Certifications, toile de confiance, sécurité, ... partie 1

Licence Ğ1:

Licence Ğ1 - v0.2.9

:date: 2017-04-04 12:59 :modifié: 2019-07-14 12:00

Licence de la monnaie et engagement de responsabilité.

Toute opération de certification d'un nouveau membre de Ğ1 doit préalablement s'accompagner de la transmission de cette licence de la monnaie Ğ1 dont le certificateur doit s'assurer qu'elle a été étudiée, comprise et acceptée par la personne qui sera certifiée.

Tout événement de rencontre concernant Ğ1 devrait s'accompagner de la transmission de cette licence, qui peut être lue à haute voix, et transmise par tout moyen.
Toile de confiance Ğ1 (TdC Ğ1)

Avertissement : Certifier n'est pas uniquement s'assurer que vous avez rencontré la personne, c'est assurer à la communauté Ğ1 que vous connaissez suffisamment bien la personne certifiée et que vous saurez ainsi la contacter facilement, et être en mesure de repérer un double compte effectué par une personne certifiée par vous-même, ou d'autres types de problèmes (disparition...), en effectuant des recoupements qui permettront de révéler le problème le cas échéant.

Conseils fortement recommandés

Bien connaître une personne suppose que vous êtes en mesure de la contacter par plusieurs moyens différents (physique, électronique, autre...) mais aussi que vous connaissez aussi plusieurs personnes qui la connaissent tout aussi bien et sont donc aussi en mesure de la contacter de même. Notamment si vous ne connaissez pas bien aucun de ses autres certificateurs c'est une indication forte que vous ne connaissez pas bien la personne et une certification de ce type déclenche une alerte vers toute la communauté Ğ1. En cas de connaissance insuffisante il convient de ne surtout pas certifier.

Ne certifiez jamais seul, mais accompagné d'au moins un autre membre de la TdC Ğ1 afin d'éviter toute erreur de manipulation. En cas d'erreur, prévenez immédiatement d'autres membres de la TdC Ğ1.

Avant toute certification, assurez-vous de vérifier si son compte (qu'il soit en cours de validation ou déjà membre) a déjà reçu une ou plusieurs certifications. Le cas échéant demandez des informations pour entrer en contact avec ses autres certificateurs afin de vérifier ensemble que vous connaissez bien la personne concernée par la création du nouveau compte, ainsi que la clé publique correspondante.

Vérifiez que le futur certifié maîtrise bien son compte : un bon moyen de vérifier cela est de transférer quelques Ğ1 vers le compte cible, et de demander ensuite un renvoi vers votre propre compte, cela assure de la bonne maîtrise par le futur certifié de sa clé privée.

Vérifiez que vos contacts ont bien étudié et compris la licence Ğ1 à jour.

Si vous vous rendez compte qu'un certificateur effectif ou potentiel du compte concerné ne connaît pas la personne concernée, alertez immédiatement des experts du sujet au sein de vos connaissance de la TdC Ğ1, afin que la procédure de validation soit vérifiée par la TdC Ğ1.

Lorsque vous êtes membre de la TdC Ğ1 et que vous vous apprêtez à certifier un nouveau compte :

Vous êtes vous assuré :

1°) De suffisamment bien connaître (pas seulement de la connaître "de visu") la personne qui déclare gérer cette clé publique (nouveau compte). Voir les conseils fortement recommandés ci-dessus pour s'assurer de "bien connaître".

2°) D'avoir personnellement vérifié avec elle qu'il s'agit bien de cette clé publique que vous vous apprêtez à certifier (voir conseils ci-dessus).

3°) D'avoir bien vérifié avec la personne concernée qu'elle a bien généré son document Duniter de révocation de compte qui lui permettra le cas échéant de pouvoir désactiver son statut de membre (cas d'un vol de compte, d'un changement de ID, d'un compte créé à tort etc.).

4a°) De rencontrer la personne physiquement pour vous assurer que c'est bien elle que vous connaissez bien et qui gère cette clé publique.

4b°) Ou bien de vérifier à distance le lien personne / clé publique en contactant

la personne par plusieurs moyens de communication différents, comme courrier papier + réseau social + forum + mail + vidéo conférence + téléphone (reconnaître la voix). Car si l'on peut pirater un compte mail ou un compte forum, il sera bien plus difficile d'imaginer pirater quatre moyens de communication distincts, et imiter l'apparence (vidéo) ainsi que la voix de la personne en plus.

Le 4a°) restant toutefois préférable au 4b°), tandis que les points 1°) 2°) et 3°) sont préalablement indispensables.

Règles abrégées de la TdC :

Chaque membre a un stock de 100 certifications possibles, qu'il ne peut émettre qu'au rythme de 1 certification / 5 jours.

Valable 2 mois, une certification pour un nouveau membre n'est définitivement adoptée que si le certifié possède au moins 4 autres certifications au bout de ces 2 mois, sinon le processus d'entrée devra être relancé.

Pour devenir un nouveau membre de la TdC Ğ1 il faut donc obtenir 5 certifications et se trouver à une distance <= 5 pas de 80% des membres référents de la TdC.

Un membre de la TdC Ğ1 est membre référent lorsqu'il a reçu et émis au moins Y[N] certifications où N est le nombre de membres de la TdC et Y[N] = plafond N^(1/5). Exemples :

Pour 1024 < N ≤ 3125 on a Y[N] = 5
Pour 7776 < N ≤ 16807 on a Y[N] = 7
pour 59049 < N ≤ 100 000 on a Y[N] = 10

Une fois que le nouveau membre est partie prenante de la TdC Ğ1 ses certifications restent valables 2 ans.

Pour rester membre il faut renouveler son accord régulièrement avec sa clé privée (tous les 12 mois) et s'assurer d'avoir toujours au moins 5 certifications valides au delà des 2 ans.

Monnaie Ğ1

Ğ1 se produit via un Dividende Universel (DU) pour tout être humain membre de la Toile de Confiance Ğ1, qui est de la forme :

1 DU par personne et par jour

Code de la monnaie Ğ1

Le montant en Ğ1 du DU est identique chaque jour jusqu'au prochain équinoxe où le DU sera alors réévalué selon la formule (avec 1 jour = 86 400 secondes) :

DUjour(équinoxe suivant) = DUjour(équinoxe) + c² (M/N)(équinoxe) / (182,625 jours)

Avec comme paramètres :

c = 4,88% / équinoxe
DU(0) = 10,00 Ğ1

Et comme variables :

M la masse monétaire totale à l'équinoxe
N le nombre de membres à l'équinoxe

Logiciels Ğ1 et licence Ğ1

Les logiciels Ğ1 permettant aux utilisateurs de gérer leur utilisation de Ğ1 doivent transmettre cette licence avec le logiciel ainsi que l'ensemble des paramètres techniques de la monnaie Ğ1 et de la TdC Ğ1 qui sont inscrits dans le bloc 0 de Ğ1. Un logiciel qui ne remplirait pas ces obligations de la licence n'est pas compatible Ğ1.

Pour plus de précisions dans les détails techniques il est possible de consulter directement le code de Duniter qui est un logiciel libre ainsi que les données de la blockchain Ğ1 en les récupérant via une instance (ou nœud) Duniter Ğ1.

Plus d'informations sur le site de l'équipe Duniter https://www.duniter.org

Comment certifier?

Rappeller des élements de base et de nos expériences:

- on peut faire des transactions payer et recevoir sans être certifié
- donc, la certification permet de participer avec d'autres personnes à la création monétaire
- la création monétaire doit être équilibrée d'une région à l'autre, y participer est une bonne chose
- participer à la création monétaire revient à être banquier d'une certaine manière
- il est mieux que quelqu'un qui participe à la création monétaire fasse circuler les junes, même si ce n'est pas une condition

- certifier peut prendre du temps et nécessite de la coordination et de la communication
- la part de création monétaire quotidienne (DU) est une bien petite somme comparé à ce que l'on peut gagner en faisant des échanges
- la certification est un jeu collectif
- la décentralisation et la toile de confiance sont liés, il n'y a pas d'autorité centrale qui décide de qui est membre co-créateur et qui ne l'est pas

Forcément, on donnera aussi des opinions ou notre vision de la june, mais il est important et convivial d'en discuter avec le futur membre.

Les règles de base:

Un certificateur ou une certificatrice:

- ne certifie qu'un seul futur membre ou membre à la fois
- certifie 5 jours après la validation de sa dernière certification
- se coordonne avec les autres certificateurs, regarde si leur certification est disponible
- vérifie si le futur membre va passer membre

Au niveau fonctionnalité du compte membre Ğ1:

- qualité des phrases de passe du compte membre (quelques chiffres, symboles, et des phrases, et pas le même que pour ğchange)
- informations sûres et bien sauvegardées
- téléchargement du fichier de révocation, explications sur son utilité
- explications sur l'adhésion annuelle, l'utilisation de cesium

On ne peut pas tout savoir dès le premier jour!

Donc, rassurer sur l'apprentissage qui se fera progressivement.

Puis, approfondissement, explications plus détaillées, règle de distance, etc…

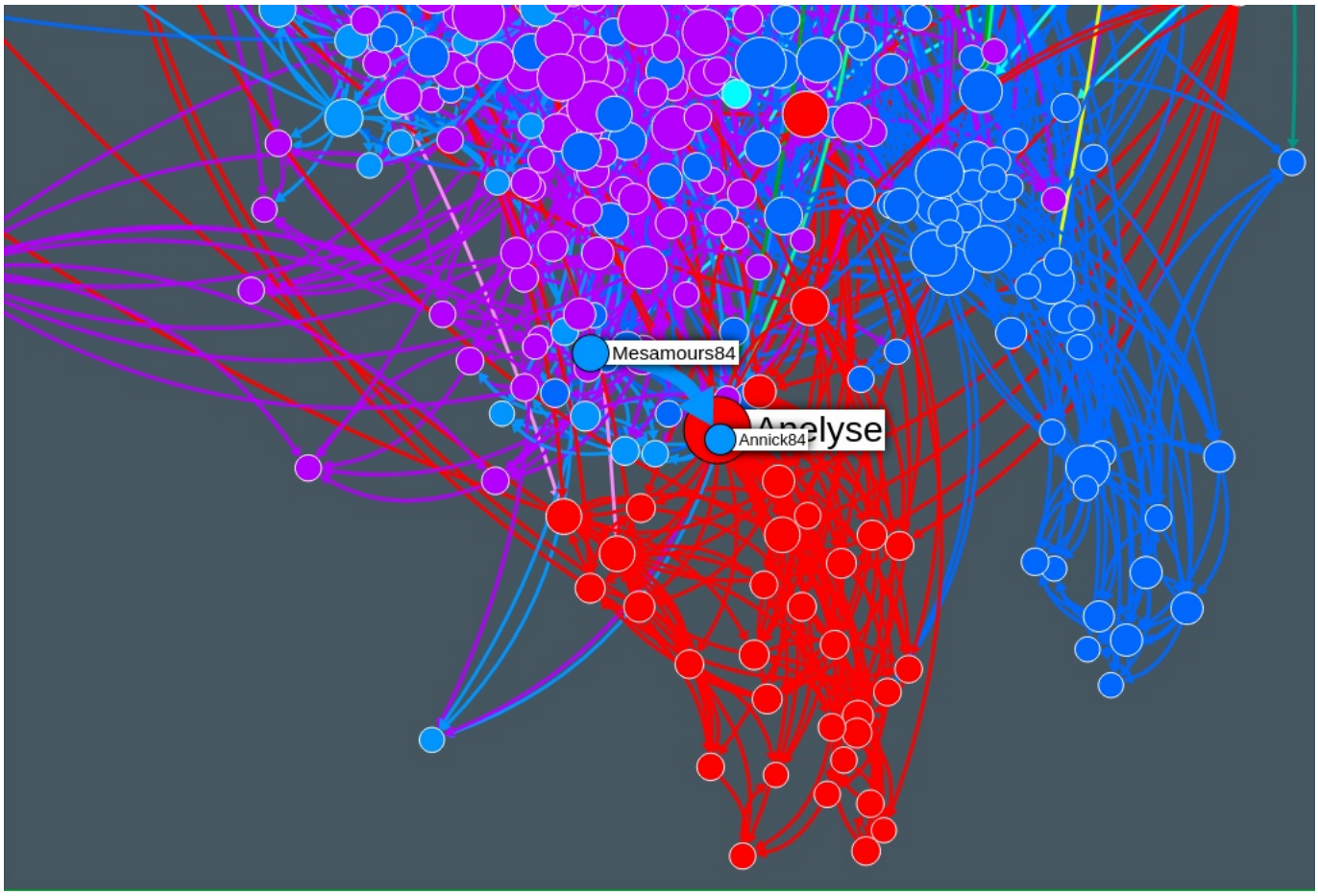
Toile de confiance Ğ1:

Les idées de base:

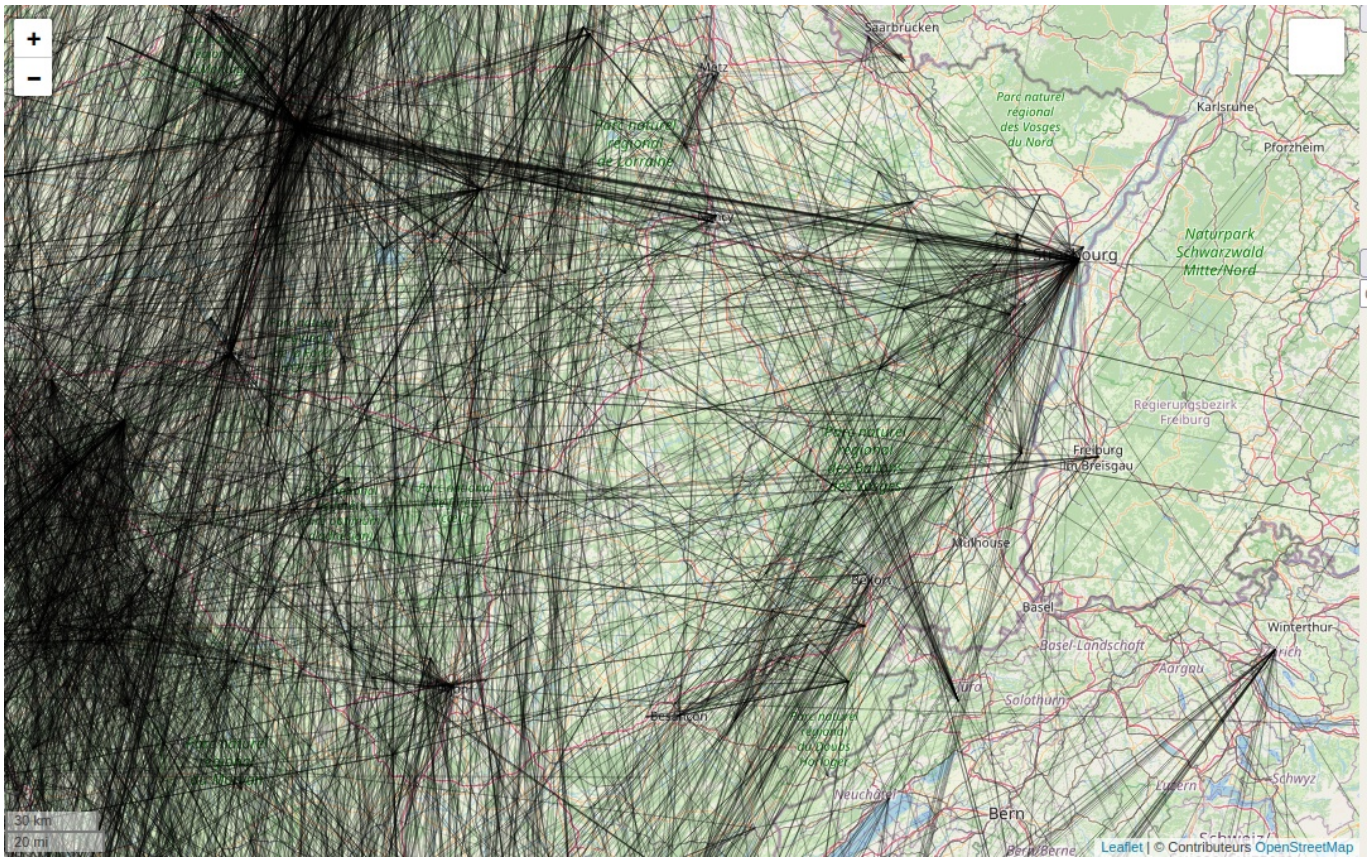
- crée la monnaie celui ou celle qui est coopté·e
- la cooptation est encadrée et freinée par des garde-fous
- la toile de confiance est une sécurité informatique décentralisée
- elle pousse à avoir un carnet d'adresse, à rencontrer les membres
- attention de ne pas donner à cette toile de confiance une signification qu'elle n'a pas

Visualisation de la toile de confiance:

wotmap.duniter.org



worldwotmap.duniter.org



Explications:

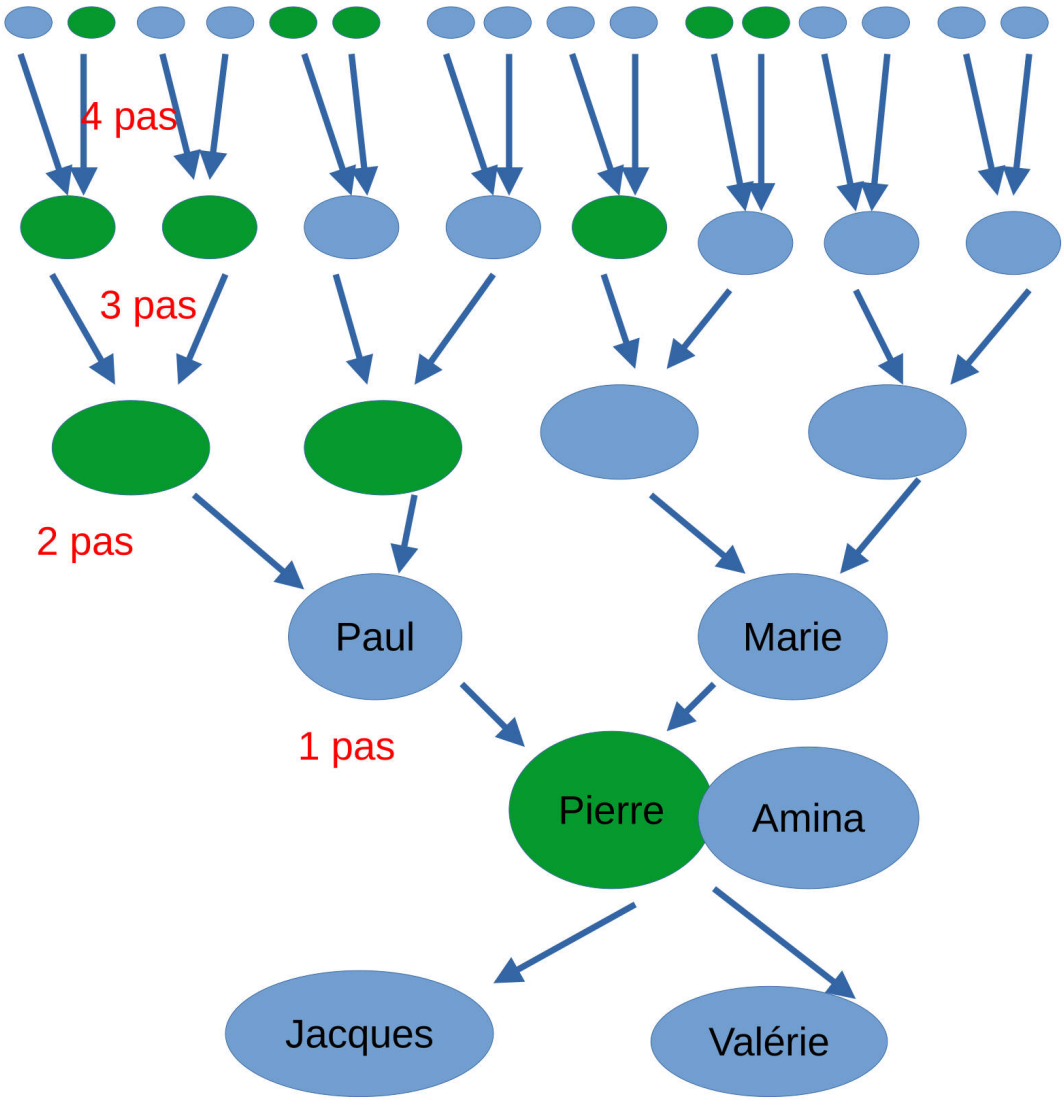
Comparaison toile de confiance – généalogie :

Vert = référent = 2 enfants et 2 parents

34 membres

Pierre avec les chemins de généalogie atteint 10 référents, 90.1%

Référent est seulement une sorte de repère de l'implication



Mais:

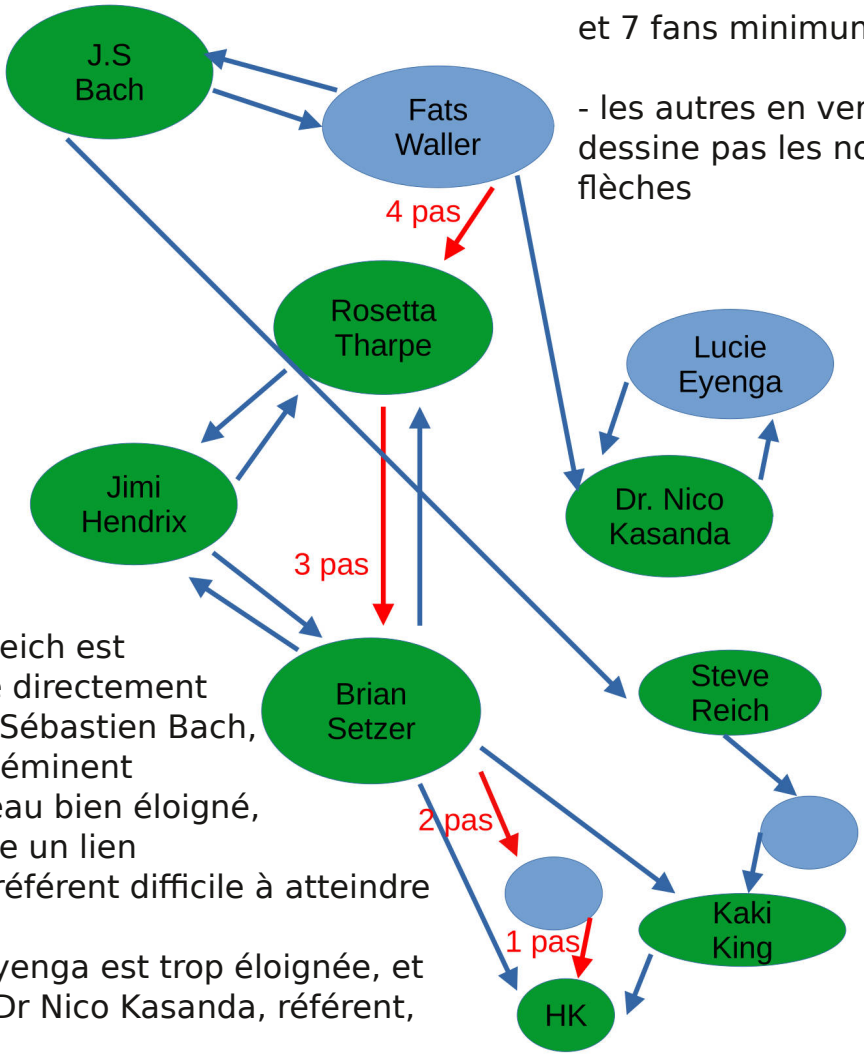
- l'exemple ici ne montre qu'une seule famille
- les "parents" dans la toile de confiance peuvent être bien plus que 2
- les liens de "parenté" de la toile de confiance peuvent aller dans les deux sens
- il y a des zones de la toile définies par des liens privilégiés entre membres
- Pierre a la confiance de sa famille, et meme de ses membres ayant 2 enfants

Pour etre plus proche de la toile de confiance de duniter:

- on met des liens dans les 2 sens entre 2 membres
- il est possible de "court-circuiter" et d'avoir un lien de confiance direct avec un membre d'un réseau éloigné
- on peut pas dessiner toutes les flèches, mais il y en a énormément

Comparaison toile de confiance – influences musicales :

(ne riez pas, c'est un peu fictionnel)



- HK a 7 influenceurs musicaux et 7 fans minimum

- les autres en vert aussi, on dessine pas les nombreuses flèches

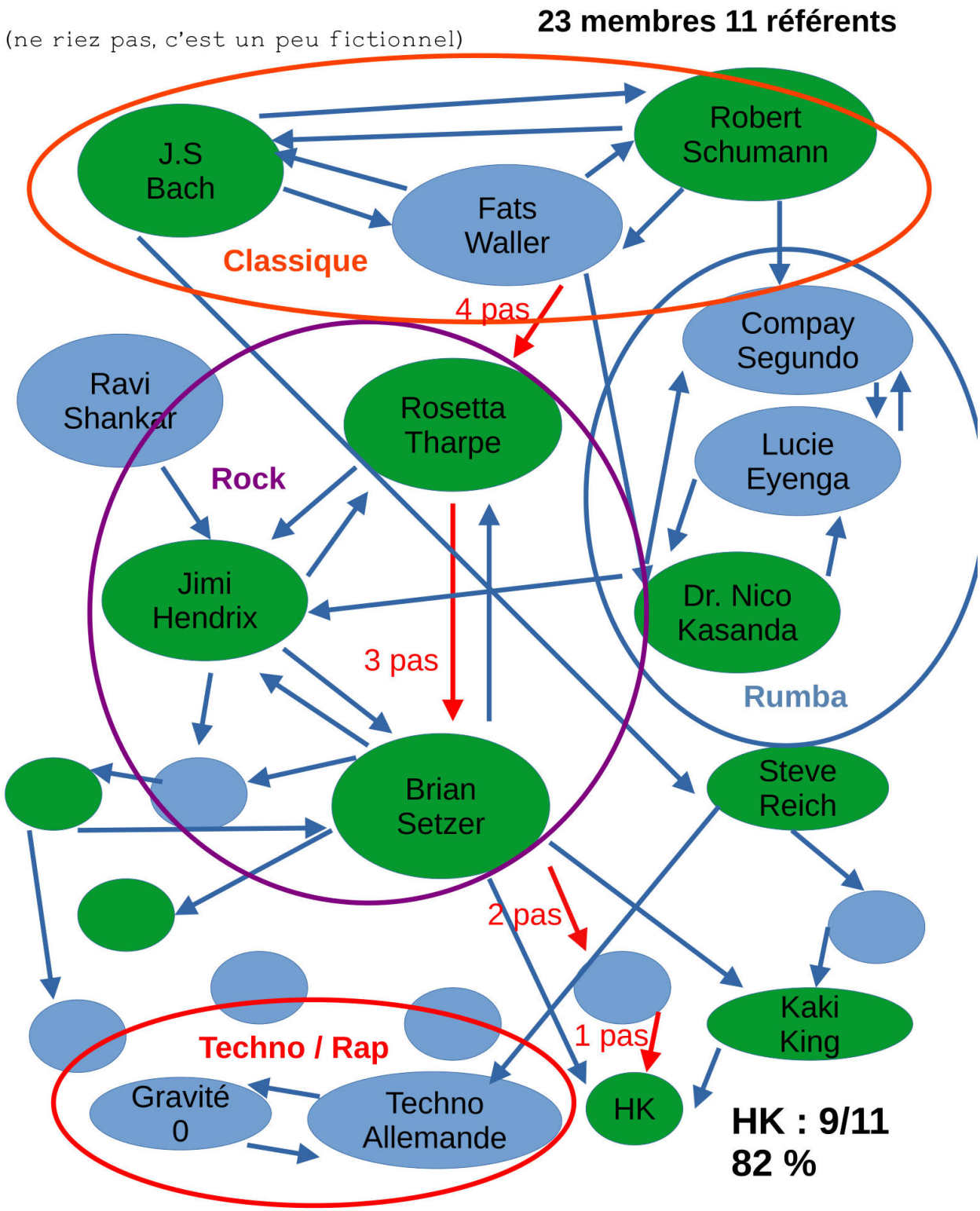
- Steve Reich est influencé directement par Jean-Sébastien Bach, membre éminent d'un réseau bien éloigné, il apporte un lien vers ce référent difficile à atteindre

- Lucie Eyenga est trop éloignée, et son ami Dr Nico Kasanda, référent, aussi

Situation avec plus de monde:

Les ellipses de couleurs représentent des zones de la toile musicale avec des liens privilégiés
On voit plus de flèches, pour montrer qu'il y a plus de chemins possibles
L'idée est de collecter les membres référents par tous les chemins possibles!

Comparaison toile de confiance – influences musicales :



HK collecte 82% de référents par ses liens musicaux, donc on peut considérer qu'il recoit assez de confiance de gens ayant eux-mêmes beaucoup de liens musicaux :)

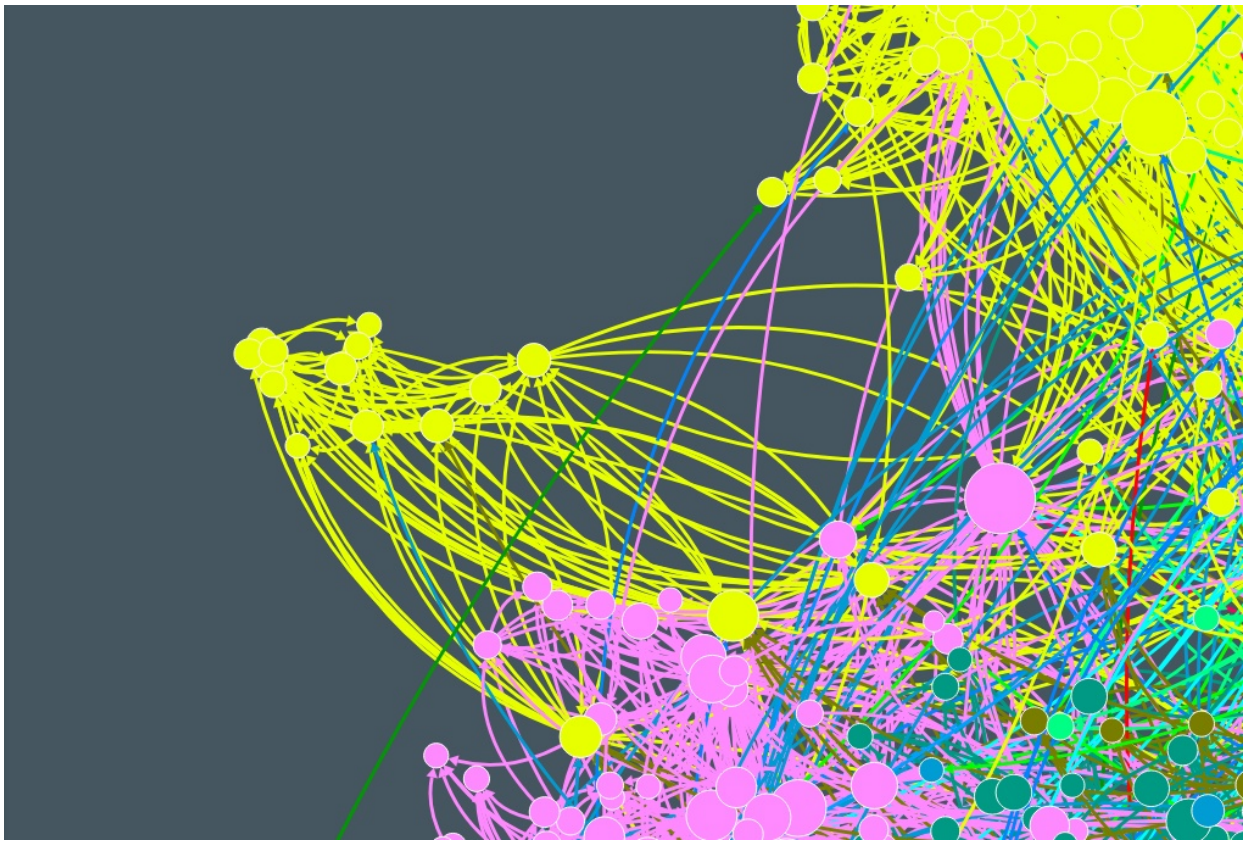
Cas d'un·e futur·e membre:

- on additionne les référents récupérés par 5 personnes minimum l'ayant coopté
- si collectivement 80% des référents sont atteints (règle de distance), la personne pourra devenir membre
- ça revient à regarder à 5 pas de ce futur membre le nombre de référents atteints
- HK a lui tout seul peut permettre à un nouveau de respecter la règle de distance

À quoi ça sert?

- éviter la création en masse de faux-comptes, tricheurs, qui peuvent certifier à leur tour
- décentraliser l'instance qui décide de qui crée la monnaie: chaque membre co-créateur décide
- indirectement avoir un carnet d'adresses, des liens avec d'autres membres, faciliter les rencontres et échanges

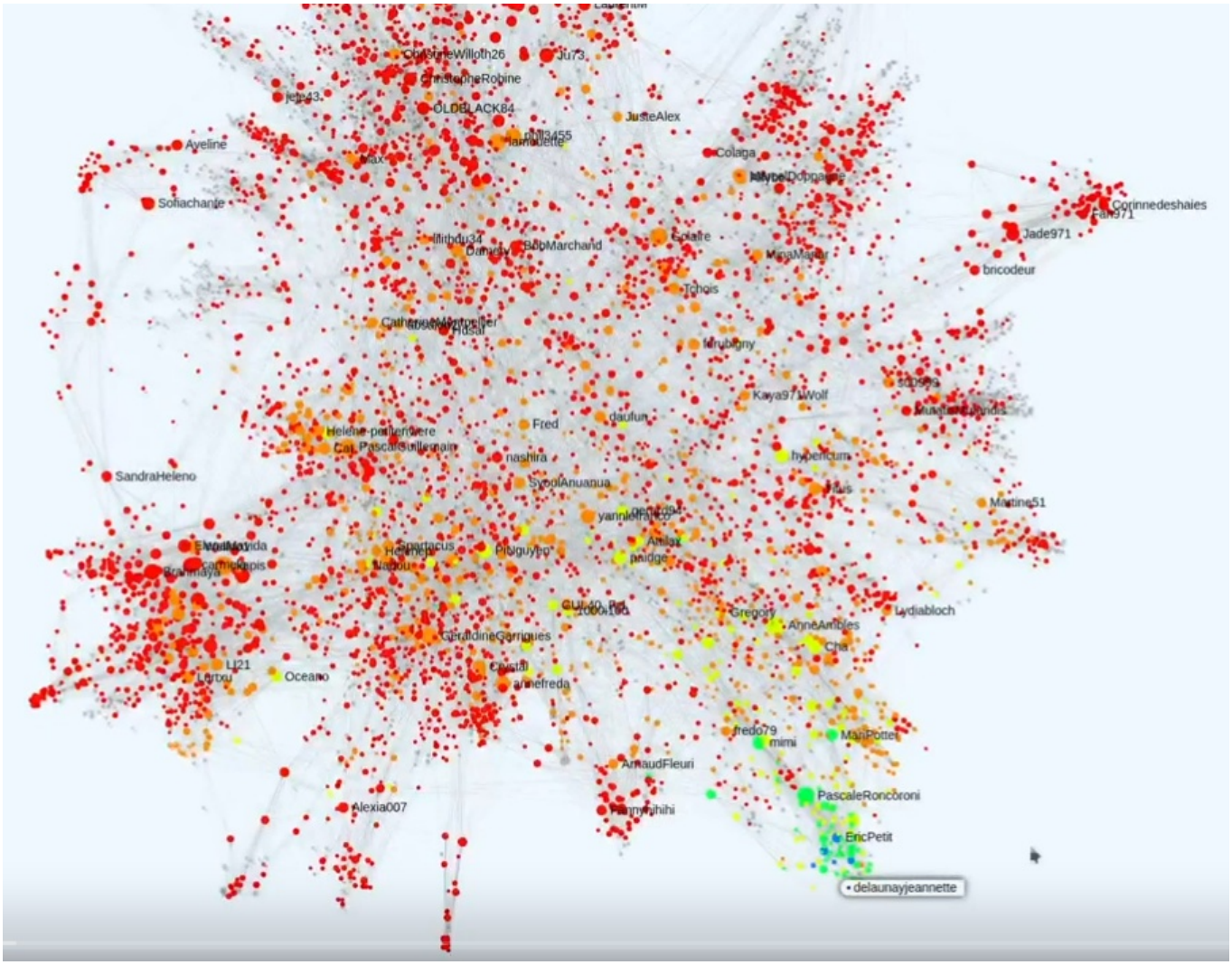
Comment ça fonctionne en cas de création en masse de faux-comptes:



Les membres isolés en jaune les plus éloignés ne sont pas certifiés par le reste de la toile
Ils sont donc situés à 2 pas du reste de la toile
2 pas de moins, ça fait beaucoup moins de référents atteints à 4 pas!

Si le reste de la toile décide de ne plus certifier ces membres, ils ne pourront pas aider à la création de nouveaux comptes membres, et une triche serait freinée.

Visualisation du nombre de référents atteints à chaque pas:



Référents atteints:

1 pas, bleu: 0.14%
2 pas, vert: 1.16%
3 pas, jaune: 4.75%
4 pas, orange: 22.94%
5 pas, rouge: 70.38%

Outils:

https://wotwizard.axiom-team.fr/fr pour faire un suivi des ses contacts, connaitre les futurs entrants et sortants

monit.g1.nordstrom.duniter.org fait un point sur les certifications des futurs membres

https://html.wotwizard.axiom-team.fr/ version texte de wotwizard, quelques fonctionnalités en plus

Et les cartes, wotmap.duniter.org worldwotmap.duniter.org carte.monnaie-libre.fr