SYNTHÈSE

Manuel Aristhor

Synthèse du 1er octobre 2026 · Manuel v1.1 · 17 pages → 2

1 Comprendre

Partie 1 du manuel

Une **blocksthor** est une blockchain de témoignages **privée et nominative**, créée et gérée par ses utilisateurs. Chaque bloc enregistre un acte, un événement ou un témoignage, horodaté et signé. Elle sert à attester des faits dans le temps, pas à ranger des fichiers.

Bloc 0 genesis réf. permanente → **Bloc 1** contient hash(0) → **Bloc 2** contient hash(1) → **… dernier bloc** état actuel

Deux mécanismes de sécurité

Le chaînage. L'empreinte SHA-256d de chaque bloc est calculée sur son contenu et sur l'empreinte du bloc précédent. Modifier un bloc ancien invalide toute la suite : la falsification se voit.

La signature. Chaque bloc est signé avec une clé privée OpenPGP. La clé publique, déposée sur Aristhor, permet à quiconque de vérifier l'identité du signataire et la validité de la signature.

Le modèle Proof of Authority

La confiance ne repose pas sur la puissance de calcul (Proof of Work - PoW) ni sur une caution (Proof of Stake - PoS), mais sur la responsabilité d'acteurs reconnus, comme des notaires tenant un registre. L'**ancrage** ajoute un tiers plus difficile à corrompre : dépôt régulier de la dernière empreinte dans un registre extérieur, comme on publiait autrefois une preuve dans un journal.

Les acteurs

Responsable	Crée la blocksthor, ajoute les blocs, définit la publication.
Utilisateurs	Invités par le responsable, ils consultent ou ajoutent selon leurs droits.
Garants	Utilisateurs qui signent une garantie sur un bloc précis pour en attester le contenu.

Repères techniques

ÉLÉMENT	FORMAT	RÔLE
Empreinte de bloc	SHA-256d, 64 car. hex	Identifie un bloc ou un fichier
Format court	`f7-4d`	Commence par f7, finit par 4d
Bloc zéro-genesis	SHA-256d	Référence permanente, ne change jamais
Dernier bloc	SHA-256d	État courant, à diffuser le plus possible
Empreinte de clé	OpenPGP, 40 car. hex	Identifie une clé publique

Outils et espaces

Le **Blocksthor Maker** fonctionne entièrement dans le navigateur : clés PGP, création de blocs, vérification d'intégrité, calcul d'empreintes, signatures, arbres de Merkle. Une version autonome (macOS, Linux, Windows) est annoncée pour un usage **AIR GAP**, sur une machine jamais connectée : c'est le niveau de sécurité élevé, face au niveau normal. Le **Blocksthor Reader** permet à tous, sans compte, de lire et vérifier. Trois espaces : **Discovery** (découverte gratuite), **Solo** (personnel), **Team** (collaboratif).

> **Cas d'usage**
> Propriété intellectuelle, preuve d'antériorité, suivi de conformité et d'audits, journal de bord certifié (travaux, livraisons), garantie de prestation par des tiers.

2 Explorer et gérer

Parties 2 et 3 du manuel

Créer et enregistrer une blocksthor

Dans le Maker : saisir les informations du bloc genesis, charger sa clé privée, créer, puis exporter en `.txt`. Sur Aristhor, *Mes blocksthor › Ajouter* : l'**import du fichier .txt** est recommandé, il remplit automatiquement blocs, référence permanente et dernière empreinte. Vérifier l'intégrité à chaque reprise de la chaîne. Pendant l'ajout de blocs, la blocksthor peut être **verrouillée**.

Publier et rendre visible

Trois options, en cascade : **recherche de blocksthor par empreinte**, **par email** et **visibilité publique ou non des blocs** (blocksthor lisible et téléchargeable). La page *Empreintes & Blocs* cherche à la fois sur la référence permanente et le dernier bloc d'une blocksthor. Un bouton publie l'empreinte sur **Mastodon**, **Telegram** ou **Bluesky** ; chaque publication est tracée dans *Publications E & B*.

Clés publiques

- Dépôt : empreinte 40 car., clé armurée, niveau de sécurité, options de recherche.
- **Toile de confiance** : les utilisateurs signent la clé d'autrui après vérification en personne.
- Révocation si clé privée perdue ou compromise ; la clé reste visible, marquée Révoquée.
- Export en `.asc`.

Blocs & garanties

- Dans le Maker : charger les éléments, calculer l'empreinte racine `merkle_root`, signer et créer le bloc.
- Une **garantie**, issue d'un appel aux garants, se crée sur Aristhor.com et se signe dans le Maker.
- Plusieurs garants d'un même bloc : les **grouper** dans un arbre de Merkle et un bloc de garanties.

Utilisateurs et compte

Seul l'administrateur d'une blocksthor invite (par email, compte Aristhor requis) ou retire un utilisateur, dans la limite du **quota** de l'offre. Un utilisateur peut se retirer ; l'administrateur non. *Mon compte* gère coordonnées, photo, mot de passe (16 car. minimum conseillés) et connexions aux réseaux sociaux. La suppression du compte est **immédiate et définitive** : exporter toutes vos blocksthor, clés et signatures de clés avant.

L'ancrage

Une blocksthor **hôte** accepte les ancrages à fréquence et jour fixes. Chaque utilisateur y déclare sa propre blocksthor. Au jour dit, les dernières empreintes de toutes les blocksthor déclarées forment un **arbre de Merkle SHA-256d**. La `merkle_root` atteste existence, intégrité collective et non-répudiation (impossibilité de nier avoir effectué l'action).

> **À conserver**
> Exporter l'arbre en `.txt` après chaque ancrage, sans jamais le modifier. Rangement conseillé : dossier `0876_block-file_anchor_fd-7d` contenant le fichier `0876_merkle_tree_fd-7d.txt` et les fichiers du bloc.

Bonnes pratiques d'organisation

- Ne mettre que l'essentiel en chaîne, avec des empreintes de fichiers compressés si possible.
- Noms en minuscules sans accents, suffixés des identifiants blocksthor et bloc : `nom_39-9b_4c-e5.jpg`.
- Tenir un tableur des correspondances blocs ↔ fichiers.
- Un fichier oublié s'ajoute dans un nouveau bloc lié à l'ancien. Le seul point critique : ne pas perdre les fichiers pour retrouver quel fichier a produit quelle empreinte.
- **Rappel** : il n'y a pas de fichier dans un bloc d'une blocksthor, mais uniquement une empreinte de fichier ou même une empreinte d'empreintes de fichiers (arbre de Merkle).

SUMMARY

Aristhor Manual

Summary of 1 October 2026 · Manual v1.1 · 17 pages → 2

1 Understanding

Part 1 of the manual

A **blocksthor** is a blockchain of testimonies that is **private and nominative**, created and managed by its users. Each block records an act, an event or a testimony, timestamped and signed. Its purpose is to attest facts over time, not to organise files.

Block 0 genesis permanent ref. → **Block 1** contains hash(0) → **Block 2** contains hash(1) → **… last block** current state

Two security mechanisms

Chaining. The SHA-256d fingerprint of each block is computed from its content and from the fingerprint of the previous block. Changing an older block invalidates everything after it, so any tampering shows.

Signature. Each block is signed with an OpenPGP private key. The public key, uploaded to Aristhor, lets anyone verify the signer's identity and the validity of the signature.

The Proof of Authority model

Trust does not rest on computing power (Proof of Work - PoW) or on a deposit (Proof of Stake - PoS), but on the accountability of recognised actors, like notaries keeping a register. **Anchoring** adds a third party that is harder to corrupt: the latest fingerprint is regularly recorded in an external register, much as a proof used to be printed in a newspaper.

The actors

Owner	Creates the blocksthor, adds blocks, defines publication.
Users	Invited by the owner, they view or add blocks according to their rights.
Guarantors	Users who sign a guarantee on a specific block to attest its content.

Technical reference

ITEM	FORMAT	ROLE
Block fingerprint	SHA-256d, 64 hex chars	Identifies a block or a file
Short format	`f7-4d`	Starts with f7, ends with 4d
Zero-genesis block	SHA-256d	Permanent reference, never changes
Last block	SHA-256d	Current state, to be shared as widely as possible
Key fingerprint	OpenPGP, 40 hex chars	Identifies a public key

Tools and spaces

The **Blocksthor Maker** works entirely in the browser: PGP keys, block creation, integrity checks, fingerprint computation, signatures, Merkle trees. A standalone version (macOS, Linux, Windows) is announced for **AIR GAP** use, on a machine that is never connected: this is the high security level, as opposed to the normal level. The **Blocksthor Reader** lets anyone read and verify, without an account. Three spaces: **Discovery** (free trial), **Solo** (personal), **Team** (collaborative).

Use cases
Intellectual property, proof of prior existence, compliance and audit tracking, certified logbook (works, deliveries), guarantee of service by third parties.

2 Explore and manage

Parts 2 and 3 of the manual

Create and register a blocksthor

In the Maker: enter the genesis block information, load your private key, create, then export to `.txt`. On Aristhor, *My blocksthor › Add*: **importing the .txt file** is recommended, as it fills in blocks, permanent reference and last fingerprint automatically. Check integrity every time you pick up the chain again. While blocks are being added, the blocksthor can be **locked**.

Publish and make visible

Three options, each building on the previous: **blocksthor search by fingerprint**, **by email**, and **public or private block visibility** (blocksthor readable and downloadable). The *Fingerprints & Blocks* page searches both the permanent reference and the last block of a blocksthor. A button publishes the fingerprint to **Mastodon**, **Telegram** or **Bluesky**; every publication is logged in *F & B Publications*.

Public keys

- Upload: 40-char fingerprint, armored key, security level, search options.
- **Web of trust**: users sign other people's keys after checking their identity in person.
- Revocation if the private key is lost or compromised; the key stays visible, marked Revoked.
- Export as `.asc`.

Blocks & guarantees

- In the Maker: load the items, compute the root fingerprint `merkle_root`, sign and create the block.
- A **guarantee**, arising from a call to guarantors, is created on Aristhor.com and signed in the Maker.
- Several guarantors of the same block: **group** them in a Merkle tree and a guarantees block.

Users and account

Only the administrator of a blocksthor invites (by email, Aristhor account required) or removes a user, within the **quota** of the plan. A user can leave; the administrator cannot. *My account* manages contact details, photo, password (at least 16 chars recommended) and social network connections. Account deletion is **immediate and permanent**: export all your blocksthor, keys and key signatures first.

Anchoring

A **host** blocksthor accepts anchors on a fixed frequency and day. Each user declares their own blocksthor in it. On the set day, the last fingerprints of all declared blocksthor form a **SHA-256d Merkle tree**. The `merkle_root` attests existence, collective integrity and non-repudiation (inability to deny having performed the action).

> **Keep this**
> Export the tree as `.txt` after every anchoring and never modify it. Recommended filing: folder `0876_block-file_anchor_fd-7d` containing the file `0876_merkle_tree_fd-7d.txt` and the block's files.

Good filing practices

- Only put what matters on the chain, with fingerprints of compressed files where possible.
- Lowercase names without accents, suffixed with the blocksthor and block identifiers: `nom_39-9b_4c-e5.jpg`.
- Keep a spreadsheet mapping blocks ↔ files.
- A forgotten file goes into a new block linked to the old one. The only critical point: not losing the files, so you can find which file produced which fingerprint.
- **Reminder**: a block of a blocksthor contains no files, only a file fingerprint, or even a fingerprint of file fingerprints (Merkle tree).