Woleet : Fournisseur d’accès à la vérité numérique

Vincent Barat, Gilles Cadignan
https://woleet.io
Livre Blanc
30 Juin 2017

Résumé

S'il est facile de faire confiance aux données créées dans un environnement bien connu - par exemple au sein d’une entreprise - les risques apparaissent lorsque ces données voyagent hors de ce cercle naturel de confiance. Afin de résoudre ce problème de perte de confiance, la solution commune est d'utiliser des tiers de confiance, ou des institutions centrales qui assureront l'intégrité et l'authenticité des données sensibles. Pour atteindre cet objectif, ces entités doivent parfois produire des vérifications manuelles ou mettre en œuvre des solutions centralisées basées sur la cryptographie. Ces procédés qui coûtent cher ajoutent frictions et délais aux processus métier. Woleet offre une plateforme middleware enrichie par une collection d’applications logicielles, tirant partie de la sécurité offerte par le protocole Bitcoin. Nos solutions assurent l'intégrité et la provenance des données en liant tout type de contenu numérique à des transactions Bitcoin immuables. Cela nous donne l'occasion de réinventer les flux de travail, en offrant un niveau continu d'authenticité durant toute la durée de vie des données.

1 Introduction

Le volume global des données numériques échangées entre les personnes ou les entreprises est en hausse continuelle. Ce n'est pas une tendance à la baisse, car de plus en plus d'applications et de plus en plus de participants sont connectés ensemble.

Des solutions comme l'horodatage numérique, meilleures que la vérification manuelle, sont coûteuses et appliquées uniquement sur un sous-ensemble de données très sensibles comme des contrats importants ou des documents financiers. En conséquence, la plupart des flux de données sont complètement exclus de ce type de solutions de sécurité. Pire, lorsque vous utilisez ces solutions et que vous payez le prix, vous vous fiez toujours entièrement aux institutions centralisées représentant, pour un attaquant externe des points de défaillance uniques qu’il devient plus facile de cibler.

L'apparition de Bitcoin en 2008 a introduit un tout nouveau type de décentralisation, basé sur la cryptographie, la théorie des jeux et le calcul distribué. Le livre blanc de Satoshi Nakamoto[1] nous montre comment échanger de la valeur en se passant d’une autorité centrale.

La valeur est quelque chose de très difficile à atteindre, en particulier dans un environnement virtuel à 100%, et ce, sans autorité centrale. Afin d'atteindre la valeur, vous devez faire confiance à la technologie sous-jacente. Bitcoin, en privilégiant sécurité extrême, neutralité et immuabilité, nous a donné l'occasion d'explorer de nouvelles façons d'aborder la confiance numérique. Woleet est une plateforme construite sur le réseau Bitcoin, liant le contenu numérique et leur signature à des transactions Bitcoin.

2 Architecture du système

2.1 Principes de conception

L'architecture système de Woleet suit plusieurs principes de conception afin d'offrir un middleware de production prêt à l'emploi, qui peut être utilisé par une application existante ou nouvelle voulant tirer parti de la puissance de la technologie blockchain appliquée à la cybersécurité.

2.1.1 Architecture en couches

L'architecture Woleet est à l'image de nos convictions sur l'avenir de la technologie blockchain. Nous pensons que le meilleur moyen de faire évoluer les applications possibles est de s'appuyer sur une architecture en couches (appelées aussi "Layer"). La plus basse étant la blockchain Bitcoin qui offre une sécurité maximale. Nous croyons en plus d'ingénierie au-dessus de ce noyau de sécurité (la racine de la confiance) pour imaginer de nouvelles fonctionnalités. Woleet explore une deuxième couche via des protocoles comme ChainPoint, décuplant les possibilités de la chaîne originelle et permettant de lier des milliers de données à une seule transaction Bitcoin.

2.1.2 API sans friction permettant plusieurs applications

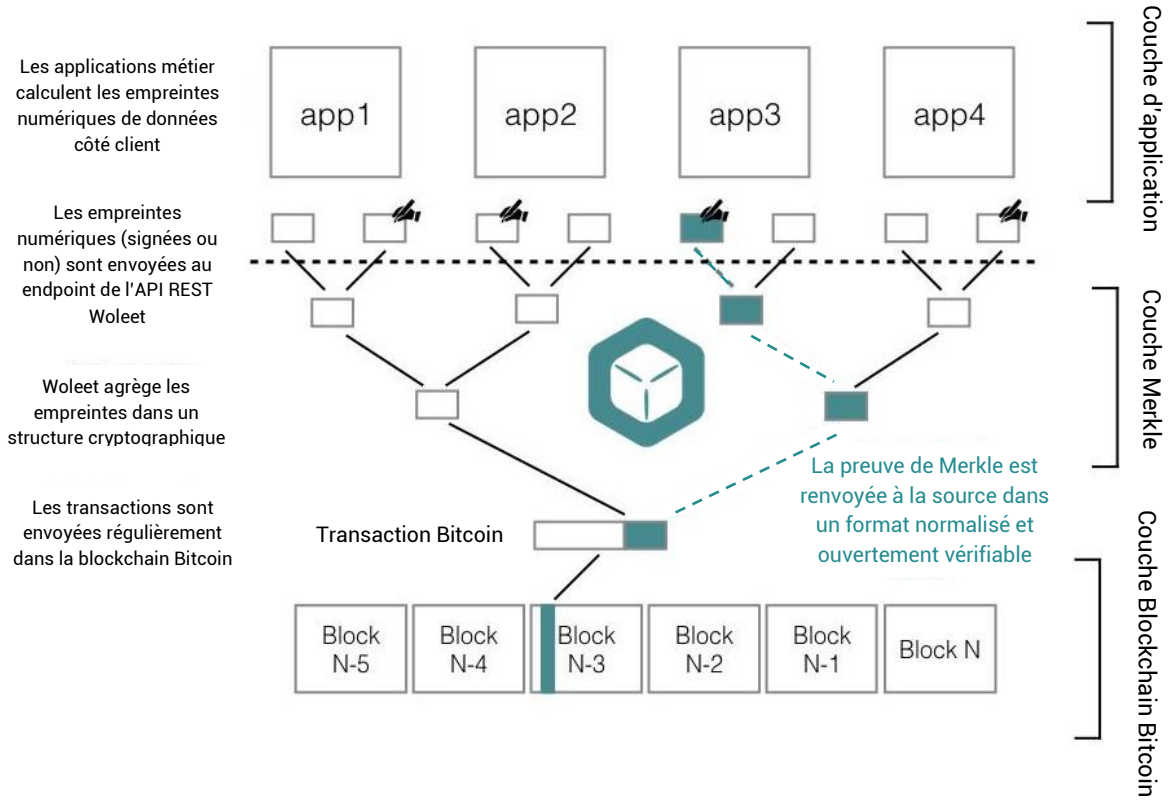
Un autre principe de conception de la plateforme Woleet est de minimiser les frictions pour l'intégration. Nous pensons que chaque système ou application existante ou nouvelle devrait pouvoir bénéficier de notre technologie avec un minimum d'effort. Même si la blockchain marque un réel changement dans la façon dont on perçoit la confiance dans les échanges numériques, nous pensons que les développeurs peuvent évoluer en douceur vers ce nouveau paradigme, sans rompre tout l'architecture existante ni faire une croix sur des années d'expertise métier.

2.1.3 Formats ouverts et véritable désintermédiation

Woleet facilite l'exploitation de sa technologie en produisant des preuves interopérables dans des formats ouverts. De cette façon, Woleet reste compatible avec d'autres systèmes compatibles avec ces formats et nos preuves restent exploitables même si nous disparaissons.

2.2 Architecture globale

L'architecture globale de Woleet est décrite comme il suit :



2.3 Couche n°1 : La blockchain Bitcoin

Bitcoin est la blockchain la plus mature, avec plus de 8 ans de preuve de travail la sécurisant et un consensus autonome hyper résilient. Au début, Bitcoin était destiné à agir comme une nouvelle forme d'argent, une monnaie utilisable de pair à pair sans autorité centrale. De nos jours les *core developers* de Bitcoin favorisent une liste de propriétés très importantes faisant de Bitcoin plus une réserve de valeur qu'une monnaie réelle. La résistance extrême du Bitcoin dans un environnement hostile le rend parfait pour être l'infrastructure neutre ultime. Nous allons explorer ces propriétés et les comparer à d'autres types de blockchains.

1. **Sans permission** : Bitcoin ne nécessite aucune permission. C'est-à-dire que toute personne exécutant un logiciel qui implémente les règles du consensus peut se brancher sur le réseau et envoyer, recevoir ou vérifier des transactions. Il s'agit d'une caractéristique très importante puisque les blockchains privées et DLT (Distributed Ledger Technology) ne fonctionnent pas de cette façon. Dans Bitcoin ou Ethereum, l'infrastructure est publique à la manière d'Internet. Au niveau des DLT, les utilisateurs doivent soutenir l'infrastructure, la maintenir, exécuter des nœuds et devenir des mineurs, tout cela à la fois. Les nouveaux participants subissent une procédure beaucoup plus douloureuse pour entrer et ont besoin d'une permission. Dans le cadre de la réalisation de preuves mondiales, ouvertes et internationales que n'importe qui peut vérifier, un protocole ne nécessitant aucune permission est obligatoire**.**

2. **Immuabilité et résistance à la censure** : Bitcoin est immuable ; depuis le 3 janvier 2009, toutes les transactions émises sur le réseau Bitcoin et enregistrées dans des blocs n'ont jamais été modifiées ou supprimées. Il s'agit d'une propriété très importante dans notre contexte, puisque nous voulons utiliser Bitcoin comme un témoin d'événements numériques, gravés dans le marbre. D'autres blockchain publiques et populaires comme Ethereum ne sont pas immuables, car certaines transactions ont été inversées. Si une personne ou un petit groupe de personnes peuvent agir d'elles-mêmes pour modifier le registre public, nous perdons automatiquement la résistance à la censure et l'immuabilité. Ces propriétés sont la base d'un système d'horodatage et d'ancrage et, encore une fois, Bitcoin respecte ce principe.
3. **Sécurité** : Bitcoin a été fortement sécurisé dès le début. L'algorithme de preuve de travail protège le registre par la puissance de calcul du réseau qui doit être défaite pour modifier le registre. Avec la valeur attachée à chaque token (ou jeton en français), Bitcoin est constamment attaqué par de nombreuses personnes, et reste toujours inviolé aujourd'hui. Bitcoin a été éprouvé tous les jours depuis le début de son existence. Jusqu'à aujourd'hui, les vulnérabilités du système sont rares et bien connues par les développeurs qui essaient toujours de trouver la solution la plus sûre pour les résoudre.
4. **Disponibilité** : Le taux de disponibilité de Bitcoin est de 99,99%. Ce taux est le résultat de la distribution du réseau. Vous pourrez toujours demander des informations à partir des milliers de nœuds connectés au réseau et envoyer des transactions.

2.3.1 Gestion des transactions

La plateforme Woleet envoie régulièrement des transactions sur le réseau Bitcoin. Nous construisons des transactions P2PKH standards avec des sorties OP_RETURN contenant uniquement des racines d'un arbre de Merkle et sans préfixe particulier. Nous utilisons un algorithme d'estimation de frais en interne, combiné avec l'estimation de nœud complet pour atteindre les meilleurs frais possibles afin de prioriser nos transactions.

2.3.5 Full Node utilisé

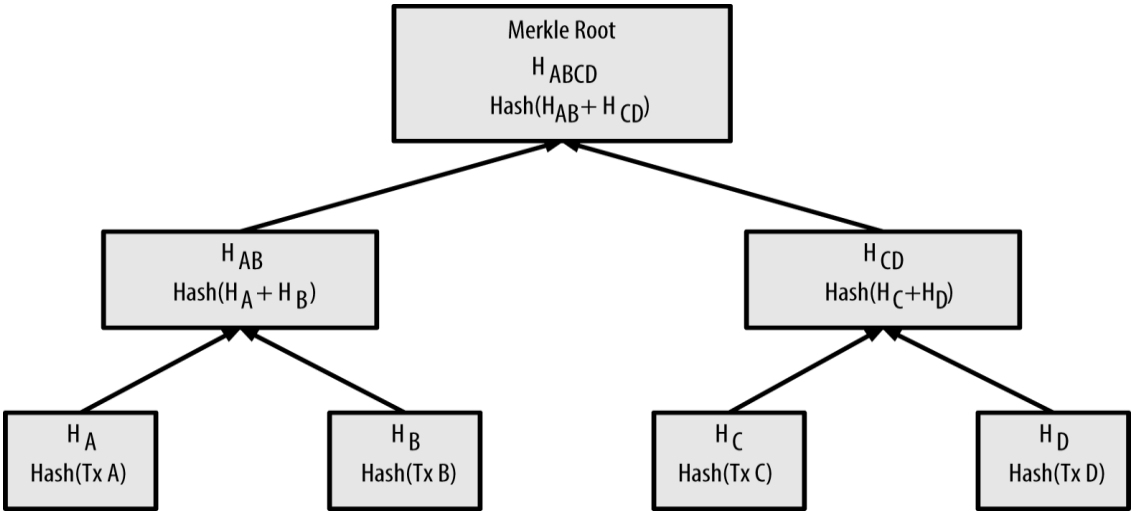
Au moment de l'écriture de ce papier, Woleet utilise l'implémentation de référence de Bitcoin (Bitcoin Core 0.15) et fait confiance à cette distribution, sur sa capacité à livrer une mise en œuvre solide, testée et évaluée par un grand nombre de développeurs. Nous estimons également que le processus de développement de Bitcoin Core est ouvert et non centralisé dans une entreprise ou un petit groupe de personnes.

2.4 Couche n°2 : Couche Merkle

La couche Merkle de la plateforme Woleet contient le moteur en charge de la factorisation de toutes les empreintes pour les ancrer dans la blockchain sous-jacente. Il agit comme un centre d'économie d'échelle capable de construire progressivement une structure d'arbre binaire - un arbre de Merkle -, avant la mise en place de la racine dans la transaction Bitcoin (dans la sortie OP_RETURN).

2.4.1 Adresser la scalabilité avec les arbres de Merkle

Les arbres de Merkle sont une structure de données commune utilisée entre autres pour vérifier l'intégrité des fichiers dans les systèmes d'exploitation. Ils sont également utilisés dans Bitcoin pour lier de façon cryptographique toutes les transactions incluses dans un bloc. Le schéma ci-dessous extrait de *Mastering Bitcoin*[2], présente une structure d'arbre de Merkle classique :



Ici, "H" est une fonction de hachage (calcul d'empreinte numérique) cryptographique. La fonction de hachage par défaut utilisée par Woleet est SHA-256. Cette fonction prend toutes les données et les transforme en un *Digest* de longueur fixe qui est unique pour chaque donnée. Il est techniquement possible des données différentes génèrent la même empreinte (le même *hash*), mais cette probabilité est trop faible pour être considérée ici (moins de 1 chance sur 2^{128}).

Woleet utilise des arborescences Merkle pour générer une racine de Merkle unique à partir d'empreintes de données, au lieu d'empreintes de transaction. Un seul arbre binaire peut être assez grand pour contenir des milliers d'empreintes. C'est ainsi que nous abordons la scalabilité et résolvons les limitations en volume de transactions de la blockchain sous-jacente.

2.4.2 Stockage de la structure et des métadonnées d'arborescence

La plateforme Woleet enregistre et sauvegarde les structures arborescentes produites dans une base de données locale. Chaque arbre de Merkle créé par la plateforme est maintenu pour faciliter la génération des reçus d'ancrage une fois que les transactions Bitcoin sont confirmées par le réseau. Il permet également de régénérer le reçu s'il est perdu par les utilisateurs. Nous recommandons fortement de stocker les reçus d'ancrage côté client afin d'être complètement indépendant pour la vérification des preuves produites.

2.5 Couche n°3 : Couche d’application

Avoir un moyen simple de graver des preuves dans une blockchain publique débloque de nombreuses possibilités du côté des applications. Les utilisateurs de Woleet peuvent enfin avoir un réel contrôle sur leurs données, s'ils identifient clairement où cette technologie peut les aider à surmonter les problèmes de confiance qu’ils ont, au niveau de certains échanges numériques critiques.

2.5.1 Choix des données à sécuriser

La première étape est d'identifier les données sensibles qui ont besoin d’être vérifiées par des clients, fournisseurs, auditeurs, collaborateurs ou partenaires d'affaires. La granularité est également importante car il est possible de sécuriser des volumes élevés sans avoir de coûts supplémentaires.

2.5.2 Confidentialité préservée

S'il est possible d'attacher des métadonnées aux demandes d'ancrage, le contenu de cette demande n'est pas remis à l'API Woleet. Ainsi, la confidentialité est conservée car la plateforme ne fonctionne qu'avec des empreintes de données calculés uniquement du côté client. Woleet n’a donc jamais accès à leur contenu réel.

2.5.3 Logiciel côté client

Woleet fournit une collection d'outils logiciels côté client capables de calculer l’empreinte des données et également de les signer via le protocole Bitcoin. Comme ils sont tous Open Source, nos outils peuvent aisément être adaptés à des besoins plus spécifiques.

2.5.4 Faciliter la vérification externe

Chaque fois qu'une ancre est confirmée par la blockchain, la vérification est possible par toute personne ayant ces deux éléments d'information :

- le fichier (ou la donnée) à vérifier,
- le reçu d’ancrage.

La vérification est alors possible avec n'importe quel outil compatible ChainPoint.

3 Horodatage de donnée

L'API Woleet crée des ancres au format ChainPoint[3], qui est défini par une spécification Open Source. Par conséquent, elles peuvent être vérifiées en utilisant n'importe quel outil compatible avec cette norme, sans aucune interaction avec Woleet, et ainsi rester vérifiable à jamais, même si Woleet cesse d’exister.

3.1 Créer des preuves d’existence

Pour créer une preuve d'existence d’une donnée spécifique, vous devez créer ce que nous appelons une « ancre ». Une ancre est fondamentalement une preuve de demande de création d'existence. Pour ce faire, il vous suffit de calculer l’empreinte SHA256 de ces

données côté client et de choisir un nom pour l'ancre. Puisque la plateforme n'a pas besoin des données réelles, il n'y a aucune limitation sur la taille ou sur le type de données, autre que le temps pour calculer l'empreinte (calculer l'empreinte d'un fichier de 1Go sur un ordinateur moderne prends quelques dizaines de secondes).

Les ancres nouvellement créées sont automatiquement collectées par la plateforme et enregistrées dans la blockchain Bitcoin : cela peut prendre de 10 minutes à quelques heures, en fonction de la charge du réseau Bitcoin et du niveau de priorité de votre compte d'utilisateur. Pour vérifier l'état de vos ancres, vous pouvez les appeler à l'aide de l'API Woleet, ou vous pouvez associer une URL de callback à une ancre que la plateforme appellera chaque fois que l'état de l'ancre sera modifié.

Une fois qu'une ancre est enregistrée dans la blockchain Bitcoin, vous pouvez récupérer le reçu d'ancrage associé à l'aide de l'API Woleet. Les reçus d'ancrage suivent la norme ChainPoint (avec quelques extensions pour les preuves de signature). Le reçu de preuve est le seul élément de données requis pour prouver l'existence ou la signature d'un fichier à une date donnée (évidemment, le fichier lui-même est également nécessaire, car il n'est pas inclus dans la réception d'ancrage). Ainsi, il est fortement recommandé que vous gardiez vos reçus d'ancrage (et vos fichiers) dans vos propres disques durs ou dans un coffre-fort numérique, de sorte que vous ne dépendez pas de l'API Woleet pour générer le reçu chaque fois que vous voulez vérifier un fichier.

3.2 Vérifier des preuves d'existence

La vérification d'une preuve d'existence à l'aide de l'API Woleet est simple : l'API s'occupe de vérifier que la preuve sous forme de reçu est valide et correctement ancrée dans une transaction Bitcoin. Il vous suffit donc de vérifier que l'empreinte SHA256 du fichier correspond à l'empreinte signalée dans le reçu.
Le processus de vérification peut également être effectué sans l'API Woleet avec le code open source existant. Woleet fournit quelques exemples sa page GitHub[4] et d'autres implémentations compatibles existent et sont faites par d'autres équipes travaillant sur la norme ChainPoint.

3.3 À propos des ancres publiques et privées

Une ancre peut être publique (qui est la valeur par défaut) ou privée.

Une ancre privée ne peut être découverte que par son propriétaire (voir l'endpoint `/anchors`). Ainsi, le propriétaire doit fournir le reçu d'ancrage ainsi que les données à toute personne voulant vérifier la preuve.
Une ancre publique est découverte par toute personne connaissant l'empreinte des données (y compris les personnes n'ayant pas de compte Woleet, voir le endpoint `/anchorids`). Cela permet à quiconque de récupérer le reçu de preuve en utilisant uniquement l'empreinte de la donnée comme entrée, puis de le vérifier en utilisant l'API Woleet (ou tout autre moyen) :

- utiliser le endpoint `/anchorids` pour récupérer l'identificateur d'ancre par son empreinte.

- utiliser le endpoint `receipt/{anchorid}` pour récupérer le reçu de preuve (qui inclut les métadonnées de l'ancre).
- utiliser le endpoint `receipt/verify` (ou tout autre outil compatible ChainPoint) pour vérifier la réception de la preuve et obtenir l'horodatage des données ou signature.

4 Preuve de signature

L'API Woleet crée des preuves de signature qui sont une extension de la même fonctionnalité de base d'ancrage de données. Ici, l'existence et l'horodatage d'une signature sont vérifiables en utilisant les mêmes outils utilisés pour vérifier les preuves d'existence.

En ce qui concerne la vérification de la validité de la signature et de l'identité du signataire, un traitement supplémentaire est effectué : puisque ce traitement peut être entièrement exécuté côté client sans données supplémentaires, des preuves de signature restent vérifiables à jamais même si Woleet cesse ses opérations.

4.1 Création de preuve de signature

Pour créer une preuve de signature d'un fichier, vous devez également créer une ancre, donc calculer l'empreinte SHA256 du fichier et choisir un nom pour cette ancre. Mais certaines données supplémentaires sont nécessaires : votre clé publique (celle associée à la clé privée utilisée pour signer l'empreinte numérique du fichier) et votre signature elle-même. Facultativement, vous pouvez fournir une URL permettant de vérifier votre identité en vous assurant que vous possédez la clé publique et le certificat TLS utilisé sur cette URL.

4.2 Vérification de preuves de signature

La vérification d'une preuve de signature à l'aide de l'API Woleet est également simple : l'API s'occupe de vérifier que le reçu de preuve est valide et correctement ancré dans une transaction Bitcoin, puis vérifie la signature, et éventuellement vérifie que le signataire possède la clé publique et le certificat TLS. Il vous suffit donc de vérifier que l'empreinte numérique du fichier corresponde à la propriété *`signedHash`* de la preuve de réception.

Pour preuve de signature, un processus de vérification supplémentaire est effectué :

- vérifiez que l'empreinte de la fonction de signature correspond à sa propriété *`target_hash`*
- vérifiez que la fonction de signature est une signature valide de la propriété *`signedHash`* pour la clé publique stockée dans la propriété *pubKey.*
- en outre, si une propriété *`identityURL`* est disponible :
    - appelez *`identityURL`* pour faire signer au destinataire des données aléatoires à l'aide de la clé publique *`pubKey`*,
    - vérifiez que la signature renvoyée est valide,
    - obtenir les certificats TLS de l'URL (il doit s'agir d'une URL https) afin d'obtenir des informations sur l'identité du signataire.

5 Cas d’utilisation

La plateforme Woleet a de nombreux cas d'utilisation applicables dans la vie réelle qui peuvent être déployés dans presque toutes les entreprises quand il s'agit de traiter la confiance numérique. Au moment de l'écriture de ce livre blanc, Woleet fournit deux primitives techniques qui peuvent être extrapolées de plus haut niveau de cas d'utilisation :

- **Preuve d’existence** : L'ancrage de données à l'aide de la plateforme Woleet offre un moyen puissant et abordable de prouver la date d'existence de n'importe quel type de données. Avoir un élément de données ancré dans un bloc peut servir de protection au niveau de la propriété intellectuelle ou peut être partagé comme preuve de transparence de données sensibles telles que des documents financiers ou des contrats. Le principal avantage de l'utilisation de la technologie Woleet est que la preuve produite peut être partagée à n'importe qui dans le monde ayant un accès Internet et un logiciel open source (et libre) capable de vérifier le reçu issu de la blockchain.
- **Preuve de signature numérique** : avec sa technologie de signature, Woleet introduit une nouvelle technique pour faire face à la signature numérique. En utilisant des clés Bitcoin pour l'identification, le processus de gains de fluidité devient beaucoup plus abordable que les solutions de signature numérique réelle.

En plus de ces deux primitives, plusieurs sujets peuvent être adressés :

- Protection de la propriété intellectuelle
- Traçabilité
- Intégration de politiques de transparence
- Connaissance du client
- Processus d’identification
- Contractualisation
- Vérification de l’intégration

6 Conclusion

La proposition de valeur actuelle de Woleet est d’entrer dans le nouveau paradigme de confiance offert par le protocole Bitcoin. En privilégiant les technologies matures et les standards ouverts, Woleet offre une vision à long terme, en choisissant des composants techniques viables et résilients. On peut sereinement construire des solutions sur le dessus de notre package technique sans s'interroger sur la compatibilité et la durabilité de l'infrastructure du système tout entier. Malgré le fait que la cybersécurité soit un nouveau sujet d’intérêt général, Woleet garantit à ses utilisateurs qu'elle fournit la technologie la plus mature disponible dans l'espace blockchain.

Références :

1. Bitcoin: A Peer-to-Peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf
2. Rebooting Web of Trust initiative
3. W3C Working group
4. chainpoint.org
5. Opentimestamps
6. Bitcoin Core Github repository