

LE DERNIER CONTRÔLE AVANT « ENVOYER »

Paiement en stablecoins : comment éviter qu'une erreur d'adresse ou de réseau ne devienne une perte définitive ?

Sécuriser chaque transaction avant son autorisation : bénéficiaire, adresse, stablecoin, réseau, contrôles internes et décision finale.

Un paiement ne devrait pas devenir exécutable simplement parce que les fonds sont disponibles.

Il doit d'abord franchir un sas de contrôle pré-transaction.

GO

GO SOUS CONDITIONS

STOP & ESCALADE



Sommaire décisionnel

Les huit contrôles qui séparent une instruction de paiement d'un transfert autorisé

Avant de cliquer sur « envoyer », l'entreprise doit prouver que chaque donnée critique a été vérifiée.

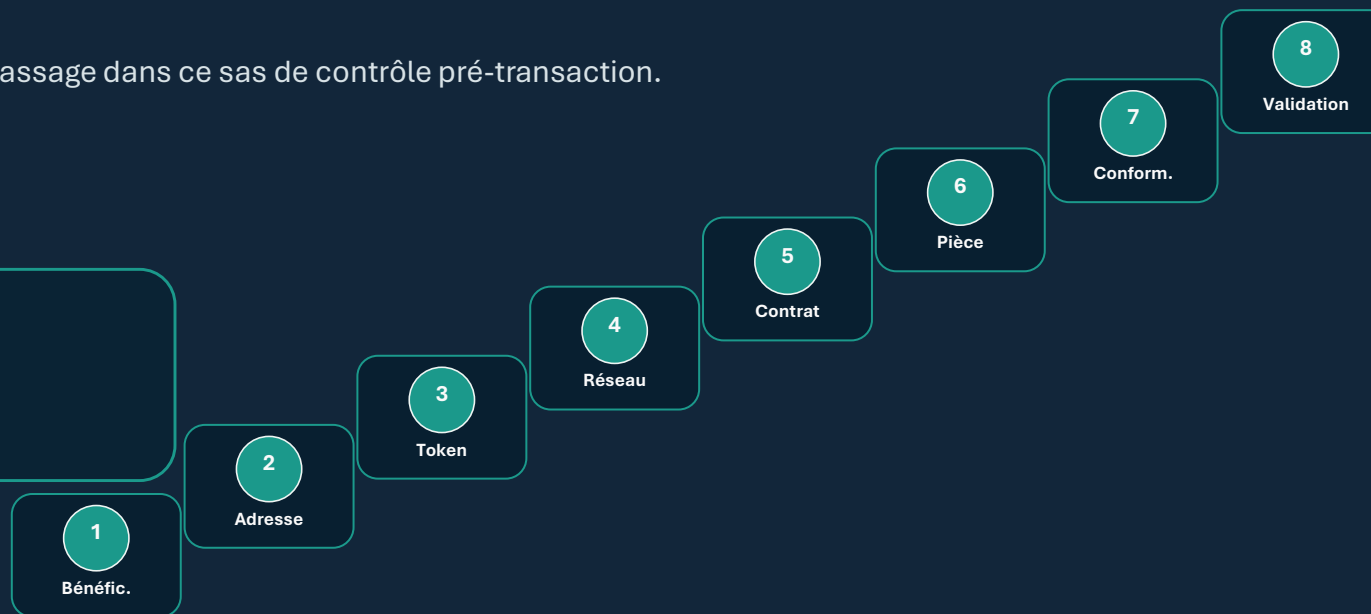
Le paiement ne devient exécutable qu'après passage dans ce sas de contrôle pré-transaction.

DÉCISION
tracée

Le parcours du guide

Instruction reçue → contrôles successifs

Décision documentée : GO · CONDITIONS · STOP



Une transaction blockchain n'est pas une instruction bancaire classique

Ce qui change : après diffusion, il ne faut présumer ni rappel, ni annulation, ni récupération automatique.

LOGIQUE BANCAIRE

Instruction → contrôles PSP/banque
→ exceptions possibles

Certains schémas prévoient des messages de retour, de rappel ou d'investigation.
Cela dépend du système de paiement et des acteurs concernés.

TRANSFERT BLOCKCHAIN

Signature → diffusion on-chain
→ finalité du réseau

Après diffusion, l'entreprise ne doit présumer ni rappel, ni annulation,
ni récupération automatique des fonds.



Décision de contrôle interne

Si l'adresse, le réseau, le token ou le bénéficiaire ne sont pas confirmés :
STOP & ESCALADE avant tout envoi.

Sources-cadre : Ethereum.org — FAQ « I sent crypto to the wrong address » & Security, consultés 26 août 2026 — <https://ethereum.org/community/support/faq/> ; <https://ethereum.org/security/> | Ethereum.org

— Proof-of-stake finality, consulté 26 août 2026

— <https://ethereum.org/developers/docs/consensus-mechanisms/pos/> | European Payments Council

— SEPA Credit Transfer rulebook and implementation guidelines, consulté 26 août 2026

— <https://www.europeanpaymentscouncil.eu/what-we-do/epc-payment-schemes/sepa-credit-transfer/sepa-credit-transfer-rulebook-and> | FATF/GAFI — Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs, 28 oct. 2021

— <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>

Vérifier le bénéficiaire et l'adresse avant de vérifier le montant

Obligation légale : selon juridiction/contrepartie

Bonne pratique : confirmation indépendante

Risque clé : une adresse copiée dans un e-mail ne suffit pas à autoriser un transfert.

Décision de contrôle interne

Nouveau bénéficiaire : pas de paiement direct.

Collecte tracée · confirmation indépendante · validation interne.

1

Collecter

Source maîtrisée
+ pièce justificative

2

Confirmer

Canal séparé
si risque ou
changement

3

Qualifier

Bénéficiaire identifié
+ wallet destinataire

4

Figer

Liste blanche
ou dossier validé

Source de l'adresse

Qui l'a fournie ?
Dans quel document ?
À quelle date ?

Canal de confirmation

E-mail seul : insuffisant
Canal séparé : téléphone, portail, contrat, prestataire

Règle de changement

Nouvelle adresse, nouveau réseau ou urgence :
STOP & confirmation renforcée

STOP & ESCALADE

Adresse nouvelle, modifiée, incohérente ou impossible à confirmer : le paiement est suspendu avant tout contrôle du montant.

Stablecoin, réseau, contrat : les 3 champs à ne jamais confondre

Question de décision : le bénéficiaire accepte-t-il exactement ce token, sur ce réseau, avec ce contrat ou identifiant ?

RÈGLE OPÉRATIONNELLE

Même nom ≠ même réseau ≠ même contrat.
Champ manquant ou incohérent = STOP & clarification.

À NE PAS OUBLIER

- Frais : prévoir le token natif requis par le réseau — par exemple ETH sur Ethereum, SOL sur Solana.
- Memo, tag ou référence de dépôt : seulement si le prestataire ou le compte destinataire l'exige.
- Compatibilité : le wallet du bénéficiaire doit recevoir ce token sur ce réseau précis.

LES 3 CHAMPS À ALIGNER AVANT EXÉCUTION

Contrôle interne — pas une obligation universelle : dépend du prestataire, du wallet, du stablecoin et de la juridiction.

1 ACTIF

Stablecoin

Ex. USDC / EURC / USDT : l'actif économique annoncé dans la facture ou le contrat.

2 INFRASTRUCTURE

Réseau

Ex. Ethereum, Solana, Base, Polygon : la chaîne sur laquelle le transfert circule.

3 IDENTIFIANT

Contrat / ID

Sur certains réseaux, le token est identifié par une adresse de contrat ou un identifiant officiel.

Autoriser seulement si les 3 informations correspondent aux instructions validées du bénéficiaire.

Contrôler la transaction avant exécution

Question de décision : l'ordre est-il complet, cohérent et autorisable avant diffusion on-chain ?

RÈGLE OPÉRATIONNELLE

**Le contrôle ne commence pas dans le wallet.
Il commence avant la saisie de la transaction.**

À QUALIFIER AVANT D'EXIGER

Obligation légale
vérifiée

Exigence du
prestataire

Bonne pratique
interne

Ne pas transformer automatiquement un contrôle interne en obligation universelle : le niveau dépend du pays, du prestataire, du corridor et du rôle de l'entreprise.

SAS DE CONTRÔLE AVANT EXÉCUTION

Le paiement ne devient exécutable que si les contrôles critiques sont verts.

1 Bénéficiaire & justificatif

Contrat, facture, motif économique, identité du destinataire.

2 Adresse & destination

Source de l'adresse, changement récent, wallet final.

3 Stablecoin & réseau

Token exact, chaîne choisie, contrat/ID, memo/tag.

4 Montant & frais

Montant attendu, devise de référence, token natif requis.

5 Conformité ciblée

Sanctions, AML/CFT ou KYT si requis ou pertinent.

6 Autorisation & preuves

Maker/checker, seuils, hash et dossier conservés.

Incohérence, champ manquant ou risque non résolu = STOP & CLARIFICATION

Whitelisting, double validation, seuils et transaction test

Question de décision : quel niveau de contrôle est proportionné au risque du paiement ?

RÈGLE OPÉRATIONNELLE

On ne renforce pas tous les paiements. On renforce ceux où l'erreur, le changement ou le montant rendent la perte difficilement acceptable.

À QUALIFIER AVANT D'APPLIQUER

Obligation vérifiée · Exigence prestataire · Bonne pratique interne

Ces dispositifs relèvent souvent du contrôle interne, sauf règle légale, contractuelle ou prestataire spécifique.

ARCHITECTURE DE CONTRÔLE PROPORTIONNÉE

Le niveau de contrôle augmente avec le caractère nouveau, sensible ou inhabituel du paiement.

1

Païement récurrent

Bénéficiaire déjà approuvé, adresse whitelisted, réseau habituel.

Validation normale

2

Nouvelle coordonnée

Nouvelle adresse, changement de réseau ou instruction reçue hors canal habituel.

Confirmation indépendante

3

Risque élevé

Montant important, corridor sensible, paiement urgent ou contrepartie nouvelle.

Double validation + seuils

4

Incertitude persistante

Adresse incohérente, test échoué, bénéficiaire non confirmé ou signal KYT non résolu.

STOP & ESCALADE

Transaction test : utile, mais non suffisante — elle réduit un risque technique, pas les risques d'identité, de fraude ou de conformité.

Le runbook de paiement : de la facture à la validation on-chain

Question de décision : le paiement a-t-il franchi toutes les portes avant d'être autorisé ?

RÈGLE OPÉRATIONNELLE

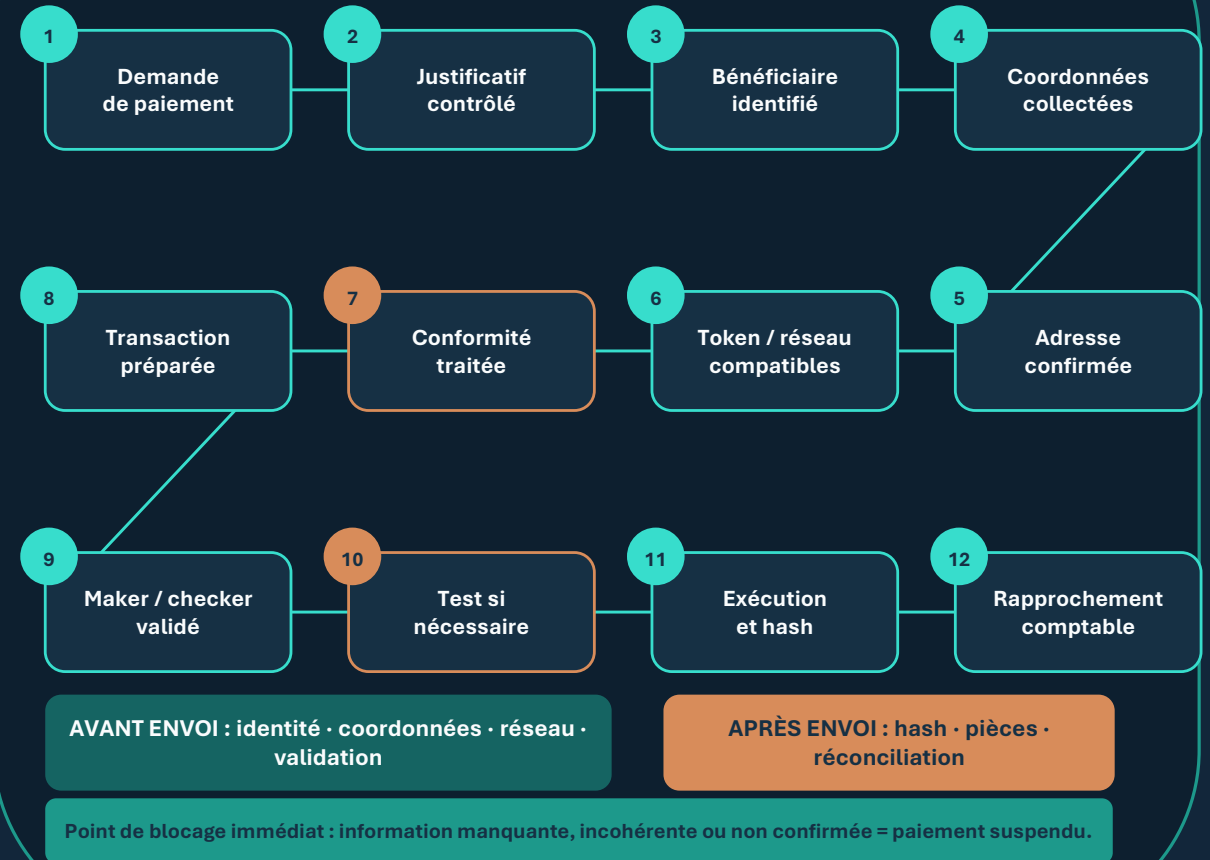
Une transaction ne part pas du wallet parce qu'elle est prête techniquement. Elle part parce qu'un chemin de preuve relie facture, bénéficiaire, adresse, réseau, validation et hash.

QUI FAIT QUOI ?

Préparateur : rassemble les pièces.
Vérificateur : contrôle les coordonnées et le réseau.
Autorisateur : décide GO / CONDITIONS / STOP.
Comptabilité : rapproche hash, facture et tiers.

PROCESSUS COMPLET AVANT & APRÈS ENVOI

Chaque étape doit laisser une preuve réutilisable par la trésorerie, la conformité et la comptabilité.



Quand faut-il bloquer le paiement ?

Question de décision : l'anomalie peut-elle être levée avant l'envoi — ou faut-il suspendre ?

RÈGLE SIMPLE

Le doute ne se règle pas après le paiement. Tant que l'adresse, le réseau, le bénéficiaire ou la conformité ne sont pas confirmés, la transaction reste non exécutable.

QUI DÉCIDE ?

Préparateur : arrête si une pièce manque.
Vérificateur : exige une confirmation indépendante.
Conformité / trésorerie : arbitre les risques spécifiques.
Autorisateur : tranche GO, CONDITIONS ou STOP.

MATRICE D'ESCALADE PRÉ-ENVOI

L'objectif n'est pas de ralentir tous les paiements : il est de bloquer ceux qui ne doivent pas partir.

GO

EXÉCUTER

- ☐ Coordonnées whitelistées
- ☐ Token, réseau et memo confirmés
- ☐ Justificatif et validation complets
- ☐ Preuves prêtes pour rapprochement

GO SOUS CONDITIONS

RENFORCER

- ☐ Nouveau bénéficiaire confirmé
- ☐ Montant inhabituel validé
- ☐ Réseau ou tag reconfirmé
- ☐ Test pertinent et cohérent

STOP & ESCALADE

SUSPENDRE

- ☐ Adresse changée au dernier moment
- ☐ Bénéficiaire ≠ wallet destinataire
- ☐ Adresse à risque non résolue
- ☐ Test échoué ou justificatif absent

Décision finale documentée : poursuivre · confirmer · suspendre · refuser

Checklist finale : autoriser ou ne pas autoriser

Décision attendue : chaque paiement doit sortir du sas avec une décision documentée — GO, GO sous conditions ou STOP & ESCALADE.

RÈGLE D'UTILISATION

Si une donnée critique manque ou change avant l'envoi, la transaction ne passe pas en GO.

CHECKLIST 2 MINUTES AVANT ENVOI

- | | |
|--|---|
| ☐ Bénéficiaire confirmé et cohérent avec le contrat | ☐ Justificatif économique disponible |
| ☐ Adresse obtenue d'une source tracée | ☐ Frais et token natif nécessaires prévus |
| ☐ Stablecoin, réseau et contrat alignés | ☐ Contrôles conformité effectués si requis |
| ☐ Memo / tag ou info de dépôt vérifié si nécessaire | ☐ Seuil et double validation appliqués |

PREUVES À CONSERVER · instruction · source adresse · confirmation · validation · hash
· facture · rapprochement

MATRICE DE DÉCISION FINALE

La décision n'est pas technique : elle est financière, opérationnelle et documentée.

GO

AUTORISER

- Tous les champs critiques sont confirmés
- Aucune modification tardive
- Justificatif et validation complets

GO SOUS CONDITIONS

RENFORCER

- Confirmation indépendante reçue
- Transaction test pertinente et cohérente
- Validation renforcée avant envoi

STOP & ESCALADE

SUSPENDRE

- Adresse, réseau ou memo non confirmé
- Anomalie ou risque non levé
- Conformité ou bénéficiaire bloquant

Avant clic final : relire écran wallet · fiche de paiement · facture · décision signée.