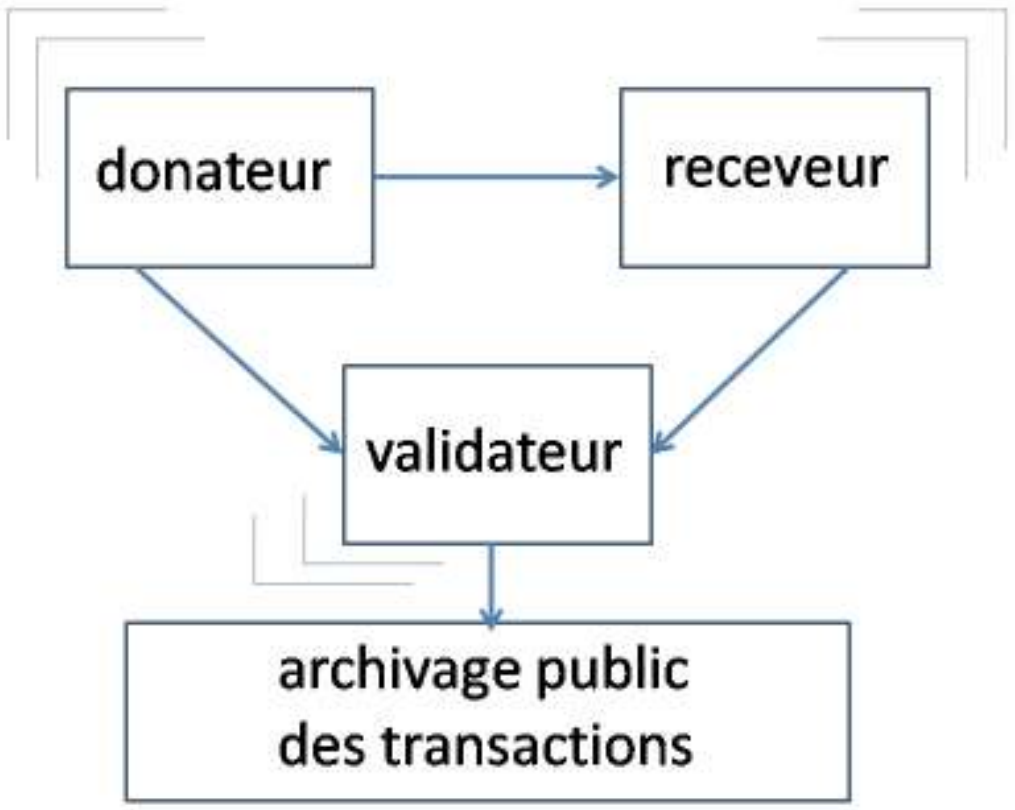
Présentation du Joussemet, projet de monnaie de la solidarité

philippe.coueignoux@eprivacy.com **Ph Coueignoux 6/2/19**

Annexe III: Considérations techniques

Schéma de principe



Technologies de base

La puissance de calcul nécessaire à un test local ne devrait pas dépasser celle des matériels informatiques dispo-nibles, tant pour les serveurs que pour les clients. De même une grande ville, a fortiori une zone qui a acquis le statut de métropole urbaine, ne devrait avoir aucun problème à offrir à tous l'accès à Internet avec une bande passante minimum.

Hormis les aspects avancés dont il est question ci-dessous, la complexité logicielle sera également limitée.

Par contre l'ergonomie des fonctionnalités requises et de leur intégration dans un système destiné au grand public demandera un soin particulier. La conception devra aussi rechercher la souplesse de façon à pouvoir prendre en compte à moindres frais les leçons reçues au cours des opérations d'écoute et de communication.

Technologies avancées

Le projet suppose la maîtrise de trois technologies avancées mais qui arrivent maintenant à maturité.

Les transactions sans contact permettent à un donateur de faire un don à un receveur avec le minimum de contraintes physiques hormis la présence en face à face des deux acteurs concernés. Elles sont le complément naturel de la nature électronique du joussemet et traduisent le caractère personnel de la reconnaissance.

Parmi les formes couramment déployées, on choisira celle qui a à la fois la plus grande diffusion et le moindre coût comparé au ressources des utilisateurs. L'intégration de la communication en champ proche (CCP) dans les téléphones mobiles est aujourd'hui le dispositif grand public le plus largement disponible. Cette solution a deux inconvénients: elle exige un contact très rapproché entre émetteur et receveur et la possession d'un téléphone mobile.

Dans la mesure où la reconnaissance de la solidarité suppose un face à face entre donneur et receveur, l'exigence d'un contact de quelques centimètres au maximum ne constitue pas un obstacle majeur au moins dans un premier temps.

L'obstacle le plus sérieux est le coût élevé d'un téléphone mobile au vu des ressources de nombreuses personnes susceptibles de recevoir des joussemets. D'un autre côté un test local n'aura pas une échelle suffisante pour justifier les frais fixes d'étude et de déploiement d'autres supports comme les cartes à puce, de coût unitaire plus faible et pouvant faire l'objet d'une subvention. On propose de contourner cette difficulté en tirant parti des coûts cassés des téléphones mobiles de seconde main. A petite échelle, on estime que la mairie en charge d'un test local trouvera en nombre suffisant pour équiper les plus démunis des téléphones que particuliers et compagnies seront prêts à contribuer par solidarité au titre du mécénat.

On notera que la possession d'un téléphone mobile n'entraîne pas de frais pour ceux qui n'auraient pas les moyens d'un abonnement. La municipalité peut par exemple leur donner accès à des lieux de recharge par pédalage, comme le font aujourd'hui certaines gares SNCF. L'impossibilité pour certains de pédaler serait, non pas un obstacle de plus, mais une opportunité à d'autres de faire preuve de solidarité en pédalant à leur place. La municipalité peut encore équiper ces lieux de recharge de transmetteurs pour servir d'intermédiaire entre un téléphone en CCP et le réseau Internet pour déclarer et valider les donations reçues ou effectuées. Par ailleurs les personnes ainsi équipées par la mairie y gagneraient la possibilité de composer en cas de nécessité les numéros d'urgence reconnus sans restriction par les compagnies de téléphonie mobile.

La solution retenue pour les contacts en face à face peut évoluer au cours du temps sans en changer la nature. Viendront se rajouter par la suite les contacts par Internet via les services de collecte en ligne.

La chaîne de blocs fournit un archivage distribué de l'ensemble des transactions et empêche de pouvoir dépenser deux fois la même monnaie électronique. Elle n'oblige pas les utilisateurs à confier la gestion de leurs avoirs à une tierce partie comme pour un compte en banque. Sachant que son système d'archivage résiste aux défaillances et aux attaques ponctuelles, c'est donc un facteur de confidentialité et de sécurité.

La meilleure solution dépend de la disponibilité, du coût d'exploitation et du débit de la mise en œuvre. Le code source de cette technologie est dans le public mais il faut la déployer dans un cadre différent du bitcoin,

son origine, car le joussemet ne partage pas ses objectifs de monnaie marchande indépendante des états.

La volonté du bitcoin de s'affranchir des états entraîne le recours à une méthode publique sans permission comme celle du bitcoin, qui met en concurrence n'importe quel agent pour le droit d'archiver chaque bloc de transactions. C'est ce recours à la concurrence qui est la cause de la consommation exaggérée d'énergie, du fort coût d'exploitation et du faible débit de transaction caractéristiques de la mise en œuvre du bitcoin.

On propose donc d'adopter une méthode avec permission comme celle mise en œuvre avec Hyperledger Fabric. Soumettant les agents chargés de l'archivage à un processus de sélection, cette approche assure un coût réduit et un débit suffisant à petite échelle tout en permettant de monter en échelle selon les besoins.

La solution précise retenue pour l'archivage peut aussi évoluer au cours du temps sans en changer la nature.

Le porte-monnaie électronique permet à chaque utilisateur de gérer ses avoirs en monnaie électronique, d'en recevoir et d'en donner. C'est un concept logiciel bien connu à l'heure actuelle et disponible gratuitement auprès de nombreuses sources. Par contre il n'est pas désirable de prendre telle quelle une application du commerce, sachant que le porte-monnaie concerné doit suivre les règles spécifiques au joussemet et s'adapter aux choix précédents de supports d'échange et d'archivage et de suivre leur évolution.

On propose donc de développer un prototype de porte-monnaie électronique dès la phase de test. Ce qui suit est un aperçu schématique de son fonctionnement, en repoussant à une phase ultérieure la mise en œuvre des services de collecte en ligne

Le joussemet se présente sous la forme de jetons émis et signés par l'Autorité ou son équivalent:

((Numéro, Date d'émission, valeur d'émission), empreinte numérique de l'Autorité sur ce triplet)

Le porte-monnaie électronique est chargé pour son détenteur de:

- calculer à tout moment le solde du compte selon la date d'émission des jetons détenus
- effectuer un don à un receveur selon le montant déclaré par le détenteur et le solde disponible
- alerter le détenteur de la réception d'un don et de l'accepter dans la limite du plafond
- communiquer le solde à l'Autorité aux dates prévues par elle sous peine de gel du compte

A chaque porte-monnaie électronique correspond une paire de chiffrement asymétrique, clé privée / clé publique. La clé publique est déclarée par son détenteur lorsque ce dernier reçoit un nouveau porte-monnaie et est archivée dans une base de données unique avec l'identité du détenteur et sa nature (particulier, service de collecte en ligne, entreprise, association, collectivité territoriale, administration). Servant d'identificateur, cette clé permettra à la fois de faire respecter le plafond et le suivi des avoirs individuels et les autres règles qui dépendent de la nature du détenteur.

Toute transmission de joussemet entre une administration et un particulier doit s'effectuer avec cette clé publique qui identifie le particulier. Par contre, pour tout autre don à recevoir, le porte-monnaie engendre une nouvelle paire de chiffrement asymétrique, clé privée / clé publique, qui masque l'identité du détenteur.

Les jetons formant un don vont d'un émetteur A à un receveur B en une transaction validée par un agent V selon le déroulement suivant:

-0- A choisit un agent V et se procure son adresse et sa clé publique Kpu(V) d'après une liste publique
-1- A lit la clé publique Kpu(B) de B, qui identifie B si nécessaire, renommée ci-après Kpu(B, J)
-2- A envoie à B, chiffré avec Kpu(B, J), le jeton J, l'adresse et la clé de V et sa clé publique Kpu(A, J)
et séquestre le jeton J dans son porte-monnaie comme 'don en cours'
-3- A envoie à V, chiffré avec la clé publique Kpu(V)
- le jeton J, sa clé publique Kpu(A, J) et la clé publique Kpu(B, J)
- son empreinte numérique sur le triplet précédent (chiffrée avec sa clé privée Kpr(A, J))
-3- B déchiffre le message de A avec sa clé privée Kpr(B, J) pour récupérer J, V et Kpu(A, J)
-4- B, si son plafond l'autorise, envoie à V, chiffré avec la clé publique Kpu(V)
- le jeton J, la clé publique Kpu(A, J) et sa clé publique Kpu(B, J)
- son empreinte numérique sur le triplet précédent (chiffrée avec sa clé privée Kpr(B, J))
séquestre le jeton J dans son porte-monnaie comme 'don potentiel'
et engendre une nouvelle paire de clé si nécessaire,
-5- V reçoit et, avec sa clé privée Kpr(V), déchiffre le message de A
V retrouve le message correspondant de B dans une fenêtre de latence maximum autorisée:
-6- V vérifie que:
- les messages de A et B proviennent bien des détenteurs des clés Kpu(A, J) et Kpu(B, J)
en retrouvant leurs empreintes grâce à Kpu(A, J) et Kpu(B, J) sur les messages reçus
- les deux parties s'accordent bien pour transférer le jeton J de Kpu(A, J) à Kpu(B, J)
- le jeton J est authentique, en vérifiant l'empreinte numérique de l'Autorité sur ce jeton
- Kpu(A, J) était bien le dernier détenteur connu du jeton J selon la chaîne de blocs
-7- V ajoute en vue de la construction d'un nouveau bloc d'archive la transaction
((jeton J, date de la transaction, Kpu(A, J), Kpu(B, J)),
empreinte numérique de V sur le quadruplet)
-8- après un délai minimal de latence:
- A vérifie dans l'archive publique le don du jeton J marqué par (Kpu(A, J), Kpu(B,J))
et élimine le jeton J du porte-monnaie ou bien le remet en avoir
- B vérifie dans l'archive publique le don du jeton J marqué par (Kpu(A, J), Kpu(B,J))
et comptabilise le jeton J dans son avoir ou bien l'élimine du porte-monnaie

Tant que la transaction concernée n'est pas archivée dans un nouveau bloc dans la chaîne publique, A peut théoriquement forcer son porte-monnaie de façon à pouvoir donner le même jeton J à un autre receveur C. En cas de conflit entre deux transactions portant sur le même jeton en provenance du même donateur qu'un agent de validation s'apprête à archiver dans le même bloc, l'agent d'archivage ne retiendra que le premier don de A dans l'ordre chronologique des transactions. On estime qu'un receveur frustré devra accepter la perte du don correspondant, sachant que, s'il connaît par ailleurs l'identité de A, il pourra lui reprocher son comportement désinvolte et, dans le cas d'une administration, prendre des mesures de rétorsion. Dans ces conditions, il est douteux que A cherche à violer le fonctionnement du porte-monnaie.

On notera enfin que le caractère public de la chaîne de blocs servant d'archive et la gestion des clés esquissée ci-dessus permettent bien la confirmation officielle des activités de solidarité de chaque particulier, soit en réception soit en contribution de joussemets en lien avec les collectivités territoriales et l'administration. Ce dispositif permet aussi la confidentialité de l'usage intermédiaire qu'en font les particuliers. Pour garantir cette dernière, il faut en plus veiller à anonymiser les communications vers les agents de vérification et donner aux particuliers la possibilité de se faire des dons à eux-mêmes, dissociant par là les identités initiales et finales d'une chaîne de donation de ses usages intermédiaires.