Foldereum

NonOpn contact@nonopn.com

November 8, 2017

Abstract

Nonopn est une société éditant la solution de certifications Foldereum permettant d'intéragir avec la blockchain Ethereum afin de proposer un ensemble de moyens de gérer la certification, l'authentification de documents, de personnes et de contenus.

I. Introduction

Nonopn se base sur une implémentation de blockchain nommée Ethereum. Une blockchain est une technologie innovante de traitements de transactions venant et vers des destinataires de façon décentralisée et sécurisée. Chaque bloc est ainsi créé et ajouté à l'ensemble de la blockchain à intervalle régulier. En fonction des implémentations de celles-ci, interviennent des mineurs qui valident les transactions en attente.

Popularisé avec la blockchain Bitcoin et son bien connu token monétaire éponyme, l'utilisation des blockchains s'intéresse énormément à l'usage fiduciaire de celles-ci. NonOpn souhaite s'abroger de ce paradigme purement monétaire et proposer de nouveaux usages directement au sein de la technologie de transport et stockage par le prisme de l'Open Source.

II. Préhistoire de la certification

Le monde de la certification est un monde extrêmement sensible et hyper centralisé. Ce dernier point présente énormément de risque dans le marché global. En effet, ce dernier est constitué de 4 groupes d'acteurs :

- Les sociétés de certification
- Les sociétés privées
- Les services publics
- Les consommateurs

Enormément de risques englobent les sociétés de certification. Elles doivent permettre à tout instant de prouver la validité et l'authenticité de documents (légaux ou non), gérer les processus de fonctionnement. Un seul maillon dans la chaine de valeur de ces sociétés et c'est l'ensemble de la profession qui est soumise à risque :

- Piratage
- Non transparence
- Centralisation de données
- Détournement de certificat
- Fraudes

Ces éléments sont tous des cas concrets de risques qui ont été pris en compte et qui, malheureusement, encore, à notre époque ne sont pas complètement gérés. NonOpn apporte une solution à ces problèmes.

III. L'empreinte

NonOpn propose donc pour ces acteurs & utilisateurs une solution concrète, simple d'intégration permettant de stocker dans un environnement sécurisé et transparent toutes ces certifications. Une certification étant un document numérique, il est possible d'effectuer un traitement dessus afin d'obtenir une donnée unique à celui-ci, agnostique du contenu et donc ne présentant aucun danger en cas de documents sensibles, confidentiels ou secrets ; NonOpn n'enregistre ni ne modifie le document original, il ne quitte d'ailleurs jamais son environnement premier.

Nous utilisons une fonction de hash prenant l'ensemble du document afin d'obtenir cette

donnée. C'est cette donnée qui est émise sur la solution de NonOpn pour y être stockée temporairement avant une validation finale dans la blockchain Ethereum.

L'empreinte étant unique, toutes modifications dans un fichier changera son empreinte. Dès ce moment, il est possible de vérifier l'intégrité d'un certificat, sa validité et surtout sa date de certification.

IV. Preuve de possession

Parce qu'un certificat permet de valider un document dans un contexte temporel, une évolution est prévu sur la plateforme. Aujourd'hui, c'est la plateforme qui connait les émetteurs d'une demande d'enregistrement de certificat. Elle est donc une autorité centrale.

Demain, il va être proposé aux clients de pouvoir générer directement via Foldereum des clés qui ne seront jamais stockées en ligne via un service annexe.

Ainsi, tout document certifié pourra l'être aussi via un système de 0-knowledge proof. NonOpn devenant un facilitateur d'accès au rèseau Ethereum dans une solution allant au delà d'une Blockchain as a Service (BaaS)

V. Modèle transactionnel d'autorité

En marge de la solution, NonOpn a développé un protocole permettant de traiter directement dans la blockchain l'ensemble de la vie autour de la certification.

Le protocole se base autour de 3 grandes notions :

- Autorité
- Acteur
- Objet

Ce triptique permet de gérer l'ensemble des informations directement de façon transparente et publique via la blockchain. Celle-ci étant immuable une fois passé un cap de confirmation, toutes les interactions d'un élément avec son environnement sont :

- immuables & sécurisées
- traçables
- auditables

VI. Fibre Open Source

Parce que les blockchains sont habituellement des environnements ouverts à tous et complètement Open Source, NonOpn édite une partie de la plateforme de façon Open Source.

Cette plateforme gère l'ensemble de la simplification de lecture de la blockchain Ethereum à travers ce qui se nomme un "explorateur". Celui-ci étant extrêmement léger, il propose de stocker l'analyse simple de chacune des transactions depuis l'origine de sa mise en service. On passe d'une interaction par "bloc" de transactions à une analyse par "transaction" directement au sein d'une base de donnée relationnelle avec des temps d'accès optimisés. A ce jour, aucun autre outil ne permet cette gestion sans devoir passer par des services tiers pouvant disparaître, modifier les données demandées voir proposer un service onéreux difficile à gérer.

Ce service est facilement réplicable se qui facilite son intégration dans des environnements autonomes et de production. Il s'intègre dans une optique de réplication et de gestion de charge dès sa conception.

Aucune logique ne vient gérer l'enregistrement dans la blockchain, les utilisateurs ne sont donc pas contraints de faire confiance à celui-ci lorsqu'il s'agit d'envoyer les informations souhaitées ; tout ayant déjà été validé par l'utilisateur, celui-ci ne fait confiance à la plateforme que pour l'envoi et la lecture aposteriori.

VII. Roadmap

- **Q4 2017** Finalisation de la plateforme
- **Q1 2018** Implémentation du protocole AAO
- **Q2 2018** Expansion des cas d'usages

VIII. Conclusion

En utilisant la solution Foldereum de NonOpn, la certification d'hier passe dans l'ère moderne de la confiance numérique au sein de l'économie réelle. Les sociétés participent à la décentralisation des usages d'hier et permettent de faire évoluer les métiers dans l'innovation numérique sans jamais participer à leur destruction.