand, owner-controlled evidence history, claim-level source authority, authenticity assessment, ownership and custody provenance, professional workflows, selective disclosure, transfer, and institutional continuity.

P4 should not try to replace brands, laboratories, authenticators, crime databases, marketplaces, appraisers, or general inventory platforms. Most are better viewed as evidence issuers, verification sources, infrastructure providers, distribution channels, or integration partners. **P4’s role is to connect their strong but partial records, preserve who said what and on what evidence, expose gaps or contradictions, and produce a portable history that remains useful beyond one transaction or provider.** The attached competitor and partnership addendum explains the overlap, P4’s present differentiation, and the circumstances in which an adjacent provider could become a direct competitor.

Category / examples	What they do	P4 response
Brand passport platforms: Aura, Arianee	Digital identities, lifecycle events, certificates, ownership experiences.	Treat as adjacent competitors and later interoperability targets; preserve their evidence.
Brand programs: Rolex CPO, Breitling passport	Brand-issued authenticity, warranty, service, and transfer within participating networks.	Recognize issuer authority; never impersonate it.
Specialists: GIA, Entrupy, credentialed appraisers	Category-specific grading, authentication, inspection, or professional opinion.	Invite or ingest limited attestations and preserve scope.
Loss / due diligence: Enquirus, Art Loss Register	Lost/stolen records, title-claim checks, due diligence, and recovery support.	Link or integrate later; do not build a global crime database first.
Marketplaces: Chrono24, eBay	Transaction-time authentication and buyer confidence inside the marketplace.	Create a dossier that exists before and survives after one transaction.
Vaults / legacy tools: Artifcts, WAX, Verisart	Inventory, storytelling, insurance convenience, certificates, or document storage.	Differentiate through claim-level evidence, rights separation, professional workflow, and append-only history.

Comparable business models. CARFAX demonstrates how records from many independent sources become more useful when organized around one physical asset and presented as a comprehensible history. Plaid demonstrates how a connective platform can integrate specialized institutions without replacing their underlying services. P4 combines those two strategic patterns: an asset-centered evidence history supported by a partner-centered integration model. The comparison is functional, not literal; unlike vehicles, most P4 assets lack a standardized VIN, mandatory title system, or uniform reporting network. The attached competitor addendum explains the analogy and its limits.

Defensible advantage

- Evidence grammar: a trusted structure for claims, issuers, support, uncertainty, supersession, disputes, and resolution.
- Professional network: qualified participants willing to issue narrowly scoped attestations and introduce clients.
- Workflow utility: outputs used in estate, insurance, appraisal, service, loss, consignment, and transfer.
- Longitudinal history: the accumulated chain of evidence and activity becomes difficult to recreate elsewhere.
- Interoperability: P4 becomes more valuable by accepting specialist and brand evidence rather than forcing every fact into a proprietary silo.
- Privacy reputation: private by default, field-level sharing, and a commitment not to sell or advertise against asset data.
- Issuer and item-binding network: verified organizations, scoped signing authority, credential status, and category-specific physical checks that make copied paperwork and cloned identifiers easier to detect.

Competitive defense is a system

No single patent, NDA, technical feature, or first-mover claim will prevent a well-funded company from competing. P4 should build mutually reinforcing defenses before and during development.

Defense layer	Action before or during launch	Defensible asset
Patents	Conduct invention-harvest sessions and file strong provisional applications before public demonstrations or campaigns; pursue only technically specific claims.	Priority dates and options around genuinely novel mechanisms.
Trade secrets	Keep fraud rules, issuer-vetting methods, scoring thresholds, internal schemas, security controls, and non-public datasets access-controlled and documented.	Knowledge that competitors cannot lawfully copy unless independently derived or reverse engineered. [26][27]
Contracts and ownership	Use confidentiality, work-made-for-hire, invention-assignment, data-use, and tightly scoped design-partner agreements.	Clear company ownership of code, inventions, feedback rights, and confidential material.
Controlled pilots	Use closed access, minimized or synthetic data where possible, watermarked materials, role-based permissions, and need-to-know technical disclosure.	Real-world learning without publishing the implementation blueprint.
Data and history	Accumulate consented asset records, status changes, anomalies, issuer behavior, category templates, and outcome data.	A longitudinal corpus and operating knowledge that are expensive to recreate.

Defense layer	Action before or during launch	Defensible asset
Channels and workflow	Embed with estate, appraisal, insurance, dealer, service, and later manufacturer workflows; earn referrals and integrations.	Distribution and switching costs based on useful work, not contractual lock-in.
Standards and partnerships	Ingest credible credentials and identifiers; remain hardware- and issuer-neutral.	A broader evidence network that complements brands and specialists instead of forcing displacement.
Trust and execution	Make narrow claims, publish clear limitations, protect privacy, respond well to incidents, and release improvements monthly.	A reputation and learning speed that a large entrant cannot buy instantly.

How P4 should approach likely entrants

Potential competitor	Strategic response
Brand consortium or manufacturer platform	Offer ingestion, preservation, status checking, and cross-brand portability. Let the brand remain the authoritative issuer.
Authentication or grading specialist	Preserve its scoped attestation and route business to it; never imply P4 has the specialist's expertise.
Marketplace or auction platform	Position P4 as the portable dossier that exists before and survives after a transaction; integrate rather than duplicate escrow or sales.
Generic vault or inventory application	Differentiate on claim-level provenance, append-only history, professional workflows, transfer, and issuer status.
Well-funded horizontal entrant	Concentrate on one defensible workflow and region, secure partner distribution, compound proprietary history, and outlearn it through focused releases.
Tag or device vendor	Use adapters and category-specific binding policies so P4 is not dependent on one tag, chip, or vendor.

7. Business Model and Pricing

Recommended model: B2B2C

Professional firms create trust, urgency, and efficient distribution. Households remain the long-term holders of their dossiers. Pricing begins as a set of testable hypotheses and becomes policy only after the validation and concierge stages reveal effort, value, and willingness to pay.

Revenue stream	Initial pricing hypothesis	Economic role
P4 Household	\$199-\$399 per year, with an initial planning price near \$250.	Recurring owner relationship and long-term evidence history.
P4 Pro	\$250-\$750 per month for a small firm, with seats/workspaces or usage tiers.	Recurring B2B revenue, distribution, and professional workflow.
Concierge onboarding	\$500-\$1,500+ per household or collection, depending on scope and travel.	Removes setup friction, funds operations, and teaches the product model.
Attestation / transaction	Fixed or partner-set fee per appraisal, authentication, transfer, or evidence event.	Monetizes high-intent events without turning P4 into the expert for every category.
Enterprise / API	Annual contract priced after proven integration value; illustrative \$100,000-\$300,000+.	Embedded distribution and scale after security and workflow maturity.

Unit economics targets

Metric	Early target	Reason
Professional gross retention	At least 85% annually after the first renewal cohort.	Channel durability matters more than vanity sign-ups.
Household annual retention	At least 75% initially; higher for professionally introduced accounts.	The dossier must remain useful after initial setup.
Blended gross margin	65%-75% during concierge-heavy launch; 80%+ as software and partner delivery scale.	Human setup work is useful but must not permanently dominate cost.
Partner-led acquisition	More than 60% of paid households by the commercial pilot.	Direct consumer advertising is likely too expensive and poorly timed.
Guided capture time	Median under 15 minutes per asset by the end of validation.	The best evidence system in the world is useless if nobody finishes the record.
CAC payback	Under 12 months for professional accounts; under 18 months for households.	Preserves capital while retention and referrals mature.

8. Go-to-Market Strategy

Phase 1: founder-led regional validation

Begin in one region where the founding team can directly observe behavior, recruit trusted professionals, and help construct early evidence packets. The goal is not geographic domination; it is rapid learning with real property and real documents.

- Interview estate attorneys, fiduciaries, appraisers, jewelers/watchmakers, art advisers, estate liquidators, and valuable-articles insurance brokers.
- Recruit at least three design partners who will test actual client cases and define the reports they would use.
- Use a concierge process so the team sees every missing field, privacy objection, awkward handoff, and liability concern before automating it.
- Charge for at least part of the pilot. Discounted payment is stronger evidence than enthusiastic free participation.

Phase 2: repeatable professional channels

Turn the strongest workflow into a packaged professional offer. Likely early wedges are estate/fiduciary intake, appraisal evidence collection, or valuable-articles insurance readiness. P4 should deepen the winning workflow without abandoning its cross-category evidence model.

Phase 3: embedded scale

After retention, onboarding, security, and partner economics are proven, pursue trust companies, wealth managers, insurance organizations, estate-planning platforms, storage providers, auction houses, and luxury resale operators. Enterprise distribution should be earned by proof, not treated as a prerequisite for launch.

Core messages

Audience	Message
Household	Keep the proof surrounding valuable property together before insurance, inheritance, loss, or sale makes the missing pieces expensive.
Professional	Turn fragmented client records into a maintained evidence packet without accepting responsibility for claims outside your role.
Enterprise partner	Add a private, auditable property-evidence workflow to a relationship your customers already trust.
Manufacturer / brand	Issue a durable, status-checkable origin credential that can remain useful through service, resale, inheritance, and transfer.

Audience	Message
What not to lead with	Blockchain, NFTs, tokens, universal title, or guaranteed authenticity. The cryptography can work quietly in the basement.

9. Product and Technology Plan

The P4 Evidence Integrity Engine

The proposed Evidence Integrity Engine is the most valuable proprietary part of P4. A digital vault, QR lookup, or attractive passport interface can be copied. A system that consistently evaluates who asserted what, about which physical article, from which evidence, at what time, and with what later changes is much harder to reproduce.

The engine should not produce a single unexplained authenticity score. It should assemble transparent evidence indicators, identify contradictions and missing links, and show the authority and scope of each source. Its output would help a buyer, heir, fiduciary, insurer, dealer, or manufacturer decide whether the evidence is sufficient for the intended transaction and whether specialist review is needed.

Engine component	What it evaluates	Proprietary value
Claim and source model	The precise assertion, its maker, the maker's authority, scope, date, status, and supporting evidence.	Creates a consistent evidence grammar across brands, categories, and professional disciplines.
Physical item binding	Serials, hallmarks, measurements, forensic images, secure-element responses, and category-specific identifiers.	Makes it harder to attach a genuine record or copied credential to a substitute article.
Lifecycle history	Possession, custody, appraisal, service, storage, loss, dispute, transfer, revocation, and correction events.	Builds a longitudinal history that becomes more valuable and harder to recreate with time.
Conflict and anomaly detection	Duplicate identifiers, incompatible locations or dates, cloned credential use, missing custody links, and contradictory claims.	Produces fraud and substitution intelligence from rules and accumulated operating data.
Selective verification	The minimum evidence a recipient needs for a defined purpose without exposing the owner's full collection or private documents.	Combines trust with privacy and supports multiple professional workflows.
Issuer and professional network	Verified organizations, delegated authority, credential status, and the limits of each participant's opinion.	Creates network value and makes P4 useful without pretending to be the authenticator for every category.

Why the original concept is practical now

The archived concept was ahead of the available commercial infrastructure. Managed encrypted storage, reliable cloud databases, mature digital signatures, verifiable credential standards, secure NFC components, modern computer vision, inexpensive high-resolution cameras, and anomaly-detection tools can now be combined without building every layer from scratch. These technologies do not make evidence true automatically. They make it practical to preserve evidence, identify its source, bind it more securely to an article, detect inconsistencies, and verify limited information without exposing the entire record.

The archive may help establish the history and continuity of the concept, but it does not by itself create patent rights or prove that every element was novel. P4 should present the history as evidence of sustained insight and product direction while asking counsel to determine which new technical implementations can be protected today.

How the proprietary value compounds

1. Early pilots establish the claim model, category templates, issuer rules, and practical evidence requirements.
2. Each consented record and later event improves P4's understanding of normal and suspicious histories.
3. Professional and manufacturer participation increases the number and authority of verifiable claims.
4. Better evidence and anomaly detection increase buyer and professional confidence, encouraging further participation.
5. The resulting longitudinal dataset, operating rules, integrations, and trusted relationships become more difficult for a new entrant to reproduce.

Patent applications should focus on technically specific, externally visible mechanisms that competitors could reverse engineer. Fraud rules, scoring weights, issuer-vetting methods, reference data, and security controls should generally remain confidential trade secrets. The combination of patents, trade secrets, proprietary data, contracts, integrations, and trusted relationships is more defensible than any single legal right.

Architecture principles

P4 should be built as an evidence-grade multi-tenant SaaS platform. It must be narrow enough for a small senior team to deliver, but serious about identity, permissions, file integrity, auditability, backup, recovery, and privacy from the first live pilot.

Layer	Pilot recommendation	Reason
Experience	Responsive web app / progressive web app	One codebase for desktop, tablet, and phone; no native apps initially.

Layer	Pilot recommendation	Reason
Front end	React / Next.js with TypeScript	Maintainable workflows, dashboards, and strong hiring market.
Back end	TypeScript API (for example NestJS) or Python FastAPI	Compact team can move quickly with disciplined service boundaries.
Database	Managed PostgreSQL	Relational model for assets, claims, roles, permissions, events, and attestations.
Evidence storage	AWS S3 or equivalent with encryption, versioning, and Object Lock/retention controls	Preserve original files and prevent silent overwrite where appropriate. [9]
Identity	Managed identity provider with MFA and role-based access	Reduce authentication risk and support professional/admin controls.
Evidence layer	SHA-256 hashes, append-only event log, timestamps, signatures, exports	Makes P4 an evidence system rather than a gallery.
Issuer trust	Verified organizations, signing keys, delegated authority, credential status and revocation	Shows who made each claim and whether that issuer still stands behind it. [10]
Physical binding	Serials, hallmarks, forensic images, tamper-evident labels, or NFC secure elements by category	Raises the cost of substituting a fake article; avoids treating a clonable QR code as authentication.
AI assistance	OCR, receipt parsing, serial capture, missing-field and image-quality checks	Reduce effort; keep AI output as draft until confirmed.
Interoperability	W3C Verifiable Credentials, GS1 identifiers, C2PA-compatible media provenance where useful	Accept and issue portable evidence rather than creating another silo. [10][11][12]
Later anchoring	Trusted timestamp or periodic Merkle-root anchoring	Optional independent proof without exposing private data or forcing wallet use.

Evidence flow

1. A household or professional creates an asset record.
2. Original files are uploaded, encrypted, versioned, and assigned a cryptographic fingerprint.
3. Claims are stored separately from evidence, with issuer, subject, date, status, and evidence grade.

4. Every meaningful action creates a protected event: creation, upload, correction, review, attestation, share, export, dispute, or transfer.
5. A qualified participant may sign a limited attestation stating precisely what was reviewed and what was concluded.
6. P4 generates a selective evidence view or signed PDF/data export with verification instructions.
7. Corrections supersede prior claims; they never silently rewrite the historical record.

Manufacturer-issued authenticity workflow

The strongest future P4 record begins at manufacture or first authorized sale. The issuer creates a unique product identity, records distinguishing characteristics, signs a narrowly worded origin or authenticity claim, binds the credential to the physical article, and publishes a status method. Authorized service centers, laboratories, dealers, and later owners append their own scoped events. A buyer can then verify the credential independently and compare it with the article before accepting a transfer. This architecture follows the issuer-holder-verifier model used by W3C Verifiable Credentials and complements GS1 identification and traceability standards. [10][11]

Blockchain position

Blockchain should not be the pilot backbone. A ledger can show that a digital fingerprint existed by a certain time; it cannot prove that a photographed watch, painting, handbag, coin, gem, or antique was genuine or that the uploader held legal title. Truth depends on source documents, identity, physical-to-digital binding, custody, expert review, and professional scope. If later used, P4 should anchor only a batch hash or Merkle root. Names, addresses, photographs, values, estate data, insurance data, and ownership details must not be published on-chain.

What not to build first

- Native iOS and Android applications.
- Tokens, NFTs, consumer wallets, or token economics.
- A public ownership registry or self-declared universal title authority.
- A marketplace, payments, escrow, or lending platform.
- Automated authenticity or appraisal conclusions presented as fact.
- Integrations with every brand, registry, insurer, or professional system.

10. Development Roadmap and Funding Gates

Stage	Duration / capital	Work	Advance only if
0. Validation	0-3 months \$25k-\$50k	20-25 interviews; evidence schema; prototype; 5-10 concierge households; 75-150 records; pricing tests.	3+ professional design partners; 5+ households; usable outputs; 2 paid or committed pilots; repeat behavior.
1. Pilot MVP	Months 4-9 \$125k-\$250k	Secure capture, evidence store, claims, event history, permissions, professional portal, sharing, PDF/data reports.	Clear wedge; completed records; acceptable capture effort; professional reliance; security plan; paid commitments.
2. Commercial pilot	Months 10-18 \$350k-\$750k	Security hardening, richer attestations, onboarding operations, partner sales, API groundwork, compliance, support.	Repeatable onboarding; retention; renewals; bounded liability; measured unit economics; partner-led acquisition.
3. Seed scale	After commercial proof Illustrative \$1.5m-\$2.5m	Expand engineering and channels; category integrations; enterprise pilots; operational security and support.	Commercial-pilot KPIs justify a specific scale plan and valuation.
4. Expansion	Evidence-driven	Portable credentials, embedded distribution, deeper integrations, selective mass-market P4 Home.	Enterprise demand, low-friction capture, reliable margins, and distribution proof.

11. Operations, Team, and Governance

Initial team

Role	Timing	Primary responsibility
Founder / product governance	Now	Evidence policy, rights/roles model, estate and fiduciary workflows, partner interviews, company narrative, and scope discipline.

Role	Timing	Primary responsibility
Lead investor / adviser	After role agreement	Stage funding, strategic input, agreed governance and information rights; operational role only if specifically defined.
Lead full-stack architect	Before software MVP	Architecture, security model, database, permissions, file integrity, deployment, code quality, and technical hiring.
Product full-stack engineer	MVP	Owner and professional workflows, capture, uploads, dashboards, exports, automated tests.
UX / product designer	Fractional from validation	Research and low-friction capture design for households and professionals.
Security / cloud reviewer	Fractional; before live data	Threat model, access controls, logging, encryption, backup, recovery, incident readiness, and independent review.
QA / test support	Fractional near pilot	Permissions, exports, workflow, edge cases, regression, and restore testing.
Counsel / category advisers	Fractional	Privacy, contracts, IP, insurance, professional-scope language, appraisal/authentication practices, and pilot agreements.

Governance recommendations

- Form a conventional operating company and assign all new product, code, design, trademarks, and documentation to it.
- Document founder and investor roles, board rights, consent rights, information rights, compensation, follow-on expectations, dilution, deadlock, and exit scenarios before substantial funding.
- Use confidentiality, work-made-for-hire, and invention-assignment agreements with employees, contractors, advisers, and design partners.
- Create a product-and-security risk committee function early, even if it is initially a quarterly founder/architect/counsel review.
- Do not form a large nonprofit standards body or global registry authority during feasibility. Design continuity safeguards now, then form a narrow independent stewardship foundation when customers, professionals, manufacturers, or other issuers begin to rely on P4 across generations.

Long term continuity and institutional stewardship

A business entity can fail, be sold, change strategy, or discontinue a product. A nonprofit can fail as well. P4 therefore needs technical, contractual, financial, and governance safeguards that work together. Owners must be able to export complete records in documented formats. Copies must be recoverable from independent backups. Critical software and documentation should enter escrow. A continuity

reserve should fund an orderly transfer. Objective failure events should activate a limited license that allows a qualified successor to keep verification and export functions operating. These duties should exist before a foundation is formed and later transfer to the foundation as an independent steward.

The operating company should retain control of product development, customer service, pricing, and the proprietary P4 Evidence Integrity Engine. The future foundation should hold or control only the assets and rights needed to prevent abandonment: continuity standards, persistent identifier policies, verification domains or successor routing, key-recovery procedures, escrow materials, reserve funds, and the right to appoint a replacement operator after defined failure events. The attached addendum proposes a board structure, formation tests, funding model, and staged transition.

Operating model

P4 should initially perform concierge onboarding itself or through closely supervised contractors. This is not the forever margin model; it is a learning engine. As category templates and AI-assisted extraction improve, routine capture can move to households and professional staff, while qualified experts retain responsibility for category-specific opinions.

12. Legal, Security, and Intellectual Property

Legal posture

- P4 records evidence and scoped statements; it does not adjudicate legal title, guarantee authenticity, set insured value, provide legal advice, or replace a qualified appraisal.
- Terms and exports must identify the issuer, scope, date, evidence grade, reliance limits, and whether a statement is user-supplied, document-supported, professional, issuer-confirmed, or externally linked.
- Professional agreements should allocate responsibility to the party actually performing the appraisal, authentication, insurance, legal, or fiduciary service.
- Counsel should analyze privacy laws, data-retention duties, incident notice, electronic signatures, consumer terms, professional liability, insurance coverage, and state-specific estate/fiduciary issues before live expansion.
- P4 should obtain appropriate cyber, technology E&O, general liability, and management-liability coverage as operations mature.

Security minimums before live pilot

Control	Minimum requirement
Identity	MFA for professional and administrative users; strong recovery and session controls.
Authorization	Least privilege, tenant isolation, explicit invitations, field/purpose-limited sharing, and access revocation.

Control	Minimum requirement
Encryption	Encryption in transit and at rest; managed keys and secrets; no sensitive content in public logs or URLs.
Evidence integrity	Original-file retention, cryptographic hashes, protected event history, signed exports, and restore tests.
Operations	Monitoring, alerts, backups, tested recovery, incident response, vendor review, and administrative audit trail.
Data minimization	Avoid exact storage/location details unless required; separate identity, asset, value, and verification data where practical.
Independent review	Threat modeling and security review before real customer data; penetration testing before broad commercial launch.

Intellectual property

The dated 2007-2015 archive is valuable evidence of authorship and unusually early product judgment, but it is not a present-day monopoly and does not automatically establish a current patent priority date. U.S. patentability generally turns on eligible subject matter, novelty, and non-obviousness.

[21][22][23][24] Public disclosures can also impair rights, especially outside the United States, so the company should obtain patent counsel before any public demo, crowdfunding campaign, technical paper, or open pilot. [25]

Preliminary patent landscape — September 2026

A preliminary, non-exhaustive search found meaningful prior art and live patent families around cryptographic provenance, ledger-based attestations, NFC-linked ownership transfer, blockchain product authentication, digital passports, and physical fingerprints. This means the broad formulation “digital passport plus QR/NFC plus ledger plus ownership transfer” is crowded and is unlikely to provide a useful monopoly by itself. Database status indicators can change and are not legal opinions.

Representative publication	Apparent overlap and status indicator	P4 implication
US 2016/0164884 A1	Cryptographic supply-chain provenance using signatures, labels, keys, and blockchain; Google Patents lists the application as abandoned, but the publication remains potential prior art. [28]	Do not rely on generic signing or ledger provenance as the invention.
US 2017/0317833 A1 / US 10,333,705 B2	Centralized or distributed-ledger attestation family with 2016 priority; an issued U.S. patent is shown. [29]	Claim-level attestation concepts require careful claim-chart analysis.

Representative publication	Apparent overlap and status indicator	P4 implication
WO 2021/215998 A1	NFC scanning, ownership verification, and ownership transfer; PCT status is shown as ceased, with related national filings. [30]	Search the U.S. and other national family members before implementing transfer.
US 2021/0103938 A1 / US 12,470,254 B2	NFC product authentication, blockchain transactions, and ownership indications; Google Patents shows an active 2025 grant and continuation activity. [31]	Secure-tag and transaction flows present a material freedom-to-operate question.
US 2022/0215382 A1 / US 12,236,419 B2	Scanned product codes, unique tokens, and blockchain product authentication; an active issued patent is shown. [32]	Avoid assuming tokenized product checks are open territory.
US 2025/0005597 A1	Physical luxury, art, or collectible goods paired with a digital passport and authentication mechanism; pending prosecution is shown. [33]	Monitor prosecution and distinguish P4's actual technical mechanism.
US 12,256,026 B2	Physical fingerprints linked to digital records and historical provenance. [34]	Category-specific image or fingerprint binding requires targeted review.

This search cannot “make sure” P4 is clear. Patent applications can remain unpublished for a period; claims may change; families differ by country; ownership and expiration require confirmation; and infringement depends on the claims, not the title or abstract. Patentability and freedom to operate are separate questions. A registered patent attorney should conduct both against the actual MVP architecture.

Most promising protection strategy

- Investigate technically specific claim-and-evidence mechanisms that combine source authority, status, supersession, dispute state, and selective disclosure—only where implementation is genuinely novel rather than an abstract business rule.
- Investigate clone or substitution detection that combines secure-element challenge-response, item-specific images or fingerprints, duplicate-use anomaly logic, revocation, and custody events.
- Investigate privacy-preserving transfer protocols that reveal only scoped evidence while preserving issuer verification and historical continuity.
- Investigate category-specific physical-to-digital binding methods. Generic inventory, QR/NFC lookup, certificates, blockchain timestamps, and ordinary ownership transfer should be treated as crowded territory.
- Patent features that will be visible and reverse engineerable; keep non-public fraud rules, thresholds, datasets, issuer-vetting methods, and operational controls as trade secrets protected by reasonable measures. [26][27]

IP work plan

1. Run a confidential invention-harvest workshop with product, technical, and category participants; separate old concepts from new technical implementation.
2. Have patent counsel search prior art and create a claim chart for the most promising mechanisms and relevant live families.
3. File one or more sufficiently detailed provisional applications before public disclosure. A thin placeholder filing may not support later claims. [25]
4. After the MVP architecture is concrete, commission a separate freedom-to-operate review and design around blocking claims where practical.
5. Before the 12-month provisional deadline, decide which inventions justify U.S. non-provisional and possible PCT filings. [25]
6. Monitor patents, standards, competitors, and product changes quarterly; update the claim chart and invention log.

13. Financial Plan

The following five-year base case is an operating model, not a forecast backed by historical company performance. It assumes P4 passes its validation gates, launches a software MVP, develops professional distribution, and begins enterprise contracts in Year 3. Management should replace every assumption with observed data as the pilot proceeds.

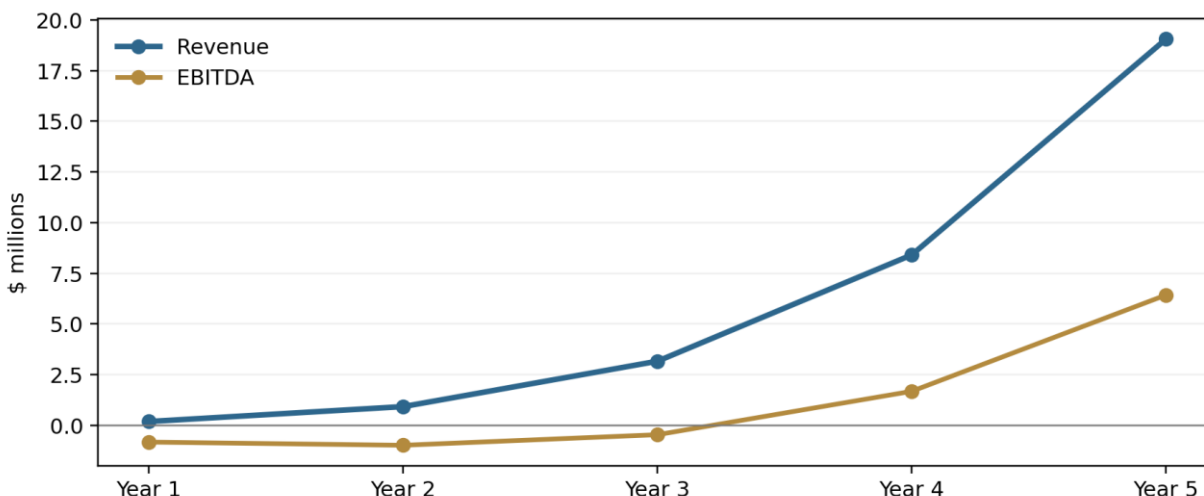
Base-case revenue model

Revenue stream	Y1	Y2	Y3	Y4	Y5
Household subscriptions	\$18,750	\$175,500	\$837,000	\$2,520,000	\$6,670,000
Professional subscriptions	\$43,200	\$252,000	\$891,000	\$2,340,000	\$5,070,000
Concierge onboarding	\$84,000	\$315,000	\$585,000	\$900,000	\$1,320,000
Attestation / transaction	\$40,000	\$180,000	\$600,000	\$1,400,000	\$3,000,000
Enterprise / API	\$0	\$0	\$250,000	\$1,250,000	\$3,000,000
Total revenue	\$185,950	\$922,500	\$3,163,000	\$8,410,000	\$19,060,000

Base-case profit model

Planning P&L	Y1	Y2	Y3	Y4	Y5
Revenue	\$185,950	\$922,500	\$3,163,000	\$8,410,000	\$19,060,000
Cost of revenue	\$65,082	\$258,300	\$727,490	\$1,682,000	\$3,430,800
Gross profit	\$120,868	\$664,200	\$2,435,510	\$6,728,000	\$15,629,200
Operating expenses	\$950,000	\$1,650,000	\$2,900,000	\$5,050,000	\$9,200,000
EBITDA	\$-829,132	\$-985,800	\$-464,490	\$1,678,000	\$6,429,200

Base-case revenue and EBITDA



Interpretation

- The model reaches approximately \$3.2 million of revenue in Year 3 and operating break-even during Year 4, not because those results are assured but because the assumed channel and retention model requires time to mature.
- The first two years remain capital intensive because security, product development, professional sales, and concierge learning precede scale.
- The cumulative modeled EBITDA deficit through Year 3 is approximately \$2.28 million. Allowing working capital and contingency suggests roughly \$2.75-\$3.25 million of staged external capital through sustainable break-even under this base case.
- Only the first \$25,000-\$50,000 validation tranche is recommended now. Later funding should be priced and authorized after measured evidence, not treated as a present commitment.
- If professional distribution or retention is weaker than assumed, capital needs rise sharply. If one workflow generates stronger partner-led acquisition and enterprise demand, break-even may arrive earlier.

How the revenue assumptions were built

The model is driver-based rather than a top-down percentage of a giant market. Household and professional subscriptions use average paid accounts during each year; year-end counts only describe the exit run rate. Transaction revenue is event volume multiplied by P4's average share. Enterprise revenue is contract count multiplied by annual contract value. These are management hypotheses, not facts obtained from the comparable companies.

Revenue driver	Y1	Y2	Y3	Y4	Y5
Average paid household accounts	75	675	3,100	9,000	23,000
Household annual price	\$250	\$260	\$270	\$280	\$290
Average paid Pro firms	8	42	135	325	650
Pro monthly ARPA	\$450	\$500	\$550	\$600	\$650
Concierge jobs × average fee	120 × \$700	450 × \$700	900 × \$650	1,500 × \$600	2,400 × \$550
P4-paid events × average revenue	800 × \$50	3,000 × \$60	8,000 × \$75	17,500 × \$80	30,000 × \$100
Enterprise contracts × ACV	0	0	2 × \$125k	5 × \$250k	10 × \$300k

Reasonableness is conditional. The price points sit inside the proposed customer ranges, but account growth, paid-event frequency, and enterprise conversion have not been validated. The pilot must measure willingness to pay, completion, professional conversion, referral rate, renewal intent, event frequency, support time, and acquisition cost before these figures are used for financing.

Cost structure and benchmark basis

Operating expense is built from the staffing and controls required for a security-sensitive software business, not from a generic small-business ratio. U.S. Bureau of Labor Statistics medians were \$135,980 for software developers and \$129,180 for information security analysts in May 2025. [35][36] P4 uses higher blended fully loaded amounts in later years to allow for seniority, payroll taxes, benefits, recruiting, contractors, and management. A 2025 private-SaaS survey reported continued focus on approximately 90% retention and EBITDA performance, while mature SaaS gross margins are commonly benchmarked around 70%-80%. [37][38] P4 begins below that range because concierge delivery and partner/event costs are deliberately heavier, then improves only if capture becomes more self-service.

Operating expense build	Y1	Y2	Y3	Y4	Y5
People and contractor compensation	\$600k	\$1.05m	\$1.90m	\$3.20m	\$5.80m
Security, legal, and insurance	\$120k	\$160k	\$250k	\$380k	\$650k
Sales, marketing, and research	\$100k	\$220k	\$430k	\$900k	\$1.70m
Software, tools, and non-COGS cloud	\$45k	\$70k	\$100k	\$170k	\$280k
General and administrative	\$45k	\$100k	\$150k	\$280k	\$500k
Contingency	\$40k	\$50k	\$70k	\$120k	\$270k
Total operating expense	\$950k	\$1.65m	\$2.90m	\$5.05m	\$9.20m

The compensation line is approximately 4, 7, 11-12, 18-19, and 31 average employee/contractor equivalents at blended fully loaded costs of roughly \$150,000, \$150,000, \$165,000, \$173,000, and \$187,000. Actual hiring may be leaner or more contractor-heavy. Cost of revenue includes direct concierge labor, partner or issuer shares, payments, production cloud use, storage, and customer support. The assumed COGS rate falls from 35% to 18%; if delivery does not become more automated and partner-led, that improvement will not occur.

Capital bridge and downside sensitivity

The cumulative modeled EBITDA loss through Year 3 is \$2,279,422. Adding 20% contingency produces approximately \$2.74 million; working-capital timing and financing friction support the rounded planning range of \$2.75-\$3.25 million through break-even. This is a staged capital envelope, not a recommendation to raise or spend it at once.

Isolated change to Year 3	Approximate Year 3 EBITDA effect
25% fewer average paid household accounts	-\$209,250
25% fewer average paid Pro firms	-\$222,750
25% fewer concierge jobs	-\$146,250
25% fewer paid attestation / transaction events	-\$150,000
Enterprise contracts delayed to Year 4	-\$250,000
Cost of revenue five percentage points higher	-\$158,150

Isolated change to Year 3	Approximate Year 3 EBITDA effect
Operating expense 10% higher	-\$290,000

Base-case Year 3 EBITDA is a loss of \$464,490. Each sensitivity is shown alone; combined downside would be materially worse. Management should maintain a rolling 18-month cash plan and fund each stage only after its evidence gate.

Capital allocation through commercial proof

Use	Indicative share	What it buys
Product and engineering	40%-50%	Senior architecture, software build, QA, cloud operations, and evidence/reporting functionality.
Security, privacy, legal, and insurance	12%-18%	Threat modeling, reviews, agreements, policies, trademark/IP work, and appropriate coverage.
Concierge pilot and customer operations	12%-18%	Real record creation, templates, onboarding, support, and measured workflow learning.
Sales, partnerships, and research	12%-18%	Founder-led recruitment, professional pilots, materials, events, and later channel sales.
Contingency and administration	10%-15%	Working capital, vendors, accounting, and unplanned pilot requirements.

14. Risks and Mitigation

Risk	Why it matters	Mitigation
Adoption / completion	Cataloging is easy to postpone and may require too much help.	Concierge start, immediate estate/insurance outputs, AI-assisted capture, time measurement, and stop gates.
Trust and authority	A startup cannot declare facts about valuable property true.	Source labels, evidence grades, scoped attestations, qualified partners, and no universal-title claims.

Risk	Why it matters	Mitigation
Physical-to-digital binding	A genuine document can be attached to the wrong object.	Serials, hallmarks, category checklists, multiple images, secure tags where useful, and reinspection events.
Credential or tag cloning	A copied QR code, transplanted tag, compromised key, or duplicate identity can make a fake appear linked to a genuine record.	Secure elements where justified, issuer key controls, revocation/status checks, duplicate-use detection, item comparison, rotation, and incident procedures.
Privacy / theft exposure	A database of valuables and locations is an attractive target.	Minimal location data, tenant isolation, encryption, MFA, least privilege, monitoring, testing, and incident readiness.
Professional liability	Users may rely on records in claims, estate disputes, or sales.	Clear scope, issuer identity, reliance limits, contracts, qualified providers, and E&O/cyber insurance.
Platform crowding	Brands and category platforms already issue passports or certificates.	Cross-brand owner control, professional workflow, portability, and integration rather than imitation.
Channel concentration	One profession or partner may control too much acquisition.	Test estate, appraisal, insurance, and dealer channels; deepen the winner while maintaining alternatives.
Capital overreach	A universal registry vision can consume money before behavior is proven.	Fixed stage gates, narrow MVP, KPI-based releases, and explicit “do not build” list.
Founder / investor ambiguity	Personal relationships can blur authority and expectations.	Written governance, roles, information rights, compensation, consent rights, and exit provisions.
Institutional continuity	A sale, insolvency, shutdown, security failure, or abandoned product could strand records that families expect to remain useful for decades.	Portable exports, documented formats, redundant backups, continuity reserve, source-code and documentation escrow, objective activation events, successor-operator rights, and later independent foundation oversight.

15. Milestones and Investment Proposal

Immediate 90-day authorization

Authorize a fixed validation budget of \$25,000-\$50,000. The stage is designed to determine whether P4 deserves a software investment and which workflow should lead the MVP. The plan assumes no particular lead investor is committed. The first money is unusually risky because it buys feasibility evidence rather than the launch of a proven business format; the protection is a small, fixed tranche with explicit stop conditions.

Validation use	Planning range	Evidence purchased
Discovery interviews and case maps	\$5k-\$8k	Problem frequency, workflow urgency, channel interest, and design-partner commitments.
Prototype, evidence schema, and reports	\$6k-\$12k	Comprehension, completion, professional usefulness, and concrete MVP scope.
Architecture and security threat model	\$4k-\$8k	Technical feasibility, risk register, data design, and build estimate.
Preliminary IP/legal and pilot contracts	\$5k-\$12k	Invention harvest, counsel-directed search, provisional decision, ownership, confidentiality, and pilot terms.
Concierge pilot operations and contingency	\$5k-\$10k	Real records, onboarding time, support burden, willingness to pay, and unexpected costs.

Weeks	Deliverable	Required evidence
1-3	20-25 structured interviews; five case maps; partner shortlist; initial evidence and privacy model.	At least 3 professional design partners and 5 households commit.
4-6	Clickable prototype; evidence grades; roles/rights model; sample passport; estate, insurance, and appraisal reports.	Users understand evidence strength and can complete one record with limited help.
7-10	Concierge pilot across 75-150 assets; professional reviews or limited attestations; real workflow exports.	Median guided capture under 15 minutes; at least 2 outputs used in real work.
11-13	Pricing results; security plan; scoped MVP backlog; pilot agreements; next-stage budget and team plan.	At least 2 paid or contractually committed professional pilots and repeat household behavior.

Decision rule at day 90

Decision	Condition
GO	Owners complete records; professionals rely on outputs; at least two channels pay or commit; onboarding effort supports tested pricing.
ADJUST	One category, workflow, or customer type produces materially stronger behavior. Deepen that wedge while preserving the shared evidence architecture.
PAUSE / STOP	Interest does not become completion and payment; professionals will not use outputs; acquisition depends on expensive consumer advertising; or liability/security cannot be bounded economically.

Financing and governance discussion

The present ask is approval of the validation tranche and governance process, not the entire five-year plan. Before funding, founders and investors should document the instrument, ownership, control, compensation, budget authority, reporting, dilution, intellectual-property assignment, related-party decisions, and exit rights with appropriate counsel.

First-money strategy and crowdfunding

Public crowdfunding is possible, but it is not the recommended first source of feasibility capital. Rewards crowdfunding requires a simple public story and fulfillment promise; P4 is a privacy-sensitive B2B2C service whose most valuable early work is confidential learning. Regulation Crowdfunding can raise up to \$5 million in a 12-month period through an SEC-registered intermediary, but it requires public issuer and offering disclosures, ongoing compliance, and securities administration. [39] That public footprint is a poor trade before invention capture, provisional filings, and paid pilot evidence.

Sequence	Indicative contribution	Confidentiality and purpose
3-5 professional design partners	\$5k-\$10k each	Private sponsorship or paid pilots under confidentiality, IP, and data-use terms; validates channel demand.
10-20 founding households	\$500-\$1,500 each	Privately recruited concierge deposits; validates willingness to pay and funds record creation.
Small private angel / SAFE / note round	Fill the remaining validation or MVP need	Appropriate only with counsel, clear governance, and no assumption that one individual funds the project.

Sequence	Indicative contribution	Confidentiality and purpose
Accelerator or non-dilutive program	Program-dependent	Use only if ownership, publicity, and disclosure requirements are acceptable.
Public rewards or equity crowdfunding	After IP filing and pilot proof	Potentially useful for market visibility or a broader raise, but accept that campaign and required offering information become public.

If crowdfunding is used later, disclose the customer problem, intended outcomes, business model, team capability, and pilot evidence—not security internals, fraud rules, claim-schema details, scoring thresholds, private datasets, or unreleased item-binding methods. Patent filings should precede the campaign. Securities counsel should confirm offering eligibility, required disclosures, intermediary selection, financial-statement requirements, investor communications, and applicable “bad actor” rules. A campaign can be managed carefully; it cannot be confidential.

Conclusion

P4 is worth testing because its commercial core is narrow and testable. The four P’s still fit: produce source-attributed evidence, preserve it against silent alteration, protect those who rely on it, and make provenance understandable. Trusted issuers can make counterfeits and fabricated histories harder to pass undetected. Portability, escrow, recovery, and later independent stewardship can keep those records useful even if the original company changes or fails. The next move is a paid validation of the Asset Evidence Passport, with continuity requirements included in the technical and legal design from the beginning.

Appendix A. MVP Requirements

Capability	MVP requirement	Acceptance test
Asset capture	Templates for watches, jewelry/gems, bags/leather goods, art/antiques, and selected collectibles.	Representative items can be documented without inventing fields.
Evidence store	Encrypted photos, video, PDFs, receipts, certificates, appraisals, service and insurance records.	Each file has source, date, fingerprint, access policy, and claim relationship.
Claim model	Issuer, subject, assertion, evidence, grade, status, effective date, and superseding event.	Corrected claims remain historical while the current view is clear.
Roles and rights	Owner, beneficial owner, custodian, fiduciary/agent, lienholder, creator, IP holder, beneficiary, verifier.	Split roles can be represented without implying unsupported legal conclusions.
Credentials / attestations	Issue or ingest a signed, scoped claim with issuer identity, authority, status, and credential metadata.	Recipient verifies who asserted what, when, whether it changed, and whether it remains current.
Sharing	Time-limited views and signed PDF/data exports with field-level disclosure.	Insurance evidence can be shared without unrelated asset or location data.
Reports	Collection schedule, insurer/appraiser packet, estate schedule, executor inventory, transfer packet.	Pilot professionals use at least two report types in real work.
History / disputes	Append-only events for capture, appraisal, service, custody, transfer, challenge, evidence, resolution, supersession.	No ordinary user can silently rewrite an earlier event.
Security	MFA, encryption, least privilege, tenant isolation, audit logs, backups, incident plan, secrets management.	Independent review and documented restore/access tests before commercial pilot.
Portability	Complete human-readable and structured export.	A household can preserve useful records outside P4 and avoid lock-in.

Appendix B. Base-Case Financial Assumptions

Driver	Y1	Y2	Y3	Y4	Y5
Year-end household accounts	150	1,200	5,000	15,000	35,000
Average paid household accounts	75	675	3,100	9,000	23,000
Average household price / year	\$250	\$260	\$270	\$280	\$290
Year-end professional firms	15	70	200	450	850
Average paid professional firms	8	42	135	325	650
Average Pro monthly revenue	\$450	\$500	\$550	\$600	\$650
Concierge jobs	120	450	900	1,500	2,400
Average concierge revenue	\$700	\$700	\$650	\$600	\$550
Paid events	800	3,000	8,000	17,500	30,000
Average P4 revenue / event	\$50	\$60	\$75	\$80	\$100
Enterprise contracts / ACV	0	0	2 / \$125k	5 / \$250k	10 / \$300k
Cost of revenue	35%	28%	23%	20%	18%
Operating expenses	\$0.95m	\$1.65m	\$2.90m	\$5.05m	\$9.20m

Subscription revenue uses average paid accounts during each year, not merely year-end counts. The model assumes falling cost of revenue as capture becomes more self-service and partner-delivered. No tax provision, interest, depreciation, stock compensation, or financing transaction is modeled. All figures should be rebuilt from actual cohort, pricing, staffing, and vendor data after validation.

Sources and Notes

[1] UBS, Global Wealth Report 2026. <https://www.ubs.com/us/en/wealth-management/insights/global-wealth-report.html>

[2] Board of Governors of the Federal Reserve System, Changes in U.S. Family Finances from 2019 to 2022 (Nov. 8, 2023). <https://www.federalreserve.gov/publications/october-2023-changes-in-us-family-finances-from-2019-to-2022.htm>

[3] U.S. Census Bureau, Census Bureau Releases New Estimates on America's Families and Living Arrangements (Dec. 2, 2025). <https://www.census.gov/newsroom/press-releases/2025/families-and-living-arrangements.html>

- [4] Chubb, Survey Finds 78% of Young Luxury Collectors Buy for Investment, But More Than Half Remain Uninsured (July 16, 2026). <https://news.na.chubb.com/2026-07-16-Chubb-Survey-Finds-78-of-Young-Luxury-Collectors-Buy-for-Investment,-But-More-Than-Half-Remain-Uninsured>
- [5] Bain & Company and Altagamma, Global luxury stabilizes amid compounding disruptions (June 25, 2026). <https://www.bain.com/about/media-center/press-releases/2026/global-luxury-stabilizes-amid-compounding-disruptions-as-brands-race-to-amplify-meaning-and-rebuild-relevance/>
- [6] Art Basel and UBS, The Art Basel and UBS Art Market Report 2026 - Global Sales. <https://theartmarket.artbasel.com/global-sales>
- [7] Cerulli Associates, Cerulli Anticipates \$124 Trillion in Wealth Will Transfer Through 2048 (Dec. 5, 2024). <https://www.cerulli.com/press-releases/cerulli-anticipates-124-trillion-in-wealth-will-transfer-through-2048>
- [8] Chubb, 2025 Wealth Survey: The Resilient Mindset (Dec. 3, 2025). <https://news.chubb.com/2025-12-03-Chubb-2025-Wealth-Survey-The-Resilient-Mindset>
- [9] Amazon Web Services, Locking objects with Object Lock, Amazon S3 User Guide. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>
- [10] World Wide Web Consortium, Verifiable Credentials Data Model v2.0 (May 15, 2025). <https://www.w3.org/TR/vc-data-model-2.0/>
- [11] GS1, Digital Product Passport. <https://www.gs1.org/standards/gs1-digital-link>
- [12] Coalition for Content Provenance and Authenticity, C2PA Technical Specifications. <https://c2pa.org/specifications/specifications/2.2/index.html>
- [13] IETF RFC 9943, An Architecture for Trustworthy and Transparent Digital Supply Chains (SCITT) (June 2026). <https://www.rfc-editor.org/rfc/rfc9943.html>
- [14] Chubb, Home and valuables loss-prevention and collection-risk resources (context for insurance workflows). <https://www.chubb.com/us-en/individuals-families/products/valuable-articles.html>
- [15] OECD and EUIPO, Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges (May 7, 2025). https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_6c1637f4-en.html
- [16] Vogue Business, Aura takes shape: Prada, OTB and LVMH weigh the future of luxury's blockchain solution (Sept. 2025). <https://www.voguebusiness.com/story/technology/aura-takes-shape-prada-otb-and-lvmh-weigh-the-future-of-luxurys-blockchain-solution>
- [17] Chrono24, Company and 2025 market review. <https://about.chrono24.com/>
- [18] Professional Sports Authenticator, company and price-guide resources. <https://www.psacard.com/priceguide>
- [19] Trust & Will, Trust & Will Secures Over \$25M in Series C (Mar. 2025). <https://www.prnewswire.com/news-releases/trust-will-secures-over-25m-in-series-c-to-expand-the-nations-leading-estate-planning-platform-302397820.html>
- [20] Vogue, How AI Is Transforming Social Media Behind the Scenes (2024), discussing Entrupy and TikTok Shop. <https://www.vogue.com/article/how-ai-is-transforming-social-media-behind-the-scenes>
- [21] 35 U.S.C. § 101, patent-eligible inventions. <https://www.law.cornell.edu/uscode/text/35/101>
- [22] 35 U.S.C. § 102, novelty and prior art. <https://www.law.cornell.edu/uscode/text/35/102>
- [23] 35 U.S.C. § 103, non-obvious subject matter. <https://www.law.cornell.edu/uscode/text/35/103>
- [24] USPTO, Subject Matter Eligibility guidance. <https://www.uspto.gov/patents/laws/examination-policy/subject-matter-eligibility>

- [25] USPTO, Provisional Application for Patent. <https://www.uspto.gov/patents/basics/apply/provisional-application>
- [26] USPTO, Trade Secret Policy. <https://www.uspto.gov/ip-policy/trade-secret-policy>
- [27] 18 U.S.C. § 1839, trade-secret definitions. <https://www.law.cornell.edu/uscode/text/18/1839>
- [28] Google Patents, US20160164884A1, Cryptographic verification of provenance in supply chain. <https://patents.google.com/patent/US20160164884A1/en>
- [29] Google Patents, US20170317833A1, attestation using a centralized or distributed ledger. <https://patents.google.com/patent/US20170317833A1/en>
- [30] Google Patents, WO2021215998A1, ownership data management and transfer. <https://patents.google.com/patent/WO2021215998A1>
- [31] Google Patents, US20210103938A1, NFC product authentication and transactions. <https://patents.google.com/patent/US20210103938A1/en>
- [32] Google Patents, US20220215382A1, product authentication using scanned codes and tokens. <https://patents.google.com/patent/US20220215382A1/en>
- [33] Google Patents, US20250005597A1, physical goods paired with digital passports. <https://patents.google.com/patent/US20250005597A1/en>
- [34] Google Patents, US12256026B2, physical fingerprints linked to digital records. <https://patents.google.com/patent/US12256026>
- [35] U.S. Bureau of Labor Statistics, Software Developers, Quality Assurance Analysts, and Testers (May 2025 wages). <https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm>
- [36] U.S. Bureau of Labor Statistics, Information Security Analysts (May 2025 wages). <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>
- [37] KeyBanc Capital Markets and Sapphire Ventures, 2025 Private SaaS Company Survey. <https://investor.key.com/press-releases/news-details/2025/PRIVATE-SAAS-COMPANY-SURVEY-REVEALS-AI-DRIVEN-TRANSFORMATION-AND-SUSTAINED-OPERATIONAL-EXCELLENCE/default.aspx>
- [38] Lighter Capital, SaaS Gross Margin Benchmarks. <https://www.lightercapital.com/blog/saas-gross-margin-benchmarks>
- [39] U.S. Securities and Exchange Commission, Regulation Crowdfunding. <https://www.sec.gov/resources-small-businesses/exempt-offerings/regulation-crowdfunding>
- [40] Kickstarter, A Year in Review: 2025 Kickstarter Highlights. <https://updates.kickstarter.com/a-year-in-review-2025-kickstarter-highlights/>
- [41] Paul Mockapetris, Domain Names - Concepts and Facilities, RFC 882, USC Information Sciences Institute (Nov. 1983). <https://www.rfc-editor.org/rfc/rfc882>
- [42] U.S. Department of Commerce, Statement of Policy on the Management of Internet Names and Addresses, commonly called the DNS White Paper (June 5, 1998). <https://www.ntia.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses>
- [43] U.S. Department of Commerce, Memorandum of Understanding with the Internet Corporation for Assigned Names and Numbers (Nov. 25, 1998). <https://www.ntia.gov/page/1998/memorandum-understanding-between-us-department-commerce-and-internet-corporation-assigned>

[44] ICANN, Amended and Restated Articles of Incorporation (Aug. 9, 2016).

<https://www.icann.org/en/governance/documents/amended-and-restated-articles-of-incorporation-of-internet-corporation-for-assigned-names-and-numbers-09-08-2016-en>

[45] Internal Revenue Service, Inurement and Private Benefit for Charitable Organizations.

<https://www.irs.gov/charities-non-profits/charitable-organizations/inurement-private-benefit-charitable-organizations>

Internal source basis

P4 Project Docs-Archive (August-September 2007); Walking Wealth / WARDTRAC materials; Survivor Locator materials; P4 Strategic Development Recommendation (Sept. 2, 2026); P4 Market Acceptance and Growth Strategy (Sept. 2, 2026); P4 Technology Build and Pilot Plan (Sept. 2026).

Third-party names and trademarks are used descriptively; no affiliation or endorsement is implied. Market figures describe populations or transaction flows, not P4 revenue. This plan is strategic and financial planning material, not legal, tax, insurance, appraisal, authentication, investment, or securities advice.

Appendix C Plain English Glossary

This glossary explains the technical, financial, legal, and organizational terms used in the plan. The definitions are practical explanations for business readers, not complete legal or engineering specifications.

ACV. Annual contract value. The average yearly revenue expected from one enterprise contract.

API. Application programming interface. A controlled way for one software system to exchange information or request a service from another.

Append only event history. A record in which new events are added but earlier events are not silently overwritten. A correction can supersede an earlier entry while leaving the original visible in the history.

Asset Evidence Passport. P4's owner-controlled record for one physical article, including claims, supporting files, sources, history, sharing rules, and verification information.

Attestation. A limited statement by an identified person or organization about what it observed, reviewed, or concluded. A digital attestation is signed electronically so the recipient can check its source and whether it changed.

Authentication. A specialist process used to form an opinion about whether an object is genuine. P4 records and verifies evidence; it does not automatically authenticate every object.

B2B2C. Business to business to consumer. P4 reaches households through professional or commercial partners as well as directly.

Blockchain. A shared ledger maintained across multiple computers. It may provide independent timestamp evidence, but it cannot establish that a physical object or an underlying claim is true.

CAC. Customer acquisition cost. Sales and marketing spending divided by the number of new customers acquired during the same period, with consistent accounting rules.

Challenge response. A security test in which a reader sends a changing challenge to a secure chip and checks the chip's cryptographic reply. It is harder to copy than a fixed printed code.

Claim. A specific statement about an article, such as its identity, origin, ownership, condition, appraisal, service, custody, or transfer.

Cloud service. Computing, databases, or storage operated in professional data centers and accessed through secure networks rather than kept only on a local computer.

COGS or cost of revenue. The direct cost of delivering revenue, such as transaction processing, production cloud use, concierge labor, partner shares, storage, and direct support.

Credential. A structured statement issued by an identified party. It may describe identity, authority, origin, inspection, service, or another limited fact or opinion.

Cryptographic agility. The ability to replace an aging or compromised encryption, signature, or hashing method without losing the record's history.

Cryptographic hash. A digital fingerprint calculated from a file or set of data. If the content changes, the fingerprint changes. A hash helps detect alteration but does not prove that the content was true when created.

Digital signature. A mathematical signature created with a private key and checked with a related public key. It can show which key signed a record and whether the signed content changed.

EBITDA. Earnings before interest, taxes, depreciation, and amortization. In this plan it is a simplified operating measure, not cash flow or net income.

Encryption. A method that makes information unreadable without the correct key. Encryption in transit protects information while moving; encryption at rest protects stored information.

Evidence grade. P4's label for the type and strength of support behind a claim, from self-recorded information through documents, professional statements, issuer confirmation, or authoritative external links.

Evidence Integrity Engine. The proposed proprietary P4 system that evaluates sources, authority, supporting evidence, physical binding, later events, conflicts, gaps, and disclosure rules. It should explain indicators rather than issue an unexplained authenticity score.

Evidence packet. A human-readable and structured export containing selected records, supporting files, history, signatures, and instructions needed for a defined purpose.

Freedom to operate. A legal analysis of whether making or selling a particular product may infringe enforceable patent claims. It is different from asking whether P4 can obtain its own patent.

HNW and UHNW. High net worth and ultra-high net worth. These labels describe people or households with substantial wealth, but thresholds vary by source.

Immutable. Literally incapable of change. P4 should avoid promising absolute immutability. Tamper-evident records, protected retention, independent backups, and visible corrections are more accurate commitments.

Issuer. The identified person or organization that makes and signs a claim or credential, such as a manufacturer, laboratory, appraiser, dealer, service center, or owner.

MFA. Multi-factor authentication. A login requires more than one kind of proof, such as a password plus a security key or phone confirmation.

MVP. Minimum viable product. The smallest secure product that can test whether customers will complete the workflow, use the output, and pay for it.

MVP gate. The measurable evidence required before the company authorizes a full minimum viable product build or the next funding stage.

Merkle root. One cryptographic fingerprint that summarizes a batch of other fingerprints. It can prove that a record belonged to a batch without publishing every private record.

Metadata. Information describing a record, such as its source, date, file type, issuer, status, or relationship to an article.

Multi tenant SaaS. One securely operated software service that supports multiple customer organizations while keeping each customer's information and permissions separated.

NFC. Near-field communication. A short-range wireless chip that compatible phones or readers can scan. A secure NFC element can perform stronger checks than a fixed code, but implementation matters.

Object Lock or WORM storage. Storage controls designed to prevent a file from being overwritten or deleted for a set period. WORM means write once, read many.

Patent priority date. The filing date used to determine which disclosures may count as prior art for claimed subject matter. Old notes can document concept history but do not automatically create a patent filing date.

PCT application. An international patent application process that preserves options to seek patents in selected countries. It is not a worldwide patent.

Persistent identifier. A stable identifier for an article or record that can continue to resolve even when software, vendors, or web domains change.

Physical to digital binding. The evidence connecting a digital record to one particular physical article, using such features as serials, measurements, detailed images, physical fingerprints, secure tags, or expert inspection.

PostgreSQL. A widely used open-source relational database. It is suited to structured records and relationships among assets, people, roles, claims, permissions, and events.

Private and public keys. A matched cryptographic pair. The private key is protected and used to sign or decrypt; the public key is distributed so others can verify a signature or encrypt information for the key holder.

Provenance. The documented source and history of an article or claim, including origin, custody, condition, service, appraisal, transfer, and later corrections.

Provisional patent application. A U.S. filing that can establish an early filing date for adequately described inventions and normally gives the applicant 12 months to file a corresponding nonprovisional application.

QR code. A printed square code read by a camera. It is convenient but can be copied, so it should act as a pointer rather than proof of authenticity by itself.

Revocation. A status change showing that an issuer no longer treats a credential, authority, or key as valid.

SaaS. Software as a service. Customers use software hosted and maintained by the provider, usually through a subscription.

Selective disclosure. Sharing only the fields and evidence needed for a specific purpose instead of exposing an owner's entire collection or full documents.

Source code escrow. A contract under which an independent custodian holds current software code and related materials for release only after specified events, such as prolonged service failure or insolvency.

Springing license. A license that remains inactive during normal operations and becomes usable only after precisely defined trigger events.

Tamper evident. Designed so unauthorized or unexplained changes can be detected. It does not mean a system can never be attacked or changed.

Tenant isolation. Technical controls that prevent one customer or organization from seeing another customer's information.

Threshold key control. A security arrangement requiring several approved people or devices to cooperate before a critical cryptographic key can be used or recovered.

Trade secret. Valuable non-public information protected through reasonable confidentiality and security measures, such as fraud rules, scoring weights, datasets, or issuer-vetting methods.

Verifiable Credential. A W3C data standard for claims that can be digitally signed and checked by another party. Verification identifies the issuer and detects changes; it does not guarantee that the underlying claim is true.

W3C. The World Wide Web Consortium, an international organization that develops open technical standards for the web.

Addendum P4 Stewardship Foundation Development Plan

Purpose. This addendum describes how P4 can combine a commercially accountable operating company with independent safeguards for records intended to remain useful across generations. It is a planning framework for counsel, investors, technical leaders, and future independent directors. It is not a commitment to a particular tax status or legal structure.

Recommended Structure

P4 should begin with a conventional for-profit operating company, referred to here as P4 Technologies. The company would raise capital, employ the team, own the product and proprietary Evidence Integrity Engine, contract with customers, and bear ordinary commercial risk. A separate P4 Stewardship Foundation should be formed only when third-party reliance makes independent continuity useful. The foundation's charter should be narrow: preserve access to essential records and verification functions if the operating company can no longer perform them, maintain continuity standards, and select a qualified successor after objective failure events.

The foundation should not ordinarily operate the consumer product, set commercial prices, direct day-to-day engineering, own unencrypted customer data, or authenticate articles. Its value comes from holding limited continuity assets, reserve funds, escrow rights, and emergency licenses beyond the reach of ordinary changes in company strategy.

Why the Structure Should Develop in Stages

Creating a full foundation before the product is feasible would add cost, governance friction, and possible tax complications without yet protecting a community that depends on P4. Waiting until a crisis would be too late. The practical answer is to design the safeguards during feasibility, place them in contracts and architecture during the pilot, and activate an independent institution when reliance, revenue, or issuer participation crosses agreed thresholds.

Stage	Organization and safeguards	Decision to advance
Stage 0 Feasibility	P4 Technologies conducts the 90-day study. The evidence schema includes portability and successor fields. Counsel maps intellectual property, customer data rights, escrow terms, and possible foundation forms. No separate foundation is required.	Advance when interviews, prototype use, paid commitments, technical feasibility, and legal review justify an MVP.
Stage 1 Pilot MVP	The operating company builds exports in documented formats, redundant backup and restore, a continuity inventory, key-recovery procedures, vendor portability, and draft escrow and springing-license agreements. A small external continuity advisory group reviews the design.	Advance when real households and professionals rely on the records, restore and export tests pass, and commercial demand supports continued operation.

Stage	Organization and safeguards	Decision to advance
Stage 2 Commercial Reliance	Form the foundation with a three-person board and independent majority. Fund a modest reserve. Place current source code, deployment instructions, schemas, and documentation in escrow. Grant a limited springing license and define objective activation events.	Advance when renewal cohorts exist, outside issuers or professional firms depend on verification, and the cost of independent governance is proportionate.
Stage 3 Network Maturity	Expand to five to seven directors. The foundation maintains continuity and issuer standards, conducts succession drills, controls critical recovery rights through multiple custodians, and can qualify more than one commercial operator.	Advance when P4 serves multiple regions or industries, material enterprise integrations exist, or failure would affect a broad community.
Stage 4 Durable Stewardship	Build a reserve or endowment sufficient for essential verification, export, notice, and transition functions. Maintain technology-migration and cryptographic-agility programs. Publish continuity reports and rehearse succession.	Maturity is measured by tested recovery, financial capacity, independent oversight, and the ability to change operators without losing usable evidence.

Continuity Assets and Responsibilities

Operating company	Stewardship foundation
Owns the commercial product, brand licenses, proprietary engine, code improvements, customer contracts, pricing, employment, sales, and ordinary operations.	Holds or controls only the rights and resources needed for continuity after defined failure events.
Maintains production systems, security, support, backups, exports, and compliance during normal operations.	Audits continuity commitments, reserve funding, escrow deposits, key-custody procedures, migration plans, and successor readiness.
May license standards and verification interfaces to partners under ordinary commercial terms.	Maintains stable identifier and minimum export specifications so records can remain interpretable across technology changes.
Retains trade secrets and confidential methods while business is operating.	Receives access to protected materials only when the agreement requires review or when an activation event occurs.
Selects vendors and product direction subject to contractual continuity duties.	Selects a qualified successor operator only after a defined trigger and an independent determination.

Foundation Board and Management

At formation, the foundation should have three voting directors: one person responsible for the founding mission, one independent director with legal or fiduciary experience, and one independent director with security, digital preservation, or infrastructure experience. The independent directors should form a majority. The foundation may initially use a part-time executive director or contracted administrator because its duties are limited.

At maturity, a five- to seven-person board could include experience in consumer or owner interests, estates and fiduciary administration, cybersecurity or digital preservation, manufacturers or credential issuers, appraisal, insurance or resale, and public-interest or standards governance. No single commercial participant should control the board. Directors should have staggered terms, conflict rules, and removal standards. Related-party decisions should require approval by disinterested directors.

Root signing or recovery authority should never rest with one person. Threshold control should require several independent custodians to approve a critical action. Changes to mission, dissolution terms, activation rules, or disposition of continuity assets should require a supermajority. On dissolution, restricted assets should transfer to another qualified stewardship organization rather than revert to insiders.

Activation Events and Successor Operation

A springing license must use events that can be proved, not subjective dissatisfaction. Counsel should tailor the definitions, cure periods, notice procedures, and dispute process. Possible triggers include:

- Bankruptcy, dissolution, or an assignment for the benefit of creditors without an approved continuity plan.
- Permanent cessation of the core record, export, or verification service.
- A prolonged service failure that is not cured within the contractually stated period.
- Failure to maintain or replenish the required continuity reserve, escrow deposits, or recoverable backups after notice and cure.
- An acquisition followed by a declared shutdown or abandonment of the protected service.
- A security or key-control failure that makes the company unable to restore trustworthy verification and export functions.

After a trigger, the foundation should first preserve data and give notice. It should then use escrowed materials and the limited license to restore essential verification and export service itself through a contractor or, preferably, appoint a qualified successor operator. The license should cover only what continuity requires. It should not become a general right to compete with a healthy operating company.

Funding the Foundation

The foundation should not depend on annual goodwill from the operating company. A staged funding formula could combine a small fixed contribution during the commercial pilot, a percentage of designated subscription or credential revenue after scale, enterprise or manufacturer stewardship fees, grants for public-interest standards work, and investment earnings from a restricted reserve. Customer prepayments that fund future service should be accounted for separately from the continuity reserve.

The mature reserve target should be calculated from the cost of maintaining essential verification, notice, export, security, legal, and migration functions for a defined transition period. The plan should

not choose a dollar amount before the architecture, record volume, vendor portability, and successor operating model are known.

Legal Form and Tax Questions

A California nonprofit public benefit corporation is one possible foundation form. Federal tax exemption under section 501(c)(3) would require a genuine charitable or public purpose and safeguards against private inurement or excessive private benefit. [44][45] If the principal purpose later becomes improving conditions across an industry, counsel might instead examine a section 501(c)(6) business league. A public benefit corporation could strengthen the operating company's stated mission but would not by itself protect records if that company failed. The final structure should follow the actual public beneficiaries, funding, control, and activities, not the appeal of a label.

What the ICANN History Does and Does Not Show

The Domain Name System did not begin as an ordinary for-profit invention. Paul Mockapetris described the early DNS design in a 1983 technical document while at the University of Southern California Information Sciences Institute. [41] The work grew within a publicly funded research and government-contract environment. Commercial companies later became important registry and registrar operators, but no single private startup invented the complete domain-name system and then converted itself into ICANN.

ICANN emerged in 1998 through a U.S. government-led transition toward private-sector, globally representative coordination. The Department of Commerce policy called for a new, not-for-profit corporation, and the Department then entered an agreement with ICANN, a California nonprofit corporation. [42][43] ICANN's current articles describe it as a nonprofit public benefit corporation that is not organized for private gain. [44]

The useful parallel for P4 is institutional evolution. Technical functions may begin under one set of sponsors and later require a more neutral steward when many independent parties rely on them. The limit is equally important. P4 would begin as a private commercial service, it would not control a global public namespace, and no government transition is assumed. Its foundation should therefore be smaller, contract-based, and limited to continuity and trust functions justified by actual adoption.

Formation Tests

Management and counsel should review foundation readiness at least annually after the MVP. Formation becomes reasonable when several of the following conditions exist:

- Customers are renewing because they expect records to remain useful for many years.
- Professional firms or manufacturers depend on P4 identifiers, status checks, or exports in their own workflows.
- A service interruption would affect enough outside parties that ordinary contract damages would not provide an adequate remedy.
- The operating company can fund independent governance, escrow, and a meaningful reserve without impairing product viability.
- The software, documentation, data formats, backups, and legal rights are mature enough that a successor could actually operate essential functions.

- Independent directors with the necessary judgment and no disabling conflicts are available.

Recommended Work During the Feasibility Study

The first continuity work is concrete and modest. Add portability and successor requirements to the MVP specification. Ask technical candidates to describe backup restoration, data export, key recovery, vendor substitution, and cryptographic migration. Ask counsel to map customer ownership and license rights, draft an escrow term sheet, define possible activation events, and compare foundation forms. Estimate the cost of essential service after a shutdown. These steps protect the long-term purpose without burdening the 90-day feasibility study with a premature institution.

Addendum P4 Competitor and Partnership Landscape

Purpose. This addendum examines the organizations and product categories cited in the business plan. It identifies what each one proves about market demand, where it overlaps with P4, where P4 remains different, and whether the more practical relationship is competition, cooperation, or both. The central conclusion is not that P4 has no competition. It is that the market consists mainly of strong but partial systems, and no reviewed public offering presently combines the full P4 model in one owner-controlled evidence and continuity platform.

Assessment limits. The analysis is based on publicly available product descriptions, help materials, terms, and company statements reviewed in September 2026. Private product roadmaps, enterprise contracts, security plans, and continuity arrangements are not visible. Therefore, statements about missing capabilities mean that a capability was not identified publicly, not that the organization has proved it does not exist.

Competitive Conclusion

P4 does not enter an empty market. It enters a fragmented ecosystem whose parts increasingly validate the original concept. Brands can establish origin. Laboratories and authenticators can issue specialized opinions. Marketplaces can inspect an item during a sale. Registries can identify lost or stolen property. Collection applications can organize information. Certificate platforms can preserve signed records. Estate-planning platforms can reach families and advisers. The unresolved problem is connecting those separate records into an owner-controlled, cross-category history that evaluates authenticity probability and evidence strength; preserves ownership, title, custody, service, disputes, corrections, and transfers; enables purpose-limited disclosure; and remains portable through organizational change.

That gap makes P4 viable, but it is not a permanent moat. Aura, Arianee, Verisart, a large marketplace, or a coalition of brands could expand into broader evidence management. P4 must therefore win through execution: useful professional workflows, superior evidence structure, portability, careful physical-to-digital binding, longitudinal history, continuity safeguards, and partnerships that make P4 more useful than a closed replacement.

Organization or category	Present relationship to P4	Preferred posture
Aura Blockchain Consortium	Closest strategic analogue for luxury digital product passports and manufacturer-issued lifecycle records.	Partner where possible; monitor as the strongest adjacent expansion threat.
Arianee	Closest infrastructure-platform analogue for interoperable digital product passports.	Integrate or license where useful; do not rebuild commodity passport plumbing merely to appear independent.

Organization or category	Present relationship to P4	Preferred posture
Verisart	Strong overlap in signed certificates, provenance history, transfer, physical links, and independent archives, especially for art.	Potential credential source or technical partner; direct competitor in art and creator-led certification.
Entrupy	Specialized authentication and fraud-detection provider for selected luxury categories.	Treat as an expert evidence issuer and referral partner, while preserving its limited scope.
Chrono24 and eBay	Transaction platforms with authentication, escrow, market data, and large buyer networks.	Use as transaction and evidence sources; avoid building a marketplace during the initial stages.
PSA and GIA	Authoritative category specialists whose certifications strongly affect reliance and value.	Ingest and verify their reports; never imply that P4 replaces their expertise.
Art Loss Register	Specialist due-diligence and lost or stolen property database.	Link or integrate checks; preserve search results and their dates as scoped evidence.
Rolex and other brand programs	Authoritative within one brand and often strongest at manufacture, service, or certified resale.	Complement the brand record before and after brand-controlled events.
Artifcts and generic inventory vaults	Owner-facing documentation, sharing, estate, insurance, and memory preservation.	Differentiate through evidence integrity and professional reliance; explore export or referral interoperability.
Trust and Will	Estate-planning distribution precedent rather than a direct asset-evidence competitor.	Potential channel or integration partner if P4 proves useful in funding and administering estate plans.

CARFAX and Plaid as Business Model Precedents

Why these examples matter. P4 does not need a precedent that duplicates its product. It needs evidence that a commercially valuable company can arrive after an industry and become important by connecting records, institutions, and services that already exist. CARFAX and Plaid illustrate complementary parts of that strategy. Neither replaced the specialized organizations producing the underlying information or services. Each created value by making fragmented systems work together more usefully.

CARFAX provides the asset-history precedent. The automotive industry, government title systems, insurers, repair facilities, auctions, manufacturers, police agencies, and dealers existed long before CARFAX. CARFAX organized reported accident, service, ownership, title, mileage, recall, and related information around a vehicle's standardized identification number. Its public materials state that its reports draw on billions of records from more than 151,000 domestic and international sources. The participating sources remain authoritative for what they report; CARFAX makes their separate records more understandable and commercially useful in one vehicle history. CARFAX also warns that its report may not contain every event and should be used with inspection and other due diligence. That limited-claim approach is directly relevant to P4. [A20]

Plaid provides the integration-platform precedent. Banks, credit unions, payment services, lenders, investment applications, and personal-finance tools can build individual connections, but doing so repeatedly is costly and inconsistent. Plaid supplies a common connectivity layer that lets consumers authorize financial applications to connect with thousands of institutions. Plaid does not need to become every bank or financial application; its network becomes valuable because it allows each participant's specialized service to operate within a larger ecosystem. Plaid publicly reports connectivity to more than 12,000 institutions. [A21]

The combined lesson for P4. P4 can pursue the CARFAX role by assembling a comprehensible evidence history around one physical article and the Plaid role by connecting manufacturers, laboratories, authenticators, appraisers, insurers, registries, marketplaces, service providers, and estate professionals. Those organizations would continue making the claims within their authority. P4 would preserve their source and scope, connect them to the correct article, expose inconsistencies, support controlled disclosure, and keep the evidence useful across transactions and generations. The analogy is strongest as a business model and weakest as a technical shortcut: movable property usually lacks a universal identifier and compulsory reporting system, so P4 must solve physical-to-digital binding, permission, evidence quality, and continuity more deliberately than CARFAX does for VIN-based vehicles.

Partnership implication. P4 should approach established specialists as an amplifier rather than a substitute. An authenticator, laboratory, brand, or registry retains ownership of its conclusion and customer relationship. P4 extends the useful life and context of that conclusion, routes appropriate users back for reinspection or updated service, and makes the specialist's work usable in estate, insurance, custody, transfer, and resale workflows. This is how apparent competitors can become evidence suppliers, distribution partners, and beneficiaries of the network.

Aura Blockchain Consortium

What it does. Aura is a nonprofit consortium established by major luxury groups. It provides private and public blockchain options and digital product passports for participating brands. Aura describes passports that can support origin, authenticity, ownership, lifecycle information, traceability, service, customer engagement, and regulatory compliance. Implementations may use NFC links and can follow an article after sale. [A1][A2]

Overlap with P4. Aura overlaps directly with manufacturer-issued product identity, signed origin information, ownership claims, lifecycle events, product-to-record links, anti-counterfeit goals, and

long-lived digital passports. Its brand membership gives it authority and distribution that a startup cannot manufacture.

P4 differentiation. Aura begins with participating luxury brands and serves their product and customer strategies. P4 begins with the owner and accepts evidence across brands, categories, vintages, estates, insurers, appraisers, dealers, laboratories, and service providers. P4 is designed to document articles that predate digital passports, items from nonparticipating brands, and collections containing unrelated categories. The Evidence Integrity Engine would compare sources and expose conflicts instead of treating one consortium credential as the complete record.

Partnership opportunity and threat. Aura credentials could become high-grade evidence within P4, while P4 could extend their usefulness into estates, insurance, appraisal, inheritance, and cross-brand collection management. Aura becomes a direct threat if it expands from brand-issued passports into owner-controlled cross-brand dossiers and professional workflows. Its nonprofit form and prominent sponsors improve institutional stability, although its public materials reviewed here do not spell out a complete successor plan if the service or a participating brand stops supporting a passport.

Arianee

What it does. Arianee provides digital-product-passport infrastructure, enterprise APIs, identifiers, software tools, and blockchain-based protocol capabilities. It emphasizes interoperability, EU compliance, and avoidance of vendor lock-in. [A3]

Overlap with P4. Arianee can support product identities, passport issuance, ownership or transfer events, brand communication, and portable verification. It is technically closer to P4's issuer and credential layer than a marketplace or inventory application.

P4 differentiation. Arianee primarily supplies infrastructure to organizations issuing product passports. P4 proposes the customer-facing evidence dossier, professional workflows, evidence grades, claim conflicts, document preservation, estate and insurance outputs, and cross-source reasoning. Arianee could provide rails; P4 provides the evidence policy and operating system around the asset.

Partnership opportunity and threat. P4 should evaluate whether Arianee can reduce development time for standards-compatible credentials or manufacturer integrations. The danger is strategic dependence: P4 must retain portable data, its own claim model, and the ability to change infrastructure providers. Arianee becomes a direct competitor if it adds owner-controlled legacy-asset onboarding and the same professional workflow network.

Verisart

What it does. Verisart issues blockchain-anchored certificates for physical and digital works. It verifies creators and issuers, records certificate changes, supports ownership transfer and QR or NFC physical links, and allows an archive to be downloaded and independently checked without Verisart. [A4][A5]

Overlap with P4. Verisart has meaningful overlap with P4's provenance history, issuer identity, digital signatures, physical binding, transfer, tamper evidence, and continuity through portable archives. Among the reviewed companies, it comes closest to demonstrating that some P4 concepts already work commercially.

P4 differentiation. Verisart is concentrated in art, creators, galleries, collectibles, and certificates. P4's proposed scope includes household collections, estates, insurance schedules, appraisals, service histories, custody, disputes, loss events, and multiple external credentials. P4 also proposes an Evidence Integrity Engine that evaluates contradictory evidence and purpose-specific sufficiency rather than relying mainly on certificate status.

Partnership opportunity and threat. P4 could ingest Verisart archives and treat verified creator or issuer certificates as strong evidence. Verisart is also a direct competitor in art and any category where it broadens its physical-item and professional workflows. P4 should study Verisart's patents and archive format during formal patent and freedom-to-operate work.

Entrupy

What it does. Entrupy provides AI-assisted authentication for selected handbags, leather goods, footwear, and apparel, along with return-fraud tools. Each accepted item receives a server-hosted certificate, and Entrupy states that qualifying authentications receive a one-year financial guarantee. It may revoke certificates when fraud, misuse, irregular activity, or other integrity concerns arise. [A6][A7]

Overlap with P4. Entrupy overlaps in item capture, image analysis, counterfeit detection, certificate verification, anomaly detection, and professional resale workflows. Its accumulated image data and category models are valuable proprietary assets.

P4 differentiation. P4 should not initially make category-authentication decisions. It preserves Entrupy's conclusion as a dated, scoped claim and places it beside invoices, manufacturer credentials, service records, ownership history, later inspections, disputes, and transfers. P4 also spans categories Entrupy does not cover and remains useful even when no authenticator can reach a conclusion.

Partnership opportunity and threat. Entrupy is a natural issuer and API partner. P4 could route appropriate articles for authentication and preserve the result, certificate status, guarantee period, and later revocation. Entrupy becomes a broader competitor if it expands its certificate into a permanent cross-category owner dossier. P4 should not imitate its model or imply that P4's evidence record carries Entrupy's authentication authority.

Chrono24 and eBay

What they do. Chrono24 operates a global luxury-watch marketplace with escrow, buyer protection, a watch-collection tool, market information, and a certified program. eBay provides transaction-time authentication for eligible watches, handbags, jewelry, sneakers, and collectibles. [A8][A9]

Overlap with P4. Both platforms collect identity, condition, price, seller, transaction, shipping, and authentication evidence at commercially important moments. They can influence buyer trust and have distribution advantages that P4 will not match early.

P4 differentiation. Marketplace evidence is normally tied to a listing or transaction. P4's record begins before a sale and continues after it, including acquisition documents, insurance, appraisal, storage, service, custody, estate instructions, loss, gifting, inheritance, and later transactions on any platform. P4 should remain neutral among marketplaces and should not hold transaction funds during the initial stages.

Partnership opportunity and threat. Marketplace receipts, authentication reports, photographs, sale results, and transfer events should enter P4 with the marketplace identified as the source. P4 can produce cleaner consignment or sale packets in return. A marketplace becomes a direct threat if it converts its collection tool into a portable cross-platform dossier, but marketplace incentives may favor keeping owners and data inside its own transaction environment.

PSA and GIA

What they do. PSA authenticates and grades trading cards, autographs, tickets, photographs, and memorabilia, assigns certification numbers, offers online certificate checks, and provides guarantees subject to its terms. PSA warns that a valid certification number alone does not eliminate the risk of a counterfeit holder or copied label. GIA examines diamonds and gemstones and issues laboratory reports containing measured and graded characteristics. [A10][A11][A12]

Overlap with P4. Both create high-authority category evidence, item identifiers, expert conclusions, and verification records. Their recognized standards can materially affect value and transaction confidence.

P4 differentiation. P4 does not replace grading laboratories. It preserves their report, who submitted or reviewed it, the physical characteristics used to match it to the article, and events occurring after certification. P4 can also flag a report number reused for incompatible articles or a grading report that no longer matches the object's current condition.

Partnership opportunity and threat. PSA and GIA should be treated as authoritative issuers. P4 could link to their verification services, preserve checks, and help owners assemble evidence before submission, insurance, transfer, or sale. Their category specialization makes partnership more logical than confrontation. They become broader competitors only if they build cross-category owner and professional evidence systems.

Art Loss Register

What it does. The Art Loss Register maintains a private database of stolen, missing, disputed, and claimed art, antiques, and collectibles. It provides search, registration, due-diligence, and recovery services to owners, insurers, police, and the art trade. [A13]

Overlap with P4. It overlaps with loss records, dispute status, due diligence, provenance checks, and recovery workflows. Its value comes from specialized data and relationships rather than from being a general household inventory.

P4 differentiation and partnership. P4 should preserve that an Art Loss Register search occurred, when it occurred, what item description was searched, and the scoped result. It should never copy or declare itself a substitute for the underlying database. A referral, search integration, or structured result credential would make both services stronger.

Brand Programs Including Rolex and Breitling

What they do. Rolex Certified Pre-Owned uses authorized retailers, brand-backed authenticity review, a seal, and a two-year international guarantee for qualifying watches. Breitling has offered blockchain-linked digital passports for its watches. Other brands provide their own certificates, service histories, registrations, warranties, and product passports. [A14][A15]

Overlap with P4. A manufacturer or its authorized network can make the strongest origin, model, production, service, and certified-resale statements for its own products. P4 cannot manufacture that authority.

P4 differentiation and partnership. A brand account is one island. P4 gives the owner one private record across Rolex, Breitling, jewelry, art, handbags, antiques, and other property. It can preserve a brand credential while adding evidence outside the brand's scope, including prior ownership, appraisals, insurance, non-authorized service, estate transfers, and later disputes. P4 should invite brands to issue credentials through or into P4 and allow the brand record to remain authoritative within its stated scope.

Artifcts and General Inventory Platforms

What they do. Artifcts helps households document objects, photographs, stories, value, location, estate or insurance information, and intended disposition. It supports private sharing, professional accounts, QR stickers, and downloadable or exportable information. It publishes specific privacy and encryption practices. [A16][A17] Generic inventory and digital-vault products provide related storage and organization functions.

Overlap with P4. This category overlaps strongly in owner capture, household organization, legacy, estate, insurance, sharing, and professional introductions. It may be the closest competitor for the household's attention and willingness to complete records.

P4 differentiation. P4 must offer more than a prettier inventory. Its case depends on claim-level source attribution, evidence grades, protected originals, signed attestations, visible supersession, issuer status, physical binding, conflict detection, purpose-limited disclosure, and verification instructions. Artifcts may be better at memories and storytelling; P4 should not dilute its evidence mission trying to win that contest.

Partnership opportunity and threat. With permission, an Artifcts or inventory export could seed a P4 evidence record, and P4 could return a verification packet for estate or insurance use. The competitive threat rises if a strong household platform adds reliable professional attestations, issuer credentials, append-only history, and institutional continuity. P4 must validate that customers will pay for the stronger evidence layer rather than assume technical sophistication creates demand.

Trust and Will

What it does. Trust and Will provides online estate-planning documents and an adviser platform. It reports serving more than one million families and working with thousands of advisers. Its platform demonstrates that guided digital workflows and professional distribution can gain adoption in a trust-sensitive field. [A18][A19]

Relationship to P4. Trust and Will is not presently a direct substitute for an asset evidence passport. Its relevance is distribution and workflow validation. Estate documents often identify classes of property without supplying the evidence an executor, trustee, insurer, appraiser, or heir will later need.

Partnership opportunity and threat. P4 could provide a verified tangible-property schedule, successor-access instructions, or funding-status workflow linked to an estate plan. Trust and Will could become a competitor if it builds a sophisticated movable-property evidence product, but integrating a specialist

may be faster and less risky for it than developing authentication, provenance, and category knowledge internally.

Standards and Infrastructure Are Complements

W3C Verifiable Credentials, GS1 Digital Link, C2PA content credentials, SCITT supply-chain transparency architecture, cloud object-retention services, identity providers, and secure NFC vendors are not ordinary competitors. They are building blocks or interoperability standards. P4 should adopt them where they improve portability, verification, or physical binding. Proprietary value should reside in evidence interpretation, workflows, data quality, category rules, fraud learning, and trusted relationships, not in renaming an open standard.

The Most Credible Future Entrants

Entrant	Why it could surpass P4	P4 response now
Luxury consortium or DPP platform	Existing brands, issuer authority, product data, capital, and millions of passports.	Own the cross-brand owner and professional workflow; integrate early; protect the Evidence Integrity Engine and portability layer.
Marketplace	Buyer traffic, transaction data, authentication operations, payments, and immediate economic incentives.	Remain marketplace-neutral and valuable before, between, and after transactions.
Authentication or grading company	Trusted category expertise, proprietary reference data, recognized certificates, and existing professional users.	Treat specialist conclusions as high-value inputs while solving cross-category history, privacy, estate, and continuity.
Inventory or estate platform	Existing household relationships, guided capture, adviser channels, and lower-friction customer acquisition.	Prove that evidence-grade records and professional reliance justify integration or a premium product.
Large horizontal technology company	Capital, identity systems, cloud infrastructure, distribution, and rapid copying capacity.	Build domain knowledge, consented longitudinal data, issuer relationships, defensible methods, and contractual channel integration before the category is obvious.

Partnership Rules

- Preserve source authority. P4 must show that the partner, not P4, made the authentication, grading, registry, or manufacturer claim.
- Keep the record portable. A partner integration must not prevent the owner from exporting a useful evidence packet or changing providers.

- Avoid exclusive dependence. P4 should support more than one authenticator, marketplace, tag vendor, cloud vendor, and credential format where economically practical.
- Use scoped contracts. Agreements should define data ownership, permitted use, issuer status, revocation, service levels, incident notice, termination exports, and continuity obligations.
- Do not surrender the engine. P4 may share results and explanations, but its non-public fraud rules, scoring logic, issuer-vetting methods, and accumulated learning should remain controlled.
- Measure the commercial benefit. Integrations should reduce capture cost, improve evidence strength, open distribution, or increase retention. Prestige alone is not a business case.

Recommended Market Position

P4 should describe itself as the owner-controlled evidence and continuity layer connecting specialized authorities. That position makes room for brands, laboratories, authenticators, marketplaces, appraisers, insurers, attorneys, fiduciaries, and registries to remain authoritative in their own fields. P4's job is to preserve and explain their evidence across the article's life, identify gaps and conflicts, control disclosure, and keep the resulting record usable through transfer and institutional change.

The viable project thesis is therefore not that competitors are weak. Several are exceptionally strong. The thesis is that their strength is specialized and fragmented. P4 becomes valuable by connecting those strong but partial systems without falsely claiming to replace them. If pilot customers do not value that connection enough to complete records and pay, the company should narrow or stop. If they do, the partner-first model can turn much of the apparent competition into distribution, evidence supply, and network value.

Sources for This Addendum

[A1] Aura Blockchain Consortium, Digital Product Passport overview. <https://auraconsortium.com/insight/the-digital-product-passport-a-new-era-of-luxury-unveiled>

[A2] Aura Blockchain Consortium, Solutions. <https://auraconsortium.com/solutions>

[A3] Arianee, Enterprise APIs and Digital Product Passport platform. <https://www.arianee.com/en/platform/api>

[A4] Verisart, How blockchain certificates work. <https://help.verisart.com/en/articles/5050610-how-do-blockchain-certificates-work>

[A5] Verisart, Certificate status and downloadable archive. <https://help.verisart.com/en/articles/4568835-what-does-certificate-status-mean>

[A6] Entrupy, Authentication Certificate. <https://www.entrupy.com/search-certificate/>

[A7] Entrupy, Financial Guarantee and Terms of Service. <https://www.entrupy.com/guarantee/> and <https://www.entrupy.com/terms-of-service/>

[A8] Chrono24, Company and services. <https://about.chrono24.com/>

[A9] eBay, Authenticity Guarantee. <https://www.ebay.com/authenticity-guarantee/>

[A10] PSA, About PSA. <https://www.psacard.com/info/about-psa>

[A11] PSA, Certificate Verification. <https://www.psacard.com/cert>

[A12] Gemological Institute of America, Diamond Grading Reports. <https://www.gia.edu/analysis-grading-sample-report-diamond>

[A13] Art Loss Register, Search, register, and recovery services. <https://www.artloss.com/>

[A14] Rolex, Certified Pre-Owned Programme. <https://www.rolex.com/buying-a-rolex/rolex-certified-pre-owned>

[A15] Breitling, Digital Passport. <https://www.breitling.com/us-en/blockchain/>

[A16] Artifcts, Product and use cases. <https://artifcts.com/>

[A17] Artifcts, Privacy and security practices. <https://artifcts.com/security-matters>

[A18] Trust and Will, Adviser platform. <https://trustandwill.com/advisors/>

[A19] Trust and Will, Company information. <https://trustandwill.com/press>

[A20] CARFAX, Vehicle History Reports and data-source description. <https://www.carfax.com/vehicle-history-reports/>

[A21] Plaid, Open-finance platform and institution connectivity. <https://plaid.com/>