Aristhor.com

🤝 Nous ne sommes riches que de nos amis.

Blockchains de témoignages

Merci à François Ragolski - Champion du monde de voltige en parapente

v1.0 – Mai 2026

 Préambule

- Découvrez les avantages de la Blocksthor d'Aristhor : une blockchain spécialement conçue pour les témoignages de tout type.
- Les sujets centraux : la **confiance** et la **vérité des faits**. Comment les propager grâce à nos proches et un peu de technique ?

🎯 Un objectif clair

- Contrer la falsification et dissiper le doute !
- Comment ?

  👉 Grâce à vos garants. A savoir votre réseau de famille, amis, collègues, voisins, etc., attestant de faits vérifiés.
- *Décentralisation et indépendance garanties.*

🧞‍♂️ Combien de temps pour dissiper un doute ?

- … juste 1 minute !
- Comment ?

  👉 Grâce à votre blocksthor, vos garants apparaissent avec leurs signatures vérifiables sur un fait précis.

- *Mode hors connexion possible.*

Sommaire des parties

Introduction

🤔 Comment « certifier » …

- … une vidéo, une photo, un tweet, un post, un accord, un contrat, une reconnaissance de dette, une tromperie commerciale, etc., TOUS EFFACÉS ou FALSIFIÉS ?
- … une figure acrobatique en parapente tellement incroyable que tout le monde pense que la photo a été créée par IA ?
- … la découverte récente d'un jumeau ?

Que faire quand St Thomias ne croit plus ce qu'il voit, ni ce qu'il entend… ?

Introduction

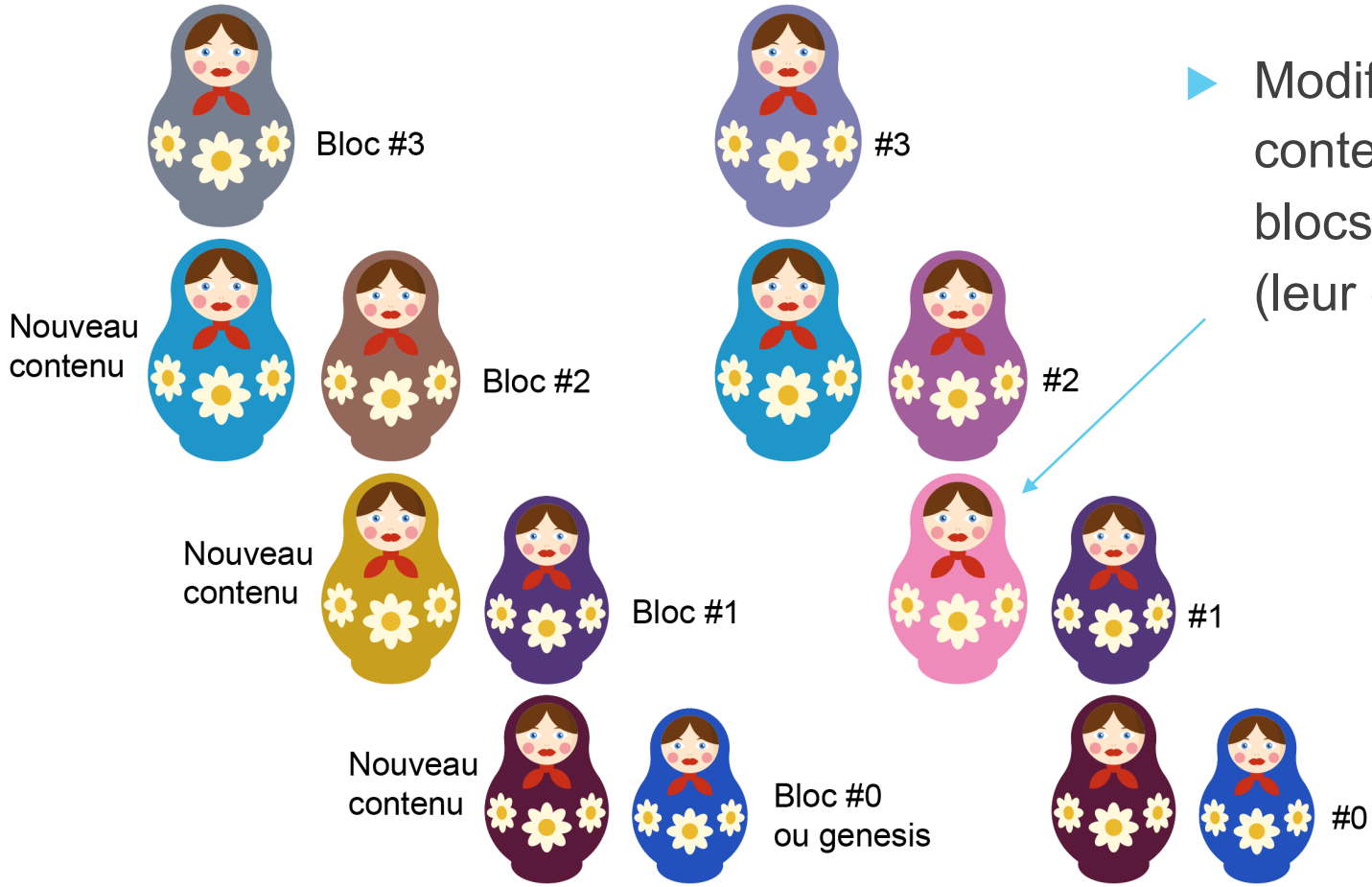
🤔 Sortir du doute ?

Tout le monde a entendu ces propos dubitatifs :

- C’est toi qui le dis donc c’est parole contre parole…
- Tu as mal lu ou mal compris…
- Ce n’est plus en ligne, tu ne peux donc pas prouver que cela y était…
- Ok tu as une capture d’écran mais tu as pu la falsifier avec un logiciel… ou à l’aide de l’IA…
- Ok, cela ressemble à sa voix mais l’IA génère n’importe quelle voix…

Introduction

Un aperçu du principe de la blockchain



- Modification du seul contenu n°2 et tous les blocs suivants sont modifiés (leur couleur change)

ARISTHOR

1ère partie

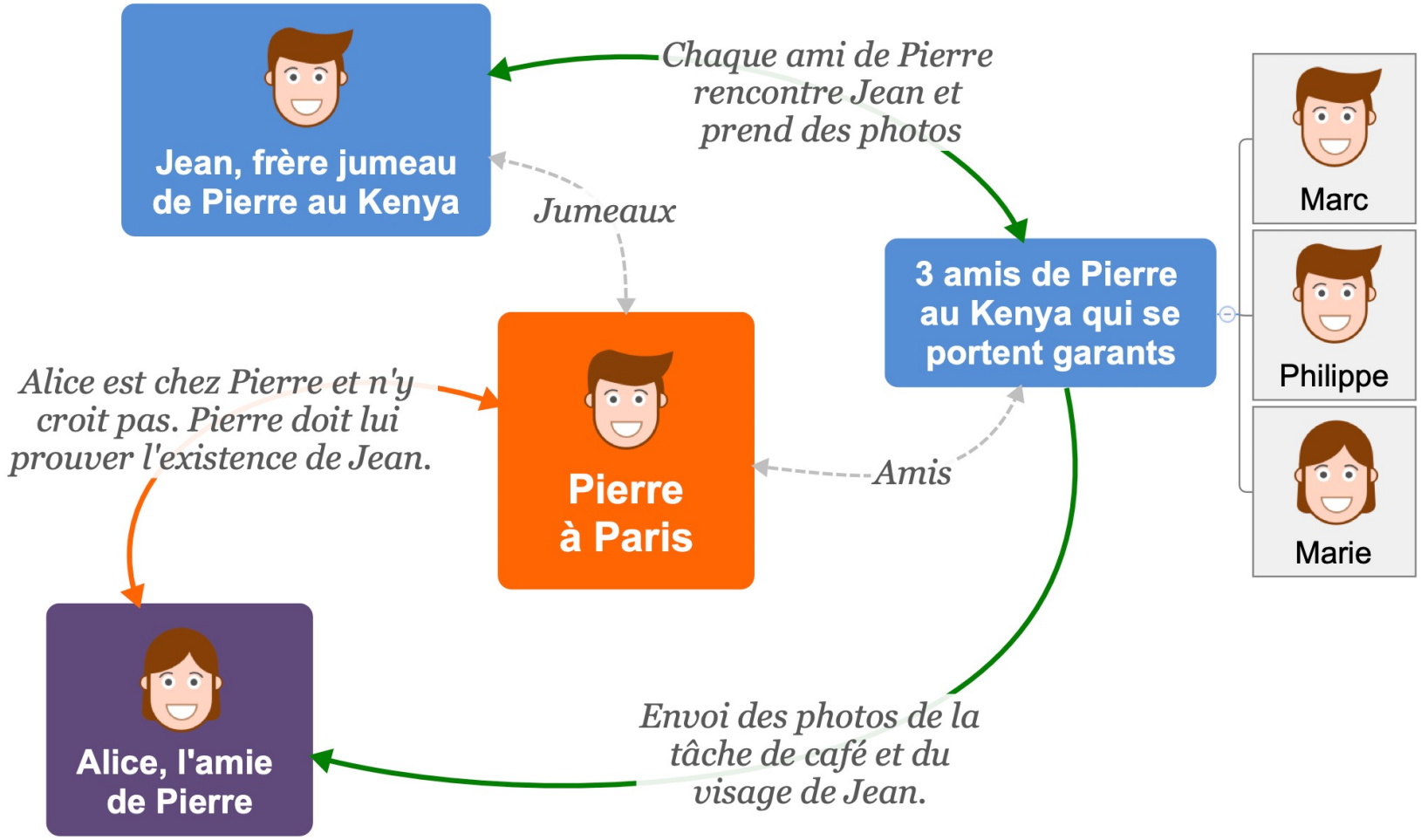
🤔 Comment certifier un fait peu probable SANS blocksthor…

- Ex : comment prouver à sa compagne l'existence d'un vrai jumeau ?

  … découvert par hasard, 35 ans plus tard, en Afrique !

1.1. 🧐 Attestons d'un jumeau SANS blockstho r !

Tâches de café et visages identiques…



ARISTHOR

1.2.😛 Processus pour convaincre Alice…

- Signatures manuscrites des photos par les amis de Pierre.
- Envois directs des photos à Alice par les trois garants.
- Alice comparera et comprendra que Pierre a bien découvert qu’il a un vrai jumeau en Afrique.

ARISTHOR

1.3.😉 Contrainte technique

Alice veut que les garants de Pierre envoient leurs photos sur son email …

- … mais la boite mail d'Alice est en déni de service aujourd'hui !
- Et demain Alice sera dans une zone blanche hors réseau…
- Dommage, Pierre a les photos mais comment prouver qu'il ne les a pas fabriquées lui-même…🤷

ARISTHOR

1.4.🤥 Fraude de Pierre et ses garants

- Aucun système n’empêche le mensonge.
- Pierre et ses garants peuvent envoyer de fausses photos mais leur réputation sera entachée.

En tout cas, des tâches de café et des visages identiques constituent une EMPREINTE d'un patrimoine génétique commun. Cette « empreinte » est indiscutable contrairement à une description d’un individu.

1.5. 👺 Piratage

- Pour des raisons inconnues, des tiers souhaitent cacher l’existence de ce jumeau durant au moins 72 heures. Des cyber-pirates sont activés.
- La boite mail d’Alice est infiltrée. Les photos faites par les garants sont interceptées et supprimées.
- Sans nouvelle des garants, Alice doute maintenant de l’équilibre psychique de Pierre…

1.6.☀ Inconvénients !

- Les garants de Pierre doivent transférer de lourdes photos à Alice. Outre le gaspillage énergétique, il faut que le réseau permette ces transferts volumineux (photos, vidéos...)
- Les garants doivent conserver durablement de lourds fichiers pour pouvoir convaincre d'autres amis de Pierre.
- Les photos peuvent être interceptées, supprimées ou falsifiées et il n'y a pas de moyen simple de s'en rendre compte.
- Pierre ne peut pas utiliser le jeu de photos déjà reçu de ses garants car il ne peut pas prouver leur non-falsification.
- Les garants doivent signer « manuscritement » les photos envoyées. S'ils mentent il n'y a pas de processus dissuasif entachant largement leur réputation.

🍀 Les 2 composants phares de la blockchain

- Avant de comprendre le fonctionnement d'une blockchain, découvrons les deux composants phares de toute blockchain : l'**empreinte** cryptographique et la **signature** numérique.

2e partie

🤔 C’est quoi une empreinte cryptographique ou « hash » en anglais ?

- L’empreinte cryptographique « condense » n’importe quelle donnée numérique, de toute taille, en une chaine de caractères toujours unique et de longueur fixe. La chaîne a le plus souvent 64 ou 128 caractères hexadécimaux*
- L’empreinte ne sert pas que dans les blockchains.

** Les caractères hexadécimaux sont les 16 caractères suivants : 0 à 9 et A à F.*
Ex : EE26B0DD4AF7E7…

2.1.🤯 Des milliards de milliards de milliards de…

- La fonction de hachage SHA-512 totalise des milliards de milliards de […] de possibilités d'empreintes… 2^{512} possibilités exactement.
- Aucune « collision* » n'a jamais été trouvée.
  ** Collision : deux données numériques différentes aboutissant à la même empreinte.*

Une preuve de fiabilité : le « hashrate » ou taux global de hachage se situe autour de 1 milliard de milliards d'empreintes calculées à chaque seconde juste pour le réseau Bitcoin en SHA-256 (2^{256} possibilités)

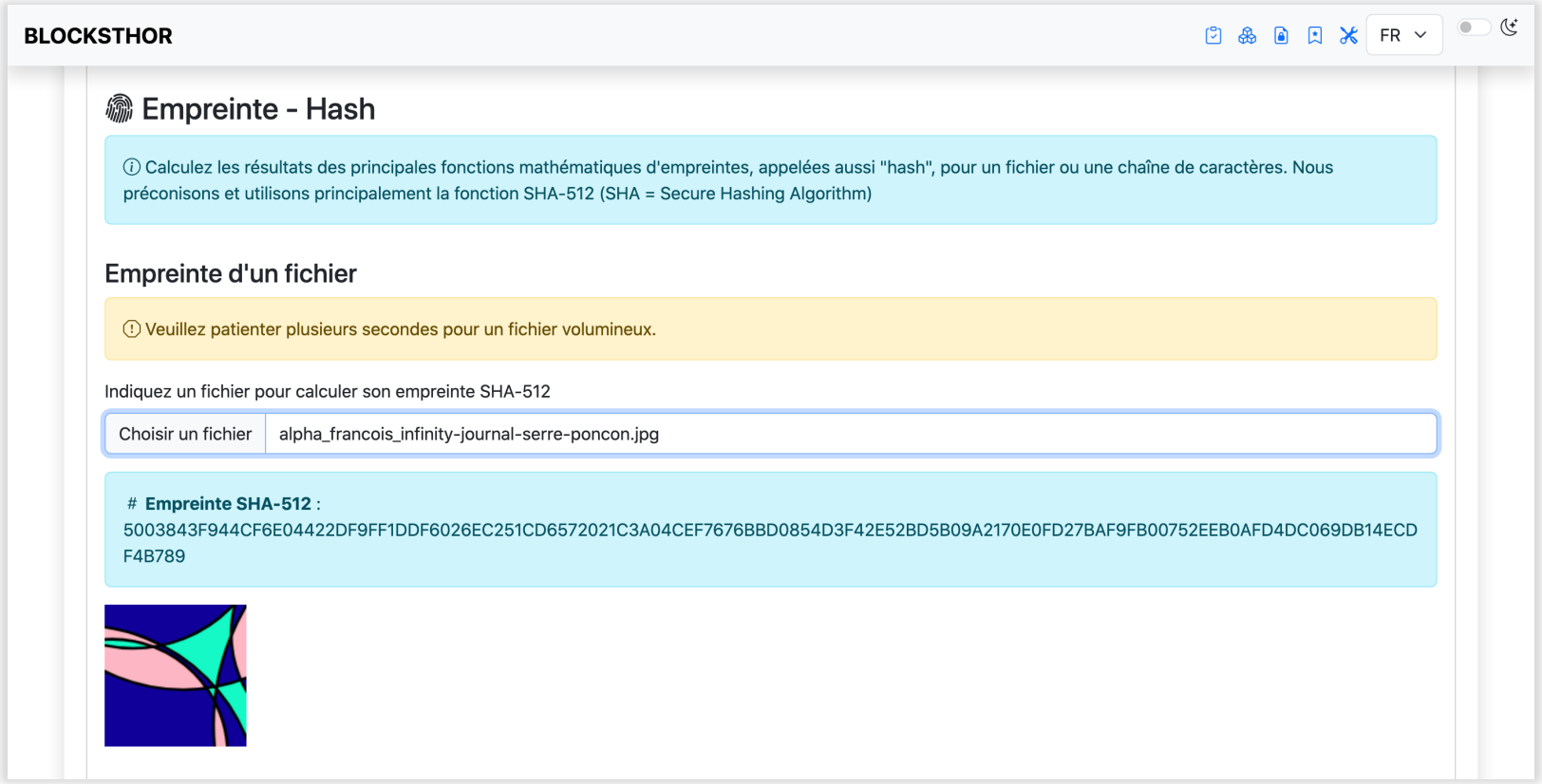
ASIC Bitmain Antminer S23 Hyd. - 580 Th/s …

2.2.🙃 Calcul de l’empreinte de cette photo

Au fait, vraie ou fausse… cette photo au-dessus du lac de Serre-Ponçon ? 🤔

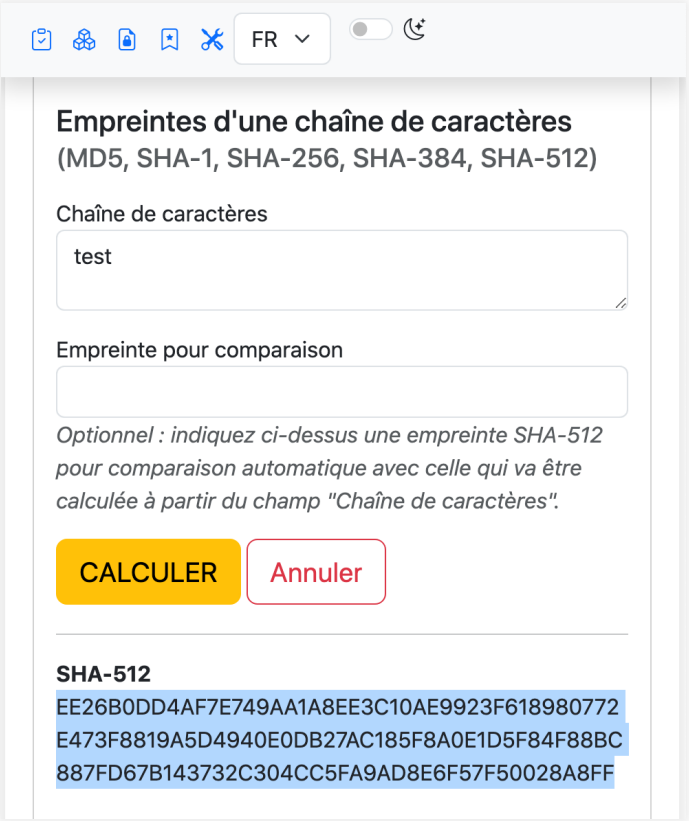
2.3.🙃 Empreinte de cette photo de parapente

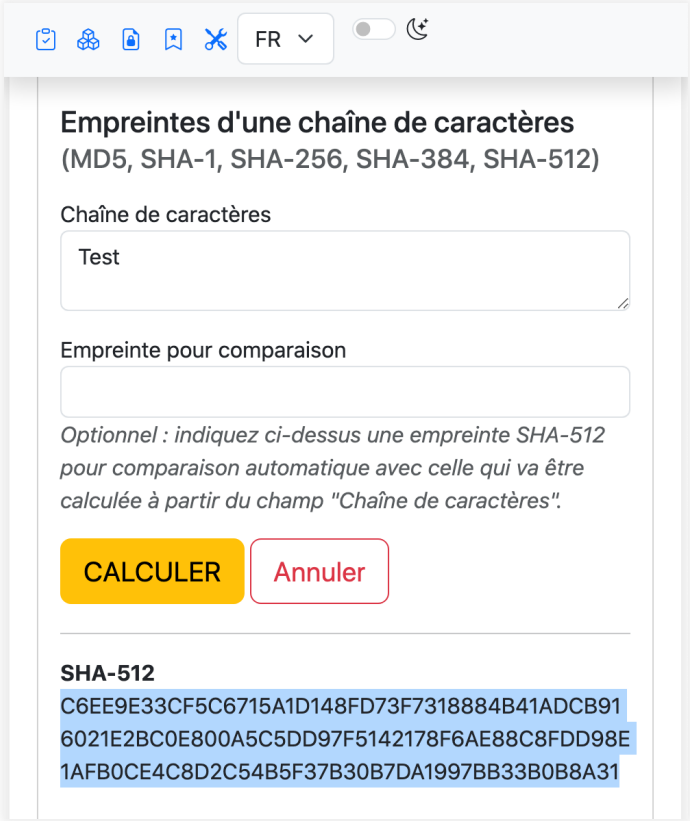
Calculons ensemble l'empreinte de cette photo de parapente « à l'envers » dont le nom de fichier est alpha_[...].jpg avec la fonction de hachage SHA-512.



2.4.🤔 Un changement mineur et tout change !

- Calcul de l'empreinte SHA-512 du mot « test » puis « Test ». Seule change la 1ère lettre mise en majuscule, or toute l'empreinte change !





ARISTHOR

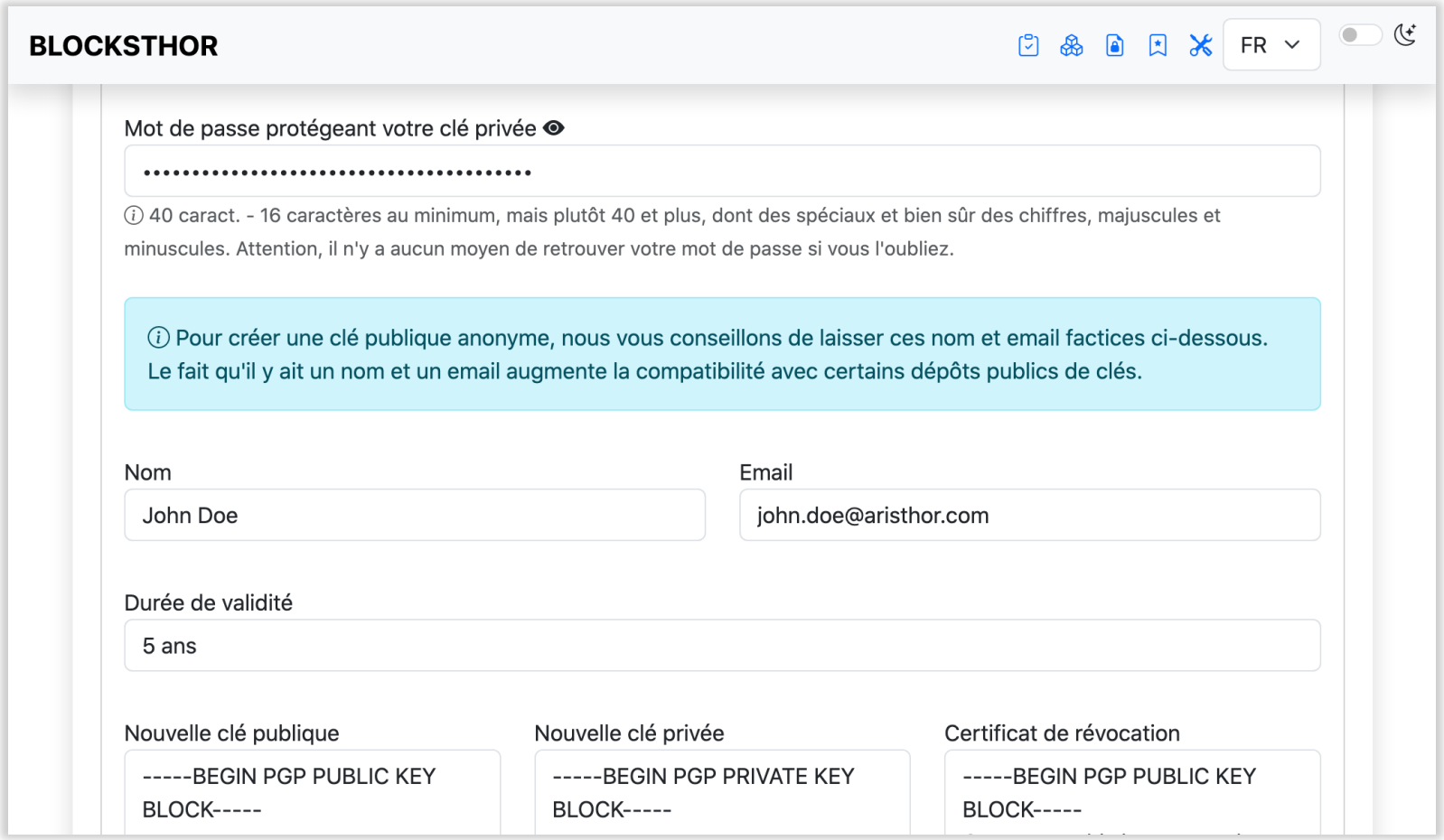
3e partie

🤔 C’est quoi une signature numérique ?

- Même idée que la signature manuscrite mais basée sur la cryptographie asymétrique. Il faut deux « clés », **une clé privée** à garder privée… et une clé publique distribuable à tous.
- **La clé privée permet de signer**. La clé publique permet de vérifier la validité de la signature.
- Le Blocksthor Maker et aristhor.com vous font tout le travail. 😇

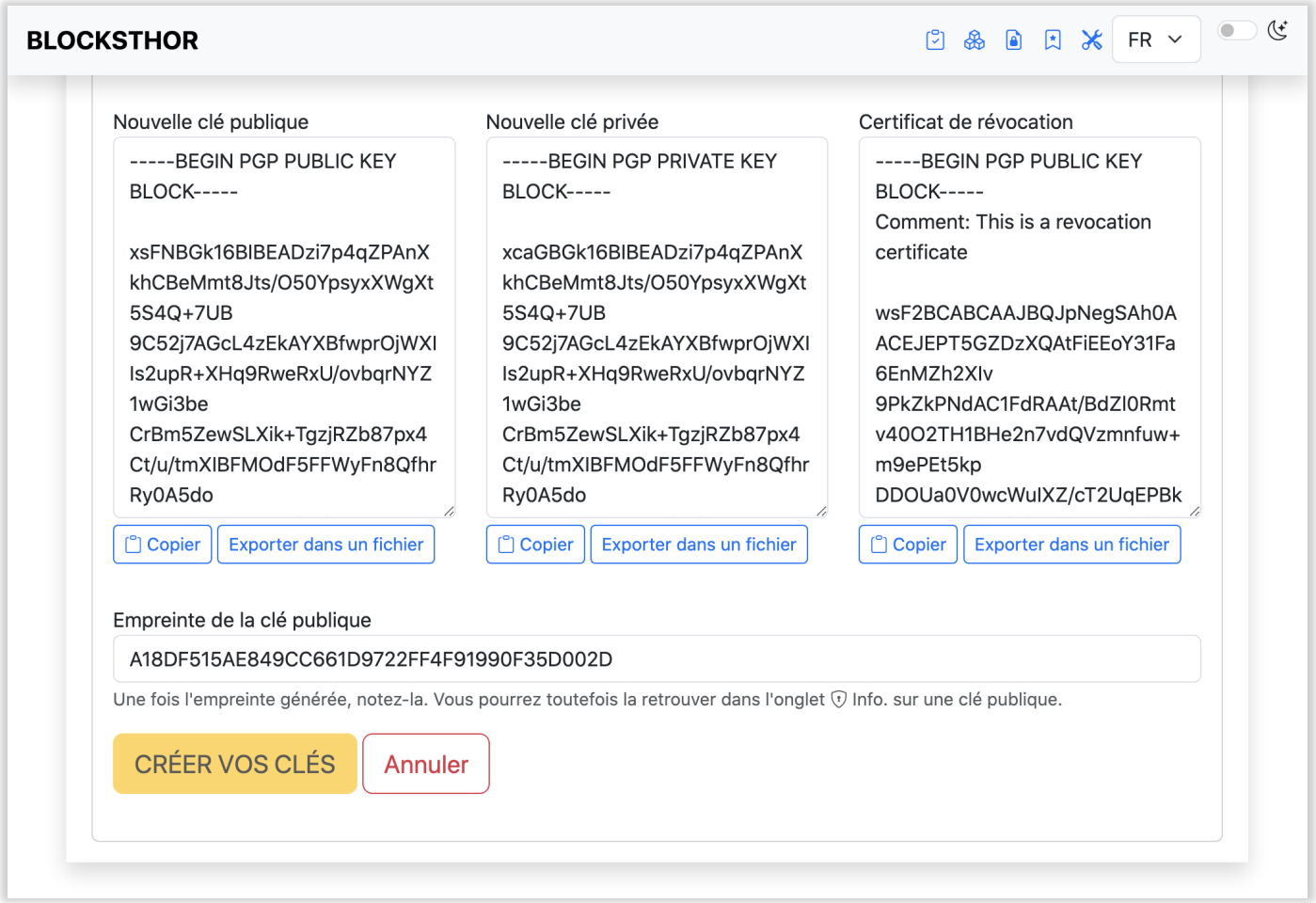
3.1.🔑 Une paire de clés numériques pour signer

- Création d'une clé publique, d'une clé privée et d'un certificat de révocation de la clé publique.

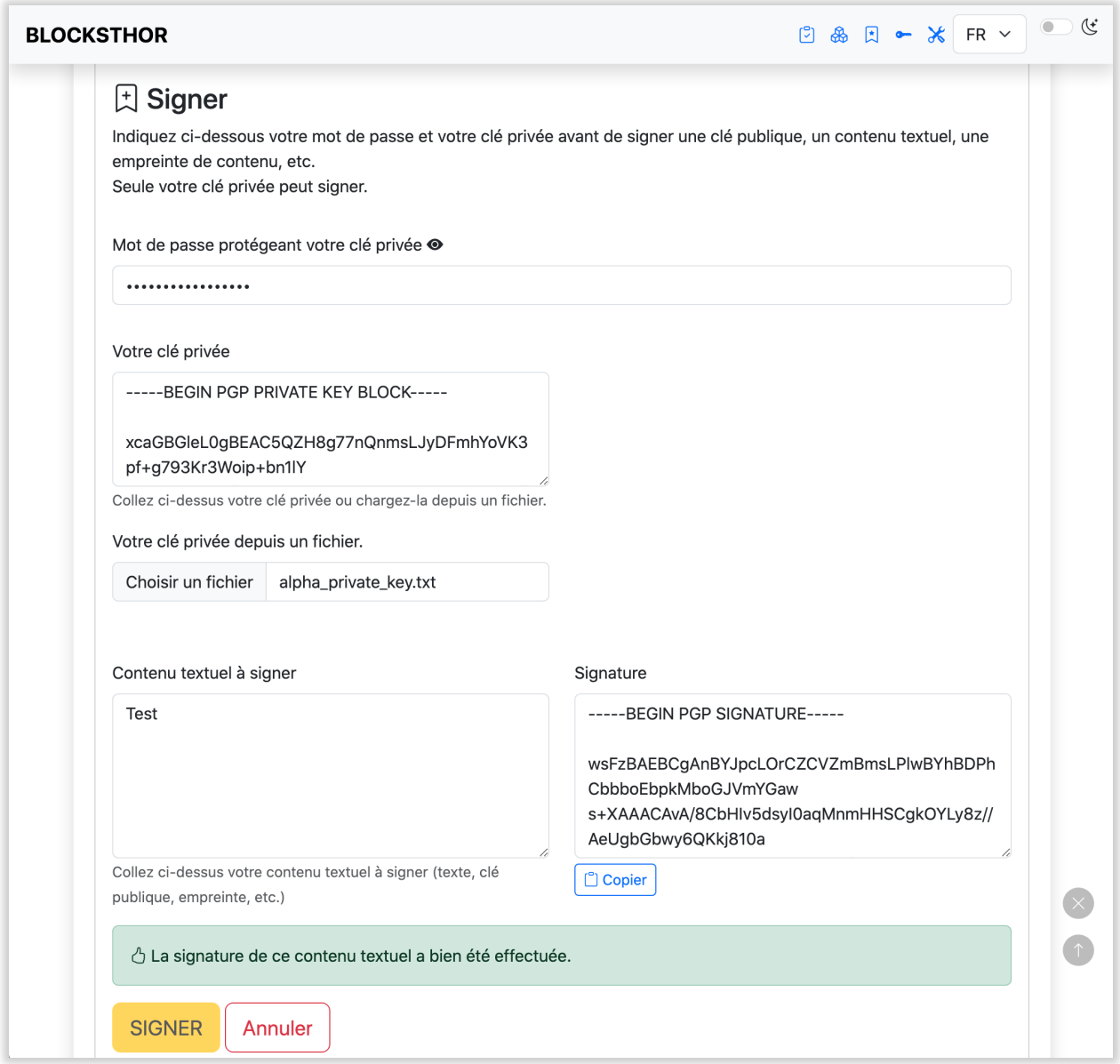


3.2.🔑 … Suite de la création des clés

- Rappel : il faut **protéger sa clé privée** ainsi que son certificat de révocation.
  Seule la clé publique se publie largement via aristhor.com et autres procédés.

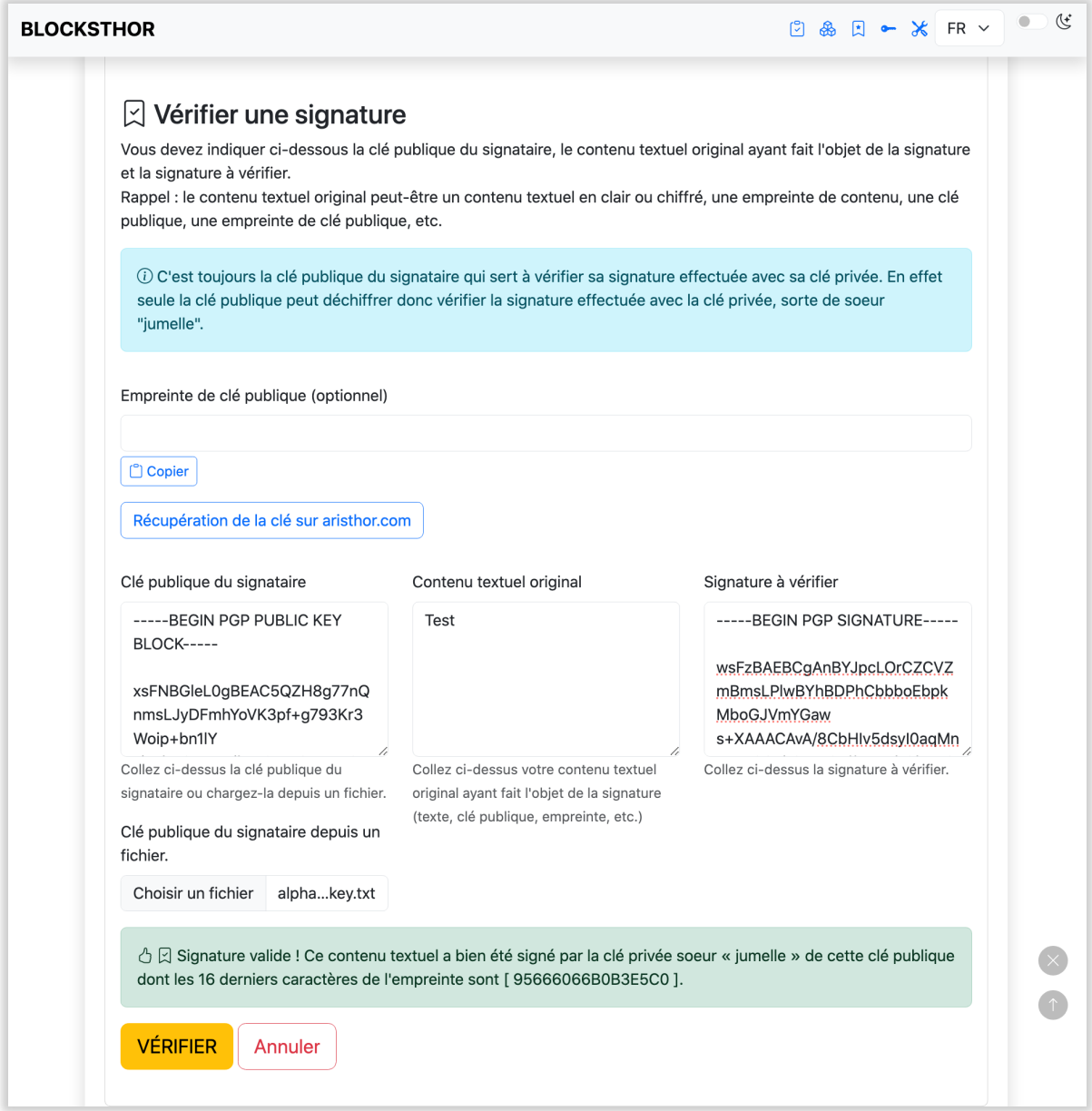


3.3.🔑 Un exemple de signature



- Signons simplement le mot « Test » avec notre clé privée.

3.4.🔑 Vérification de la signature



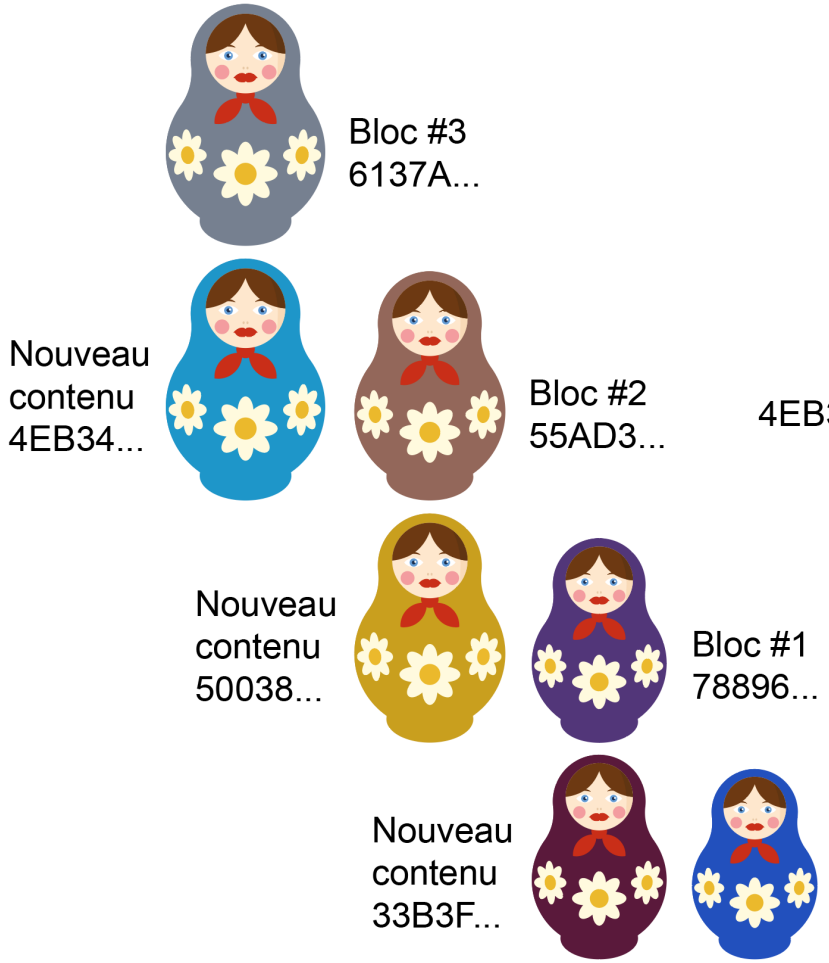
- Vérification de la signature du mot « Test » avec la clé publique liée à la clé privée « signataire ».

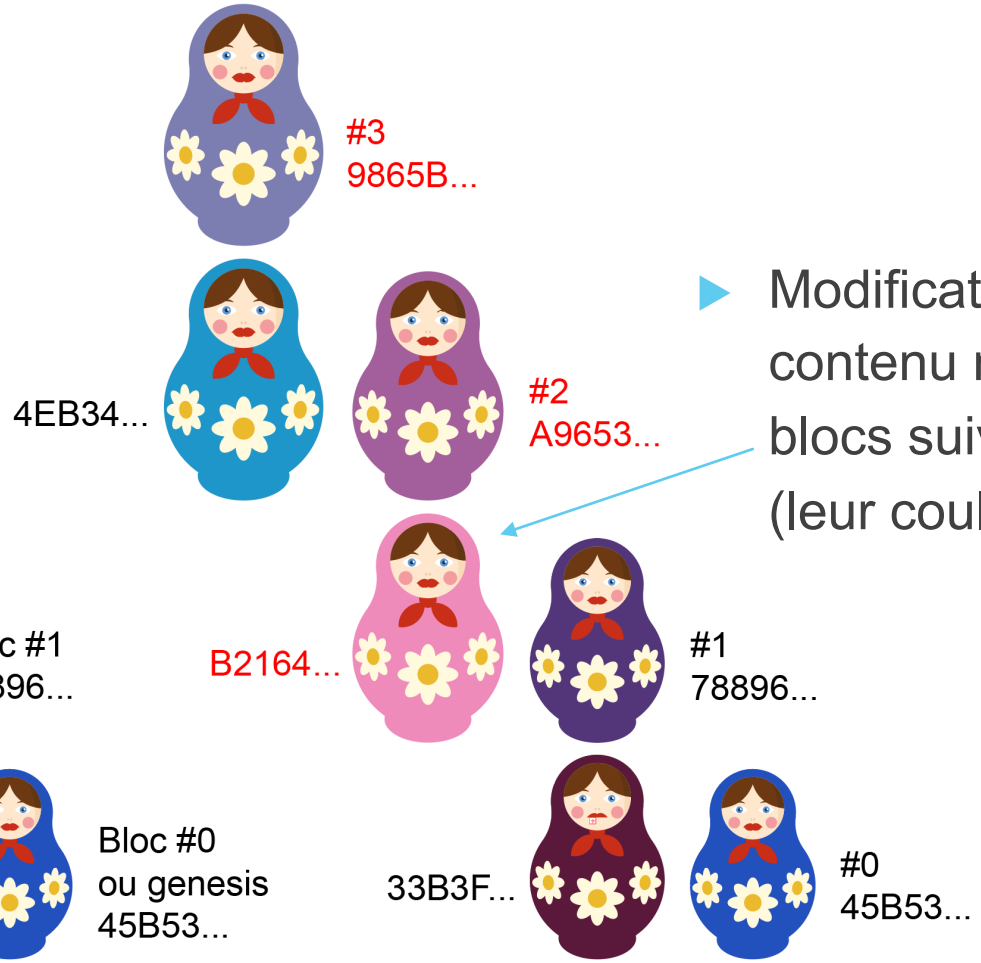
4e partie

🤔 C’est quoi une chaîne de blocs ?

- Une blockchain est un registre sécurisé. Les blocs sont comme les pages « indéchirables » d’un grand livre numérique.
- En somme, un simple fichier texte incluant des données quasi impossibles à falsifier.
- Le Blocksthor Maker et le site aristhor.com gèrent vos blockchains privées spécifiquement conçues pour sécuriser des témoignages sur tout évènement de la vie.

4.1.☀ Blocs d'une blockchain = Poupées russes dont les couleurs se mélangeraient



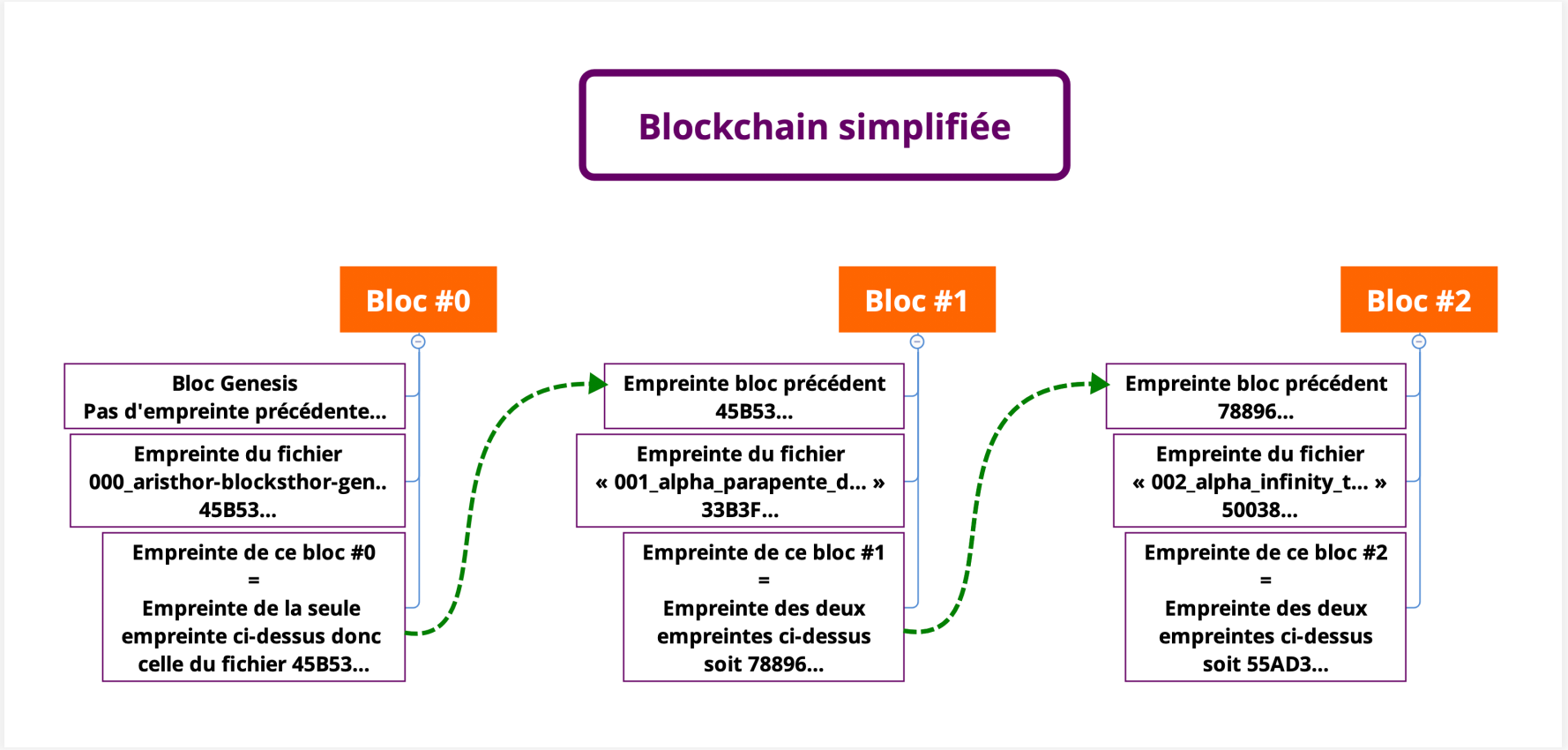


- Modification du seul contenu n°2 et tous les blocs suivants sont modifiés (leur couleur change)

4.2.☀ Comment fonctionne une blockchain ?

- Etudions une blockchain très simplifiée SANS signature numérique et contenant qu'une empreinte de fichier par bloc.

Dans une blockchain blocksthor non simplifiée les informations sécurisées et signées dans chaque bloc sont plus nombreuses et les empreintes se calculent différemment, notamment avec un arbre de Merkle.



4.3.☀ Création du bloc Genesis et 2 blocs standards

Bloc Genesis ou bloc # 0

Empreinte du fichier « **000_aristhor-blocksthor-maker-genesis-block-1.0.pdf** » pour initier la blockchain *(notion simplifiée pour cette présentation)* : 45B53…

Comme il n'y a pas de bloc précédent au bloc zéro alors l'empreinte de ce bloc n°0 est juste celle du fichier de ce bloc donc 45B53…

Bloc # 1

Calcul de l'empreinte de ce bloc n°1 qui correspond à l'empreinte des deux empreintes ci-après
[l'empreinte du bloc précédent Genesis ou n°0] + [l'empreinte du fichier de ce bloc n°1
« 001_alpha_parapente_d….png »] séparées par un tiret soit [45B53…-33B3F…] = 78896…

Bloc # 2

Calcul de l'empreinte de ce bloc n°2 qui correspond à l'empreinte des deux empreintes ci-après
[l'empreinte du bloc n°1] + [l'empreinte du fichier de ce bloc n°2 « 002_alpha_infinity_tumbling_....jpg »]
séparées par un tiret soit
[78896…-50038…] = 55AD3…

4.4.☀️ Détails du calcul de l’empreinte du bloc # 2…

BLOCKSTHOR FR

Empreintes d'une chaîne de caractères
(MD5, SHA-1, SHA-256, SHA-384, SHA-512)

Chaîne de caractères

7889664EE3568F7B4F223F0D084AFB16CD8BCE5CDD0506179B4A791D6590177F19AA240CCBC673BC0CA42D05F0C823784FCC8F24F2DD63F73A0CEBBB4F118448-5003843F944CF6E04422DF9FF1DDF6026EC251CD6572021C3A04CEF7676BBD0854D3F42E52BD5B09A2170E0FD27BAF9FB00752EEB0AFD4DC069DB14ECDF4B789

Empreinte pour comparaison

Optionnel : indiquez ci-dessus une empreinte SHA-512 pour comparaison automatique avec celle qui va être calculée à partir du champ "Chaîne de caractères".

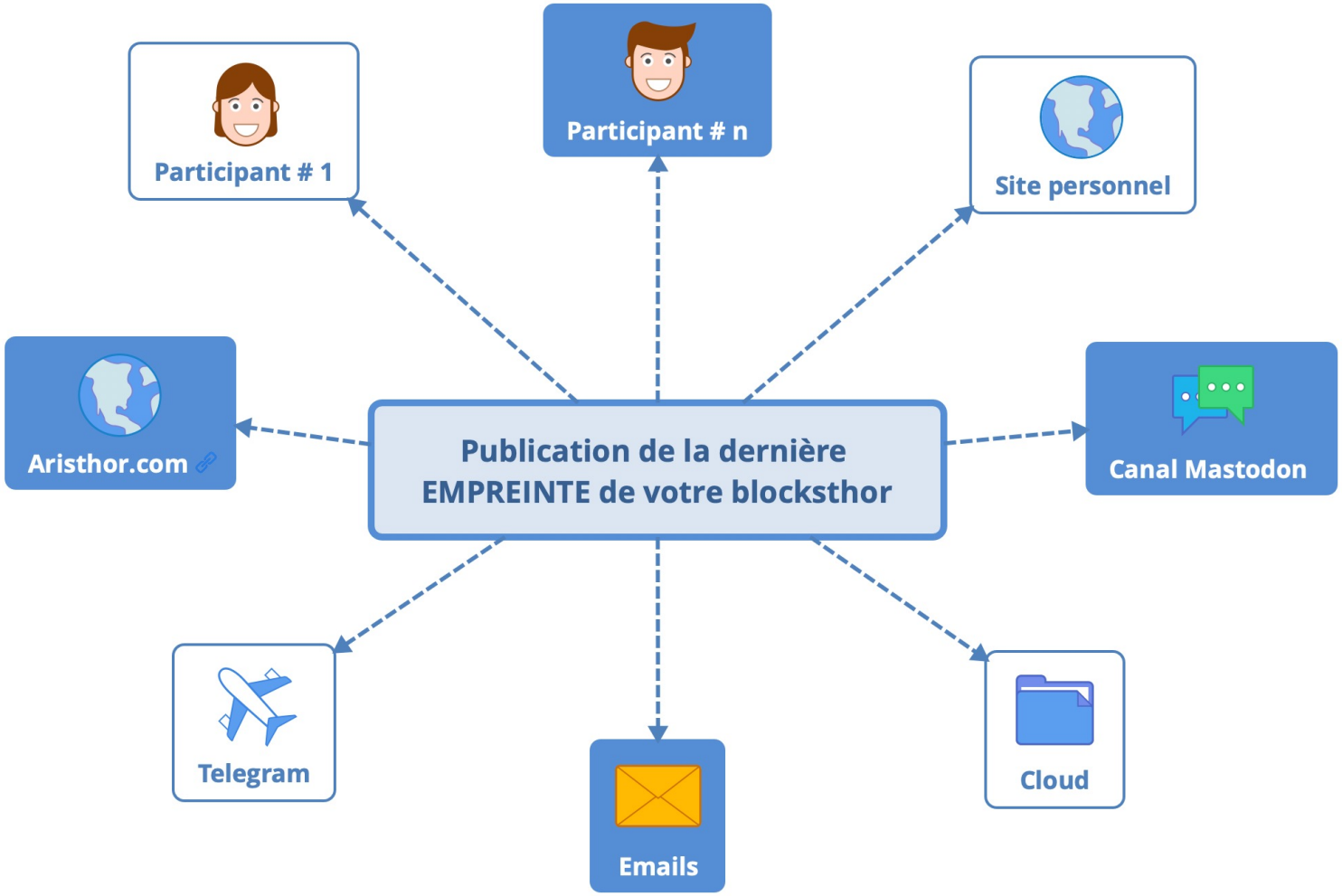
CALCULER Annuler

SHA-512

55AD3AE5ADA9C6B685D17C58435DFAAA71EA4BA47CCD80EC44364C3F9D412FB0433F7E056D2961E3C68DCCC0C94C9EAD19404C9B9F95DBB6D48287AD0CB5F159

4.5. Large diffusion de l'empreinte de la blockchain

- L'empreinte du dernier bloc garantit l'intégrité des blocs précédents. Plus cette empreinte est diffusée moins une copie falsifiée d'une blockchain peut exister...



5e partie

☀ Comment fonctionne une Blocksthor ?

A garder en tête : vous pouvez créer plusieurs blocksthor pour vos différents besoins (famille, maison, sport, pro, entreprise, association, collectif, évènement, etc.)

- Une Blocksthor d'Aristhor est une blockchain privée sans preuve de travail PoW *(Proof of Work)*
- Utilisation d'un consensus simplifié par preuve d'autorité PoA *(Proof of Authority)*
- Un consensus paramétrable

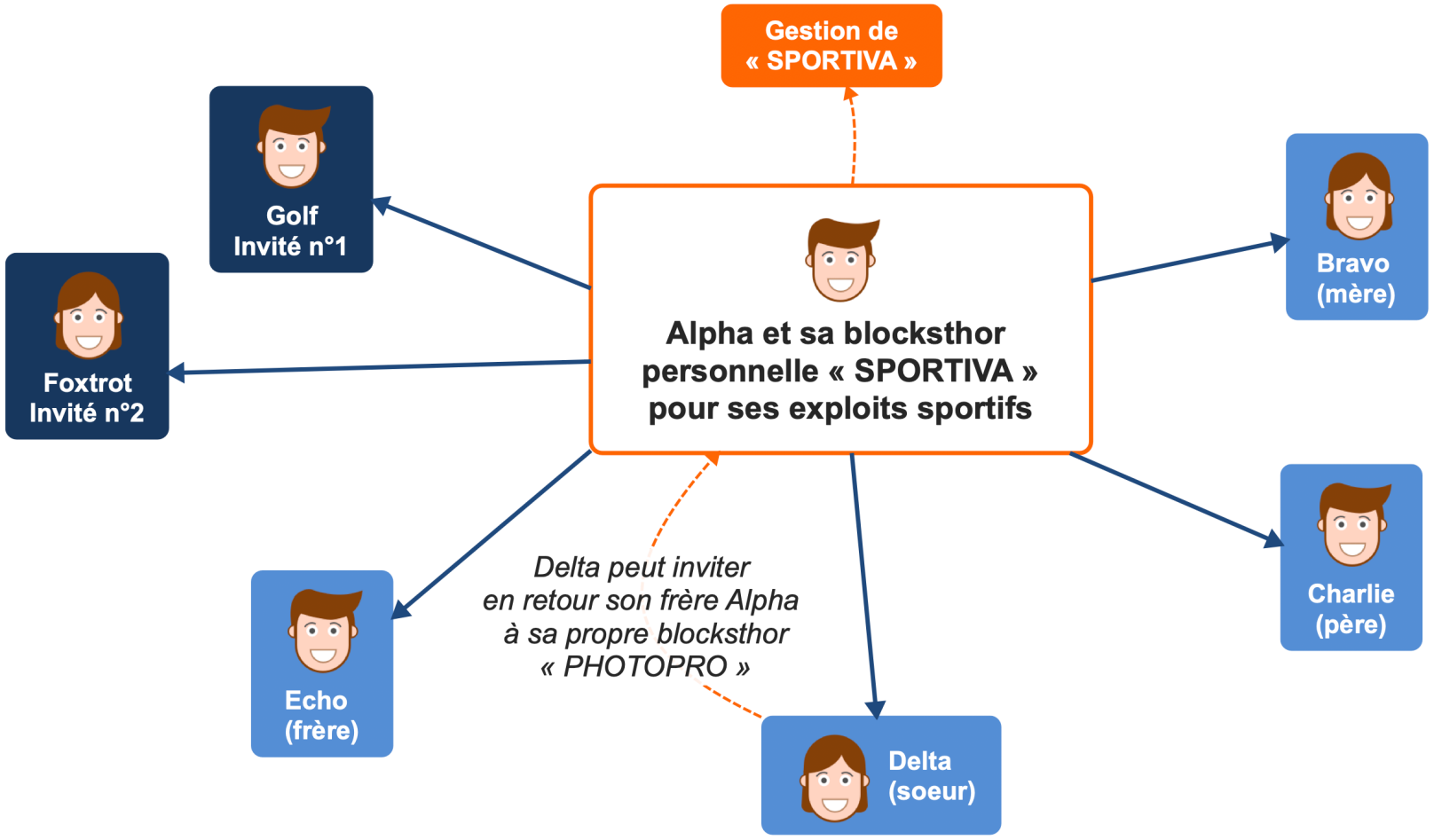
Ex : les empreintes des clés publiques des signataires sont indiquées dans le fichier bloc zéro. Cela signifie qu'un bloc ne sera valide QUE s'il est garanti au moins par ces signataires.

5.1.☀️ La Blocksthor vous aide à prouver le très « difficile à croire »

Cette photo est-elle vraiment sans trucage, notamment par IA ?! Une blocksthor dédiée aux exploits sportifs de ce parapentiste aiderait beaucoup pour le savoir…

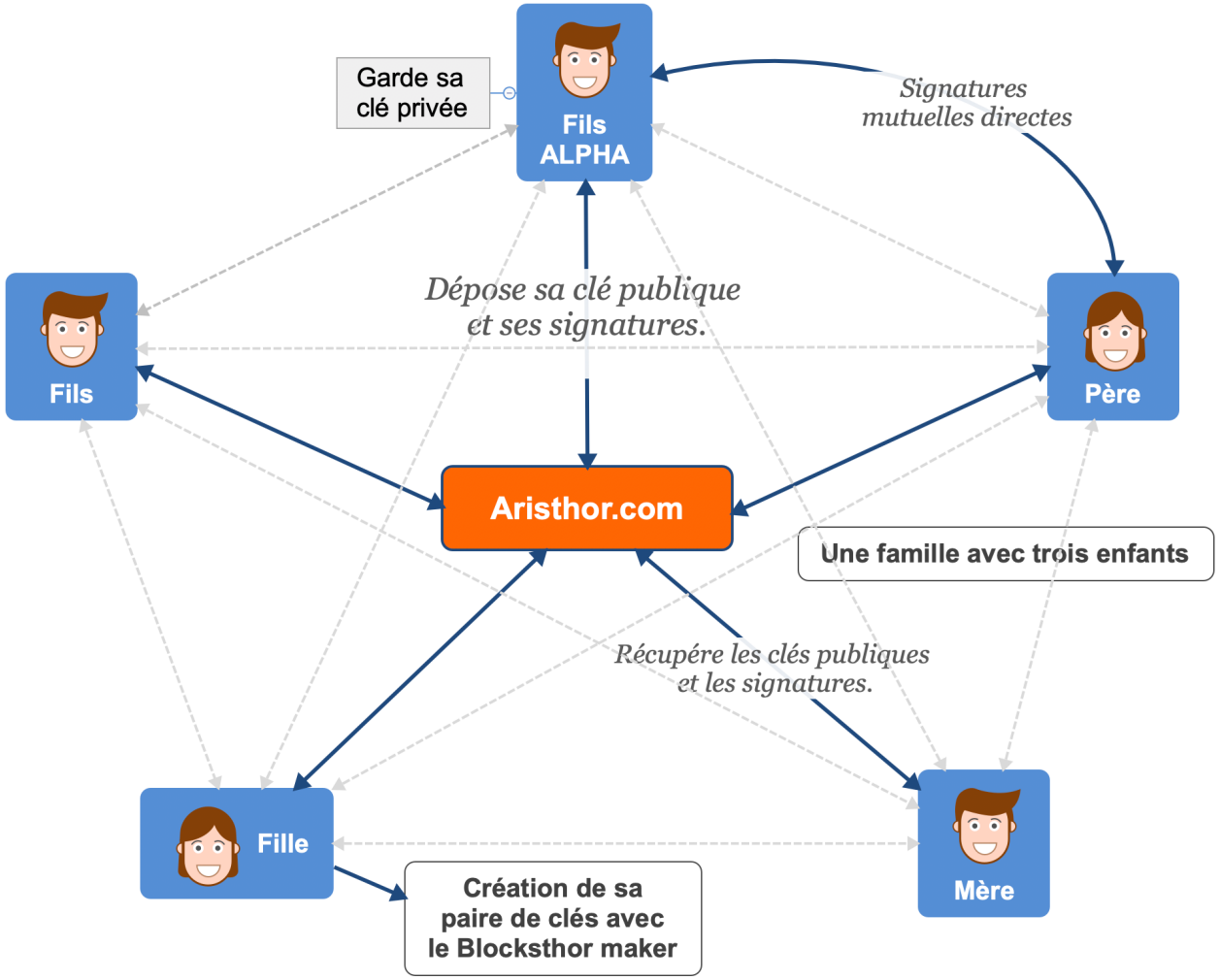
5.2. Alpha et sa blocksthor d'exploits sportifs

- Alpha, fils d'une famille de 3 enfants, invite toute sa famille et deux amis à participer à sa blocksthor. Ils deviennent ainsi les garants de ses exploits notamment en parapente.



5.3. 🔑 Gestion des paires de clés pour signer

- Gestion des clés des membres de la blocksthor « SPORTIVA » du fils Alpha *(hors invités)*



5.4. 🔑 Bloc #2 signé de la blocksthor SPORTIVA

Informations sur le bloc

Identifiant de ce bloc : 2

Numéro(s) des bloc(s) lié(s) : 5 (garantie)

Nom et version du Blocksthor maker : ARISTHOR-BLOCKSTHOR-MAKER-1.0

Réf. permanente de la blocksthor :
E969FB7627CEFAC0F852ABBA5686B3C83072BF90E490527D363F068D484C26C42DE60416D2169B81D5F32FB24946C53BE33F3E9A65CDCAABAF31051D25174507

Date et horaire de création de ce bloc : 11-01-2026 - 16:44:59
Timestamp de création de ce bloc : 1768146299

Empreinte SHA-512 du bloc précédent :
2FBE989381B54F031CE6EE5E66019E5250A9C32BEE6882E57C55C809F8626A1424EF60E1162D94878B2F9D6F879F810C2F3A9A129C00A8DF88F63E86D2BB930E

Empreinte SHA-512 du bloc lié (optionnel) : néant

Empreinte de clé publique de l'émetteur de ce bloc :
33E109B6DBA046E990C6E81895666066B0B3E5C0

Empreinte de clé publique du destinataire de ce bloc (optionnel) : néant

Empreinte SHA-512 du fichier inséré :
5003843F944CF6E04422DF9FF1DDF6026EC251CD6572021C3A04CEF7676BBD0854D3F42E52BD5B09A2170E0FD27BAF9FB00752EEB0AFD4DC069DB14ECDF4B789

Est-ce un fichier de garanties ? : Non

Est-ce un fichier de garanties ? : Non

Commentaire (optionnel) : néant

Type de signature du bloc : RSA

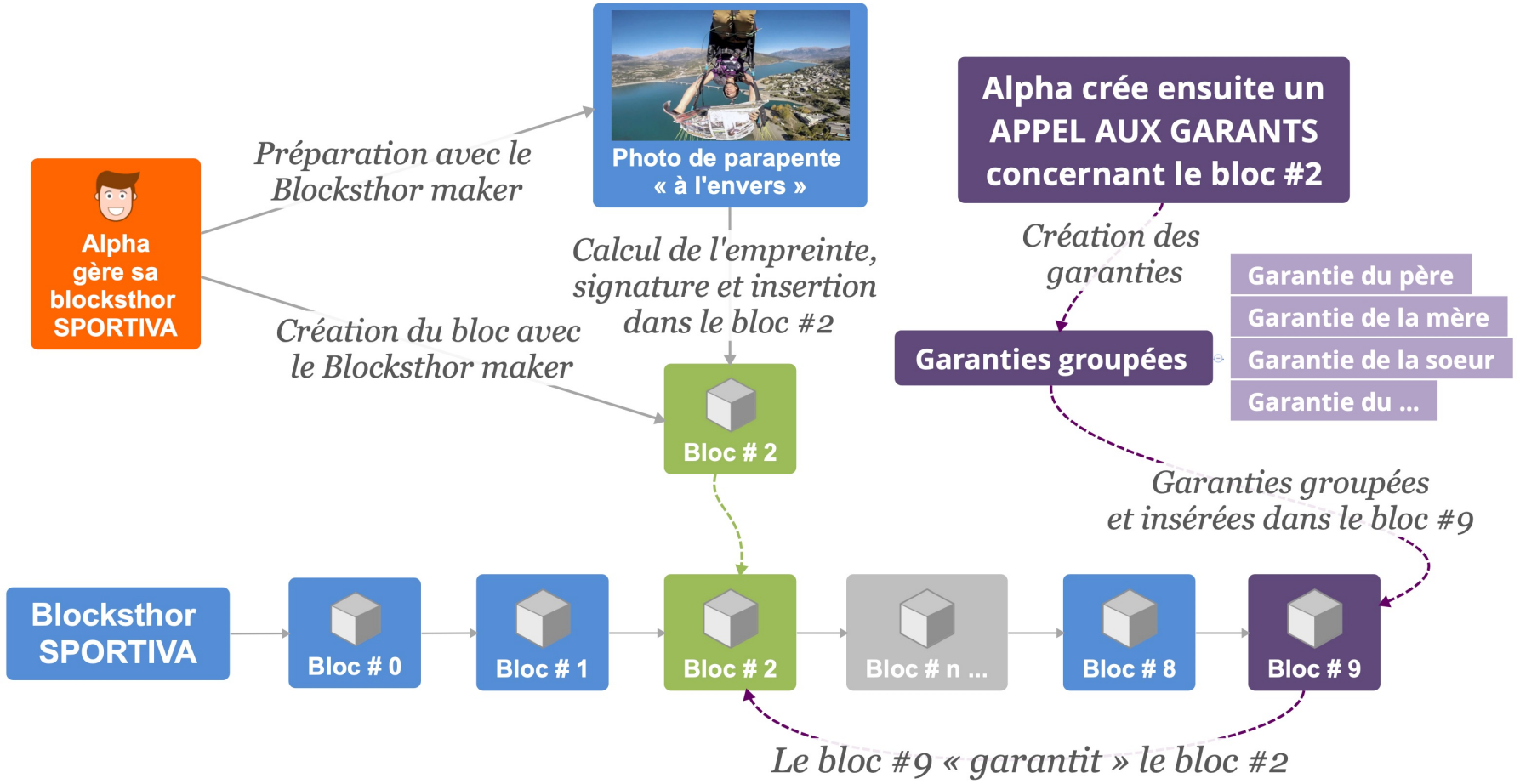
Signature de ce bloc : -----BEGIN PGP SIGNATURE-----

wsFyBAEBCgAnBYJpY8V7CZCVZmBmsLPlwBYhBDPhCbbboEbpkMboGJVmYGaw
s+XAAADm9Q/2MQ0tPlajyq48iPpkrV+C5bQ0Usu914JymWlcKRlmq6H6F2uK
NwmMlBuWo09Z9aSbxjLqygPFdz9LRHUlsWaYF+KxT+fpdR7Srw7NYPEpQoOG
8CTS5ko4W2kSjlSX5YA1mjwsjXl2WfhLAiyhel2X2V7dhCnVmhUhQFKptObi
ER1qg9iRlA0oCx5rndY0x+lw25E5BRuPcGSXrbWKnr6jDd46nkWJaONC5yB+
SdoJ8Cqqpn0VLB8byQ/02zQyzS9VH5KaxoQ6YiX5DXdTjfB00Hr16WilP5+0
dTZtLGidrB5rfsNR49l3Ezotc+v69c91amEewUHLVvHcyIP3yvUelXcJe2LK
EsKuEp+UMRVxdLS5Oa58bPXwhDnQS3pRRDTx4Eq9wRJ/pTyxHhaUR+YeG0ID
jCXL5aTgBOj+iC0N1f8MsCzQir98D0zak5fEDdzSwS/H+iXp+TEflWGW3mKQ
ne7glyUBBqLoCsf4SgF70ON7z65GygTRg/A1Kjx8SD9WvZTXHbtE3aJAzVIc
2cs6fyn/dXc5zNKOUTmxftDa71TGe6t48wNKhD0VTvjJe0/cBV3WZ4+O+pZz
Z+p5Z6wfnSJGNOuxvyG+KdJo4fKMfmZGOLm1VdaOMk82k3l17sd9Li25YFu0
RKVpNXq+vyMKsK6P4whQgDGuHs5SUi72mg==
=ON39
-----END PGP SIGNATURE-----

Empreinte SHA-512 de ce bloc :
BB9FF81DCB1B081026E2D0A35D31EBE44E7B29D9AF38C140995896D415B0C6B92D9B252BF8A7DBDF22DFA47922F76E8D89FC29970D016B214F3855F9DCF80342

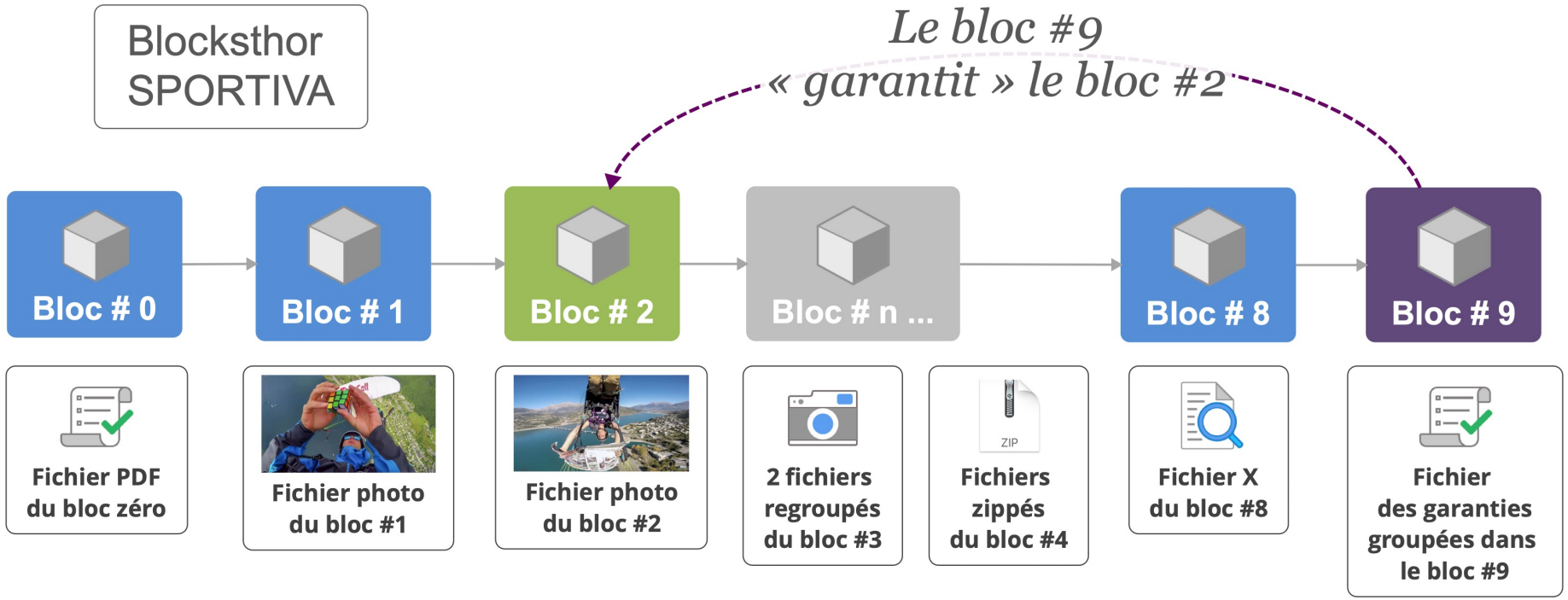
5.5. Bloc #2 avec la photo de parapente « à l'envers »

- Alpha insère l'empreinte de la photo de lui lisant le journal « à l'envers » en parapente dans le bloc #2 de sa blocksthor. Alpha crée ensuite sur aristhor.com un appel aux garants. Le temps que les garants créent leurs garanties, ces dernières ne seront insérées que plus tard au bloc #9.



5.6.☀ Blocs de SPORTIVA avec les fichiers

- Il peut n'y avoir que l'empreinte d'un fichier par bloc. Plusieurs fichiers peuvent aussi être regroupés dans un dossier. Un arbre de Merkle calcule alors l'empreinte « racine » de tous ces fichiers et c'est cette empreinte « racine » qui sera insérée dans le bloc.



Blocksthor
SPORTIVA

Le bloc #9
« garantit » le bloc #2

ARISTHOR

Bloc # 0 | Bloc # 1 | Bloc # 2 | Bloc # n ... | Bloc # 8 | Bloc # 9

Fichier PDF du bloc zéro


Fichier photo du bloc #1

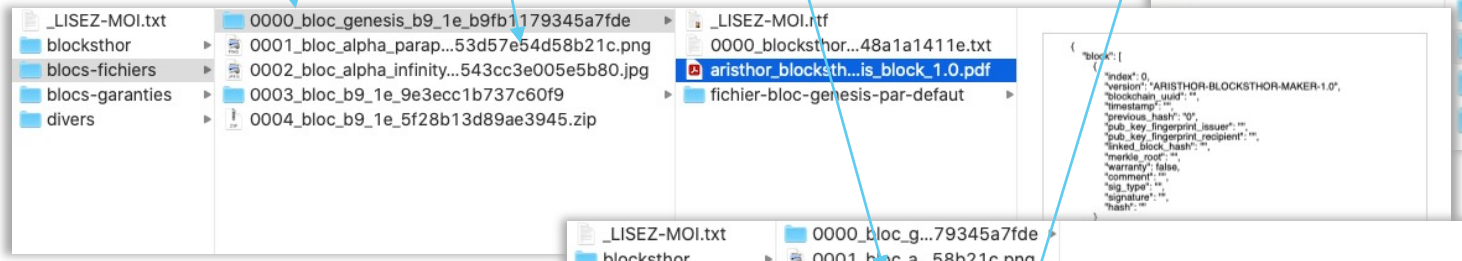

Fichier photo du bloc #2

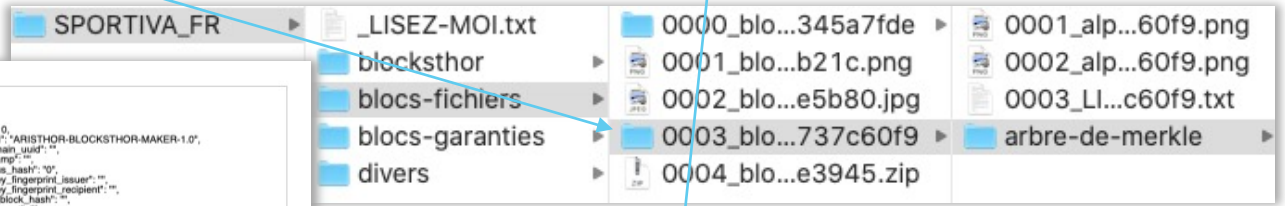
2 fichiers regroupés du bloc #3

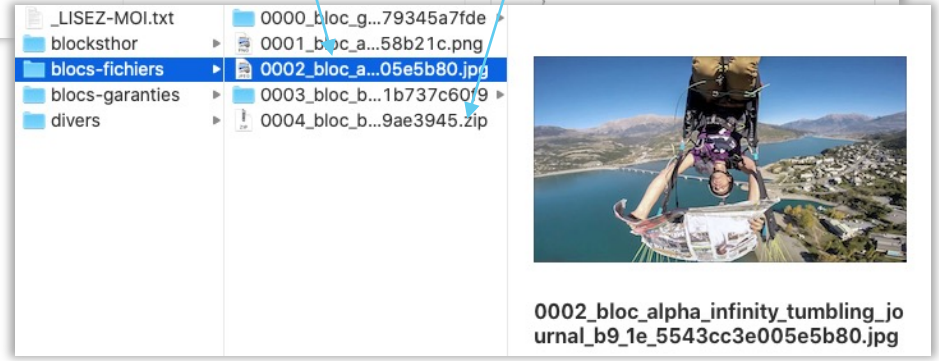
Fichiers zippés du bloc #4

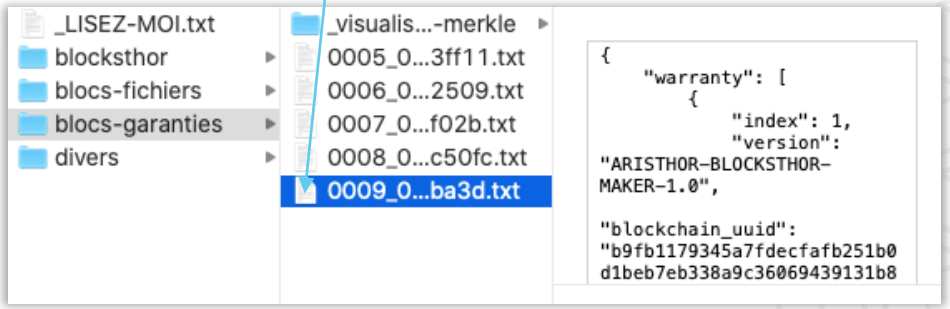
Fichier X du bloc #8

Fichier des garanties groupées dans le bloc #9





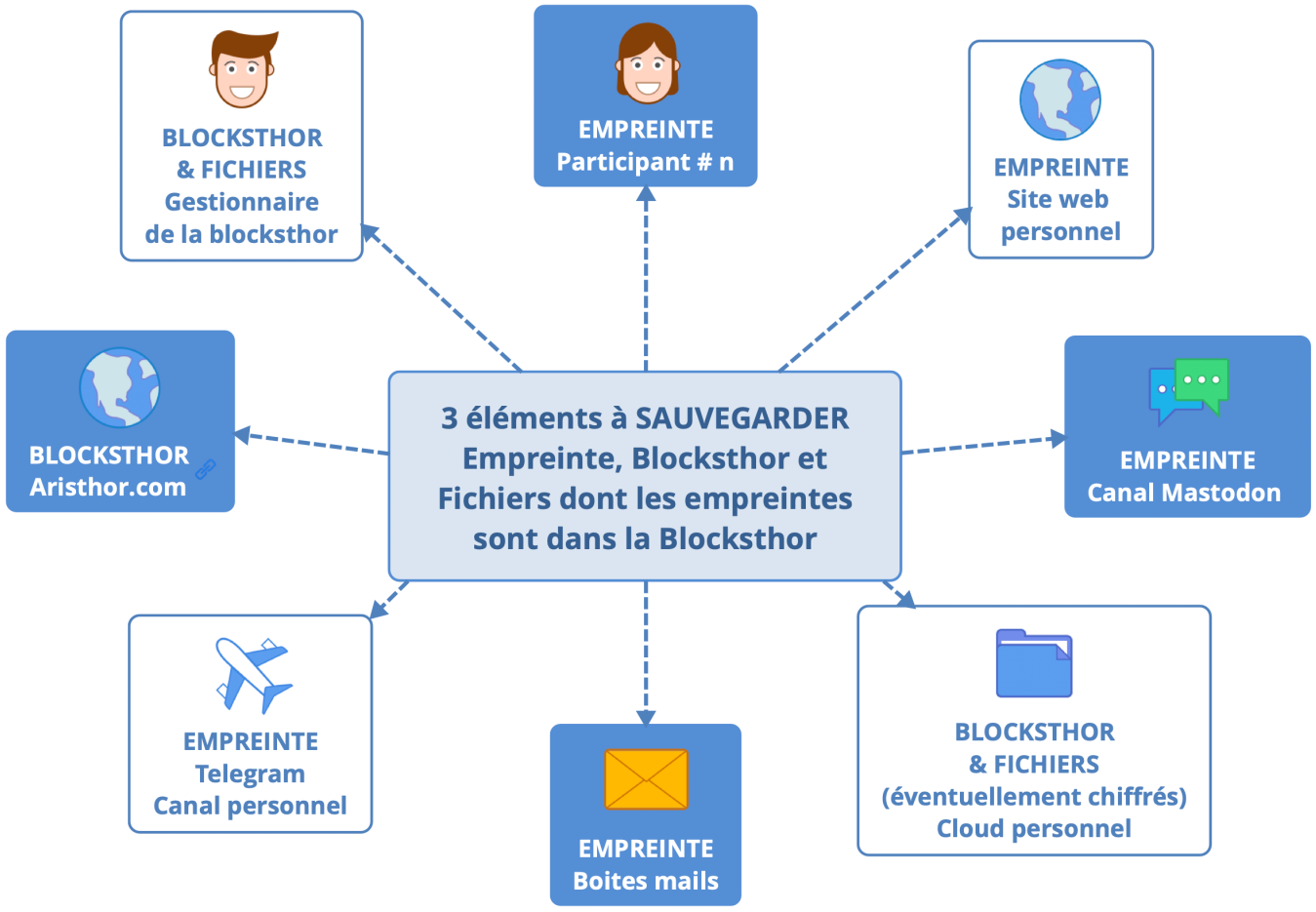




- Rappel : ce sont les empreintes qui sont intégrées dans votre blocksthor, PAS les fichiers.

5.7. Fichiers, Empreinte et Blocksthor elle-même…

- Les fichiers sont sauvegardés à plusieurs emplacements mais moins nombreux que les « lieux » de diffusion de l'empreinte et de la blocksthor. Ceux qui stockent la blocksthor en entier, avec tous les blocs, ont de fait l'empreinte du dernier bloc.
  Point important : une seule copie des fichiers suffit à maintenir la fiabilité et l'utilité d'une blocksthor.



5.8.☀ Rappel des avantages de la blocksthor SPORTIVA

- La famille d'Alpha n'a pas à transférer de lourdes photos prouvant leur présence lors de ces figures d'Alpha mais juste l'empreinte du dernier bloc de sa blocksthor SPORTIVA.
- L'empreinte étant indiquée à plusieurs emplacements tels les comptes de réseaux sociaux des membres de la famille, la vérification qu'il s'agit de la vraie blocksthor SPORTIVA est facilitée.
- Alpha peut utiliser ses photos sur son smartphone pour convaincre n'importe qui. L'empreinte diffusée de SPORTIVA suffit pour prouver l'existence des garanties.
- Le stockage durable de lourds fichiers n'est plus nécessaire pour chaque membre de SPORTIVA. Seul Alpha doit conserver au moins un jeu de photos.
- Les signatures intégrées des membres traduisent leur approbation. S'ils mentaient, la réputation de cette famille serait entachée via leurs clés publiques : alerte par une contre-blocksthor tierce, etc. Dissuasif...

5.9.☀ Avantages de la blockchain Blocksthor dans le cas de la découverte du jumeau de Pierre !

- Les garants de Pierre n'auraient pas eu à transférer de lourdes photos à Alice mais juste l'empreinte du dernier bloc de la blocksthor de Pierre.
- L'empreinte étant indiquée à plusieurs emplacements tels les comptes de réseaux sociaux des garants, l'éventuelle falsification de l'empreinte lors de l'envoi par mail à Alice serait détectable. Elle ne correspondrait plus à celle indiquée à ces multiples emplacements par les garants et également par Pierre.
- Pierre pourrait utiliser son jeu de photos déjà reçu de ses garants. L'empreinte diffusée suffit pour prouver l'existence de ces garanties signées de ces photos.
- Le stockage durable de lourdes photos ne serait plus nécessaire par les garants de Pierre au Kenya. Seul Pierre aurait à conserver un jeu de photos.
- En cas de fraude des garants et de Pierre, leur réputation à chacun serait entachée en raison de la traçabilité de leur mensonge…

5.10.☀️ Apport global de la Blocksthor

- Contribue à protéger le réel de la falsification.
- Combat les mensonges et la confusion.
- Moins de réel, c'est moins de confiance. Moins de confiance c'est moins d'échange. Moins d'échange, c'est moins de partage et de construction. Avec moins de réel, le « prince du mensonge » accroit son règne et tout s'oriente vers le factice et le décadent... 😈

Aristhor restaure la confiance par le témoignage humain. Même imparfait, il était autrefois la norme en phase avec la vie et les liens humains.

6e partie

🙂 Mise en pratique

- Explorez la blocksthor SPORTIVA
- Créez votre blocksthor
- Ajoutez un bloc à votre blocksthor
- Connectez-vous sur aristhor.com
- Créez un appel à vos garants
- Créez une garantie
- Ajoutez un bloc lié incluant des garanties
- Diffusez l’empreinte de votre blocksthor

🤔 Lexique

- **Empreinte cryptographique** : l'équivalent de l'empreinte digitale pour un humain mais pour n'importe quelle donnée numérique, tels un son, une photo, une vidéo, un logiciel, etc.
- **Cryptographie asymétrique** : procédé permettant la signature numérique entre autres. Ce procédé de chiffrement des données (cryptage) a la spécificité de ne pas nécessiter d'échange, au préalable, d'une clé secrète entre celui qui signe et toute personne souhaitant vérifier la validité de cette signature.
- **Signature numérique** : [voir Cryptographie asymétrique ci-dessus]. Une signature n'est que l'empreinte, chiffrée par une clé privée, d'une donnée numérique. La clé publique, liée à la clé privée « signataire », permet de déchiffrer la signature donc l'empreinte et, par comparaison d'empreintes, de vérifier la validité de la signature.
- **Blockchain** : un registre comme un journal de bord ou un grand livre de compte avec la spécificité d'être sécurisé. Plus précisément : un algorithme incluant une phase de signature numérique d'une « page » de données. Ensuite une empreinte cryptographique de cette page est calculée et un double de cette empreinte est inséré dans la page suivante. Le tout forme de multiples pages « indéchirables » tel un livre bien relié. Remplacez les mots « livre bien relié » par « chaine » puis « pages indéchirables » par « blocs » et vous obtenez « chaine de blocs (ou blockchain) » au lieu de « livre bien relié de pages indéchirables ».
- **Consensus** : le mode décisionnel autorisant ou non l'intervention sur une blockchain tel qu'avoir le droit d'ajouter des blocs.
- **Preuve de Travail** (PoW – Proof of Work) : un consensus lié au « travail » effectué. La blockchain Bitcoin utilise la PoW. Le « travail » se nomme alors minage et correspond à un calcul massif et décentralisé d'empreintes.
- **Preuve d'Autorité** (PoA – Proof of Authority) : un consensus lié à l'identité et au statut des personnes impliquées. La blockchain Blocksthor d'Aristhor utilise la PoA. A la différence de la PoW, la PoA consomme très peu d'énergie.🍀

📗 Historique & Remerciements

- Historiquement, la Blocksthor est née en interne pour sécuriser le suivi d'interventions informatiques sensibles.
- L'amélioration de cet outil et sa sortie publique ont été accélérées en raison d'un choc personnel du fondateur. A savoir l'enlèvement parental de son fils dès sa naissance, son appropriation et la falsification de son identité réelle en l'affublant d'un prénom et nom étrangers.
  L'acquisition et la sécurisation des pièces juridiques et personnelles du dossier sont facilitées par une blocksthor.
- Vifs remerciements à ceux ayant contribué au développement de la Blocksthor et aux proches ayant soutenu dans cette épreuve le fondateur d'Aristhor, toujours sans nouvelle de son fils. Son combat, empreint d'inquiétude pour la sécurité de son enfant, dure déjà depuis plus de 18 mois.
- Aristhor restera durablement un fournisseur d'outils novateurs contre la falsification.

Merci pour votre attention. 🙏