Réseau blockchain de traitement décentralisé des paiements

Slava Gomzin, Dan Itkis

Version 3

Octobre 2018

Traduction : Stéphane Gariazzo

La version initiale a été publiée en juin 2017

Résumé
Généralités
Avantages du traitement décentralisé des paiements
Terminologie
Échantillon d'autorisations
DAPI
Courtier
Super-nœud complet
GRAFT
GRAFT Point of Sale
GRAFT Wallet
GRFT
Jeton marchand
Passerelle de paiement
Jeton de paiement ("à valeur stable")
Super-nœud proxy
VChain (chaîne virtuelle)
Frais de transaction
Intérêt de facturer des frais
Facturer la bonne personne
Micropaiements : comment payer un café en cryptomonnaie ?
Frais de transaction GRAFT
Frais imputés aux marchands et fournisseurs de services
Transferts de fonds gratuits : transactions authentifiées
Confidentialité
Utilité d'une blockchain privée
CryptoNote : la base de la confidentialité
Transactions privées
Traitement des transactions
Problème lié au délai de confirmation : lancement des autorisations en temps réel
Super-nœuds
DAPI
Validations en temps réel par un échantillon d'autorisations
Verrouillage du compte d'autorisation
Niveaux d'un super-nœud
Nœuds de minage

Récompenses pour validation (minage)
Niveaux d'un super-nœud complet
Caution déléguée
Échantillon d'autorisations
Super-nœuds proxy
Récompenses des super-nœuds
Évolutivité
Validation des transactions hors ligne
Passerelles de paiement pour les marchands et les fournisseurs de services
Types de transaction et processus de paiement
Autorisation
Pré-autorisation
Validation
Vente
Transfert
Annulation
Émission
Utilisation
Échange
Planification
Dépôt de garantie
Remboursement
Traitement de transactions en utilisant des jetons GRFT comme mode de paiement
Traitement des transactions via d'autres modes de paiement
Courtiers
Agent de paiement
Aspects techniques et économiques des agents de paiement et d'encaissement
Agents de paiement/d'encaissement
Au-delà des paiements aux marchands : la plateforme d'échange décentralisée (DEX)
Courtier d'échange
Agent d'encaissement
Courtier de rechargement
Paiements aux marchands
Volatilité
Jeton de paiement ("à valeur stable")
Garantie des jetons de paiement

Traitement des paiements
Jetons marchands et VChains
Jetons marchands
Types de jetons marchands
Types de transaction pour les jetons marchands
Frais associés aux jetons marchands
VChains
Frais associés à la VChain
Crédit communautaire décentralisé
Sécurité
Disponibilité
Gestion des identités
Identification, authentification et autorisation
Vérification d'identité
Score de réputation : éclairer les ténèbres
Support client, résolution des conflits et garantie des paiements
Applications pour les utilisateurs
Conclusion
Références

Résumé

GRAFT (*Global Real-Time Authorizations and Funds Transfers*) est une solution Open Source globale décentralisée, basée sur la blockchain et accessible à tous, combinant une plateforme de traitement et une passerelle de paiement. N'importe quel acheteur et n'importe quel marchand peuvent utiliser GRAFT, de façon totalement décentralisée et peu onéreuse. L'écosystème GRAFT est ouvert : chacun peut participer au fonctionnement de la blockchain GRAFT et à la mise en œuvre des services réseau.

GRAFT utilise des processus et des protocoles de traitement des paiements semblables à ceux employés par les systèmes traditionnels de paiement électronique (cartes de débit, de crédit et prépayées, par exemple), qui sont déjà utilisés en toute confiance par des millions de consommateurs et de marchands à travers le monde. Cette approche vise à faciliter et à accélérer l'adoption généralisée de GRAFT en tant que plateforme de paiement. De plus, elle évite de recourir à des intermédiaires centralisés (passerelles et processeurs de paiement), qui sont actuellement nécessaires pour faciliter les transactions entre acheteurs et marchands.

Généralités

Le Bitcoin[1] a été créé comme une "monnaie virtuelle". Initialement, il s'agissait d'un système de paiement sécurisé, mais relativement lent, qui n'était pas en mesure de remplacer les cartes de paiement en ligne, ni de concurrencer les cartes de débit/crédit et les espèces utilisées dans les magasins physiques (Figure 1).

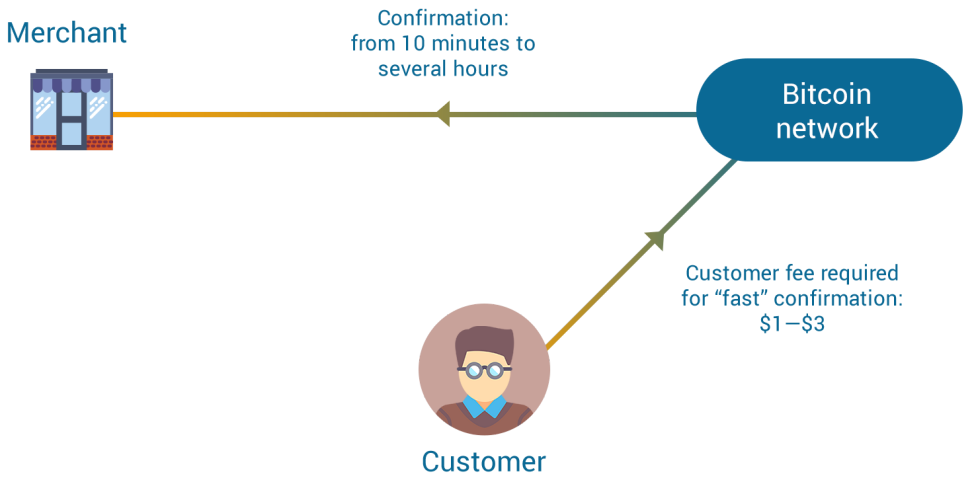

Figure 1 : Traitement d'une transaction en Bitcoin sans intermédiaire centralisé

Malgré l'amélioration des délais de confirmation de certaines cryptomonnaies et de certains jetons cryptographiques existants[2], ceux-ci ne permettent toujours pas de traiter des types de transaction essentiels comme l'autorisation et la validation. C'est pourquoi nous pensons que les secteurs de la vente au détail, de l'hôtellerie-restauration et du commerce de proximité ne peuvent adopter ces cryptomonnaies sans utiliser des intermédiaires (passerelles et processeurs de paiement)[3] pour faire le lien (Figure 2). Toutefois, dans le cadre d'une transaction de paiement cryptographique, l'existence même de processeurs de paiement (qui prennent généralement la forme d'une entreprise commerciale centralisée, réglementée par les pouvoirs publics et contrôlée par des actionnaires) va à l'encontre de certains principes fondamentaux des cryptomonnaies et des jetons cryptographiques : la décentralisation, la confidentialité et l'indépendance.

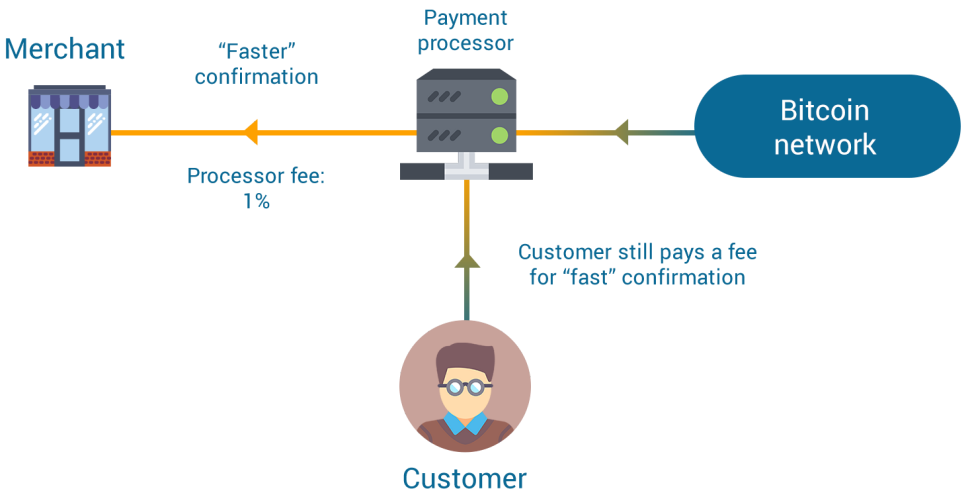

Figure 2 : Traitement d'une transaction en Bitcoin par un intermédiaire centralisé

La plupart des marchands ne sont pas en mesure d'accepter des cryptomonnaies sans passer par un processeur de paiement tiers, en raison de l'approche unique utilisée par les réseaux de blockchain pour le traitement des transactions. Ce processus est basé sur un concept différent des systèmes de paiement électronique traditionnels. Malgré quelques imperfections inhérentes à ces derniers, les technologies développées autour de ces systèmes ont accumulé énormément d'expérience côté marchand et de confiance côté utilisateur.

Il existe plusieurs différences de taille entre les méthodes utilisées par les systèmes de paiement traditionnels et cryptographiques pour gérer les transactions. Dans la plupart des cas, ces différences rendent les systèmes de paiement cryptographique moins attrayants pour les marchands et/ou les consommateurs. La liste ci-dessous répertorie quelques-unes des limites techniques et des failles

commerciales que présentent les systèmes existants de paiement cryptographique par rapport aux systèmes de paiement électronique traditionnels :

- Non prise en charge de tous les types de transaction essentiels
- Processus de paiement inadaptés
- Délais de confirmation longs
- Frais de transaction non équilibrés et non prévisibles
- Impossibilité de traiter les micro-paiements et les débits répétés (abonnements)
- Non prise en charge des transactions hors ligne
- Faible évolutivité
- Volatilité
- Sécurité incomplète
- Absence de confidentialité en raison de la traçabilité de la blockchain
- Absence de confiance entre l'acheteur et le marchand
- Utilité contestable
- Ergonomie limitée des interfaces utilisateur
- Support client limité

GRAFT a pour objectif de résoudre ces problèmes en créant une plateforme qui, à terme, doit permettre pour la première fois l'adoption généralisée des paiements cryptographiques par un maximum de marchands et de consommateurs, tout en respectant les principes de base des cryptomonnaies et des jetons cryptographiques.

Avantages du traitement décentralisé des paiements

Qu'est-ce qui peut inciter un consommateur à commencer à utiliser des cryptomonnaies ou des jetons cryptographiques au lieu (ou en plus) de ses cartes bancaires, de PayPal ou d'Apple Pay ? Et pourquoi un marchand choisirait-il d'accepter des cryptomonnaies ou des jetons cryptographiques en plus (ou au lieu) des modes de paiement existants ? Évidemment, si nous n'avions pas les réponses à ces questions simples, la rédaction de ce livre blanc n'aurait eu aucun intérêt.

La réponse à la première question peut se composer de plusieurs éléments, car différentes raisons (combinées ou distinctes) peuvent inciter des particuliers à conserver leur argent sous la forme d'une cryptomonnaie ou de jetons cryptographiques. En revanche, la réponse à la deuxième question est relativement simple. Les marchands veulent élargir leur clientèle afin d'accroître leur chiffre d'affaires.

S'ils identifient un nombre important de clients potentiels qui préfèrent, pour une raison ou une autre, utiliser des cryptomonnaies ou des jetons cryptographiques, ils commenceront à accepter ce type de paiement. Or, GRAFT leur offre une occasion unique d'accepter des paiements par cryptomonnaie ou jetons cryptographiques directement auprès de leurs clients, sans intermédiaire et avec des frais extrêmement faibles.

GRAFT est un processeur de paiement décentralisé dont le fonctionnement est basé sur des jetons utilitaires numériques. Il est donc capable de faciliter le cycle de paiement complet sans faire intervenir de cryptomonnaies, jetons cryptographiques ou actifs externes. Toutefois, GRAFT proposera également le Bitcoin et plusieurs cryptomonnaies de premier plan, ainsi que des jetons cryptographiques, comme option supplémentaire pour les acheteurs et comme mode de paiement accepté par les marchands. Grâce à cette fonctionnalité, les marchands n'auront plus besoin de s'associer à différents fournisseurs de logiciels de paiement (centralisés). En outre, les utilisateurs n'auront plus besoin de s'inscrire à des services centralisés, ni d'apprendre à se servir de plusieurs applications de portefeuille.

Terminologie

Échantillon d'autorisations

Groupe de "super-nœuds" complets sélectionnés, qui approuvent les paiements en temps réel et garantissent que l'acheteur ne peut pas dépenser les mêmes fonds plusieurs fois avant l'écriture de la transaction dans la blockchain.

DAPI

API décentralisée sans état ("stateless"), implémentée par les super-nœuds pour prendre en charge les applications client léger comme GRAFT Wallet, GRAFT Point of Sale, ainsi que les applications tierces de point de vente et de cartes d'achat. Le code source du SDK GRAFT est transmis aux fournisseurs tiers d'applications de point de vente et de portefeuille afin de faciliter leur intégration dans GRAFT.

Courtier

Extension du protocole GRAFT hébergée sur un super-nœud ou un groupe de super-nœuds et par l'opérateur du super-nœud. Les courtiers implémentent des fonctionnalités spéciales supplémentaires

qui ne peuvent pas être exécutées automatiquement par un réseau totalement décentralisé et/ou qui nécessitent un cadre réglementaire particulier. Exemples de **courtiers** : courtier acceptant les paiements en Bitcoin, agent d'encaissement en monnaie fiduciaire.

Super-nœud complet

Serveur indépendant actif en permanence ("*always-on*") qui exécute l'implémentation combinée du nœud de la blockchain GRAFT et du nœud de la DAPI GRAFT, traite les autorisations en temps réel, échange les appels DAPI entre les acheteurs, les courtiers et les marchands, et héberge les services tiers comme l'échange instantané de cryptomonnaies au sein du réseau GRAFT, l'acceptation des cartes de crédit/débit et les paiements en faveur des marchands. Les super-nœuds gèrent collectivement la deuxième couche du réseau GRAFT à l'aide d'un algorithme de preuve d'enjeu (POS, *Proof of Stake*).

GRAFT

1. *Global Real-time Authorizations and Funds Transfers* (transferts de fonds et autorisations en temps réel à l'échelle mondiale). Il s'agit d'une plateforme internationale, ouverte et décentralisée, qui assure le traitement et l'exécution en temps réel de paiements en faveur des marchands et de transferts de fonds. Elle est basée sur une blockchain intraçable, une API décentralisée et une communauté ouverte de courtiers qui acceptent diverses méthodes de paiement et de versement, dont les cryptomonnaies, les jetons cryptographiques, ainsi que les cartes de crédit et les virements bancaires traditionnels.

2. Le terme anglais "graft" signifie également "greffe", c'est-à-dire une plante dans laquelle on implante une petite branche ou un bourgeon d'une autre plante pour la faire croître en faisant corps avec la première[4]. La greffe est une technique perfectionnée qui permet aux botanistes, agriculteurs, jardiniers et autres amateurs d'ajouter du tissu vivant d'une plante à une autre[5]. Grâce à cette technique, les meilleures caractéristiques de différentes plantes peuvent s'unir pour former un élément de meilleure qualité et plus intéressant que les éléments d'origine.

GRAFT Point of Sale

Applications "allégées" pour mobile et ordinateur, qui permettent aux marchands d'accepter des paiements en jetons GRAFT, Bitcoins, altcoins ou cartes de crédit/débit, d'émettre et d'utiliser des

chèques-cadeaux, des points de fidélité et des avoirs en magasin, et de configurer des paiements en jetons GRAFT, Bitcoins, altcoins ou monnaies fiduciaires locales.

GRAFT Wallet

Extensions applicatives "allégées" pour ordinateur, mobile et navigateur permettant d'effectuer des paiements et des transferts de fonds avec des jetons GRAFT, d'autres cryptomonnaies de premier plan, des jetons cryptographiques ou des cartes de crédit/débit, via un appel à la DAPI GRAFT.

GRFT

Jeton cryptographique natif accepté par la blockchain GRAFT et utilisé pour les autorisations de paiement en temps réel, les transferts de fonds, et les paiements entre acheteurs et marchands.

Jeton marchand

Contrat intelligent ("*smart contract*") prédéfini grâce auquel le marchand peut créer un jeton privé appartenant à son propriétaire. Les jetons marchands permettent de mettre en œuvre des fonctions importantes comme le jeton de paiement en faveur du marchand ("*stablecoin*", cryptomonnaie stable), et des systèmes propriétaires en réseau fermé pour les points de fidélité, les chèques-cadeaux, les avoirs en magasin et les bons de réduction proposés par les marchands.

Passerelle de paiement

Elle permet aux marchands et/ou aux fournisseurs de services de paiement de gérer la configuration de leurs terminaux de paiement (adresse de portefeuille, par exemple) et de définir les frais spécifiques facturés par le fournisseur. De plus, elle génère des rapports et des analyses supplémentaires sur les transactions.

Jeton de paiement ("à valeur stable")

Il représente une monnaie fiduciaire locale et peut faire l'objet d'une transaction sur la blockchain GRAFT en temps réel via le réseau de super-nœuds de la blockchain. Le jeton de paiement est basé sur la technologie des jetons marchands GRAFT (semblable aux chèques-cadeaux, récompenses et autres types de jetons marchands).

Super-nœud proxy

Il s'agit d'un super-nœud qui facilite la transaction avec le marchand en communiquant avec le point de vente du marchand et/ou le portefeuille de l'acheteur d'une part, et avec le reste des super-nœuds de l'échantillon d'autorisations d'autre part.

VChain (chaîne virtuelle)

"Compte marchand" indépendant, décentralisé et virtuel, où les marchands peuvent créer des jetons marchands, et configurer les déclencheurs et les règles d'autorisation et de paiement qui auront un impact sur leurs transactions.

Frais de transaction

Tout d'abord, pourquoi est-il nécessaire d'appliquer des frais de transaction ? En effet, la blockchain ne repose sur aucune entreprise commerciale. Alors pourquoi les utilisateurs devraient-ils payer des frais ? Qui les collecte ? Et quelle commission le percepteur doit-il facturer ?

Intérêt de facturer des frais

Le fonctionnement de réseaux de cryptomonnaies et de jetons cryptographiques sécurisés et hautement disponibles nécessite de multiples nœuds (serveurs) puissants, répartis dans le monde entier. Qui va gérer ces serveurs, et quels facteurs de motivation et d'incitation pourraient faciliter la gestion du nœud blockchain ? Pour le Bitcoin, les autres réseaux cryptographiques et les réseaux de jetons cryptographiques, le financement est obtenu grâce aux frais de minage et de transaction (les propriétaires du nœud gagnent de l'argent en minant de nouveaux jetons à partir de chaque bloc et en prélevant une commission sur chaque transaction).
Le minage a un autre but : l'injection constante et régulière de nouveaux jetons dans le système pour que la liquidité puisse répondre à la demande croissante de jetons supplémentaires, au fur et à mesure de la progression de l'adoption et de l'utilisation. Plus le système fera des adeptes, plus les opérateurs du nœud percevront des revenus liés aux frais de transaction. La prime de minage peut donc être diminuée progressivement avec chaque nouveau bloc afin de limiter l'offre globale.

Dans un monde idéal, les cryptomonnaies et les jetons cryptographiques seraient accessibles à tous gratuitement. En réalité, certains réseaux promettent des transactions gratuites[6]. Dans d'autres

réseaux, y compris Bitcoin, les frais permettent de prioriser les transactions et de "résoudre" le problème de l'évolutivité.

Toutefois, dans le réseau GRAFT, les frais sont mis en place pour deux raisons. La première consiste à éviter toute utilisation abusive du réseau, ainsi que les problèmes connexes liés aux performances et à la taille de la blockchain (par exemple, l'utilisation du réseau réel pour effectuer des tests). Si une transaction est totalement gratuite, on pourrait transférer indéfiniment un même montant entre deux comptes. La deuxième raison est la suivante : ces frais deviennent le seul facteur d'incitation pour les opérateurs du nœud lorsque la prime de minage devient trop faible.

Facturer la bonne personne

Les frais de transaction des Bitcoins et des jetons cryptographiques posent problème, car ils ne sont pas facturés à la bonne personne. C'est encore pire que pour les paiements traditionnels par carte, car une transaction en cryptomonnaie ou en jetons cryptographiques entraîne des frais à la fois pour l'acheteur et pour le marchand : l'acheteur paie le réseau de cryptomonnaie ou de jetons cryptographiques, et le marchand rémunère le processeur de paiement. Le payeur moyen est souvent perturbé par le processus, qui se rapproche plus d'un jeu d'argent et ne fournit pas d'explications claires sur la grille tarifaire, ce qui ne rend pas les paiements par cryptomonnaie ou jetons cryptographiques très attrayants.

Micropaiements : comment payer un café en cryptomonnaie ?

Actuellement, le Bitcoin est confronté à un autre problème : son incapacité à traiter les micropaiements en raison des frais de transaction élevés[7]. Pour résoudre ce problème, GRAFT adopte une démarche unique concernant les frais de transaction.

Frais de transaction GRAFT

Dans l'écosystème de GRAFT, **le payeur ne paie aucuns frais**. Tous les frais sont supportés par le destinataire du paiement (marchand ou bénéficiaire). Avec GRAFT, les micropaiements sont possibles, car les frais sont très faibles (par rapport aux cartes de crédit, aux processeurs de paiements en ligne, aux cryptomonnaies et aux autres jetons cryptographiques)[8].

Tableau 1 : Système de récompenses/frais de transaction GRAFT

		1	2	3
		Transfert standard de personne à personne (P2P)	**Transaction RTA (autorisation en temps réel) (GRFT)**	**Transaction RTA avec courtier altcoin (Bitcoin accepté)**
a	**Récompense versée au super-nœud proxy du portefeuille de l'émetteur**	0,1 GRFT*	0,05 %*	0,05 %*
b	**Récompense versée au super-nœud complet (membre de l'échantillon d'autorisations)**	N/A	0,0625 %**	0,0625 %**
c	**Récompense versée au courtier**	N/A	N/A	0,25 %**
d	**Récompense versée au mineur (règlement)**	Variable (dépend de la taille de la transaction en Ko)	Configurable*** Min. : 0,1 GRFT	Configurable*** Min. : 0,1 GRFT
e	**Récompense versée au super-nœud proxy de la passerelle du bénéficiaire/du point de vente du marchand****	N/A	0,05 %****	0,05 %****
	Montant forfaitaire total payé par l'émetteur de la transaction (acheteur dans la RTA)	a1 + d1	0	0*****
	Montant forfaitaire total payé par le destinataire de la transaction (marchand dans la RTA)	0	a2 + b2x8 + d2 + e2	a3 + b3x8 + c3 + d3 + e3
	Montant total facturé à l'émetteur de la transaction	Montant de la transaction + a1 + d1	Montant de la transaction	Montant de la transaction
	Montant total des fonds disponibles pour le destinataire de la transaction	Montant de la transaction	Montant de la transaction - (a2 + b2x8 + d2 + e2)	Montant de la transaction - (a3 + b3x8 + c3 + d3 + e3)

* Le super-nœud **proxy** du portefeuille peut être un serveur propriétaire ou un cluster public hébergé par un fournisseur de services. Vous pouvez exécuter et utiliser votre propre super-nœud **proxy** propriétaire pour éviter l'ensemble des frais intermédiaires. Pour facturer les frais, le super-nœud doit détenir une "caution" (*stake*).

** Pour participer au traitement de cette transaction RTA et recevoir cette récompense, le super-nœud complet ou le courtier doivent détenir une "caution" (*stake*).

*** Définie par le fournisseur de services de paiement ou le propriétaire du super-nœud proxy du point de vente.

**** Le super-nœud proxy du point de vente peut être un serveur indépendant propriétaire, intégré à l'infrastructure du marchand, ou faire partie d'une passerelle d'e-commerce et/ou d'un terminal de paiement géré par le fournisseur de services de paiement. Pour recevoir cette récompense, le super-nœud du point de vente doit détenir une caution (*stake*).

***** N'inclut pas les frais du réseau d'altcoins.

Les récompenses du super-nœud proxy (a1, a2, a3, e2, et e3 dans le tableau 1) permettront une décentralisation totale de l'infrastructure réseau. Si vous n'appréciez pas le cluster de super-nœuds proxy hébergé par un fournisseur de services spécifiques, vous pourrez faire appel à d'autres fournisseurs pour connecter votre portefeuille ou votre point de vente. Pour recevoir la récompense, le super-nœud proxy doit apporter la preuve d'un portefeuille de caution unique associé à l'adresse IP publique du super-nœud. Le montant de la caution du super-nœud proxy s'élève à 250 000 GRFT.

Contrairement à un super-nœud d'échantillon d'autorisations, le super-nœud proxy reste opérationnel même sans caution. Toutefois, un super-nœud proxy sans caution ne peut pas facturer de frais. Cette fonctionnalité est réservée aux super-nœuds proxy propriétaires. Les utilisateurs qui ont de fortes exigences en termes de confidentialité peuvent donc héberger leurs propres points d'entrée sur le réseau. En l'absence de caution, la récompense du super-nœud proxy sera envoyée à l'adresse du portefeuille de dons à la communauté GRAFT. Ainsi, le montant total des frais de transaction, composé de plusieurs éléments, reste toujours cohérent quel que soit le statut des super-nœuds proxy.

Un forfait est payé au mineur pour le règlement de transactions RTA (d2, d3). Les frais de minage sont

généralement calculés selon la taille d'enregistrement de la transaction, en Ko (d1). Dans le cadre des transactions RTA, ces frais de minage ne peuvent pas être variables, car le total des frais payés par le marchand serait incohérent et imprévisible, ce qui n'est pas acceptable dans la plupart des cas. De plus, ces frais ne peuvent pas être proportionnels à la valeur de la transaction (comme pour les frais des super-nœuds), car les frais de minage sont visibles sur la blockchain, ce qui signifie que le montant de la transaction pourrait être calculé à partir d'une commission proportionnelle (nous devrions toutefois résoudre ce problème à l'avenir). C'est pourquoi nous avons défini un forfait configurable simple, avec un montant minimal de 0,1 GRFT.

Les frais associés aux transactions RTA avec courtiers sont les mêmes que les frais RTA (colonne 2), avec un supplément de 0,25 % prélevé par le courtier (également payé par le marchand).

Frais imputés aux marchands et fournisseurs de services

Les fournisseurs de services de paiement peuvent définir une grille tarifaire conforme à leur modèle économique, et les frais peuvent être structurés par niveaux et assortis d'options. Voici un exemple :

Transactions inférieures à 10 $: 2 %
Transactions supérieures à 10 $: 1 %
Montant de transaction minimal : 1 $
Mineur : 0,1 GRFT
Transactions en altcoins : +0,25 %
Paiements instantanés en altcoins ou en monnaie fiduciaire : +0,25 %

L'exemple ci-dessous illustre une transaction en altcoins de 20 $ et les frais associés, basés sur la grille tarifaire de référence d'un fournisseur de services de paiement.

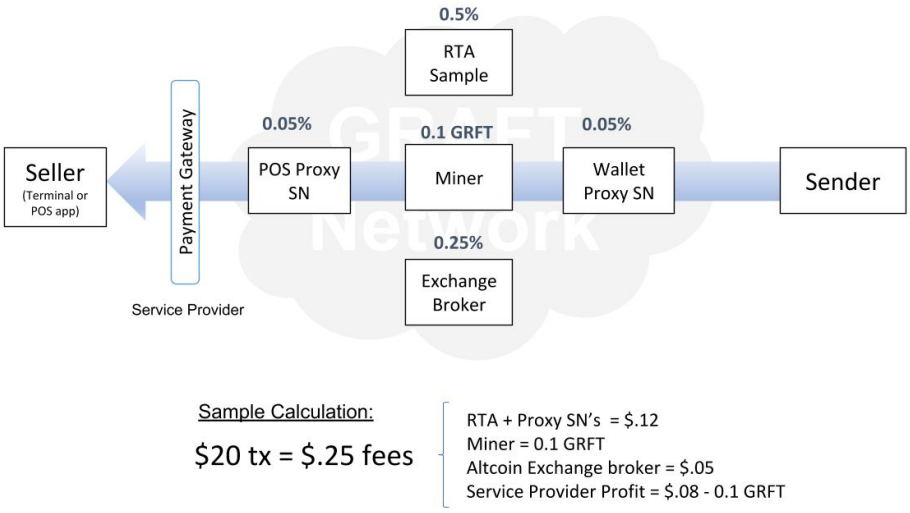

Figure 3 : Exemple de répartition des récompenses/frais pour une transaction GRAFT

Transferts de fonds gratuits : transactions authentifiées

Certains réseaux de paiement, comme l'ACH (*Automated Clearing House*, Système Interbancaire de Télécompensation) ou PayPal, proposent des transferts gratuits entre comptes utilisateur. Afin de concurrencer ces réseaux de paiement traditionnels, GRAFT permettra d'effectuer des transferts gratuits limités entre portefeuilles d'utilisateur authentifiés.

En règle générale, les réseaux de cryptomonnaie ne peuvent pas "se permettre" de proposer des transactions gratuites pour trois raisons principales :

- Absence d'incitation pour les mineurs
- Risque d'attaques par déni de service distribué (DDoS)
- Croissance incontrôlée de la blockchain

Pour résoudre le premier problème (absence de motivation pour les mineurs), GRAFT sépare les paiements et les transferts. Les super-nœuds (mineurs) perçoivent donc des frais de transaction pour les paiements instantanés, qui constituent la majorité des transactions, tandis que les transferts gratuits sont traités avec un niveau de priorité inférieur.

Le deuxième problème (attaques DDoS) est résolu par l'identification et l'authentification volontaires des utilisateurs. Bien entendu, "rien n'est vraiment gratuit", et les utilisateurs "paieront" donc d'une certaine façon, en fournissant leur identité au réseau afin de garantir un usage raisonnable (en limitant le nombre et la fréquence des transferts gratuits par utilisateur), ce qui évitera l'utilisation abusive du réseau. Grâce à une technologie d'authentification par preuve à divulgation nulle de connaissance, les utilisateurs pourront prouver leur identité sans compromettre leur confidentialité.

Le dernier problème (croissance incontrôlée de la taille des blocs) est résolu grâce à plusieurs solutions, telles que des intervalles courts entre les blocs, une taille de bloc illimitée et une taille de transaction standard limitée pour des types de transactions spécifiques (par exemple, pour les transferts gratuits). De plus, pour valider la transaction de transfert gratuit, une des parties doit prouver qu'elle a déjà effectué des transactions de type "paiements commerciaux" par le passé.

Confidentialité

Nous avons parfois une vision déformée du besoin de confidentialité. En réalité, une majorité d'acheteurs légitimes ne voient aucun inconvénient à divulguer leur identité au marchand, en particulier si cela leur est profitable, ou si une telle divulgation est nécessaire pour le traitement de la transaction. De même, les acheteurs veulent s'assurer que le marchand à qui ils envoient un paiement est bien le destinataire visé, et non un usurpateur. Ni le marchand, ni l'acheteur ne souhaitent qu'un tiers soit capable de reconnaître leur identité et de consulter tous les détails de leurs transactions en analysant la blockchain accessible au public.

La confidentialité constitue un sujet sensible pour les cryptomonnaies et le secteur des paiements en général. Elle nécessite un éventail de mesures qui va de l'anonymat complet à la transparence totale, selon ce que décident le vendeur et l'acheteur. Par exemple, le vendeur peut être légalement contraint d'obtenir et de vérifier certaines données personnelles, comme l'âge pour les achats d'alcool ou de cigarettes, ou le code postal pour le calcul des taxes que doivent appliquer les marchands en ligne. Par ailleurs, l'acheteur peut accepter ou non de divulguer tout ou partie des éléments de son identité et doit être en position de le faire. Si le vendeur et l'acheteur s'entendent sur les éléments d'identité à partager, la transaction peut se poursuivre. De plus, dans de nombreuses situations, le marchand a l'obligation d'établir l'authenticité d'un élément d'identité.

Pour résoudre ce problème, nous considérons que la meilleure méthode consiste à utiliser un système de vérification de l'identité et de partage des éléments d'identité. Celui-ci doit être conforme aux recommandations en matière d'identité numérique élaborées par les organismes gouvernementaux de réglementation et axées sur l'amélioration de la protection de la vie privée (NIST 800-63 aux États-Unis ou RGPD dans l'Union européenne). Ces normes exigent de différencier la vérification d'identité et l'authentification[9].

GRAFT mettra en place un profil d'identité numérique associé à l'application GRAFT Wallet. Il sera possible de partager les données de l'identité numérique avec le cocontractant de façon incrémentielle et selon les autorisations utilisateur au moment de la transaction. Ces autorisations

portent notamment sur le partage sélectif de certains éléments (comme l'âge, l'adresse et le nom), par transaction.

GRAFT met en œuvre le protocole d'enregistrement des transactions sous-jacents **CryptoNote[10]**, qui offre un niveau élevé de confidentialité par rapport au Bitcoin et aux autres cryptomonnaies et jetons cryptographiques, car il masque les informations sur l'émetteur et le destinataire.

Utilité d'une blockchain privée

La principale innovation du Bitcoin repose sur un registre ouvert accessible à n'importe quel nœud participant au réseau, car la transaction doit être validée pour s'assurer qu'il n'y a pas de double dépense. Toutefois, cela signifie également que n'importe quelle personne dans le monde peut consulter la transaction et les soldes sur les portefeuilles correspondants. Contrairement aux cartes de paiement, les portefeuilles Bitcoin sont en principe anonymes, car les enregistrements de transactions ne sont pas directement associés à l'identité de leur propriétaire. À première vue, il semble que cette fonctionnalité compense le fait que les enregistrements de transactions sont bien en vue sur la blockchain, visibles par tous. Toutefois, certaines techniques permettent aux observateurs d'associer les adresses à des identités[11]. Lorsque cette situation se produit, toutes vos transactions deviennent visibles définitivement, car la blockchain existera toujours et ne peut pas être supprimée.

CryptoNote nous est indispensable pour concurrencer les systèmes de paiement traditionnels comme le réseau Visa ou PayPal qui, en réalité, offrent à leurs clients une bien meilleure confidentialité que la plupart des cryptomonnaies existantes.

Lorsque vous insérez votre carte de paiement dans le terminal d'un point de vente ou cliquez sur le bouton "Payer" de PayPal, seules deux entités au monde sont au courant de la transaction : le réseau de paiement (Visa ou PayPal dans notre cas) et le marchand. En réalité, bien entendu, d'autres entreprises sont "au courant" de votre transaction, car le réseau de paiement est plus complexe. Cette liste inclut, au minimum, la banque émettrice (celle qui vous a fourni votre carte de paiement), la banque acquéreur (celle qui approuve le paiement), la passerelle de paiement (qui achemine votre transaction vers la banque acquéreur ou le processeur de paiement concerné) et le processeur de paiement (qui traite le paiement et l'encaissement par le marchand). Toutefois, la liste des entreprises est encore limitée, car elles doivent respecter des réglementations en matière de sécurité et de confidentialité, et elles ont généralement mis en place des contrôles de sécurité satisfaisants qui protègent vos enregistrements de transactions des regards indiscrets. Bien sûr, les entités de cette liste peuvent se faire pirater ou peuvent transmettre vos informations aux services de police. Pour

simplifier, nous partons du principe que des gens pris au hasard ne peuvent pas accéder à vos transactions par carte de paiement dans la plupart des situations, ce qui n'est pas le cas avec la plupart des blockchains.

CryptoNote : la base de la confidentialité

CryptoNote se démarque de tous les autres protocoles de blockchain, car il nous permet d'obtenir ce dont nous avons tous besoin : la confidentialité. Nous la considérons souvent comme un acquis, et nous la regrettons seulement lorsqu'elle nous est confisquée. Cela peut sembler ironique, mais le Bitcoin et ses dérivés régressent dans le domaine de la confidentialité par rapport aux systèmes de paiement plus anciens comme les espèces ou même les cartes de paiement, qui sont devenus le symbole peu glorieux de l'atteinte à la sécurité et à la confidentialité. Les créateurs du Bitcoin n'ont pas réfléchi à la confidentialité, ou ils n'ont simplement pas eu le temps de résoudre tous les problèmes qui se posaient, ce qui est parfaitement compréhensible, car ils avaient un défi encore plus important à relever : l'existence même de la technologie blockchain.

CryptoNote bénéficie de tous les avantages bien connus des technologies de blockchain tout en leur "restituant" les fonctions de confidentialité qu'elles ont perdues : **paiements non traçables**, **non-associativité des transactions**, **résistance à l'analyse de la blockchain** et **confidentialité des montants des transactions.** En outre, pour compléter le tableau, GRAFT ajoute des **montants de frais de transaction confidentiels**. CryptoNote crée une base solide et idéale pour élaborer diverses fonctionnalités liées au secteur, que GRAFT met en avant pour conquérir l'univers des paiements.

Transactions privées

GRAFT utilise plusieurs mécanismes cryptographiques conçus par CryptoNote et Monero pour masquer les enregistrements de transactions et ne les rendre visibles qu'aux propriétaires des données :

Adresses de destination "furtives" à usage unique

Au lieu d'envoyer directement le paiement à l'adresse du destinataire, une clé de destination unique ponctuelle est créée pour chaque transaction. Cette clé est générée de façon cryptographique à partir de l'adresse publique du destinataire, de telle sorte qu'il est impossible de l'associer à l'adresse ou à d'autres clés. Par conséquent, **le destinataire peut publier une adresse unique et recevoir des paiements qu'il est impossible d'associer à une transaction,** et **aucun observateur ne peut**

déterminer si des transactions ont été envoyées à une adresse spécifique ni associer deux adresses ensemble.

Signatures de cercle à usage unique

Ces signatures **masquent l'identité de l'émetteur**. Chaque transaction effectuée sur n'importe quelle blockchain est signée par la clé privée de l'émetteur, ce qui permet au réseau de confirmer l'authenticité de la transaction. Au lieu de créer une seule signature, plusieurs signatures (le "cercle") sont générées. Elles sont toutes valides, car elles représentent les sorties réelles des autres émetteurs. Toutefois, l'observateur ne peut pas déterminer qui est l'émetteur réel. Le réseau ne peut pas identifier la sortie spécifique utilisée, car elle est dissimulée parmi les autres signatures de cercle. Par contre, le réseau vérifie qu'aucune sortie de la totalité du cercle n'est dépensée plusieurs fois, ce qui permet d'éviter efficacement les doubles dépenses.

RCT (Ring Confidential Transactions)

Cette méthode **rend invisibles les montants des transactions sur la blockchain**. Le montant de la transaction est crypté par l'émetteur, et seul le destinataire du paiement peut décoder le montant réel. Les observateurs tiers ne peuvent pas décrypter ce montant, mais ils peuvent vérifier que la somme n'a pas été dépensée plusieurs fois et qu'aucune nouvelle somme n'a été créée dans le cadre de cette transaction.

Traitement des transactions

Le monde évolue vers des appareils de plus en plus fins. Dans le monde entier, les utilisateurs se tournent de plus en plus vers les smartphones et les tablettes, et délaissent les postes de travail et les ordinateurs portables. C'est pourquoi nous pensons qu'un modèle supérieur de paiements cryptographiques décentralisés ne doit pas reposer que sur des nœuds individuels de petite taille, hébergés sur des ordinateurs personnels, mais aussi sur des super-nœuds dédiés et puissants, hébergés par des professionnels, avec des applications de clients légers connectées à un échantillon d'autorisations (un groupe de super-nœuds sélectionnés de façon aléatoire par un algorithme anti-fraude spécial) via des appels DAPI.

Problème lié au délai de confirmation : lancement des autorisations en temps réel

La durée des délais de confirmation[12] (de plusieurs minutes à plusieurs heures selon les frais de transaction) constitue l'une des principales raisons pour lesquelles les secteurs du commerce de détail et de l'hôtellerie-restauration peinent à adopter les cryptomonnaies et les jetons cryptographiques. Les clients n'aiment pas attendre et, par conséquent, les marchands exigent un traitement quasi-instantané des paiements. Contrairement aux autres réseaux de cryptomonnaies qui ont essayé de résoudre le problème en introduisant des systèmes complémentaires ou des types de transactions spécifiques, GRAFT traitera toutes les transactions de paiement en "temps réel" (nous prévoyons que la plupart des transactions seront exécutées en moins de trois secondes). Il faut souligner que GRAFT parvient à réaliser ce paiement en temps réel sans facturer de frais supplémentaires au client.

Pour ce faire, GRAFT utilise un consensus de super-nœuds actifs en permanence ("échantillon d'autorisations"), capable d'effectuer une mise en attente d'autorisation instantanée et distribuée sur le compte de l'acheteur, et de communiquer la réponse au client, généralement en quelques millisecondes. De plus, les super-nœuds surveillent la blockchain GRAFT pour qu'aucune transaction ne puisse être autorisée "hors chaîne".

Super-nœuds

Toutes les transactions sont traitées en temps réel par le réseau de nœuds du réseau GRAFT (super-nœuds). Des frais de transaction sont payés par le destinataire (marchand) aux super-nœuds qui font partie de l'échantillon d'autorisations et (éventuellement) aux courtiers participant au traitement de la transaction. Les propriétaires des super-nœuds sont responsables de toutes les transactions qu'ils traitent. Cette responsabilité est liée à un intérêt financier (frais de transaction).

DAPI

Contrairement aux API habituelles, qui sont hébergées sur un serveur ou dans une ferme de serveurs, la DAPI ne dispose pas d'une adresse unique, car elle est exécutée sur plusieurs super-nœuds. Chaque nœud peut répondre à l'appel DAPI à tout moment. Les appels DAPI sont "sans état". En d'autres termes, les super-nœuds ne maintiennent pas de session permanente avec le client, et toutes les données nécessaires au traitement sont instantanément distribuées et disponibles sur tous les nœuds. L'application cliente, qui consomme la DAPI, établit une liste des super-nœuds proxy avec lesquels elle communique. Toutefois, l'application cliente est libre de sélectionner un super-nœud spécifique en qui elle a confiance et d'y rester "fidèle". Par exemple, les utilisateurs d'un portefeuille ou

d'un point de vente marchand peuvent décider d'héberger leur propre super-nœud proxy, auquel ils font confiance. Même si un tel super-nœud "privé" peut ne pas être autorisé à participer à l'échantillon d'autorisations en raison de ressources limitées (cf. la section "Algorithme de sélection de l'échantillon d'autorisations" ci-dessous), il peut fournir une couche de confidentialité supplémentaire à leurs propriétaires.

Validations en temps réel par un échantillon d'autorisations

Avec certaines cryptomonnaies, l'intervalle entre les blocs (règlements) est inférieur à 2 minutes. Toutefois, la réduction de cet intervalle ne permet pas d'exécuter ces transactions en "temps réel". Pour résoudre ce problème, le système de super-nœuds GRAFT utilise des échantillons d'autorisations lorsque les validations sont émises en temps réel par le groupe de super-nœuds sélectionné. Selon nous, cette structure garantit que l'acheteur ne peut pas dépenser le même montant plusieurs fois tant que la transaction n'est pas validée (écrite dans la blockchain). La validation (ou le minage) nécessite généralement plusieurs minutes.

Contrairement à la plupart des systèmes de paiement cryptographique, chaque paiement effectué sur le réseau GRAFT est divisé en deux phases : l'autorisation et la validation. Comme dans l'univers du paiement traditionnel, l'autorisation se produit en temps réel, tandis que la validation est effectuée plus tard, généralement dans un délai de deux minutes (contre plusieurs heures, voire plusieurs jours, avec les réseaux de paiement traditionnels).

Verrouillage du compte d'autorisation

Une "image clé" correspond au mécanisme utilisé par CryptoNote pour valider les nouvelles transactions et empêcher les doubles dépenses sans compromettre la confidentialité de l'émetteur. L'image clé est une "empreinte" unique qui représente l'adresse et le montant de la dépense sans divulguer aucun détail sur l'acheteur ni le montant. Par nature, une image clé ne peut être utilisée qu'une seule fois. Par conséquent, si une personne essaie d'utiliser plusieurs fois la même image clé, cela indique une tentative de double dépense. Le portefeuille de l'acheteur fournit l'image clé unique de la transaction à venir au réseau de super-nœuds. Ainsi, il verrouille temporairement son compte de dépense, et aucune autre transaction associée à la même image clé (c'est-à-dire issue du même compte) ne peut se produire tant que la transaction verrouillée n'a pas été validée ou que le verrouillage n'a pas été supprimé. Si l'acheteur essaie de finaliser la transaction avec une image clé différente de celle utilisée dans le cadre du verrouillage initial, la transaction est également refusée par les super-nœuds.

Par ailleurs, l'image clé ne contient aucune information sur l'acheteur ni sur son portefeuille, ce qui garantit la sécurité, l'anonymat et l'intraçabilité de l'opération. En outre, toute trace de communication entre l'acheteur (application portefeuille), le marchand (application point de vente) et les super-nœuds (super-nœuds de relais ou d'échantillon sélectionnés) pendant la phase d'autorisation est supprimée une fois la transaction validée (écrite dans la blockchain et confirmée par 10 blocs).

Niveaux d'un super-nœud

Un nœud GRAFT est appelé "super-nœud", car il exécute plus de fonctions que les nœuds traditionnels des réseaux de blockchain. Les propriétaires de super-nœuds doivent répondre à des exigences plus nombreuses. GRAFT est un réseau ouvert et décentralisé permettant à n'importe qui d'exécuter un super-nœud, mais il existe différents niveaux de super-nœud, chacun d'entre eux étant associé à différentes conditions et récompenses.

Le **super-nœud proxy** correspond au "niveau d'entrée" : n'importe qui peut installer le logiciel de super-nœud et héberger le super-nœud proxy, qui remplit les fonctions suivantes :

- Relais de confiance pour les personnes qui ont les exigences les plus élevées en termes de confidentialité, pour qu'ils puissent héberger leur propre "serveur de portefeuille"
- "Serveur de magasin" pour les marchands de grande taille, ce qui permet un traitement des transactions encore plus fiable et plus rapide
- "Nœud de sortie" public reliant les points de vente et les portefeuilles mobiles au réseau GRAFT (IP publique requise). Le super-nœud proxy public peut obtenir des récompenses s'il possède une caution.

Le **super-nœud complet** est à la fois validateur et fournisseur de services. De plus, l'exécution des fonctions d'un super-nœud complet nécessite une caution (solde de caution associé à l'adresse du super-nœud). Les frais de service et de transaction sont versés à un super-nœud complet qui possède une caution et émet des validations en temps réel.

Nœuds de minage

Pendant que la deuxième couche du réseau GRAFT, composée de nœuds "point de vente", exécute les fonctions d'autorisation et d'échange, la première couche, composée de nœuds de réseau "preuve de travail" (PoW, *Proof of Work*), exécute la fonction de validation en générant de nouveaux blocs et en les ajoutant à la blockchain.

Récompenses pour validation (minage)

Les nœuds de minage obtiennent des récompenses pour le minage de blocs PoW, mais ils perçoivent aussi des honoraires de "validation" pour les transferts standards et les transactions RTA.

Récompense pour validation (transaction RTA) : variable

Déterminée par le fournisseur de services de paiement via la passerelle de paiement (elle doit être supérieure à 0,1 GRFT).

Frais de transaction versés au mineur (transfert non RTA) : variable

Variable (dépend de la taille de la transaction en Ko)

Récompense pour minage de blocs (Coinbase)

La récompense pour minage de blocs est versée au nœud de minage qui résout le nouveau bloc. Elle diminue progressivement pour chaque nouveau bloc, selon la formule suivante : $(M - A) \times 2^{-19} \times 10^{-10} / 2$, où A = offre en circulation et M = offre totale $(2^{64} - 1)$ en unités atomiques (10^{-10}). L'idée est la suivante : à l'avenir, il y a aura de plus en plus de transactions, ce qui permettra aux mineurs de s'assurer des revenus durables grâce aux frais de transaction.

Niveaux d'un super-nœud complet

GRAFT implémente un modèle de caution à quatre niveaux, dans lequel un niveau plus élevé a plus de chances d'être sélectionné dans l'échantillon d'autorisations, même si le processus de sélection est aléatoire.

50 000 GRFT – Niveau 1
90 000 GRFT – Niveau 2
150 000 GRFT – Niveau 3
250 000 GRFT – Niveau 4

Chaque niveau participe à une sélection aléatoire de deux super-nœuds d'échantillon (où N correspond au numéro de niveau). Ainsi, naturellement, un super-nœud de niveau 4 a plus de chances d'être sélectionné en raison du nombre limité de super-nœuds de ce type. Les emplacements "vides" sont remplis par les niveaux supérieurs (ou inférieurs s'il n'y en a pas). Cet algorithme est également adaptatif, car il "régule" le nombre moyen de super-nœuds complets à chaque niveau.

Caution déléguée

Les soldes de plusieurs portefeuilles peuvent être "délégués" à un seul super-nœud complet afin de constituer une caution suffisamment importante pour exécuter un super-nœud complet. Les revenus sont répartis entre les portefeuilles en fonction de la part de la caution. Le solde minimum d'une caution déléguée est de 5 000 GRFT.

Échantillon d'autorisations

Pour effectuer des autorisations en temps réel, le réseau GRAFT s'appuie sur l'échantillon d'autorisations : il s'agit d'un groupe de super-nœuds de confiance sélectionnés, qui "représenteront" le réseau et valideront les transactions, en évitant les doubles dépenses et en signant la validation instantanée avant que la transaction ne soit "confirmée" sur la blockchain GRAFT (c'est-à-dire, avant qu'elle ne soit ajoutée au bloc et que celui-ci ne soit ajouté à la blockchain).

L'échantillon d'autorisations est composé de huit super-nœuds sélectionnés de façon aléatoire à partir d'une liste dynamique de super-nœuds. La sélection est aléatoire, mais le résultat est déterministe pour toute personne qui calcule la formule. Le propriétaire du super-nœud doit conserver un solde de caution dans un portefeuille associé au super-nœud. Le solde minimum requis démarre à 50 000 GRFT.

Lorsque le point de vente du marchand lance une nouvelle demande de transaction, celle-ci se voit attribuer la hauteur de bloc actuelle qui définit l'échantillon d'autorisations. Cette hauteur peut être incrémentée au cours de la transaction, mais elle n'a pas d'impact sur la hauteur d'échantillon attribuée initialement à la demande de transaction. Le super-nœud proxy du marchand qui formule initialement la demande de transaction sélectionne les super-nœuds de l'échantillon, mais cette sélection est validée par chaque membre de l'échantillon et par le super-nœud proxy du portefeuille.

Afin d'accélérer le processus d'autorisation, l'application de point de vente du marchand peut donner l'ordre aux super-nœuds de l'échantillon d'autorisations d'ignorer les réponses du reste de cet échantillon dès qu'elle reçoit plus de 50 % des réponses approuvées en provenance des super-nœuds "les plus rapides" et aucune réponse refusée.

Super-nœuds proxy

N'importe quel nœud de l'échantillon d'autorisations peut aussi être un super-nœud proxy. Il s'agit du relais qui facilite la transaction du marchand en communiquant avec le point de vente du marchand

et/ou le portefeuille de l'acheteur d'une part, et avec le reste des super-nœuds de l'échantillon d'autorisations d'autre part. Le super-nœud proxy peut être sélectionné de façon aléatoire par le point de vente ou le portefeuille à partir de l'échantillon d'autorisations actuel associé à la transaction. Le point de vente ou le portefeuille peuvent aussi sélectionner un super-nœud qui ne fait pas partie de l'échantillon d'autorisations. Ainsi, un point de vente ou un portefeuille peuvent héberger leurs propres super-nœuds proxy s'ils souhaitent bénéficier d'une couche supplémentaire de sécurité et de confidentialité. Le super-nœud proxy peut obtenir des récompenses s'il possède une caution.

Récompenses des super-nœuds

Chaque super-nœud reçoit une part des frais de transaction pour chaque transaction qu'il traite. Les récompenses sont payées par le destinataire (marchand).

Récompense d'un super-nœud complet pour toute transaction RTA : 0,5 %

Un huitième de ces frais (soit 0,0625 % du montant total de la transaction RTA) sont versés à chaque super-nœud complet participant à l'échantillon d'autorisations RTA.

Récompense d'un super-nœud proxy pour toute transaction RTA : 0,1 %

La moitié de ces frais (soit 0,05 % du montant total de la transaction RTA) est versée à chaque super-nœud de la paire de super-nœuds proxy qui fournit la connectivité dans le réseau (super-nœuds proxy du point de vente et du portefeuille).

Récompense du super-nœud proxy du portefeuille (transfert non RTA) : 0,1 GRFT

Ces frais sont facturés par le super-nœud proxy du portefeuille au portefeuille de l'émetteur (sur mobile ou ordinateur), en plus des frais de réseau existants (récompense du mineur).

Évolutivité

L'évolutivité d'un réseau de paiement donné désigne sa capacité à traiter simultanément un grand nombre de transactions sans dégrader les performances. Pour optimiser son évolutivité, le réseau GRAFT prend certaines mesures. Par exemple, il définit la fréquence de création de blocs sur deux minutes et supprime la limitation de la taille des blocs. Cela permet de créer des blocs de transactions plus souvent, et chaque bloc peut contenir davantage de transactions. Ce type de mesure n'est pas unique, et d'autres cryptomonnaies et jetons cryptographiques adoptent des approches similaires. Toutefois, GRAFT est géré par des super-nœuds ultra-performants et toujours actifs, qui valident et autorisent les transactions en temps réel. Par conséquent, chaque super-nœud dispose non seulement de la copie la plus récente de la blockchain complète, mais conserve également la liste de

toutes les demandes d'autorisation en attente et des transactions finalisées jusqu'à ce qu'elles soient ajoutées à la blockchain. Cette architecture à deux niveaux permet d'absorber les fortes augmentations de demandes associées (par exemple, les impacts liés à la saison ou à des événements, ou d'autres changements concernant les activités des acheteurs et des marchands).

Validation des transactions hors ligne

Si vous connaissez le processus de paiements par carte, vous savez qu'une transaction peut parfois être approuvée par un marchand sans validation simultanée par la banque. C'est ce qu'on appelle une approbation (ou autorisation) hors ligne ou locale (ou parfois en mode différé), car une telle autorisation est transmise au serveur une fois la connexion au réseau rétablie.

Toutefois, dans le cas des paiements cryptographiques, nous partons généralement du principe que le réseau est disponible 24h/24 et 7j/7, et qu'il n'y a jamais de temps d'arrêt. Mais cette hypothèse n'est pas toujours vraie. Dans certaines situations, les marchands prennent un risque et approuvent des transactions localement, car le risque d'un seul rejet de débit est inférieur à celui de perdre plusieurs clients. En général, un montant limite total est défini pour les autorisations locales. Lorsque le système atteint cette limite (le risque maximal), il arrête d'émettre des approbations locales jusqu'à ce que le réseau soit rétabli. Toutefois, en cas de brève interruption, l'autorisation locale peut passer inaperçue, aussi bien auprès du caissier que de l'acheteur.

L'application point de vente du marchand fournie par GRAFT et le super-nœud proxy seront en mesure de traiter des transactions cryptographiques hors ligne basées sur le même principe s'ils ne peuvent pas communiquer avec l'échantillon d'autorisations ni obtenir un consensus, et si le marchand est prêt à prendre un tel risque. La décision concernant l'approbation hors ligne sera également basée sur les scores de réputation de l'acheteur et du super-nœud.

Passerelles de paiement pour les marchands et les fournisseurs de services

Le fournisseur de services de paiement (MSP, *Merchant Service Provider*) est l'un des principaux acteurs de l'écosystème GRAFT. Le MSP a pour mission de fournir des services de réseau de paiement aux marchands et d'assister ces derniers, d'assurer la disponibilité du réseau (on parle généralement de contrat de niveau de service ou de SLA, pour *Service Level Agreement*), de fournir et de gérer l'équipement (les terminaux de paiement, par exemple) et de fournir des rapports.

Pour permettre au MSP de remplir cette mission, celui-ci doit disposer d'un autre type de serveur qui effectuera les tâches suivantes :

- Gérer la configuration du terminal (y compris l'adresse du portefeuille)
- Traiter l'aspect économique des commissions propre aux MSP (un MSP peut choisir de gérer les niveaux de service différemment ou de facturer des frais différents selon le montant de la transaction)
- Fournir aux marchands des rapports et des analyses sur les transactions

Une telle passerelle de paiement peut être conçue et mise en œuvre par un tiers (par exemple, un processeur de paiement traditionnel qui souhaite ajouter les paiements en cryptomonnaies à sa gamme de services). GRAFT crée une "implémentation de référence" afin d'accroître rapidement le taux d'adoption dans le cadre de sa stratégie d'introduction sur le marché.

GRAFT étant un réseau de paiement décentralisé, la passerelle de paiement est une application Open Source multi-tenant et multi-instance, et n'importe qui peut héberger sa propre passerelle de paiement et devenir fournisseur de services sur le réseau. La passerelle de paiement correspond à ce "cinquième" élément censé gérer les applications de paiement GRAFT sur les terminaux de paiement matériels et les interfaces d'e-commerce GRAFT, et les associer aux super-nœuds GRAFT. Comme elle bénéficie de la visibilité des transactions, elle est considérée comme une application "back-office" du marchand.

Types de transaction et processus de paiement

GRAFT a mis au point les processus et types de transaction suivants afin de faciliter les transactions des marchands, et de faciliter l'utilisation des applications de paiement et de point de vente actuelles.

Autorisation

La transaction "Autorisation" est utilisée lorsque le montant final exact de la transaction n'est pas connu au moment du déclenchement de la vente. Exemples : prépaiement à la pompe dans une station-service, remise des clés d'un véhicule de location, réservation d'une chambre ou enregistrement à l'hôtel, "paiement à table" dans un restaurant.

Ce type de transaction est semblable à une autorisation de carte de crédit : l'autorisation est initiée par le marchand et confirmée par le payeur. Le compte du payeur est temporairement verrouillé pour le

montant et la durée (nombre de blocs) demandés par le bénéficiaire et confirmés par le payeur, ou jusqu'à ce que le montant soit confirmé par une transaction "Validation" ultérieure. Le verrouillage d'autorisation peut aussi être désactivé par une transaction "Annulation" émise par le bénéficiaire avant la date/l'heure d'expiration. Les fonds sont automatiquement restitués au payeur par le réseau après la date/l'heure d'expiration si le bénéficiaire ne les a pas réclamés en envoyant une transaction "Validation".

Pré-autorisation

Ce type de transaction est semblable à la transaction "Autorisation" à long terme, à une différence près : le payeur ne garantit pas que les fonds seront disponibles à la fin de l'opération. "Pré-autorisation" est un contrat à long terme entre le payeur et le bénéficiaire. Toutefois, contrairement à la transaction "Autorisation" (que le bénéficiaire ne peut pas annuler), la transaction "Pré-autorisation" peut être annulée à tout moment en transférant les fonds depuis le compte associé à la transaction pré-autorisée.

La transaction "Pré-autorisation" est adaptée aux dispositifs de paiement à long terme (par exemple, un abonnement mensuel à un service ou la facturation quotidienne d'une chambre d'hôtel). Le bénéficiaire indique (et le payeur confirme) le montant maximal d'un débit, le nombre total de débits et l'intervalle minimum entre deux débits.

Validation

La transaction "Validation" finalise le paiement initié par les transactions "Autorisation" ou "Pré-autorisation". Son montant réel peut être inférieur au montant préalablement autorisé. Plusieurs transactions "Validation" peuvent avoir lieu, mais le montant total ne dépassera jamais le montant de la transaction "Autorisation".

La transaction "Validation" est utilisée une fois qu'une transaction préalablement autorisée est finalisée et que le montant exact est connu (par exemple, lors du paiement à la pompe une fois le plein effectué, lors de la restitution d'une voiture de location, lors du départ de l'hôtel ou lors du paiement de l'addition au restaurant après avoir ajouté le pourboire).

Vente

La transaction "Vente" correspond au traitement séquentiel et automatique de la transaction "Autorisation/Validation" par le réseau, sous la forme d'une seule transaction. Il s'agit d'une transaction marchande classique dans une boutique en ligne ou un magasin physique.

Transfert

La transaction "Transfert" permet de transférer de l'argent entre des comptes GRAFT. C'est la même transaction que "Vente", mais elle est initiée par l'émetteur, sans autorisation du destinataire. Elle peut être utilisée pour les paiements en peer-to-peer, les échanges et les transferts entre comptes.

Annulation

La transaction "Annulation" permet d'annuler la transaction "Autorisation" et de débloquer les fonds autorisés (en d'autres termes, de déverrouiller le compte).

Émission

La transaction "Émission" active une carte prépayée, un chèque-cadeau, des points de fidélité, un avoir en magasin ou un bon de réduction GRAFT.

Utilisation

La transaction "Utilisation" permet d'effectuer un paiement via une carte prépayée, un chèque-cadeau, des points de fidélité, un avoir en magasin ou un bon de réduction préalablement émis par GRAFT.

Échange

La transaction "Échange" permet d'échanger des fonds entre des jetons GRAFT et d'autres cryptomonnaies, jetons cryptographiques et monnaies fiduciaires locales de premier plan, en profitant de la meilleure offre des super-nœuds.

Planification

La transaction "Planification" permet de programmer une transaction pour qu'elle s'exécute à une heure ou une date ultérieure. Cette opération nécessite une confirmation supplémentaire de l'utilisateur.

Dépôt de garantie

La transaction "**Dépôt de garantie"** permet de déposer les fonds en garantie, en associant un déclencheur d'événement à activer lorsque les fonds seront débloqués.

Remboursement

La transaction "Remboursement" renvoie les fonds désignés par la clé de transaction. Elle nécessite une autorisation de retour de marchandise (RMA, *Return Merchandise Authorization*) de la part du vendeur.

Traitement de transactions en utilisant des jetons GRFT comme mode de paiement

Contrairement au Bitcoin et aux autres cryptomonnaies et jetons cryptographiques, et comme pour les cartes de paiement, les demandes de transaction de paiement sont mises en forme et émises par le destinataire (marchand). Il existe une seule exception : les transactions "Transfert" et "Échange" sont initiées par l'émetteur (toute personne qui souhaite déplacer des fonds entre deux comptes GRAFT). Toutefois, contrairement aux cartes de crédit et de débit, les demandes de paiement sont explicitement confirmées par l'acheteur, sur la demande de l'application GRAFT Wallet, avant que celle-ci ne signe numériquement la transaction et ne l'envoie au réseau. La seule exception concerne la fonction "Utiliser" en cas d'utilisation d'une carte-cadeau imprimée ou plastique ou d'un bon de réduction qui peut être scanné par l'application de paiement du marchand, si le client ne souhaite pas utiliser l'application mobile ou s'il ne dispose pas d'un compte GRAFT.

Traitement des transactions via d'autres modes de paiement

Afin d'offrir une expérience utilisateur optimale aux acheteurs et de meilleurs taux de conversion aux marchands, une transaction de paiement GRAFT peut accepter comme source différents jetons cryptographiques, cryptomonnaies ou devises fiduciaires locales compatibles (sous la forme d'une carte de débit/crédit), via l'application GRAFT Wallet de l'acheteur. Des frais de change, des frais bancaires et des frais de traitement des cartes de crédit/débit (facturés au marchand en graftcoins) peuvent s'appliquer en conséquence, en plus des frais de transaction GRAFT standards. Nous prévoyons que ces frais seront supportés par le bénéficiaire du paiement et qu'ils seront transparents pour le payeur, car le mode de paiement n'aura pas d'incidence sur le prix de vente. Le processus de conversion instantané automatique de GRAFT favorisera l'adoption des paiements cryptographiques par les utilisateurs standards qui ne maîtrisent pas suffisamment les écosystèmes des cryptomonnaies et des jetons cryptographiques et qui préfèrent encore les modes de paiement traditionnels, mais qui recherchent une meilleure sécurité et confidentialité, et un anonymat complet, pour leurs transactions.

Si un acheteur décide de payer avec une autre cryptomonnaie, des jetons cryptographiques ou une carte de crédit/débit, le réseau GRAFT échange automatiquement la cryptomonnaie ou les jetons cryptographiques, ou convertit le paiement par carte de crédit (effectué en monnaie fiduciaire locale) en GRFT (en temps réel) dans le cadre du processus de transaction, par le biais de courtiers. Les courtiers, qui utilisent des super-nœuds GRAFT, sont chargés d'exécuter les opérations de change, de facturer les acheteurs et d'effectuer les paiements auprès des marchands. Si l'acheteur choisit une autre cryptomonnaie, des jetons cryptographiques ou une carte de crédit/débit comme mode de paiement, l'échantillon du super-nœud sélectionne automatiquement la meilleure offre parmi tous les courtiers, en tenant compte d'une part des choix précédents du marchand, et d'autre part d'une combinaison du meilleur taux de change et du score de réputation le plus élevé.

Courtiers

Si un client paie en jetons GRAFT et que le marchand veut être payé en jetons GRAFT, les fonds sont automatiquement et instantanément débités du compte de l'acheteur et déposés sur le compte du marchand par le réseau GRAFT. En revanche, si le client souhaite payer via un autre mode de paiement et/ou que le marchand veut être payé dans une autre devise, le réseau GRAFT doit utiliser un mécanisme spécial.

Afin de faciliter les éléments de traitement du paiement qui ne peuvent pas être décentralisés, mais qui sont encore très demandés par les consommateurs et les marchands, le réseau GRAFT fait intervenir un courtier. Lorsque le réseau GRAFT ne peut pas procéder lui-même au traitement d'une opération spécifique de façon totalement décentralisée, il délègue cette opération au réseau de courtiers. Les marchands peuvent choisir un seul courtier (par exemple, le moins cher ou celui en qui ils ont le plus confiance) ou un groupe de courtiers.

Le courtier est chargé d'assurer la sécurité et le respect des réglementations relatives au traitement des cartes de paiement et des opérations de change, y compris la conformité à la norme PCI DSS et à la législation sur la lutte contre le blanchiment d'argent[13].

Voici les différents types de courtiers :

Courtiers côté marchand/point de vente :

- Agent de paiement (*pay-in broker*)
- Agent d'encaissement (*payout broker*)

Courtiers côté acheteur/portefeuille :

- Courtier d'échange (*interchange broker*)
- Courtier de rechargement (*top-up broker*)

Un ensemble de courtiers en cryptomonnaies sera disponible pour chaque grande cryptomonnaie répertoriée sur https://coinmarketcap.com/, à commencer par les premières du "Top 10" par capitalisation de marché. Les courtiers stimuleront la liquidité en activant différentes options de paiement, aussi bien du côté acheteur que du côté marchand de la transaction.

Les courtiers en cryptomonnaie seront mis en place en collaboration avec des plateformes d'échange nouvelles et/ou existantes. À terme, plusieurs choix seront proposés pour chaque cryptomonnaie, et les courtiers pourront donc se faire concurrence pour proposer les meilleurs services et tarifs. La nature décentralisée du réseau sera préservée grâce à la variété des services, et à l'automatisation des processus d'inscription, de sélection et d'exécution. Chaque ensemble inclut quatre courtiers mis en place pour chaque cryptomonnaie.

Les agents de paiement et d'encaissement utilisent l'application GRAFT POS et les terminaux de paiement physiques pour permettre au marchand d'accepter la cryptomonnaie sélectionnée comme mode de paiement, tout en exécutant les transactions de paiement avec l'application GRAFT Wallet ou d'autres portefeuilles de cryptomonnaie.

Les courtiers d'échange et de rechargement utilisent les applications GRAFT Wallet pour permettre à l'acheteur d'utiliser la cryptomonnaie sélectionnée comme mode de paiement lorsqu'il effectue un paiement auprès de l'application GRAFT POS, d'une application de portefeuille native, d'une application POS non GRAFT intégrée avec la DAPI GRAFT ou d'une application POS non GRAFT qui accepte la cryptomonnaie sélectionnée.

Agent de paiement

L'agent de paiement permet d'accepter des modes de paiement différents des jetons GRFT natifs. Il convertit immédiatement le montant du paiement en jetons GRFT et les dépose sur le compte du marchand. L'agent de paiement agit en temps réel et prend part à la transaction entre l'acheteur et le marchand. Du point de vue de l'acheteur, la transaction paraît semblable à une transaction standard entre des portefeuilles de cryptomonnaie natifs.

L'agent de paiement utilise l'application GRAFT POS pour faciliter l'acceptation de la cryptomonnaie sélectionnée comme mode de paiement lorsque l'acheteur ne dispose pas d'un portefeuille GRAFT. Les frais de transaction (dans la cryptomonnaie sélectionnée) sont toujours payés par l'acheteur, sauf si ce dernier utilise l'application GRAFT Wallet. Dans ce cas, le portefeuille reconnaît l'application GRAFT POS et convertit automatiquement la transaction de paiement en une transaction instantanée en GRFT.

Le paiement en faveur du marchand est traité instantanément en GRFT par l'agent de paiement (si l'agent d'encaissement correspondant est activé, le paiement peut être effectué dans une autre cryptomonnaie ou en monnaie fiduciaire).

Exemples d'agent de paiement :

- Agent de paiement en Bitcoins
- Agent de paiement en Ethers
- Agent de paiement par carte de crédit

Aspects techniques et économiques des agents de paiement et d'encaissement

L'agent de paiement prend un certain risque en acceptant la cryptomonnaie du paiement tout en débloquant rapidement les GRFT en échange (sans attendre la validation de la transaction dans la cryptomonnaie choisie). Ce risque est atténué par les montants relativement peu élevés (ou moins élevés) des transactions de vente au détail, et il est soumis à l'échantillon d'autorisations qui valide la transaction via le réseau d'origine de la devise. Le risque pour le marchand est atténué par une transaction de garantie GRFT (dont le montant est égal à celui du paiement entrant) qui est générée par le courtier au début de la transaction. Cette garantie est mise en attente par l'échantillon d'autorisations jusqu'à ce que l'agent de paiement approuve le paiement en altcoins au bénéfice du marchand. Dès que la transaction en altcoins (de l'acheteur à l'agent de paiement) a été reçue et validée, l'échantillon d'autorisations approuve le paiement à destination du marchand et débloque le paiement en GRFT (de l'agent de paiement au marchand). L'agent de paiement a la possibilité de définir différentes limites pour divers montants/niveaux de risque et d'historique.

En échange de ce service, l'agent de paiement déduit des frais de change de 0,25 % du paiement GRFT destiné au marchand, tandis que les super-nœuds participant à l'échantillon d'autorisations facturent leurs frais de transaction GRFT standards (0,5 %).

Le diagramme de séquence (ou organigramme) ci-dessous illustre la façon dont l'agent de paiement

acceptant le Bitcoin effectue l'opération de change et accepte le paiement en Bitcoins pour le compte du point de vente du marchand. L'acheteur peut utiliser n'importe quel portefeuille acceptant les Bitcoins. Le marchand reçoit le paiement en GRFT.

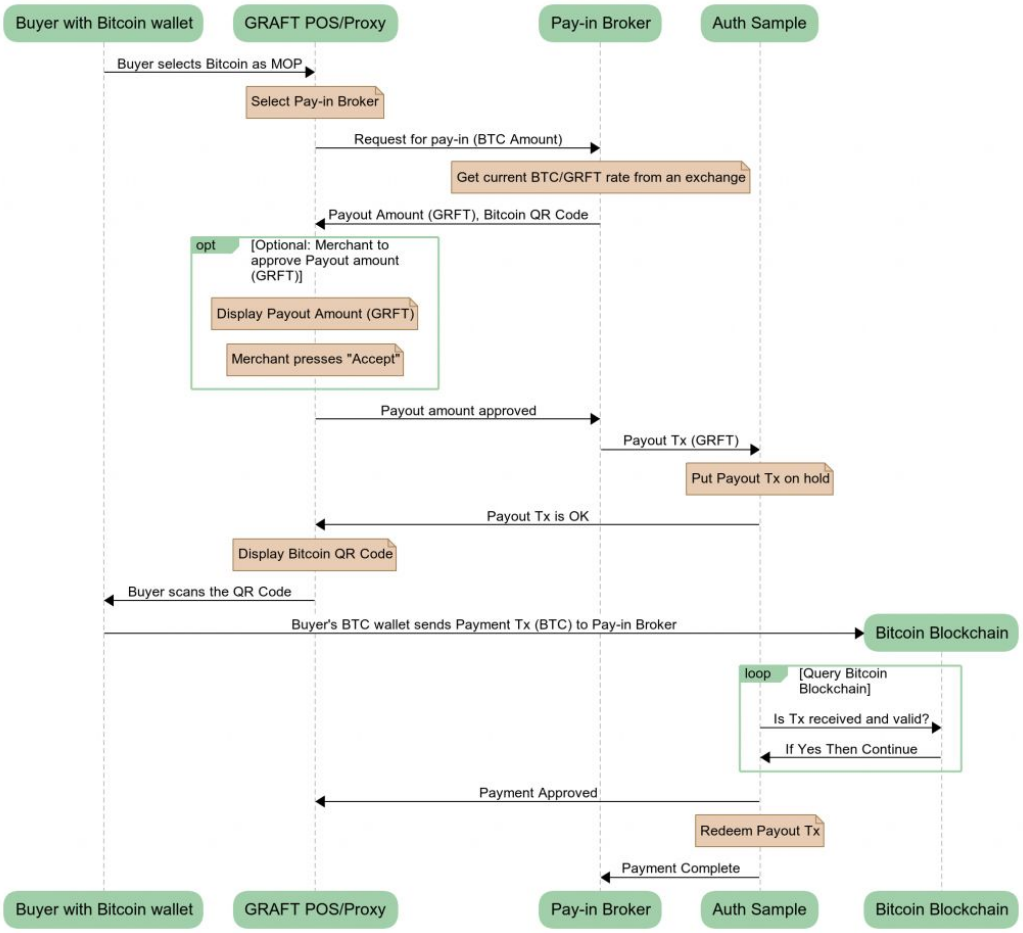

Figure 5 : Processus d'une transaction via un agent de paiement Bitcoin/GRAFT

L'agent d'encaissement convertit les GRFT dans la monnaie de paiement choisie par le marchand. La transaction est asymétrique. En d'autres termes, la validation de la deuxième étape du paiement est généralement plus longue (parfois beaucoup plus longue) côté destinataire. Pour s'assurer que l'agent d'encaissement effectue le paiement sans double dépense, il doit déposer une garantie dont le montant est égal à celui de la transaction. Pour permettre ce dépôt de garantie, l'échantillon d'autorisations met en attente le paiement GRFT émis par le marchand. Si l'échantillon d'autorisations constate (après le délai de grâce) que le marchand n'a pas reçu les fonds du paiement, il annule la transaction, et l'agent d'encaissement ne reçoit pas le paiement GRFT en provenance du marchand.

En échange de ce service, l'agent d'encaissement perçoit des frais de change de 0,25 %. En outre, les super-nœuds de l'échantillon d'autorisations facturent leurs frais de transaction standards (0,5 %).

Agents de paiement/d'encaissement

Un même courtier peut alterner (et sera très probablement amené à le faire) entre le rôle d'agent de paiement et d'agent d'encaissement. Prenons l'exemple d'un courtier de Bitcoin qui souhaite réaliser des opérations de change en paiement et en encaissement.

Il dispose d'un portefeuille Bitcoin contenant 0,01 BTC. Le courtier reçoit une demande de paiement d'un marchand consistant à convertir 100 GRFT en 0,01 BTC (en partant du principe que le taux de change actuel est le suivant : 0,01 BTC = 100 GRFT). Le processus de cette transaction entre le courtier et le marchand est illustré dans le schéma ci-dessous.

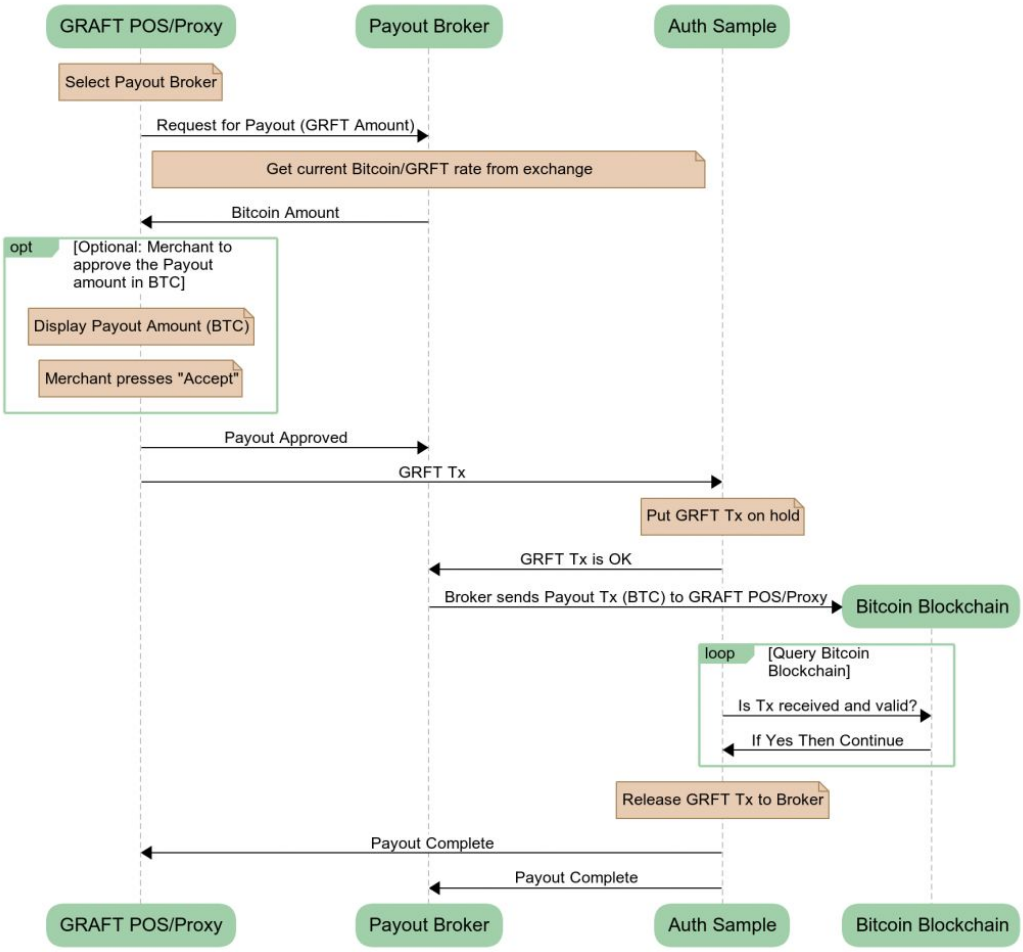

Figure 6 : Processus d'une transaction via un agent d'encaissement Bitcoin/GRAFT

Le courtier accepte la demande et envoie 0,01 BTC (moins les frais de réseau Bitcoin) au marchand, tandis que le marchand génère le paiement de 100,75 GRFT (montant de 100 GRFT + commission de courtage de 0,25 GRFT + commission de l'échantillon d'autorisations de 0,5 GRFT) à destination du courtier et le transmet à l'échantillon d'autorisations. L'échantillon met en attente la transaction de 100,75 GRFT et envoie une notification au courtier, qui envoie alors 0,01 BTC au marchand. Dès la validation de la transaction BTC (après 10 à 60 minutes, de façon purement hypothétique et en fonction des frais de réseau Bitcoin), la transaction de 100 GRFT est déclenchée et le courtier dispose maintenant du paiement de 100 GRFT auquel s'ajoute le bénéfice de 0,25 GRFT.

Il peut alors prendre le rôle d'agent de paiement. À ce titre, il reçoit la demande consistant à convertir 0,01 Bitcoin en 100 GRFT. Le courtier accepte cette demande et transfère 100 GRFT (moins les frais). Dès la réception du paiement de 0,01 BTC, le courtier peut de nouveau tenir le rôle d'agent d'encaissement, et il dispose désormais de 0,01 BTC avec la réalisation d'un bénéfice de 0,25 GRFT.

En partant du principe (de manière prudente) qu'un seul cycle de paiement/encaissement prend 1 heure, le courtier peut percevoir environ 12 % de commissions en 24 heures (sans capitalisation des intérêts), ce qui en fait un modèle économique lucratif pour le courtier* (*il ne s'agit que d'une estimation).

Au-delà des paiements aux marchands : la plateforme d'échange décentralisée (DEX)

Le système de courtier décrit ci-dessus peut fonctionner au-delà de l'écosystème de paiement prévu par GRAFT et s'intégrer dans une plateforme d'échange décentralisée (ou DEX, *Decentralized Exchange*) en temps réel. Sachant que les opérations de change non approuvées ("swaps atomiques") sont proches du temps réel pour l'entité externe qui exploite la couche d'autorisation/de validation GRAFT (réseau de super-nœuds GRAFT), ces mêmes swaps atomiques peuvent être développés pour permettre des opérations de change en temps réel (par exemple, BTC<->ETH).

Courtier d'échange

Le courtier d'échange utilise l'application GRAFT Wallet pour faciliter le paiement à destination d'un portefeuille de cryptomonnaie natif ou d'un point de vente non GRAFT acceptant la cryptomonnaie. Le courtier d'échange crée une transaction de cryptomonnaie standard au format natif pour le réseau concerné et l'envoie à l'adresse native du destinataire. Dans une telle situation, les frais de transaction réseau sont facturés à l'émetteur, car la transaction n'est pas entièrement exécutée par le réseau GRAFT. Le traitement du paiement n'est pas instantané, car le destinataire ne participe pas au réseau

GRAFT. Ce scénario est moins avantageux qu'une transaction GRFT, tant pour l'acheteur que pour le marchand, car la transaction est moins rapide et l'acheteur doit payer des frais de transaction. Toutefois, elle est acceptée par GRAFT pour faire en sorte que le portefeuille de l'acheteur reste flexible et utile même en dehors de l'écosystème GRAFT.

Le courtier d'échange convertit instantanément le montant de GRFT nécessaire à partir du compte de l'acheteur dans la cryptomonnaie sélectionnée. L'acheteur verse une petite commission de change au courtier d'échange, qui peut être payée selon un taux de change.

Exemples de courtier d'échange :

- Courtier d'échange Bitcoin
- Courtier d'échange Ether

Agent d'encaissement

L'agent d'encaissement permet d'effectuer des retraits depuis un compte marchand GRAFT en Bitcoins, en altcoins ou en monnaie fiduciaire locale. L'encaissement peut être effectué manuellement ou automatiquement.

Les frais de paiement/taux de change applicables aux encaissements traités par un agent de paiement ou d'encaissement peuvent varier selon la fréquence de l'encaissement. En fonction du volume de transactions, le coût d'un encaissement quotidien peut être largement inférieur à celui des encaissements instantanés. En effet, le courtier peut ainsi accumuler davantage de fonds et ne payer qu'une commission de réseau pour une seule transaction d'encaissement, alors qu'il doit payer une commission distincte pour chaque transaction d'encaissement instantané.

Exemples d'agent d'encaissement :

- Agent d'encaissement par jetons GRAFT ("à valeur stable")
- Agent d'encaissement USDT
- Agent d'encaissement via le Système Interbancaire de Télécompensation
- Agent d'encaissement PayPal
- Agent d'encaissement Bitcoin

Courtier de rechargement

Le courtier de rechargement permet de recharger un portefeuille en échangeant des Bitcoins, des altcoins ou une monnaie fiduciaire locale contre des GRFT. Ce scénario est le plus avantageux pour l'acheteur et le marchand, car tous les frais (y compris les frais de réseau de la cryptomonnaie cible) sont payés par le marchand, et le paiement est approuvé instantanément. Pour l'acheteur, les avantages sont évidents : aucuns frais ne sont associés au paiement, et il a la possibilité de payer, avec la cryptomonnaie cible, un marchand qui n'accepte pas cette dernière. Pour le marchand, il est important de bénéficier d'une autorisation instantanée, car il peut ainsi servir un plus grand nombre de clients en temps réel et accepter des paiements dans différentes cryptomonnaies. Le fait que tous les frais soient payés par le marchand, comme pour les paiements "classiques" par carte de débit/crédit, permet de proposer des taux de conversion bien plus intéressants aux clients.

De plus, le courtier de rechargement peut effectuer des opérations de change à la demande, pour des montants plus élevés et avec des taux plus intéressants.

Exemples de courtier de rechargement :

- Courtier de rechargement par carte de crédit
- Courtier de rechargement en Bitcoins
- Courtier de rechargement via le Système Interbancaire de Télécompensation

Paiements aux marchands

Un marchand peut décider de recevoir les recettes des transactions dans d'autres cryptomonnaies, telles que des Bitcoins, des jetons cryptographiques, des jetons de paiement ("à valeur stable") ou dans une monnaie fiduciaire locale. Dans ce cas, la devise de paiement de la transaction sera traitée par un courtier dans le cadre de cette même transaction ou ultérieurement, en fonction des paramètres définis par le marchand. Cela permet de garantir que le produit de la vente correspondra, pour le marchand, au prix exact dans la devise locale, moins les frais applicables. L'échantillon de super-nœuds sélectionne automatiquement la meilleure offre parmi celles de tous les courtiers, selon une combinaison basée sur les choix précédents du marchand, le meilleur taux de change et le score de réputation le plus élevé.

Volatilité

La plupart des marchands veulent être payés dans leur devise locale. Ils utilisent la monnaie fiduciaire (et non les Bitcoins, ni d'autres cryptomonnaies ou jetons cryptographiques) pour se réapprovisionner,

payer leurs factures et payer les salaires de leurs employés. De plus, ils peuvent être amenés à effectuer des remboursements en monnaie fiduciaire en cas de retours de produits. La plupart des marchands ne peuvent pas se permettre d'être exposés à une forte volatilité, en particuliers les petits commerçants. Les jetons Graft (GRFT) étant échangeables, leur volatilité peut être problématique lorsqu'ils sont utilisés directement pour les paiements en faveur des marchands. Pour résoudre le problème de la volatilité, GRAFT utilise une exécution instantanée du traitement des transactions en temps réel, qui limite les éventuelles pertes de valeur générées par la volatilité, ainsi que des jetons de paiement spéciaux "à valeur stable". L'application de paiement du marchand peut adapter automatiquement le montant de la transaction au taux de change en cours et le convertir dans la devise locale via une plateforme d'échange en ligne juste après la fin de la transaction.

Jeton de paiement ("à valeur stable")

Le jeton de paiement est un type spécifique de jeton marchand qui permettra de faciliter les paiements aux marchands dans une monnaie fiduciaire locale afin de faire le lien entre les deux univers : les transactions en cryptomonnaie et les opérations commerciales en monnaie fiduciaire. Il représente une monnaie fiduciaire locale et peut faire l'objet d'une transaction sur la blockchain GRAFT en temps réel via le réseau de super-nœuds de la blockchain. Le jeton de paiement est basé sur la technologie des jetons marchands GRAFT (semblable aux chèques-cadeaux, récompenses et autres types de jetons marchands).

Garantie des jetons de paiement

La création de jetons de paiement a pour principal objectif de proposer une méthode simple et fiable aux marchands leur permettant d'être payés dans des monnaies fiduciaires locales stables tout en évitant de passer par des processeurs de paiement centralisés. Les jetons de paiement sont émis et gérés par des assureurs de jetons responsables (des banques, par exemple). Lorsqu'une personne (comme l'agent d'encaissement) achète des jetons de paiement à l'assureur de jetons, l'entreprise génère la quantité de jetons nécessaire et les transfère à l'acheteur en échange d'un montant équivalent en monnaie fiduciaire. Lorsqu'une personne (le marchand ou l'agent d'encaissement pour le compte du marchand) revend des jetons de paiement à l'assureur de jetons, l'entreprise détruit les jetons et verse au vendeur un montant équivalent en monnaie fiduciaire locale. Ainsi, les jetons de paiement sont toujours garantis par un montant suffisant en monnaie fiduciaire, et leur prix reste identique et équivaut au flottement de la monnaie fiduciaire correspondante. Par exemple, 100 GRAFT.USD peuvent toujours être achetés ou vendus pour 100 $US. Les jetons de paiement seront émis par des assureurs de jetons agréés, uniquement en échange d'un montant équivalent en

monnaie fiduciaire. De plus, les droits permettant de gérer des jetons de paiement spécifiques peuvent être délégués (sous licence) à des banques commerciales locales ou même à des administrations nationales.

Traitement des paiements

Il existe différentes options de paiement : les jetons GRAFT, la cryptomonnaie d'origine ou une autre cryptomonnaie, les jetons de paiement GRAFT ou une monnaie fiduciaire locale (tableau 2). Des services d'agent d'encaissement sont disponibles sur GRAFT pour chacune de ces options. Lorsque le marchand sélectionne les modes de paiement qu'il souhaite accepter et la méthode d'encaissement, l'application GRAFT Point of Sale lui présente toutes les options disponibles en matière de courtage, selon son identité et sa situation géographique. Le marchand peut alors souscrire aux services de courtage de son choix. Si plusieurs agents d'encaissement sont disponibles pour le même type d'échange et sélectionnés par le marchand, l'application GRAFT Point of Sale sélectionne automatiquement la meilleure offre lors de l'exécution de la transaction.

Tableau 2 : Exemples de modes de paiement et d'encaissement acceptés

Mode de paiement sélectionné par le client	Méthode d'encaissement sélectionnée par le marchand	Courtier compatible	Agent d'encaissement
GRFT	GRFT	Aucun (réseau GRAFT)	Aucun (réseau GRAFT)
Paiement via un chèque-cadeau, des points de fidélité, un avoir magasin	N/A	Aucun (réseau GRAFT)	N/A
GRFT	USD	Aucun (réseau GRAFT)	Agent d'encaissement par virement bancaire
GRFT	Bitcoins	Aucun (réseau GRAFT)	Agent d'encaissement Bitcoin
Bitcoins	GRFT	Courtier compatible Bitcoin	Aucun (réseau GRAFT)

Bitcoins	GRFT	Courtier compatible Bitcoin	Agent d'encaissement Bitcoin
Bitcoins	USD	Courtier compatible Bitcoin	Agent d'encaissement par virement bancaire
Carte de crédit	GRFT	Courtier compatible carte de crédit	Aucun (réseau GRAFT)
Carte de crédit	Bitcoins	Courtier compatible carte de crédit	Agent d'encaissement Bitcoin
Carte de crédit	USD	Courtier compatible carte de crédit	Agent d'encaissement par virement bancaire

Jetons marchands et VChains

Les marchands souhaitent pouvoir effectuer des transactions rapides et peu onéreuses, mais ils attachent aussi une grande importance à la fidélité des clients et au branding. Cet aspect sera couvert par la couche "jeton" de la monnaie GRAFT. Le jeton représente une utilisation de GRAFT propre à un domaine (marchand). Il offre des fonctionnalités adossées à un contrat intelligent ("*smart contract*"), comme l'accumulation et l'utilisation de points de fidélité, des points de récompense, des remises en fonction des ventes ou des dépenses, l'alignement sur les prix des concurrents, des bons de réduction et des avoirs en magasin.

Par exemple, une chaîne de restauration rapide pourrait créer un jeton marchand et y associer des règles de promotion qui permettraient à un client d'obtenir des remises sur les boissons fraîches à un certain moment de la journée. Il comptabiliserait les achats auprès de l'établissement et proposerait des récompenses en fonction de l'activité ou de la non-activité. Les jetons marchands GRAFT peuvent constituer un mécanisme très efficace pour la gestion des bons de réduction, en permettant aux marchands de se lancer dans la création de bons de réduction et de définir les règles d'affectation au sein de leur domaine/réseau.

Jetons marchands

Un jeton marchand est un contrat intelligent ("*smart contract*") prédéfini qui permet de créer un jeton privé appartenant à son propriétaire. Contrairement à d'autres contrats intelligents et plateformes de

jetons, la création de jetons marchands GRAFT ne nécessite aucune programmation et peut être effectuée par n'importe qui.

Les fonctionnalités commerciales décrites ci-dessous sont généralement synonymes de fournisseurs de services tiers complexes et de frais de mise en œuvre élevés. Elles sont donc souvent inaccessibles pour les PME et très onéreuses pour les grandes entreprises. Grâce aux jetons marchands GRAFT, tout marchand peut mettre en œuvre ces fonctionnalités commerciales stratégiques sans fournir beaucoup d'efforts et pour un coût peu élevé.

Types de jetons marchands

Les jetons marchands permettront aux marchands de créer et d'utiliser leurs propres produits en réseau ouvert et en réseau fermé[14] (chèques-cadeaux, points de fidélité ou avoirs en magasin) en quelques minutes, sans aucun investissement initial ni aucuns frais, et sans avoir à s'enregistrer auprès d'une quelconque autorité centralisée. Les marchands pourront vendre et accepter des chèques-cadeaux sur leur site Web ou dans leurs magasins physiques, dans la devise locale, dans d'autres cryptomonnaies, en jetons cryptographiques ou en GRFT.

Toutes les transactions GRAFT, y compris l'émission et l'encaissement des chèques-cadeaux, des points de fidélité et des avoirs en magasin sont traités en temps réel à l'aide d'une API standard, qui peut s'intégrer facilement dans des applications de point de vente existantes.

Avoirs en magasin

Les avoirs en magasin sont généralement utilisés par les marchands en cas de retours ou d'échanges d'articles, lorsqu'un retour ne peut pas être effectué via le mode de paiement d'origine ou si la politique de retour du marchand ne permet pas un remboursement total. Pour résumer, l'avoir en magasin transforme le retour d'article en échange, de sorte que le marchand ne perd pas le client ni le chiffre d'affaires correspondant.

Les jetons d'avoir en magasin peuvent être associés au prix de l'article dans la monnaie fiduciaire locale. Le client peut ainsi utiliser ces jetons pour son prochain achat au lieu ou en plus du paiement en monnaie fiduciaire locale. Généralement, les jetons d'avoir en magasin n'ont pas de date d'expiration (ou celle-ci est très lointaine), car ils remplacent pratiquement la monnaie fiduciaire.

Points de fidélité

Les points de fidélité constituent un outil marketing efficace qui attire les clients et les incite à dépenser davantage. Ils peuvent être attribués pour chaque achat, ou sous la forme d'une prime

ponctuelle ou d'un autre modèle de récompense. Ces points de fidélité peuvent permettre d'acheter des articles spécifiques ou n'importe quel article, ou être convertis en espèces. Ils ne sont pas forcément associés directement à une monnaie fiduciaire ou une cryptomonnaie, car ils peuvent être dépensés dans le but d'obtenir une remise ou d'acheter des articles propres au programme de fidélité, qui ne sont pas disponibles avec d'autres modes de paiement.

Les points de fidélité sont généralement associés à des dates d'expiration relativement proches. Le marchand encourage ainsi les clients à collecter plus de points de fidélité et évite l'accumulation de très grandes quantités de points de fidélité, qui pourraient devenir inutilisables à terme.

Chèques-cadeaux

Les marchands peuvent émettre des chèques-cadeaux pour attirer des clients. Afin d'accroître leur intérêt, les chèques-cadeaux peuvent être vendus avec une remise (et donc moins chers que leur prix nominal). Généralement, les jetons de chèque-cadeau n'ont pas de date d'expiration (ou celle-ci est très lointaine), car ils représentent essentiellement la monnaie fiduciaire.

Les clients peuvent acheter des chèques-cadeaux auprès de différents marchands et places de marché, en ligne et en magasin, et les payer en monnaie fiduciaire locale, en cryptomonnaie ou en jetons cryptographiques. La valeur du chèque-cadeau ou de l'avoir en magasin dans la monnaie fiduciaire locale est garantie par le marchand émetteur et par le réseau. Il conserve donc toujours sa valeur nominale initiale. Les clients peuvent utiliser les chèques-cadeaux dans le magasin du marchand émetteur (selon sa valeur nominale dans la devise locale) ou les vendre à tout moment sur la place de marché en monnaie fiduciaire locale, cryptomonnaie ou jetons cryptographiques, selon sa valeur marchande actuelle.

Bons de réduction

Les bons de réduction peuvent être utilisés pour des promotions ponctuelles ou à long terme. Ils peuvent être distribués à tout le monde ou à certaines personnes, dans un portefeuille ou au format papier. Ensuite, le bon de réduction peut être scanné sur le point de vente afin d'obtenir une remise ou même un article gratuit.

Types de transaction pour les jetons marchands

Création

Cette transaction consiste à créer un jeton marchand ("contrat intelligent" ou "*smart contract*"). Elle peut être effectuée à l'aide d'une application de point de vente.

Renouvellement

Cette transaction consiste à renouveler un jeton marchand ("contrat intelligent"). Elle peut être effectuée à l'aide d'une application de point de vente.

Ajout

Cette transaction consiste à injecter des jetons marchands supplémentaires dans le circuit.

Émission

Le point de vente du marchand envoie des jetons marchands au portefeuille du client ou imprime un portefeuille papier.

Utilisation

Le client utilise des jetons marchands sur le point de vente du marchand via une application de portefeuille ou un portefeuille papier.

Frais associés aux jetons marchands

Tous les frais associés aux jetons marchands sont payés aux super-nœuds inclus dans l'échantillon d'autorisations.

Frais de transaction liés aux jetons marchands

Le marchand paie systématiquement les frais de transaction des jetons (et l'acheteur ne paie donc jamais de frais). Des frais de transaction s'appliquent à chaque transaction impliquant un jeton marchand, y compris l'ajout, l'émission et l'utilisation.

Frais d'initialisation et de renouvellement

La transaction "Création" initiale génère des frais particuliers plus élevés, car elle est associée au nommage du jeton. Pour éviter tout "cybersquattage", les frais initiaux seront fixés à un montant raisonnable, ce qui permettra d'éviter une utilisation abusive massive.

VChains

VChain permet de créer une chaîne virtuelle de magasins, de façon à connecter plusieurs points de vente à la même "blockchain virtuelle". Le terme "VChain" a donc un double sens : "chaîne virtuelle" et "blockchain virtuelle". VChain crée une plateforme commune privée pour la gestion des jetons marchands et des catalogues de produits.

Un marchand peut créer sa propre VChain privée, à laquelle il sera le seul à pouvoir accéder, qui contiendra toutes les informations sur ses jetons. VChain permet de connecter plusieurs points de vente ou même de créer une chaîne de magasins. Les points de vente appartenant à la même VChain peuvent émettre et accepter les mêmes jetons marchands, utiliser le même catalogue de produits partagé (stocké et mis à jour sur la blockchain), générer des rapports cumulés sur les transactions, etc.

Les acheteurs peuvent utiliser la VChain pour connecter plusieurs portefeuilles, ce qui leur permet de gérer plusieurs comptes et de déplacer des fonds entre ces comptes sans payer de frais. Cette fonctionnalité est utile pour les comptes familiaux et professionnels.

Frais associés à la VChain

La VChain entraîne des frais annuels d'initialisation (création du contrat intelligent VChain) et des frais de renouvellement. Ces frais sont nécessaires pour assurer le traitement sécurisé du contrat intelligent et éviter toute utilisation abusive du système. Des frais annuels distincts sont facturés pour l'ajout d'un autre point de vente ou portefeuille à la VChain.
Tous les frais associés à la VChain sont payés aux super-nœuds inclus dans l'échantillon d'autorisations.

Crédit communautaire décentralisé

Un écosystème de crédit communautaire décentralisé se compose de consommateurs de crédits (titulaires de crédits, acheteurs), de fournisseurs de crédits, de fournisseurs d'identité et de marchands (vendeurs). Le réseau GRAFT facilite la communication et les transactions entre les parties, et applique les règles communes visant à minimiser le risque de fraude.

Le réseau GRAFT met en relation des consommateurs de crédits potentiels et des fournisseurs de crédits qui proposent des crédits aux consommateurs. Toute personne disposant de l'application GRAFT Wallet gratuite peut devenir consommateur de crédits. Toute personne disposant de l'application GRAFT Wallet gratuite et présentant un solde positif peut devenir fournisseur de crédits. Toute personne disposant de l'application GRAFT Point of Sale gratuite ou d'un point de vente tiers intégré avec le SDK GRAFT peut devenir marchand. Le fournisseur d'identité est implémenté sous la forme d'un plug-in de service sur le super-nœud GRAFT. Le fournisseur d'identité utilise une API ouverte, qui permet de préserver le caractère ouvert et décentralisé de l'écosystème dans son ensemble.

Les fournisseurs de crédits définissent leurs exigences concernant le minimum d'informations d'identité à spécifier pour recevoir le crédit, la limite de crédit maximale, la limite de crédit maximale globale (via plusieurs fournisseurs), le taux d'intérêt, ainsi que le montant minimum et la fréquence minimale des remboursements. Les consommateurs de crédits peuvent obtenir un crédit auprès de plusieurs fournisseurs, à condition que l'état actuel de leur compte réponde aux exigences de chaque fournisseur. Les fournisseurs d'identité tiers valident et confirment les éléments d'identité fournis par le consommateur. Ainsi, les fournisseurs de crédits n'ont pas à se charger de la validation de l'identité, et le titulaire du crédit bénéficie d'un certain niveau d'anonymat et de confidentialité. Les fournisseurs d'identité connaissent donc l'identité réelle du consommateur, et ils peuvent tenir à jour leur score de réputation à long terme indépendamment du réseau ou des fournisseurs de crédits. Les fournisseurs de crédits perçoivent une part des frais de transaction pour chaque paiement effectué grâce à un crédit octroyé.

Chaque consommateur de crédit se voit attribuer un score de réputation. Celui-ci est calculé automatiquement en fonction de l'historique du consommateur, et du niveau des éléments d'identité fournis par le titulaire et validés par les fournisseurs d'identité. Le score initial, avant toute validation de l'identité et toute collecte des données de l'historique, est défini sur 0. Il augmente en fonction du nombre d'éléments d'identité fournis et validés (permis de conduire, données biométriques, numéro de sécurité sociale, par exemple), et plus il augmente, plus le titulaire est digne de confiance. Un historique de remboursements positif augmente le score de réputation en conséquence.

Les marchands ne sont que les destinataires de la transaction avec les consommateurs de crédits, et sont isolés de la relation entre les titulaires, les fournisseurs de crédits et les fournisseurs d'identité, ce qui élimine totalement le risque d'une fraude à leur encontre. Les fournisseurs de crédits assument tous les risques potentiels de fraude et toutes les dépenses, qui sont compensés par la part des frais de traitement des transactions et les intérêts qu'ils perçoivent. Toutefois, les marchands peuvent participer au processus en proposant des avantages, comme le cashback, ou même tenir le rôle de fournisseurs de crédits.

Sécurité

Comme le montrent les récentes failles de sécurité majeures observées dans les secteurs du commerce de détail et de l'hôtellerie, la sécurité constitue un élément essentiel de tout écosystème de paiement. Pour atteindre un niveau de sécurité optimal, il faut que la sécurité fasse partie intégrante de la conception du système et qu'elle ne soit pas un module ajouté une fois l'implémentation effectuée. La sécurité d'un système de paiement ne concerne pas seulement la sécurité des

informations, mais aussi la sécurité financière. En plus des fonctionnalités de sécurité standards héritées de ses prédécesseurs, GRAFT prévoit de mettre en œuvre plusieurs améliorations qui bénéficieront aussi bien aux acheteurs qu'aux marchands.

Disponibilité

Le réseau distribué de super-nœuds "*always-on*" (toujours actifs) garantit la disponibilité globale du réseau. Les applications client communiquent simultanément avec plusieurs super-nœuds afin d'obtenir le consensus requis pour l'autorisation. Si l'un des super-nœuds de l'échantillon n'est pas disponible, il est automatiquement remplacé par un autre issu de la liste des candidats à l'échantillon d'autorisations, qui comporte un nombre de candidats quasiment illimité.

Gestion des identités

Le fait de s'appuyer sur les portefeuilles pour gérer les utilisateurs entraîne un risque de sécurité majeur, car les portefeuilles sont généralement libres de mettre en œuvre leurs propres mesures de sécurité et peuvent être mis en danger individuellement. Afin de protéger le réseau et d'assurer l'intégrité des identités des utilisateurs, GRAFT mettra en place un service distribué de fournisseur d'identité (intégré dans le super-nœud), qui sera disponible pour les portefeuilles sous la forme d'un appel à l'API OAuth2 d'OpenID Connect.

Ainsi, quelle que soit l'implémentation du portefeuille, la vérification et l'authentification des utilisateurs seront effectuées par le réseau GRAFT, ce qui évitera de mettre en danger les identités des utilisateurs, ainsi que le risque d'attaques par usurpation, par rejeu et "de l'homme du milieu".

Identification, authentification et autorisation

Les méthodes d'authentification/d'autorisation utilisées par les cryptomonnaies existantes relèvent de l'application de l'utilisateur (le portefeuille, par exemple) et ont souvent été considérées comme un détail. Toutefois, dans le contexte de transactions financières entre acheteurs et vendeurs, où un certain niveau de confiance doit être établi entre les parties, où les réglementations et la conformité sont à prendre en compte, et où des possibilités de recours doivent être proposées, il devient essentiel de mettre en place un système d'authentification/d'autorisation performant.

Vérification d'identité

La vérification de l'identité est une question délicate, car elle comporte des aspects concernant la réglementation et la confidentialité. De plus, il n'est pas évident de mettre en place un processus de vérification d'identité efficace.

Pour comprendre à quel point la vérification d'identité est nécessaire, pensez au marchand qui doit demander une vérification d'identité très poussée pour s'assurer que l'acheteur a le droit d'acheter des médicaments sur ordonnance, voire encore plus poussée pour l'achat d'armes (conformément aux dispositions du document *NIST Special Publication 800-63A* aux États-Unis). Inversement, les acheteurs qui achètent des produits sur le marché de l'occasion souhaitent probablement se protéger contre les produits volés en demandant au vendeur de fournir une preuve d'identité de niveau supérieur.

GRAFT exige que les applications client respectent les normes de vérification d'identité associées aux lois spécifiques de chaque juridiction. Les super-nœuds fourniront des ressources informatiques en matière de vérification d'identité et de détection des fraudes afin d'aider les marchands (et les utilisateurs) à se mettre en conformité, et d'assurer l'intégrité du réseau de paiement et la sécurité des transactions. Pour limiter l'exposition des utilisateurs lorsque le partage de leurs informations d'identité complètes n'est pas souhaitable ou contraire à la réglementation (RGPD, par exemple), GRAFT facilitera la demande et le partage des éléments d'identité (comme l'âge et l'adresse de la personne concernée), afin de garantir la conformité avec les lois et réglementations locales. Nous souhaitons également ajouter davantage de métadonnées au partage des attributs d'identité pour permettre une logique métier supplémentaire (vérification des interactions médicamenteuses ou points de fidélité, par exemple).

GRAFT offrira la possibilité d'un contrôle multi-utilisateur (plusieurs utilisateurs peuvent accéder au même compte marchand) et d'un service de garde (*custody*) multi-utilisateur (deux utilisateurs ou plus sont nécessaires pour débloquer certaines fonctions comme le transfert de fonds à partir du compte).

Score de réputation : éclairer les ténèbres

GRAFT adopte une approche basée sur le risque pour le traitement des transactions. Chaque participant du réseau se voit attribuer un score de réputation, qui est mis à jour automatiquement en fonction des nouvelles données collectées par le système. S'ils le souhaitent, les acheteurs, les marchands et les propriétaires de super-nœuds peuvent associer leur identité partielle à leur compte afin de divulguer et d'améliorer leur score de réputation. Cette association ne nuira pas à l'intraçabilité des transactions.

Le système de score de réputation aide les membres de l'écosystème à prendre des décisions judicieuses sans compromettre leur sécurité et leur confidentialité. Par exemple, un marchand peut tenir compte du score de réputation d'un acheteur lorsqu'il prend des décisions concernant les limites

d'autorisation avant l'autorisation instantanée. De même, l'acheteur peut consulter le score de réputation d'un marchand avant d'effectuer un paiement pour des produits qui ne peuvent pas être livrés immédiatement. Les acheteurs et les marchands peuvent vérifier le score de réputation du super-nœud avec lequel ils communiquent, et les super-nœuds proxy peuvent à leur tour tenir compte du score de réputation d'un courtier avant de décider de faire appel à lui dans le cadre d'une transaction.

Le score de réputation des utilisateurs s'avère tout aussi important dans le contexte des crédits communautaires, où il inclut des éléments d'évaluation des risques basés sur l'historique des paiements.

Les super-nœuds sont chargés de surveiller, de calculer, de mettre à jour et de valider les scores de réputation des acheteurs, des marchands et des autres super-nœuds. Ces scores sont calculés à l'aide d'algorithmes spécifiques d'analyse prédictive, qui produisent des résultats facilement compréhensibles sur une échelle de 0 à 100, et qui ne peuvent permettre de divulguer aucune information concernant le nombre, le montant, la date ou la nature des transactions.

Support client, résolution des conflits et garantie des paiements

L'adoption généralisée des cryptomonnaies et des jetons cryptographiques par les consommateurs et les marchands se heurte à l'obstacle suivant : peu de spécialistes ou de marchands sont capables de répondre à leurs questions et de résoudre leurs problèmes techniques et commerciaux. De plus, il n'est pas possible de "corriger" une transaction erronée en cryptomonnaie ou en jetons cryptographiques suite à une erreur humaine, une activité frauduleuse ou un incident technique. Bien entendu, tous ces problèmes s'expliquent et se justifient par l'aspect décentralisé, anonyme et indépendant des paiements cryptographiques. Toutefois, ces bonnes raisons ne permettent pas de résoudre les problèmes. Pour y remédier, la communauté Open Source a lancé un support client facultatif dédié aux produits Open Source gratuits. Le système d'exploitation Linux (supporté par Redhat) et la base de données MySQL (supportée par Oracle) font partie des nombreux exemples illustrant un support de niveau commercial pour des produits Open Source gratuits.

Afin de faciliter l'adoption des paiements GRAFT, la Fondation GRAFT fournit gratuitement un support client et des services de résolution des conflits aux titulaires d'un compte GRAFT. Les marchands qui génèrent des volumes de transactions élevés peuvent bénéficier d'un support et d'une assistance en temps réel pour la résolution des conflits, disponibles 24h/24 et 7j/7. La Fondation GRAFT et/ou les courtiers peuvent assurer les paiements jusqu'à l'équivalent de 100 USD, et dédommager les clients ou les marchands en cas de perte financière en raison d'une fraude ou de problèmes techniques.

Applications pour les utilisateurs

Toutes les applications utilisateurs GRAFT sont des clients "légers" qui ne stockent pas la blockchain et ne traitent aucune transaction. Ces applications utilisent des appels à l'API distante pour communiquer avec les nœuds GRAFT toujours actifs ("*always-on*"), qui minent les nouveaux blocs de transactions et traitent les demandes de transaction en temps réel.

Les utilisateurs qui souhaitent bénéficier d'un contrôle plus strict de la confidentialité, l'anonymat et la disponibilité (par exemple, les marchands de grande taille ou les organisations secrètes) peuvent exécuter leur propre super-nœud (voire plusieurs super-nœuds). Ceux-ci seront chargés de communiquer de façon exclusive et confidentielle avec leurs applications client, de transférer les messages et les transactions aux autres super-nœuds, d'émettre des autorisations hors ligne, et de miner les GRAFT nécessaires au fonctionnement des programmes de fidélité, de chèques-cadeaux et d'avoirs en magasin.

Exemples d'applications pour les consommateurs :

- Applications de point de vente marchand sur ordinateur et sur mobile, permettant d'accepter les paiements en jetons GRAFT, Bitcoins, altcoins et cartes de crédit/débit, et de configurer les encaissements en Bitcoins, altcoins et d'autres monnaies fiduciaires locales, qui peuvent être utilisées aussi bien par les acheteurs que par les marchands.
- Applications de portefeuille sous forme d'extensions de navigateur Chrome pour ordinateur et pour mobile, permettant d'effectuer des paiements en jetons GRAFT, Bitcoins, altcoins et cartes de crédit/débit (via des courtiers instantanés), et d'émettre et de recevoir des virements en jetons GRAFT.
- Le SDK GRAFT sera compatible avec les logiciels de point de vente et les systèmes de paniers d'achat des principaux marchands afin de traiter aussi bien les transactions dans les boutiques en ligne que dans les établissements physiques. GRAFT proposera une carte à puce GRAFT comme mode de paiement. En plus de servir de "porte-clés", cette carte stockera les signatures biométriques de l'utilisateur et un ensemble de mots de passe mémorisés ou disponibles, qui pourront être utilisés pour l'authentification au niveau du terminal. La Fondation GRAFT et les agents de change financeront la production des cartes à puce et des lecteurs de cartes à puce.

En plus de prendre en charge les transactions avec les consommateurs (B2C), GRAFT prendra en charge les transactions B2B (interentreprises) et s'intégrera dans les processus d'entreprise existants.

Ces processus peuvent être aussi simples que le recouvrement automatique selon les modalités de paiement prévues (30, 60 ou 90 jours nets, par exemple). Il peut aussi s'agir de processus plus complexes, comme le règlement de la facture douanière de l'expéditeur et sa prise en compte dans le cadre des transactions globales, ou la distribution des fonds selon les étapes atteintes et les approbations des clients.

GRAFT est également bien adapté à l'Internet des objets, car certains de ces objets connectés doivent "facturer" les données ou les services qu'ils proposent. Par exemple, un marchand physique pourrait commander un camion en fonction des niveaux de stocks déterminés par des capteurs et des systèmes backend.

Conclusion

GRAFT n'existerait pas sans ses prédécesseurs. Il est basé sur des idées, des technologies et des principes développés et testés par les créateurs d'autres jetons utilitaires cryptographiques. Grâce aux technologies les plus récentes développées par la communauté de la cryptographie et à des solutions nouvelles dédiées à la sécurité et au traitement des transactions, GRAFT sera en mesure de concurrencer les modes de paiement traditionnels et les processeurs de paiement centralisés existants.

Références

1. Bitcoin : https://bitcoin.org/fr/

2. Dash : https://www.dash.org/fr/

3. Bitpay : https://bitpay.com/

4. Définition de "GRAFT" en anglais (Merriam-Webster, 2017) : https://www.merriam-webster.com/dictionary/graft#h2

5. "What Is GRAFTing? - Definition & Methods", Study.com (2017) : http://study.com/academy/lesson/what-is-grafting-definition-methods-quiz.html

6. IOTA : https://iota.org/

7. Graphique de l'historique des frais de transaction moyens (Bitcoin, Ethereum, Litecoin, Dash, Monero), Bitinfocharts.com : https://bitinfocharts.com/comparison/transactionfees-btc-eth-ltc-dash-xmr-sma7.html#1y

8. PayPal : https://www.paypal.com/us/webapps/mpp/merchant-fees

9. "NIST Special Publication 800-63. Revision 3. Digital Identity Guidelines", NIST (2017) : https://pages.nist.gov/800-63-3/sp800-63-3.html

10. CryptoNote : https://cryptonote.org/

11. "Top Seven Ways Your Identity Can Be Linked to Your Bitcoin Address", 99 Bitcoins : https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/

12. Délai médian de confirmation, Blockchain : https://blockchain.info/charts/median-confirmation-time?timespan=30days

13. Norme de sécurité de l'industrie des cartes de paiement. "Requirements and Security Assessment Procedures". Conseil des normes de sécurité PCI Version 3.2 (2016) : https://pcicompliance.stanford.edu/sites/default/files/pci_dss_v3-2.pdf

14. Que sont les chèques-cadeaux en réseau ouvert et en réseau fermé ? (en anglais), Shelley Hunter, GiftCards.com : https://www.giftcards.com/gcgf/open-loop-versus-closed-loop-gift-cards