Raptoreum:
Un Système Flexible Pour la Création et le Transfert de "*Futures*", d'Actifs et de Contrats.

Le mot Raptoreum est issu de la combinaison de Ravencoin et Ethereum. Un corbeau (*Raven*) étant considéré comme un rapace (*Raptor*) "honoraire", et étant donné que nous sommes un *fork* de Ravencoin ajoutant des *smart contracts*, ce nom est parfaitement adapté. Un grand merci du fond du coeur aux développeurs de Bitcoin et Ravencoin, sans qui nous n'aurions pas cet excellent code-base à partir duquel bâtir.

Introduction

Raptoreum a débuté avec une idée assez simple: intégrer des *smart contracts* qui permettraient des transferts *on-chain* sur le code-base Ravencoin sans avoir recours à un tiers de confiance (adieu les places de marché centralisées), avec toutefois l'automatisation des actifs et RTM (Raptoreum). Le projet a rapidement évolué en ajoutant des fonctionnalités innovantes qui non seulement enrichissent la couche des actifs, mais en adoptant également des fonctionnalités susceptibles de profiter à d'autres projets basés sur la technologie blockchain. Raptoreum est conçu pour permettre à quiconque de créer rapidement et facilement un actif digital et de le transférer en toute sécurité via des transferts *on-chain* sans avoir recours à un de tiers de confiance.

Raptoreum est un *fork* du code source Ravencoin et hérite donc de ses fonctionnalités actuelles et futures telles que les actifs numériques, le vote, les dividendes et la messagerie. Nous étendons davantage les capacités des actifs en leur ajoutant les fonctionnalités suivantes:

- la faculté d'enfermer un montant de X pièces ou actifs numériques à l'intérieur d'un actif. Les pièces étant libérés à un numéro de bloc ou horodatage déterminé.

- des transferts d'actifs et jetons natifs numériques *on-chain* sans tiers de confiance VIA des *smart contracts*.

Ces fonctionnalités additionelles élargissent les faculté et facilité d'utilisation de la couche des actifs Raptoreum à une plus grande variété d'industries dans le cadre des Applications Distribuées. Les DAPPs possèdent un rôle crucial pour favoriser l'adoption de masse et Raptoreum espère aider à fournir des alternatives et possibilités supplémentaires pour les développeurs de DAPP.

L'un de nos objectif est non seulement de générer des idées novatrices pour Raptoreum, mais également d'apporter notre contribution à la communauté crypto en général et à la

réussite d'autres projets basés sur la technologie Blockchain, avec des fonctionalités en open-source que chacun est libre d'utiliser.

Prysm, qui est notre système de protection contre les attaques 51% / double dépense sera en open-source et disponible pour quiconque souhaiterait l'utiliser. Les évènements récents dans la cryptosphère montrent à quel point ce type de fonctionalité est important. Il n'y aura pas de garantie que cela sera 100% infaillible, mais aucun système nécessitant un consensus ne peut prétendre l'être.

Problèmatiques que Raptoreum Tente de Résoudre

Encourager l'Adoption de Masse: L'un des plus gros enjeu auquel les Cryptos dans leur ensemble sont confrontés reste l'adoption massive. Raptoreum aide à résoudre ce problème en offrant à quiconque la possibilité d'émettre des jetons numérique de ce que bon leur semble, et ce de manière simple et intuitive. En plus de cela, nous offrons la flexibilité et les capacités des *smarts contracts*, ce qui permet aux développeurs de DAPP de créer facilement des applications distribuées couvrant une vaste gamme d'utilisation pouvant aller des jeux de hasard jusqu'à l'éducation.

Résistance aux FPGA et ASIC: Raptoreum s'engage à maintenir les ASIC et FPGA hors du réseau afin de conserver la possibilité de minage par tous, sans que cela ne nécessite l'utilisation d'un matériel spécialisé très coûteux.

Dans le cadre de nos efforts permettant de rendre ceci possible, nous allons déployer notre propre algorithme de Preuve de Travail (*POW*) baptisé "GhostRider" [3]. GhostRider utilise la sélection aléatoire du x16r associée au CNv1-8. Il en résulte un algorithme dissuadant les ASIC et les FGPA en les rendant bien trop onéreux pour un gain minime à la clé.

En plus de ça, nous développons la possibilité d'ajuster l'algorithme "à la volée". Cela permettra à Raptoreum de modifier rapidement certains paramètres algorithmique avec pour effet de se débarasser des ASICS et FGPA si ceux-ci venaient à être repérés sur le réseau, sans avoir à recourir au processus complet de *fork* qui reste coûteux et précaire.

En ce qui concerne le processus de *fork on-chain*, un point peu discuté mais crucial dans l'ensemble des débats concernant les *forks*, est que chaque fois qu'une chaine est forkée, la sécurité diminue dans la mesure où l'on peut commencer à déterminer des points de corrélation entre la chaîne originale et ses ramifications. Cela est dû au fait que des clés privées, et autres, sont utilisés sur plusieurs chaînes, étant donné que les mêmes adresses figurent sur les deux chaînes à partir du *snapshot*. En gardant cela à l'esprit, RTM ne planifie qu'un seul *fork* afin d'activer la couche des actifs numériques environ 12 mois après son lancement.

Protection Contre les 51% et Double Dépense: En 2018, le nombre d'attaques 51% fructueuses a fortement augmenté et cette tendance devrait se poursuivre en 2019. En 2018, 20 millions de dollars ont été volés en raison de ces attaques [1], et à cela s'ajoutent des atteintes portées à la réputation des projets qui peuvent être dévastatrices. Le coût nécessaire pour effectuer une attaque 51% est inférieur à ce que la plupart imaginent [2]. Raptoreum travaille sur un système de protection contre cela dénommé "Prysm" qui sera en open-source et dont tout le monde pourra profiter. Les noeuds-service (s*ervicenodes*) sont responsables de la gestion de Prysm.

Hyper Inflation: Les masternodes, bien qu'étant des outils puissants, peuvent provoquer une hyper inflation susceptible d'entrainer le crash d'une monnaie sur les marchés et causer des dommages irreversibles à un projet. Raptoreum adopte un système original de cautions et de récompenses progressant par paliers afin d'éviter cet écueuil (voir **Servicenodes**).

Mise à l'échelle (*scaling*): Raptoreum n'ajoute pas des contrats comme Ethereum. A la place, les servicenodes seront utilisés pour fournir ce service, ce qui procurera une meilleure scalabilité et évitera les problèmes de mise à l'échelle qu'Ethereum a pu rencontrer.

Servicenodes

Les servicenodes jouent plusieurs rôles cruciaux sur le réseau Raptoreum. Ils sont responsables du stockage et de l'exécution des *smart contracts* ainsi que de l'exécution de PRYSM, notre système de défense à 2 volets contre les attaques 51% / double dépense. Raptoreum utilise une courbe d'émissions originale basée sur un système de servicenodes avec des cautions et des récompenses progressant par paliers. Ainsi, on évite l'hyper inflation qui porte atteinte à beaucoup d'autres monnaies qui utilisent les Master/Service-nodes.

Hardware: Afin d'exécuter cet éventail de fonctions, les spécifications prévisionnelles (à confirmer) pour héberger un servicenode devraient être une configuration de 4 core à 8 Go.

Raptoreum Servicenodes: En ce qui concerne les récompenses des noeuds, elles ne fonctionnent pas tout à fait de manière traditionelle, dans la mesure où il a été prouvé à maintes reprises que cela avait pour conséquence de compromettre la viabilité des projets sur le long terme. Nous avons opté pour l'approche consistant à les rémunérer en fonction

des services rendus au réseau, ce qui s'oppose à ce que font nombre d'autres monnaies actuellement.

Les noeuds exécutant PRYSM seront payés par les "frais d'actifs", qui sinon seraient brûlés lors de leur création, et qui s'ajoutent aux 5% de récompenses de bloc. Oui, cela aura pour effet de supprimer une partie du caractère déflationiste lié autrement au processus de création d'actifs. Cependant, cela permettra dans le même temps de faire fonctionner une chaîne dont la réorganisation sera quasiment impossible au-delà de quelques blocs, permettant ainsi des transferts à la fois rapides mais également sûrs.

Les noeuds exécutant la couche des contrats recevront 15% de récompenses de bloc.

Récompenses et RSI globaux des service nodes: Dans l'optique d'un réseau pleinement développé de 4 à 6000 service nodes avec une caution maximale de 1,9 millions de RTM, le retour sur investissement annuel devrait se situer entre 8 et 12% en fonction du nombre exact de noeuds sur le réseau, etc… Il ne s'agit pas là d'un niveau de rentabilité déraisonnable, étant donné que les coûts d'installation et d'exploitation d'un noeud ne sont pas négligeables.

Structure des récompenses:

Block #	Block Reward	Miner Reward	Contract layer Reward	PRYSM Reward	Developer reward	Service Node collateral
0-719	4	1	1	1	1	500,000
720-5,759	5,000	4,750	0	0	250	500,000
5,760-85,767	5,000	3,750	750	250+ asset fees	250	500,000
85,768-128,291	5,000	3,750	750	250+ asset fees	250	600,000
128,292-170,815	5,000	3,750	750	250+ asset fees	250	700,000
170,816-213,339	5,000	3,750	750	250+ asset fees	250	800,0000
213,340-255,863	5,000	3,750	750	250+ asset fees	250	900,000
255,864-298,387	5,000	3,750	750	250+ asset fees	250	1,000,000

298,388-340,911	5,000	3,750	750	250+ asset fees	250	1,150,000
340,912-383,435	5,000	3,750	750	250+ asset fees	250	1,300,000
383,436-425,959	5,000	3,750	750	250+ asset fees	250	1,450,000
425,960-468,483	5,000	3,750	750	250+ asset fees	250	1,600,000
468,484-511,007	5,000	3,750	750	250+ asset fees	250	1,750,000
511,008-553,531	5,000	3,750	750	250+ asset fees	250	1,900,000
553,532-574,793	4,990	3,742.5	748.5	249.5+ asset fees	249.5	1,900,000
574,794-596,055	4,980	3,735	747	249+ asset fees	249	1,900,000
597,056-xxx,xxx	4,970	3,727.5	745.5	248.5+ asset fees	248.5	1,900,000

Sources:

[1] 2018 51% and double spend attacks: https://thenextweb.com/hardfork/2018/10/23/cryptocurrency-51-percent-attacks/

[2] Cost to perform 51% attacks: https://www.crypto51.app/

[3] Raptoreum GhostRider Explained: https://medium.com/@kawwwoin/raptoreums-ghostrider-algorithm-explained-93f1f8070158

(Traduction française: Duckavenger)