Credentials Before the Standard: Pricing Network Effects in Verifiable-Identity Platforms

An M&A framework for separating accepted trust, option value and standards risk in three-sided credential networks

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

Verifiable-identity platforms coordinate three economically distinct groups: credential issuers, holders and verifiers. Each group can make the network more useful to the others. A university credential attracts employers only when the employer accepts it; employer acceptance makes the credential more useful to graduates; holder demand can encourage more institutions to issue compatible evidence. This creates a network-effects thesis. It does not create a valuation answer. Before standards, implementation profiles and legal reliance converge, a platform can accumulate integrations, wallets and issued credentials while producing little transferable acceptance or durable contribution.

This paper develops a Credential Network Pricing Framework for boards, investors and acquirers. It treats network value as accepted, repeatable and economically productive trust rather than participant counts. The framework maps issuer quality, holder liquidity, verifier acceptance, trust infrastructure, workflow conversion, interoperability, liability and standards exposure. It translates these elements into an acceptance graph, cohort metrics, contribution economics, scenario valuation, deal protections and a post-completion operating plan.

Primary sources show meaningful convergence and material residual uncertainty. The W3C Verifiable Credentials Data Model 2.0 became a Recommendation in May 2025. OpenID for Verifiable Credential Issuance 1.0 became final in September 2025. NIST Special Publication 800-63C-4 defines federation and subscriber-controlled-wallet requirements. The European Digital Identity Wallet architecture, implementing regulations and reference implementation provide a large-scale legal and technical profile. World Bank ID4D guidance explains the roles, public-interest constraints and possible charging models of identity providers and relying parties. These sources establish implementable building blocks. They also show that technical compatibility, assurance, legal recognition and commercial acceptance remain separate tests.

A wholly hypothetical acquisition case applies the framework to a credential-network company serving education, employment and financial-services workflows. The case begins with 3.2 million issued credentials, 1.4 million active holders, 180 contracted verifiers and 4.8 million annual presentation attempts. It prices the company from accepted presentations, verifier retention, cross-workflow reuse, contribution margin and migration cost. Every amount, rate, multiple and operating assumption is illustrative management input. It is not observed company data, a market forecast, a valuation opinion or an offer of financing.

The central conclusion is that pre-standard network effects should be priced through evidence-weighted cohorts. Issuer and verifier counts earn value only when governed trust relationships create

accepted workflows. Holder scale earns value when credentials remain active, portable and repeatedly useful. Proprietary extensions can improve product performance and create future migration cost. Open standards can reduce technical lock-in while increasing the importance of distribution, assurance, workflow design and liability allocation. Acquirers should separate current earnings, validated network uplift, standards option value and remediation exposure, then pay each component through the instrument best suited to its evidence.

JEL Classification: G24, G34, L14, L15, L86, O31, O33

Keywords: verifiable credentials, digital identity, network effects, platform valuation, M&A, interoperability, digital wallets, issuer networks, verifier adoption, standards risk

This paper is an educational and structural analysis prepared for research purposes. It is not investment advice, an offer, or a solicitation. It contains no client information.

1. DEFINE THE ACQUISITION QUESTION

The acquisition question is whether the target owns a transferable trust network or a collection of integrations that may need to be rebuilt. A network can have issuers, holders and verifiers in a database without creating reciprocal economic benefit. The buyer needs evidence that a credential issued by an authorised party reaches an active holder, satisfies a verifier's policy and completes a valuable workflow.

This paper uses network effects in a disciplined sense. The presence of one participant group must improve utility, conversion, cost or retention for another group. The benefit should be measurable and capable of surviving ownership change, standards migration and customer renewal.

The decision should therefore begin with accepted workflow outcomes. It should then trace backwards through presentation, wallet, issuance, proofing and source authority. That sequence prevents registrations, credentials and logos from becoming valuation substitutes for economic activity.

Table 1. Credential-network value layers and acquisition evidence

Value layer	Minimum evidence	Principal risk	Transaction treatment
Issuer supply	Authorised issuers, live schemas and governed lifecycle	Nominal issuers without active issuance	Value active credential cohorts only
Holder liquidity	Active wallets and usable credentials	Downloads or dormant credentials	Cohort retention and reuse test
Verifier demand	Production integrations and accepted decisions	Contracted logos without traffic	Price accepted workflows
Trust infrastructure	Keys, registries, status and assurance mapping	Hidden dependence on one operator	Condition and remediation reserve
Interoperability	Multi-party production tests on named profiles	Standards claim without portability	Discount migration exposure
Economics	Revenue, contribution and renewal by workflow	Subsidised volume and negative marginal cost	Underwrite verified contribution

Each layer needs a stable definition, an evidence source and a transferability test.

2. MODEL A THREE-SIDED NETWORK

Verifiable-identity platforms differ from simple two-sided marketplaces because the holder mediates the relationship between issuer and verifier. The issuer creates a claim. The holder

stores or controls it and chooses when to present it. The verifier determines whether the claim is acceptable for a specific purpose. A platform may also provide wallets, trust registries, status services, orchestration and evidence retention.

Each side has a different adoption decision. Issuers consider authority, issuance cost, reach and governance. Holders consider utility, privacy, recovery and effort. Verifiers consider legal reliance, assurance, integration cost, fraud, conversion and liability. Price can sit on any side and may be zero for one participant group.

The valuation model should preserve these separate decisions. A blended user count hides the direction and strength of cross-group effects. It can also hide a subsidised side whose participation does not continue after an acquisition.

3. SEPARATE PARTICIPANT COUNTS FROM NETWORK EFFECTS

A participant count is a stock. A network effect is a change in utility caused by participation elsewhere in the system. Ten additional issuers can strengthen the network when they supply credentials demanded by current verifiers. They can weaken unit economics when they introduce low-use schemas, support obligations and trust-review cost.

The buyer should test incremental effects. When a verifier is added, do more holders present credentials? Do existing issuers see more accepted use? Does verifier acquisition become easier? When an issuer is added, does acceptance expand or does fragmentation increase?

Regression, cohort and event-study methods can help when data quality permits. A practical first test compares matched cohorts before and after a new high-value issuer or verifier goes live. The analysis should control for marketing, mandatory use, seasonality and customer-specific rollout.

4. MAP THE ACCEPTANCE GRAPH

The acceptance graph connects credential types, issuers, holders, wallets, verifiers and workflows. An edge exists only when production evidence shows that a verifier accepted a named credential under a defined policy. A contract, sandbox test or technical connection should have a separate status.

The graph should include version, jurisdiction, assurance, status method, transaction volume, conversion and economic contribution. It should also identify which participant introduced the relationship and which party controls renewal.

Graph structure matters. A dense cluster can indicate strong reuse across several workflows. A hub-and-spoke pattern can reveal dependence on one national identity rail, one anchor issuer or one large verifier. Fragmented islands can indicate that the apparent network is several bespoke projects sharing a brand.

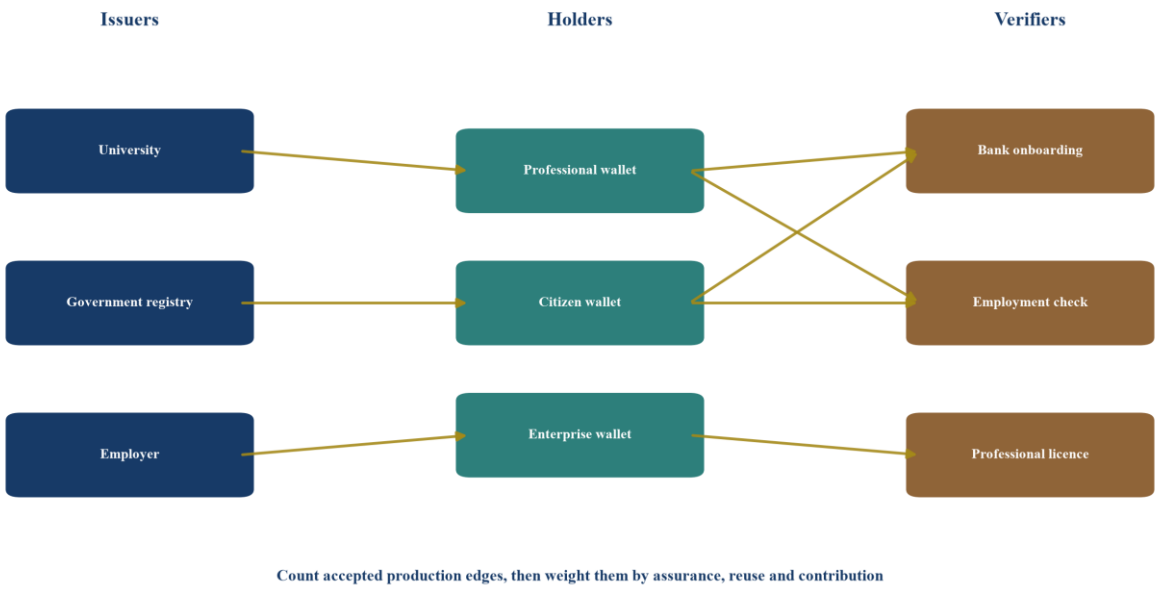

Figure 1. Acceptance graph for a three-sided credential network

Economic edges exist only where production credentials complete accepted workflows.

5. DISTINGUISH DIRECT AND CROSS-SIDE EFFECTS

Direct effects arise among participants of the same type. A verifier may benefit when common tooling, shared policy libraries and community testing expand. It may also face congestion, common-mode risk or weaker differentiation. Issuers can benefit from shared schemas and wallet reach while competing for attention and trust.

Cross-side effects are more central. More high-quality issuers can increase holder utility and verifier coverage. More active holders can improve the case for verifier integration. More accepting verifiers can increase credential value and issuer willingness to participate.

The diligence model should assign a direction, mechanism, lag and evidence level to each proposed effect. Statements such as every new participant makes the network stronger are too broad for valuation. The effect can be positive, negligible or negative depending on the participant and workflow.

6. START WITH VERIFIER ACCEPTANCE

Verifier acceptance is the hardest evidence and often the strongest economic anchor. The verifier bears integration cost and may retain responsibility for the regulated decision. Its production use demonstrates that the credential satisfies a real policy, service and risk threshold.

Acceptance should be measured at workflow level. A bank can accept one government credential for low-risk access and reject it for customer due diligence. An employer can accept a qualification credential while requiring separate identity evidence. A platform logo on a customer page does not define this boundary.

The buyer should obtain policy configurations, transaction logs, exception outcomes, customer attestations and renewal data. Revenue should reconcile to accepted presentations or contracted platform value. Pilot and sandbox traffic should remain separate.

7. GRADE ISSUER QUALITY

Issuer quality combines authority, assurance, data provenance, operational controls, lifecycle management and demand for the credential. A government registry, regulated professional body, university and employer carry different authority for different claims.

The buyer should score each issuer by active credentials, accepted workflows, status performance, key governance, error correction, renewal and contractual durability. One high-authority issuer can create more network utility than many self-attested or weakly governed sources.

Issuer concentration requires context. Dependence on a national rail can strengthen trust and lower proofing cost. It can also create political, contractual and change-of-control exposure. The valuation should reflect both utility and control.

8. MEASURE HOLDER LIQUIDITY

Holder liquidity describes whether people or organisations possess usable credentials and can present them when demanded. It is stronger than wallet downloads and broader than monthly logins. A liquid holder base has active credentials, functioning recovery, available devices and repeated opportunities to transact.

The core cohort follows issuance through activation, first presentation, first acceptance, independent reuse and retention. It should distinguish mandatory from voluntary use, same-verifier reuse from cross-verifier reuse and single-purpose credentials from broad identity evidence.

Dormant credentials create service cost and little current network value. They may retain option value when an anchor verifier is expected to launch. That option should be priced separately from proven activity.

9. DEFINE QUALIFIED REUSE

Qualified reuse occurs when an active credential supports a separate accepted workflow after the initial transaction. A second presentation inside one onboarding session should not automatically count. The definition can require a new time, product, verifier or sector depending on the thesis.

Cross-verifier reuse is strong evidence of portability. Cross-sector reuse is stronger when legal and semantic requirements differ. Same-verifier repeat use can still create value through lower authentication cost and customer retention.

The data model should capture credential, holder, verifier, workflow, result, status and timestamp while respecting privacy. The buyer should confirm that reported reuse is not created by retries, batch processing or test traffic.

10. TREAT STANDARDS AS LAYERED

Standardisation occurs at several layers: data model, credential format, issuance protocol, presentation protocol, cryptographic profile, semantic schema, status method, trust registry and legal reliance. Convergence at one layer does not resolve the others.

W3C Verifiable Credentials Data Model 2.0 defines a common model for issuer, holder, subject, claims and proof. OpenID4VCI 1.0 specifies credential issuance. NIST SP 800-63C-4 provides

requirements for federation and subscriber-controlled wallets. The EUDI Wallet architecture profiles roles and components for a specific legal ecosystem.

The standards ledger should record version, maturity, customer dependency, proprietary extension, migration path and expected support period. This turns an abstract standards risk into a costed operating exposure.

11. PRICE PROTOCOL MATURITY

A final specification reduces one category of change risk. It does not establish universal implementation, conformance, certification or customer acceptance. A technically mature protocol can sit inside a commercially immature ecosystem.

The buyer should examine how much of the target's code follows the published profile, how much depends on drafts and how much uses proprietary behaviour. Production interoperability tests should involve independent counterparties rather than the target's own demo components.

Protocol maturity can lower future integration cost and broaden addressable demand. It can also reduce proprietary lock-in and place pressure on verification fees. The valuation model should reflect both effects.

12. PRICE SEMANTIC INTEROPERABILITY

Two credentials can use compatible envelopes and carry attributes with different meaning. Employment status may reflect payroll, contract, licence or self-declaration. Qualification levels and company authority can differ across jurisdictions.

Semantic governance requires schemas, definitions, source authority, versioning and use-case policy. The verifier needs to know what a claim means and what it does not mean. A generic verified label can conceal a material decision gap.

The buyer should value credential types with clear semantics, authoritative sources and broad verifier acceptance. Custom schemas tied to one client may generate revenue and impose maintenance cost. They belong in customer economics rather than network breadth.

13. PRICE TRUST-FRAMEWORK DEPENDENCE

Trust frameworks determine who can issue, hold, verify and rely on credentials. They can include certification, registries, contracts, audit and redress. Technical verification proves integrity and origin. It does not decide whether an issuer is authorised for the transaction.

The European framework uses wallet certification, issuer trust and relying-party registration. NIST requires trust agreements for federation contexts. National systems can depend on government designation and local service terms. Commercial consortiums can rely on contractual membership.

The buyer should map which trust frameworks support each revenue stream. It should test change-of-control, geographic scope, revocation, audit and exit. Value that depends on non-transferable designation requires transaction conditions or contingent consideration.

14. TEST LEGAL ACCEPTANCE SEPARATELY

Legal acceptance can be mandatory, permitted or uncertain. It can vary by credential, sector, jurisdiction and transaction risk. The same technical presentation can receive different treatment in banking, employment, healthcare and public services.

The regulatory map should identify decision owner, legal basis, assurance, recordkeeping, privacy, status, electronic-signature effect and redress. Counsel should confirm the position at signing and closing.

Valuation credit should follow the narrowest evidence. A cross-border standard can create technical option value. Local legal recognition and verifier policy determine current revenue. The model should avoid converting a global technical addressable market into near-term accepted volume.

Table 2. Standards and acceptance risk map

Layer	Evidence of maturity	Residual exposure	Valuation response
Data model	Published recommendation and production implementation	Divergent credential formats or extensions	Credit common model; cost adapters
Issuance	Final protocol and independent conformance tests	Customer-specific profiles and legacy APIs	Value reusable connectors
Presentation	Multi-wallet and multi-verifier tests	Device, browser and transport differences	Apply migration reserve
Semantics	Governed schemas and authoritative sources	Same label with different meaning	Value accepted schema cohorts
Trust	Registry, certification, audit and enforceable contracts	Non-transferable status or local restriction	Condition or contingent value
Legal reliance	Written rule and production policy	Sector and jurisdiction differences	Price only current accepted scope

The table separates technical compatibility from governed reliance.

15. EVALUATE OPEN STANDARDS AND DEFENSIBILITY

Open standards can expand the ecosystem by lowering integration and switching barriers. They can also weaken a moat based solely on proprietary interfaces. Defensibility then moves toward trusted distribution, workflow embedding, fraud intelligence, assurance, policy tooling, service quality and contractual position.

The buyer should ask which capabilities become commodities after convergence. Basic issuance and verification may face price pressure. Credential-specific data access, regulated workflow orchestration and evidence operations can remain differentiated.

The target should demonstrate why customers stay when credentials can move. Retention based on service quality and embedded decision workflows can be durable. Retention based on blocked export can attract regulatory and customer resistance.

16. IDENTIFY SINGLE-HOMING AND MULTI-HOMING

Participants may single-home on one platform or use several. An issuer can publish credentials through multiple wallets. A verifier can accept several formats and trust frameworks. Holders can maintain several wallets. Multi-homing weakens exclusivity and can strengthen overall adoption.

The buyer should measure exclusivity at workflow level. A verifier may integrate one orchestration provider while accepting credentials from many issuers. An issuer may use one platform because integration and governance cost make parallel operation unattractive.

Switching and multi-homing costs should be decomposed into technical migration, policy reapproval, certification, data portability, holder communication and operational retraining. Contractual restrictions should be distinguished from product advantage.

17. FIND THE CRITICAL MASS THRESHOLD

Critical mass is the participation level at which enough useful interactions occur to sustain adoption. It is not a universal count. A professional-licensing network may need a small number of high-authority issuers and regulated employers. A general consumer wallet may need broad verifier coverage.

The target should identify the smallest viable cluster for each workflow. The cluster includes required credential types, available holders, accepting verifiers and trust infrastructure. Contribution should cover ongoing support and governance.

The acquirer should test whether each cluster survives the loss of its largest participant. A cluster that collapses after one contract ends has anchor dependence rather than self-sustaining network economics.

18. MEASURE LOCAL DENSITY BEFORE GLOBAL BREADTH

Network value often develops through dense local clusters. A credential accepted by many employers in one labour market may create more utility than a globally portable credential accepted by few organisations. Density improves discovery, support and repeat use.

The acceptance graph should calculate active edges per credential and per workflow. It should show concentration, geographic coverage and cross-cluster bridges. Growth plans should identify which new participant closes a valuable gap.

The buyer should resist headline claims based on countries or integrations. Geographic breadth can add legal and support complexity. Dense, profitable clusters can fund later expansion and deserve separate valuation.

19. TRACK CONVERSION THROUGH THE NETWORK FUNNEL

The funnel begins with addressable holders and ends with accepted workflow completion. Intermediate stages include eligible credentials, active wallets, presentation requests, holder consent, cryptographic verification, policy acceptance and business completion.

Drop-off should be attributed to a specific cause: missing credential, wallet failure, user refusal, status failure, policy mismatch, verifier error or downstream rejection. This identifies whether growth requires product work, participant acquisition or regulatory change.

Reported presentation success can overstate value when the business workflow later fails. Revenue and retention should be reconciled to the final accepted outcome that the customer purchased.

20. BUILD CREDENTIAL-LEVEL COHORTS

Credential-level cohorts show how supply matures. For each issuance month and credential type, the buyer should measure activation, first acceptance, reuse, status failure, refresh, revocation and support cost.

A high-volume credential can have low utility when issued pre-emptively. A smaller cohort can be valuable when tied to frequent high-value workflows. Cohorts should be segmented by issuer and profile version.

Migration risk is visible when older cohorts use deprecated formats or keys. The model should cost reissuance, holder communication and verifier updates. It should avoid assuming every historical credential converts to the future standard.

21. BUILD VERIFIER-LEVEL COHORTS

Verifier cohorts should begin when production acceptance starts. The buyer should measure time to launch, integration cost, accepted volume, workflow expansion, renewal, support, exception handling and contribution.

Early verifiers can require bespoke work and receive discounts. Later cohorts should show shorter implementation and higher repeatability if the platform is maturing. A falling deployment cost is evidence of productisation.

Verifier retention should be assessed against transaction cycles. A university recruitment credential may be seasonal. A low monthly figure can still represent strong annual renewal. The unit of analysis should match the workflow.

22. RECONCILE CONTRACTED AND ACTIVE VERIFIERS

Contracted verifiers include customers in procurement, integration, pilot, production and dormant states. Only production customers with accepted activity demonstrate current network demand. Pipeline retains option value and requires probability weighting.

The data room should reconcile CRM, contracts, implementation records, transaction logs, invoices and renewals. Definitions should be stable across board reporting and diligence.

The buyer should identify verifier activation time and abandonment. A large signed backlog can indicate demand and implementation bottlenecks. Consideration tied to production acceptance can align value with delivery.

23. ANALYSE PRICING BY PARTICIPANT SIDE

Identity networks can charge issuers, verifiers, wallet providers, holders or sponsors. World Bank ID4D guidance recognises relying-party fees and warns that excessive charges can suppress demand and exclusion. Public-interest and regulatory constraints can limit pricing freedom.

The platform should disclose list, contracted and realised price by service. Free issuance can seed credential supply. Free holder access can support inclusion. Verifier fees can reflect avoided proofing cost, fraud reduction or conversion.

The buyer should test incidence. A nominal verifier fee can be passed to users or suppliers. A sponsor can fund the network. Revenue durability depends on who receives measurable benefit and who has legal or commercial ability to pay.

24. PRICE BELOW THE PARTICIPATION CEILING

In a multi-sided network, the optimal price on one side can be below cost when participation creates value elsewhere. The subsidy should have a defined purpose, duration and evidence of cross-side uplift.

The buyer should identify the participation ceiling for each side. Verifier price cannot exceed avoided cost and incremental value over viable alternatives. Issuer price cannot exceed distribution and workflow benefit after governance cost. Holder charges can reduce inclusion and adoption.

Scenario analysis should show volume and contribution under price changes. A network whose growth depends on permanent discounts without cross-side monetisation may have weak economics despite strong activity.

25. BUILD CONTRIBUTION ECONOMICS BY ACCEPTED PRESENTATION

Gross revenue should be reconciled to accepted presentations, subscriptions, implementation and managed services. Variable cost includes trust checks, status services, cloud, fraud, support, wallet operations, third-party data and payment fees.

Contribution per accepted presentation can improve with scale when fixed connectors and policy work are reused. It can deteriorate when new jurisdictions, schemas and exceptions add complexity. The model should therefore track cost by workflow and cohort.

The buyer should separate current contribution from expected operating leverage. Standard convergence can lower marginal integration cost and reduce pricing. The net effect belongs in scenarios rather than a single margin assumption.

26. ALLOCATE TRUST AND LIABILITY COST

Network value depends on responsibility when a credential is wrong, stale, compromised or misused. Issuers, wallets, trust registries, the platform and verifiers control different failure points.

The unit-economics model should include insurance, audit, certification, complaints, fraud losses, remediation and reserves. A platform can report positive software margin while customers absorb identity losses. That allocation may change after acquisition or regulation.

Contracts should map duties and caps by event. The valuation should test whether historic loss experience is representative and whether a broader verifier base creates correlated exposure.

27. MODEL STANDARDS MIGRATION COST

Migration cost includes protocol changes, credential reissuance, wallet updates, verifier integration, policy approval, conformance testing, certification, support and parallel operation. The cost can sit with the platform or be shared with participants.

The migration inventory should map every credential and verifier to the current profile and target profile. It should identify hard dependencies, unsupported devices and contractual change rights.

The buyer should set a cost, schedule and contingency for each cohort. A broad historical credential base can increase headline scale and create a large migration liability. Consideration should reflect the net position.

28. TEST BACKWARD COMPATIBILITY

Backward compatibility allows old credentials or integrations to remain usable while a new profile is adopted. It can protect holder utility and customer continuity. It can also prolong weak algorithms, fragmented semantics and operational complexity.

The target should state its support policy, sunset process and verifier behaviour. The buyer should test whether old credentials can be validated securely and whether reissuance is required for stronger holder binding or assurance.

Parallel profiles need monitoring, status and incident coverage. Their cost should be visible. A clean migration path can be a differentiator when customers face ecosystem-wide change.

29. DISTINGUISH OPTION VALUE FROM CURRENT VALUE

Pre-standard platforms can hold valuable options: relationships with anchor issuers, reusable connectors, policy knowledge, certification progress and a holder base capable of migration. These assets can accelerate entry into a converged market.

Option value should have a trigger, expiry, cost and probability. An unsigned memorandum or untested standard should receive less weight than a funded implementation with named milestones. The model should avoid placing uncertain upside into current recurring revenue.

Deal structure can preserve the option without paying full value at closing. Milestone consideration, earn-outs, seller rollover and staged acquisition can link payment to standards adoption and accepted activity.

30. USE AN EVIDENCE-WEIGHTED NETWORK SCORE

An evidence-weighted score combines issuer quality, holder liquidity, verifier acceptance, reuse, contribution, interoperability, trust and migration readiness. Each component should derive from measured data and a documented scale.

Weights should reflect the thesis. A buyer seeking regulated financial-services workflows can place greater weight on assurance, verifier policy and liability. A workforce platform can emphasise issuer authority, employer density and portability.

The score is a decision aid and should not replace valuation. It exposes weak assumptions, supports sensitivity analysis and links diligence to deal protection.

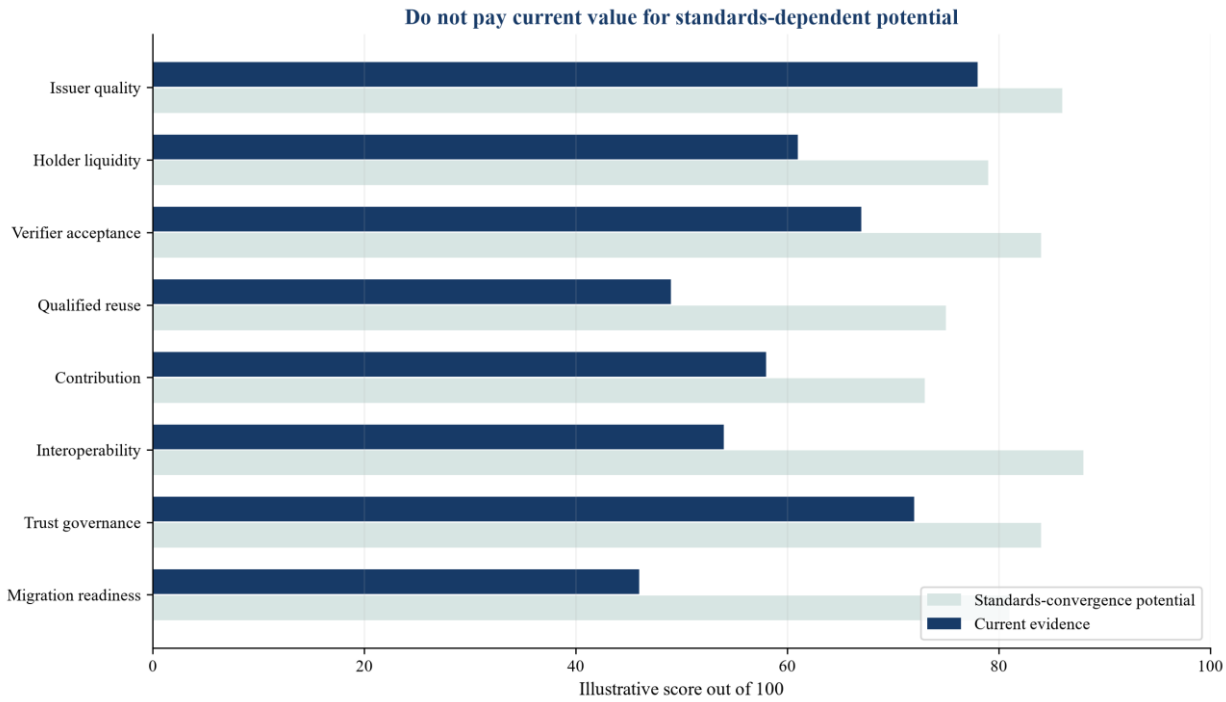

Figure 2. Evidence-weighted network score

The illustrative profile distinguishes current strength from standards-dependent potential.

31. CONSTRUCT THE HYPOTHETICAL CASE

The hypothetical target supplies credentials for education, employment and financial-services workflows. It reports 3.2 million issued credentials, 1.4 million active holders, 180 contracted verifiers and 4.8 million annual presentation attempts. Of the contracted verifiers, 118 are in production and 92 generated accepted activity in the most recent twelve months.

The model assumes 3.5 million accepted presentations after technical, policy and business-workflow rejection. Realised revenue averages USD 0.92 per accepted presentation. Subscription, implementation and issuer-service revenue add USD 3.1 million. Variable cost includes cloud, status services, support, fraud operations and third-party data.

Every input is hypothetical. The case illustrates a method. It is not evidence about a named company, market size, pricing norm, transaction or expected outcome.

32. RECONCILE THE HYPOTHETICAL FUNNEL

The case begins with 4.8 million presentation attempts. Technical verification succeeds for 4.4 million. Verifier policy accepts 3.8 million. The downstream workflow completes for 3.5 million. Each step uses a different denominator and indicates a different improvement opportunity.

The 700,000-attempt gap between technical success and completed workflow is commercially significant. Part can reflect credential semantics, missing supplementary evidence, status, user abandonment or the verifier's product policy.

The buyer should value the 3.5 million completed workflows as current activity. It can assign option value to recoverable funnel loss after product and policy analysis. It should not treat every attempt as monetisable volume.

33. CALCULATE THE HYPOTHETICAL BASE CASE

At USD 0.92 realised revenue per accepted presentation, transaction revenue is USD 3.22 million. Adding USD 3.1 million of subscriptions, implementation and issuer services produces USD 6.32 million of total revenue.

Assumed variable cost is USD 0.31 per accepted presentation, or USD 1.09 million. Other directly attributable service cost is USD 1.25 million. Contribution is therefore USD 3.98 million before product development, general overhead and standards migration.

The model treats contribution as the current economic base. It then adds or subtracts value for retention, network growth, concentration, migration, liability and option scenarios. The figures are illustrative and should be replaced with verified company evidence.

34. TEST NETWORK UPLIFT

The base case assumes that adding an anchor employment verifier increases qualified reuse by four percentage points within affected holder cohorts. It also assumes that an additional authoritative qualification issuer improves acceptance among employment verifiers.

The uplift should be measured through cohorts and matched comparisons. Marketing, seasonality and mandatory rollout can create apparent network effects. The buyer should require a defined observation period and stable event classification.

Only verified incremental contribution should enter current value. A plausible cross-side mechanism without observed evidence belongs in the option case.

35. APPLY CONCENTRATION DISCOUNTS

The hypothetical network receives 38 percent of accepted activity from its largest verifier and 62 percent from its five largest verifiers. One national registry supports 46 percent of issued active credentials.

These relationships can create trust and distribution. They also expose revenue and network utility to renewal, policy and change-of-control risk. The loss of an anchor can affect several participant groups at once.

The buyer should model participant loss as a graph shock rather than a simple revenue reduction. It should include lower holder utility, weaker issuer attraction and stranded integration cost.

Table 3. Hypothetical valuation bridge

Component	Illustrative basis	Value logic	Deal response
Current contribution	USD 3.98m before central overhead	Verified accepted workflows and contracted services	Cash-flow valuation
Network uplift	Cohort-tested cross-side contribution	Incremental value from dense accepted edges	Partial upfront credit
Standards option	Probability-weighted migration and new acceptance	Future profile convergence	Milestone consideration
Anchor concentration	Graph shock from participant loss	Revenue and utility dependence	Discount and consent condition
Migration exposure	Reissuance, verifier updates and parallel support	Cost to reach target profile	Reserve or price adjustment
Liability exposure	Fraud, redress, audit and contractual caps	Downside from failed reliance	Indemnity, insurance and escrow

All amounts and probabilities are illustrative management inputs, not observed market data.

36. DESIGN SCENARIO VALUATION

The downside case assumes slower verifier activation, price compression and higher migration cost. The base case uses current accepted activity and a measured expansion plan. The upside case requires independent interoperability, improved qualified reuse and successful entry into additional regulated workflows.

Each scenario should state participant growth, acceptance conversion, realised price, variable cost, renewal, concentration and migration. The model should not use one network-effect multiplier across all revenue.

Probability weights are management judgements unless supported by observed cohorts and contracts. They should be disclosed as such and tested through sensitivity analysis.

37. SELECT THE TRANSACTION INSTRUMENT

Current earnings can support upfront consideration. Standards-dependent expansion can support earn-out or contingent value rights. Migration liabilities can support holdback, escrow or price adjustment. Key trust relationships can become conditions precedent.

The earn-out metric should be difficult to manipulate and aligned with economic value. Accepted production workflows, retained verifiers and contribution are stronger than credentials issued or wallets downloaded. The agreement should define exclusions, data access and dispute resolution.

Seller rollover can align long-term network development. It should not replace a clear operating plan or conceal unsupported valuation.

38. BUILD THE DILIGENCE EVIDENCE ROOM

The evidence room should include participant registers, trust agreements, schemas, standards ledger, key and status architecture, contracts, policy configurations, event definitions, transaction logs, invoices, cohorts, support, incidents, audits and migration plans.

Samples should allow reconstruction of an accepted workflow from issuance through business completion. The buyer should test rejected and disputed cases as well as successes.

Evidence quality should be scored by source, completeness, period and reconciliation. Management presentations can explain the thesis. System records, customer evidence and authoritative registers should substantiate it.

39. PLAN THE FIRST ONE HUNDRED DAYS

The first one hundred days should protect current trust relationships and establish one network operating model. The buyer should preserve keys, registries, status, certification, service levels, redress and participant communication.

It should create a unified participant taxonomy, acceptance graph, standards ledger and economics dashboard. Duplicate schemas and integrations can then be prioritised by activity and migration need.

Early product decisions should focus on high-density clusters. Broad platform consolidation without workflow evidence can disrupt acceptance. Governance should assign owners for issuer, holder, verifier, standards and liability outcomes.

40. GOVERN THE STANDARDS ROADMAP

The standards roadmap should connect technical releases to participant obligations and commercial value. It should identify profiles, conformance, certification, migration windows, customer commitments and sunset decisions.

A cross-functional committee should include product, engineering, security, legal, compliance, customer operations and finance. Decisions should record evidence, affected cohorts, cost and rollback.

The board should receive progress through accepted-workflow coverage and migration risk, not protocol completion alone. Technical delivery matters when it protects or expands governed reliance.

41. USE A BOARD SCORECARD

The board scorecard should track active issuers, liquid holders, production verifiers, accepted workflows, qualified reuse, contribution, concentration, incidents, complaints, profile coverage and migration cost.

Metrics need definitions and reconciliations. The scorecard should show both level and cohort movement. A rising verifier count can coexist with declining acceptance if implementation quality weakens.

Board decisions should link to price, structure, investment, standards support, participant strategy or risk appetite. Metrics that do not change a decision should be removed or moved to operations.

Table 4. Board and investment-committee scorecard

Domain	Core measure	Warning signal	Decision response
Acceptance	Completed regulated workflows	Technical success without business completion	Fix policy or claims
Network	Qualified reuse and graph density	Participant count grows while edges remain sparse	Refocus acquisition
Economics	Contribution by workflow and cohort	Volume grows with falling contribution	Reprice or redesign
Standards	Production coverage on target profiles	Large legacy cohort without migration path	Fund reserve and milestones
Trust	Registry, status and assurance performance	Unauthorised issuer or stale credential accepted	Suspend and remediate
Concentration	Activity and utility dependency	Anchor controls several network sides	Obtain consent and diversify
Liability	Loss, complaints, redress and insurance	Contractual gaps or correlated exposure	Restructure protection
Transferability	Change-of-control and data portability	Critical designation or integration terminates	Condition closing

Minimum evidence should be agreed before signing and maintained after completion.

42. CONCLUDE WITH ACCEPTED TRUST

Verifiable-identity networks can create valuable cross-side effects. Their economics depend on accepted trust: authoritative credentials, active holders and verifiers that complete real workflows under a governed policy. Participant counts describe reach. Accepted edges, reuse and contribution demonstrate value.

Before standards converge, the buyer should separate current activity, network uplift, option value and migration exposure. It should price each with evidence suited to the claim. Open standards can expand participation and reduce technical lock-in. They make distribution, assurance, workflow integration, service quality and liability more important.

The disciplined sequence is to map the acceptance graph, grade participant quality, build cohorts, reconcile the funnel, calculate contribution, cost migration, shock anchor relationships and structure consideration around verified outcomes. This approach allows an acquirer to pay for trust that works today while retaining participation in credible future convergence.

REFERENCES

[1] Armstrong, Mark. Competition in Two-Sided Markets. RAND Journal of Economics, 37(3), 2006. https://doi.org/10.1111/j.1756-2171.2006.tb00037.x

[2] National Institute of Standards and Technology. NIST SP 800-63C-4: Digital Identity Guidelines, Federation and Assertions. August 2025. https://doi.org/10.6028/NIST.SP.800-63C-4

[3] National Institute of Standards and Technology. Subscriber-Controlled Wallets. https://pages.nist.gov/800-63-4/sp800-63c/Wallets/

[4] World Wide Web Consortium. Verifiable Credentials Data Model v2.0. W3C Recommendation, 15 May 2025. https://www.w3.org/TR/vc-data-model-2.0/

[5] World Wide Web Consortium. W3C publishes Verifiable Credentials 2.0 as a W3C Standard. 15 May 2025. https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/

[6] OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0. Final Specification, 16 September 2025. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-final.html

[7] OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0 Final Specification Approved. 16 September 2025. https://openid.net/openid-for-verifiable-credential-issuance-1-final-specification-approved/

[8] European Parliament and Council. Regulation (EU) 2024/1183 establishing the European Digital Identity Framework. 11 April 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[9] European Commission. European Digital Identity Wallet Architecture and Reference Framework. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

[10] European Commission. Technical Specifications for the EU Digital Identity Wallet. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/869793973/Technical+Specifications

[11] European Commission. New round of EU Digital Identity Wallet implementing regulations. 7 May 2025. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/896827698/European+Commission+adopts+new+round+of+EU+Digital+Identity+Wallet+implementing+regulations

[12] European Commission. EUDI Wallet Reference Implementation. https://docs.eudi.dev/latest/

[13] World Bank Identification for Development. ID 101: Basic Concepts. https://id4d.worldbank.org/guide/id-101-basic-concepts

[14] World Bank Identification for Development. Business Models. https://id4d.worldbank.org/guide/business-models

[15] World Bank Identification for Development. Credentials and Authentication. https://id4d.worldbank.org/guide/credentials-authentication

[16] World Bank Identification for Development. Pillar 2: Design. https://id4d.worldbank.org/guide/pillar-2-design

[17] World Bank. Principles on Identification for Sustainable Development: Toward the Digital Age. 2017. https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

[18] World Bank. Verifiable Credentials for MSMEs in the Dominican Republic. 7 January 2026. https://www.worldbank.org/en/brief/2026/01/07/verifiable-credentials-for-msmes-in-the-dominican-republic

ABOUT THE AUTHOR

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and close.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners he is Managing Partner, leading the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.