Ğ1 v2.0 : Ce qui va changer

Éloïs SANCHEZ - 14 Juillet 2022

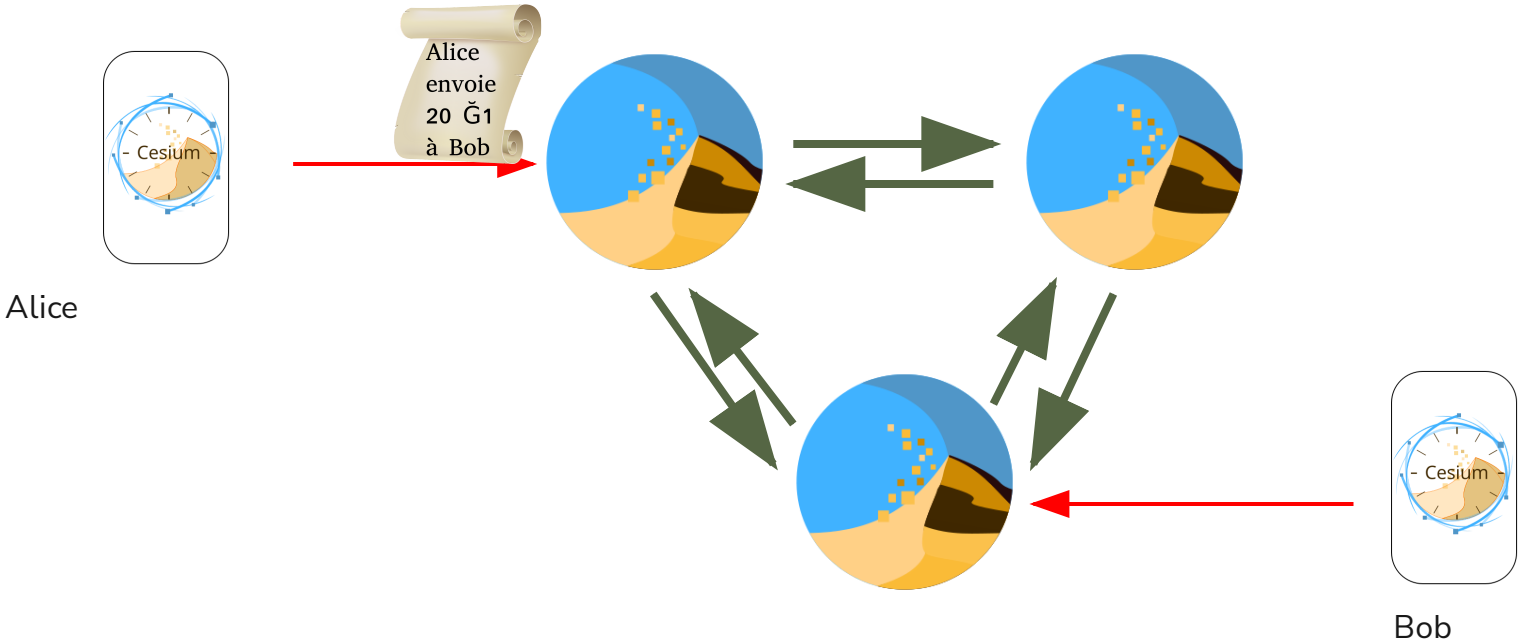
Sommaire

La Ğ1 en apparence

Alice Bob

- Comment contacter le tel/ordi de Bob ?
- Et si Bob n’est pas en ligne ?
- Où sont sauvegardées les informations ?
- ⇒ Cesium ne peut pas fonctionner tout seul

La Ğ1 en réalité



Pourquoi arrêter Duniter v1 ?

- Plus en développement actif, plus de nouvelle fonctionnalité depuis 4 ans, en "maintenance minimale".
- Déjà des problèmes de charge (alors que 6000 utilisateurs c'est rien).
- Designé à 90% par cgeek entre 2014 et 2017
  - Il n'avait pas de compétence spécifique blockchain
  - Il n'y avait pas d'utilisateurs, seuls quelques dizaines de geek 🤓.
- Codé de manière trop spécifique, pas assez flexible/évolutif ⇒ trop difficile à faire évoluer.

Les objectifs de Duniter v2

1. Pérenniser la Ğ1 (pour qu'elle ne s'arrête pas).
2. Réduire notre travail de développement à ce qui est spécifique à la monnaie libre, déléguer le reste à un « framework blockchain ».
3. Corriger la plupart des problèmes de Duniter v1 (notamment la synchro des « piscines »).
4. Ajouter de nouvelles fonctionnalités utiles et demandées depuis des années (comme le prélèvement automatique)
5. Intégrer des mécanismes de prises de décision directement dans la blockchain (demandera d'abord des longs échanges sur les modalités).

Les nouvelles interfaces

Ğecko

- Développé par Étienne Bouché (poka)
- Mobile et Ordinateur (web)
- Interface intuitive pour les nouveaux
- Projet de travailler avec un·e pro UX design

Cesium v2

- Développé par Benoit Lavenier (kimamila)
- Mobile et Ordinateur ?
- Interface proche de Cesium v1 ?

Changement délais

Ğ1 v1

- Un bloc toutes les 5 minutes environ.
- Transaction en blockchain en 10-15 min.
- Finalisation probabiliste, forks toujours possible (très impropable au bout de quelques heures).

Ğ1 v2

- Un bloc toutes les 6 secondes précisément.
- Transaction en blockchain en 5 à 10 secondes.
- Finalisation absolue, fork impossible après finalisation (~30 s quand le réseau va bien).

Changement capacités

- ~ 100 transferts par block

⇒ < 100 transfers / 5min !

- 300 transferts par bloc

⇒ = 15 000 transfers / 5min !

Changement certifications

Ğ1 v1

- On peut émettre plusieurs certif en même temps.
- Les certifications restent en « piscine » jusqu'à leur validation définitive (une tous les 5 jours) ou expiration (2 mois).

⇒ Problèmes de synchro (car certifs pas en blockchain)

⇒ Problèmes de disponibilité des certif qui retardent les nouveaux entrants si trop de certif émises

Ğ1 v2

- On ne peut émettre une certification que si la précédente à été émise il y a 5 jours ou plus.
- Disparition des « piscines », toute certification est inscrite dans la blockchain dès son émission.

⇒ Plus de prob. de synchro, on voit les mêmes certif partout (car en blockchain)

⇒ Plus de notion de « disponibilité », toute certif émise est instantannément validée et en blockchain.

Changement identités

Ğ1 v1

- On peut transformer n'importe quel compte et compte membre (=créer son identité).
- L'identité reste en « piscine » jusqu'à sa validation définitive (5 cert dispo + distance) ou expiration (2 mois).

⇒ problèmes de synchro (car identité pas en blockchain), selon le noeud vous ne pouvez pas certifier la personne.

Ğ1 v2

- L'identité doit être créée par le 1er certificateur.
- Puis l'utilisateur doit confirmer sa création d'identité.
- Puis d'autres membres peuvent le certifier.
- L'identité passe au statut "validée" dès que les conditions sont réunies (5 certif + distance) ou est supprimée au bout de 2 mois.

⇒ Tout le monde voit la même identité partout (car en blockchain)

Nouvelle fonctionnalités

Changer la clé publique de son compte membre

Ğ1 v1

- Il faut révoquer son compte membre et en créer un nouveau ➪ on perd toutes ses certifications.

Ğ1 v2

- On pourra modifier sa clé publique en conservant ses certifications.
- Pour que ce soit sécurisé : l'ancienne clé publique pourra toujours révoquer l'identité pendant quelques mois.

Nouvelle fonctionnalités

Multi-signature onchain

Ğ1 v1

- Possible, mais les signatures doivent être réunies offchain.

⇒ Nécessite de se réunir physiquement ou de partager un fichier, trop technique.

Ğ1 v2

- Chaque co-signataire peut publier seul sa signature en blockchain sans avoir besoin de se synchroniser avec les autres ou de partager un ficher.
- On définit une liste de clés publiques et un seuil, par exemple 3 parmi 5.

⇒ Permettra de créer et utiliser un compte collectif sans compétences techniques (à condition qu'une interface l'expose).

Nouvelle fonctionnalités

Compte délégué

Ğ1 v1

- Impossible.

Ğ1 v2

- On pourra donner certains droits sur notre compte à un autre compte (délégataire), comme le droit de transférer de la monnaie.
- On pourra optionellement imposer un délai au délégataire, délai pendant lequel on peut "annuler" l'action.
- Cas d'usages possibles:
  - Une asso peut nommer son trésorier comme délégataire avec un délai d'une semaine (ou autre).
  - Un membre peut donner accès à ses DU à un simple portefeuille sur son mobile.

Nouvelle fonctionnalités

Autorisation de prélèvement

Ğ1 v1

- Impossible.

Ğ1 v2

- On pourra autoriser le versement d'une somme précise chaque mois* vers un destinataire précis.
- *Période paramétrable : 1 mois, 3 mois, 1 semaine, 1 jour, ce qu'on veut.
- Le montant pourra être exprimé en Ğ1 ou en DUĞ1 (automatiquement réévalué).
- N'importe qui pourra « exécuter » le prélèvement quand une « période » est écoulée.
- Chaque autorisation sera révocable sans conditions ni délai.

⇒ Au plus tard quelques mois après le passage à la v2.

Plan de migration

- ✅ Développer une 1ère PoC.
- ✅ lancer une 1ère monnaie de test pour les développeurs (ĞDev).
- ✅ 1ère batterie de tests sur la ĞDev.
- ☐ Étalonner les « poids » (en cours...).
- ☐ Ajouter les fonctionnalités manquantes.
- ☐ 2ème batterie de tests sur la ĞDev (avec tests de charge).
- ☐ Coder de quoi convertir DB duniter V1 en genesis state Duniter v2.
- ☐ Tester la migration à blanc.
- ☐ Lancer la 2ème monnaie de test (ĞTest) basée sur l'état de la ğ1-test où de la Ğ1.
- ☐ 1ère batterie de tests sur la ĞTest (avec tests de charge).
- ☐ Attendre que les nouvelles interfaces soit prètes.
- ☐ Lancer la « Ğ1-mirror », une copie temporaire de la Ğ1.
- ☐ Campagne de tests utilisateurs sur la « Ğ1-mirror ».
- ☐ Intégrer les retours de cette campagne.
- ☐ Annonce d'une date officielle de migration de la prod.

Questions/Réponses

Merci de votre attention.