16/03/2026

Livre Blanc : Ingénierie de Continuité des Actifs Numériques - Résolution de la Mort Numérique en Droit Successoral Suisse

Benjamin Maillard
MAILLARD DIGITAL CONTINUITY

Table des matières

1. Introduction

Le paysage patrimonial de la Suisse romande, et singulièrement celui de l'arc lémanique englobant les cantons de Genève et de Vaud, fait face à une mutation structurelle d'une ampleur inédite. L'intégration systémique des actifs numériques, allant des données cryptographiques pures aux jetons de valeur et cryptomonnaies, au sein des portefeuilles privés redéfinit radicalement les contours de la transmission successorale. Au cœur de cette démocratisation se trouve un segment démographique spécifique et particulièrement dense en Suisse : la clientèle qualifiée de « Mass Affluent ». Ce segment, composé de cadres supérieurs, de professions libérales, de médecins et d'entrepreneurs locaux, se caractérise par la détention de portefeuilles numériques dont la valorisation fluctue généralement entre 50'000 et 500'000 francs suisses (CHF).[1]

Ces investisseurs ont dépassé le stade de l'expérimentation spéculative sur les plateformes d'échange de détail pour s'inscrire dans une logique rigoureuse de préservation patrimoniale à long terme. Toutefois, la gestion de cette richesse numérique engendre une vulnérabilité systémique majeure. Contrairement à la clientèle institutionnelle ou aux individus très fortunés (HNWI) qui s'appuient sur des banques dépositaires régulées ou des infrastructures de *Family Offices*, le segment Mass Affluent recourt de manière prépondérante à l'auto-garde, couramment désignée sous les termes de *Self-Custody* ou de *Shadow Custody*. Cette gestion autonome, orchestrée au moyen de dispositifs matériels cryptographiques conservés sans la moindre gouvernance formelle, garantit au détenteur une souveraineté absolue sur ses actifs et une immunité totale contre le risque de faillite d'une contrepartie bancaire.

Néanmoins, cette architecture technologique soulève un paradoxe redoutable en matière de droit successoral suisse. L'absence de tiers de confiance transforme cette souveraineté technologique du vivant de l'investisseur en un risque de destruction de valeur définitive en cas d'incapacité de discernement ou de décès. Ce phénomène clinique, qualifié de « mort numérique », constitue un angle mort procédural aux conséquences dévastatrices pour les études notariales, les avocats d'affaires et les exécuteurs testamentaires mandatés pour liquider la succession.[2]

L'analyse exhaustive présentée dans ce rapport démontre comment l'ingénierie de continuité numérique agit comme l'unique solvant technique face à ce blocage juridique. En traduisant des processus cryptographiques de pointe tels que le quorum multi-signatures, le partage de secret de Shamir, et l'hygiène des environnements strictement *Air-Gapped* en garanties juridiques irréfutables, il devient possible d'assurer la transmission de ces actifs. Cette démarche garantit simultanément aux professionnels du droit notarial une absence totale de risque fiduciaire, une immunité quant à la responsabilité technologique, et la certitude d'une liquidation fluide de la masse successorale.

[1] Consulter l'étude HSLU, Consuler l'étude HSLU éditée par SIX Group
[2] Consulter l'article sur legal-testa.ch

2. Le Risque Systémique : La "Mort Numérique" et l'Impasse Successorale

La mort numérique survient avec une brutalité absolue lorsqu'un testateur décède ou perd sa capacité d'agir sans avoir préalablement documenté et testé une gouvernance formelle de ses accès cryptographiques. Contrairement aux actifs bancaires traditionnels pour lesquels une simple injonction judiciaire ou un certificat d'héritier suffit à débloquer les fonds auprès de l'établissement financier, l'accès aux registres distribués (technologie DLT) repose exclusivement sur les mathématiques de la cryptographie asymétrique.

2.1. L'Inviolabilité Cryptographique et la Suprématie du Mur Mathématique

Dans le paradigme de l'auto-garde, les actifs numériques n'existent physiquement nulle part ; ils ne sont que des inscriptions inaltérables sur un registre public décentralisé. La possession matérielle de l'actif se définit alors exclusivement par la maîtrise de la clé privée cryptographique, seule entité capable de générer une signature valide pour mouvoir la valeur patrimoniale. En l'absence du code PIN d'accès au dispositif matériel ou de la phrase de récupération (couramment appelée *Seed Phrase*) permettant de dériver cette clé privée, l'intégralité de la masse patrimoniale numérique est irrémédiablement inaccessible.

La cryptographie asymétrique qui sécurise des réseaux tels que Bitcoin ou Ethereum ne prévoit aucun mécanisme de contournement. Il n'existe aucun administrateur central habilité à réinitialiser un mot de passe, ni aucune porte dérobée (*backdoor*) technique permettant l'intervention de la force publique pour forcer l'accès aux fonds. Les héritiers, même légitimés par un acte de notoriété ou un certificat d'héritier incontestable, se heurtent à un mur mathématique absolu. L'algorithme est fondamentalement indifférent au droit civil. Si les actifs étaient conservés auprès d'une plateforme d'échange centralisée, des démarches administratives longues et onéreuses pourraient théoriquement aboutir, bien que souvent entravées par des juridictions étrangères. À l'inverse, dans le cas de l'auto-garde propre au segment Mass Affluent, l'absence de transmission explicite de l'entropie entraîne la perte pure, simple et irréversible du capital.

2.2. La Paralysie du Mandat Notarial et le Blocage de la Masse Successorale

En droit suisse, le notaire est investi de l'obligation légale rigoureuse de dresser un inventaire successoral exhaustif, de garantir la conservation des actifs, et d'exécuter la liquidation du régime matrimonial préalablement au partage définitif. Lorsqu'un défunt laisse un portefeuille numérique formellement identifié mais techniquement inaccessible, l'étude notariale fait face à une paralysie procédurale d'une extrême sévérité.

L'incapacité factuelle d'accéder aux fonds bloque la clôture de l'inventaire et fausse mathématiquement la valorisation de la masse successorale globale. Tant que la valeur exacte, la volatilité et la liquidité de cet actif ne sont pas réglées, le partage de l'intégralité de la succession demeure juridiquement en suspens. Ce blocage contamine le reste du patrimoine, qui peut inclure des portefeuilles de titres traditionnels, des liquidités bancaires et des parcs immobiliers évalués à plusieurs millions de francs.

Les actifs numériques font intégralement partie des biens soumis à la liquidation du régime matrimonial et doivent être intégrés au calcul strict des parts réservataires des héritiers. L'extrême volatilité inhérente à cette classe d'actifs aggrave la complexité du blocage. Si un actif crypto inaccessible connaît une appréciation fulgurante durant la période de latence successorale, il modifie les équilibres patrimoniaux et peut potentiellement léser les parts réservataires d'autres héritiers, exposant l'exécuteur testamentaire et le notaire instrumentant à des litiges intra-familiaux longs et coûteux, fondés sur un calcul erroné des quotités disponibles.

2.3. Le Risque Fiscal, la Responsabilité Fiduciaire et le Gel des Émoluments

Au-delà de la paralysie civile, ce blocage génère un risque fiscal majeur et inéluctable. L'administration fiscale suisse exige la déclaration précise de la valeur vénale de l'ensemble des actifs au jour exact du décès, indépendamment de leur accessibilité pratique pour les hoirs. Si l'existence de l'actif numérique est connue de l'administration cantonale des impôts – par exemple, par le biais d'analyses de traces de virements bancaires antérieurs émis depuis les comptes suisses du défunt vers des plateformes d'échange (*Fiat On-Ramps*) – la taxation successorale sera impitoyablement appliquée. Les héritiers se retrouvent alors contraints d'acquitter un impôt sur un capital virtuellement évalué à plusieurs centaines de milliers de francs qu'ils sont dans l'incapacité de liquider.

Pour l'étude notariale, les conséquences opérationnelles de cette impasse se traduisent par une altération directe et quantifiable de sa rentabilité financière. Le blocage du dossier retarde indéfiniment la clôture de la liquidation et, par voie de conséquence, la facturation finale des émoluments notariaux. L'analyse clinique des barèmes cantonaux démontre que l'enjeu financier

direct pour le notaire sur l'actif numérique en lui-même est marginal. Dans le canton de Genève, par exemple, le règlement sur les émoluments des notaires (REmNot) stipule un taux d'imposition dégressif, facturant un droit proportionnel de 7,5‰ pour une valeur allant jusqu'à 100'000 francs, puis de 5‰ de 100'001 à 200'000 francs.[3] Ainsi, un portefeuille cryptographique isolé et évalué à 100'000 CHF ne génère que quelques centaines de francs d'émoluments directs pour l'étude.

Le véritable levier incitatif, l'accroche commerciale fondamentale justifiant l'intervention d'un expert externe, ne réside donc absolument pas dans la préservation de la valeur nominale de l'actif numérique, mais dans la nécessité absolue de dissoudre le goulot d'étranglement administratif. L'ingénierie de continuité agit comme un solvant procédural : en garantissant un accès irréfutable aux 100'000 CHF numériques, elle assure au notaire que la succession globale de trois millions de francs sera liquidée avec une vélocité optimale, permettant la facturation immédiate de ses honoraires globaux tout en le prémunissant contre toute accusation de négligence fiduciaire.

3. L'Ingénierie de Continuité : Mécanique de la Solution Technique

Face au risque cataclysmique de la mort numérique, l'orientation systématique du client vers des solutions de garde bancaires traditionnelles ou des plateformes de détail s'avère à la fois économiquement irrationnelle et techniquement inadéquate pour la tranche des patrimoines « Mass Affluent ».

3.1. L'Inadéquation Structurelle de l'Offre Centralisée

Les banques dépositaires spécialisées de premier rang (Tier 1), sévèrement régulées par l'Autorité fédérale de surveillance des marchés financiers (FINMA), déploient des modèles d'affaires reposant sur des frais de garde récurrents. Ces frais sont structurellement calculés sur la masse sous gestion (AUM) et oscillent de manière générale entre 0.4% et 0.6% par année. Pour un client détenant un portefeuille numérique de 500'000 CHF, l'externalisation de la sécurité auprès de ces établissements engendre une charge récurrente annuelle de près de 3'000 CHF. Ce modèle impose un coût de possession prohibitif qui érode silencieusement le capital sur le long terme.

En parallèle, les plateformes de détail et courtiers en ligne grand public opèrent sous le modèle de la détention omnibus. Dans cette architecture, les clés privées appartiennent exclusivement à la plateforme, ravalant le client au rang de simple créancier chirographaire. Bien que ces acteurs affichent des tarifs de garde annuels artificiellement bas et souvent plafonnés à des montants dérisoires (environ 200 CHF par an), leur viabilité économique repose sur la ponction

[3] Règlement sur les émoluments des notaires

de marges transactionnelles massives (*spreads*) et de commissions de courtage pouvant atteindre 1% lors de chaque mouvement ou rééquilibrage de portefeuille. Plus critiquement, sous l'angle du droit successoral, ces plateformes centralisées confisquent la souveraineté patrimoniale et imposent des procédures de conformité (*Compliance*) post-mortem opaques, standardisées et d'une lenteur inacceptable, paralysant l'exécuteur testamentaire face à des services juridiques souvent situés hors de la juridiction suisse.

Modèle de Conservation	**Structure des Coûts pour 500k CHF**	**Souveraineté du Client**	**Vélocité de la Succession**
Banque Dépositaire (Tier 1)	~3'000 CHF / an (Récurrent)	Limitée (Risque de contrepartie)	Moyenne (Lourdeur administrative)
Plateforme de Détail (Omnibus)	Frais cachés (Spreads jusqu'à 1%)	Nulle (Le client n'a pas les clés)	Lente (Juridictions étrangères fréquentes)
Ingénierie de Continuité (Auto-garde)	~3'000 CHF (Honoraires uniques)	**Absolue** (Non-Custodial)	**Immédiate** (Contrôlée par le notaire)

La résolution clinique de ce problème réside dans le déploiement d'une architecture de continuité patrimoniale en auto-garde stricte (*Non-Custodial*), tarifée sous la forme d'un honoraire d'ingénierie unique (modèle « One-Off ») facturé entre 2'500 et 3'500 CHF. Face aux rentes perpétuelles des banques dépositaires, le retour sur investissement (ROI) pour le client est mathématiquement irréfutable et s'atteint en moins de 14 mois. Cette ingénierie s'articule autour de deux protocoles cryptographiques avancés, déployés en fonction de la topologie spécifique de la blockchain ciblée.

3.2. Protocole A : L'Architecture du Quorum Multi-Signatures (Multi-sig)

L'architecture Multi-signatures altère fondamentalement le paradigme traditionnel de la signature cryptographique. Au lieu de concentrer le pouvoir sur une clé privée unique (créant un point de défaillance unique ou *Single Point of Failure*), le protocole exige la réunion d'un quorum défini de signatures indépendantes pour valider l'exécution d'un contrat intelligent ou la diffusion d'une transaction sur le registre.

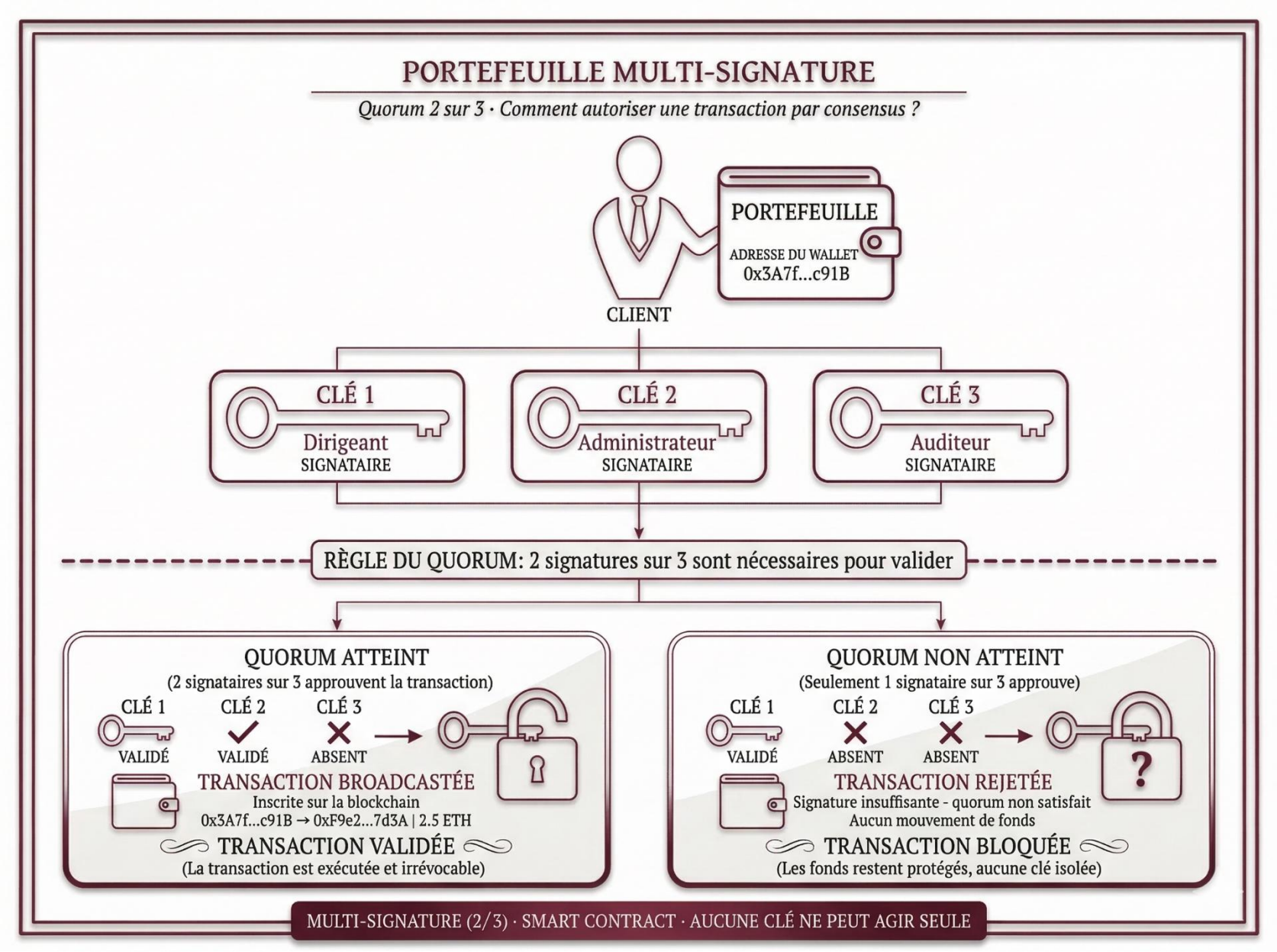
Sur le plan de l'ingénierie, un schéma Multi-sig est défini par un ratio mathématique strict M-sur-N, où N représente la population totale de clés privées distinctes provisionnées par le système, et M représente le seuil minimal de signatures requises pour satisfaire le script cryptographique (par exemple, le standard *Pay-to-Script-Hash* sur le réseau Bitcoin).

Dans le cadre précis de la planification successorale suisse pour la clientèle Mass Affluent, l'infrastructure de référence déployée est un quorum 2-sur-3 ($M = 2$, $N = 3$). La ségrégation des clés est orchestrée avec une granularité juridique stricte :

Entité Dépositaire	Rôle dans l'Architecture de Continuité	Localisation de la Clé Cryptographique	Capacité d'Action Unilatérale
1. Le Client (Testateur)	Détenteur souverain et utilisateur opérationnel du vivant.	Clé 1 (Isolée sur son propre *Hardware Wallet*).	**Nulle**. L'action requiert l'apport de la Clé 2 ou de la Clé 3.
2. L'Étude Notariale	Tiers de confiance institutionnel et exécuteur de la volonté.	Clé 2 (Sur support inaltérable physique scellé au coffre).	**Nulle**. L'action requiert l'apport de la Clé 1 ou de la Clé 3.
3. Le Cabinet	Fournisseur de technologie et clé de	Clé 3 (Générée et conservée dans une	**Nulle**. L'action requiert l'apport de la Clé 1 ou de

d'Ingénierie	recouvrement en dernier recours.	infrastructure hautement sécurisée).	la Clé 2.

Cette topologie asymétrique garantit mathématiquement qu'aucune entité, quelles que soient ses intentions ou son niveau de compromission informatique, ne peut agir seule de manière unilatérale. Du vivant du client, ce dernier conserve un usage fluide de son portefeuille, sachant qu'en cas de sinistre domestique détruisant sa Clé 1, il peut convoquer l'ingénieur (Clé 3) et le notaire (Clé 2) pour initier une procédure de restauration. En cas de décès formellement constaté, l'exécuteur testamentaire (muni de la Clé 2) collabore avec l'ingénieur en continuité (Clé 3) pour transférer le patrimoine vers la masse successorale liquidée. L'utilisation du standard PSBT (*Partially Signed Bitcoin Transactions*) permet à cette transaction d'être signée séquentiellement hors ligne, garantissant que les clés privées ne sont jamais réunies simultanément sur un même équipement connecté.


PORTEFEUILLE MULTI-SIGNATURE
Quorum 2 sur 3 · Comment autoriser une transaction par consensus ?
PORTEFEUILLE
ADRESSE DU WALLET
0x3A7f...c91B
CLIENT
CLÉ 1
Dirigeant
SIGNATAIRE
CLÉ 2
Administrateur
SIGNATAIRE
CLÉ 3
Auditeur
SIGNATAIRE
RÈGLE DU QUORUM: 2 signatures sur 3 sont nécessaires pour valider
QUORUM ATTEINT
(2 signataires sur 3 approuvent la transaction)
CLÉ 1
CLÉ 2
CLÉ 3
VALIDÉ
VALIDÉ
ABSENT
TRANSACTION BROADCASTÉE
Inscrite sur la blockchain
0x3A7f...c91B → 0xF9e2...7d3A | 2.5 ETH
TRANSACTION VALIDÉE
(La transaction est exécutée et irrévocable)
QUORUM NON ATTEINT
(Seulement 1 signataire sur 3 approuve)
CLÉ 1
CLÉ 2
CLÉ 3
VALIDÉ
ABSENT
ABSENT
TRANSACTION REJETÉE
Signature insuffisante - quorum non satisfait
Aucun mouvement de fonds
TRANSACTION BLOQUÉE
(Les fonds restent protégés, aucune clé isolée)
MULTI-SIGNATURE (2/3) · SMART CONTRACT · AUCUNE CLÉ NE PEUT AGIR SEULE

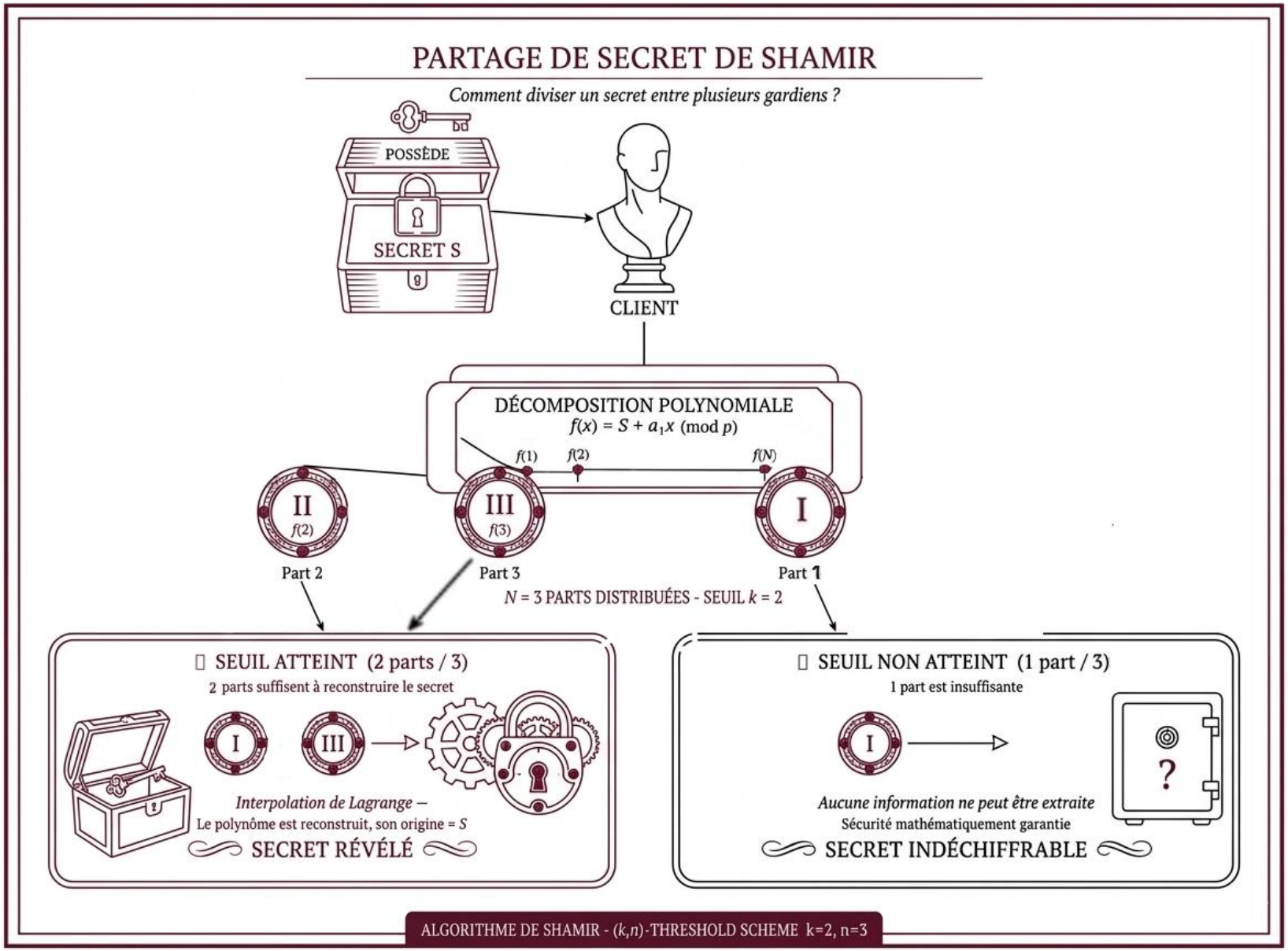
3.3. Protocole B : Le Partage de Secret Cryptographique (Shamir's Secret Sharing)

Certaines infrastructures de registres distribués, en raison de choix architecturaux spécifiques, ne prennent pas en charge le standard Multi-signatures de manière native, ou exigent pour ce faire le déploiement de contrats intelligents coûteux, complexes et potentiellement vulnérables à des failles de code. Face à ces contraintes, l'ingénierie de continuité recourt à un algorithme cryptographique d'une pureté absolue, opéré non pas sur la blockchain, mais directement au niveau mathématique de la clé privée elle-même : le Partage de Secret de Shamir (SSS).

Conçu en 1979 par le cryptographe Adi Shamir, cet algorithme repose sur les propriétés inviolables de l'interpolation polynomiale dans un corps fini. Le théorème postule qu'il faut rigoureusement k points distincts pour définir de manière univoque un polynôme de degré $k-1$ (à l'instar des principes de géométrie euclidienne exigeant deux points pour tracer une ligne droite unique, ou trois points pour définir une parabole singulière). Dans l'exécution de ce protocole, l'entropie originelle (la racine cryptographique de la totalité de la richesse) est mathématiquement encodée comme l'ordonnée à l'origine du polynôme. L'algorithme calcule et génère ensuite N points de coordonnées (les fragments, couramment appelés *shares*) distribués sur cette courbe.

Une erreur dramatique, fréquemment observée dans l'auto-garde amateure (*Shadow Custody*), consiste à fractionner manuellement et de manière littérale une phrase de récupération standard (BIP-39) de 24 mots, en confiant par exemple les 12 premiers mots à un proche et les 12 derniers à un coffre bancaire. Cette méthode empirique détruit instantanément l'intégrité du secret en réduisant l'entropie de manière exponentielle, livrant ainsi la moitié de la clé à d'éventuels attaquants qui peuvent alors reconstituer la totalité de la phrase par une simple attaque de force brute informatique.

L'ingénierie institutionnelle s'interdit formellement ces pratiques et déploie exclusivement le standard SLIP-0039, spécifiquement développé pour appliquer l'algorithme de Shamir à la génération de portefeuilles hiérarchiques déterministes. Contrairement au BIP-39, le standard SLIP-0039 génère des fragments de 20 ou 33 mots qui intègrent leur propre vérification cryptographique. La caractéristique fondamentale et inégalable de l'algorithme de Shamir est sa sécurité parfaite du point de vue de la théorie de l'information : la possession de $k-1$ fragments (soit un fragment de moins que le quorum minimal requis) ne révèle absolument aucune information calculable, probabiliste ou statistique sur le secret original. Le patrimoine demeure cryptographiquement inviolable jusqu'à la seconde précise où le quorum exact est réuni par les héritiers, sous la supervision formelle et procédurale du notaire instrumentant.


PARTAGE DE SECRET DE SHAMIR
Comment diviser un secret entre plusieurs gardiens ?
POSSÈDE
SECRET S
CLIENT
DÉCOMPOSITION POLYNOMIALE
$f(x) = S + a_1 x \pmod p$
f(1)
f(2)
f(N)
II
f(2)
III
f(3)
I
Part 2
Part 3
Part 1
N = 3 PARTS DISTRIBUÉES - SEUIL k = 2
SEUIL ATTEINT (2 parts / 3)
2 parts suffisent à reconstruire le secret
I
III
Interpolation de Lagrange –
Le polynôme est reconstruit, son origine = S
SECRET RÉVÉLÉ
SEUIL NON ATTEINT (1 part / 3)
1 part est insuffisante
I
?
Aucune information ne peut être extraite
Sécurité mathématiquement garantie
SECRET INDÉCHIFFRABLE
ALGORITHME DE SHAMIR - (k,n)-THRESHOLD SCHEME k=2, n=3

3.4. Hygiène "Air-Gapped" et Sélection de l'Architecture Matérielle

L'exécution de ces algorithmes d'une sensibilité extrême exige un environnement informatique de niveau laboratoire, absolu, stérile et incorruptible. L'usage de machines généralistes (ordinateurs personnels, smartphones) connectées aux réseaux de télécommunications, sujettes aux logiciels malveillants (*Malwares*), à l'extraction de mémoire vive et aux failles de systèmes d'exploitation riches, est proscrit de manière catégorique. L'architecture s'appuie de manière exclusive sur des dispositifs matériels dédiés (*Hardware Wallets*) opérant selon le dogme du « Air-Gapped » (une déconnexion physique totale de toute interface réseau, Bluetooth ou Wi-Fi).

L'évaluation clinique menée par le cabinet d'ingénierie restreint le choix à des dispositifs éprouvés face aux vecteurs d'attaques physiques et distants, tels que la BitBox02 ou le Keystone 3 Pro.

Dispositif Matériel	**Architecture de Sécurité**	**Mécanisme d'Isolation (Air-Gap)**	**Protection Anti-Exfiltration**
BitBox02 (Manufacturé en Suisse)	Dual-Chip (Microcontrôleur ATSAMD51J20A + Puce Secure Element ATECC608B).	Filaire (USB-C) avec communication chiffrée (*Noise Protocol*) bloquant l'interception.	Protocole *Anti-Klepto* (mitigation des fuites de clés par manipulation malveillante du Nonce).
Keystone 3 Pro	Triple Secure Element (Puces de sécurité isolées, certification de grade militaire EAL6+).	Strictement Air-Gapped (Absence de port de données USB, communication exclusive par QR codes).	Mécanismes d'autodestruction physique (*Anti-tamper*) et architecture PSBT transparente.

Ces dispositifs bénéficient de micrologiciels (*Firmwares*) 100% Open-Source, soumis à des audits tiers rigoureux et permettant des compilations reproductibles (*Deterministic Builds*), garantissant à l'ingénieur que le code source publié correspond à l'octet près au code exécuté sur la machine, excluant ainsi l'introduction de toute porte dérobée (*Backdoor*) lors de la chaîne de fabrication.

4. Le Bouclier Légal et la Ségrégation des Risques

L'intégration d'un prestataire technologique externe dans le traitement juridique de successions financières complexes sur l'arc lémanique ne peut se réaliser sans une définition clinique, transparente et irréfutable des responsabilités légales. La thèse centrale de l'ingénierie de continuité affirme que le cabinet technique s'extrait totalement de la régulation financière lourde grâce à la démonstration mathématique incontestable de son incapacité d'action.

4.1. L'Exemption LBA et le Dogme Absolu du « Verfügungsmacht »

Le droit suisse, par le biais de la Loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (LBA), impose des contraintes de diligence particulièrement lourdes, chronophages et onéreuses (identification formelle KYC, documentation AML, audits externes réguliers) à quiconque revêt la qualité d'« intermédiaire financier ». La frontière juridique définissant l'assujettissement à cette loi, telle qu'interprétée par la doctrine et la jurisprudence de l'Autorité fédérale de surveillance des marchés financiers (FINMA), réside dans un critère matériel absolu : la détention du pouvoir de disposition effectif, ou *Verfügungsmacht*.[4]

Le *Verfügungsmacht* désigne la capacité technique, factuelle et unilatérale pour une entité d'initier un transfert de la valeur patrimoniale vers un tiers, et ce, indépendamment du droit de propriété civil sous-jacent. L'importance matricielle de ce concept a été entérinée lors de l'adoption de la Loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués (Loi DLT) en 2021.[5] Cette législation a modifié la Loi fédérale sur la poursuite pour dettes et la faillite (LP) en y introduisant l'article 242a, clarifiant le statut des actifs numériques en cas d'insolvabilité d'un prestataire.

Le Message du Conseil fédéral et les communications de la FINMA (notamment la communication 01/2026 et 08/2023) précisent de manière univoque que si une entité ne dispose pas d'un pouvoir de disposition effectif et exclusif sur les clés privées (par exemple, parce qu'elle ne détient qu'un seul fragment inopérant), l'actif numérique n'est pas réputé être en sa possession ni sous sa garde. Dès lors, l'actif peut être légalement distrait (*segregated*) et n'entre

[4] Communication FINMA 01/26, Rapport CF Blockchain
[5] Loi DLT

pas dans la masse en faillite du prestataire.[6]

Par une analogie stricte validée par le régulateur suisse, ce critère de la LP s'applique à la détermination de l'assujettissement à la LBA : si un prestataire ne dispose pas d'un pouvoir de disposition effectif et exclusif permettant de mouvoir les fonds de manière autonome, il ne « conserve » pas la valeur patrimoniale et n'« aide pas à la transférer » au sens de la loi.

Les démonstrations mathématiques abordées à la section précédente garantissent structurellement cette absence de *Verfügungsmacht* :

- **Dans le cadre de l'architecture Multi-sig :** La cryptographie sous-jacente au réseau blockchain rejettera systématiquement et inexorablement toute transaction ne présentant pas au minimum les deux signatures valides requises par le quorum. Le cabinet d'ingénierie, ne détenant physiquement et mathématiquement qu'une seule clé de secours sur les trois existantes, possède un pouvoir de disposition strictement égal à zéro. Il lui est cryptographiquement impossible de forger la signature manquante.
- **Dans le cadre du protocole de Shamir :** La cinématique d'intégration impose que le prestataire ne génère l'entropie qu'en présence du client, s'assurant que les fragments générés soient immédiatement dispersés (client, coffre bancaire, étude notariale) sans en conserver la moindre copie complète. En outre, la mémoire vive de l'équipement est cryptographiquement purgée (*Zeroization*) à l'issue de l'opération.

L'impossibilité d'une collusion ou d'un détournement unilatéral étant ainsi scellée par les mathématiques du protocole, le cabinet d'ingénierie n'intervient qu'en qualité de fournisseur de technologie neutre (*Technology Provider*). Il s'extrait techniquement de la chaîne de signature et échappe totalement à l'assujettissement à la LBA ainsi qu'à la surveillance prudentielle de la FINMA. Cette démonstration constitue le bouclier juridique suprême garantissant à l'étude notariale prescriptrice que le déploiement de cette solution n'engage aucune faille de conformité réglementaire susceptible d'éclabousser son mandat.

4.2. L'Immunité face à la LSFin et la Rigueur de l'Agnosticisme Financier

Afin de préserver l'étanchéité de ce bouclier juridique vis-à-vis de la clientèle de particuliers, il est impératif d'écarter tout risque de requalification de l'intervention en « conseil financier », une activité lourdement encadrée par la Loi sur les Services Financiers (LSFin). La LSFin exige que quiconque émette des recommandations personnalisées sur l'achat, la vente, la détention ou l'allocation d'instruments financiers s'inscrive à un registre des conseillers, documente des formations continues et s'affilie à un organe de médiation.

[6] Consulter la jurisprudence

La neutralisation juridique de ce risque repose sur la standardisation rigoureuse et contractuelle de la prestation. L'intervention de l'architecte en sécurité de l'information est exclusivement cantonnée à l'ingénierie des systèmes et au maintien de la continuité d'accès, excluant avec la plus grande fermeté toute incursion dans l'ingénierie financière.

Le mandat liant l'ingénieur au client stipule explicitement que :

1. L'expert ne fournit aucune recommandation ni opinion sur la pertinence de l'allocation du portefeuille (par exemple, il ne s'exprime jamais sur la pondération stratégique entre le Bitcoin, l'Ethereum ou des stablecoins).
2. L'expert n'assiste en aucun cas le client dans l'exécution opérationnelle de transactions sur les plateformes de marché (*Trading* ou *Swapping*).
3. Le livrable technique fourni (le Classeur de Plan de Continuité) est constitué de Procédures Opératoires Standards (SOP) strictement agnostiques quant à la nature des jetons cryptographiques hébergés par le client.

En documentant formellement ces limitations, la qualification de prestataire de services financiers est juridiquement invalidée, consolidant le statut exclusif d'expert indépendant en sécurité des données de registre distribué.

4.3. Ségrégation des Risques et Responsabilité Technologique (Obligation de Moyens)

Notre cabinet intervient exclusivement en qualité d'architecte de systèmes d'information, déployant une infrastructure dont la sécurité repose sur les mathématiques et non sur la confiance. En vertu de notre architecture strictement « Non-Custodial », nous ne détenons à aucun moment le pouvoir de disposition effectif (*Verfügungsmacht*) sur les actifs numériques de nos mandants.

Cette impossibilité structurelle et cryptographique d'interagir unilatéralement avec les fonds rend conceptuellement obsolète le recours à une police d'assurance financière spécialisée. On n'assure pas un risque de détournement qui a été éliminé à la source par l'ingénierie. Par conséquent, notre prestation technique n'inclut aucune couverture d'assurance tierce portant sur la valeur fluctuante ou la perte accidentelle du sous-jacent cryptographique.

Notre modèle de continuité ne s'articule pas autour d'une illusoire promesse de dédommagement financier, mais garantit l'inviolabilité algorithmique du protocole livré au jour de son déploiement. Conformément aux dispositions impératives de l'Article 100 du Code des obligations suisse (CO), notre engagement contractuel se limite à une obligation de moyens techniques. Notre responsabilité civile est expressément et irrévocablement plafonnée au strict remboursement des honoraires d'ingénierie facturés, sous la seule réserve légale du dol ou de la faute grave dûment prouvée.

Le testateur, en assumant la souveraineté absolue et intransmissible inhérente à l'auto-garde (Self-Custody), endosse l'intégralité du risque financier post-déploiement. Cette compartimentation clinique et asymétrique des risques protège formellement l'étude notariale prescriptrice : elle garantit au notaire l'absence totale de responsabilité solidaire liée à la volatilité des marchés ou aux potentielles failles d'hygiène numérique du client.

5. L'Intégration Opérationnelle : La Mécanique Clinique de la Résilience

Pour qu'un mandat forfaitaire de résolution successorale s'intègre harmonieusement dans les processus chronométrés du notariat lémanique tout en générant un taux horaire viable pour le prestataire, la prestation ne souffre d'aucune improvisation. L'exécution opérationnelle requiert une précision chirurgicale et une standardisation militaire à chaque étape. L'ingénierie, bien qu'extrêmement complexe, doit devenir transparente et invisible pour le client, et fluidement intégrée pour le juriste.

5.1. Phase 1 : Le "Pre-Provisioning" en Laboratoire Stérile

Afin de compresser au maximum le temps d'intervention physique au domicile du client et d'éliminer drastiquement les vecteurs d'attaque environnementaux, l'intégralité de la phase d'initialisation technologique est reléguée et exécutée dans le laboratoire stérile du cabinet d'ingénierie. Ce protocole préalable, qualifié de *Pre-Provisioning*, observe une série d'étapes impitoyables :

1. **Inspection de la Chaîne d'Approvisionnement (*Supply Chain*) :** Le matériel est commandé en direct auprès des manufactures de sécurité. À la réception, les dispositifs sont inspectés sous scellés. L'intégrité absolue des emballages de sécurité inviolables (*Tamper-evident bags*) est vérifiée sous lumière spécifique afin d'écarter toute suspicion de compromission matérielle en transit (*Interdiction Attack* opérée par l'interception et la modification d'un colis).
2. **Attestation Cryptographique et Flashage du Firmware :** C'est l'étape la plus névralgique du processus de durcissement. Le dispositif subit une vérification d'authenticité cryptographique de l'appareil (via la clé *Device Attestation Key*) lors de son premier branchement au sein du laboratoire. Par la suite, le micrologiciel est mis à jour. Cette opération ne doit jamais être effectuée sur un réseau Wi-Fi incertain chez le client. L'ingénieur télécharge le code source officiel, calcule les signatures cryptographiques (SHA-256 Checksums) et garantit que celles-ci correspondent formellement aux clés publiques des développeurs certifiés. Ce processus assure que le firmware installé est mathématiquement garanti sans altération ou composant malveillant de type *Backdoor*.
3. **Durcissement Matériel Extrême (*Hardening*) :** Le dispositif est configuré pour opérer avec la surface d'attaque la plus restreinte possible. Les modules de communication secondaires et non essentiels sont impitoyablement désactivés (désactivation matérielle

du module Bluetooth, forçage des protocoles de communication par lecture optique de QR codes ou via transfert par carte MicroSD isolée) pour préparer le dispositif à un usage strictement *Air-Gapped*.

5.2. Phase 2 : La "Key Ceremony" (Cérémonie des Clés)

La « Key Ceremony » désigne l'intervention physique, menée sur site, consacrée à l'acte fondateur de la transmission patrimoniale : la génération, la sauvegarde et la fragmentation de l'entropie. Cette cérémonie est un processus chorégraphié, didactique pour le client, et exécuté dans un isolement réseau absolu.

Sous la supervision technique étroite de l'ingénieur, mais opéré physiquement par le client pour garantir le principe du *Verfügungsmacht*, le dispositif utilise son générateur de nombres aléatoires véritable (TRNG) pour générer la racine cryptographique de la richesse. Pour pallier la vulnérabilité désastreuse du papier face aux éléments domestiques (incendies, dégâts d'eau, encre s'effaçant avec le temps), les éléments cryptographiques (que ce soient les fragments polynomiaux de l'algorithme de Shamir ou les graines de récupération du schéma Multi-sig) ne sont jamais imprimés. L'ingénieur met à disposition des gabarits de frappe industriels et des plaques de titane résistant à des températures extrêmes (jusqu'à 1'600°C) et à la corrosion. Sous un contrôle visuel absolu, l'empreinte cryptographique y est poinçonnée de manière indélébile.

Afin de mitiger le risque critique d’erreur humaine lors de la frappe physique de l’entropie sur les supports de titane, le protocole de Maillard Custody impose une phase de validation mathématique immédiate, dite "Dry-Run".

Une fois l’empreinte cryptographique matérialisée par le client sur ses plaques de titane, l’appareil de génération est réinitialisé ("Wiped") à l’état d’usine. Le client procède alors à une tentative de restauration complète de l’accès à partir de ses plaques de titane nouvellement frappées. Cette procédure, observée par l’ingénieur sans accès aux informations sensibles, permet de certifier l’exactitude de la sauvegarde physique avant le scellage fiduciaire des fragments. Cette étape clé convertit l'obligation de moyens de l’ingénieur en une validation de résultat opératoire pour le dispositif de continuité.

Une fois matérialisés, ces éléments physiques entrent dans la cinématique de ségrégation. Les fragments ou les sauvegardes électroniques chiffrées sur cartes MicroSD sont immédiatement introduits dans des enveloppes de sécurité inviolables et numérotées, scellées de manière indétectable en cas de manipulation. Le client organise instantanément la dispersion de ces enveloppes vers les coffres forts désignés et l'étude notariale, rompant ainsi tout point de défaillance géographique unique.

L'étape ultime, validant juridiquement l'absence de garde par le prestataire, consiste en la

stérilisation cryptographique (*Zeroization*). L'équipement informatique ayant facilité la configuration et la mémoire vive (RAM) des dispositifs de transfert sont purgés selon les standards militaires de destruction de données. Aucune trace numérique persistante, aucune photographie et aucun cache logiciel de l'entropie ne subsiste au sein du cabinet d'ingénierie.

5.3. Le Livrable Institutionnel : Le Classeur de Plan de Continuité

L'achèvement du processus d'intégration opérationnelle se concrétise par la compilation et la remise automatisée d'un livrable à haute valeur ajoutée : le Classeur de Plan de Continuité. Ce document institutionnel, massif dans son apparence mais hautement optimisé dans sa production via l'injection dynamique de variables, constitue le trait d'union fondamental entre la technique brute et l'acte juridique notarié.

Il rassemble l'ensemble des Procédures Opératoires Standards (SOP) agnostiques destinées à guider pas à pas les héritiers, ignorant sciemment toute mention de conseil financier pour asseoir le bouclier LSFin. Surtout, ce classeur centralise les identifiants séquentiels des enveloppes scellées et les clés publiques étendues (*xpub*). L'intégration de la clé publique étendue (*xpub*) est une fonctionnalité d'audit d'une puissance déterminante pour l'exécuteur testamentaire : elle lui confère la capacité mathématique de reconstituer l'historique complet des transactions et de réaliser un audit comptable en lecture seule (*Read-only*) de la valorisation exacte de la masse successorale à la seconde près, sans jamais posséder la capacité cryptographique de dépenser ou de mouvoir les fonds.

Muni de ces éléments techniques traduits dans un langage procédural clair, le notaire est en mesure d'intégrer officiellement et sereinement ces actifs autrefois « invisibles » dans la planification globale de la succession. Il rédige les codicilles appropriés, formalise les conventions de dépôt fiduciaire et clôture son inventaire avec certitude. L'intervention transforme de facto une menace d'opacité irréversible et un potentiel litige successoral en un dossier patrimonial documenté, sécurisé par des protocoles mathématiques asymétriques, et prêt à être liquidé avec la même fluidité, la même prévisibilité juridique et la même rentabilité que l'immobilier traditionnel.

6. Conclusion

L'omission persistante d'une gouvernance technologique rigoureuse entourant la détention d'actifs numériques auto-gérés par le segment « Mass Affluent » expose les études notariales de Suisse romande à un risque systémique majeur. La « mort numérique » d'un testateur, en opposant le mur mathématique de la cryptographie aux prérogatives du droit civil, paralyse l'inventaire, bloque la liquidation du régime matrimonial, fausse dramatiquement le calcul des parts réservataires et gèle indéfiniment la facturation des émoluments notariaux.

Tenter de contourner ce risque en incitant la clientèle à déléguer la garde de son patrimoine numérique à des acteurs bancaires institutionnels ou à des plateformes de détail se heurte frontalement aux contraintes économiques d'un capital plafonné. Cette démarche, onéreuse et lente, pénalise financièrement l'investisseur tout en le dépossédant de sa souveraineté patrimoniale souveraine.

L'ingénierie de continuité patrimoniale, déployée selon des protocoles cryptographiques d'une rigueur clinique (Quorum Multi-signatures, Partage de Secret de Shamir sur des infrastructures matérielles strictement *Air-Gapped*), s'impose comme la seule réponse holistique à cette équation complexe. En prouvant l'impossibilité mathématique absolue d'exercer un pouvoir de disposition effectif (*Verfügungsmacht*), l'architecture garantit au prestataire l'exemption légale aux exigences pesantes de la LBA (qualification de *Technology Provider*). Elle autorise dès lors le notariat à se décharger de l'exhaustivité du risque technologique sur un partenaire couvert par une assurance responsabilité civile professionnelle suisse spécifique, tout en préservant pour l'étude l'exclusive souveraineté de la rédaction, du conseil fiduciaire et de la facturation juridique de l'acte. L'impasse technologique est ainsi définitivement métamorphosée en un processus procéduralement sain, sécurisé et immédiatement facturable.

Nous invitons les associés d'études notariales et les cabinets d'avocats d'affaires de l'arc lémanique à nous contacter pour une évaluation factuelle de l'intégration de ce protocole de sécurité et de continuité au sein de l'architecture de leurs mandats successoraux en cours, spécifiquement pour la tranche des patrimoines « Mass Affluent ».

7. Bibliographie & Références Institutionnelles

1. **Lois, Règlements et Jurisprudence**

- **Conseil fédéral suisse**, *Message relatif à l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués (TRD)*. Lien officiel Admin.ch.
- **République et canton de Genève**, *Règlement sur les émoluments des notaires (REmNot)*, rsGE E 6 05.03. Lien officiel SIL Genève.
- **Tribunal cantonal (Fribourg)**, *Cour d'appel civil : Arrêt du 4 avril 2025* (Dossier 101_2024_217). Consulter la jurisprudence.

2. **Directives Réglementaires et Rapports Officiels**

- **Autorité fédérale de surveillance des marchés financiers (FINMA)**, *Communication FINMA sur la surveillance 01/2026*. Consulter le document FINMA.

- **Conseil fédéral suisse,** *Rapport sur les monnaies virtuelles* (Rapport CF Blockchain). *Consulter le rapport.*

3. **Études de Marché et Académiques**

- **Université de Lucerne (HSLU)**, *IFZ FinTech Study 2026 - An Overview of Swiss FinTech*. Consulter l'étude.

- **Université de Lucerne (HSLU)**, *IFZ FinTech Study 2022 - An Overview of Swiss FinTech*, édité par SIX Group. Consulter l'étude.

4. **Documentation d'Assurance et Doctrine**

- **Zurich Compagnie d'Assurances SA**, *Conditions : Responsabilité civile professionnelle pour les prestataires technologiques*. Consulter les conditions.

- **Baloise Assurance**, *Assurance responsabilité civile d'entreprise pour les prestataires de services informatiques* (CGA 230). Consulter le document.

- **Legal-Testa (Cabinet)**, *Inclure ses crypto-actifs dans son testament en Suisse*. Lire l'article.