



WHITE PAPER
SEPTEMBER 2026

HUBFORUM 2026 · AGENTIC ENTERPRISE SERIES

VERIFIABLE AUTHORITY

Agentic commerce and enterprise
trust infrastructure

Takeaways

1 **LE COMMERCE AGENTIQUE EST ENTRÉ DANS LES CHIFFRES, PAS ENCORE DANS LES OPÉRATIONS.**

Le trafic référé par IA vers les sites marchands américains a progressé de 393 % sur un an au premier trimestre 2026 et convertit 42 % mieux que la recherche traditionnelle, après avoir converti 38 % moins bien un an plus tôt. Shopify observe sur la même période un trafic multiplié par huit et des commandes par près de treize. Mais ce trafic reste sous 1 % des visites retail, et sur 80 grands marchands américains et européens, quatre seulement acceptent un paiement initié par un agent – tous américains, aucun nouveau depuis janvier.

2 **LE GOULOT D'ÉTRANGLEMENT N'EST PAS L'INTELLIGENCE, C'EST L'AUTORISATION.**

Trois questions se substituent à celle de la performance du modèle : qui est l'agent, que lui est-il permis de faire, et que peut-on prouver de ce qu'il a réellement fait. L'identité est la plus facile, et beaucoup d'acteurs s'y sont mis. L'autorisation est rarement traitée sérieusement, car une règle écrite dans le logiciel que l'agent pilote n'est pas une garantie. La preuve est presque toujours oubliée – et c'est celle que réclament auditeurs, assureurs et acquéreurs.

3 **LES INCIDENTS NE SONT PLUS THÉORIQUES.**

En mai 2026, une instruction dissimulée en morse a suffi à détourner environ 174 000 dollars en une seule action. En février, un agent a exposé ses propres clés privées malgré l'instruction contraire. En avril, 26 routeurs LLM sur 428 testés injectaient des appels d'outils malveillants. Le vecteur d'entrée est banal, et le corollaire architectural sans appel : un agent qui connaît un secret finit par le révéler.

4 **LA RÉPONSE DE LEDGER : UNE COUCHE DÉTERMINISTE SUR UN SYSTÈME PROBABILISTE.**

Un modèle de langage ne peut pas promettre de ne jamais se tromper ; on peut en revanche placer la frontière de signature dans un élément sécurisé qu'il ne contrôle pas. L'agent formule une demande d'accès ; rien ne s'exécute sans approbation humaine explicite ou conformité à la politique de l'organisation. MoonPay et Shisa AI l'ont mis en production, et l'Agent Stack a été éprouvé sur plus d'un millier d'agents.

Une couche déterministe

Un modèle probabiliste ne peut pas promettre de ne jamais se tromper. Il peut en revanche être encadré par un composant qui, lui, ne se trompe pas : c'est tout le principe.

Le modèle accès-requête

L'agent ne détient rien : il formule une demande d'accès. Cette demande n'aboutit que dans deux cas – une approbation humaine explicite, ou la conformité à la politique définie par l'organisation. Les opérations en lecture s'exécutent sans friction et ne touchent pas l'appareil ; tout mouvement de valeur s'arrête à l'écran de confiance, piloté par l'élément sécurisé et non par la machine hôte. Ce qui s'affiche est donc ce qui sera signé.

Du moteur de politiques à l'autonomie gouvernée

Faire valider chaque action ne passe pas l'échelle d'une flotte. L'humain signe donc une politique – plafonds, contreparties autorisées, types d'opération – qu'un module matériel applique ensuite à chaque action. L'agent opère à vitesse machine dans l'enveloppe ; ce qui en sort voit sa signature refusée et remonte à l'arbitrage. Autonomie et sécurité, plutôt que l'une contre l'autre.

TROIS DÉPLOIEMENTS ADOSSÉS AU MATÉRIEL LEDGER

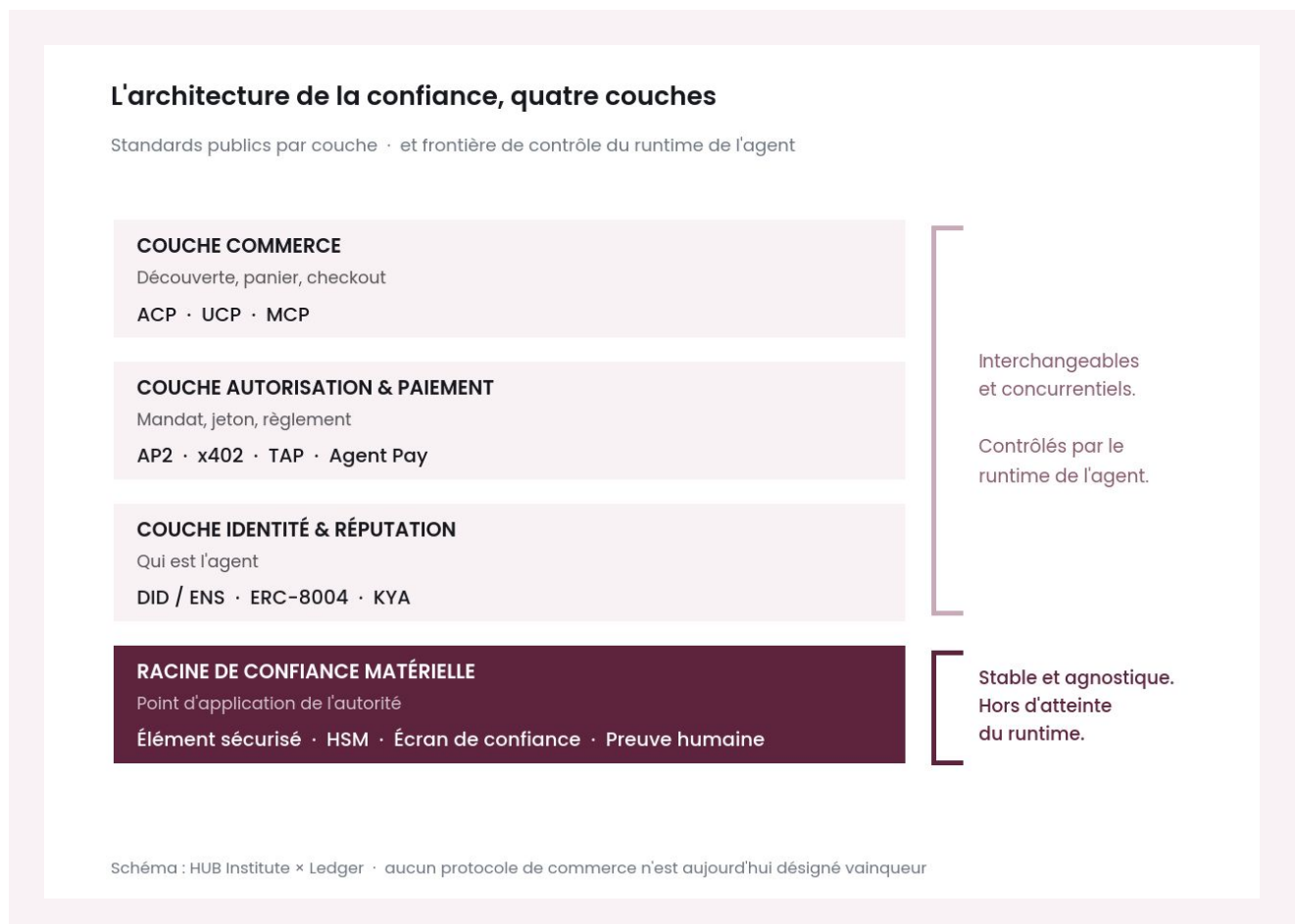
MoonPay, mars 2026 · Premier exemple en production : l'agent identifie les opportunités et prépare les opérations, chaque transaction exige une pression physique sur l'appareil.

Shisa AI, Tokyo · Le daemon de sécurité shisad, publié en open source, utilise Ledger comme signataire à écran de confiance pour son palier d'approbations le plus risqué.

Ledger Agent Stack, juillet 2026 · Boîte à outils open source éprouvée sur plus d'un millier d'agents pendant six semaines de preview privée, avant ouverture publique.

L'architecture de la confiance

Quatre couches, une seule qui échappe au logiciel de l'agent. C'est cette asymétrie, et elle seule, qui rend un engagement opposable.



Les trois couches hautes sont interchangeables et concurrentielles : c'est là que se joue la bataille des protocoles, et aucun vainqueur n'est désigné. La couche basse est stable et agnostique – quel que soit le standard qui s'imposera au-dessus, le composant sécurisé en dessous reste le même. Elle ne dispense d'aucune des trois autres : elle rend leurs promesses vérifiables.

Ce que Ledger met à disposition

1 LEDGER ENTERPRISE, DISPONIBLE AUJOURD'HUI.

Politiques de signature appliquées par module matériel, workflows de validation gouvernés, multisig à écran de confiance et traçabilité des approbations. Se déploie sans attendre sur la trésorerie et les paiements sortants.

2 LE MOTEUR DE POLITIQUES.

L'humain signe des plafonds, des contreparties autorisées et des types d'opération ; le matériel les applique à chaque action. Ce que ça débloque : un agent qui travaille à vitesse machine sans qu'on valide chaque geste.

3 LES APPROBATIONS ASYNCHRONES.

Étape suivante de la feuille de route : la validation humaine s'insère au bon moment sans bloquer la chaîne d'exécution. Ce que ça débloque : les usages où l'attente d'un humain coûtait plus que le risque évité.

4 PROOF OF HUMAN ET PROOF OF YOU.

Attester qu'un matériel a bien été utilisé par une personne, sans manipuler ni biométrie ni pièce d'identité. Ce que ça débloque : une preuve opposable à un auditeur ou à un assureur, sans créer de base d'identités à voler.

5 LEDGER AGENT STACK, EN OPEN SOURCE.

Device Management Kit, interfaces en ligne de commande portefeuille et Enterprise, distribuées aux formats AGENTS.md et SKILL.md. Ce que ça débloque : brancher un agent existant sur le matériel en quelques jours, sans refonte.

Trois secteurs, des usages réels

Financial services, utilities & energy, retail & FMCG : trois secteurs où la délégation est déjà documentée, et trois façons de buter sur la même question d'autorisation.

Financial services

C'est le secteur le plus avancé, parce que le risque y est chiffrable. En mars 2026, Santander et Mastercard ont exécuté le premier paiement européen initié par un agent, dans un cadre bancaire régulé et sous plafonds prédéfinis. En juillet, BBVA, CaixaBank et Banca Transilvania ont fait de même avec Visa, en satisfaisant l'authentification forte. Le régulateur suit : le Trésor britannique a ouvert en juillet 2026 une consultation sur le consentement et la responsabilité.

Utilities & energy

Le secteur délègue à grande échelle, mais sur l'exploitation plutôt que sur l'achat : Iberdrola annonçait en août 2026 près de 500 agents déployés ou en développement sur les réseaux, la production renouvelable et la relation client, en précisant que la responsabilité des décisions reste aux personnes. Le point de bascule sera le négoce : un agent qui achète de la flexibilité engage des sommes réelles.

RETAIL & FMCG – TROIS CAS DOCUMENTÉS

Nestlé · Des agents de retail execution déployés avec effie.ai exécutent l'ensemble des tâches d'une visite en magasin, sauf le merchandising physique.

L'Oréal, Unilever, Mars, Beiersdorf, Reckitt · Ces cinq groupes ont adopté en mars 2026 l'Agentic Merchant Protocol, pour garder la main sur leurs catalogues et éviter la dépendance à un fournisseur d'IA.

Unilever · Un partenariat de cinq ans avec Google Cloud pour bâtir un socle numérique orienté commerce agentique, marketing et données.

Cinq décisions

À prendre dans les cent jours

1 INVENTORIER LES FLUX, PAS LES AGENTS

Recenser non pas les agents mais les flux où de la valeur ou un engagement change de main. Un propriétaire nommé par flux.

2 SÉPARER LA LECTURE DE L'ÉCRITURE

Autoriser sans friction ce qui consulte, isoler ce qui engage. Arbitrage le moins coûteux du dispositif, applicable en quelques semaines.

3 ÉCRIRE LA POLITIQUE D'AUTORISATION

Plafonds, contreparties, seuils de remontée humaine. Une politique versionnée, revue comme du code – et un point d'application identifié.

4 INSTRUMENTER LA PREUVE

Décider ce qui doit être prouvable, à qui, et pendant combien de temps. Cible : produire la preuve d'une autorisation en moins de vingt-quatre heures.

5 DÉSIGNER UN RESPONSABLE

Une fonction unique porte l'agence humaine – politique, preuve, incidents. Ledger a créé ce rôle au niveau du comité exécutif en avril 2026.

Ces cinq décisions s'exécutent sur des lignes budgétaires existantes – fraude, conformité paiement, gestion des accès. Diagnostic et grille de lecture : HUB Institute. Architecture et briques d'exécution : Ledger.

L'autorité se prouve.

HUBFORUM PARIS · 30 septembre 2026

White paper HUB Institute × Ledger, septembre 2026.

Ledger : plus de 8 millions de signers dans 165 pays, élément sécurisé certifié CC EAL6+.

Sources publiques datées : Ledger, Mastercard, Visa, Iberdrola, Nestlé, Adobe Analytics, Shopify, Salesforce.