



ARISTHOR

Blocksthor — Blockchains de témoignages

SÉCURITÉ

Changer de clé signataire

Procédure de changement de clé signataire pour votre blocksthor



Changer la clé signataire de votre blocksthor

Cinq étapes suffisent pour remplacer la paire de clés gérant les blocs de votre blocksthor — lors d'un renouvellement planifié ou si vous pensez que votre clé privée actuelle est compromise.

1

Créer et publier une nouvelle clé

Créez une nouvelle paire de clés via le **Blocksthor Maker**, puis publiez la nouvelle clé publique (menu « Clés publiques » sur aristhor.com). La clé privée associée reste secrète : c'est elle qui signera désormais tous vos blocs.

2

Créer un bloc annonçant la nouvelle clé

Créez un bloc incluant l'empreinte **sha256d** de l'identifiant long (40 caractères) de votre nouvelle clé publique. Calculez cette empreinte dans l'onglet « Empreintes » de la section « Outils » du Blocksthor Maker.

Ajoutez en anglais, en commentaire du bloc : « New public key 33e109b6dba046e990c6e81895666066b0b3e5c0 », où 33e109... est l'identifiant long de votre nouvelle clé. Signez ce nouveau bloc avec la nouvelle clé privée associée, et liez ce bloc au bloc zéro (bloc genesis) de votre blocksthor.

3

Lancer un appel aux garants

Sur ce nouveau bloc, lancez un **appel aux garants** pour attester de la nouvelle clé publique : plus les témoins-garants sont nombreux, plus ce changement de clé est crédible et incontestable.

4

Publier au maximum l'empreinte de ce nouveau bloc

Diffusez le plus largement possible l'empreinte de ce nouveau dernier bloc — celui qui inclut l'empreinte de la nouvelle clé publique qui sera utilisée à l'avenir. Plus la publication est large, plus votre changement de clé est incontestable.

5

Révoquer et publier l'ancienne clé

Révoquez l'ancienne clé et publiez cette révocation : chacun saura ainsi que seule la nouvelle clé engage désormais votre blocksthor.

Rappel

Tout événement de fonctionnement de votre blocksthor doit être décrit et inclus dans un bloc, lui-même lié au bloc zéro-genesis. Le changement de clé signataire ne fait pas exception.

Résultat

Votre blocksthor est désormais signée avec votre nouvelle clé privée : la chaîne reste continue, publique et vérifiable, et l'ancienne paire de clés ne peut plus engager votre blocksthor.

Assistance

Questions ? Rendez-vous sur aristhor.com — rubriques Documentation et FAQ — ou contactez-nous via la page [Nous contacter](#).



ARISTHOR

Blocksthor — Blockchains of Testimonies

SECURITY

Changing your signing key

Procedure for changing the signing key of your blocksthor



Changing the signing key of your blocksthor

Five steps are enough to replace the key pair managing the blocks of your blocksthor — whether as part of a scheduled renewal or because you believe your current private key has been compromised.

1

Create and publish a new key

Create a new key pair using the **Blocksthor Maker**, then publish the new public key (the “Public keys” menu on aristhor.com). The associated private key remains secret: it is the one that will now sign all your blocks.

2

Create a block announcing the new key

Create a block including the **sha256d** fingerprint of the long identifier (40 characters) of your new public key. Calculate this fingerprint in the “Fingerprints” tab of the “Tools” section of the Blocksthor Maker.

Add, in English, as the block’s comment: “New public key 33e109b6dba046e990c6e81895666066b0b3e5c0”, where 33e109... is the long identifier of your new key. Sign this new block with the new associated private key, and link this block to the zero block (genesis block) of your blocksthor.

3

Launch a call for guarantors

On this new block, launch a **call for guarantors** to attest to the new public key: the more witness-guarantors there are, the more credible and undeniable this key change becomes.

4

Publish the fingerprint of this new block as widely as possible

Spread the fingerprint of this new latest block as widely as possible — the one that includes the fingerprint of the new public key that will be used going forward. The wider the publication, the more undeniable your key change becomes.

5

Revoke and publish the old key

Revoke the old key and publish this revocation: everyone will then know that only the new key now commits your blocksthor.

Reminder

Every operational event of your blocksthor must be described and included in a block, itself linked to the zero-genesis block. Changing the signing key is no exception.

Result

Your blocksthor is now signed with your new private key: the chain remains continuous, public and verifiable, and the old key pair can no longer commit your blocksthor.

Support

Questions? Visit aristhor.com — Documentation and FAQ sections — or contact us via the Contact page.