탈 중앙형 사이버 위협 인텔리전스 시장.

POLYSWARM

Table of Contents

PolySwarm 개요

Polyswarm은 Ethereum 스마트 컨트랙트와 블록체인 기술로 구현된 분산식 위협 인텔리전스 시장입니다.

Polyswarm은 연간 85억 달러 규모의 안티바이러스 및 자동화된 위협 인텔리전스 영역[1]의 빠른 혁신에 대한 인센티브를 제공하고 있습니다. 또한, 파일과 네트워크 트래픽, URL의 관리와 관련된 *시기적절*하고 *정확한* 사이버 위협 인텔리전스에 따른 경제적 인센티브 보상을 장려하고 있습니다.

PolySwarm은 기업, 소비자, 벤더 및 다양한 지역 출신의 보안 전문가가 참여하는 실시간 위협 탐지 생태계를 정의합니다. 전문가들은 최신 위협을 자율적으로 조사하는 "마이크로 엔진(micro-engine)" 개발로 경쟁을 벌이면서 경쟁자를 뛰어넘고자 합니다. PolySwarm의 "작업 증명(Proof of Work)"은 위협 탐지 정확도입니다. 즉, 시장은 기업과 최종 사용자를 가장 잘 방어한 전문가에게 바운티를 제공합니다.

오늘날의 임시 시장에 비해 PolySwarm은 진입 장벽을 낮추고 더욱 광범위한 커버리지 옵션을 제공하고 중복 노력을 억제해서 제품과 위협 인텔리전스 피드의 상호운용성을 보장할 것입니다.

경제적인 측면에서 보았을 때, PolySwarm은 숙련된 기술이 필요한 예측 시장[2]이라고 할 수 있습니다. 수천 개의 마이크로 엔진("작업자")은 인간의 관여 없이 *기계의* 속도로 최근의 멀웨어 진화 동향을 조사합니다.

PolySwarm은 **PolySwarm Pte. Ltd.**("PolySwarm Pte. Ltd.")가 ERC20 호환 **Nectar** ("NCT") 유틸리티 토큰 판매에서 발생하는 자금으로 개발할 예정입니다.

유틸리티 토큰으로서의 PolySwarm은 부가가치를 창출하고 활발히 활동하는 참가자에 대한 **수수료 부과 및 분배**(상세한 정보는 6쪽 참조)를 통해 정직한 시장 참가자에게 바운티를 제공합니다. 경제적인 측면에서 보았을 때, 이는 Nectar 투기를 억제하는 측면이 있습니다

배경

오늘날 기업들은 안티바이러스 구독과 위협 인텔리전스 피드, 다양한 형태의 동적 분석 엔진 등의 임의적인 혼합 형태를 갖추며 진화하고 있는 적대적 사이버 활동을 방어하고 있습니다. 사용자는 각 솔루션의 장단점을 고려하여 그나마 환경에 가장 적합한 것을 결정해야 합니다.

현재의 시장 형태에서는 폭넓은 위협 커버리지를 제공하는 솔루션이 출시되기 어렵습니다.

1 Jefferies Cyber Security Primer. 2017년 1월 18일.
2 https://en.wikipedia.org/wiki/Prediction_market

현재의 솔루션은 적절한 위협 방어에만 초점을 맞춥니다. 이는 모두 오늘날 시장의 경제적 작동 원리에 따른 결과입니다.

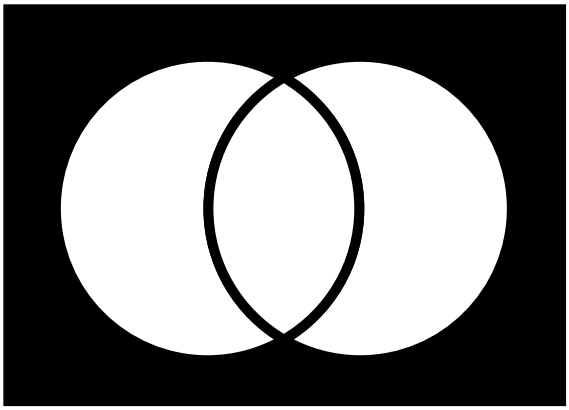


그림 A: 검은색 사각형은 기업이 만날 가능성이 있는 모든 위협을 나타냅니다. 흰색 원은 안티바이러스 제품 1과 2입니다.

WannaCry[3]를 탐지하지 못하는 안티바이러스 솔루션을 무시하기는 쉽지만(타당하기도 하지만), 그렇게 함으로써 시장에서는 사실상 벤더의 커버리지 중복을 부추기게 됩니다. 이러한 시장 비효율로 인해 중복 비용이 발생합니다. 이것이 전형적인 공유지의 비극(tragedy of the commons)에 해당하는 상황입니다.

마찬가지로, 일반적이지 않은 영역의 전문 지식을 개발하고자 하는 벤더가 있다고 가정해 보겠습니다. '일반적인 영역'을 대부분 기업이 직면하는 위협이라고 생각하는 경우, 전문적 벤더를 대상으로는 판매가 어려울 것입니다. 여러분만이 보유하고 있는 탐지/예방/완화 능력을 활용하여 멀웨어에 대비해야 한다는 주장과 함께, 잠재 고객을 어떻게 설득하시겠습니까?

마지막으로, 방어 주체들은 여러 가지 기존 솔루션을 조합할 수 없기 때문에 대부분의 상황에서 결합에 따른 커버리지가 불가능합니다.

반면, PolySwarm은 다양한 지역 출신의 보안 전문가가 개발한 수천 개의 "마이크로 엔진" 작업자들이 제공하는 광범위한 커버리지로 구성된 생태계를 조성하고 있습니다.

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

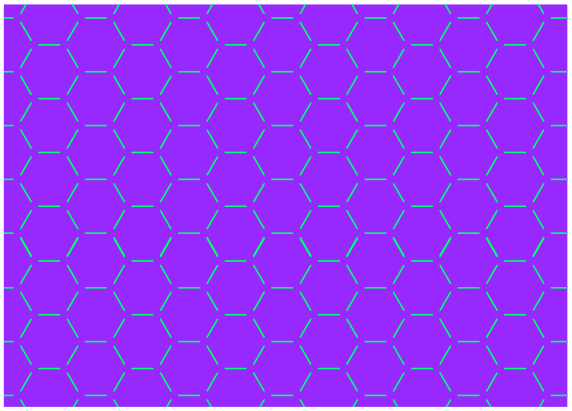


그림 B: PolySwarm은 광범위한 위협 커버리지를 제공하는 생태계(ecosystem)를 조성할 것입니다.

PolySwarm은 보안 전문가를 위한 합법적인 수입원을 제공합니다.

일부 보안 전문가는 지역 경제가 정직한 작업을 충분히 뒷받침해주지 못할 때 랜섬웨어를 개발하거나 봇을 운영하고, 다른 악의적 목적에 자신의 기술을 사용하기도 합니다. PolySwarm는 지역에 구애받지 않는 대안, 즉 정직한 일에 대한 자유로운 바운티를 제공합니다. 전문가는 인터넷을 더욱 안전한 공간으로 만들기 위해 경쟁합니다.

PolySwarm은 사용자를 가장 우선으로 생각합니다.

PolySwarm 시장은 가장 중요한 곳, 즉 정확한 악의적 의도 탐지("위협 인텔리전스")에 경제적 인센티브가 향하게 합니다. 정확도는 **중재된 합의(Mediated Consensus)**(자세한 정보는 11쪽 참조)라는 새로운 프로세스에 따라 결정됩니다.

간단히 말해, PolySwarm은 사용자가 시기적절하게 광범위한 크라우드소싱 보안 전문 지식에 접근할 수 있도록 합니다. 의심스러운 파일을 신속히 살펴보아야 할 필요가 있습니까? PolySwarm™을 사용해보십시오.

위협 인텔리전스 시장의 재구성

PolySwarm Nectar("NCT") 토큰은 새로운 시장의 기반을 형성하며, 파일과 네트워크 트래픽, URL(총칭하여 "아티팩트")에 숨겨진 악의적 의도를 시기적절하고 정확히 밝혀내고자 하는 수요를 충족하기 위해 새로운 도구를 사용합니다. 이런 새로운 도구는 정확한 결과에 따른 피드백 루프로 위협 인텔리전스 분야에서 혁신을 일으키는 데 직접적인 인센티브를 제공할 수 있도록 구성되었습니다.

PolySwarm은 스팸을 억제하고 정직하고 능동적인 시장 참여를 촉진하기 위해 수수료를 부과하고 있습니다. 수수료는 스팸에 악용될 만한 거래 유형을 대상으로 평가하여 부과한 다음, 능동적인 생태계 참가자에게 분배됩니다. 능동적인 생태계 참가자는 아티팩트를 가져와서 아티팩트에 악의적 의도가 숨어 있는지 밝힙니다. 이러한 참가도는 슬라이딩 방식으로 측정됩니다. 즉, 오래된 시장 참여는 "서서히 밀려나" 지속적인 시장 참여를 유도합니다.

PolySwarm 1.0(및 본 문서)은 부울(악성/양성) 판정에만 사용할 수 있지만 PolySwarm 팀에서는 단순히 악성/양성을 판정하는 데서 나아가 더욱 큰 구상을 하고 있습니다. PolySwarm 1.0을 개발하면서 멀웨어군 등의 아티팩트 메타데이터 생성을

촉진하고, 스마트 컨트랙트 시장 설계, 중재된 합의, 정보 보안 집중 등의 PolySwarm 콘셉트로 취약성 버그 보상[4] 등의 관련 시장에 파괴적 혁신을 일으킬 방안을 모색할 것입니다.

PolySwarm 도구 설명에 앞서 이를 활용할 참가자 분류를 설명하겠습니다.

참가자

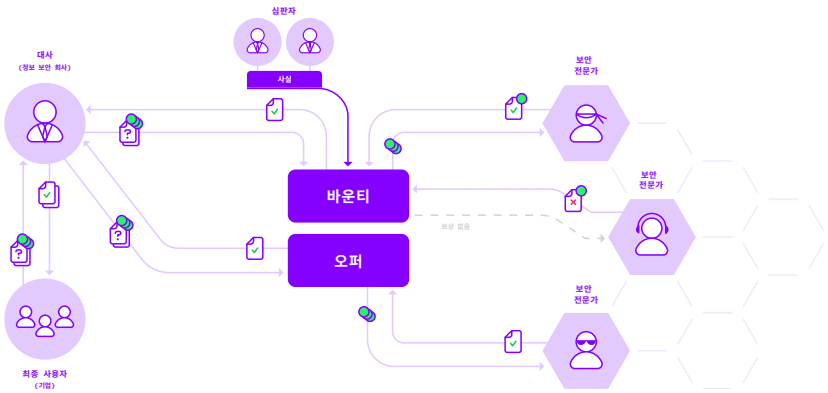


그림 C: PolySwarm 바운티 및 오퍼 수명 주기 개요.

최종 사용자: 의심스러운 아티팩트를 보유한 기업 및 가정 사용자. 최종 사용자(End User)는 바운티와 오퍼(잠시 후 자세히 설명)를 통해 PolySwarm 시장에 참가하여 시기적절하고 정확한 악의적 의도를 분류하고 추출합니다.

보안 전문가("전문가"): 다양한 지역 출신의 멀웨어 전문가 및 리버스 엔지니어. 전문가(Expert)는 가장 최근의 의심스러운 아티팩트를 분석하고 악의적 의도를 판정하는 PolySwarm에 연결된 탐지 엔진("작업자")을 관리합니다. 전문가가 "

4 "HackerOne but distributed, pseudonymous, and unfettered by jurisdictional encumbrances. Powered by blockchain." 이 문서에서는 다루지 않습니다.

의견(Assertions)”을 제출합니다. 의견이란 아티팩트의 악의적 의도를 분석한 결과를 반영한 공개 보고서입니다. 정확한 의견을 제출한 전문가는 그 노력에 대한 바운티를 받습니다(NCT로 제공).

여기까지 핵심 참가자를 설명해 드렸습니다. 간결하게 설명하는 것이 좋지만, 이것만으로는 PolySwarm에 대해 제대로 설명할 수 없습니다. 기술적으로 PolySwarm은 상기에 명시한 두 참가자만 사용할 수 있습니다. 그러나, 현실에서는 대부분 **최종 사용자**가 PolySwarm 시장과의 접촉을 외부에 위탁하는 편을 선호하기 때문에 그렇게 되지는 않을 것입니다. 자세한 내용을 설명하기 전에 **대사**(다른 참가자)와 이러한 대사의 하위분류에 대해 소개하겠습니다.

대사: 최종 사용자가 쉽게 PolySwarm 시장의 혜택을 누리도록 도와주는 기업입니다. 대사(Ambassador)는 고객(최종 사용자)으로부터 전통적 방식에 따른 지시(예: 구독 요금)와 의심스러운 아티팩트를 받아서 고객을 대신하여 시장에 **바운티**와 **오퍼**를 제시합니다. 대사의 책임은 다양한 전문가의 의견을 걸러서 고객에게 전달할 수 있는 단순한 **악성** 또는 **양성** 결정으로 바꿉니다.

이러한 정제 과정을 가장 단순하게 적용하는 방법은 전문가가 제공한 의견에 평균을 내는 것입니다. 그러나 이런 알고리즘이 인간 전문가의 참여는 고사하고 베이시안 분석[5]을 이길 가능성은 낮습니다. 기존 안티바이러스 및 위협 인텔리전스 기업이 초기에 대사 자격으로 PolySwarm 시장에 참가하고, PolySwarm으로 의심스러운 아티팩트를 분류함으로써 회사의 전문성을 키울 것입니다.

사용자의 입장에서는 PolySwarm 지원 보호로 간편하게 업그레이드할 수 있습니다. 평판이 우수한 대사를 선택하고 구독 요금을 지불하면 됩니다.

대사의 평판은 실제 결과에 대한 과거의 판정 실적을 기준으로 합니다. 대사는 평판을 높이고 새로운 고객을 모으고자 하는 내적 동기 외에도 수수료 할인을 이용하기 위해 자신의 판정을 공개할 유인이 있습니다(이 절차는 추후에 상세히 설명하겠습니다). 이러한 공개적 판정으로 대사는 데이터가 포함된 실제 아티팩트에 대한 현실적 실적을 평가한 “평가표”를 보유하게 됩니다. 이는 오늘날 시장에서는 존재하지 않습니다[6].

심판자: 악의적 의도를 판정하는 책임을 맡은 최상위 대사. 일정 비율의 대사(발생하는 수수료 기준)는 “심판자(Arbiter)”로 지정합니다.

PolySwarm은 개발 과정에서 PolySwarm 팀과 자주 교류하고자 하는 평판이 우수한 기존 위협 인텔리전스 벤더에게 결정권을 부여합니다. 또한, 플랫폼 버그를 찾아서 해결하고 생태계에서 이해를 구축하도록 도울 것입니다.

PolySwarm 1.0이 출시 준비를 완료하면 지정된 심판자는 최상위 대사에 해당하는 볼륨을 유지해야 심판자 지위를 유지할 수 있습니다.

5 Kantchelian, Alex, 외 “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 가장 유사한 것은 AV 비교입니다(https://www.av-comparatives.org/).

예측 시장, 심판자 및 중재된 합의

PolySwarm 생태계에서 보안 전문가는 마이크로 엔진 작업자를 개발하고 의심스러운 아티팩트를 신속하고 정확하게 조사하기 위해 서로 경쟁을 벌입니다. 이러한 조사는 아티팩트의 악의적 의도가 명확히 드러나기 전에 기계의 속도로 수행합니다.

이 설계는 예측 시장과 다소 공통점이 있습니다. 즉, 정확도를 바탕으로 과거의 의견에 바운티를 제공하지만 두 가지 중요한 지점에서 차이가 있습니다.

1. **아티팩트 분류에는 미래 데이터가 필요하지 않습니다.** 아티팩트는 작업자에게 제공되는 즉시 악성인지 "정답"을 확인할 수 있습니다. PolySwarm은 불명확한 것은 조금도 남기지 않는 기술 기반 설계 형태를 갖추고 있습니다[7].

2. **사실을 밝히는 데는 언제나 전문성이 필요합니다.** 이는 숙련되지 않은 참가자가 관찰하고 이벤트가 발생하면 기록하는 예측 시장의 "보편적 관찰성(universal observability)"과는 대조를 이룹니다(Augur[8] 등의 암호화 시장 포함).

항목 1은 PolySwarm의 도박 억제 수단입니다[9].

항목 2는 "관계자들이 지속적으로 실제 사실을 밝힐 유인을 제공할 수 있는 가장 좋은 방법이 무엇인가?"라는 기술적 어려움이 있습니다. PolySwarm은 심판자 등급과 "중재된 합의"라는 프로세스로 이를 해결할 것입니다.

중재된 합의는 다른 시장 설계 프로젝트에서도 이용될 만한 일반적 설계 패러다임입니다. 즉, 중재된 합의는 중요한 작업을 참가자의 부분 집합에 맡기는 시장 설계입니다. 참가자는 다음 요건을 갖추어야 합니다.

1. 작업을 완료할 자격이 있어야 합니다(프로세스 전문성).

2. 시장의 전반적 건전성과 이해가 상충하여야 합니다(공유지의 비극 회피).

7 이론상에 해당합니다. 실제로는 2가지 이상의 이벤트에서 불확실성이 발생할 수 있습니다. (1) 심판자가 사실을 잘못 판정해서 잘못된 전문가에게 보상이 분배될 경우, (2) 전문가의 분석이 사실과 일치하여 정확하지만 전문가가 악의적 의도의 경계에서 의견이 일치하지 않을 경우(PolySwarm을 넘어서는 의미론적 문제). 예를 들어, '애드웨어가 멀웨어인가, 단순히 사람들이 원치 않는 애플리케이션인가'와 같은 문제가 있습니다. 이런 변수는 PolySwarm 생태계의 기술 기반 성격을 근본적으로 손상시키지 않습니다.

8 https://augur.net/

9 아티팩트의 악의적 의도에 대한 추측, 내기, 도박 또는 기타 운에 따른 내기는 모든 사람에게 이익이 되지 않고 PolySwarm은 이러한 플랫폼 악용이 불가능하도록 설계되었습니다.

PolySwarm은 위의 두 가지 제약을 충족하도록 설계했습니다. 일반적으로 심판자 등급은 특정 기간에 PolySwarm 생태계에서 가장 활동이 많은 대사의 등급으로 정의됩니다. 심판자들은 대사로서 고객과 계약을 맺고, 판정을 바탕으로 보안 전문가의 의견을 걸러냅니다. 고객은 이들이 자동화된 전문성(필요할 경우 인간의 전문성)이 있고 이를 수행할 수 있다고 신뢰합니다. 이러한 회사는 이미 정확도에 대한 공개 기록을 유지할 유인이 있습니다(항목 1).

심판자는 가장 활발히 활동하는 대사로서 PolySwarm 생태계의 정직/부정직에 따라 발생하는 이익과 손실이 가장 큽니다. 생태계에 대한 신뢰에 많은 이익이 걸려 있기 때문에 시장이 건전해야 재정적 이익을 얻을 수 있습니다(항목 2).

PolySwarm은 심판자-보안 전문가의 결탁 등과 같이 심판자가 지위를 악용하지 못하도록 수수료를 보조적 방어 수단으로 도입했습니다.

사실 판정

현재 심판자 투표 절차의 상세한 기술 정보 대부분은 일부러 명확히 결정하지 않았습니다. 그 이유는 간단합니다. 심판자 결정 프로세스의 상세한 정보는 사실상 다른 모든 PolySwarm 프로세스의 구체적인 정보에 따라 예측되고 다른 프로세스에서 변화가 있을 것을 예상하기 때문입니다.

그래서 다음의 고차원적 설계 선택으로 이 프로세스에 가치를 부여할 수 있을 것으로 생각합니다.

1. 심판자는 **과반수 의결을** 통해 진실에 대한 합의에 도달합니다.

2. 이러한 투표는 **일괄 이더리움 체인(Ethereum chain en masse)**(주기당 다수의 표)으로 채굴하여 PolySwarm 생태계에서 시간과 비용(이더리움 가스)을 절약합니다.

3. 참가를 독려하기 위해, **심판자에게는 아티팩트 판정 투표에 대한 수수료를 바운티로 제공합니다.**

4. **심판자는 특정 아티팩트에 대한 투표를 기권**할 수 있습니다. 예를 들어, 심판자는 특정 아티팩트의 악의적 의도를 판정할 자격이 부족하다고 생각하는 경우 기권이 가능합니다.

5. 심판자는 필요에 따라 **추가 대사에게 투표권을 자동으로 위임하여(볼륨순으로)** 모든 사실 판정에 대한 정족수를 보장할 수 있습니다.

6. 필요한 경우, **지금과 마찬가지로 참가자들이 심판자의 판정에 이의를 제기할 수 있습니다.** 심판자가 잘못 분류했다고 지적하는 등, 아티팩트의 악성/양성을 설명하는 블로그 게시글이나 기술 문서를 사용합니다. 이를 외부 PR 중심적 피드백 루프(PR-driven feedback loop)라고 합니다.

PolySwarm 팀은 개발 과정에서 심판자 투표와 인센티브 구조와 관련된 세부 사항을 반복적으로 개발할 예정입니다. 이 설계에서는 초기 심판자 피드백이 매우 중요할 것으로 생각합니다. 연구 주제로는 다음이 포함됩니다.

- 최소 심판자 정족수 비율
- 심판자 유예 절차(정족수를 채울 수 없을 경우)
- 적절한 수수료 바운티 구조
- 시기적절한 사실 판정을 위한 인센티브(예: 투표에 참여한 처음 X명의 심판자에게만 바운티 제공)
- 불참에 대한 페널티(예: 심판자가 일정 기간에 X%의 아티팩트에 대한 사실 판정을 하지 않을 경우 심판자 지위 철회)
- (필요에 따라) 왜곡된 인센티브에 대한 추가 억제책 적용

도구

오퍼

PolySwarm은 최종 사용자와 대사에게[10] 위협 인텔리전스 시장의 효용을 높이는 2가지 핵심 도구를 공개합니다.

PolySwarm 오퍼: 악의적 의도 판정을 평판이 우수한 보안 전문가에게 직접 요청합니다. PolySwarm은 이런 연구자 수천 명에게 매끄럽게 접근할 방법을 제공하여, 비전통적인 참가자와도 기존의 정보 공유 계약을 체결할 수 있도록 지원합니다. 이러한 만남은 Raiden[11] 스타일 오퍼 채널에서 일어납니다(자세한 내용은 추후 공개). 채널이 설정되면, 오퍼는 밀리초 단위의 간격으로 아티팩트 조사 결과를 제공합니다.

바운티

PolySwarm 바운티: 서부 개척 시대 스타일의 “현상수배(Wanted)” 포스터에 아티팩트 콘텐츠를 공개합니다(예: 현상 수배:
대상 아티팩트: 악성/양성? 바운티: 1000 NCT). 보안 전문가는 바운티를 두고 경쟁하여 명성을 얻습니다(평판 구축). 오늘날에는 시장과의 직접 아날로그 형태가 존재하지 않습니다.

10 이후부터 최종 사용자와 대사는 대사로 줄여서 지칭합니다. 최종 사용자는 스스로 대사로 행동할 수 있습니다. 일부 대기업에서 이러한 방식으로 참여할 것으로 예상합니다.
11 http://raiden.network/

*오퍼*는 오늘날의 온디맨드 스캔 시장과 가장 가까우며, 밀리초의 지연 속도로 운영됩니다.

대사는 오퍼와 아티팩트를 선택한 보안 전문가에게 직접 발행합니다. 선택적으로 비밀 유지 계약을 체결하기도 합니다. 각 전문가는 제시된 아티팩트에 대해 정확한 의견을 제공할 수 있는지 판단하고 그에 따라 오퍼를 수락합니다. 전문가는 자는신이 없다면 평판이 하락하지 않도록 오퍼를 거절할 수 있습니다. 전문가가 오퍼를 받아들일 경우, 전문가는 시기적절하게 악의적 의도에 대한 의견을 제출해야 합니다. 모든 도구에 대한 토큰 수집과 바운티는 전적으로 탈중앙형 스마트 컨트랙트에 따라 관리 및 실행됩니다.

오퍼를 발행하려면, 해당 아티팩트를 분석할 역량이 있는 전문가가 있어야 합니다. 매칭을 간편하게 하기 위해 전문가는 Ethereum dApp Registries[12]과 유사한 PolySwarm 작업자 등록부의 명단을 통해 자신의 전문성을 홍보하고 유사한 바운티에 참여하여 성공함으로써 공개적으로 평판을 누적합니다.

바운티는 오퍼보다 저렴하고, 미리 특정 전문가를 알고 있을 필요가 없지만 모두에게 제공되는 것은 아닙니다.

첫째, 바운티는 이더리움 블록으로 채굴되어야 합니다. 이더리움 블록은 약 15초마다 발생합니다. 이러한 조건에서 가장 유리한 시간 비용에 해당합니다. 둘째, 바운티를 걸 때는 아티팩트를 공개해야 합니다[13]. 정보를 모두 공개하고 공개된 장소에 게시하지 않으면, 서부 개척 시대식 "현상수배(Wanted)" 포스터는 그다지 쓸모가 없을 것입니다. 마찬가지로, 바운티는 바운티 제공자가 아티팩트를 격리하거나 격리를 해제할 만한 정보를 제공하겠다는 공개적인 전자식 (계약에 명시된) 약속입니다. 또한, 바운티는 *사실*을 성립시키는 피드백 루프의 중요한 구성 요소입니다.

12 자세한 정보는 28쪽의 **작업자 등록부** 를 참조하십시오.

13 PolySwarm 1.0에는 맞지만, 이후 버전에서도 적용될지는 알 수 없습니다. **아티팩트 기밀유지를 참조하십시오.**

정확도에 따른 보상

오늘날의 시장과 달리, PolySwarm 시장은 위협 인텔리전스의 정확도에만 근거하여 정확한 보상을 제공하기 때문에 전문가들이 탐지 정확도에 최적화하고 (거짓 양성/음성 최소화) 대사가 고객을 대신하여 최대한의 가치를 창출할 수 있도록 지원합니다. PolySwarm은 전문가의 의견과 심판자가 정한 사실 사이의 일치 (불일치)로 정확도를 정의합니다.

이 정확도 피드백 루프는 PolySwarm 바운티에 따라 움직입니다. 각 바운티에서 정확한 의견을 제시한 전문가에게는 보상을 제공하고 부정확한 의견을 제출한 전문가에게는 불이익을 줍니다. 이 모든 것은 대사와 전문가가 결탁할 인센티브를 제거한 상태에서 적용됩니다[14]. PolySwarm 오퍼는 전통적인 1:1 거래 관계를 수립할 수 있는 편리한 수단이지만, 이러한 정확도 방정식이 적용되지 않습니다.

PolySwarm 시장에서 사실은 다음과 같이 생산, 소비됩니다.

1. 대사가 아티팩트에 바운티를 걸고 그에 따른 수수료를 납부합니다.

2. 바운티 의견 제출이 마감되기 전까지 여러 전문가가 이 아티팩트에 대한 의견을 제시합니다. 각각의 의견에는 전문가가 자신의 주장에 대한 자신감을 반영하여 스스로 선택한 NCT 금액(“입찰”)을 겁니다. 수수료는 이러한 “입찰” 비율에 따라 평가됩니다. 이러한 주장은 의견 제출이 마감 될 때까지 비밀에 부쳐집니다.

3. 대사는 전문가의 의견을 고려하여 재량에 따라 판정을 내리고, 고객에게 이를 전달합니다. 대사는 이러한 판정을 공개하여 평판을 올리고 수수료 할인을 받고자 합니다(자세한 내용은 추후 공개).

4. 시간이 지난 후(예: 아티팩트에 바운티가 걸리고 7일 후), 심판자들에게 아티팩트가 악성/양성인지 확인할 기회를 제공합니다. 나중에 확인된 사실은 아티팩트 판정을 신속히 전달하는 것을 저해하는 요소가 아닙니다. 즉, 대사는 고객에게 결과를 전달하기 전에 사실 판정을 기다릴 필요가 없고 이를 기다려서도 안 됩니다.

5. 정족수의 심판자가 아티팩트의 사실 여부를 판정합니다. 아직 사실에 대한 투표 전환 프로세스의 세부 사항은 결정되지 않았습니다. 단순 다수결 투표나 비례 다수결 투표가 될 가능성이 있습니다(예: 참가 시장 수 기준). 이와 관련된 상세한 정보는 프로토타입 개발에서 결정됩니다.

6. 사실이 확인된 후, 바운티 스마트 컨트랙트에 따라 정확한 의견을 제출한 전문가에게 NCT를 지급합니다. 지급하는 NCT 금액은 전체 정확한 입찰 풀 대비 전문가의 입찰 금액에 비례합니다.

14 **여기에는 전문가와 바운티에 투표하는 심판자가 결탁할 가능성도 포함됩니다. PolySwarm 수수료 구조는 단일 심판자가 사실을 흔들어서 결탁한 공모자가 바운티를 받게 하는 것보다 심판자가 시장에 의심을 주입하는 비용이 더 크게 설정되어 있습니다.**

표면상으로는 여기에 고전적인 예측 시장이 적합한 듯 보입니다. 전문가가 의견을 제출하고 나중이 이러한 의견을 사실과 비교한 다음, 최종적으로 정확도에 따라 보상과 불이익을 적용하기 때문입니다. 하지만, 고전적인 예측 시장은 모든 참가자가 사실을 검증할 수 있다고 암묵적으로 가정하기 때문에 PolySwarm에서는 문제가 됩니다. 선거 당선자를 묻거나 금 가격을 예상하는 예측 시장에서는 특정 날짜만큼 금액을 금액이 초과하더라도 쉽게 정산할 수 있습니다. 모든 참가자가 예측 기간이 끝난 후에도 데이터 지점을 검증할 수 있기 때문입니다. 누가 선거에서 이겼는지, 금 가격이 예측 가격을 넘어섰는지 확인할 수 있습니다.

의심스러운 아티팩트의 악의적 의도를 판정하는 작업에 필요한 전문성을 PolySwarm 참가자들이 모두 동일하게 보유하고 있지는 않습니다. 이러한 문제는 의료 진단에 적용되는 예측 시장과 유사합니다[15]. 여기서는 의사마다 전문성 정도가 다릅니다.

PolySwarm은 심판자에게 사실 판정을 맡깁니다. 오늘날의 시장에서 심판자의 역할은 기존의 안티바이러스 회사가 채우고 있습니다. 이 회사는 VirusTotal 등의 서비스를 통해 "사실"에 "투표"합니다(그리고 공개적인 책임을 집니다). PolySwarm 시장에서는 심판자들이 시장 참여에 따라 결정되며, 새로운 참가자에게 기득권을 흔들 기회가 제공됩니다.

요컨대 이 프로세스는 심판자들이 시장 전체의 이익에 따라 사실을 판정할 때 실사를 수행하는 데 리소스를 투자할 인센티브를 적절히 제공합니다.

엘리트 그룹이 사실 "판정자"로 활동하는 개념은 다른 부문에도 적용할 수 있습니다. 다른 사업자들이 사실을 알아내는 데 전문 지식이 필요한 토큰 플랫폼에서 이 메커니즘을 실험하게 될 것으로 예상합니다.

수수료

수수료(Fee)는 PolySwarm 시장에서 다양한 거래에 대해 평가되고, 2가지 목표를 달성하도록 설계되었습니다.

1. **최소한의 이더리움 가스 비용이 발생하는 활동에 인센티브를 제공하여 PolySwarm 시장의 효율을 향상합니다.** PolySwarm 거래에는 고정 수수료를 적용하여 불필요한 거래(스팸 거래 포함)로 인해 시장 전체에 불필요한 가스 비용이 발생하는 행동을 억제합니다. PolySwarm 이 수수료를 이더리움 가스 비용과 독립시키기 위해서는 PolySwarm 시장에 반드시 NCT가 필요합니다.

2. **능동적인 PolySwarm 시장 참가자에게 (정직한) 참여에 비례하여 보상을 제공합니다.** 수수료는 아티팩트 소개를 통해 PolySwarm 생태계를 적극적으로 활용하는 참가자(바운티를 게시하는 대사)와 아티팩트의 악의적 의도에 대한 사실을 판정하는 참가자(사실 판정에서 정족수에 해당하는 심판자)에게 수수료를 지급합니다.

PolySwarm 팀은 네트워크 개발 시 상기 언급한 수수료 구조를 제거하고 건전한 시장을 가장 잘 촉진할 수 있는 방식으로 필요에 따라 반복 적용할 것입니다.

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

대사가 지급하는 바운티 게시 수수료

대사가 PolySwarm 시장에 바운티를 걸면, 스마트 컨트랙트에 보관된 자금에 따라 다음과 같은 수수료가 부과됩니다.

1. **정액 등록 수수료.** 수수료가 정액이기 때문에 대사는 여러 아티팩트를 하나의 바운티로 모아서 시장 전체의 네트워크에 대한 부담과 가스 비용을 줄일 수 있습니다.

2. **바운티에 비례하는 수수료.** 초기 바운티 금액이 높은 것이 더욱 적극적인 전문가 반응을 이끌어낼 것입니다. 이 비례 수수료는 전문가의 관심도(및 네트워크 부담)에 따라 수수료를 조정합니다.

전문가가 지급하는 바운티 의견 제출 수수료

전문가가 바운티에 대해 의견을 제출할 경우, 스마트 컨트랙트에 보관된 자금에 따라 다음과 같은 수수료가 부과됩니다.

1. **정액 의견 제출 수수료.** 이 정액 수수료는 네트워크 속도를 저하시키는 반복적 의견 제출을 억제합니다.

2. **입찰 금액에 비례하는 수수료.**

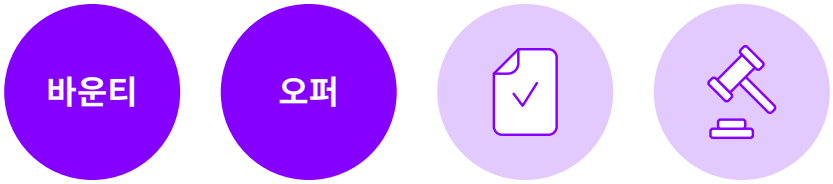
오퍼 채널 정산: 대사 수수료

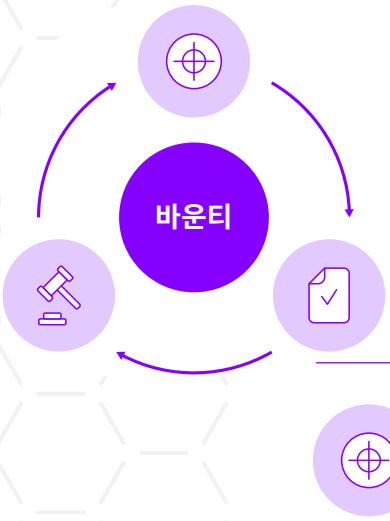
오퍼는 Raiden 스타일 오퍼 채널에서 발생하며, 대사와 전문가 사이에 직접 성립합니다. 대사 및/또는 전문가가 오퍼 채널을 블록체인에 설정하기로 결정하는 경우, 채널 스마트 컨트랙트에서 다음과 같이 수수료를 부과합니다.

1. **채널로 전송되는 순 NCT의 비율.** 이 수수료는 채널을 열었을 때 대사가 제공하는 토큰에 따라 평가합니다. 채널이 닫히면 이 수수료는 사용하지
않은 채널 토큰에 비례하여 대사에게 반환됩니다.

프로토콜 상세 정보

여기서는 PolySwarm 바운티, 오퍼, 의견, 판정에 대해 자세히 설명합니다. 바운티와 오퍼는 총칭하여 PolySwarm 등록이라고 합니다. PolySwarm 보고서는 바운티, 오퍼, 의견 또는 판정의 형태를 띠고 있습니다.





바운티 수명 주기

대사가 시장에 바운티를 걸고자 할 경우,
대사는 PolySwarm 바운티 스마트
컨트랙트에 요청하여 내역서를 등록합니다.

바운티 내역서에는 다음 항목이 포함됩니다.

1. **등록 GUID:** 등록을 위해 사용되는 전역 고유 식별자입니다.
2. **대사의 ID.** 내역서에 서명하는 형식으로 표시되며, 대사 주소를 가지고 있는 사람이면 누구나 확인할 수 있습니다(주소에서 얻은 공개 키).
3. **바운티 게시 수수료.** 고정 금액 + 바운티 비율(상기 "수수료" 섹션에서 설명) 입니다. 대사가 나중에 판정을 공개적으로 제출하면 할인이 적용됩니다.
4. **바운티.** 이 금액은 바운티 게시 수수료와 함께 스마트 컨트랙트에 공개되며, 정확한 의견을 제출한 전문가에게 지급됩니다(전문가 응답이 없을 시 환불). 이 금액은 이더리움 또는 비트코인의 거래 수수료와 유사하며, 바운티에 주의를 집중시킬 때 유용합니다.
5. **아티팩트의 암호화 해시.** 구성할 수 있지만, 현재는 SHA256로 설정되어 있습니다. 이는 아티팩트를 고유하게 식별합니다.
6. **아티팩트의 URI.** 저장 비용으로 인해 아티팩트는 체인에 저장하지 않습니다. 아티팩트 저장과 전달을 아웃소싱하는 2차 시장이 나타나서[16] 일부 대사가 이후 경쟁력 분석을 위해 모든 평가한 아티팩트 사본을 보관하게 될 것으로 예상합니다.
7. **의견 제출 마감:** 의견 제출 마감 기한입니다. 대사는 특정 아티팩트에 적용되는 요건에 따라 분석 기간을 연장/단축할 수 있습니다. 심층적 분석이 필요한 아티팩트는 시간이 더 많이 필요하고(또한, 주의를 끌기 위해 높은 바운티를 걸 것입니다) 어떤 아티팩트는 빠른 마감이 필요할 경우도 있을 것입니다.

바운티가 게시되면 전문가는 아티팩트가 자신의 기술에 맞는지, 예상한 보상이 적절한지 결정합니다. 예상 보상은 아티팩트의 악의적 의도 판정에 대한 이들의 신뢰도(확신도)에 따라 달라집니다.

참가하기로 결정한 전문가는 자신의 신뢰도(및 위험 감수도)를 나타내는 의견 입찰을 제출합니다. 바운티와 모든 부정확한 입찰 합계 금액을 정확한 입찰에 지급하며,
이 금액은 전체 정확한 입찰 금액 대비 각 전문가의 입찰 금액에 비례합니다.

16 위 내용 및 기타 예상 보조 시장에 대한 의견은 추후 제공될 예정입니다.

다음 예시를 참조하십시오(단순화하기 위해 수수료는 제외했습니다).

1. 대사가 2 NCT로 바운티를 게시합니다. 이 2 NCT는 바운티 스마트 컨트랙트에 보관됩니다. 현재까지는 2 NCT 바운티가 정확한 의견을 제출한 전문가가 가져갈 전체 "포상금(pot)"입니다.

2. 전문가 A와 전문가 B가 아티팩트를 살펴보고 해당 아티팩트가 *양성*이라는 의견을 제출하기로 했습니다. 이들은 각각 자신의 의견에 5 NCT와 3 NCT를 입찰합니다.

3. 전문가 C와 전문가 D가 아티팩트를 살펴보고 해당 아티팩트가 *악성*이라는 의견을 제출하기로 했습니다. 이들은 각각 자신의 의견에 1 NCT와 4 NCT를 입찰합니다.

4. 시간이 지나서 심판자가 사실을 판정하고 아티팩트가 *악성*인 것으로 결정했습니다. 그러므로 전문가 A와 B는 *부정확*한 의견을 제출하였고, 전문가 C와 D는 *정확한* 의견을 제출하였습니다.

5. 바운티와 전문가 A와 B가 제시한 입찰 금액의 합계가 "포상금"을 구성하고, 전문가 C와 D에 비례적으로 지급됩니다. 포상금은 2 + 5 + 3 = 10 NCT입니다.

6. 전문가 C는 정확한 의견을 제출했고 입찰 금액은 정확한 의견을 제시한 입찰 금액 합계의 1/5입니다. 전문가 C는 자신의 포상금과 입찰금을 돌려받습니다. 1 + 1/5 * 10 = 3 NCT.

7. 전문가 D는 정확한 의견을 제출했고 입찰 금액은 정확한 의견을 제시한 입찰 금액 합계의 4/5입니다. 전문가 D는 자신의 포상금과 입찰금을 돌려받습니다. 4 + 4/5 * 10 = 12 NCT.

바운티 의견 제출에는 다음 내용이 포함됩니다.

1. **등록 GUID + 암호화 해시:** 홍보 중인 바운티 등록에 대한 고유한 참조 정보입니다.

2. **전문가 ID:** 마찬가지로 내역서의 서명에 해당합니다.

3. **의견 제출 수수료:** 고정 금액 + 입찰 금액 비율입니다("수수료" 섹션 참조).

4. **입찰 금액.**

5. **의견:** 아티팩트의 악의적 의도에 대한 "악성" 또는 "양성" 부울을 의미합니다. 바운티 의견 제출 마감이 지날 때까지 의견은 공개하지 않습니다. 블라인드 제출 + 공개 기간을 결합한 방법으로 비밀을 유지할 수 있을 것으로 생각합니다.

6. **(선택)메타데이터:** 의견을 형성할 때 얻은 정보를 판정 계산에 활용하도록 대사에게 부가가치로 제공하는 정보입니다(예: 멀웨어군). 전문가는 자신을 차별화하고 향후 사업을 유치하기 위한 수단으로 이 정보를 자발적으로 제공할 수 있습니다.

의견이 제출되는 동안 대사는 의견을 평가하고, 내부 실사 활동을 결합하여 "악성" 또는 "양성" 판정을 내립니다. 대사는 아티팩트의 악의적 의도에 대한 최종 응답으로 이 판정을 고객에게 전달합니다. 대사는 판정 마감이 다가오기 전에 판정을 공개할 수 있습니다(수수료 할인을 통해 판정 공개 권장).

공개된 판정에는 다음 항목이 포함됩니다.

1. **등록 GUID:** 홍보 중인 바운티 등록에 대한 참조 정보입니다.

2. **대사의 NCT ID.** 마찬가지로 내역서의 서명에 해당합니다.

3. **판정:** 아티팩트의 악의적 의도에 대한 “악성” 또는 “양성” 부울을 의미합니다.

시간이 지나면, 심판자 수는 정족수에 도달하여 아티팩트에 대한 사실을 판정합니다. 이렇게 판정된 사실은 각 전문가의 의견과 비교하고 정확한 의견을 제출한 전문가에 NCT를 지급합니다.

오퍼 수명 주기

대사가 특정 전문가에게 오퍼를 발행하고자 할 경우, 대사가 Raiden 스타일 채널을 전문가에게 개방합니다.

다음을 포함한 전문가와의 **오퍼 채널** 스마트 컨트랙트를 인스턴스화합니다.

1. **대사와 전문가의 ID.**
2. **채널 잔고:** 대사가 채널 종료 시각에 전문가에게 정산하고자 하는 최대 순 NCT(+수수료).

오퍼 채널이 설정되면 대사가 0개 이상의 오퍼를 전문가에게 발행합니다.
각 오퍼에는 다음이 포함됩니다.

1. **등록 GUID:** 등록을 위해 사용되는 전역 고유 식별자입니다.
2. **오퍼 금액.** 이 금액은 오퍼 채널 스마트 컨트랙트 잔액(-수수료)를 초과할 수 없습니다.
3. **아티팩트의 암호화 해시.**
4. **아티팩트의 URI.** 아티팩트는 오퍼를 받는 사람에 대해 암호화하거나 다른 방식으로 액세스를 차단하여 비밀을 유지할 수 있습니다.
5. **참여 마감:** 참여 응답 마감(아래에 설명).
6. **의견 제출 마감:** 이 오퍼에 대한 의견 제출 마감.

오퍼가 제출되면 전문가(오퍼를 받는 사람)는 오퍼를 수락하거나 거절할 수 있습니다. 각 오퍼를 받는 사람은 기간과 오퍼 금액에 비해 오퍼를 평가할 가치가 있는지 결정합니다.

오퍼를 받는 사람은 정확한 결과를 제출하는 능력에 따라 향후 사업 운영이 달라집니다. 오퍼를 받는 사람이 일정 기간에 정확한 결과를 제출할 자신이 없을 경우(예: 아티팩트가 분석할 수 없는 파일 형식일 경우) 오퍼를 거절할 수 있습니다.

오퍼를 받는 사람이 오퍼를 거절할 경우, 참여 “거절문”을 발행하거나 참여 마감이 만료되기를 기다립니다. 오퍼를 받는 사람이 참여 마감을 기다리기보다는 적극적으로 거절해야 할 가능성이 큽니다. 대사는 미리 거절하여 다음 단계로 진행할 수 있게 해주는 전문가를 선호할 가능성이 크기 때문입니다.

오퍼를 받는 사람이 오퍼를 수락하면 참여 마감 전에 참여 “수락문”을 발행합니다.

참여 내역서에는 다음 항목이 포함됩니다.

1. **등록 GUID + 해시:** 홍보 중인 바운티 등록에 대한 참조 정보입니다.
2. **참여 신청:** 오퍼를 받는 사람이 오퍼에 참여하고 오퍼의 의견 제출 마감일 전에 의견을 제출할 것을 약속하는 “수락” 또는 “거절” 부울.

오퍼를 받는 사람이 오퍼를 수락하면 의견 제출 마감일까지 오퍼에 대한 의견을 제출해야 합니다.

이런 **의견**에는 다음 항목이 포함됩니다.

1. **등록 GUID + 해시:** 홍보 중인 바운티 등록에 대한 고유한 참조 정보입니다.
2. **의견:** 아티팩트의 악의적 의도에 대한 “악성” 또는 “양성” 부울을 의미합니다.
3. **(선택)메타데이터:** 의견을 형성할 때 얻은 정보를 판정 계산에 활용하도록 대사에게 부가가치로 제공하는 정보입니다(예: 멀웨어군). 전문가는 자신을 차별화하고 향후 오퍼를 얻기 위한 수단으로 이 정보를 자발적으로 제공할 수 있습니다.

전문가가 대사에게 자신의 의견을 제출하고 나면, 대사가 오퍼 금액을 제공할 것을 약속하는 Raiden 스타일 메시지에 서명합니다. 그러므로 전문가는 1회만 분석하면 됩니다. 모든 전달된 금액의 합계는 오퍼 채널이 종료되었을 때 블록체인에 정산됩니다.

바운티와 달리 오퍼는 체인 내 사실 판정 피드백 메커니즘이 없습니다. 대신 마감 전에 의견을 제출하지 못하거나 부정확한 의견(나중에 체인 외부 분석에서 결정)을 제출한 전문가는 향후 오퍼를 받지 못할 수 있습니다. 그러므로, 평판 관리가 체인 외부 피드백과 유사한 역할을 하여 오퍼를 받는 사람이 정직성을 유지하도록 시장 차원에서 압력을 넣습니다.

오퍼 채널이 종료되면, 전송된 순 NCT에서 수수료를 징수합니다. 다른 수수료와 마찬가지로 이 수수료는 능동적인 시장 참가자에게 지급됩니다. 이 수수료는 마스터 오퍼 채널 스마트 컨트랙트에서 집행하고, 여기서는 규칙을 따르지 않는 오퍼 채널을 설정할 수 없습니다.

평판

다른 토큰 플랫폼(예: Augur)과 달리, **PolySwarm은 평판의 개념을 공식화하지 않고 시장 거래 내부에 포함시켰습니다.**

그 이유는 간단합니다. 여러 시장 참가자가 어느 데이터 지점에 가치를 두는지, 이러한 데이터 지점을 어떻게 평가하는지 예측하기 어렵기 때문입니다. 대사 A에 알맞은 것이 대사 B에게도 맞는다고 할 수 없으므로, 일괄적인 가정으로 두 사람이 움직이게 하는 것은 소용이 없습니다. 그래서 PolySwarm의 역학은 평판에 영향을 미칠 만한 유용한 입력값으로 대표되는 데이터 종류를 공개하도록 의무화하거나
그러한 인센티브를 제공합니다.

평판 알고리즘은 의견을 판정으로 정제하는 알고리즘과 마찬가지로 영업 기밀로 간주될 가능성이 큽니다. 대사는 자신의 아티팩트 워크로드에 가장 알맞은 전문가에게 접근하여 자신을 차별화할 것입니다. 전문가는 사실에 부합하는 정확한 의견을 제출한 기록을 유지함으로써 자신을 차별화할 것입니다. 또는, 아티팩트가 감염되었다고 생각하는 멀웨어군 등의 메타데이터를 제공할 수도 있습니다.

앞으로 개발된 대사 시스템 구현 프로토타입에서는 다양한 데이터 지점을 단순한 평판 "점수"와 이해하기 쉬운 색상표로 정리할 예정입니다. 이러한 참조 자료 정리는 대부분에게 유용하겠지만, 참가자가 원하는 대로 교체/수정될 수 있습니다. 전문가는 대사를 평가하는 평판 시스템을 구현하기를 원할 수 있으나, 이런 시스템의 비즈니스 로직은 더욱 복잡하고 참가자마다 상당히 다를 수 있습니다.

참조 PolySwarm 디먼(daemon)은 오래된 데이터를 "*감쇠*"시켜서 참가자 평판을 "*밀어내기*" 방식으로 관리할 것입니다. 이러한 밀어내기 방식을 사용해야 새로운 시장 참가자의 진입이 차단되지 않을 것입니다.

참조 대사 구현에서는 다음의 데이터 지점을 활용할 예정입니다.

1. **의견 정확도**(사실 및/또는 체인 외부 분석과 비교).

2. **바운티와 오퍼에 대한 응답 빈도 및 평균 응답 시간.** 오퍼의 경우, 대사는 오퍼 채널에서만 관찰 가능한 집계 데이터를 공개할 수 있습니다. 대사는 빠르고 일관적인 응답 시간을 보여주는 전문가를 선호할 수 있습니다.

3. **오퍼에 제공된 아티팩트의 기밀을 유지할 수 있는 능력.** 시장 내부, 시장 외부 분석을 모두 포함할 가능성이 큽니다.

대사는 경쟁자의 과거 판정을 검토하고 오류를 찾아낼 수 있습니다(예: 대사 A는 어떤 샘플이 사실 악성인데 양성으로 판정했다고 언급). 전문가는 전반적으로 실사를 하지 못하거나 특정 상황에서 자주 틀리는 대사와의 거래를 회피할 가능성이 큽니다(예: 대사 A는 Microsoft Word 문서를 자주 잘못 분류하여, 특정 전문가들이 대사 A를 대신하여 Word 문서 분석을 회피하는 경우). 즉, 전문가는 대사의 판정 정확도에 주로 관심을 보일 것입니다.

소비자는 종합적인 소비자 보고서 또는 대사의 실적을 보여주는 AV 비교식 웹사이트와 게시물을 이용하여, 악의적 의도가 있는 것으로 알려진 샘플과 대사가 고객에게 제출한 판정이 일치하는지 확인할 수 있습니다.

작업자 등록부

PolySwarm 생태계의 전문가는 대부분의 경우, 전문성을 자동화된 작업자에 담을 것입니다. *작업자(Worker)*는 바운티와 *오퍼*에 자동 응답하는 시스템으로, 특정 파일 유형이나 네트워크 트래픽에 전문화되어 있을 수 있습니다. PolySwarm 시장은 전문가가 무엇을 제공하는지 쉽게 발견할 수 있도록 탈중앙형 작업자 등록부를 제공합니다.

작업자를 공개 등록하기 위한 공통 인터페이스와 기술어를 개발할 예정입니다. 이러한 구성 요소는 PolySwarm 등록부와 상호작용하고, 이는 처음의 Ethereum dApp 등록부 스마트 컨트랙트를 모방합니다. PolySwarm 작업자 등록부는 특정 기술 세트를 홍보하는 설명이 포함되어 있습니다(예: “Mac OS Mach-O 바이너리 전문” 또는 “Microsoft Word 문서 처리”).

아티팩트 기밀 유지

PolySwarm 시장에서는 *오퍼* 도구를 통해 가장 엄격한 아티팩트의 기밀 정보 공개 기능을 제공합니다. 그러나 추가적인 예방 조치를 기울이지 않을 경우, 오퍼를 사용하는 대사는 보안 전문가의 의도와 범죄자를 영구히 차단할 수 있는 기술적 능력을 신뢰할 수밖에 없습니다.

이러한 신뢰의 필요로 인해 2차 시장이 나타나고, 신뢰를 최소화하거나 강화하기 위한 새로운 기술 응용 방식이 나타날 것으로 생각합니다. PolySwarm에서 기밀 유지 요구 사항을 해결하기 위해 내장한 도구의 예시는 다음과 같습니다.

Intel SGX를 통한 신뢰 최소화

Intel SGX는 Skylake 프로세서 제품군과 함께 제공되는 신기술입니다. SGX는 상위 수준에서 “엔클레이브(enclave)” 내에 불투명한 연산 환경을 제공합니다. SGX 엔클레이브의 메모리 내용은 권한 수준과 관계없이 동일한 시스템의 다른 소프트웨어와 사용자에게 제공되지 않습니다. PolySwarm의 경우, SGX 엔클레이브는 전문가가 아티팩트를 조사자에게 공개하거나 전문가의 인텔리전스를 다른 사람에게 공개하지 않고 전문가가 아티팩트를 스캔할 수 있게 해줍니다. 그러므로 SGX는 대사와 전문가 사이의 상호 신뢰를 낮춥니다.

전문가는 아티팩트와 자신의 인텔리전스가 입력된 공인(및 입증된) SGX 엔클레이브를 실행하여 의견을 생성하고 대사에 제출할 수 있습니다. 극복해야 할 기술적 장애가 있지만, 탈 중앙형 방식으로 인클래브를 서로 부트스트래핑하면서 SGX를 내장, 확장할 수 있으리라 생각합니다. 이후 PolySwarm을 반복 적용하면서 대사가 PolySwarm 시장에 "SGX 바운티" 내역서를 작성하여 아티팩트를 부트스트랩된 엔클레이브에만 공개하는 기능을 개발할 수도 있습니다.

SaaS(Scan-as-a-Service) 대사를 통한 신뢰 강화

전문가는 PolySwarm에서 기인한 사유 또는 그 외의 여러 가지 이유로 제3자에게 연산 작업을 위탁할 수 있습니다. 예를 들어, 많은 전문가가 AWS, Google Compute Engine, Azure 또는 기타 온디맨드 연산 서비스를 활용하여 PolySwarm 시장 수요에 맞추어 의견 제출 파이프라인을 확장할 것으로
기대합니다. 이는 오로지 PolySwarm으로 인한 연산 결정은 아닙니다.

SaaS 엔티티가 자연스럽게 나타날 수 있도록 PolySwarm에서 인센티브를 제공할 것입니다. 기밀 유지와 관련하여, 참가자들은 대사와 전문가 사이에서 신뢰할 수 있는 제3자 역할을 하는 SaaS 회사를 설립하고 두 주체 사이에서 기밀 유지 계약을 관리할 것입니다. 이러한 SaaS 기업은 SGX 엔클레이브와 마찬가지로 전문가로부터 아티팩트를 보호하고 대사로부터 전문가의 인텔리전스 상세 정보를 보호합니다.

대사는 신분을 알 수 없는 여러 개인 전문가보다는 공개적으로 평판이 알려진 제3자 SaaS 엔티티를 신뢰하기 쉬울 것입니다. 이런 대사는 전문가보다는 SaaS 엔티티를 대상으로 한 오퍼를 더 많이 작성할 것입니다.

추가 시장

PolySwarm 시장은 여러 가지 추가 시장 수요를 창출할 것입니다. 추가적인 기밀 유지 관리와 관련하여 앞서 이러한 시장 (Scan-as-a-Service)을 설명했습니다. 다음은 그 외에 추가로 발생할 가능성이 있는 시장의 예시입니다.

대사

분명히 나타날 만한 시장이고, 본 문서 전체에서 상세히 설명하였습니다. 많은 소비자가 대사를 통해 시장과 거래를 하고자 하겠지만, 반드시 대사를 통해 거래해야 하는 것은 아닙니다.

아티팩트 게시 서비스

바운티나 오퍼를 게시할 때 대사는 전문가에게 아티팩트를 제공해야 합니다.
아티팩트 호스팅 엔티티가 이러한 서비스를 제공하여 매끄럽게 아티팩트를 공유할 것입니다.
이들의 고객은 소비자와 대사입니다. 많은 대사가 아티팩트 게시
서비스를 제공할 것으로 예상합니다.

평판 추적 서비스

미국에서는 은행들이 각 개인의 신용도에 대한 “실제 정보(facts)”를 관리할
때 3개의 신용 평가 기관을 이용하고 있습니다. PolySwarm 시장에서도 유사한 수요가 나타날 것입니다. 시장 참가자들은 앞서 설명한 여러 가지 이유로 각
참가자의 신뢰도를 측정하고 싶어 할 것입니다. 참가자의 신용도를 추적하고 이러한 정보를 제공하여 상대방의 위험을 완화하는 평판 서비스가 등장할 가능성이 큽니다.

로드맵

PolySwarm의 예상 개발 마일스톤은 다음과 같습니다. 각 마일스톤은 (1) 새로운 기능을 제공하고 (2) 새로운 대사, 전문가, 최종 사용자 거래를 지원하는 문서와 테스트를 제공합니다.

PolySwarm은 모든 거래 기록을 영구적으로 보관해야 하는 비트코인이나 이더리움 등의
네트워크에 비해 개발 시 장점이 명확합니다. 사실이 판정되거나 오퍼 채널이 체인에서 종료되면, 대사와 전문가는 해당 거래에서 받아야 할 것, 즉 아티팩트와 관련된 인텔리전스와 NCT를
받습니다. 이러한 원소성은 자율을 제공하며, 따라서 다른 네트워크에서 발생하는 비용이나 동의 문제 없이 1.0 릴리스까지는 이전
버전과 호환되지 않는 영구적인 변경 사항을 적용할 수 있습니다.

V0.1 Alpha (2018년30월4일)

PolySwarm Alpha는 토큰 판매가 완료된 후 바운티에 대한 종단간 워크플로 프로토타입을 제공합니다. 이 최초 릴리스에서 PolySwarm 팀은 본격적으로 부트스트래핑 프로세스를 시작할 것입니다. 대사와 전문가는 PolySwarm 테스트 네트워크(“테스트넷”)를 통해 거래합니다.
PolySwarm 테스트넷에 기본적인
바운티 스마트 컨트랙트가 제공되어, 대사는 바운티를 게시하고 전문가는 의견을 제출한 다음 대사가 판정을 내릴 수 있게 됩니다.

PolySwarm Alpha는 다음과 같은 기능이 적용됩니다.

- 바운티 금액과 수수료를 보관하고, 의견을 받고, 판정을 게시하고,
  정확한 전문가에게 보상을 제공하는 “바운티 관리자” 스마트 컨트랙트

- PolySwarm 스토리지에서 아티팩트를 게시/조회(예: S3 및/또는 IPFS)
- 바운티 만료 시 심판자를 선정하는 알고리즘 프로토타입
- 바운티 게시, 의견 제출 응답, 심판자 사실 판정을 위한 참조 구현

V0.2 Beta (2018년31월5일)

PolySwarm Beta는 PolySwarm 오퍼를 Raiden 스타일 채널을 통해 지원하는 데 집중합니다. 오퍼는 바운티에 비해 더욱 많은 양의 아티팩트 평가를 처리할 수 있도록 설계되고, 따라서 각 거래에서 더욱 효율적인 블록체인 정산을 요구하게 될 것입니다. PolySwarm Beta는 오퍼 스마트 컨트랙트를 구현할 것입니다. 이 계약은 테스트넷을 사용하는 대사와 전문가가 직접적인 P2P Raiden 스타일 채널을 설정하는 기능을 구현할 예정입니다.

PolySwarm Beta는 다음과 같은 기능이 적용됩니다.

- 오퍼 채널
  - 탈 중앙형 채널 설정
  - 단일 채널을 통해 다중 오퍼
  - 채널 종료 시 NCT 정산
- 오퍼 생성 및 응답에 대한 참조 구현
- 심판자 사실 판정 알림 및 응답을 위한 참조 구현
- 수수료 징수 및 분배 스마트 컨트랙트
- 특정 아티팩트 볼륨에 필요한 신뢰 조사 및 측정(NCT 기준)
- 오퍼/바운티 개발 툴킷: 전문가 및 대사가 바운티/오퍼를 자동 서비스할 수 있는 프레임워크 테스트 및 구현

V0.3 Gamma (2018년31월7일)

PolySwarm Gamma는 대사, 전문가, 심판자 사이의 협력을 촉진하는 매칭 기능을 제공하는 데 초점을 맞춥니다. 전문가는 특정 아티팩트 유형에 맞추어 작업자에 전문 지식을 담을 수 있습니다. 이러한 작업자를 PolySwarm 등록부에 홍보할 수 있을 것입니다. 이 작업자 등록부는 Stable 릴리스 이전에 대사가 위험 없이 작업자와 거래할 수 있도록 지원합니다(Gamma는 PolySwarm 테스트넷을 계속 활용).

또한, 이 릴리스는 Alpha 및 Beta의 피드백과 경험을 반영하여 바운티 도구를 강화, 확장할 것입니다. 예를 들어, 바운티는 다른 전문가에게 공개되지 않고 의견 제출 마감이 지난 후에만 공개되는 기능이 적용될 것입니다.PolySwarm Gamma는 다음과 같은 기능이 적용됩니다.

- 아티팩트 분석 능력과 전문가 작성 출처(평판에 사용)를 설명하는 작업자 기술어(WDL)

- 작업자와 그 기능의 검색 가능한 분산 등록부.
- 마감 전 바운티에 제출된 의견 기밀 유지
- 심판자 선정, 응답, 종단간 바운티 피드백 루프 확정

Gamma에서 기능이 완성될 것으로 예상합니다.

Polyswarm 1.0 (2018년 Q4)

PolySwarm Stable은 PolySwarm 테스트넷(테스트 토큰)에서 실제 PolySwarm 시장으로 이동하기 전에 PolySwarm Gamma의 버그를 제거하는 데 집중할 것입니다.

도전 목표와 시간/자금 여유에 따라, Stable에 대상을 제한하는 바운티 제도를 통해 1등급 아티팩트 기밀 유지 기능을 도입할 수도 있습니다.

Polyswarm 2.0 (2019년 Q2)

현재 PolySwarm의 2차 안정화 릴리스는 2가지 목표가 있습니다. 오퍼와 바운티에서 다양한 아티팩트 형식(예: URL과 네트워크 스트림)을 처리하고 기업과 가정 사용자가 PolySwarm을 간편하게 사용할 수 있도록 하는 것입니다.

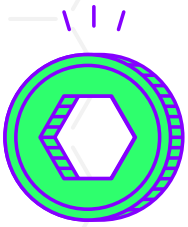
향후 PolySwarm 릴리스에서 아티팩트 형식을 확대하면 호스팅 콘텐츠에 대한 바운티와 오퍼를 직접 게시하여 최종 사용자 URL의 피싱 시도를 자동으로 탐지할 수 있을 것입니다.

안정화 이후부터는 PolySwarm의 보호 기능을 엔드포인트까지 직접적으로 확장하는 것을 우선합니다. PolySwarm의 인텔리전스에 기초하여 악성 아티팩트를 자동으로 차단하는 엔드포인트 보호 스위트의 오픈 소스 참조 구현을 개발할 예정입니다. 이러한 오픈 에이전트 프레임워크는 최종 사용자의 사용을 확대하는 열쇠로 작용할 것입니다.

향후 도입 기능

향후 PolySwarm 릴리스에서는 최신 위협 동향과 실제 네트워크 사용을 반영할 것입니다. PolySwarm 사용량을 관찰한 결과에 따라 다음 기능으로 네트워크는 물론이고 최종 사용자 보호라는 목표에 여러 가지로 도움이 되리라 생각합니다.

- 유연한 아티팩트 기밀유
  - 기본: 아티팩트는 전문가 또는 SaaS 제공업체에 선택적으로 공개됩니다.
  - 고급: 아티팩트는 완전히 동형 엔진의 SGX 엔클레이브 외부에는 절대 공개되지 않습니다.
- 새 도구(예: 구독이 가능한 위협 피드)
- 현재의 엔드포인트 보호 스위트를 대체하는 엔드포인트 상주 작업자 컨테이너에 대한 배포 지원



토큰 판매

기술 개발, 커뮤니티 참여, PolySwarm 생태계 참가자 지원은 PolySwarm Pte. Ltd.가 PolySwarm's Nectar 유틸리티 토큰 (NCT) 판매로 얻은 자금으로 수행합니다.

이러한 토큰은 참가자가 위협 인텔리전스와 교환합니다. NCT는 바운티 게시, 오퍼 채널 설정/해체/교환, 의견 등록 및 사실 판정과 같은 모든 주요 PolySwarm 거래에서 사용됩니다. 유틸리티별 NCT 토큰을 판매함으로써 NCT와 위협 인텔리전스의 환율은 규모가 큰 이더리움(ETH) 시장의 변동성과 분리됩니다.
따라서, ETH 변동을 염려하지 않고 PolySwarm에 능동적으로 참여할 수 있습니다.

이 섹션에서는 PolySwarm 토큰의 역학을 간략히 설명할 것입니다. 이 문서와 토큰 판매 계약(“계약”) 사이에 상충이 발생할 경우, 계약을 우선합니다.

토큰 판매 계약은 온라인에서 확인할 수 있습니다.

일정

PolySwarm Pte. Ltd. 는 현재 초청한 참가자를 대상으로 토큰을 사전 판매 중입니다. 공개 NCT 판매는 2018년 2월 6일 19:00 UTC에 적격 구매자에게 공개할 예정입니다. 판매는 2018년 3월 8일 19:00 UTC에 종료됩니다.

판매 요건

NCT는 이더리움(ETH)으로만 구매가 가능합니다. 잠재적 구매자께서는 판매 전에 충분히 ETH를 확보하시는 것이 좋습니다.

토큰 판매는 고객 알기 제도(Know Your Customer, KYC) 관리 및 고유한 기술적 메커니즘의 결합을 통해 다음과 같은 KYC 데이터 지점과 구매를 연계합니다. 출신 국가, 이메일 주소, 이름, IP 주소, 토큰 판매 계약 이용약관 수락.

상한/제한

새 토큰은 토큰 판매 기간이 종료된 후 생성됩니다.

NCT 토큰의 총 개수는 토큰 판매 중에 결정합니다.

토큰 개수는 상한이 있습니다. 이 상한은 최대 자금 지원 달러(USD) 상한, NCT 가격(ETH 기준), 현재 ETH-USD 환율에 따라 결정됩니다. NCT 상한, 가격, 자금 분할 등의 자세한 정보는 토큰 판매 웹페이지를 참조하십시오.

할당

NCT 토큰의 70%는 토큰 판매 기간 중 판매가 완료됩니다.

나머지 50% 중의 15%는 PolySwarm 생태계를 부트스트랩하는 데 관심이 있는 기업, 전문가, 벤더, 보안 전문가에게 “배분”됩니다. 수령자는 PolySwarm Pte. Ltd.의 단독 재량으로 결정합니다.

나머지 15%는 PolySwarm Pte. Ltd.가 PolySwarm 생태계 도입을 촉진하는 데 가장 좋은 방법으로 사용할 것입니다. 예를 들어, 토큰을 PolySwarm “해커톤”에 참가할 인센티브로 사용할 수 있습니다.”. 이러한 할당은 PolySwarm Pte. Ltd.의 단독 재량으로 결정됩니다.

분배

PolySwarm의 Nectar 유틸리티 토큰(“NCT”) 판매로 얻은 ETH는 다음과 같이 분배할 예정입니다.

- **54.51%** –프로토콜 및 소프트웨어 개발
- **3.00%** – 사무실 운영비
- **4.06%** – 간접 운영비(출장, 호스팅 등)
- **14.49%** – 법무 관련 지출
- **13.62%** – 마케팅 관련 지출
- **10.32%** – 세금

PolySwarm 팀은 2019/2020년에 법무 지출이 증가할 것으로 예상합니다. 잉여금은 마케팅, 간접비, 개발자 연봉으로 재분배됩니다.

예상 세금 10.32%는 낮은 편이지만 불합리할 수준은 아닙니다. 자금이 PolySwarm의 개발과 홍보에 할당되기 때문에,
참가자는 펀딩 자금이 많을수록 더 많은 이익을 얻게 될 것입니다.

면책

이 백서는 미래의 토큰 구매자에게 기술적 배경을 제공하기 위해 작성되었습니다. PolySwarm 토큰 판매 자금은 본 문서에서 설명한 경제적 도구의 첫 프로토타입 개발과 테스트에 이용됩니다. 여느 신중한 참가자와 마찬가지로, 당사도 본 문서에 기록된 세부 정보가 안정화 이전 개발 및 테스트 단계에서 변경될 수도 있음을 예상하고 있습니다. PolySwarm Pte. Ltd.와 토큰 구매자는 PolySwarm을 통해 위협 인텔리전스 산업에 진정한 와해를
일으킬 시장을 만드는 것에 이해관계를 함께 합니다.

결론

PolySwarm은 ERC20 토큰인 NCT와 연결된 신생 시장으로, 보안 전문가와 벤더, 기업 간의 새로운 상호작용을 촉진함으로써 위협 인텔리전스 산업에서 와해성 혁신을 일으키고자 합니다. PolySwarm 팀은 소프트웨어 개발 자금을 마련하고 새로운 시장을 중심으로 커뮤니티를 키우기 위해 토큰을 출시할 것입니다.

사용자를 **All Angles™**로부터 보호하는 데 동참해 주십시오.

polyswarm.io