Blockchain et monnaies numériques

Entre encadrement européen et défis technologiques

Loïc Miller

5 décembre 2025

CentraleSupélec | université PARIS-SACLAY

PiRATV

L'euro numérique, qu'est-ce que c'est ?

Une monnaie numérique publique, émise par la BCE

- Complète les pièces et billets
- Accessible à **toute personne ou entreprise** de la zone euro
- Stocké dans un compte via banque/intermédiaire agréé
- Un euro numérique = un euro en cash

Pas une crypto-monnaie : garantie publique, stabilité, convertibilité assurée

Pourquoi faire ?

Souveraineté européenne

13/20 pays en zone euro → réseaux de cartes internationaux (VISA/Mastercard)

Paiement mobile dominé par **Apple Pay/Google Pay**

Fragmentation des paiements

Systèmes nationaux (CB, Girocard, iDEAL, Bizum, EPS) **non interopérables**

Paiements transfrontières reposent presque entièrement sur VISA/Mastercard

Pourquoi faire ? (cont.)

Déclin du cash comme moyen de paiement

- Le cash est la **seule forme de monnaie centrale accessible au public**
- Son utilisation **chute rapidement** : 68% des paiements en 2016, 43% en 2024[1]
- Le reste (virements/prêts) repose sur des **acteurs privés** (banques, big tech)
- **Réduction de légitimité/capacité d'action/confiance systémique**

Avantages variés

- **Coûts réduits** pour les utilisateurs, **résilience** (payer hors ligne, infra. distribuée)
- Stabilité et confiance : euro numérique **garanti par la BCE**

[1] Banque de France - L'usage des espèces se réduit au profit des paiements par carte et mobile

Avancement du projet

Phases successives

2020 : premier rapport de la BCE sur l'euro numérique

2021–2023 : **phase d'investigation** (faisabilité, architecture, prototypes)

2023–2025 : **phase de préparation** :

Élaboration du **rulebook** (règles et standards communs)

Sélection de prestataires techniques (app, SDK, offline, antifraude...)

Expérimentation avec **70 acteurs** (banques, fintechs, universités)

Étapes à venir

2026 : adoption attendue du règlement (Parlement & Conseil)

2027 : lancement possible d'un **pilote en conditions réelles**

2029 : **première émission potentielle** de l'euro numérique

Investigation – Besoins utilisateurs

Commerçants

- **Frais bas** et prévisibles
- **Fiabilité** même en cas de faible connectivité (mode hors ligne)
- Moindre charge administrative, règlement immédiat des fonds

Citoyens

- Paiements **simples, rapides, sécurisés**
- **Suivi en temps réel** des dépenses
- Utilisable partout dans la zone euro

Confidentialité (pseudonymat, mode hors ligne)

Investigation – Innovations étudiées

Nouveaux usages de paiement – Programmabilité

Paiement hors ligne : fonctionnement sans réseau, confidentialité

Paiements conditionnels : pay-on-delivery/per-use, remboursements automatisés

Réservation de fonds : montant bloqué puis libéré une fois la condition remplie

Simplification et modernisation

E-tickets : reçus électroniques chiffrés, **réduction des coûts/déchets**

Mobilité et transports : tap-and-go, calcul automatique du meilleur tarif

Inclusion financière

Portefeuilles éducatifs pour enfants

Accès simplifié aux aides, aux réductions et aux services publics

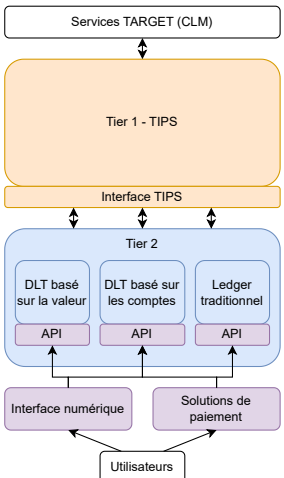
Concrètement, comment ça marcherait ? Le “Tiered model”

Terminologie

TARGET - Infrastructures de paiement de **gros** de l’Eurosystème

CLM - Gestion centralisée de la **liquidité** des banques

TIPS - Plateforme de paiements **instantanés** (SEPA Instant)



Concrètement, comment ça marcherait ? Le “Tiered model” (cont.)

Tier 1 : Eurosystème

Registre **centralisé** (multi-région, haute résilience)

Émission des euros numériques et **règlement final**

Pas de consensus distribué

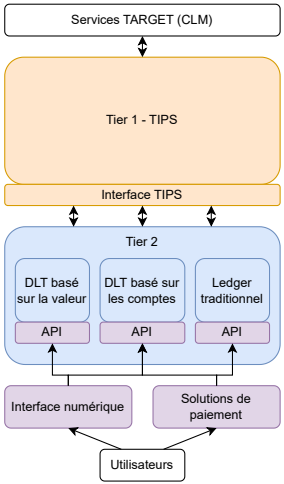
Tier 2 : banques (BNP Paribas), PSP (Revolut), ...

Gestion des portefeuilles/comptes utilisateurs

KYC/AML, interface client, services additionnels

Ledger distribué ou non, au choix

Contrôle total sur l’émission/la quantité en circulation



Partenaires technologiques sélectionnés (15/10/2025)

Finalisé après un Call for Applications.

Composant	Prestataires sélectionnés
Alias lookup	Sapient GmbH & Tremend ▪ equensWorldline
Gestion risque & fraude	Feedzai ▪ Capgemini Deutschland
Application mobile & SDK	Almaviva SpA & Fabrick SpA ▪ Sapient & Tremend
Paiement hors ligne	Giesecke+Devrient ▪ equensWorldline
Échange sécurisé des données	Senacor FCS ▪ equensWorldline

Accords signés - développement effectif conditionné à l'adoption du rulebook

Expérimentation – Choix technologique au niveau 2

Flexibilité pour les intermédiaires

- **Infrastructures classiques** : bases SQL, API, systèmes de paiement existants
- DLT **privés/permissionnés**
- DLT **publics/non-permissionnés**

Espace d'innovation pour Tier 2

- **Programmabilité** : règles de paiement, automatisation
- **Tokenisation d'actifs**, intégration Web3
- Services à valeur ajoutée au-dessus de l'euro numérique

Ledgers testés au niveau Tier 2

Technologie	Accès	Permissions	Modèle	Remarques
Hyperledger Besu	Privé	Permissionné	Compte/valeur	Compatible EVM, smart contracts
Hyperledger Fabric	Privé	Permissionné	Compte/valeur	Architecture modulaire
Tezos	Privé	Permissionné	Valeur	Version interne (fork privé)
NEM (fork privé)	Privé	Permissionné	Valeur	Blockchain entreprise, contrôlée
Ledger bancaire traditionnel (SQL)	Privé	N/A	Compte	Pas de consensus distribué

Aucun ledger public/non-permissionné n'a été testé

Pourquoi utiliser une blockchain...

...privée ?

- Automatisation par **smart contracts**
  - Paiements conditionnels
  - Réservation de fonds
- Traçabilité sectorielle pour **auditer**

...publique ?

- **Notarisation** : preuve d'existence / horodatage immuable
- **Tokenisation externe** : représentation d'actifs dans l'écosystème Web3
- **Interopérabilité** : ponts avec écosystèmes DeFi
- **Transparence** : publication de certaines opérations

Avec modération - La vision de la BCE sur les cryptoactifs

Bitcoin selon la BCE

Bitcoin = **cryptoactif** : pas d'émetteur public ni d'entité responsable.

Très peu accepté pour les paiements ; **transactions lentes et coûteuses**.

Risques pour l'utilisateur

Pas de protection légale : aucune garantie si perte/vol.

Volatilité extrême : pas une **réserve de valeur** fiable.

Actif **spéculatif** : gains possibles mais risque élevé de perte.

Les stablecoins selon la BCE

Stablecoins = promesse d'une entreprise privée, sans garantie publique.

Incertitude sur les réserves réelles et la capacité de remboursement.

La BCE a raison sur les cryptoactifs

Système de paiements **sans tiers de confiance** (e.g., banque, Etat)

Ces cryptoactifs sont-ils des monnaies?

- Unité de compte – Mesure commune pour comparer les biens
- **Intermédiaire entre les échanges** – A la place de l'échange de biens
- **Réserve de valeur** – Transfert du pouvoir d'achat dans le temps, valeur stable

Pour l'instant, les cryptoactifs restent des monnaies partielles

- Intermédiaire entre les échanges – **Verrous technologiques**

Les verrous technologiques de la blockchain

Verrou 1 - Passage à l'échelle – Stockage

650 Go pour Bitcoin, 1.3To pour Ethereum

Données de la blockchain **grandissent linéairement**

Verrou 2 - Passage à l'échelle – Débit

Limites **inhérentes**

5-7 tx/s pour Bitcoin, 13-15 tx/s pour Ethereum

2000-65,000+ tx/s pour VISA

Verrou 3 - Consensus – Alternatives

Preuve de travail et **environnement**

Verrou 1 - Le stockage

Verrou 1 - Passage à l'échelle du stockage

Travaux réalisés avec Dorian Pacaud, Nathanël Derousseaux-Lebert, Emmanuelle Anceaume, Romaric Ludinard (CCS'25)

Deux types de données

- Application (e.g. transactions, soldes de comptes)
- Consensus (e.g. Merkle root, nonce)

Les données d'application peuvent croître/décroître, mais les **données de consensus croissent linéairement dans le temps**.

Actuellement...

- 780 Go pour Bitcoin
- 1,4 To pour Ethereum

Prohibitif pour les appareils mobiles ou la communication inter-chaînes

Clients légers et super-légers

Simplified Payment Verification (SPV)[2]

Télécharge uniquement les en-têtes de blocs (données de consensus)

Complexité **linéaire**

FlyClient[3]

Le participant qui bootstrappe demande des blocs spécifiques en défi/réponse

Complexité **logarithmique**, **interactif** $\rightarrow$ On conserve l'intégralité de la chaîne

[2] Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. 2008

[3] Bünz *et al.* *FlyClient: Super-Light Client for Cryptocurrencies*. S&P 2020

Clients légers et super-légers (cont.)

Non-Interactive Proof of Proof-of-Work (NIPoPoW)[4]

Les **provers** construisent et envoient des preuves à un **verifier**, qui accepte la bonne

Preuve = représentation **succincte** de la blockchain sous-jacente

Une interaction, mais **ne fonctionne que si la difficulté de minage est constante**

Diamond block NIPoPoWs[5]

Attribution d'un poids aux blocs $\rightarrow$ empêche la suppression de blocs bien choisis

Meilleure tolérance aux adversaires $(1/2)$, mais toujours avec difficulté constante

[4] Kiayias *et al.* Mining in Logarithmic Space. CCS 2021

[5] Jain *et al.* Extending The Boundaries and Exploring The Limits Of Blockchain Compression. SRDS 2023

Le problème auquel on apporte une réponse

Peut-on construire et vérifier **sans interaction** une représentation **succincte** d'une blockchain basée sur la preuve de travail dans un système **non-permissionné** ?

Protocole de prover sécurisé

Succinctess — $|\Pi| = O(\log |\mathcal{C}|)$, où $\Pi = \mathsf{Compress}(\mathcal{C})$

Onlineness (minage sur la preuve) — $\mathsf{State}(\mathcal{C}) = \mathsf{State}(\Pi)$

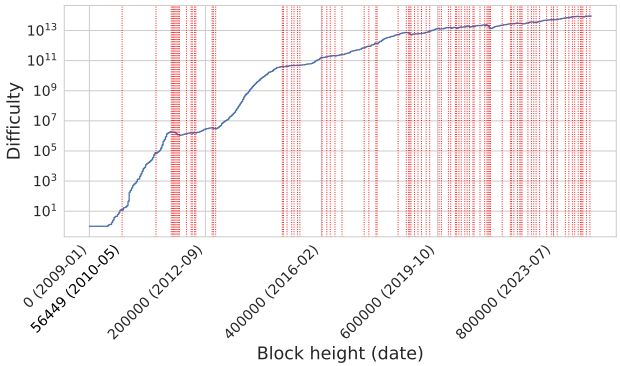
Protocole de verifier sécurisé

Security — $\mathsf{Compare}(\Pi, \Pi') = \Pi$, où Π est la preuve accumulant la plus grande quantité de difficulté

Difficulté variable dans un système non-permissionné

Les participants peuvent **rejoindre** ou **quitter** le réseau à tout moment

Target recalculée à chaque époque (2 016 blocs) $\rightarrow$ maintenir un délai inter-blocs de 10 minutes



Défis

1. **Stratégie d'échantillonnage des blocs**

   Quels blocs ? **Combien** ?

   Des empreintes de blocs identiques peuvent masquer des difficultés différentes, affectant la **rareté**

2. **Prévention des attaques à faible difficulté**

   Impossible de vérifier que la difficulté des blocs échantillonnés est légitime

   Présentation d'une preuve **indiscernable** de celle des participants honnêtes

   Présentation d'une preuve pour une chaîne plus longue (difficulté réduite)

3. **Choix d'un paramètre de sécurité robuste K**

   Choisir K pour que le verifier rejette les NIPoPoWs invalides w.h.p.

Défi 1 - Superblocs

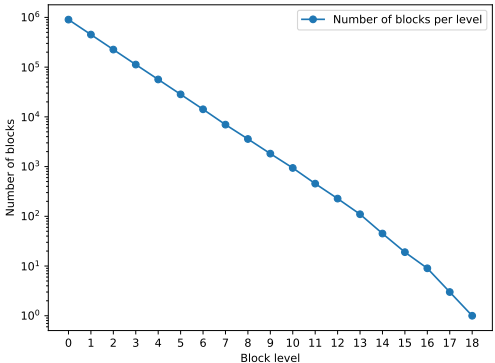
Tout bloc valide satisfait la Proof-of-Work pour une target T : $H(ctr||x||s) \leq T$

Les superblocs satisfont **"mieux"** la PoW :

$$H(ctr||x||s) \leq \frac{T}{2^{\mu}} \; avec \; \mu \in \mathbb{N}$$

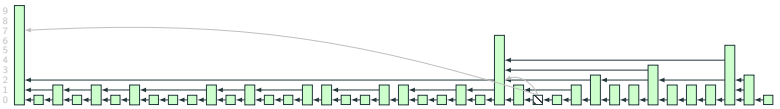
où μ désigne le **niveau** du bloc

Obtenir un bloc de niveau 5 demande en moyenne 2^5 blocs valides

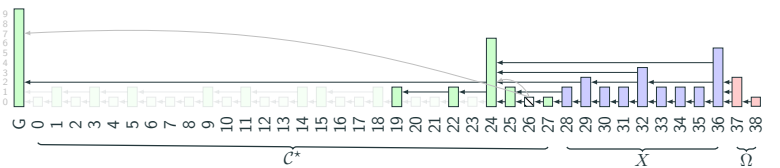


Défi 1 - Compression de la blockchain

(a) Bitcoin avant compression.



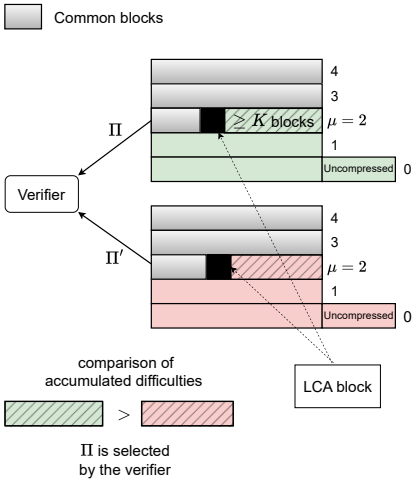
(b) La hauteur d'un bloc représente son niveau, les flèches représentent la structure d'inter-liaison.



(c) NIPoPoW

Conserver les derniers $X + k$ blocs, et les derniers $2K$ blocs à chaque niveau est **suffisant** pour qu'un vérificateur soit **convaincu** que la preuve présentée est **correcte**

Défis 2 & 3 - Comparer les preuves via le Dernier Ancêtre Commun (LCA)



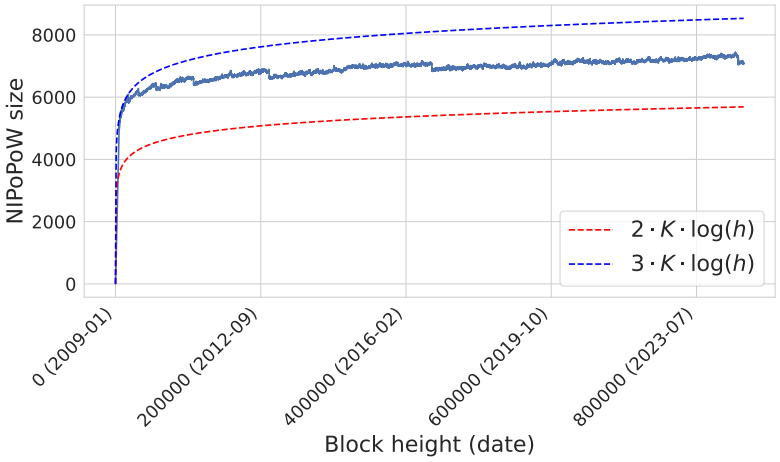
LCA — Dernier bloc partagé par Π et Π'

Π ou Π' possède **au moins K blocs** après le LCA

Borne inférieure sur K via distribution de Poisson et **Gambler's ruin** avec récompenses variables

Taille de la preuve à partir des données Bitcoin

On garde 7 075 blocs (**327 MB + snapshot**) sur 865 043 (**650 GB**) (oct. 2024)



Points clés

Contributions

- Construction d'une NIPoPoW fonctionnant avec une **difficulté variable**
- Preuves de sécurité et de succinctness, dimensionnement du paramètre K
- Implémentation et mesures utilisant les données de Bitcoin

Perspectives

- Améliorer pour un adversaire à $1/2$
- Preuves non-interactives pour d'autres types de consensus, e.g. **Proof-of-Stake**

Verrou 2 - Le débit

Verrou 2 - Passage à l'échelle du débit

Bitcoin - 5-7 tx/s

Ethereum - 13-15 tx/s

VISA - 2000-65,000+ tx/s

Ces débits sont intrinsèquement limités

Quel est le problème avec e.g. Bitcoin ?

Problèmes inhérents au fonctionnement des blockchains type Bitcoin

Raison 1 - Chaque nœud garde une copie du ledger

Plus il y a de nœuds, plus la **latence** augmente

Gossip de 2MB à 90% de 4000 nœuds prends ~ 50 secondes

En un sens, Bitcoin sacrifie le passage à l'échelle pour la **décentralisation**

Raison 2 - Le débit reste fixe

Comment faire pour augmenter le débit?

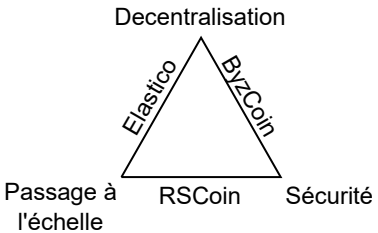
Trilemme de la blockchain

Vitalik Buterin - Inevitable tradeoffs between 3 significant properties

Décentralisation - Chaque nœud garde une copie du ledger

Sécurité - Les nœuds sont en accord sur l'état du ledger

Passage à l'échelle - Le débit augmente avec le nombre de nœuds



Tradeoffs difficiles à éviter

Plusieurs solutions possibles

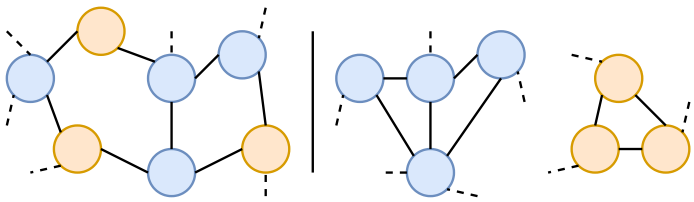
Layer 0 - Optimisation sous-jacente (BDN, bloXroute)

Layer 1 - On-chain (SegWit, DAG, **sharding**, consensus)

Layer 2 - Off-chain (state channels, side chain, cross-chain, off-chain)

Vitalik Buterin - Sharding is the most promising solution to break the trilemma

Types de sharding - Sharding du réseau

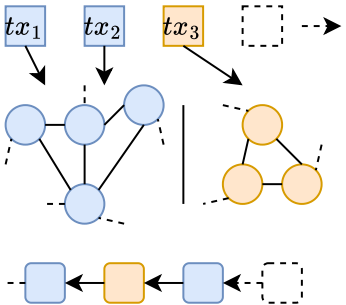


On divise le réseau en **comités/shards**

Sharding au niveau des **communications**

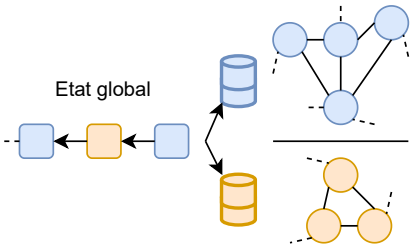
Types de sharding - Sharding des transactions

Diviser les **transactions** en groupes



Types de sharding - Sharding de l'état

Diviser le **stockage** entre les shards



Avancement en recherche

Pas de simulation/plateforme expérimentale

- Difficulté pour **tester/valider** de nouvelles idées
- La plupart des protocoles de sharding modifient e.g. Bitcoin/Ethereum
- $\Rightarrow$ Composants très connectés, **pas modulaire**

Pas d'outils de benchmark

- Difficile de **comparer les protocoles**
- Difficile de **reproduire les résultats**
- Code pratiquement jamais en ligne

En cours d'implémentation dans Ethereum

Récapitulatif

Verrou 1 - Passage à l'échelle – Stockage

Travaux sur les **NIPoPoWs**

Verrou 2 - Passage à l'échelle – Débit

Pistes : **sharding**, graphes orientés

Verrou 3 - Consensus – Alternatives

Preuve d'**enjeu** à la place de la preuve de travail

Comment combiner ces solutions entre elles ?

Ouvertures sur l'euro numérique

Questions non-abordées/en suspens

- Argent public vs privé - place du secteur bancaire ?
- Plafond sur les avoirs - **stabilité vs liberté d'usage**
- Coûts et seigneuriage - qui paie quoi ?
- Confidentialité - cash-like vs conformité AML
- Programmabilité - **services+ vs monnaie conditionnée**
- Dépendance réseau/énergie, rôle du hors ligne

Géopolitique

- Stratégie des U.S. ?
- Initiative des BRICS ?
- Rôle international de l'euro ?

Gouvernance

- **Europe centralisée vs fédérale ?** (T. Sowell)

Why the uncompressed part?

Parameter χ spans two epochs

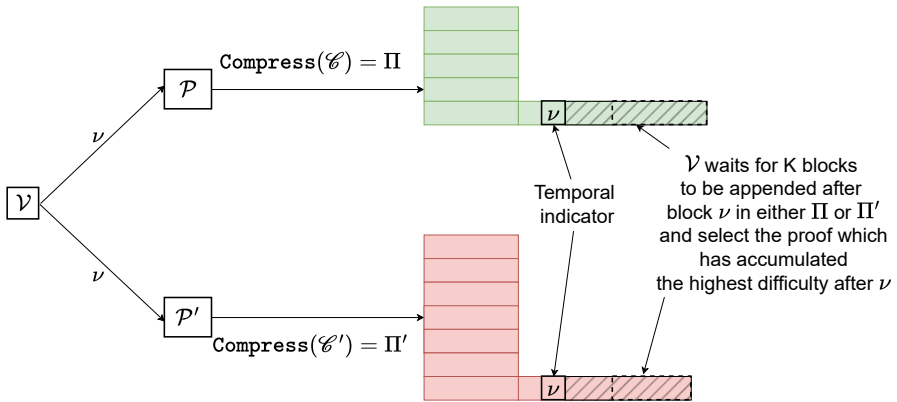
Guarantees the uncompressed subchain contains at least all blocks in one epoch

Difficulties of following blocks **can be checked**.

What happens if there is no LCA?

Temporal indicator sent by verifier at bootstrap

Insertion into coinbase with OP_RETURN message

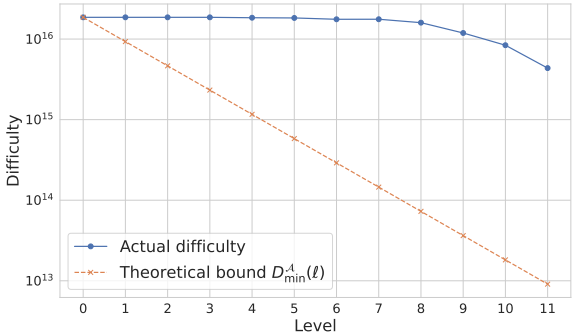


Dimensioning of security parameter K

Two-phase competition between two teams

Probability to **catch up** $\Pr\{C_n^\alpha\}$

Gambler's ruin + Poisson



$D_{\min}^{\mathcal{A}}(0)$ is the **highest quantity of difficulty needed**.

NIPoPoW's well chosen blocks: superblocks

Any valid block satisfies the Proof-of-Work equation for target T:

$$H(ctr||x||s) \leq T$$

NIPoPoW's well chosen blocks: superblocks

Any valid block satisfies the Proof-of-Work equation for target T:

$$H(ctr||x||s) \leq T$$

Superblocks satisfy this equation **"better"**:

$$H(ctr||x||s) \leq \frac{T}{2^{\mu}} \; with \; \mu \in \mathbb{N}$$

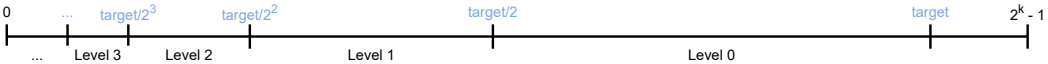
NIPoPoW's well chosen blocks: superblocks

Any valid block satisfies the Proof-of-Work equation for target T:

$$H(ctr||x||s) \leq T$$

Superblocks satisfy this equation **"better"**:

$$H(ctr||x||s) \leq \frac{T}{2^{\mu}} \; with \; \mu \in \mathbb{N}$$



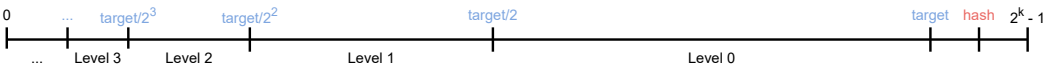
NIPoPoW's well chosen blocks: superblocks

Any valid block satisfies the Proof-of-Work equation for target T:

$$H(ctr||x||s) \leq T$$

Superblocks satisfy this equation **"better"**:

$$H(ctr||x||s) \leq \frac{T}{2^{\mu}} \; with \; \mu \in \mathbb{N}$$



NIPoPoW's well chosen blocks: superblocks

Any valid block satisfies the Proof-of-Work equation for target T:

$$H(ctr||x||s) \leq T$$

Superblocks satisfy this equation **"better"**:

$$H(ctr||x||s) \leq \frac{T}{2^{\mu}} \; with \; \mu \in \mathbb{N}$$

NIPoPoW's well chosen blocks: superblocks

Any valid block satisfies the Proof-of-Work equation for target T:

$$H(ctr||x||s) \leq T$$

Superblocks satisfy this equation **"better"**:

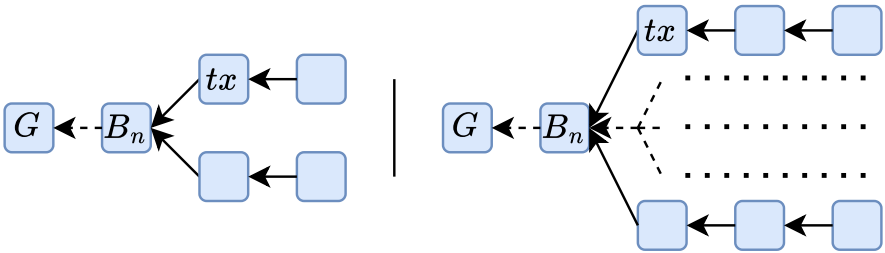
$$H(ctr||x||s) \leq \frac{T}{2^{\mu}} \; with \; \mu \in \mathbb{N}$$

Obtaining a level 5 block takes on average 2^5 valid blocks.

Pourquoi ne pas augmenter la taille des blocs?

Augmenter la taille des blocs augmente la latence

Pourquoi ne pas réduire le délai inter-bloc?



Une réduction du délai inter-bloc augmente le nombre de **forks**

Plus de forks $\Rightarrow$ **Temps de confirmation** de tx augmente