Un Marché Décentralisé de l'Intelligence Sur Les Menaces Cybernétiques.

POLYSWARM

Table of Contents

PolySwarm en 60 Secondes

PolySwarm est un marché décentralisé de l'intelligence sur les menaces cybernétiques rendu possible grâce aux smart contrats Ethereum et la technologie blockchain.

PolySwarm incite à l'innovation rapide des logiciels antivirus et intelligence automatisée des menaces cybernétique, un marché qui a un chiffre d'affaire de $8,5 Milliards de dollars par an[1]. PolySwarm offre une incitation économique précises qui récompense les renseignements rapide et précis sur les menaces liées aux fichiers, au trafic réseau et aux URLs.

PolySwarm définit un écosystème de détection des menaces en temps réel impliquant des entreprises, des consommateurs, des fournisseurs et des experts en sécurité géographiquement diversifiés. Les experts développent et perfectionnent des «micromoteurs» concurrents qui enquêtent de manière autonome sur les dernières menaces, essayant de surpasser leur concurrence. La «preuve de travail» de PolySwarm est la précision de la détection des menaces: le marché récompense les experts les mieux à même de défendre les entreprises et les utilisateurs finaux.

Relativement au marché ponctuel d'aujourd'hui, PolySwarm réduira la barrière à l'entrée, offrira des options de couverture plus larges, découragera les efforts de duplication et assurera l'interopérabilité entre les produits et les flux de renseignements sur les menaces.

Sur le plan économique, PolySwarm fonctionne comme un jeu de compétition pour les compétences sur un marché de prédiction[2] avec des milliers de micromoteurs (“travailleurs”) qui étudient les dernières évolutions des logiciels malveillants à la vitesse de la machine.

PolySwarm sera développé par **PolySwarm Pte. Ltd.** avec un financement provenant de la vente de jetons utilitaires **Nectar** ("NCT") compatibles ERC20.

En tant que marque utilitaire, PolySwarm décourage économiquement la spéculation Nectar en récompensant la participation honnête du marché par la collecte et la distribution des frais (détaillés à la page 6) aux participants actifs à valeur ajoutée.

---

1 Jefferies Cyber Security Primer. January 18, 2017.
2 https://en.wikipedia.org/wiki/Prediction_market

Historique

Les entreprises d'aujourd'hui dépendent d'un mix ad hoc d'abonnements antivirus, de sources d'informations sur les menaces et de moteurs d'analyse dynamiques variés pour se défendre contre une cyber activité conflictuelle évolutive. Les utilisateurs doivent peser les avantages et désavantages présentés par chaque solution et décider de l'ajustement du moins pire pour leur environnement.

Le marché d'aujourd'hui décourage les solutions qui offrent une couverture large des menaces.

Les solutions d'aujourd'hui se concentrent sur une zone de confort des menaces – un résultat direct de l'économie de marché d'aujourd'hui.

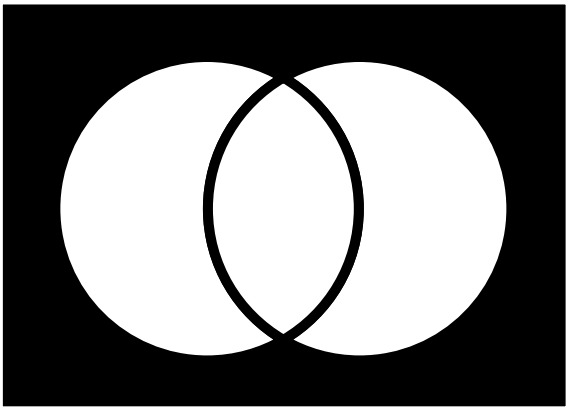


Figure A: Le rectangle noir représente toutes les menaces qu'une compagnie peut rencontrer; les cercles blancs sont les produits antivirus numéro 1 and 2 respectivement.

C'est facile(et peut-être justifiable) d'ignorer un une solution antivirus qui ne détecte WannaCry[3], mais en faisant ça, le marché d'aujourd'hui récompense le couvrage redondant parmis les vendeurs- un marché inefficient qui cause une duplication des coûts. Ceci est une tragédie classique de la situation courant.

Similairement, envisagez un fournisseur qui choisit de développer une expertise en dehors de cette zone de confort. Si la zone de confort est définie par l'ensemble des menaces rencontrées par la plupart des entreprises, les ventes de ce fournisseur spécialisé seront difficiles. Comment allez vous convaincre un potentiel

3 https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

client qu'il ferait face à des logiciels malveillants dont vous êtes uniquement qualifiés pour détecter, prévenir ou atténuer?

Finalement, les défenseurs ne peuvent pas mélanger et faire correspondre de nombreuses solutions actuelles, ce qui rend la combinaison des couvertures impossible dans de nombreux scénarios.

En revanche, PolySwarm encouragera un écosystème de large couverture alimenté par des milliers de travailleurs “micromoteurs”, écrits par des experts en sécurité géographiquement diversifiés.

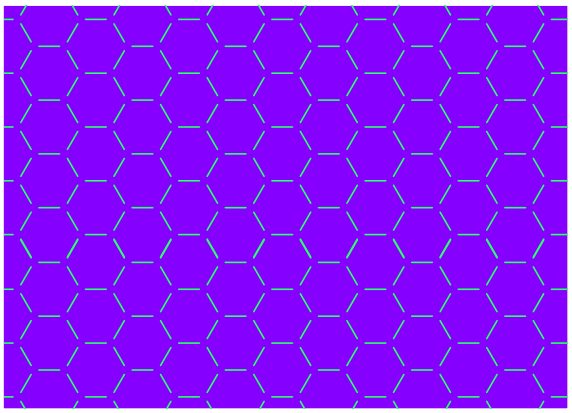


Figure B: PolySwarm encouragera un écosystème générant une couverture étendue des menaces.

PolySwarm fournit une source de revenu légitime pour les experts en sécurité.

Lorsque l'économie locale ne peut pas supporter un travail honnête, certains experts en sécurité développent des rançongiciels, exploitent des bots et utilisent leurs compétences pour le mal. PolySwarm offre une alternative sans région: une récompense sans souci pour un travail honnête. Les experts se font concurrence pour rendre Internet plus sécurisé.

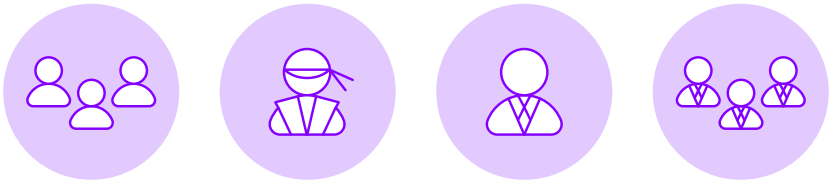
PolySwarm prioritize le besoin des utilisateurs.

Le marché de PolySwarm dirige les incitations économiques là où cela compte le plus: vers une détection précise des malveillants ("intelligence sur les menaces"). L'exactitude est déterminée par un nouveau processus que nous appelons Consensus Négocié.

En bref, PolySwarm fournit aux utilisateurs un accès rapide à une vaste et participative expertise de sécurité. Si vous avez besoin de diagnostiquer rapidement un fichier suspect? Juste Swarm It™ (Swarmez le).

Réinventer le Marché de l'Intelligence sur les Menaces

Les jetons Nectar ("NCT") de PolySwarm forment la base d'un nouveau marché qui introduit de nouveaux instruments pour satisfaire la demande d'affirmations précises et opportunes concernant la possible nuisance des fichiers, le trafic réseau et les URL, collectivement appelés Artefacts. Ces nouveaux instruments sont structurés pour stimuler directement l'innovation dans l'espace de l'intelligence sur les menaces grâce à une boucle de rétroaction basée sur des résultats correct.



Enterprises **Experts** **Ambassadeurs** **Arbitres**

PolySwarm utilise des frais pour décourager le spam et encourager un engagement commercial honnête et actif. Les frais sont évalués sur les types de transactions qui peuvent être utilisés abusivement pour le spam, puis distribués aux participants actifs de l'écosystème; ceux qui introduisent des artefacts et déterminent la vérité sur le des artefacts malveillants. Cette participation est mesurée en mode fenêtre glissante, “retraite” les anciennes contributions au marché, ce qui incite à la poursuite de la participation au marché.

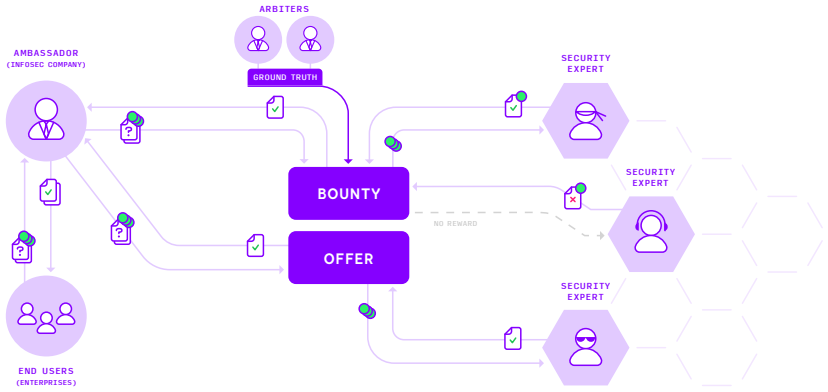
PolySwarm 1.0 (et ce document) se concentrera exclusivement sur la détermination booléenne (malveillante/bénigne), mais l'équipe de PolySwarm a des plans plus ambitieux au delà de juste améliorer la détermination booléenne des malveillances. Pendant le développement de PolySwarm 1.0, l'équipe étudiera des méthodes pour inciter à la production de métadonnées telles que la famille de logiciels malveillants et comment les concepts de base de PolySwarm tels que la conception de marché de smart contracts, Consensus Médiatisé et la sécurité de l'information peuvent changer les marchés reliés tels que les primes de bogues[4].

Avant d'introduire les instruments de PolySwarm, nous présentons les classes de participants qui les utiliseront.

---

4 “HackerOne but distributed, pseudonymous, and unfettered by jurisdictional encumbrances. Powered by blockchain.” Non couvert par ce document.

Les Participants



Utilisateurs: Utilisateurs professionnels et particuliers avec des artefacts suspects. Les utilisateurs participent au marché de PolySwarm par l'intermédiaire des Primes et des Offres (plus de détails sur ces derniers dans un instant) et extraient des classifications rapides et correctes des inimitiés.

Experts en sécurité ("Experts"): Experts en logiciels malveillants géographiquement diversifiés et aussi ingénieurs du reverse engineering. Les experts dissèquent les derniers artefacts suspects et maintiennent des moteurs de détection ("Ouvriers" ou "Travailleurs") connectés à PolySwarm qui déterminent une mauvaise intention. Les experts s'engagent à "Assertions", et déclarations publiques qui reflètent les résultats de leur analyse dans l'intimité de l'Artefact. Ceux qui ont commis une assertion précise sont récompensés (en NCT) pour leurs efforts.

C'est en fait ça en ce qui concerne les participants principaux. La simplicité est bien, mais c'est loin de toute l'histoire de PolySwarm. Techniquement, PolySwarm pourrait travailler uniquement avec ces deux classes de participants. D'un point de vue réaliste, ce ne sera pas le cas, car la plupart des utilisateurs préfèreront externaliser le processus d'interfaçage avec le marché de PolySwarm. Avant d'aller plus loin, nous vous présentons maintenant les Ambassadeurs (une autre classe de participants) et une certaine sous-classe de ces Ambassadeurs.

Ambassadeurs: Des entreprises qui permettent aux utilisateurs finaux de bénéficier du marché PolySwarm. Les Ambassadeurs collectent des fiat traditionnels (par exemple des frais d'abonnement) et des artefacts suspects auprès de leurs clients (utilisateurs) et introduisent des primes et des offres sur le marché au nom de leurs clients. C'est la responsabilité des Ambassadeurs de distiller les assertions de divers experts dans un verdict simple assertant que l'artefact est malveillant ou bénigne et les livrent à leurs clients..

Une approche triviale, peut-être naïve pour cette distillation pourrait être de simplement faire la moyenne des affirmations fournies par les experts. Il est cependant improbable qu'un tel algorithme puisse concurrencer favorablement contre une analyse Bayésienne, sans parler de l'implication d'experts humains. Nous prévoyons que les entreprises d'antivirus et de l'intelligence sur les menaces participeront au marché de PolySwarm en tant qu'entreprise ambassadrices, augmentant ainsi leur expertise interne grâce au diagnostic des artefacts suspects par PolySwarm.

Du point de vue de l'utilisateur, la mise à niveau vers une protection protégée par PolySwarm est un processus facile: choisissez un Ambassadeur réputé et payez des frais d'abonnement.

La réputation d'un Ambassadeur est basée sur la performance passée de verdict par rapport à la vérité terrain. Les Ambassadeurs sont encouragés à rendre leurs verdicts publics en raison de leur désir inhérent de bâtir leur réputation et d'attirer de nouveaux clients, ainsi que de profiter d'une réduction sur les frais (ce processus est détaillé plus tard). Ces verdicts publics permettent la création d'une "carte de pointage" de l'Ambassadeur qui évalue les performances réelles par rapport aux artefacts non synthétiques avec des données qui ne sont tout simplement pas disponibles sur le marché actuel[6].

Arbitres: Des Ambassadeurs de haut niveau qui qui ont la responsabilité de déterminer la vérité terrain d'un fichier malveillant. Un certain pourcentage d'Ambassadeurs (en termes de frais générés) seront considérés comme des "arbitres".

Pendant le développement, PolySwarm attribuera l'Arbitrage à des fournisseurs réputés qui fournissent l'intelligence sur les menaces et sont prêts à maintenir un engagement fréquent avec l'équipe de PolySwarm pour identifier et corriger les bogues de la plateforme et

---

5 Kantchelian, Alex, et al. "Better malware ground truth: Techniques for weighting anti-virus vendor labels." Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. ACM, 2015.
6 L'analogue le plus proche est AV Comparatives **(https://www.av-comparatives.org/).**

à susciter l'intérêt pour l'écosystème.

Une fois que PolySwarm 1.0 est prêt pour le lancement, ces Arbitres désignés devront maintenir des volumes d'Ambassadeurs de haut niveau pour maintenir leur statut d'Arbitre.

Marchés de prédiction, Arbitres et consensus négocié

Dans l'écosystème PolySwarm, les experts en sécurité développent des travailleurs de micromoteurs qui compétissent pour enquêter rapidement et précisément les artefacts suspects. Cette enquête se déroule à la vitesse de la machine – bien avant que le verdict sur le statut de malveillance d'un artefact ait été établi.

Ce design partage certaines similitudes avec les marchés de prédiction, c'est-à-dire récompenser des assertions basées sur l'exactitude, mais diffère dans deux points critiques:

1. **Pas besoin de données futures pour classifier un artefact.** La réponse “correcte” pour savoir si un artefact est malveillant peut être toujours déterminée avec certitude dès que les données sont accessible aux travailleurs. PolySwarm a un design basé sur les compétences où rien n'est laissé au hasard[7].

2. **La détermination de la vérité nécessitera toujours une expertise.** Cela est contraire à “l'observabilité universelle” des marchés de prédiction (y compris les crypto-marchés comme Augur[8]) qui comptent sur des participants non qualifiés pour observer et enregistrer les événements au fur et à mesure qu'ils surviennent.

Point #1 Polyswarm est dissuasif au jeux de hasard deterrent[9].

---

7 PolySwarm a un design basé sur les compétences où rien n'est laissé au hasard en théorie. Mais en pratique, au moins deux événements pourraient introduire une incertitude: (1) Les arbitres déterminent incorrectement la vérité terrain entraînant la distribution des récompenses aux mauvais experts. (2) L'analyse de l'expert est correcte selon la vérité terrain, mais l'expert n'est pas d'accord sur les limites de la malveillance – un problème de sémantique plus grand que PolySwarm. Les adwares ou logiciels publicitaires sont-ils malveillants ou simplement des applications potentiellement indésirables? Aucune de ces variables ne nuit fondamentalement à la nature basée sur les compétences de l'écosystème PolySwarm.

8 https://augur.net/

9 Deviner, parier, jouer ou d'autres paris basés sur le hasard sur malveillance de l'artefact est mauvais pour tout le monde et PolySwarm est spécifiquement conçu pour être inhospitalier à cette mauvaise utilisation de la plate-forme.

Point #2 Quelle est la meilleure façon d'inciter les autorités à produire continuellement une vérité terrain?La réponse de PolySwarm est la classe d'Arbitre et un processus que nous désignons par Consensus Négocié.

Le Consensus Négocié est un paradigme de conception générique qui, nous l'espérons, trouvera sa place dans d'autres projets de design de marché. En bref, Mediated Consensus est une conception de marché qui confie une tâche critique à un sous-ensemble de participants. Ces participants:

1. Sont qualifiés pour la tâche (possèdent une expertise).
2. Ont leurs intérêts alignés sur la santé globale du marché (en évitant la tragédie des biens communs).

Nous avons conçu des arbitres pour satisfaire ces deux contraintes. Par définition, la classe Arbitre est définie comme les Ambassadeurs les plus actifs de l'écosystème PolySwarm à un moment donné.

En tant qu'Ambassadeurs, les clients sont invités par leurs clients à exprimer les affirmations de Security Experts en verdicts. Les clients leur font confiance pour posséder et exercer une expertise humaine automatisée et, au besoin, humaine. Ces entreprises ont déjà tout intérêt à maintenir un dossier public d'exactitude (Point 1).

Puisqu'ils sont les plus actifs Ambassadeurs, les arbitres ont le plus à gagner ou à perdre si l'écosystème PolySwarm est honnête ou malhonnête. Leur grand intérêt et confiance en l'écosystème s'alignent à leurs intérêts financiers sur la santé du marché (Point # 2).

Nous avons conçu les frais comme une défense supplémentaire contre les abus du statut d'Arbitre tels que la collusion entre Arbitre et Expert de Sécurité.

Détermination de la Vérité terrain

La plupart des détails techniques du processus de vote Arbitre sont intentionnellement laissés indéfinis à ce moment. La raison en est simple: les spécificités du processus décisionnel d'Arbitre reposent sur les spécificités de pratiquement tous les autres processus PolySwarm – et nous attendons des variations dans d'autres processus.

Cela étant dit, nous prévoyons que les choix de conception de haut niveau suivants apporteront de la valeur dans ce processus:

1. Les Arbitres atteignent un consensus sur la vérité terrain par **vote de la majorité.**

2. Ces votes sont **minés en masse sur la chaîne Ethereum** (plusieurs votes par cycle), ce qui permet d'économiser du temps et de l'argent (gaz Ethereum) pour l'écosystème PolySwarm.

3. Pour encourager leur participation, les **Arbitres sont récompensés avec des frais pour voter sur les vérités fondamentales.**

4. **Les Arbitres peuvent s'abstenir de voter sur un artefacts particulier.** Ils peuvent choisir cela par exemple, s'ils se sentent non-qualifiés pour déterminer qu'un artefact est malveillant.

5. Si nécessaire, **le privilège de vote** des Arbitres est **automatiquement** délégué à d'autres Ambassadeurs (en ordre de volume) pour **s'assurer d'un quorum** pour déterminer la vérité terrain.

6. Si nécessaire, **nous nous attendons à des participants** qui questionnent les déterminations des arbitres comme **c'est le cas aujourd'hui:** avec un article de blog ou un document technique décrivant la nature malveillante ou bénigne d'un artefact qu'une autorité tel qu'un arbitre a mal différencié: une boucle de rétroaction extern.

L'équipe de PolySwarm développera itérativement les détails sur les structures de vote et la motivation des arbitres pendant le développement. Nous espérons à ce que les premières réactions d'Arbitres soient déterminantes pour cette conception.

Les sujets de recherche incluent, mais ne sont pas limités à:

- Pourcentage minimum de quorum d'arbitres
- Procédure de report de l'arbitre (pour quand le quorum ne peut être atteint
- Structure de récompense appropriée
- Promotion à la détermination de la vérité terrain en temps opportun, par ex. Seuls les premiers arbitres à voter reçoivent une récompense

- Pénalité pour non-participation, par exemple Les arbitres doivent voter sur la vérité du terrain pour X% des artefacts pendant une période provisoire, sinon leur statut d'arbitre est révoqué
- (Si nécessaire) des moyens de dissuasion supplémentaires contre les incitations perverses

Les Instruments

PolySwarm propose deux instruments principaux aux utilisateurs et aux Ambassadeurs[10] qui ont accru l'efficacité du marché des renseignements sur les menace:

OFFER

Les Offres PolySwarm: Les demandes adressées directement à des experts en sécurité réputés pour leur prédiction des menaces. PolySwarm fournit un accès sans friction à des milliers chercheurs de ce type, permettant des accords traditionnels de partage d'informations avec des participants non traditionnels. Cette interaction se produit dans les chaînes d'offre de style Raiden[11]–(détaillés plus tard). Une fois les chaînes sont établis, les offres fournissent une latence à l'échelle de milliseconde pour l'enquête des artefacts.

BOUNTY

Les Primes de PolySwarm: Les Primes PolySwarm: une affiche "Wanted" de style Wild-West avec le contenu d'artefact qui l'accompagne (par exemple, Wanted: This Artifact: Malicieux ou Bénigne? Récompense: 1000 NCT). Les experts en sécurité se font un nom (construisent la réputation) en compétissant avec succès pour les primes. Aucun analogue direct n'existe sur le marché d'aujourd'hui.

Les offres sont les plus proches analogies du marché de diagnostics sur commande et fonctionnent avec une latence de l'ordre de la milliseconde.

Les Ambassadeurs envoient des offres et des artefacts directement aux experts en sécurité choisis, le cas échéant en vertu d'un accord de non-divulgation. Chaque Expert choisit d'accepter ou non l'Offre en fonction de sa confiance dans une Assertion de rendu précise pour l'Artefact fourni. Les experts peuvent choisir de refuser s'ils

---

10 Ci-après, les Utilisateurs et les Ambassadeurs sont abrégés en Ambassadeurs. Les Utilisateurs peuvent agir comme leur propre Ambassadeur. Nous espérons la participation de certaines grandes entreprises de cette manière.

11 http://raiden.network/

ne sont pas sûrs de ne pas nuire à leur réputation. Si l'Expert accepte l'Offre, l'Expert s'engage à fournir à une Assertion pour diagnostique la malveillance de l'artefact en temps opportun. La collection de jetons et les récompenses pour tous les instruments sont gérés et exécutés entièrement par des smart contrats distribués.

Le lancement d'une offre nécessite une certaine familiarité avec les experts les mieux équipés pour disséquer l'artefact en question. Pour faciliter ce jumelage, les experts font la promotion de leurs spécialités via des listes dans le registre des travailleurs de PolySwarm – l'analogie de PolySwarm à au registres Ethereum dApp[12] et établissent une réputation publique en participant avec succès à des primes similaires.

Les primes sont moins chères que les offres et ne nécessitent aucune connaissance préalable d'experts spécifiques, mais les primes ne sont pas pour tout le monde.

Tout d'abord, les primes doivent être minées dans un bloc Ethereum, qui se produit environ toutes les 15 secondes – de loin le coût en temps dominant dans cet arrangement. Deuxièmement, lorsque vous placez une Prime, l'Artefact doit être rendu public[13]. Après tout, les affiches "Wanted" de Wild-West ne seraient pas d'une grande aide si elles n'étaient pas affichées dans un endroit public avec toutes les informations connues. De la même manière, les Bounties représentaient un engagement public, intelligent (comme dans le contrat) pour récompenser les fournisseurs d'informations qui mènent à la mise en quarantaine ou à l'exonération d'Artefacts. Les primes constituent également une composante essentielle de la boucle de rétroaction qui établit la vérité terrain.

Récompensant la Précision

Contrairement au marché actuel, le marché de PolySwarm offre des récompenses précises basées uniquement sur l'exactitude de l'intelligences sur les menaces, incitant les experts à optimiser leur précision de détection (faux positifs et faux négatifs) et permettant aux Ambassadeurs d'extraire la valeur maximale pour leurs clients. PolySwarm définit la précision comme un accord (ou non) entre les assertions des experts et la vérité terrain définie par l'Arbitre.

Cette boucle de rétroaction de précision est conduite par les primes de PolySwarm. Chaque prime récompense les experts qui rendent

12 Voir la section Registre de Travailleurs pour plus de détails.
13 Vrai pour PolySwarm 1.0, pas nécessairement vrai dans les itérations futures. Voir le document Confidentialité de l'Artefact.

une assertion précise et pénalise les experts qui font une assertion inexacte – tout en évitant l'introduction d'incitations à la collusion entre les Ambassadeurs et les experts[14]. Les offres PolySwarm offrent un moyen pratique d'atteindre les relations d'affaires traditionnelles 1:1 (entre deux parties), mais ne tiennent pas compte l'exactitude de cette équation.

La vérité terrain est produite et utilisée sur le marché de PolySwarm de la manière suivant:

1. Un Ambassadeur place une prime sur un artefact, en soumettant une frais pour le fair.

2. Plusieurs experts font leurs assertions sur cet artefact avant le délai d'assertion de la prime. Chaque assertion est accompagnée d'un montant NCT choisi par l'expert (une “offre”) qui reflète la confiance de l'expert dans leur assertion. Un frai est assigné en tant que pourcentage de cette “offre”. Ces affirmations sont confidentielles jusqu'au délai de l'assertion.

3. L'Ambassadeur décide le verdict, en tenant compte des assertions des experts, selon ce qu'il juge opportun, et remet ce verdict à leur client. L'Ambassadeur est encouragé à rendre ce Verdict public afin d'élever sa réputation et bénéficier d'une réduction sur les Frais (détaillée plus tard).

4. Plus tard (par exemple, 7 jours après le placement de l'Artefact en Prime), les Arbitres ont l'opportunité de voter pour savoir si l'Artefact est en fait malveillant ou bénigne. Cette vérité terrain déterminée plus tard N'EST PAS UN BLOQUEUR POUR RETOURNER RAPIDEMENT DES VERDICTS DES ARTEFACTS. En d'autres mots, les Ambassadeurs n'ont pas besoin (et ne devraient pas) d’attendre la détermination de la vérité terrain avant de le retourner à leur client.

5. Un groupe d'Arbitres détermine le statut de vérité terrain sur l'Artefact. Les détails de ce vote pour fonder le processus de conversion de la vérité n’est pas encore déterminé. Les arrangements possibles sont un vote majoritaire simple ou un vote majoritaire proportionnel (par exemple, basé sur le montant de la participation au marché). Ces spécificités seront déterminées lors du développement du prototype.

6. Avec la vérité terrain établie, le contrat NCT de prime attribué aux experts qui ont rendu des assertions précises. Le montant de NCT attribué est proportionnel au montant de l'offre de l'expert par rapport au nombre total d'offres précises.

---

14 Cela inclut l'intérêt potentiel de connivence entre les experts et les arbitres qui votent pour leurs propres Primes. La structure des frais de PolySwarm est conçue de telle sorte qu'aucun Arbitre ne peut influencer suffisamment la vérité terrain pour faire en sorte qu'un expert en connivence reçoive une prime supérieure au coût de l'arbiter pour semer un doute dans le marché.

Il semblerait qu'un marché classique de prédiction conviendrait bien ici: les experts rendent des assertions et, à une date ultérieure, ces assertions sont comparées à la vérité, déclenchant finalement des récompenses et des pénalités basées sur leur exactitude. Le problème pour PolySwarm est que les marchés de prédiction classiques supposent implicitement une source de vérité vérifiable par tous les participants. Un marché de prédiction qui demande qui va gagner une élection ou si le prix de l'or dépassera un certain montant d'un certain jour est facilement réglé parce que tous les participants peuvent vérifier ces points de données après la période de prédiction: Qui a gagné l'élection? L'or a-t-il dépassé le prix final?

La détermination de la malveillance d'un artefact suspect exige une expertise qui n'est pas uniformément partagée entre les participants de PolySwarm. Cette énigme a des analogues aux marchés de prédiction appliqués aux diagnostics[15] médicaux, où les médecins apportent différents perspectives d'expertise à défendre.

PolySwarm a confiance au verdict des Arbitres dans la détermination de la vérité au terrain aux arbitres. Dans le marché actuel, le rôle de l'Arbitre est effectivement fait par les sociétés traditionnelles d'antivirus. Ces entreprises "votent" (et sont tenus publiquement responsables) sur "la vérité terrain" via des services comme VirusTotal. Dans le marché de PolySwarm, l'ensemble des arbitres n'est déterminé que par la participation au marché, ce qui permet à de nouveaux participants de changer l'établissement.

En résumé, nous croyons que ce processus incite correctement les arbitres à engager des ressources pour faire preuve de diligence raisonnable lorsqu'ils déterminent la vérité au profit du marché dans son ensemble.

Ce concept d'un groupe d'élite de “vérificateurs” de la vérité terrain est applicable à d'autres secteurs. Nous prévoyons que d'autres exploreront la faisabilité de l'utilisation de ce mécanisme dans d'autres plateformes de crypto-jetons qui exigent des connaissances spécialisées pour arriver à la vérité terrain.

15 Kurvers, Ralf HJM, et al. "Boosting medical diagnostics by pooling independent judgments." Proceedings of the National Academy of Sciences (2016): [201601827].

Frais

Les frais sont évalués pour diverses transactions sur le marché de PolySwarm et sont conçus pour atteindre deux objectifs:

1. **Promouvoir l'efficacité sur le marché de PolySwarm en encourageant des actions qui réduisent au minimum le coût de l'Ethereum.** Des frais à taux fixe sont appliqués aux transactions PolySwarm pour décourager les comportements qui généreraient des transactions superflues (y compris les transactions de spam) et engendront donc des coûts de inutiles sur le marché. Le besoin pour PolySwarm de réduire ces frais indépendamment du coût de l'Ethereum est l'une des raisons pour lesquelles la création de NCT est essentielle à l'existence du marché de PolySwarm.

2. **Récompenser les participants au marché PolySwarm actifs en proportion de leur participation (honnête).** Les frais sont attribués aux participants qui utilisent activement l'écosystème PolySwarm via l'introduction d'Artefacts (Ambassadeurs plaçant des primes) et la détermination de la vérité sur l'erreur des artefacts (Arbitres atteignant un accord sur la vérité).

Pendant le développement de la communauté, l'équipe de PolySwarm mettra en œuvre les structures de frais présentées ci-dessus, répétant au besoin pour mieux encourager un bon marché.

Frais de placement de primes Payés par Les Ambassadeurs

Quand un Ambassadeur poster une prime sur le marché de PolySwarm, les frais suivants s'appliquent aux fonds détenus dans le smart contrat:

1. **Un frais fixe de soumission.** Ces frais fixes encouragent l'Ambassadeur à regrouper plusieurs artefacts en une seule prime, ce qui réduit la pression sur le réseau et les coûts pour tous.

2. **Un frais proportionnel au montant de la prime.** Les primes avec un montant de prime initial plus élevé attireront probablement plus de réponses d'experts. Ce frais proportionnel est évaluée en fonction de l'intérêt de l'expert (et du flux du réseau).

Frais de Prime d'Assertion Payés par les Experts

Quand un expert rend une assertion contre une prime, les frais

suivants sont imposés sur les fonds contenus dans le smart contrat:

1. **Des frais fixes d'assertion.** Cette redevance fixe désincite les assertions répétées qui peuvent ralentir le réseau.

2. **Des frais proportionnels à la somme de l'enchère.**

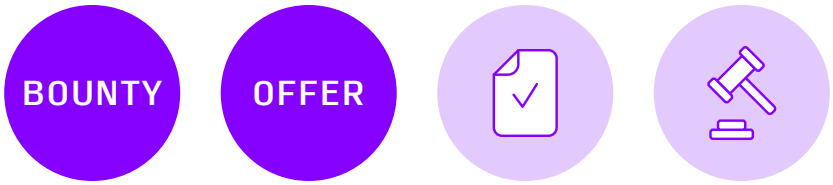
Règlement de Chaîne d'Offre: Frais des Ambassadeurs

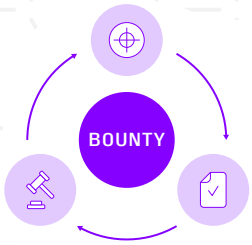
Les offres ont lieu dans les chaînes d'offre de style Raiden, établis directement entre les Ambassadeurs et les experts. Lorsqu'un Ambassadeur et ou un expert décide de régler sa chaîne d'offre dans la blockchain, les frais suivants sont attribués par la chaîne du smart contract:

1. **Un pourcentage du NCT net transféré sur la chaîne.** Ce frais sont imposé sur les jetons fournis par l'Ambassadeur lorsque la chaîne est ouverte. Lorsque la chaîne est fermée, ces frais sont remboursés à l'Ambassadeur proportionnellement au reste de jetons de chaîne inutilisés.

Détails des Protocoles

Dans les lignes suivantes, nous soulignons les détails sur les primes, offres, assertions et verdicts de PolySwarm. Les primes et les offres sont collectivement appelées listes PolySwarm. Une déclaration PolySwarm est l'une des suivantes: Prime, Offre, Assertion ou Verdict.





Cycle De Vie De La Prime

Quand un Ambassadeur veut placer une prime sur le marché, l'Ambassadeur poste une Déclaration par un appel à la prime smart contrat de PolySwarm.

La déclaration de prime contient les éléments suivants:

1. **Un Listing GUID:** Un identifiant global unique pour le listing. (GUID: globally-unique identifier).

2. **L'identité de l'Ambassadeur.** En forme de signature sur la Déclaration, vérifiable par toute personne en possession de l'adresse de l'Ambassadeur (les clés publiques sont dérivées des adresses).

3. **Un frais de placement de Prime.** Ce prix est placé dans le smart contrat intelligent en plus des frais de placement de primes et est attribué aux experts qui rendent des correctes et précises assertions (ou remboursés si les experts ne répondent pas). Ce montant comparable à des frais de transaction dans Ethereum ou Bitcoin et est utile pour attirer l'attention sur la Prime.

4. **The Bounty Amount.** This amount is placed into the smart contract alongside the Bounty Placement Fee and is awarded to Experts that render accurate Assertions (or refunded if no Experts respond). This amount is akin to a transaction fee in Ethereum or Bitcoin and is useful to call attention to the Bounty.

5. **Hash cryptographique de l'Artefact.** Configurable, mais actuellement SHA256. Ceci identifie uniquement l'Artefact.

6. **L'URI(Unique Resource Identifier) de l'artefact.** Dû aux coûts de stockage, les artefacts ne sont pas stockés sur la chaîne. Nous prévoyons un marché secondaire pour l'entreposage et la livraison d'Artefacts[16] et que certains Ambassadeurs choisiront de conserver une copie de tous les artefacts essaimés pour une analyse de compétition ultérieure.

7. **Délai de l'assertion:** date limite pour l'assertion. L'Ambassadeur peut choisir de raccourcir ou d'allonger les périodes d'analyse en fonction de leurs besoins pour un Artefact particulier. Les artefacts qui nécessitent une analyse plus

16 Des commentaire sur ce marché et d'autres marchés secondaires anticipés seront fournis plus tard.

approfondie requièrent probablement plus de temps (et sont susceptibles d'être plus élevés), alors que d'autres artefacts peuvent nécessiter un délai d'exécution rapide.

Une fois la prime est postée, les Experts détermineront si l'Artefact correspond à leurs compétences et si leur récompense offerte mérite leur attention. Cette récompense attendue est fonction de leur niveau de confiance concernant la malveillance de l'artefact.

Les experts qui choisissent de participer placent des offres sur leurs assertions qui représentent leur niveau de confiance (et leur tolérance au risque). Le montant de la prime plus la somme totale de toutes les offres inexactes sont attribués aux offres précises proportionnellement au montant de la soumission par rapport au montant total de la soumission.

Considérons l'exemple suivant (les frais sont ignorés ici pour plus de simplicité):

1. Un Ambassadeur place une Prime avec 2 NCT. Ces 2 NCT sont placés dans la Prime du smart Contract. Cependant, la sommes de ces 2 NCT constitue l'entièreté du potentiel “pot” à gagner pour une assertion correcte par les Experts.

2. Les Experts A et B étudient l’Artefact et décident après leur analyze que l’Artefact de la Prime est bénigne. Ils placent respectivement une enchère de 3 et 5 NCT sur leurs assertions.

3. Les experts C et D étudient l'Artefact et décident d'affirmer que l'Artefact de la Prime est en effet malveillant. Ils placent une offre de 1 et 4 NCT su leurs Assertions, respectivement.

4. Un moment plus tard, les arbitres établissent la vérité et déterminent que l'artefact était en fait malveillant. Les experts A et B ont donc rendu des assertions incorrectes; Les experts C et D ont rendu des assertions correctes.

5. La somme de la Prime plus les offres placées par les experts A et B constituent le "pot" qui est attribué proportionnellement aux experts C et D. Ce pot est de 2 + 5 + 3 = 10 NCT.

6. L'expert C a fait une assertion précise et son offre représentait ⅕ du montant total exact de la soumission. L'Expert C obtient sa soumission plus sa part du pot: 1 + ⅕ * 10 = 3 NCT.

7. L'expert D a fait une assertion précise et son offre représentait ⅘ du montant total de la soumission. L'expert D récupère sa soumission plus sa part du pot: 4 + ⅘ * 10 = 12 NCT.

Les Assertions de Primes contiennent:

1. **Listing GUID + Hash Cryptographique:** Une référence unique de la liste des primes.

2. **L'identité de l'Expert:** Encore une fois, comme une signature sur la déclaration.

3. **Frais d'Assertion:** Ces frais représentent un montant fixe + un pourcentage du montant de la soumission (voir la section “Frais”.

4. **Montant de l'Enchère.**

5. **L'assertion:** Une détermination booléenne "malicieuse" ou "bénigne"concernant la nature de l'artefact. Les assertions sont gardées secrètes jusqu'à l'expiration du délai d'assertion de Prime. Nous comptons utiliser des engagements aveugles + pour révéler la phase pour atteindre cette propriété.

6. **(Optionnel) Métadonnées:** Informations dérivées lors de la génération d'assertion et proposées en tant que valeur ajoutée à l'Ambassadeur à utiliser dans leur calcul Verdict (par exemple, famille de programmes malveillants). Les experts peuvent proposer cette information comme un moyen de se différencier et d'attirer des entreprises futures.

Avec Assertions en continu, l'Ambassadeur pèse Assertions et incorpore leurs propres efforts de diligence raisonnable internes, produisant un verdict "malveillant" ou "bénigne". L'Ambassadeur remet ce verdict à leur client comme leur ultime réponse concernant le malicieux de l'artefact. L'Ambassadeur peut également choisir de rendre ce Verdict public (et est incité à le faire via la réduction des frais) avant la date limite du Verdict.

Verdicts publics contient les éléments suivants:

1. **GUID de la Liste:** une référence à la liste d'invités.

2. **The Ambassador’s NCT Identity:** Encore une fois, comme une signature sur la déclaration.

3. **Le Verdict:** Une détermination booléenne "malveillante" ou "bénigne" concernant le malveillant de l'Artefact.

Un moment plus tard, les Arbitres atteignent le quorum sur la vérité de terrain concernant l'Artefact. Cette vérité de base est comparée aux assertions de chaque expert et NCT est attribué pour des assertions précises.

Cycle de vie de l’Offre

Lorsqu'un Ambassadeur souhaite placer des offres à un expert choisi, l'Ambassadeur ouvre une chaîne de style Raiden avec l'expert.

Ceci est fait en initiant un smart contrat de chaîne d'offre avec l'expert qui inclut les éléments suivants:

1. **Identités de l'Ambassadeur et de l'expert.**
2. **La solde chaîn:** Le maximum net montant de NCT que l'Ambassadeur est à l'aise de régler avec l'expert au moment de la fermeture de la chaîne (plus les frais).

Une fois la chaîne d'offre est établie, l'Ambassadeur envoie zéro ou plusieurs Offres à l'Expert. Chaque offre comprend les éléments suivant:

1. **GUID de la liste:** Un identifiant global unique pour la liste.
2. **Le montant de l’offre.** Ce montant ne doit pas dépasser le solde restant du contrat intelligent de la chaîne d'offres (moins les frais.
3. **Hash cryptographique de l'artefact.**
4. **L'URI de l'artefact.** L'artefact est éventuellement crypté à l'identité du destinataire ou autrement protégé pour assurer la confidentialité.
5. **Date limite d'engagement:** Date limite pour la réponse à l'engagement (décrite ci-dessous.
6. **Date limite d'assertion:** date limite pour l'assertion de cette offre.

Lorsqu'il est présenté avec une offre, l'expert (le pollicité) peut choisir de s'engager dans l'offre ou de l'ignorer. Chaque arbitre détermine si cet artefact mérite d'être évalué pour le montant offert dans le temps alloué.

L'activité future de l'Offeree est basée sur sa capacité à produire des résultats précis. Si le destinataire n'est pas confiant dans sa capacité à produire un résultat précis dans le temps alloué (par exemple, l'artefact est un type de fichier que le destinataire est mal équipé pour analyser), elle peut choisir de rejeter l'offre.

Si le destinataire décide de rejeter l'offre, elle émet activement une déclaration de mission de «refus» ou attend simplement que la date limite de participation expire. Il appartiendrait à l'arbitre de rejeter activement, plutôt que d'attendre l'engagement de la date limite, car les Ambassadeurs favoriseront probablement les experts qui ne les forcent pas à attendre la date limite d'engagement pour déterminer les prochaines étapes.

Si le destinataire accepte l'offre, elle émet une déclaration de participation «acceptant» avant la date limite d'engagement.

Les déclarations d'engagement contiennent les éléments suivants:

1. **Listing GUID + Hash:** Une référence à la liste d'invités.

2. **Engagement Commitment:** Un «acceptation» ou un «refus» booléen qui stipule si le destinataire s'engagera avec cette offre et commettra une assertion avant la date limite d'assertion de l'offre.

Une fois que le pollicité a accepté une offre, le pollicité a jusqu'à la date limite pour présenter une assertion contre l'offre.

Ces assertions contiennent les éléments suivants:

1. **Listing GUID + Hash:** Référence unique à la liste d'invités.

2. **L'assertion:** Une détermination booléenne "malveillante" ou "bénigne" concernant la malveillance de l'artefact.

3. **Métadonnées(Optionnelles):** Informations dérivées lors de la génération d'assertion et proposées en tant que valeur ajoutée à l'Ambassadeur à utiliser dans leur calcul Verdict (par exemple, famille de programmes malveillants). Les experts peuvent proposer cette information comme un moyen de se différencier et d'attirer de futurs engagements.

Une fois que l'expert a remis son assertion à l'Ambassadeur, l'Ambassadeur signe un message de style Raiden qui s'engage à fournir également le montant de l'offre, de sorte que l'expert ne risque à aucun moment plus que le résultat d'une seule analyse. La

somme de tous ces montants est réglée sur la blockchain lorsque le canal d'offre est fermé.

Contrairement aux primes, les offres n'incorporent pas un mécanisme de rétroaction de la vérité terrain sur la chaîne. Au lieu de cela, les Officiels qui échouent à rendre une Assertion avant la date limite ou à rendre une Assertion inexacte (comme déterminé par des analyses hors chaîne ultérieures) peuvent ne pas attirer de futurs engagements. La maintenance de la réputation s'apparente alors à une boucle de rétroaction hors chaîne qui utilise la pression du marché pour maintenir l'honnêteté des Offres.

Lorsqu'un canal d'offre est fermé, des frais sont perçus sur le NCT net transféré. Comme pour tous les frais, ces frais sont accordés aux participants actifs du marché. Les frais sont appliqués par le contrat intelligent maître d'offre Channel Channel qui refuse d'établir des canaux d'offre non conformes.

Réputation

Contrairement à d'autres plates-formes de jetons (par exemple, Augur), PolySwarm ne tente pas de formaliser la notion de réputation et de l'intégrer dans les transactions de marché.

La raison en est simple: il est incroyablement difficile d'anticiper les points de données que les différents participants apprécient – et comment ces points de données sont pesés. La meilleure solution pour l'Ambassadeur Le meilleur choix pour l'Ambassadeur B et il serait possible de les faire fonctionner tous les deux sous l'hypothèse que c'était le cas. Au lieu de cela, la mécanique de PolySwarm exige simplement ou encourage la divulgation des types de données[17] qui représentent probablement une contribution utile à une fonction de réputation.

Les algorithmes de réputation seront probablement considérés comme un secret commercial de la même manière que les algorithmes de distillation Assertion to Verdict. Les Ambassadeurs se différencieront en engageant des experts optimaux pour leur charge de travail sur les artefacts. Les experts se différencieront en conservant un historique favorable des assertions correctes par rapport à la vérité terrain. Et, en option, en fournissant des métadonnées, par exemple, la famille de logiciels malveillants à laquelle un artefact particulier appartient.

Le prototype d'implémentation d'Ambassadeur à développer va distiller

différents points de données en un simple «score» de réputation et un schéma de couleurs facile à comprendre. Cette distillation de référence sera probablement utile à beaucoup, mais peut être remplacée ou modifiée selon les besoins des participants. Les experts voudront probablement mettre en place un système de réputation pour évaluer les Ambassadeurs, mais la logique métier d'un tel système devrait être plus complexe et différer considérablement entre les participants.

La référence daemon de PolySwarm va "désintégrer" les anciennes données, maintenant une "fenêtre glissante" dans la réputation des participants. Nous croyons qu'une approche par fenêtre glissante est nécessaire pour éviter le lock-out de nouveaux participants au marché.

Nous prévoyons d'utiliser les points de données suivants dans une implémentation de référence Ambassadeur:

1. **Précision de l'assertion** (par rapport à la vérité du terrain et / ou aux analyses hors chaîne).

2. **Fréquence et temps de réponse moyens pour les primes et les offres.** Dans le cas des offres, les Ambassadeurs peuvent choisir de publier des données agrégées qui ne sont normalement observables que dans un canal d'offre. Les Ambassadeurs peuvent favoriser les experts qui démontrent des temps de réponse rapides et constants.

3. **L'habileté de maintenir la confidentialité des artefacts livrés dans le cadre des offres.** Ceci est susceptible d'hybride sur le marché, l'analyse hors march.

Les Ambassadeurs peuvent choisir de passer en revue les verdicts passés de leurs concurrents et tenter de découvrir des erreurs (par exemple, l'Ambassadeur A a déclaré que l'échantillon était bénin alors qu'en fait il était malveillant). Les experts peuvent chercher à éviter de faire affaire avec des Ambassadeurs dont la diligence raisonnable ne tient pas le coup en général ou qui est plus souvent incorrecte dans certaines circonstances (p. Ex. Ambassadeur A documents Microsoft Word fréquemment mal classés, certains experts évitant d'analyser des documents Word au nom de l'Ambassadeur A) En d'autres termes, parmi les autres contributions, les experts peuvent être intéressés par la précision du verdict des Ambassadeurs.

Les consommateurs s'appuieront probablement sur des sites Web et des publications de style Consumer Reports ou AV Comparatives qui rapportent les antécédents de chaque Ambassadeur, peut-être avec des exemples d'intrants connus et vérifiant que le verdict d'un Ambassadeur correspond toujours à ce qu'il représente à ses clients.

Registre des travailleurs

Les experts de l'écosystème PolySwarm choisiront, dans de nombreux cas, d'encapsuler leur expertise dans des travailleurs automatisés. Les travailleurs sont des systèmes qui répondent automatiquement aux Primes et aux Offres, peut-être avec une expertise pour certains types de fichiers ou le trafic réseau. Le marché de PolySwarm fournira un registre des travailleurs distribué pour faciliter la découverte des offres des experts.

Nous développerons une interface commune et un langage de description pour les travailleurs enregistrés au public. Ces composants interagiront avec le registre PolySwarm modélisé après les contrats intelligents initiaux du registre Ethereum dApp. Le registre des travailleurs de PolySwarm contiendra des descriptions qui annoncent des compétences particulières (par exemple, “Je vais bien avec les binaires Mach-O du Mac OS” ou “Je gère les documents Microsoft Word”).

Confidentialité des artefacts

La divulgation confidentielle d'Artefacts est une fonctionnalité de première classe sur le marché de PolySwarm via l'instrument d'offre. Néanmoins, sans prendre de précautions supplémentaires, les Ambassadeurs utilisant les offres doivent faire confiance aux motivations et à la capacité technique de Security Experts pour parer les attaquants, éventuellement à perpétuité.

Nous nous attendons à ce que cette exigence de confiance donné naissance à des marchés secondaires et à de nouvelles applications technologiques dans le but de minimiser ou de consolider la confiance. Voici des exemples d'instruments construits sur PolySwarm pour répondre aux exigences de confidentialité.

Minimisation de la confiance via Intel SGX

Intel SGX est une nouvelle technologie initialement livrée avec la famille de processeurs Skylake. À un niveau élevé, SGX Fournit des environnements de calcul opaques à l'intérieur des "enclaves". contenu de la mémoire des enclaves SGX ne sont pas disponibles pour d'autres logiciels et utilisateurs sur le même système, quel que soit

le niveau d'autorisation. Dans le contexte de PolySwarm, enclaves SGX experts permettrait de numériser sans révéler les artefacts artefacts au chercheur et sans révéler l'intelligence des experts à quelqu'un d'autre. SGX promet donc une réduction de la confiance mutuelle entre les Ambassadeurs et les experts.

Les experts peuvent choisir d'exécuter accrédité (et attesté) enclaves de SGX qui ingèrent l'artefact et leur intelligence et produit un Assertion qui peut être remis à l'Ambassadeur. Il y a des obstacles techniques à surmonter, mais nous sommes confiants SGX peuvent être des enclaves intégrées et mis à l'échelle bootstrapping un avec l'autre de manière distribuée. itérations futures de PolySwarm Ambassadeurs mai pour permettre aux futurs auteurs des déclarations "SGX Prime" sur le marché du PolySwarm, révélant les artefacts que des enclaves bootstrap.

Consolidation de la confiance via les Ambassadeurs SaaS (Scan-as-a-Service)

Les experts peuvent choisir d'externaliser des tâches de calcul à des tiers pour un certain nombre de raisons qui peuvent ou non être spécifiques à PolySwarm. Par exemple, nous nous attendons à ce que de nombreux experts utilisent AWS, Google Compute Engine, Azure ou d'autres services de calcul à la demande pour étendre leur pipeline Assertion en réponse à la demande du marché de PolySwarm. Ce n'est pas une décision de calcul intrinsèquement motivée par PolySwarm.

Nous prévoyons que les incitations spécifiques à PolySwarm pour les entités SaaS se produiront naturellement. Dans le cadre de la confidentialité, les participants créeront des sociétés SaaS qui serviront de tiers de confiance entre les Ambassadeurs et les experts et maintiendront des accords de non-divulgation avec les deux. Ces sociétés SaaS serviraient le même objectif que les enclaves SGX - protéger les artefacts des experts et les renseignements des Ambassadeurs.

Les Ambassadeurs peuvent trouver plus facile de faire confiance à des entités SaaS tierces ayant une réputation publique plutôt qu'à un grand nombre d'experts individuels dont l'identité pourrait ne pas être connue. De tels Ambassadeurs rédigeront plus d'offres destinées aux entités SaaS que directement aux experts.

Marchés Supplémentaires

Le marché de PolySwarm créera une demande pour un certain nombre de marchés supplémentaires. Un tel marché (Scan-as-a-Service) a déjà été discuté dans le contexte de contrôles de confidentialité supplémentaires. Voici quelques marchés supplémentaires attendus ci dessous.

Ambassadeurs

Ceci un marché évident et très discuté tout au long de ce document. De nombreux Consommateurs choisiront de faire affaire avec le marché par l'entremise d'un Ambassadeur, mais travailler avec un Ambassadeur n'est pas une exigence stricte.

Publication des Services d'Artefacts

Lors du dépôt d'une prime ou d'une offre, l'Ambassadeur doit mettre son artefact à la disposition des Experts. Les entités d'hébergement d'artefacts offriront ce service, ce qui rendra ce partage transparent. Leurs clients seront des consommateurs et des Ambassadeurs. Nous attendons de nombreux Ambassadeurs qu'ils offrent également des services d'édition d'artéfact.

Services de suivi de la réputation

Aux États-Unis, les banques font confiance à trois bureaux de crédit pour tenir un registre des "faits" concernant la fiabilité individuelle. Le marché de PolySwarm présentera une demande similaire; Les participants au marché voudront quantifier la fiabilité des autres participants pour diverses raisons déjà discutées. Il est probable que des services de réputation surviendront pour suivre la fiabilité des participants et offrir cette information pour atténuer le risque de contrepartie.

Feuille de Route

Nous présentons ici les jalons préliminaires du développement de PolySwarm. Chaque étape: (1) offrira de nouvelles fonctionnalités et (2) fournira de la documentation et des tests permettant de nouvelles transactions avec les Ambassadeurs, experts et utilisateurs finaux.

PolySwarm est à un avantage développemental distinct par rapport aux réseaux comme Bitcoin et Ethereum qui doivent conserver toutes les transactions à perpétuité. Dans PolySwarm, une fois les vérités fondamentales sont déterminées ou une chaîne d'offre est mis à la chaîne, les Ambassadeurs et les Experts ont reçu ce dont ils ont besoin de cette transaction: l'intelligence concernant l'artefact et la NCT, respectivement. Cette atomicité fournit une marge de manœuvre et nous permet d'effectuer des modifications incompatibles avec les versions antérieures, jusqu'à la version 1.0, sans les problèmes de coût et de consensus rencontrés dans d'autres réseaux.

V0.1 Alpha (30 Avril 2018)

PolySwarm Alpha se concentrera sur la fourniture d'un flux de travail prototype de bout en bout pour les primes après l'expiration d'un jeton réussi. Cette version initiale permettra à l'équipe de PolySwarm de commencer le processus d'amorçage avec sérieux. Les Ambassadeurs et les experts pourront effectuer des transactions via le réseau de test PolySwarm ("testnet"). Les contrats intelligents Bounty de base seront disponibles sur le testnet PolySwarm, permettant aux Ambassadeurs de placer des primes, des experts pour rendre des assertions, et des Ambassadeurs pour rendre des verdicts

Nous prévoyons que PolySwarm Alpha réalisera les tâches suivantes:

- Un smart contrat “Manager de prime” qui contient les montants et les frais de primes, accepte les assertions, publie les verdicts et récompense les experts exacts.
- Publication et récupération d'artefacts vers ou depuis un stockage hors PolySwarm (par exemple, Amazon S3 et ou IPFS)
- Algorithme de prototype pour la sélection des arbitres à l'expiration de prime
- Implémentations de référence pour la publication Prime, la réponse Assertion et la détermination de la vérité terrain d'arbitrage

V0.2 Beta (31 Mai 2018)

PolySwarm Beta se concentrera sur la fourniture de l'offre PolySwarm sur les chaînes de style Raiden. Les offres sont conçues pour faciliter l'évaluation des artefacts à plus haut débit par rapport aux primes et, en tant que telles, exigent un règlement plus précis de la chaîne de blocs pour chaque transaction. PolySwarm Beta mettra en œuvre des contrats intelligents Offer. Nous prévoyons mettre en œuvre cette fonctionnalité en tant que canaux de style Raiden directs, de pair à pair, établis entre des Ambassadeurs et des experts utilisant le testnet.

Nous anticipons que PolySwarm Beta accomplira les tâches suivantes:

- Chaînes d'offres
    - Etablissement des chaine distribuées
    - Multiples offres à partir d'une chaîne
    - Réglage du NCT a la clôture de la chaîne
- Implémentation de la référence pour la production des offres et réponses aux offres
- Implémentation de la référence pour les Arbitrer la vérité terrain et les réponses
- Collection des frais et distribution des smart contract
- Rechercher et quantifier la confiance (en NCT) requise pour un volume spécifique d'artefacts
- Boîte à outils de développement des offres / primes: un cadre de test et de mise en œuvre pour les experts et les Ambassadeurs afin d'automatiser l'entretien des primes et des offres

V0.3 Gamma (31 Juillet 2018)

PolySwarm Gamma se concentrera sur la fourniture de fonctionnalités de mise en relation qui facilitent la collaboration entre les Ambassadeurs, les experts et les arbitres. Les experts seront en mesure d'encapsuler leur expertise dans les travailleurs à specialisés l'écoute de types spécifiques d'artefact. Nous nous attendons à ce qu'ils soient en mesure de promouvoir ces travailleurs dans un registre PolySwarm. Ce registre des travailleurs devrait permettre

aux Ambassadeurs de s'engager avec les travailleurs sans risque avant le lancement de la version Stable (la version Gamma continuera d'utiliser le testnet PolySwarm).

Additionnellement, cette version considérera l'amélioration et l'extension de la Prime selon des commentaires et expériences des utilisateurs des versions Alpha et Beta. Par d'exemple, nous prévoyons que les Primes bénéficieront de la possibilité de demander des Assertions qui sont gardées confidentielles par d'autres Experts et qui ne seront révélées qu'après la date limite d'Assertion.

Nous anticipons que PolySwarm Gamma accomplira les tâches suivantes:

- Langage de description de l'ouvrier/travailleur (Worker Description Language–WDL) décrivant les capacités d'analyse des artefacts et l'attribution de l'auteur expert (pour la réputation)
- Un registre de travailleurs Distribué, consultable y compris leurs capacité.
- Confidentialité pour les assertions de primes avant l’échéance
- Finaliser la sélection des arbitres, la réponse et la boucle de rétroaction des primes de bout à bout

Finaliser la sélection des arbitres, la réponse et la boucle de rétroaction des primes de bout à bouta.

V1.0 Stable (Q4 2018)

PolySwarm Stable se concentrera sur l'élimination des bogues dans PolySwarm Gamma avant la migration du testnet PolySwarm (jetons de test) vers le véritable marché de PolySwarm.

En tant qu'objectif ambitieux et que le temps et le financement le permettent, Stable peut introduire la confidentialité de l'Artefact de première classe via une Prime à une audience limitée et publique.

V2.0 Future (Q2 2019)

La deuxième version stable de PolySwarm a actuellement deux objectifs principaux: élargir les offres et les primes pour gérer un plus large éventail de types d'artefacts (par exemple, URL et flux réseau) et faciliter l'utilisation de PolySwarm pour les utilisateurs d'entreprise et particuliers.

L'extension du type d'artefact dans les versions futures de PolySwarm devrait permettre de gérer, par exemple, la détection automatisée de détection d'hameçonnage(phishing) des URL d'utilisateurs en plaçant des primes et des offres directement sur le contenu hébergé.

L'extension des protections de PolySwarm directement au point de terminaison sera une priorité pour le développement post-stable. Nous prévoyons de développer une implémentation de référence Open Source d'une suite de protection Endpoint qui bloque automatiquement les artefacts malveillants basés sur l'intelligence de PolySwarm. Nous voyons ce cadre d'agent ouvert comme une clé pour l'adoption généralisée des utilisateurs.

Futures Fonctionnalités

Les prochaines versions de PolySwarm refléteront l'évolution du paysage des menaces et l'utilisation réelle du réseau. Nous voyons plusieurs opportunités, en fonction de l'utilisation observée de PolySwarm, pour que les fonctionnalités suivantes bénéficient au réseau et à l'objectif ultime de la protection de l'utilisateur:

- FFlexible Confidentialité de l'artefact
    - Basic: Artefacts sélectivement divulgués à des experts ou à des fournisseurs SaaS
    - Advanced: Artefacts jamais révélés à quiconque en dehors des enclaves SGX de moteurs entièrement homomorphes
- Nouveaux Instruments (par exemple des données sur les menaces prêtes pour s'y abonner)
- Prise en charge du déploiement pour les conteneurs Travailleurs résidant en point de terminaison qui supplantent les suites de protection de point de terminaison d'aujourd'hui

Vente de Jeton

Le développement technique, l'engagement communautaire et la sensibilisation des participants à l'écosystème PolySwarm seront assurés par PolySwarm Pte. Ltd. grâce au financement de la vente des jetons d'utilité Nectar (NCT) de PolySwarm.

Ces jetons seront échangés par les participants pour des

renseignements sur les menaces. NCT alimente toutes les interactions majeures de PolySwarm: placement de primes, établissement / démontage / échange de chaînes d'offre, enregistrement d'assertion et détermination de la vérité basique. En vendant des jetons NCT spécifiques à l'entreprise, les taux de change de NCT contre les menaces devraient être isolés de la volatilité sur le grand marché des ETH, garantissant une participation active à PolySwarm sans se préoccuper des fluctuations de l'ETH.

Cette section est destinée à donner un aperçu de haut niveau de la tokenomics de PolySwarm. En cas de conflit entre ce document et le contrat de vente de jetons (“Contrat”), l'Accord prévaudra. **Le contrat de vente de jeton est disponible en ligne**.

Horaire

PolySwarm Pte. Ltd. exploite actuellement une pré-vente de jetons pour les participants invités. La vente publique NCT devrait ouvrir aux acheteurs qualifiés le 20 Février 2018 à 19h00 GMT. Elle est prévue d'être fermée le 22 Mars 2018 à 19h00 GMT.

Conditions d’Achat

NCT sera disponible exclusivement à l'achat avec Ether (ETH). Il est conseillé aux acheteurs potentiels de sécuriser suffisamment d'ETH avant la vente.

Le jeton utilisera les contrôles Connaissez Votre Client (CVC) avec un mécanisme technique unique pour obtenir des achats spécifiques aux points de données CVC, y compris, mais sans s'y limiter: Pays d'origine, adresse e-mail, nom complet, adresse IP et acceptation des conditions du Contrat d'Agrément de Vente de Jeton.

Caps / Limites

Aucun nouveau jeton ne sera créé après la fin periode de vente du jeton.

Le nombre total de jetons NCT sera déterminé pendant la sortie du jeton.

Le nombre maximum de jetons est plafonné. Ce plafond est basé sur le plafond du financement maximal en USD, le prix du NCT (en ETH) et le taux de change actuel entre ETH et USD. Reportez-vous à la page Vente de Jetons[18] pour plus de détails sur les limites de NCT, le prix, les tranches de financement et plus encore.

Allocation

70% des jetons NCT seront vendus lors de la Vente de Jetons.

15% des 30% restants seront "largués" vers des entreprises, des fournisseurs et des experts en sécurité intéressés à aider à amorcer l'écosystème PolySwarm. Les récipiendaires seront choisis à la seule discrétion de PolySwarm Pte. Ltd.

Les 15% de jetons finaux seront utilisés par PolySwarm Pte. Ltd. de manière à accélérer l'adoption de l'écosystème PolySwarm. À titre d'exemple illustratif, les jetons peuvent être offerts comme une incitation à participer aux "hackathons" de PolySwarm. Cette attribution sera à la seule discrétion de PolySwarm. Pte. Ltd.

Distribution

Nous prévoyons que l'ETH dérivé de la sortie des jetons utilitaires Nectar de PolySwarm ("NCT") sera alloué de la manière suivante:

54,51% – Protocole et Développement de Logiciels
3,00% – Frais de bureau
4,06% – Frais généraux opérationnels (déplacements, hébergement, etc.)
14,49% – Frais légaux
13,62% – Marketing
10,32% – Taxe

L'équipe de PolySwarm s'attend à ce que les dépenses juridiques diminuent au cours de l'exercice de l'an 2019/2020. Le surplus sera redistribué dans les salaires de marketing, de frais généraux et de développeurs. Notre taxe estimée à 10,32% est faible, mais pas déraisonnable. C'est bon pour les participants: plus de fonds seront alloués directement au développement et à la promotion de PolySwarm.

Disclaimer

Ce livre blanc est destiné à fournir des informations techniques aux acheteurs potentiels de jetons. Le jeton PolySwarm sert à financer le développement initial de prototypes et le test des instruments économiques présentés ici. Nous nous attendons, comme tout participant prudent, à ce que les détails présentés dans ce document puissent changer au cours des périodes de développement et d'essai pré-stables. Les intérêts de PolySwarm Pte. Ltd. et des acquéreurs de jetons sont alignés pour faire de PolySwarm un marché viable qui change réellement l'industrie des intelligences sur les menaces cybernétiques.

Conclusion

PolySwarm est un nouveau marché et un ERC20 jeton associé, NCT, qui est destiné à changer l'industrie de l'intelligence des menaces en facilitant de nouvelles méthodes d'interaction entre les experts en sécurité, les fournisseurs et les entreprises. L'équipe de PolySwarm effectuera un lancement de jeton pour financer le développement de logiciels et cultiver une communauté autour de ce nouveau marché.

Nous espérons que vous vous joindrez à nous pour protéger les utilisateurs de tous angles **All Angles™**.

polyswarm.io