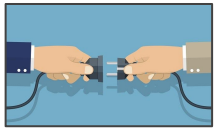
Intégration des blockchains pour la supply chain

En pratique

Chain Accelerator
by ON-X GROUPE

Pourquoi ?

POURQUOI EN ACCÉLÉRÉ :)
RÉPARER L'INTEROPÉRABILITÉ



- La supply chain repose sur l'interopérabilité
- Les standards de l'interopérabilité n'intègrent pas de moyens résilients pour la vérification des flux et des opérations des tiers
- En l'état il est trop risqué d'intégrer des innovations tiers et de partager les informations sans un effort de contrôle et de filtre asynchrone
- Cette rupture est à l'origine de nombreuses autres failles humaines et de détournements via l'exploitation tierce des infrastructures numériques et des données alors ouvertes pour ce contrôle
- Les besoins des services internes, de la chaîne de valeur et des business sont synchrones, pressés par la traçabilité croissante et souffrent partout de cet état de fait : manque de performance, d'agilité, de coopération à grande échelle, de fiabilité, d'auditabilité, et des analyses par métiers et donc "silotés"
- Dans une ère numérique, la supply chain est bridé par une interopérabilité asynchrone due à au manque de résilience des infrastructures numériques (blockchains incluses)
- Dans le spatial, ce sera pire, car qui pourra opérer ces contrôles et arbitrages suffisamment rapidement et sans tension pour une multitudes d'acteurs, équipements et des services en interaction en orbites ?
- Grâce aux crypto-monnaies, un modèle économique ad'hoc permet de rendre résilients les acteurs de la sécurisation.
- Ce socle résilient ouvre la voie à divers niveaux de réseaux de preuves distribuées, permettant des messages et transactions confidentiels et vérifiables
- **Il s'agit d'intégrer un réseau résilients de preuves, et de nouveaux standards d'interopérabilité adaptés à l'ère numériques**
- **Pour les "makers" par les "makers"**

INTEROPÉRABILITÉ

L'interopérabilité fait référence à la capacité des systèmes informatiques ou des logiciels à **échanger et à utiliser des informations.**

Dans la supply chain:

- **des médiums techniques, très numériques, et**
- **des standards internationaux**

Quelle valeur fait office de standard transactionnel universel ? (medium)

INTER-OPÉRER EST VITAL POUR LA SUPPLY CHAIN

❖ La synchronisation est un facteur de compétitivité

Les acteurs doivent **coopérer** pour suivre le rythme de plus en plus exigeant et variable de la **distribution mondiale en temps réel sur internet**

❖ Les flux tirés entre ces acteurs qui contribuent au produit

personnalisation, paramétrage selon les pays, exigences croissante de traçabilité

❖ De plus en plus de documentation transverse

Conditions de production, origines, formations, douanes, autres éléments réglementaires et comptables… à **tenir à jour et partager sur divers niveaux de confidentialité**

LE COEUR TRANSACTIONNEL DE L'ÉCONOMIE RÉELLE EST EN SOUFFRANCE

- **Malgré des business synchrones la co-production reste asynchrone**

Entre les fournisseurs, distributeurs, magasins, transporteurs, tous co-producteurs.

- Pour l'Institution of Civil Engineering : **les enjeux d'interopérabilité sont l'un des obstacles majeurs à la réalisation de la valeur de la transformation numérique**

La transformation numérique est soumise aux enjeux d'interopérabilité.

MANQUE DE CONFIANCE DANS LES INFRASTRUCTURES NUMÉRIQUES

L'interopérabilité joue encore mal son rôle clé dans la performance et l'agilité, la coproduction tout au long de la logistique, contrôle financier, analyse de risque, de la production, de la recherche, de la distribution, des ventes, de la recherche, du “cross”-marketing...

- **Tous ces processus sont coopératifs entre des acteurs qui ne peuvent pas aisément partager leurs états opérationnels**
  - Le flux de états entre les acteurs est asynchrone, peu vérifiable, très partiel, en silos par les acteurs et par nature

IMPACTS POUR LA SUPPLY CHAIN

Lorsqu'il y a un manque de coopération, ou/et une rupture vers les systèmes, ou/et un état opérationnel non vérifiable :

➢ Porte est ouverte aux erreurs, aux fraudes, à la malveillance, à l'espionnage et aux tensions entre partenaires et avec les institutions

IMPACTS POUR LA SUPPLY CHAIN

❖ Intégration du e-commerce

20 ans plus tard … la dure réalité des sites d'achats groupés et ceux qui ont réussi sont les leaders

❖ Nouvelle logistique humanitaire d'urgence

ex. Faible retour après des catastrophes naturelles

❖ Nouvelle urgence sanitaire

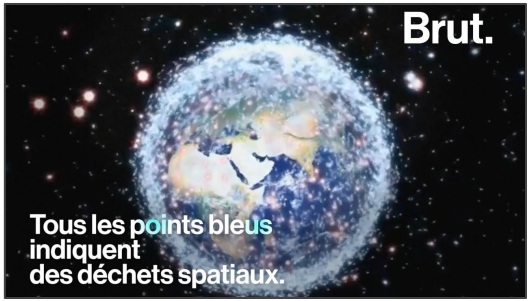
COVID: le manque d'agilité entre circuits

❖ Exigences exponentielles sur la (réelle) traçabilité

Mal adressée avec une exposition des données plus nombreuses, horodatés, signées mais pas peu vérifiables

CRITIQUE POUR LES SUPPLY CHAINS DU SPATIAL

- **L'intégration des flux du spatial dans les supply chains au sol et sa supply chain propre :**
  - aux services en orbites vers la terre (observation de la terre : santé, agriculture, recherche, climat, assurances, votes, domotique, transactions…)
  - aux qualifications et opérations de maintenance et de transport
  - aux équipements et ressources assemblés et/ou transporté et/ou partagés
  - aux missions spatiales
  - à la gestion des débris en orbites et des cycles de vie des matériels
  - aux services entre les équipements en orbite
  - aux services des missions et vaisseaux autonomes
  - aux services des missions d'extractions minières



CRITIQUE EN FINANCE : LACUNE DE LA LUTTE CONTRE LE BLANCHIMENT #FinCENFiles

- Dans la finance et chez les régulateurs, malgré la nationalisation partielle des banques, leurs implications dans les banques centrales, malgré les réglementations fortes et les processus KYC / AML, les FinCENFiles révèlent l'inefficacité des vérifications et des règles opérationnelles d'application.

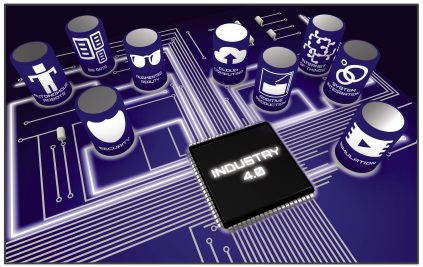
- Les banques ont ainsi permis le financement et le blanchiment de l'argent du terrorisme, de la fraude, de la corruption, des criminels, du contournement des règles internationales, avec des conséquences humaines dramatiques.

- Les informations étaient présentes mais il n'y a pas eu les interventions requises, notamment :

  - faute d'interopérabilité
  - **faute de moyens de vérification des exécutions opérationnelles des acteurs**
  - de failles humaines (& corruptions)

CRITIQUE POUR L'INDUSTRIE 4.0 : FREIN À L'INTÉGRATION DE L'INNOVATION

- Sans trop s'exposer et sans trop partager, mais dans un flux continu.
- Pour rester compétitives, les industries sont contraintes d'intégrer à un rythme exponentiel divers nouveaux flux



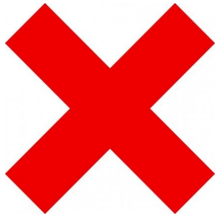
=> Elles atteignent une limite liée à la vérifiabilité et aux compétences requises pour ce diagnostic

- l'interopérabilité conduit à un risque majeur de perte de contrôle des données et des informations qui circulent entre les équipements.
- Sans pouvoir maîtriser le risque dans le système d'information, les flux et parfois les projets sont interrompus

ERE NUMERIQUE

Tout le monde, chaque industrie et chaque organisation est contraint par le manque de confiance :

- dans les infrastructures numériques
- dans l'exécution réelle dans organisations humaines



LA PIÈCE MANQUANTE DANS LE SYSTÈME D'INFORMATIONS

Ce n'est pas l'objet :

- Des outils du système d'information, TMS, ERP, BPM, CRM…
- Des moyens de sécurité et d'intégration des données
- Des réseaux et interfaces disponibles pour échanger les informations

Il manque une brique technique pour vérifier et protéger la confidentialité : des flux EDI, certificats, certificats, opérations, rapports, données, accords, transactions… **reçus des processus transverses des industries et des plateformes.**

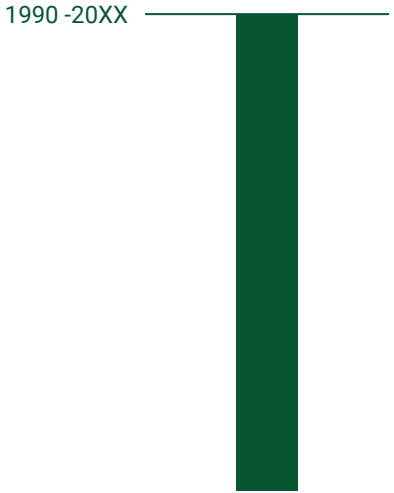
POURQUOI CONTRIBUER À CONSTRUIRE ET DÉPLOYER CETTE BRIQUE MANQUANTE ?

Il n’y aura pas de politique commune :

- Qui finance des infrastructures transverses ?
- Qui peut choisir de (dé)gouverner ces infrastructures ?

=> Codons ce réseau résilient de preuves transverses, totalement ad’hoc et sans compromis

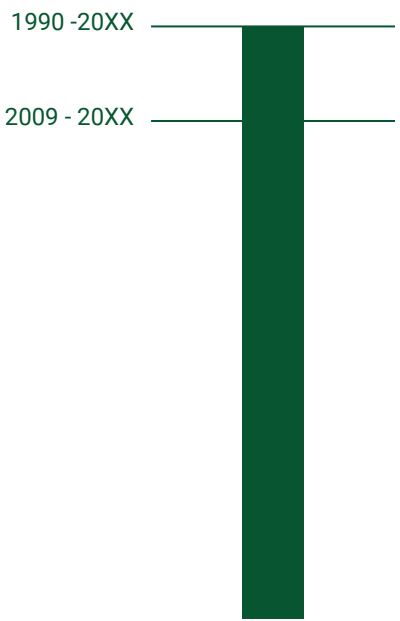
ERE NUMÉRIQUE AVANT/APRÈS LES CRYPTO-MONNAIES



Avant les crypto-monnaies : facile de corrompre les infrastructures, centraliser les données des industries et institutions, et de les traiter avec opacité

- Les systèmes d'informations, blockchains incluses ne permettaient pas d'assurer la résilience (exploitations tierces, espionnage, corruption...)
- Énormément d'équipements et réseaux tiers (opérateur télécom, serveurs de temps, autorités de certifications…).
- Arbitrage obligatoirement centralisé sur les enrôlements et sur les versions concurrentes des historiques sur les réseaux.

ERE NUMÉRIQUE AVANT/APRÈS LES CRYPTO-MONNAIES

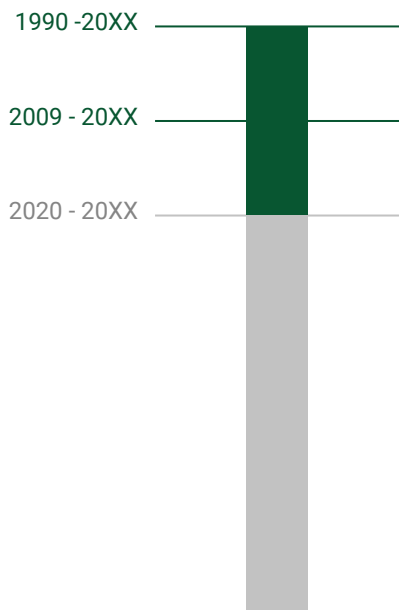


Avant les crypto-monnaies : facile de corrompre les infrastructures, centraliser les données des industries et institutions, et de les traiter avec opacité

Avec les crypto-monnaies : un modèle économique viable et robuste pour la résilience des opérateurs de la sécurisation des échanges sur les infrastructures numériques (niveau 1)

- L'invention d'une monnaies de la résilience des infrastructures numérique
- Spécifique, minimaliste, strictement mathématique, de juste émission de jetons contre de l'énergie à bas coût et l'investissement dans un matériel spécifique pour les calculs qui sécurisent le réseau
- Requiert une décentralisation et une résilience à tout (dont les gouvernances et les régulations).

ERE NUMÉRIQUE AVANT/APRÈS LES CRYPTO-MONNAIES



Avant les crypto-monnaies : facile de corrompre les infrastructures, centraliser les données des industries et institutions, et de les traiter avec opacité

Avec les crypto-monnaies : un modèle économique viable et robuste pour la résilience des opérateurs de la sécurisation des échanges sur les infrastructures numériques (niveau 1)

Après les crypto-monnaies : des réseaux de blockchains confidentielles pour la co-vérification d'exécutions, de preuves opérationnelles et des médiums/standards communs (niveaux 2, avec des états agrégés et certifiées sur le niveau 1 résilient)

- Des représentations multi-signées et programmables de tous biens et services physiques ou numériques, matériels ou immatériels, fongibles ou non fongibles, quantifiables ou non quantifiable, provenant d'humains ou de machines, on-line ou off-line…

ERE NUMERIQUE : DEBRIDER L'INTEROPÉRABILITÉ

Au final, un systèmes vérifiable permettant des flux numériques :

- ❖ Plus ouverts que le souverain
- ❖ Plus protecteurs que les GAFAMs

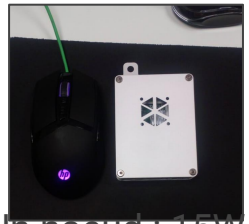
L’opportunité de nouveaux standards numériques, universels et vérifiables :

- ❖ Sécuriser nos messages et transactions dans une ère numérique
- ❖ Débrider l'interopérabilité entres les systèmes d’information

Comment ?

En pratique

SANS COMPROMIS



Un noeud : 15W

- Urbanisé
- Résilient
- Sécurisé
- Confidentiel
- Auditable
- Fiable
- Rapide
- Scalable
- “Vert”
- Transactions gratuites
- Inter-opérable

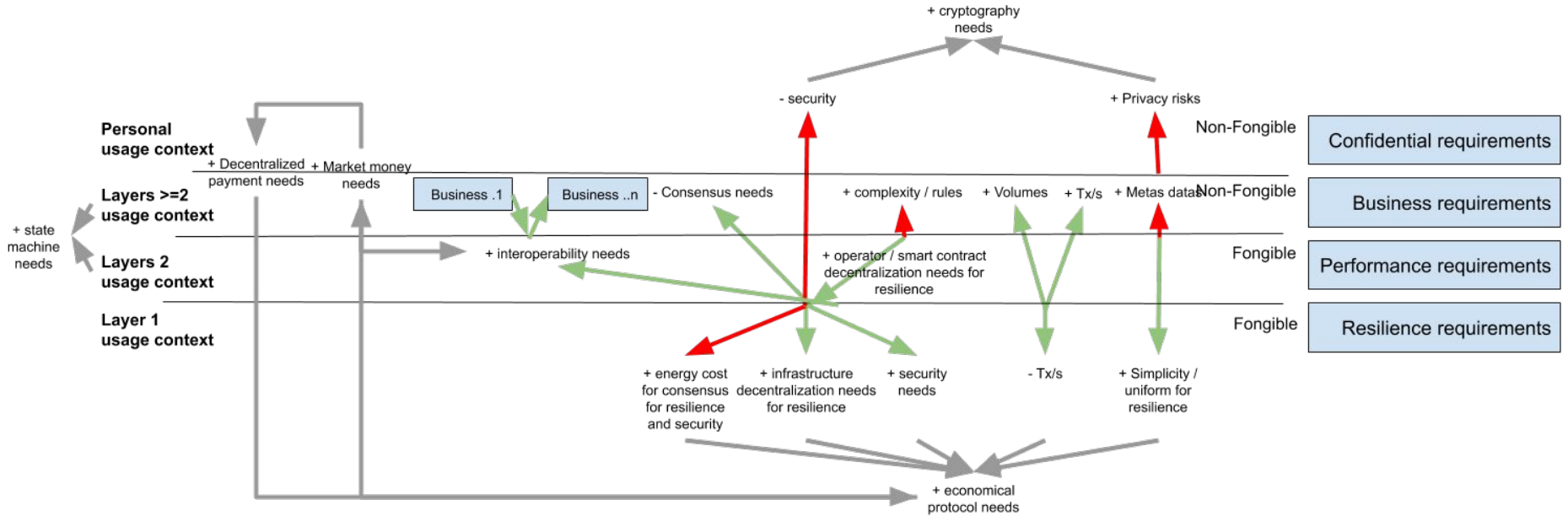
Et bien plus…

- **Un plan B financier et une sécurisation des flux à l’international**
- Urbanisé : à la fois publique, fédéré, et privé; fongible et non fongible, de certifications uniques et d’agrégats…
- Résilient sans compromis avec de la Proof Of Work
- Résilient sans coût énergétique déraisonnable
- Résilient aux centralisations géographiques
- Hautement sécurité, pas de code “maison” en dehors des API métier des noeuds, pas de langages turing complet, pas de blockchain indexées par les adresses, pas de validations techniques via des serveurs tiers (certifcats, serveurs de temps…)
- Très rapide, sans limite de passage à l’échelle
- Quasiment gratuit à la transaction
- Sans smart contrat (les multi-signatures natives remplissent toutes les exigences)
- Confidentiel par défaut
- Auditable avec des clés d'audit reposant sur zero knowledge proof
- Interopérable entre les services et réseaux
- Représentant des biens physiques, numériques, matériels, immatériels, fongibles, non fongibles…
- Certifiant ces représentations
- Agile dans les gouvernances, pouvant être complexes, régies par les utilisateurs
- Evolutif fonctionnellement et techniquement (Agnostique techniquement
- Sans dépendance aucune à une communauté tierce
- Autonome jusque dans une maintenance minimaliste et sans acteur ou système tiers (pas de certificats)
- Intégration natives des mécanismes de dépôts, garanties, tiers encaissements…

OSER REBATTRE LES CARTES DES CHOIX TECHNOLOGIQUES

- **Nouveaux frameworks** : Elements, Zendoo…
- **Innovations et outils dans les multi-signatures** : taproot, schnoor...
- **Nouvelles architectures en couches** : sidechains, canaux, pegs…
- **Utilisation plus industrielle/intégrée de technologies confirmées** : Bitcoin 12 ans sans interruption et la résilience du PoW
- **Obsolescences à venir :** smart contracts, PoS, du choix de technologies en fonction de registres public/privé/consortium...

POURQUOI URBANISER ?



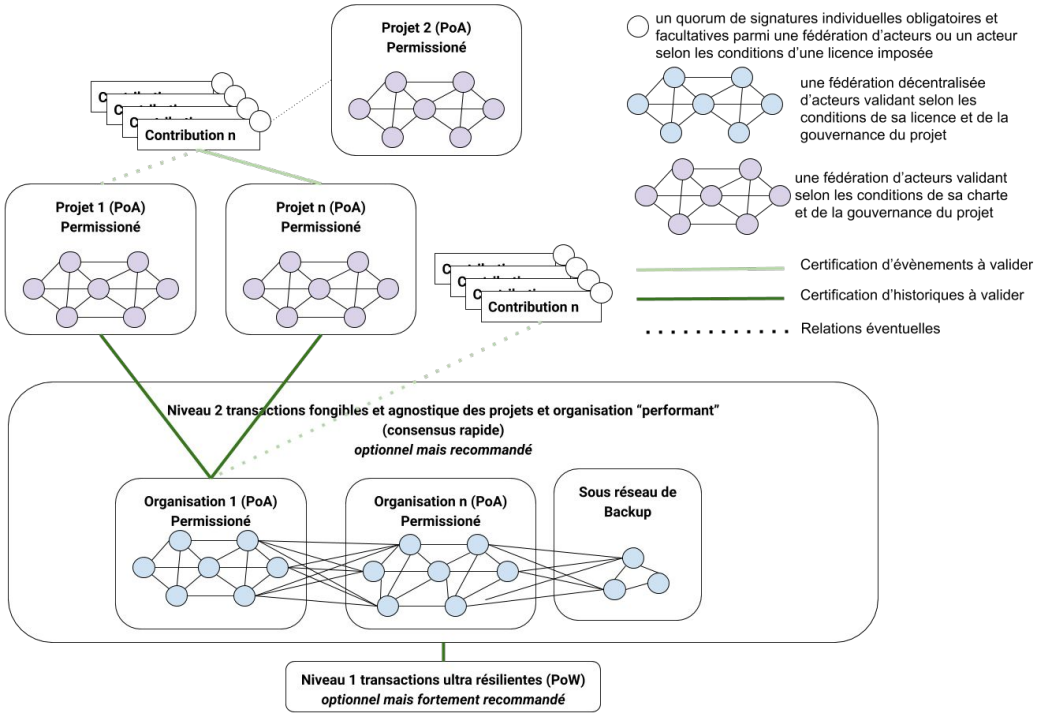
Comment urbaniser ?

Cas de bitcoin

1 transaction sur Bitcoin peut certifier des milliers de transactions en layer 2.

Bitcoin est un excellent moyen de sécurisation “ l’aveugle” (agrégat distinctif) et à bas coût énergétique.

Le système est relativement agnostique technologiquement.

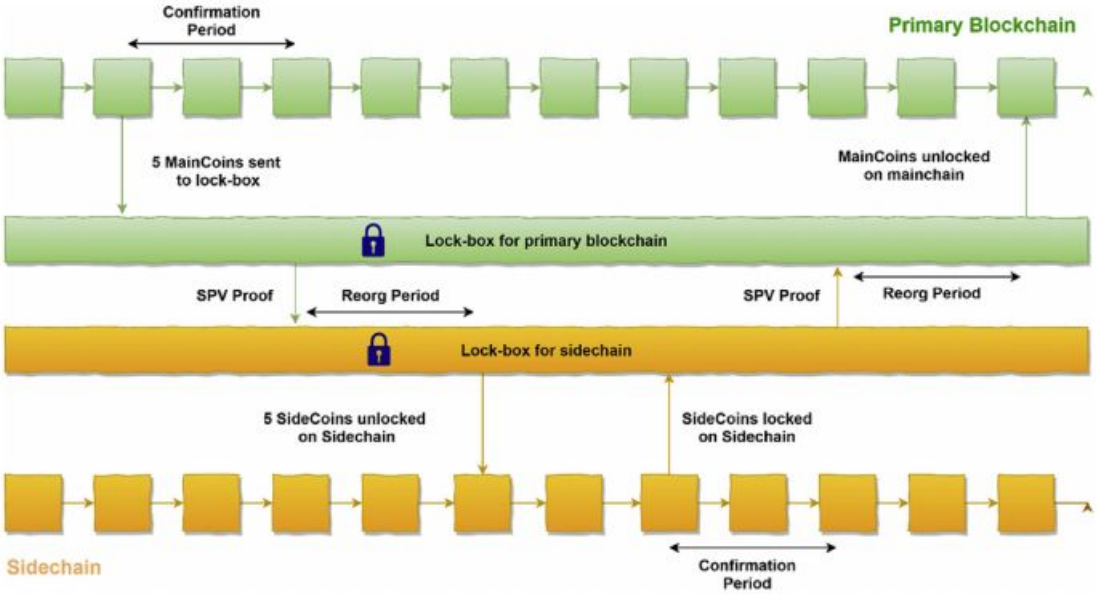


COMMENT INTER-OPERER DES BLOCKCHAINS ?

SPV (preuves de possession)

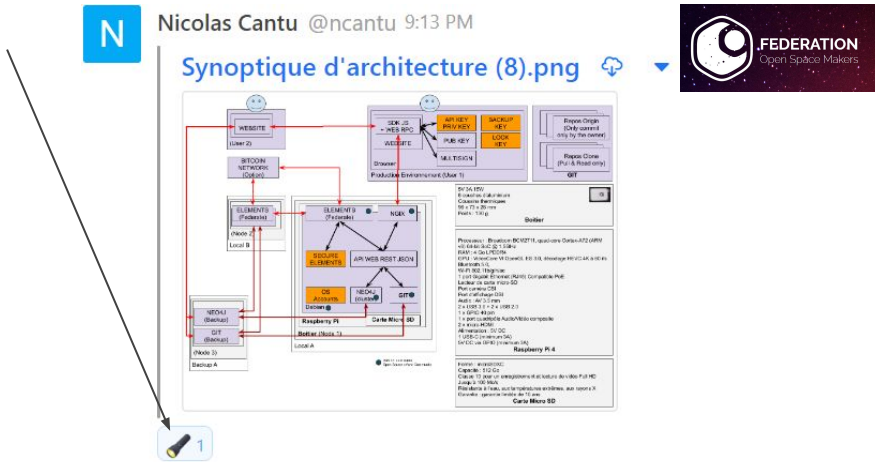
échangées via

2 peg way



COMMENT L'UTILISATEUR PROCÈDE-T-IL ?

En un clic: je protège ma propriété intellectuelle, j'émets un droit qui correspond à l'organisation à laquelle appartient mon projet, à la charte de mon projet, à la licence de mon projet et à mon rôle dans les divers niveau, intégrant les droits parents, NDA, recherche fine et confidentielle, conditions de transferts...



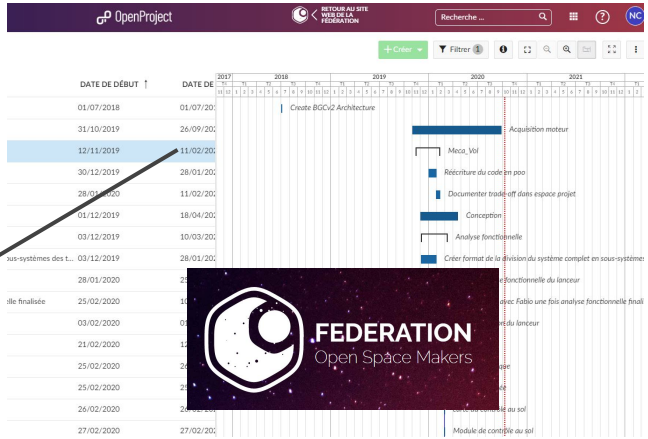
En un scan: mon vétérinaire est réglé de sa prestation en fonction de ma couverture mutuelle et le carnet de santé de Tagada est mis à jour via un QR sur le colier connecté (LoRa)

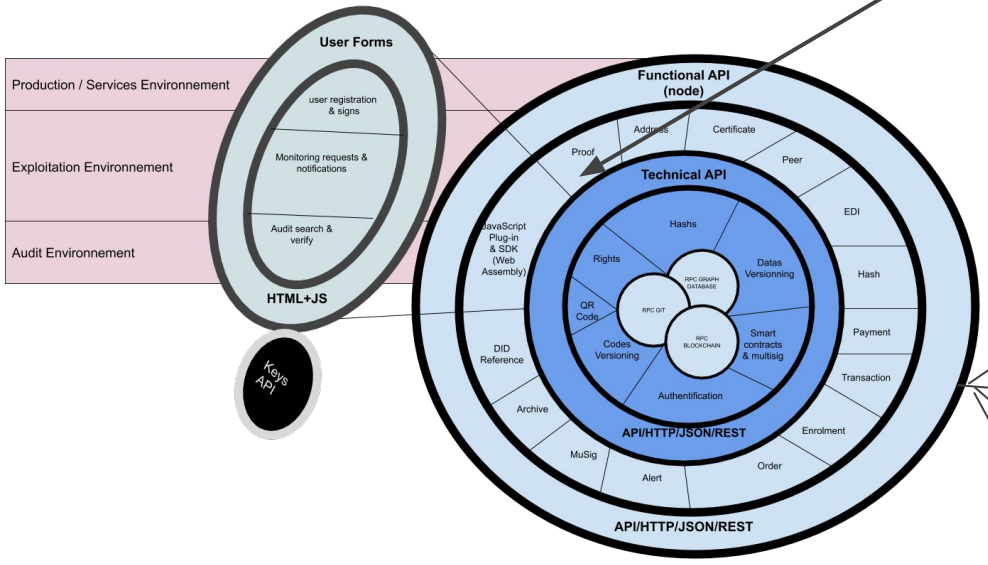
LAEKA
The care we share

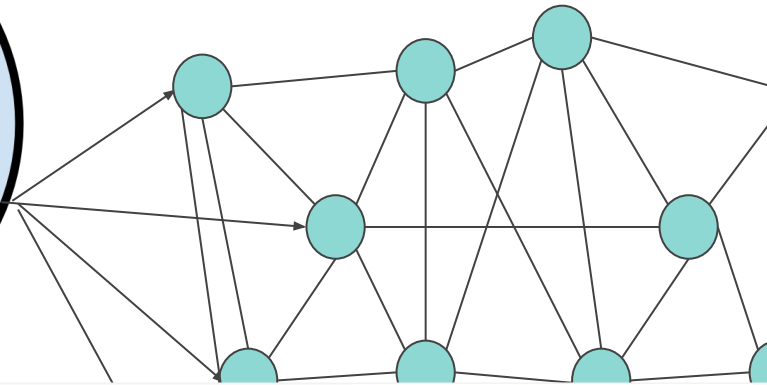
Chain Accelerator
by ON-X GROUPE

Automatiquement: à la fin d'une tâche dans un outil, cet état est envoyé pour preuve et certification.

COMMENT LES SYSTÈMES PROCÈDENT-ILS ?

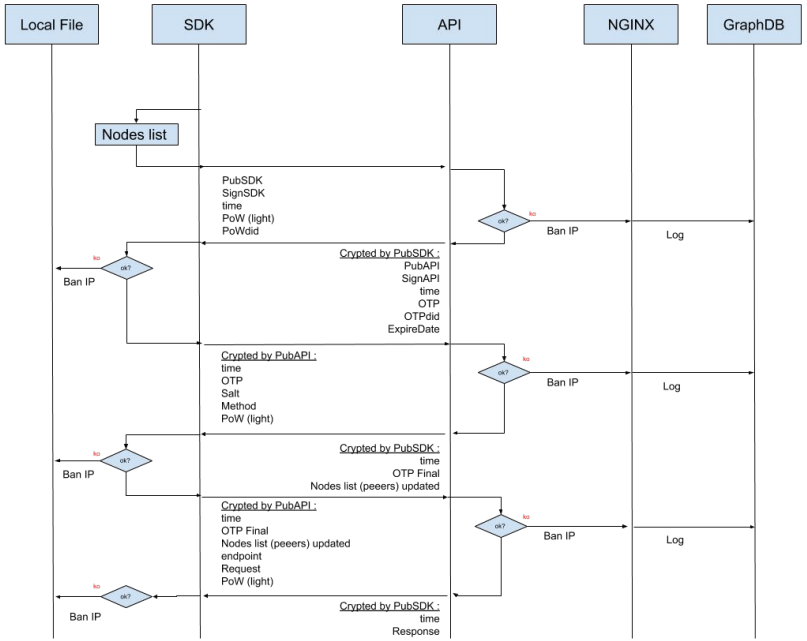






Chain Accelerator
by ON-X GROUPE

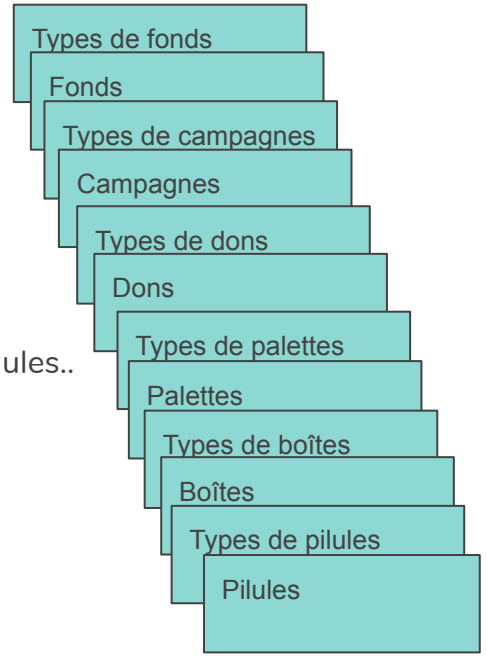
COMMENT SÉCURISER LES FLUX VERS LES APIs WEB (W3C DIC & VC) DU RÉSEAU SANS CERTIFICAT ?



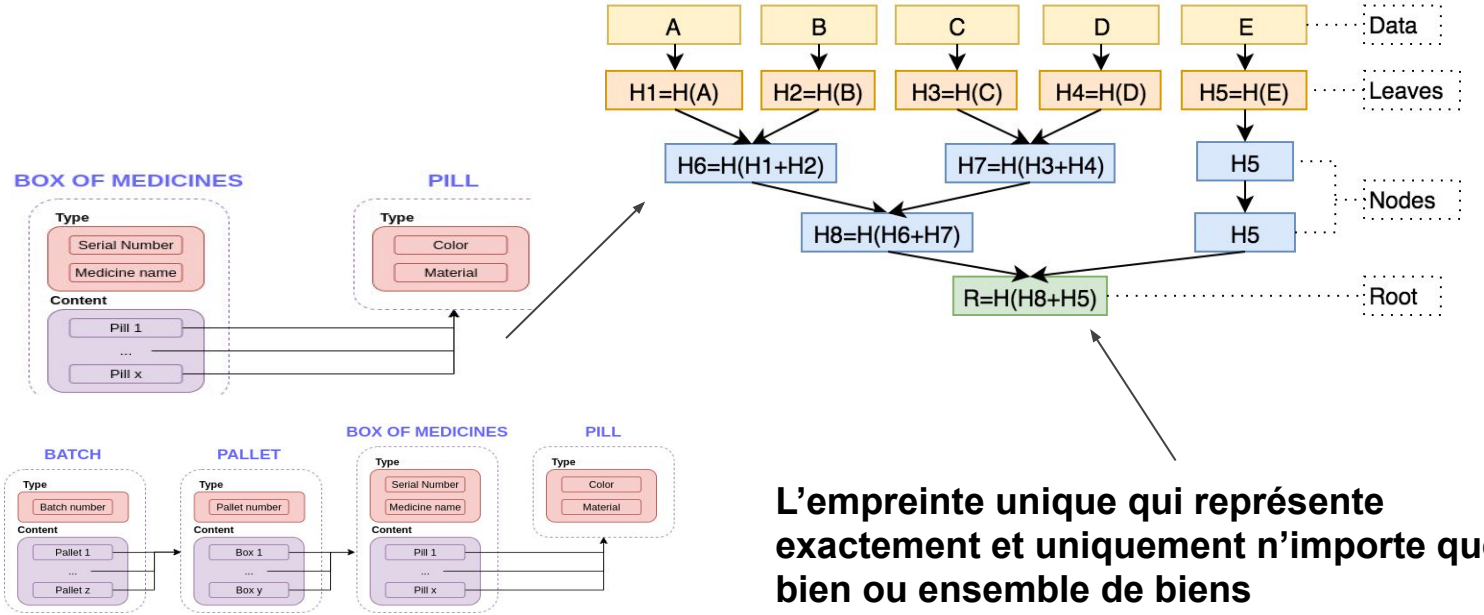
Chain Accelerator
by ON-X GROUPE

COMMENT REPRÉSENTER DIFFÉRENTS NIVEAUX DE GESTION LOGISTIQUE DANS MA PREUVE ?

- **Dispensation à la pilulle**
- **Plusieurs types différents** dans une même boîte
- **Relations aléatoires** entre les pilules, les fonds, palettes, boîtes...
- **Des relations en n (expéditeurs) to m** (destinataires) pour chaque types
- **Des volumes variables** pour le même type de campagnes, palettes, boîtes, types de pilules..
- **De grands volumes**
- **Mauvaise connectivité**
- **Environnement parfois peu adapté** au matériel informatique (électricité)
- **Normes pas toujours suffisantes** pour décrire les pilules et/ou le contenu des boîtes

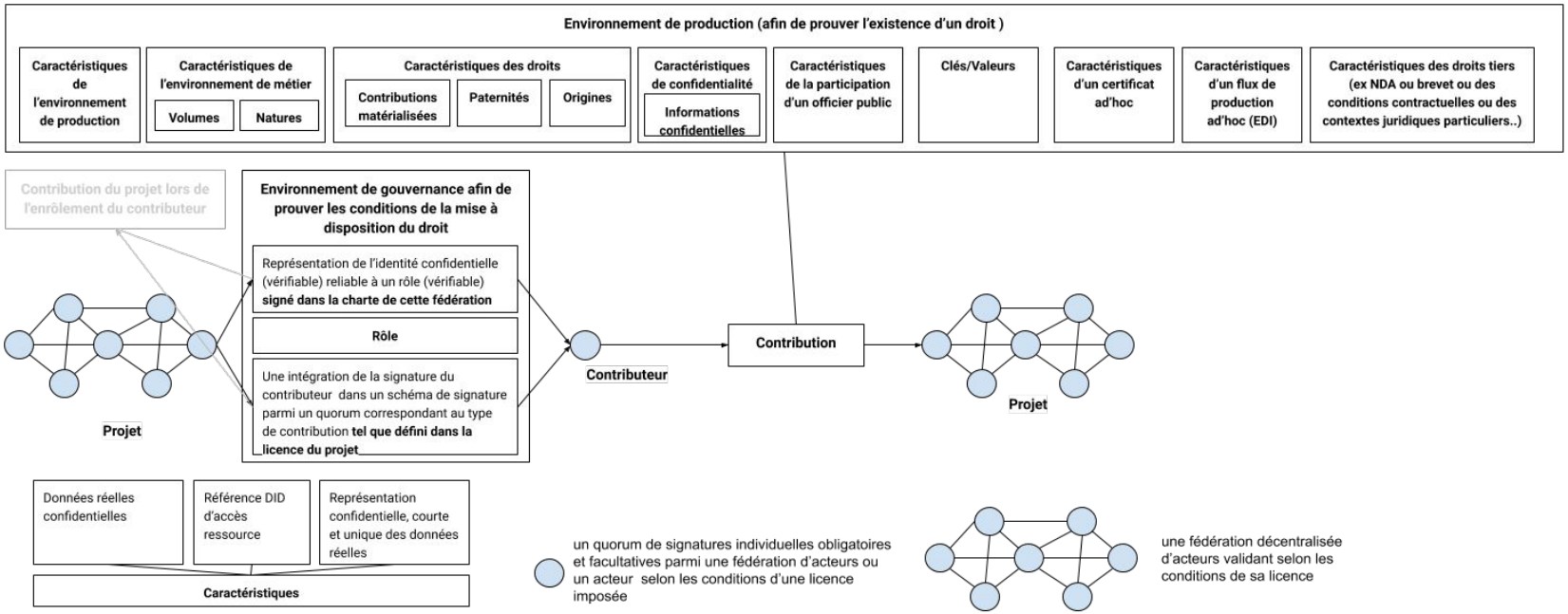


COMMENT REPRÉSENTER DIFFÉRENTS NIVEAUX DE GESTION LOGISTIQUE DANS MA PREUVE ?



L'empreinte unique qui représente exactement et uniquement n'importe quel bien ou ensemble de biens

COMMENT CONSTRUIRE UNE PREUVE ?



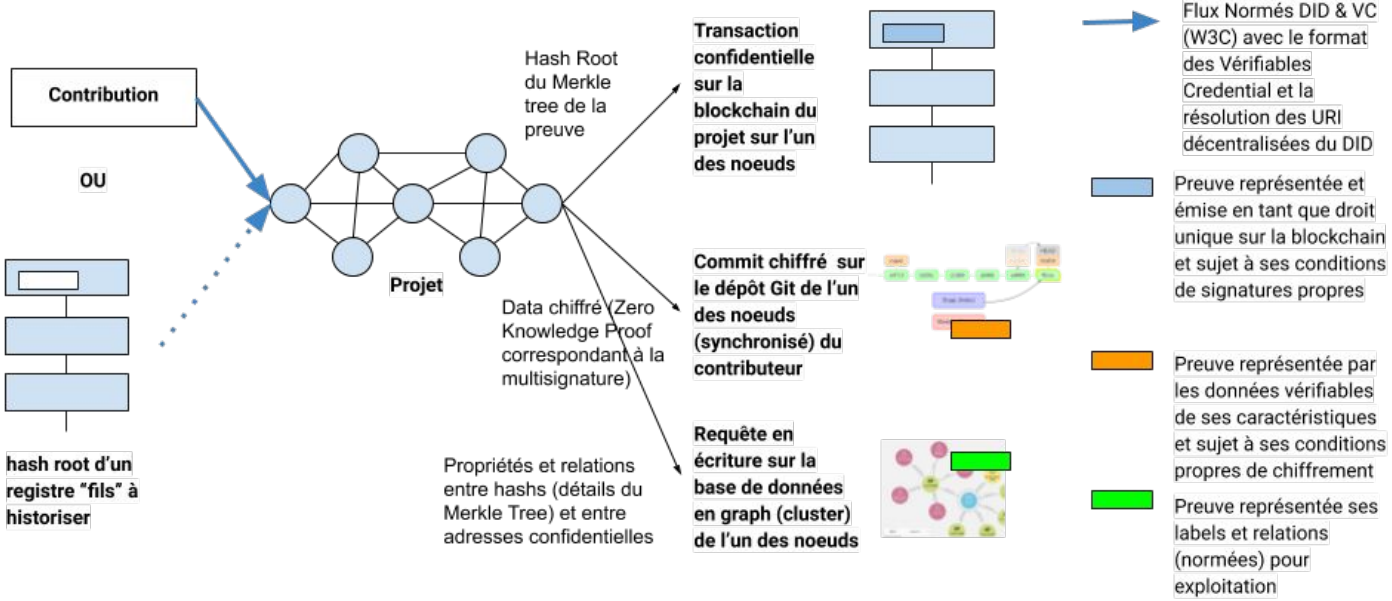
Chain Accelerator
by ON-X GROUPE

COMMENT CERTIFIER DES REPRÉSENTATIONS UNIQUES ET ÉMETTRE DES DROITS ET DES MÉDIUMS DE VALEURS ?

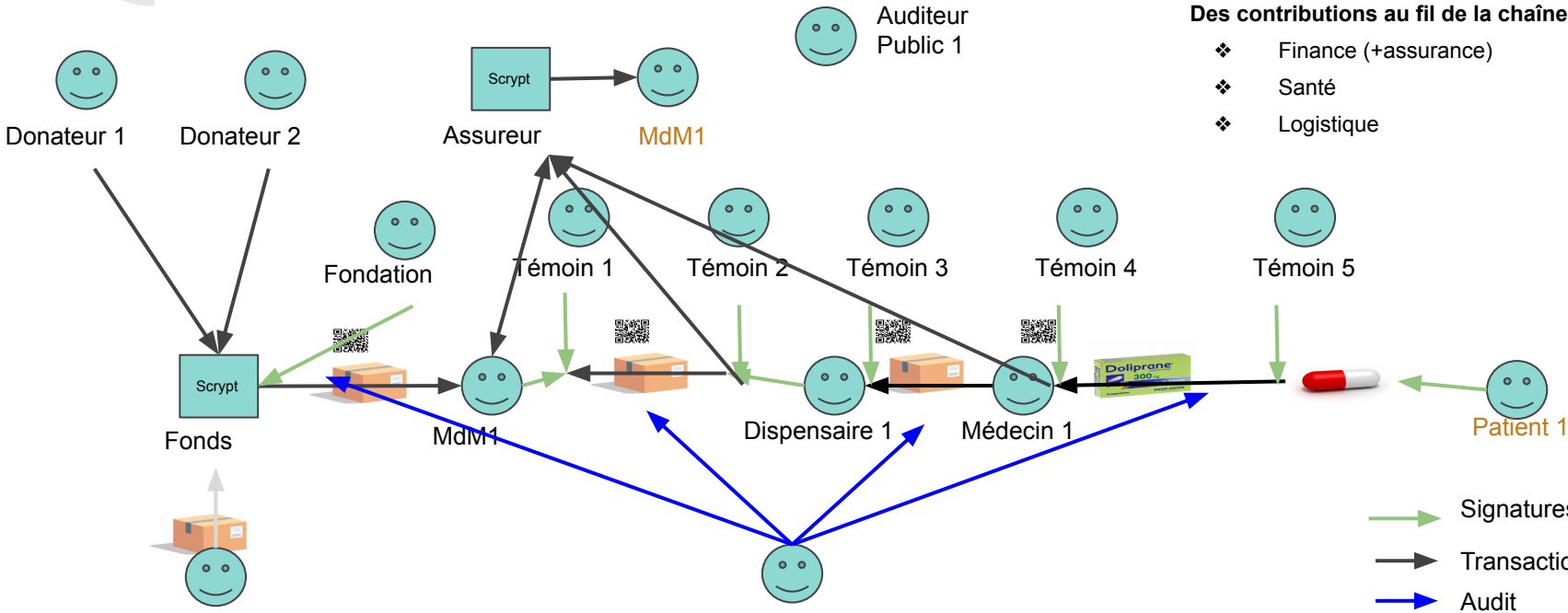
Natif, sans smart contract “maison” :

- **Confidentiel par défaut + clés d’audit**
- **(re)Emissions de tokens**
- **Peg in/out**

Autonomie complète de l’utilisateur côté client (Js), sans plug-in navigateur, sans interaction avec les noeuds pour créer ses transactions, les signer, les rendre confidentielles



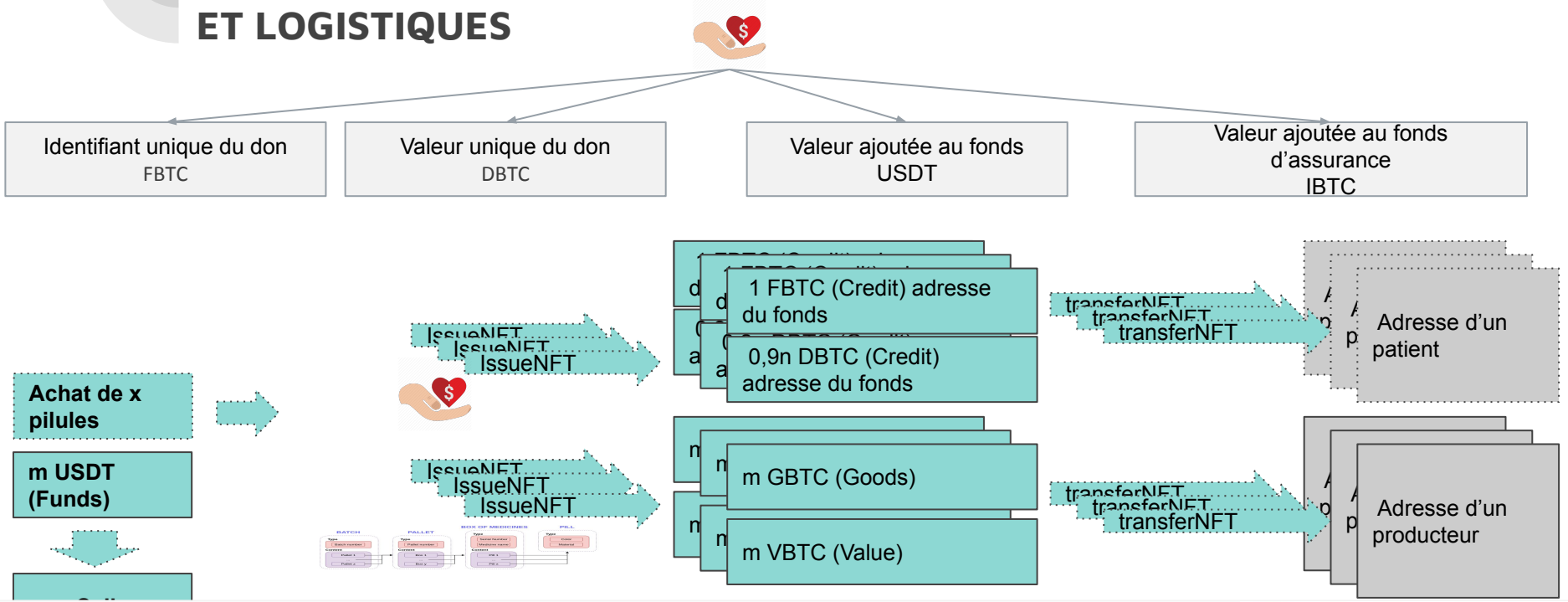
COMMENT TRACER LA DISPENSATION A LA PILLULE PRÈS ?



Des contributions au fil de la chaîne fusionnée :

- Finance (+assurance)
- Santé
- Logistique

COMMENT TRACER SYNCHRONISER LES FLUX FINANCIER ET LOGISTIQUES

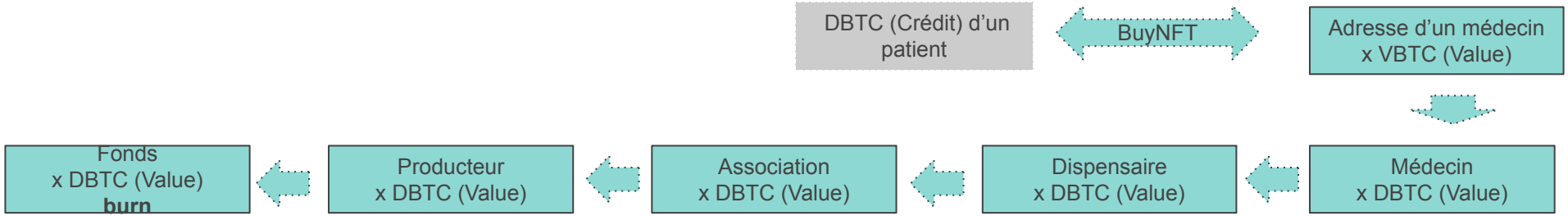


Chain Accelerator by ON-X GROUPE

COMMENT TRACER SYNCHRONISER LES FLUX FINANCIER ET LOGISTIQUES

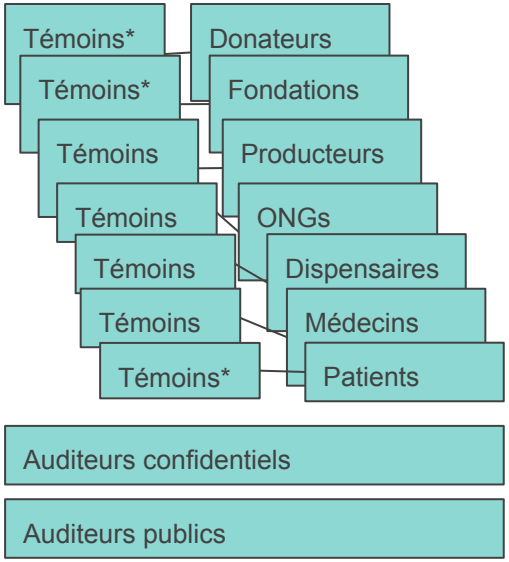
Traçabilité des marchandises

Traçabilité des fonds



COMMENT REPRÉSENTER DES ORGANISATIONS COMPLEXES ET TRANSVERSES ?

- **Nombreuses parties prenantes**
- **Intérêts divergents.**
- **International dont des zones en conflits**
- **Fort besoin d'audit** : des dons, des médications, des flux de marchandise, contre le marché noir...
- **Besoins de confidentialité médicale**
- **Besoins de confidentialité business**
- **Risques sur l'image** en fonction des comportements des opérateurs
- **Des opérateurs hétérogènes difficiles à suivre**
- **Difficultés à former sur place**
- **Patients non équipés, sans dossier**



COMMENT SONT SÉCURISÉES LES CLÉS SUR LES OUTILS WEB ?

$user = (likely@$signer || ($timeout && $recovery)) && $lock

Policy langage

Un script simple et interprétable (lisible) pour une vérification mathématique non turing complet

La lecture du code réellement exécuté et de l'état de la stack induit, donc vérifiable

Pas de smart contract "maison"

PrivKey Master	PrivKey Backup 1	PrivKey Lock 1	PrivKey Backup 2	PrivKey Lock 2
PubKey M	PubKey B1	PubKey L1	PubKey B2	PubKey L2

~~Basic Sig~~
Minsc

```
// Private Key
$master = pk(M);

// Required lock keys 1 ou 2
// for "disable" a master key, stoled for example
$lock = likely@pk(L1)  || pk(L2);

// Backups keys
$recovery = likely@pk(B1) || pk(B2);

// Timeout for transactions with this multisig using a relative time
$timeout = older(600 blocks);

// if there is no lock key in the multi-sign private key is not enough
$signer = $master;

// Condition of usage for recovery after timeout
$bs = (likely@$signer || ($timeout && $recovery)) && $lock
```

Json

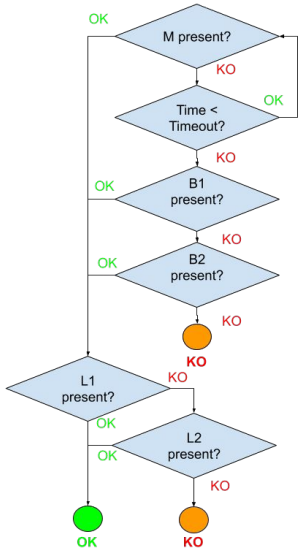
```
{
  "pol": {
    "simp": {
      "value": "pk(M)"
    },
    "or": {
      "simp": {
        "value": "older(600 blocks)"
      },
      "and": {
        "serv": {
          "value": {
            "serv": {
              "likely": true,
              "value": "pk(B1)"
            },
            "or": {
```

Policy
or(10@and(pk(M),or(10@pk(L1),pk(L2))),and(older(600),or(10@pk(B1),pk(B2))))

Miniscript
andor(pk(M),c:or_i(pk_h(L2),pk_k(L1)),and_v(vc:or_i(pk_h(B2),pk_h(B1)),older(600)))

Bitcoin Script

```
<M> OP_CHECKSIG OP_NOTIF
  OP_IF
    OP_DUP OP_HASH160 <HASH160(B2)>
OP_EQUALVERIFY
  OP_ELSE
    OP_DUP OP_HASH160 <HASH160(B1)>
OP_EQUALVERIFY
  OP_ENDIF
  OP_CHECKSIGVERIFY <5802>
OP_CHECKSEQUENCEVERIFY
OP_ELSE
  OP_IF
    OP_DUP OP_HASH160 <HASH160(L2)>
OP_EQUALVERIFY
  OP_ELSE
    <L1>
  OP_ENDIF
  OP_CHECKSIG
OP_ENDIF
```



Chain Accelerator by ON-X GROUPE

COMMENT CRÉER DES MULTI-SIGNATURES COMPLEXES ?

$org = all($parents) && thresh(X, $board) && all($cosigners) && any($members)

ParentOrganization1 or none OrgSig PO1	ParentOrganization... or none OrgSig PO...	ParentOrganizationp or none OrgSig POp
Cosigner1 or none BasicSig C1	Cosigner... BasicSig C...	Cosignerq or none BasicSig Cq
Organization1 Board1 BasicSig O1B1	Organization1 Board... BasicSig O1B...	Organization1 Boardn BasicSig O1Bn
Organization1 Member1 BasicSig O1M1	Organization1 Member... BasicSig O1M...	Organization1 Memberm BasicSig O1Mm

Organization Sig
Minsc

```
// Parent orgninization keys  (OrgSig)
$parents = [ $os1, $os2, $os3 ];

// Board members keys  (BasicSig)
$board = [ pk(B1), pk(B...), pk(Bn) ];

// Co-signer members keys (BasicSig)
$cosigners = [ pk(C1), pk(C...), pk(Cq) ];

// Organization members keys (OrgSig)
$members = [ pk(M1), pk(M...), pk(Mm) ];
```

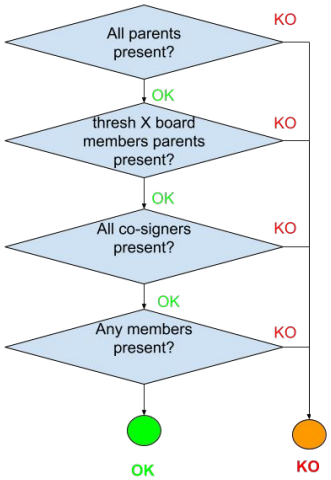
Policy

```
thresh(4,thresh(1,thresh(3,pk(PO1),pk(PO3),pk(POp)
)),thresh(3,pk(B1),pk(B3),pk(Bn)),thresh(3,pk(C1),pk(
C3),pk(Cq)),thresh(1,pk(M1),pk(M3),pk(Mm)))
```

Miniscript

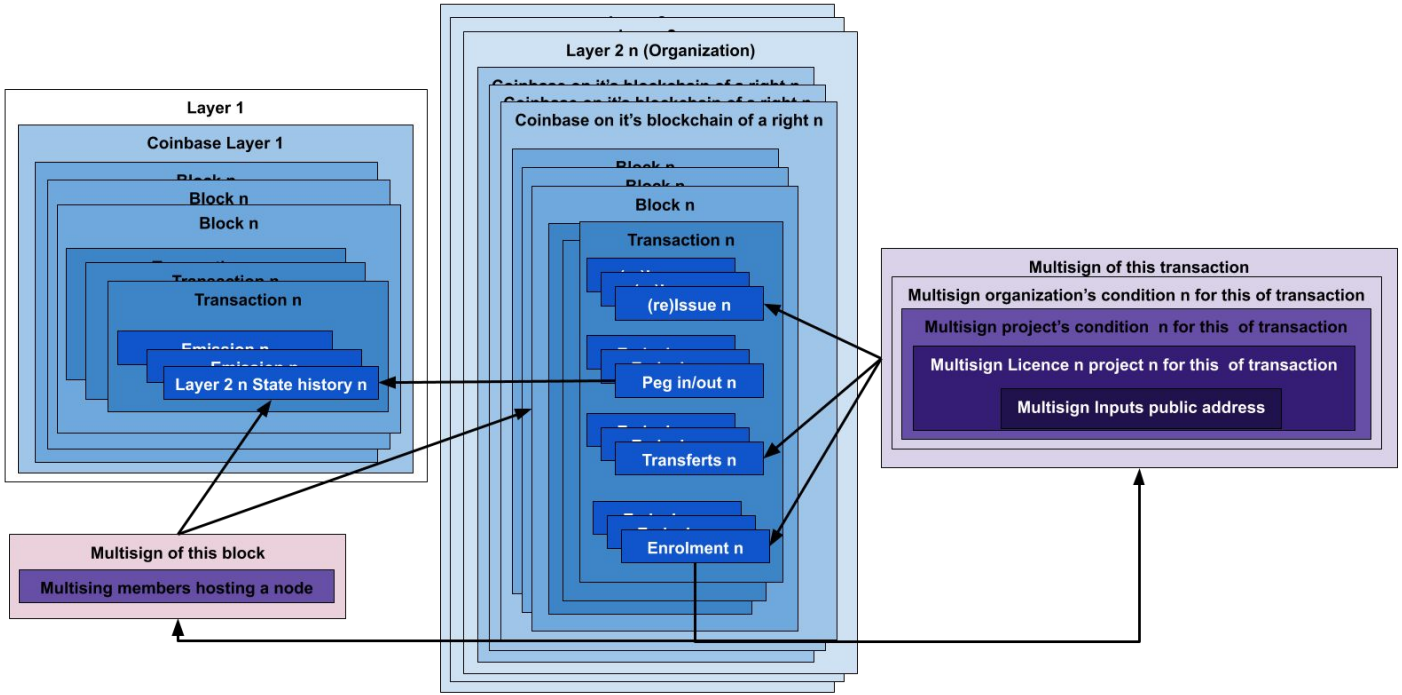
```
and_v(and_v(v:pk(PO1),and_v(v:pk(PO3),v:pk(POp))
),and_v(and_v(v:pk(B1),and_v(v:pk(B3),v:pk(Bn))),an
d_v(or_c(pk(M1),or_c(pk(Mm),v:pkh(M3))),and_v(v:p
k(C1),and_v(v:pk(C3),pk(Cq))))))
```

Bitcoin Script



COMMENT ENRÔLER SANS INFRASTRUCTURE CENTRALE ?

GOUVERNANCE = MULTI-SIGNATURE UTILISATEURS

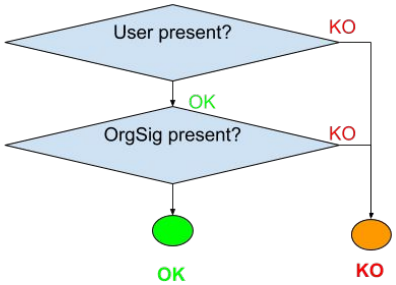


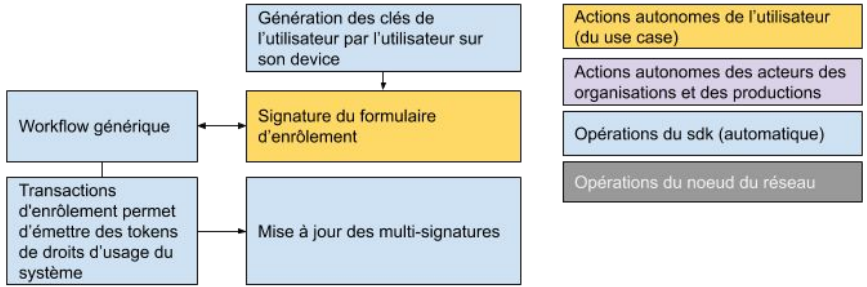
COMMENT ENRÔLER SANS INFRASTRUCTURE CENTRALE ?

$role = $user && $org

Enrolment
Organization1 Member1
Minsc

```
// User Key (BasicSig)
$user = $bs; // eg. BasicSig

// Organization Key (multisig)
// including parent and co-signer (licence)
$org = $os; // eg. OrgSig

$user && $org

Json
{
  "userBasicSig": {},
  "and": {
    "orgSig": {}
  }
}
```





COMMENT VALIDER LES ÉMISSIONS DES PREUVES, DROITS ET VALEURS ?

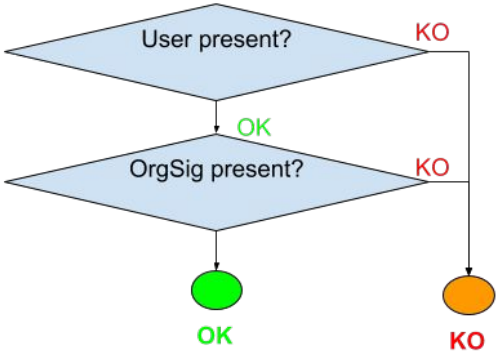
$issue = $user && $org

Issuement
Organization1 Member1
Minsc

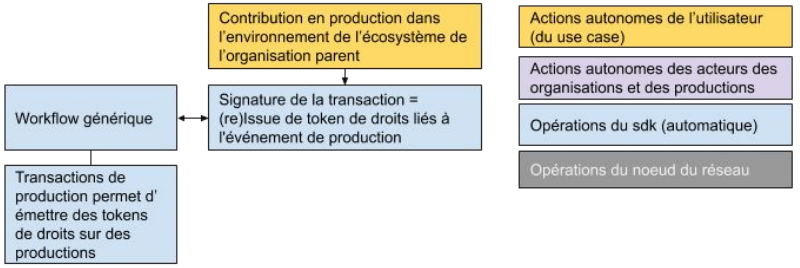
```
// User Key (BasicSig)
$user = $bs; // eg. BasicSig

// Organization Key (multisig)
$org = $os; // eg. OrgSig

$user && $org
```

Json

```
{
  "userBasicSig": {},
  "and": {
    "orgSig": {}
```



+ Le script comporte une output avec le hash root unique et spécifique de la preuve associée



COMMENT VALIDER LES TRANSFERTS ?

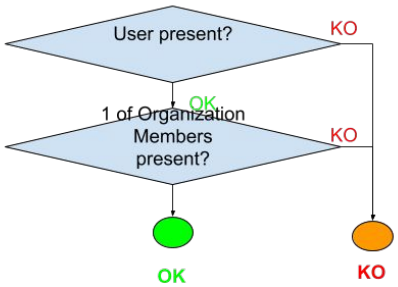
$transaction = $user && $org

Transactions from UserA to an User into OrganizationC
Organization1 Member1
Minsc

```
// UserA Key (BasicSig)
$user = $bs; // eg. BasicSig

// Organization Key (multisig)
$board = [ pk(B1), pk(B...), pk(Bn) ];
$org = $board;

// User and 1 user into the Organization
$user && (1 of $org);
```

Json

```
{
  "userBasicSig": {},
  "and": {
    "quorum": {
      "x": 1,
```



Workflow générique

Transactions d' échange de tokens de droits de production

L'utilisateur (ou chacun des membre d'une organisation) souhaite céder ou vendre ses droits

Actions autonomes de l'utilisateur (du use case)

Actions autonomes des acteurs des organisations et des productions

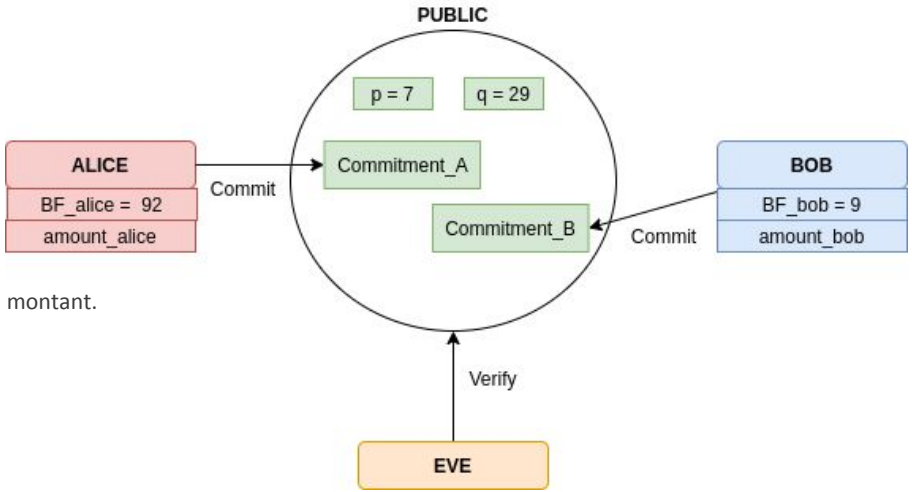
Opérations du sdk (automatique)

Opérations du noeud du réseau

COMMENT EST CREE LA CONFIDENTIALITE ? (Zero Knowledge Proof)

Propriété homomorphe de l'engagement de Pederson

Calculons l'engagement d'Alice. Elle envoie 5 BTC.
Ca = PC(BF_alice, amount_alice) = BF_alice * 7 + amount_alice * 29 = 92 * 7 + **5** * 29 = 789
Et puis l'engagement de Bob. Il reçoit 5 BTC.
Cb = PC(BF_bob, amount_bob) = BF_bob * 7 + amount_bob * 29 = 9 * 7 + **5** * 29 = 208
Enfin, Eve peut calculer la différence entre Ca et Cb:
Ca — Cb = 789 – 208 = 581
Et puis appliquez un modulo p = 7 :
581 % 7 = **0**
Eve voit que le résultat est égal à 0. Elle peut conclure qu'Alice et Bob ont engagé le même montant.
Cela signifie que la transaction est valide.
Imaginons que Bob ment et engage un montant de 8 BTC. Donc:
Cb = PC(BF_bob, amount_bob) = BF_bob * 7 + amount_bob * 29 = 9 * 7 + **8** * 29 = 295
Et quand Eve essaiera de vérifier la transaction:
(Ca — Cb) % p = (789–295) % 7 = 494 % 7 = **4**
Comme (Ca — Cb)%p n'est pas égal à zéro, la transaction n'est donc pas confirmée.
Eve sait que quelqu'un a menti.

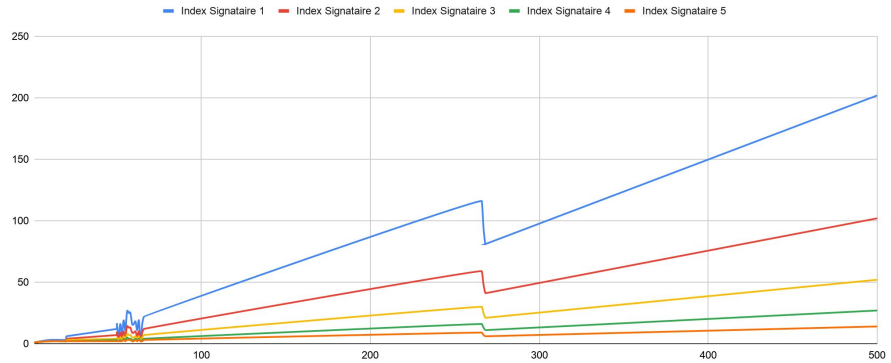


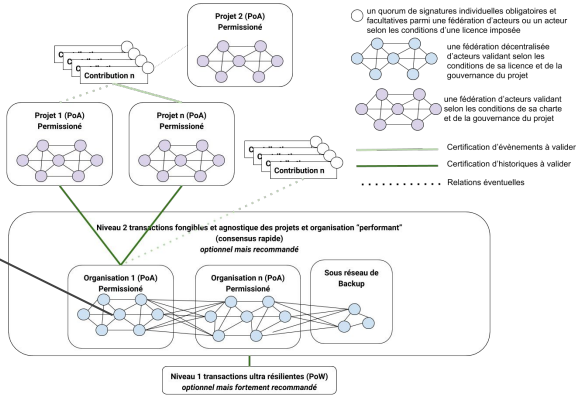
COMMENT LES RÉSEAUX NON RÉSILIENTS (Layers 2, 3…) SIGNENT-ILS LES BLOCS AVANT LE PEG IN/OUT ?

Choisir simplement, clairement les participants (et pouvoir le vérifier facilement) :

```
i(n=1) = ARRONDI.INF( ( MOD(#block; Somme des Nodes enrôlés ) / 2 ) + 1 )
i(n>1) = ARRONDI.INF( ( i( n - 1 ) / 2 ) + 1 )
```

De l'entropie et un déploiement maîtrisé





Questions