

폴리스웜(Polyswarm)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다.

탈중앙화 사이버 위협 인텔리전스 마켓

Polyswarm

60초 안에 보는 폴리스웜

폴리스웜은 이더리움 스마트 계약과 블록체인 기술로 가능해진 탈중앙화 위협 인텔리전스 마켓입니다.

폴리스웜은 연간 85억 달러 규모의 안티바이러스 및 자동화된 사이버 위협 인텔리전스 시장에서 *시의적절*하고 *정확한* 위협 인텔리전스(파일, 네트워크 트래픽, URL의 악성 의도)에 대해 보상하는 정밀한 경제적 인센티브를 통해 빠른 혁신을 촉진합니다.

폴리스웜은 기업, 소비자, 벤더, 그리고 지리적으로 다양한 보안 전문가가 참여하는 실시간 위협 탐지 생태계를 정의합니다. 전문가들은 경쟁적인 *마이크로 엔진(micro-engines)*을 개발·연마하며 최신 위협을 자율적으로 조사하고 경쟁자를 능가하려 합니다. 폴리스웜의 *작업 증명(Proof of Work)*은 위협 탐지 정확도입니다. 마켓은 기업과 최종 사용자를 가장 잘 방어할 수 있는 전문가들에게 보상을 제공합니다.

오늘날의 임시적(ad hoc) 시장과 비교할 때, **폴리스웜**은 진입 장벽을 낮추고, 더 폭넓은 커버리지를 제공하며, 중복 노력을 방지하고, 제품 및 위협 인텔리전스 피드 간 상호운용성을 보장합니다.

경제적으로 **폴리스웜**은 예측 시장에 기술적 숙련도를 요구하는 변형으로 기능합니다. 수천 개의 마이크로 엔진(*작업자*)이 최신 악성코드 진화를 인간 개입 없이 기계 속도로 조사합니다.

폴리스웜은 ERC20 호환 **Nectar (“NCT”)** 유틸리티 토큰의 판매로부터 조달된 자금으로 **Polyswarm Pte. Ltd.** 가 개발합니다.

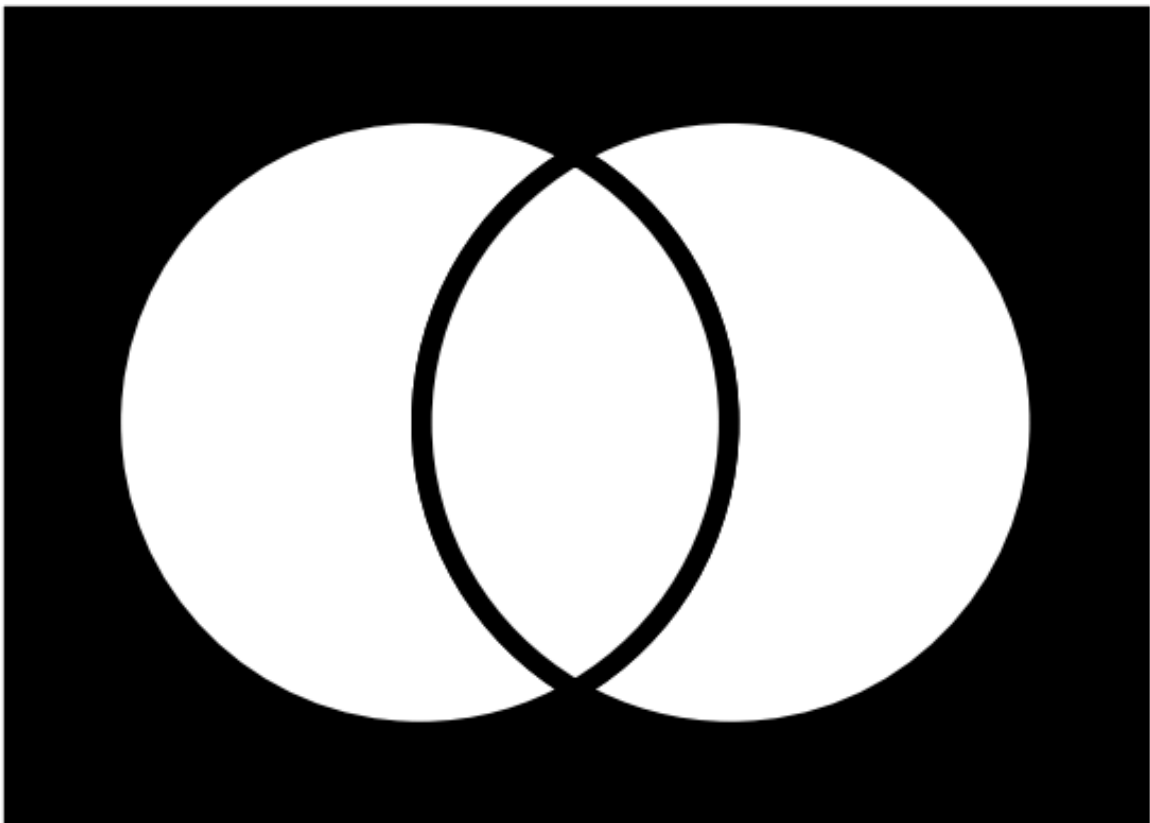
유틸리티 토큰으로서, **폴리스웜**은 수수료를 가치 있는 활동을 하는 참여자들에게 분배함으로써 정직한 시장 참여를 보상하고, Nectar에 대한 단순 투자를 경제적으로 억제합니다.

배경

오늘날 기업들은 진화하는 적대적 사이버 활동에 대응하기 위해 임시적 혼합물(ad-hoc mix)인 안티바이러스 구독, 위협 인텔리전스 피드, 다양한 동적 분석 엔진에 의존합니다. 사용자는 각 솔루션이 제공하는 장단점을 저울질하고 자신의 환경에 가장 덜 나쁜 적합성을 선택해야 합니다.

오늘날의 시장은 폭넓은 위협 커버리지를 제공하는 솔루션을 억제합니다.

오늘날의 솔루션은 시장 경제학의 직접적인 결과로, 위협의 특정 "안전 구역"에 집중합니다.



[Figure A: 검은 사각형은 기업이 직면할 수 있는 모든 위협을 나타내며, 흰색 원은 각각 안티바이러스 제품 #1과 #2를 의미합니다.]

WannaCry를 탐지하지 못하는 안티바이러스 솔루션을 무시하는 것은 쉽고(어쩌면 정당화될 수 있지만), 그렇게 함으로써 오늘날의 시장은 벤더 간 중복 커버리지를 사실상 보상하게 됩니다. 이는 중복 비용을 초래하는 전형적인 공유지의 비극(tragedy of the commons) 상황입니다.

비슷하게, 이 안전 구역 밖의 전문성을 개발하기로 선택한 벤더를 생각해 봅시다. 안전 구역이 대부분의 기업이 직면하는 위협 집합으로 정의된다면, 이 특화된 벤더의 판매는 어려울 것입니다. 자신만이 탐지/차단/완화할 수 있는 악성코드를 고객이 반드시 다루게 될 것이라고 어떻게 설득하겠습니까?

마지막으로, 방어자들은 오늘날의 많은 솔루션을 혼합·매치할 수 없어서, 많은 시나리오에서 조합적 커버리지가 불가능합니다.

대조적으로, **폴리스웜**은 지리적으로 다양한 보안 전문가들이 작성한 수천 개의 *마이크로 엔진* 작업자들에 의해 구동되는 폭넓은 커버리지 생태계를 조성할 것입니다.

폴리스웜은 보안 전문가에게 합법적인 수익원을 제공합니다

지역 경제가 충분한 정직한 일을 지원하지 못할 때, 일부 보안 전문가는 랜섬웨어를 개발하거나 봇을 운영하거나, 기타 악용 행위로 기술을 악용하기도 합니다. 폴리스웜은 정직한 일에 대한 보상을 국경 없이 제공하는 대안을 마련합니다. 전문가들은 인터넷을 더 안전한 공간으로 만들기 위해 경쟁합니다.

폴리스웜은 사용자를 최우선으로 둡니다

폴리스웜 마켓은 경제적 인센티브를 가장 중요한 곳, 즉 정확한 악의 탐지(*위협 인텔리전스*)에 집중시킵니다. 정확도는 우리가 **완화된 합의(Mediated Consensus)**라 부르는 새로운 과정(10쪽에 자세히 설명됨)을 통해 결정됩니다.

간단히 말해, 폴리스웜은 사용자에게 폭넓고, 클라우드소싱된 보안 전문성에 대한 시의적절한 접근을 제공합니다. 의심스러운 파일을 신속히 분류해야 합니까? **Just Swarm It™**.

위협 인텔리전스 시장의 재창조

폴리스웜의 **Nectar (“NCT”)** 토큰은 파일, 네트워크 트래픽, URL(통칭하여 아티팩트)의 악의 여부에 대한 시의적절하고 정확한 주장 수요를 충족하기 위해 새로운 도구를 도입하는 새로운 시장의 기초를 형성합니다. 이러한 새로운 도구는 정확한 결과에 의해 구동되는 피드백 루프를 통해 위협 인텔리전스 분야에서 혁신을 직접적으로 장려하도록 설계되었습니다.

폴리스웜은 **수수료(Fees)**를 활용하여 스팸을 억제하고 정직하고 적극적인 시장 참여를 장려합니다. 수수료는 스팸 남용 가능성이 있는 트랜잭션 유형에 부과되며, 아티팩트를 제출하고 그 악의 여부에 대한 근본적 진실을 결정하는 활발한 생태계 참여자들에게 분배됩니다. 이 참여는 슬라이딩 윈도우 방식으로 측정되며, 오래된 기여는 “ageing-off”되어 지속적인 시장 참여를 유도합니다.

폴리스웜 1.0(그리고 본 문서)은 악성/정상 여부라는 불리언 결정에만 집중합니다. 그러나 폴리스웜 팀은 불리언 악의 탐지 시장을 교란하는 것을 넘어 더 큰 계획을 가지고 있습니다. 폴리스웜 1.0 개발 중에, 팀은 악성 코드 패밀리와 같은 아티팩트 메타데이터 생산을 장려하는 방법을 탐구할 것입니다. 또한 스마트 계약 시장 설계, **완화된 합의(Mediated Consensus)**, 정보 보안 중심과 같은 폴리스웜의 핵심 개념이 취약점 버그 바운티 등 관련 시장을 어떻게 교란할 수 있을지도 모색할 것입니다.

폴리스웜의 도구들을 소개하기 전에, 이를 활용할 참가자 계층을 먼저 소개합니다.

참가자



[Figure C: 폴리스웜의 바운티 및 오퍼 라이프사이클 개요.]

최종 사용자(End Users)

의심스러운 아티팩트를 가진 기업 및 개인 사용자. 최종 사용자는 폴리스웜 마켓에서 바운티와 오퍼를 통해 참여하며, 시의적절하고 정확한 악의 분류를 얻게 됩니다.

보안 전문가(Experts)

지리적으로 다양한 악성코드 전문가 및 리버스 엔지니어. 이들은 최신 의심 아티팩트를 분석하고 폴리스웜과 연결된 탐지 엔진(“workers”)을 유지하여 악의 여부를 판단합니다. 전문가들은 아티팩트의 악의 여부에 대한 분석 결과를 반영하는 공개 진술인 *검사*를 제출합니다. 정확한 검사를 제출한 전문가들은 그 노력에 대해 NCT로 보상받습니다.

핵심 참여자는 사실 여기까지입니다. 단순함은 좋지만, 이것이 폴리스웜의 전부는 아닙니다. 기술적으로는 폴리스웜이 이 두 가지 참여자 계층만으로도 작동할 수 있습니다. 그러나 현실적으로는 대부분의 **최종 사용자**가 폴리스웜 마켓과의 세부적인 상호작용을 직접 처리하는 것을 원하지 않을 것입니다.

여기서 **엠버서더** 라는 또 다른 참가자와 이들의 하위 계층을 소개해야 합니다.

엠버서더

최종 사용자가 폴리스웜 마켓의 혜택을 쉽게 누릴 수 있도록 돕는 기업입니다. 엠버서더는 고객(최종 사용자)으로부터 전통적 화폐(예: 구독료)와 의심 아티팩트를 수집하고, 이를 대신하여 **바운티**와 **오퍼**를 마켓에 제출합니다. 엠버서더의 책임은 다양한 전문가들의 검사를 간단한 **악성** 또는 **정상** 평결로 정제하여 고객에게 전달하는 것입니다.

이 정제의 단순한, 어쩌면 순진한 접근은 전문가들의 주장을 단순 평균하는 것일 수 있습니다. 그러나 이러한 알고리즘이 베이지안 분석은 물론 전문가의 인간적 개입과 경쟁할 수 있을 가능성은 낮습니다. 우리는 기존의 안티바이러스 및 위협 인텔리전스 기업들이 초기 엠버서더로서 폴리스웜 마켓에 참여하여, 내부 전문성을 폴리스웜 기반 의심 아티팩트 분류로 보강할 것으로 예상합니다.

사용자 관점에서, 폴리스웜 지원 보호로 업그레이드하는 것은 간단합니다: 평판 좋은 엠버서더를 선택하고 구독료를 지불하면 됩니다.

엠버서더의 평판은 실제 진실에 비추어 본 과거 평결 성과에 기반합니다. 엠버서더는 평판을 쌓고 새로운 고객을 유치하려는 본능적 욕구와 수수료 할인 혜택을 얻으려는 동기 때문에 자신의 평결을 공개하도록 장려됩니다(이 과정은 후술됨). 이러한 공개 평결은 현실 세계의 성능을 비합성(non-synthetic) 아티팩트에 대해 평가하는 엠버서더 **점수표(scorecard)** 생성을 가능하게 합니다. 오늘날의 시장에서는 전혀 볼 수 없는 데이터입니다.

아비터(Arbiter)

악의 여부에 대한 근본적 진실을 결정하는 최상위 엠버서더입니다. 수수료 기준으로 상위 일정 비율의 엠버서더가 **아비터**로 간주됩니다.

개발 단계에서, 폴리스웜은 폴리스웜 팀과 긴밀히 협력하고, 플랫폼 버그 식별·해결을 돕고, 생태계 관심을 구축하는 데 기여이 참여하는 기존 평판 좋은 위협 인텔리전스 벤더들에게 Arbitership을 부여할 것입니다.

폴리스웜 1.0이 출시 준비가 되면, 지정된 아비터는 아비터 지위를 유지하기 위해 최상위 엠버서더 활동량을 유지해야 합니다.

예측 시장, 아비터 & 완화된 합의

폴리스웜 생태계에서 보안 전문가들은 의심 아티팩트를 신속하고 정확하게 조사하기 위해 경쟁하는 마이크로 엔진을 개발합니다. 이 조사는 기계 속도로 수행되며, 아티팩트의 악의 여부에 대한 진실이 확립되기 전입니다.

이 설계는 예측 시장과 일부 유사성을 갖지만, 두 가지 중요한 점에서 다릅니다:

1. 아티팩트를 정확히 분류하기 위해 미래 데이터가 필요하지 않음

아티팩트가 악성인지 여부에 대한 “정답”은 작업자가 사용할 수 있게 되는 시점에 언제든지 확실히 결정될 수 있습니다. 폴리스웜은 아무 것도 우연에 맡기지 않는 기술 기반 설계입니다.

2. 근본적 진실 결정에는 항상 전문성이 필요함

이는 사건이 발생하는 대로 숙련되지 않은 참여자들이 관찰·기록하는 “*보편적 관측 가능성*”에 의존하는 예측 시장(예: **Augur**)과는 대조적입니다.

항목 #1은 폴리스웜의 도박 억제 장치입니다.

항목 #2는 기술적 도전을 제시합니다: 근본적 진실을 지속적으로 생산하도록 권위를 장려하는 최선의 방법은 무엇인가?

폴리스웜의 답은 아비터 계층과 우리가 **완화된 합의**라 부르는 과정입니다.

완화된 합의는 우리가 다른 시장 설계 프로젝트에서도 채택되기를 바라는 일반적 설계 패러다임입니다. 간단히 말해, 완화된 합의는 중요한 과제를 일부 참여자 집합에 위임하는 시장 설계입니다. 이들은:

1. 과제를 완료할 자격이 있으며(전문성을 보유),
2. 시장의 전반적 건전성과 이해가 일치합니다(공유지의 비극을 피함).

우리는 아비터를 이 두 조건을 충족하도록 설계했습니다. 정의상, 아비터 계층은 특정 시점에서 폴리스웜 생태계에서 가장 활발한 앰버서더로 구성됩니다.

앰버서더로서, 아비터는 고객과 계약해 보안 전문가들의 검사를 평결로 정제합니다. 고객은 이들이 자동화된, 필요 시 인간 전문성을 발휘할 수 있는 역량을 가지고 있다고 신뢰합니다. 이러한 기업들은 이미 정확도에 대한 공개 기록을 유지할 기득권을 가지고 있습니다(항목 #1).

가장 활발한 앰버서더인 아비터는 정직한 폴리스웜 생태계에서는 가장 큰 이익을, 부정직한 생태계에서는 가장 큰 손실을 입습니다. 따라서 이들의 대규모 이해관계는 시장의 건전성과 일치합니다(항목 #2).

우리는 아비터-보안 전문가 간 담합과 같은 아비터 남용을 방지하기 위해 수수료를 보완적 방어 장치로 설계했습니다.

최종 결과값(ground truth) 결정

아비터 투표 과정의 대부분의 기술적 세부사항은 현재 의도적으로 정의되지 않은 상태로 남겨두고 있습니다. 그 이유는 간단합니다. 아비터 결정 과정의 구체적인 내용은 사실상 폴리스웜의 모든 다른 과정의 구체적 사항에 달려 있으며, 우리는 다른 과정에서의 변화를 예상하기 때문입니다.

그렇긴 하지만, 다음과 같은 상위 수준 설계 선택이 이 과정에 가치를 제공할 것이라 기대합니다:

1. 아비터는 **다수결 투표**를 통해 최종 결과값에 합의합니다.
2. 이러한 투표는 **이더리움 체인에 대량으로 마이닝**됩니다(주기마다 다수의 투표), 폴리스웜 생태계의 시간과 비용(Ethereum 가스)을 절약합니다.
3. 참여를 장려하기 위해, **아비터는 아티팩트의 최종 결과값에 대한 투표에 수수료(Fees)로 보상을 받습니다.**
4. **아비터는 특정 아티팩트에 대해 투표를 기권**할 수 있습니다. 예를 들어, 특정 아티팩트의 악의 여부를 판단할 자격이 없다고 느낄 경우 기권할 수 있습니다.
5. 필요한 경우, **아비터 투표 권한은 자동으로 추가 앰버서더에게 위임**되어 모든 최종 결과값 결정에서 정족수를 확보합니다.
6. 필요한 경우, **참가자들이 아비터 결정에 도전**하기를 기대합니다. 예컨대 아비터와 같은 권위자가 아티팩트를 잘못 분류했을 때, 블로그 글이나 기술 문서를 통해 해당 아티팩트의 악성 또는 정상 성격을 설명하는 방식입니다. 이는 외부 PR 기반 피드백 루프입니다.

폴리스웜 팀은 개발 과정에서 아비터 투표 및 인센티브 구조에 관한 세부사항을 반복적으로 발전시켜 나갈 것입니다. 우리는 초기 아비터 피드백이 이 설계에 핵심적일 것으로 예상합니다.

연구 주제는 다음을 포함하되, 이에 국한되지 않습니다:

- 최소 아비터 정족수 비율.
- 정족수를 충족할 수 없을 때 아비터 이양 절차.
- 적절한 수수료 보상 구조.
- 시의적절한 최종 결과값 결정을 위한 인센티브(예: 최초 X명의 아비터만 보상).
- 불참에 대한 페널티(예: 아비터는 특정 기간 동안 X% 이상의 아티팩트에 투표해야 하며, 그렇지 않으면 아비터 지위 박탈).
- (필요 시) 왜곡된 인센티브에 대한 추가 억제책.

도구(Instruments)

폴리스웜은 최종 사용자와 앰버서더에게 위협 인텔리전스 시장의 효율성을 높이는 두 가지 핵심 도구를 제공합니다:

폴리스웜 오퍼

신뢰할 수 있는 보안 전문가에게 악의 예측을 직접 요청하는 방식입니다. 폴리스웜은 수천 명의 연구자에게 마찰 없는 접근을 제공하여, 전통적 정보 공유 계약을 비전통적 참여자들과 체결할 수 있게 합니다.

이 상호작용은 **Raiden 스타일 오퍼 채널**(뒤에 자세히 설명됨) 내부에서 발생합니다. 채널이 설정되면, 오퍼는 아티팩트 조사를 밀리초 단위의 지연으로 제공합니다.

폴리스웜 바운티

야생 서부식 “현상수배” 포스터와 유사하며 아티팩트 내용이 함께 포함됩니다(예: *현상수배: 이 아티팩트 – 악성인가 정상인가? 보상: 1000 NCT*). 보안 전문가들은 현상금을 성공적으로 획득하여 자신의 명성을 쌓습니다. 오늘날 시장에는 이에 직접적으로 대응되는 유사 사례가 없습니다.

오퍼는 오늘날의 온디맨드 스캐닝 시장에 가장 가까운 유사체이며, 밀리초 단위의 지연으로 동작합니다.

앰버서더는 NDA 하에 선택된 보안 전문가에게 오퍼s와 아티팩트를 직접 전달할 수 있습니다. 각 전문가는 주어진 아티팩트에 대해 정확한 주장을 할 자신이 있는지에 따라 오퍼를 수락 여부를 결정합니다. 신뢰도에 부정적 영향을 줄 수 있으면 거절할 수도 있습니다. 오퍼를 수락하면, 전문가는 시의적절한 악의 주장을 제공해야 합니다. 모든 도구의 토큰 수집과 보상은 분산형 스마트 계약에 의해 전적으로 관리·실행됩니다.

오퍼 발행에는 아티팩트를 분석하기에 가장 적합한 전문가를 파악하는 일정 수준의 친숙함이 필요합니다. 이를 쉽게 하기 위해, 전문가들은 **폴리스웜 워커 레지스트리**(이더리움 dApp 레지스트리의 폴리스웜 버전)에 자신의 전문성을 등록하여 광고하며, 유사한 바운티에 성공적으로 참여하여 공개 명성을 쌓습니다.

바운티는 오퍼보다 저렴하며 특정 전문가에 대한 사전 친숙함이 필요하지 않지만, 모든 사용자에게 적합하지는 않습니다.

1. **바운티는 반드시 이더리움 블록에 마이닝되어야** 하며, 이는 약 15초마다 발생합니다. 이 과정이 이 구조에서 가장 지배적인 시간 비용입니다.
2. **바운티를 게시할 때, 아티팩트는 반드시 공개되어야¹³ 합니다.** 결국, 야생 서부의 “현상수배” 포스터가 모든 알려진 정보와 함께 공개된 장소에 게시되지 않았다면 아무런 쓸모가 없었을 것입니다.

마찬가지로, 바운티는 아티팩트를 격리하거나 무죄로 입증하는 데 기여한 이들에게 보상을 약속하는 공개적이고 스마트(계약 기반)한 약속을 나타냅니다. 또한 바운티는 최종 결과값을 확립하는 피드백 루프의 핵심 구성 요소입니다.

정확성에 대한 보상

오늘날의 시장과 달리, 폴리스웜 마켓은 위협 인텔리전스의 정확성에만 기반한 정밀한 보상을 제공합니다. 이는 전문가들이 탐지 정확도(거짓 양성 및 거짓 음성을 최소화)에만 집중하도록 장려하며, 앰버서더가 고객을 대신해 최대한의 가치를 끌어낼 수 있도록 합니다. 폴리스웜은 정확성을 전문가들의 검사와 아비터가 정의한 최종 결과값 간의 일치 여부로 정의합니다.

이 정확성 피드백 루프는 **폴리스웜 바운티**에 의해 구동됩니다. 각 바운티는 정확한 주장을 제출한 전문가에게 보상을 지급하고, 부정확한 주장을 제출한 전문가를 벌하며, 앰버서더와 전문가 간 담합 인센티브의 도입을 피합니다. **폴리스웜 오픈**은 전통적인 1:1 비즈니스 관계를 구축하는 편리한 수단을 제공하지만, 이 정확성 방식에는 포함되지 않습니다.

폴리스웜 마켓에서 최종 결과값이 생산되고 소비되는 방식:

1. 앰버서더가 아티팩트에 대해 바운티를 걸고, 이를 위해 수수료를 제출합니다.
2. 다양한 전문가들이 바운티의 주장 마감 기한 전에 이 아티팩트에 대한 주장을 제출합니다. 각 주장은 전문가가 선택한 NCT 금액(**입찰가**)과 함께 제출되며, 이는 전문가의 자신감을 반영합니다. 수수료는 이 **입찰가**의 일정 비율로 부과됩니다. 이러한 검사는 마감 기한까지 비공개로 유지됩니다.
3. 앰버서더는 전문가들의 검사를 고려하여 평결을 산출하고 이를 고객에게 전달합니다. 앰버서더는 자신의 평판을 쌓고 수수료 할인을 받기 위해 평결을 공개하도록 장려됩니다(자세한 내용은 후술).
4. 이후 시점(예: 바운티 게시 후 7일)에, 아비터는 해당 아티팩트가 실제로 악성인지 정상인지 투표할 기회를 가집니다. 이 나중에 결정되는 최종 결과값은 **신속한 평결 반환을 막지 않습니다**. 즉, 앰버서더는 고객에게 결과를 반환하기 전에 최종 결과값 결정을 기다릴 필요가 없으며, 기다려서도 안 됩니다.
5. 아비터 정족수가 아티팩트의 최종 결과값 상태를 결정합니다. 이 투표 결과를 최종 결과값으로 변환하는 구체적 과정은 아직 결정되지 않았습니다. 가능한 방식으로는 단순 다수결이나 시장 참여 정도에 기반한 비례 다수결이 있습니다. 이 구체 사항은 프로토타입 개발 과정에서 결정될 것입니다.
6. 최종 결과값이 확립되면, 바운티 스마트 계약은 정확한 검사를 제출한 전문가에게 NCT를 지급합니다. 지급액은 전체 정확한 입찰 풀에 대한 전문가의 입찰가 비율에 비례합니다.

표면적으로는 고전적인 예측 시장이 여기에 적합해 보일 수 있습니다. 전문가들이 검사를 제출하고, 이후 이 검사가 최종 결과값과 비교되어 정확성에 따라 보상과 벌칙이 주어지는 구조입니다. 문제는 고전적 예측 시장은 모든 참가자가 검증할 수 있는 최종 결과값 원천을 암묵적으로 전제한다는 점입니다. 선거 결과나 금값이 특정 시점에 특정 가격을 초과했는지 여부는 예측 기간이 끝난 후 누구나 검증할 수 있습니다.

그러나 의심 아티팩트의 악의 여부를 결정하는 데에는 폴리스웜 참가자 전체가 공유하지 않는 전문성이 필요합니다. 이 문제는 의학적 진단에 적용된 예측 시장과 유사합니다. 의사들이 다양한 수준의 전문성을 활용하는 경우와 비슷합니다.

폴리스웜은 최종 결과값 결정을 아비터에 위임합니다. 오늘날 시장에서 아비터의 역할은 사실상 전통적 안티 바이러스 기업들이 맡고 있습니다. 이들은 VirusTotal 같은 서비스에서 “투표” 하고, “최종 결과값”에 대해 공개적으로 책임을 집니다. 폴리스웜 마켓에서 아비터 집합은 전적으로 시장 참여에 의해 결정되며, 새로운 플레이어가 기존 질서를 뒤흔들 기회를 제공합니다.

결론적으로, 우리는 이 과정이 아비터가 시장 전체의 이익을 위해 최종 결과값을 결정할 때 충분한 자원을 투입하도록 올바르게 인센티브를 부여한다고 믿습니다.

이러한 최종 결과값 “검증자” 집단 개념은 다른 분야에도 적용 가능합니다. 우리는 다른 이들이 이 메커니즘을 전문 지식이 필요한 다른 토큰 플랫폼에 도입하는 가능성을 탐구할 것으로 예상합니다.

수수료(Fees)

폴리스웜 마켓에서 다양한 트랜잭션에 대해 수수료가 부과되며, 이는 두 가지 목표를 달성하도록 설계되었습니다:

1. 최소한의 Ethereum 가스 비용으로 효율성 촉진

폴리스웜 트랜잭션에 고정 효율 수수료가 적용되어, 불필요한 트랜잭션(스팸 트랜잭션 포함)을 억제하고 시장 전반의 가스 비용을 줄입니다. 폴리스웜이 이러한 수수료를 Ethereum 가스 비용과 독립적으로 조정해야 하는 필요성은 NCT 생성이 폴리스웜 마켓의 존재에 필수적인 여러 이유 중 하나입니다.

2. 정직한 참여 비례 보상

수수료는 폴리스웜 생태계를 적극적으로 활용하는 참가자, 즉 아티팩트를 제출하는 앰버서더(바운티 발행)와 아티팩트의 악의 여부에 대해 최종 결과값을 확립하는 아비터(최종 결과값 합의)에 분배됩니다.

네트워크 개발 중에 폴리스웜 팀은 위 수수료 구조를 “레드팀(red-team)” 방식으로 검증하고, 건강한 시장을 가장 잘 장려할 수 있도록 필요 시 반복적으로 개선할 것입니다.

앰버서더가 지불하는 바운티 게시 수수료

앰버서더가 폴리스웜 마켓에 바운티를 등록할 때, 스마트 계약에 보관된 자금에서 다음 수수료가 부과됩니다:

1. **고정 게시 수수료.** 이 수수료는 앰버서더가 여러 아티팩트를 단일 바운티로 묶도록 장려하여 네트워크 부하와 전체 가스 비용을 줄입니다.
2. **바운티 금액 비례 수수료.** 초기 바운티 금액이 클수록 더 많은 전문가 응답을 유도할 가능성이 높습니다. 이 비례 수수료는 전문가 참여와 네트워크 부하에 맞춰 수수료를 확장합니다.

전문가가 지불하는 바운티 주장 수수료

전문가가 바운티에 대해 주장을 제출할 때, 스마트 계약에 보관된 자금에서 다음 수수료가 부과됩니다:

1. **고정 주장 수수료.** 이 수수료는 네트워크를 느리게 할 수 있는 반복 검사를 억제합니다.

2. 입찰가 금액 비례 수수료.

오퍼 채널 정산: 앰버서더 수수료

오퍼는 앰버서더와 전문가 간 직접 설정된 Raiden 스타일 오퍼 채널에서 발생합니다. 앰버서더와/또는 전문가가 오퍼 채널을 블록체인으로 정산하기로 결정할 때, 채널 스마트 계약은 다음 수수료를 부과합니다:

1. **채널을 통해 전송된 순 NCT의 일정 비율.** 이 수수료는 채널 개설 시 앰버서더가 제공한 토큰에 부과됩니다. 채널이 종료될 때, 사용되지 않은 채널 토큰에 비례해 이 수수료는 앰버서더에게 환불됩니다.

프로토콜 세부사항

여기서는 폴리스웜 바운티, 오퍼, 검사, 평결을 상세히 설명합니다. 바운티와 오퍼는 통칭하여 **폴리스웜 리스팅**이라 부릅니다. 폴리스웜 성명은 바운티, 오퍼, 주장 또는 평결을 포함합니다.

바운티 라이프사이클

앰버서더가 마켓에 바운티를 걸고자 할 때, 폴리스웜 바운티 스마트 계약 호출을 통해 성명을 등록합니다.

바운티 성명은 다음 항목을 포함합니다:

1. **Listing GUID:** 리스팅에 대한 전역 고유 식별자.
2. **앰버서더의 신원.** 이는 성명에 대한 서명 형태로, 앰버서더 주소를 가진 누구나 검증할 수 있습니다(공개키는 주소로부터 파생).
3. **바운티 게시 수수료.** 이는 고정 금액 + 바운티 금액의 일정 비율입니다(앞의 “수수료” 섹션에서 설명됨). 앰버서더가 나중에 평결을 공개적으로 제출하면 할인이 적용됩니다.
4. **바운티 금액.** 이 금액은 바운티 게시 수수료와 함께 스마트 계약에 보관되며, 정확한 검사를 제출한 전문가에게 지급됩니다(응답이 없을 경우 환불). 이 금액은 Ethereum 또는 Bitcoin의 트랜잭션 수수료와 유사하며, 바운티에 주의를 끌기 위해 유용합니다.
5. **아티팩트의 암호학적 해시.** 구성 가능하며 현재는 SHA256. 아티팩트를 고유하게 식별합니다.
6. **아티팩트의 URI.** 저장 비용 때문에 아티팩트는 온체인에 저장되지 않습니다. 우리는 아티팩트 저장 및 전달을 외부에 위임하는 2차 시장이 등장할 것으로 예상하며, 일부 앰버서더는 이후 경쟁 분석을 위해 모든 아티팩트 사본을 보관할 수 있습니다.

7. **주장 마감 기한.** 주장 제출 마감 기한입니다. 앰버서더는 특정 아티팩트에 대한 요구에 따라 분석 기간을 단축하거나 연장할 수 있습니다. 심층 분석이 필요한 아티팩트는 더 긴 시간이 필요할 수 있으며, 더 큰 바운티 금액이 관심을 끌 가능성이 있습니다. 반대로, 다른 아티팩트는 빠른 처리 시간이 요구될 수 있습니다.

바운티가 등록되면, 전문가들은 해당 아티팩트가 자신의 전문 분야에 적합한지, 예상 보상이 주목할 만한 가치가 있는지를 판단합니다. 이 예상 보상은 아티팩트의 악의 여부에 대한 자신감 구간의 함수입니다.

참여하기로 한 전문가들은 자신감(및 위험 감수)을 반영하는 입찰가를 주장과 함께 제출합니다. 바운티 금액과 모든 부정확한 입찰의 합은, 정확한 입찰을 제출한 전문가들에게 각자의 입찰가 비율에 따라 분배됩니다.

다음 예시를 고려해 봅시다(단순화를 위해 수수료는 생략):

1. 앰버서더가 2 NCT의 바운티를 겁니다. 이 2 NCT는 바운티 스마트 계약에 예치됩니다. 현재까지 이 2 NCT가 정확한 전문가들에게 잠재적으로 분배될 전체 “*pot*”을 구성합니다.
2. 전문가 A와 B는 아티팩트를 분석하고 해당 아티팩트가 **정상**이라고 주장합니다. 각각 5 NCT와 3 NCT를 입찰가로 걸었습니다.
3. 전문가 C와 D는 아티팩트를 분석하고 해당 아티팩트가 **악성**이라고 주장합니다. 각각 1 NCT와 4 NCT를 입찰가로 걸었습니다.
4. 이후 아비터가 최종 결과값을 확립한 결과, 아티팩트가 실제로 **악성**임이 밝혀집니다. 따라서 전문가 A와 B는 **부정확한** 주장을, 전문가 C와 D는 **정확한** 주장을 제출한 것입니다.
5. 바운티 금액(2 NCT)과 전문가 A와 B가 걸 입찰가(5+3 NCT)가 합쳐져 전문가 C와 D에게 분배될 “*팟*”을 형성합니다. 총합은 $2 + 5 + 3 = 10$ NCT입니다.
6. 전문가 C는 정확한 주장을 제출했으며, 그의 입찰가는 전체 정확한 입찰가 금액의 $1/5$ 을 차지합니다. 따라서 입찰가 1 NCT가 반환되고, *pot*의 자신의 몫을 더해 받습니다: $1 + 1/5 * 10 = 3$ NCT.
7. 전문가 D는 정확한 주장을 제출했으며, 그의 입찰가는 전체 정확한 입찰가 금액의 $4/5$ 를 차지합니다. 따라서 입찰가 4 NCT가 반환되고, *pot*의 자신의 몫을 더해 받습니다: $4 + 4/5 * 10 = 12$ NCT.

바운티 검사는 다음을 포함합니다:

1. **Listing GUID + 암호학적 해시:** 해당 바운티 리스팅에 대한 고유 참조.
2. **전문가의 신원:** 성명에 대한 서명 형태.
3. **주장 수수료:** 고정 금액 + 입찰가 금액의 일정 비율(“수수료” 섹션 참조).
4. **입찰가 금액.**
5. **주장:** 아티팩트의 악의 여부에 대한 불리언 값 “**악성**” 또는 “**정상**”. 검사는 바운티 주장 마감 기한까지 비공개로 유지됩니다. 이를 위해 블라인드 커밋 + 공개 단계 방식을 사용할 것으로 예상합니다.

6. **(선택적) 메타데이터:** 주장 생성 중 도출된 정보로, 앰버서더가 평결 산출 시 활용할 수 있는 부가 가치 데이터(예: 악성코드 패밀리). 전문가는 스스로를 차별화하고 향후 기회를 끌어들이기 위해 이 정보를 제공할 수 있습니다.

검사가 들어오면, 앰버서더는 이들을 평가하고 자체적인 실사를 포함하여 “악성” 또는 “정상” 평결을 산출합니다. 앰버서더는 아티팩트의 악의 여부에 대한 최종 응답으로 이 평결을 고객에게 전달합니다. 앰버서더는 평결 마감 기한 전에 이 평결을 공개적으로 게시할 수도 있으며, 이는 수수료 할인을 통해 장려됩니다.

공개 평결은 다음을 포함합니다:

1. **Listing GUID:** 해당 리스팅에 대한 참조.
2. **앰버서더의 NCT 신원:** 성명에 대한 서명 형태.
3. **평결:** 아티팩트의 악의 여부에 대한 불리언 값 “악성” 또는 “정상”.

이후 아비터가 아티팩트에 대한 최종 결과값에 정족수를 달성합니다. 이 최종 결과값은 각 전문가들의 검사와 비교되며, 정확한 검사에 대해 NCT가 보상으로 지급됩니다.

오퍼 라이프사이클

앰버서더가 특정 전문가에게 오퍼를 발행하려면, 해당 전문가와 Raiden 스타일의 채널을 엽니다.

이는 전문가와 함께 **오퍼 채널** 스마트 계약을 인스턴스화하여 수행되며, 여기에는 다음이 포함됩니다:

1. **앰버서더와 전문가의 신원.**
2. **채널 잔액:** 채널 종료 시 앰버서더가 전문가에게 정산하는 데 감수할 수 있는 최대 NCT 금액(수수료 포함).

오퍼 채널이 설정되면, 앰버서더는 전문가에게 0개 이상의 오퍼s를 발행합니다. 각 오퍼에는 다음이 포함됩니다:

1. **Listing GUID:** 리스팅에 대한 전역 고유 식별자.
2. **오퍼 금액.** 이 금액은 오퍼 채널 스마트 계약에 남아 있는 잔액(수수료 제외)을 초과할 수 없습니다.
3. **아티팩트의 암호학적 해시.**
4. **아티팩트의 URI.** 아티팩트는 오퍼ee의 신원에 맞게 암호화되거나 접근 보호 처리되어 기밀성을 보장할 수 있습니다.
5. **참가 마감 기한:** 응답 제출 기한.
6. **주장 마감 기한:** 해당 오퍼에 대한 주장 제출 기한.

오퍼를 받은 전문가(Offeree)는 이 오퍼에 응할지 무시할지 선택할 수 있습니다. 각 오퍼를 받은 전문가는 주어진 시간 내 오퍼 받은 금액으로 이 아티팩트를 평가할 가치가 있는지 판단합니다.

오퍼를 받은 전문가의 향후 비즈니스는 정확한 결과를 산출하는 능력에 달려 있습니다. 만약 오퍼를 받은 전문가가 주어진 시간 내 정확한 결과를 산출할 자신이 없다면(예: 아티팩트가 오퍼를 받은 전문가가 분석하기 어려운 파일 형식일 경우), 오퍼를 거절할 수 있습니다.

오퍼를 받은 전문가가 오퍼를 거절하기로 결정하면, “거절(decline)” 참가 성명을 발행하거나 참가 마감 기한이 만료되도록 둘 수 있습니다. 그러나 앰버서더는 기다리지 않고 즉시 다음 단계를 결정할 수 있는 전문가를 선호하기 때문에, 오퍼를 받은 전문가가 적극적으로 거절하는 편이 더 유리할 수 있습니다.

오퍼를 받은 전문가가 오퍼를 수락하기로 결정하면, 참가 마감 기한 전에 “accept” 참가 성명을 발행합니다.

참가 성명은 다음을 포함합니다:

1. **Listing GUID + 해시:** 해당 리스팅에 대한 참조.
2. **참가 약속:** 오퍼를 받은 전문가가 이 오퍼에 응해 주장을 제출할 것인지 여부를 나타내는 불리언 값 “accept” 또는 “decline”.

오퍼를 받은 전문가가 오퍼를 수락하면, 주장 마감 기한까지 해당 오퍼에 대한 주장을 제출해야 합니다.

이러한 검사는 다음을 포함합니다:

1. **Listing GUID + 해시:** 해당 리스팅에 대한 고유 참조.
2. **주장:** 아티팩트의 악의 여부에 대한 불리언 값 “악성” 또는 “정상”.
3. **(선택적) 메타데이터:** 주장 생성 중 도출된 정보로, 앰버서더가 평결 산출 시 활용할 수 있는 부가 가치 데이터(예: 악성코드 패밀리). 전문가는 자신을 차별화하고 향후 기회를 끌어들이기 위해 이 정보를 제공할 수 있습니다.

전문가가 주장을 앰버서더에게 제출하면, 앰버서더는 Raiden 스타일 메시지에 서명하여 오퍼 금액 지급을 약속합니다. 따라서 전문가가 감수하는 위험은 단일 분석 결과물 이상이 되지 않습니다. 이러한 금액들의 합은 오퍼 채널이 종료될 때 블록체인에 정산됩니다.

바운티와 달리, 오퍼는 온체인 최종 결과값 피드백 메커니즘을 포함하지 않습니다. 대신 주장 마감 기한 전에 주장을 제출하지 못하거나, (후속 오프체인 분석 결과) 부정확한 주장을 제출한 오퍼를 받은 전문가는 향후 참여 기회를 얻지 못할 수 있습니다. 따라서 평판 유지가 오프체인 피드백 루프와 유사해지며, 시장 압력을 통해 오퍼를 받은 전문가의 정직성을 유지하게 됩니다.

오퍼 채널이 종료되면, 순 NCT 전송액에 대해 수수료가 부과됩니다. 모든 수수료와 마찬가지로, 이 수수료는 활발한 시장 참여자에게 분배됩니다. 수수료는 마스터 오퍼 채널 스마트 계약에 의해 강제되며, 규격에 맞지 않는 오퍼 채널은 생성이 거부됩니다.

평판(Reputation)

다른 토큰 플랫폼(예: Augur)과 달리, 폴리스웜은 평판의 개념을 형식화하여 시장 거래에 내장하려 하지 않습니다.

그 이유는 간단합니다. 어떤 데이터 포인트가 다양한 참가자들에게 가치가 있으며, 그것이 어떻게 가중되는지를 미리 예측하는 것은 매우 어렵기 때문입니다. 앰버서더 A에게 최적의 조건이 앰버서더 B에게도 최적이라는 가정을 강요하는 것은 무의미합니다. 대신 폴리스웜 메커니즘은 평판 함수에 유용한 입력으로 작용할 수 있는 데이터 유형의 공개를 단순히 의무화하거나 장려합니다.

평판 알고리즘은 주장을 평결로 정제하는 알고리즘과 마찬가지로 영업 비밀로 간주될 가능성이 높습니다. 앰버서더는 아티팩트 작업량에 최적의 전문가와 협력함으로써 차별화할 것입니다. 전문가들은 최종 결과값과 비교했을 때 정확한 검사의 우수한 기록을 유지함으로써 자신을 차별화할 것입니다. 또한 선택적으로, 특정 아티팩트가 속한다고 판단하는 악성코드 패밀리와 같은 메타데이터를 제공함으로써 차별화할 수도 있습니다.

개발될 프로토타입 앰버서더 구현체는 다양한 데이터 포인트를 단순한 평판 “점수”와 이해하기 쉬운 색상 체계로 정제할 것입니다. 이 참조 정제는 많은 이들에게 도움이 되겠지만, 참가자들이 필요에 따라 교체하거나 수정할 수 있습니다. 전문가들도 앰버서더를 평가하기 위한 평판 시스템을 구현하고자 할 수 있지만, 이러한 시스템의 비즈니스 로직은 훨씬 더 복잡하고 참가자별로 더 큰 차이가 있을 것으로 예상됩니다.

참조 폴리스웜 데몬은 오래된 데이터를 “슬라이딩 윈도우” 방식으로 “감쇠(decay)”하여 참가자의 평판을 유지합니다. 우리는 새로운 시장 참가자가 배제되지 않도록 하기 위해 슬라이딩 윈도우 접근이 필요하다고 믿습니다.

우리는 참조 앰버서더 구현에서 다음 데이터 포인트를 사용할 것으로 예상합니다:

1. **주장 정확도** (최종 결과값 및/또는 오프체인 분석과의 비교).
2. **바운티 및 오퍼 모두에 대한 빈도 및 평균 응답 시간.** 오퍼의 경우, 앰버서더는 오퍼 채널 내에서만 관찰 가능한 집계 데이터를 공개하기로 선택할 수 있습니다. 앰버서더는 빠르고 일관된 응답 시간을 보이는 전문가를 선호할 수 있습니다.
3. **오퍼 하에 전달된 아티팩트의 기밀 유지 능력.** 이는 온마켓·오프마켓 분석이 혼합된 형태일 가능성이 높습니다.

앰버서더는 경쟁사의 과거 평결을 검토하고 오류를 발견하려 할 수 있습니다(예: 앰버서더 A가 표본을 정상으로 분류했으나 실제로는 악성이었을 때). 전문가들은 일반적으로 이러한 실사가 신뢰할 수 없거나, 특정 상황에서 빈번히 잘못되는 앰버서더와의 협력을 피하려 할 수 있습니다(예: 앰버서더 A가 Microsoft Word 문서를 자주 잘못 분류하여 특정 전문가들이 앰버서더 A를 대신해 Word 문서를 분석하지 않는 경우). 다시 말해, 전문가들은 앰버서더의 평결 정확도에 관심을 가질 수 있습니다.

소비자들은 Consumer Reports 또는 AV Comparatives 스타일의 웹사이트와 출판물을 통해 각 앰버서더의 기록에 대한 집계 정보를 참고할 가능성이 높습니다. 이러한 보고서는 알려진 악의 여부를 가진 샘플 입력을 활용하고, 앰버서더의 평결이 항상 고객에게 전달한 내용과 일치하는지를 검증할 수 있습니다.

워커 레지스트리(Worker Registry)

폴리스웜 생태계의 전문가들은 많은 경우, 자신의 전문성을 자동화된 Workers에 캡슐화하기로 선택할 것입니다.

Workers는 특정 파일 형식이나 네트워크 트래픽에 대한 전문성을 가지고 바운티와 오퍼에 자동으로 응답하는 시스템입니다. 폴리스웜 마켓플레이스는 전문가들의 서비스를 쉽게 탐색할 수 있도록 분산형 워커 레지스트리를 제공합니다.

우리는 워커를 공개적으로 등록하기 위한 공통 인터페이스와 기술 언어를 개발할 것입니다. 이 구성 요소들은 초기 이더리움 dApp 레지스트리 스마트 계약을 모델로 한 폴리스웜 레지스트리와 상호작용합니다. 폴리스웜의 워커 레지스트리는 특정 기술 역량을 광고하는 설명을 포함할 것입니다(예: “나는 Mac OS Mach-O 바이너리에 강하다” 혹은 “Microsoft Word 문서를 처리한다”).

아티팩트 기밀성(Artifact Confidentiality)

아티팩트의 기밀 공개는 오퍼 도구를 통해 폴리스웜 마켓플레이스에서 일급 기능으로 지원됩니다. 그럼에도 불구하고 추가적인 조치를 취하지 않으면, 오퍼를 사용하는 앰버서더는 보안 전문가들의 동기와 기술적 능력이 공격을 방어할 수 있다고, 아마도 영구적으로, 신뢰해야 합니다.

우리는 이러한 신뢰 요구가 신뢰를 최소화하거나 통합하기 위한 2차 시장 및 새로운 기술 응용을 촉진할 것으로 예상합니다. 아래는 기밀성 요구를 더 잘 충족하기 위해 폴리스웜 위에 구축될 수 있는 몇 가지 도구의 예시입니다.

Intel SGX를 통한 신뢰 최소화

Intel SGX는 처음으로 Skylake 프로세서 계열에 탑재된 새로운 기술입니다. SGX는 “enclaves” 내부에서 불투명한 계산 환경을 제공합니다. SGX enclave의 메모리 내용은 동일한 시스템의 다른 소프트웨어나 사용자에게 권한 수준과 무관하게 접근할 수 없습니다. 폴리스웜 맥락에서, SGX enclave는 전문가가 아티팩트를 연구자에게 노출하지 않고, 또한 전문가의 인텔리전스를 누구에게도 공개하지 않고 아티팩트를 스캔할 수 있게 합니다. 따라서 SGX는 앰버서더와 전문가들 간 상호 신뢰를 줄일 수 있는 가능성을 제공합니다.

전문가들은 인증된(그리고 검증된) SGX enclave를 실행해 아티팩트와 인텔리전스를 받아들이고, 앰버서더에게 반환할 주장을 생성할 수 있습니다. 기술적 난관이 있지만, SGX가 분산형 방식으로 서로 부트스트랩되는 enclave를 통해 통합·확장될 수 있다고 확신합니다. 미래 버전의 폴리스웜에서는 앰버서더가 아티팩트를 부트스트랩된 enclave에만 공개하는 “SGX 바운티”를 시장에 게시할 수 있을 것입니다.

Scan-as-a-Service(SaaS) 앰버서더를 통한 신뢰 통합

전문가들은 폴리스웜에 특화된 이유가 있든 없든, 다양한 이유로 계산 작업을 제3자에게 아웃소싱할 수 있습니다. 예를 들어, 많은 전문가가 AWS, Google Compute Engine, Azure와 같은 온디맨드 컴퓨팅 서비스를 활용해 폴리스웜 시장 수요에 맞춰 주장 파이프라인을 확장할 것으로 예상됩니다. 이는 폴리스웜 동기만으로 결정된 선택은 아닙니다.

폴리스웜에 특화된 SaaS 주체에 대한 인센티브는 자연스럽게 발생할 것입니다. 기밀성 맥락에서, 참여자들은 앰버서더와 전문가 사이에서 신뢰할 수 있는 제3자로 작동하며 양쪽과 비밀유지협약(NDA)을 유지하는 SaaS 회사를 설립할 것입니다. 이러한 SaaS 회사들은 SGX enclave와 동일한 목적을 수행하며, 아티팩트를 전문가로부터 보호하고 인텔리전스 세부사항을 앰버서더로부터 보호합니다.

앰버서더는 신원이 불분명한 다수의 전문가보다 공신력 있는 평판을 가진 제3자 SaaS 회사를 더 신뢰하기 쉬울 수 있습니다. 따라서 이들은 전문가에게 직접적으로 오퍼를 보내는 대신 SaaS 주체에게 더 많은 오퍼를 보낼 것입니다.

추가 시장

폴리스웜 마켓은 여러 추가 시장에 대한 수요를 창출할 것입니다. 그중 하나인 (Scan-as-a-Service)는 앞서 추가 기밀성 제어 수단으로 논의되었습니다. 아래는 추가로 예상되는 시장들입니다.

앰버서더

이는 명백하며, 본 문서 전반에서 많이 다루어졌습니다. 많은 소비자는 앰버서더를 통해 시장과 거래하는 것을 선택할 것이지만, 앰버서더를 반드시 거칠 필요는 없습니다.

아티팩트 퍼블리싱 서비스

바운티나 오퍼를 게시할 때, 앰버서더는 아티팩트를 전문가들이 접근할 수 있게 해야 합니다. 아티팩트 호스팅 엔티티는 이 서비스를 제공하여 공유를 원활하게 만듭니다. 고객은 소비자와 앰버서더가 될 것입니다. 우리는 많은 앰버서더가 아티팩트 퍼블리싱 서비스도 함께 제공할 것으로 예상합니다.

평판 추적 서비스

미국에서는 은행이 개인의 신뢰도를 나타내는 “사실” 장부를 유지하기 위해 3개의 신용 평가 기관을 신뢰합니다. 폴리스웜 마켓에서도 유사한 수요가 발생할 것입니다. 시장 참여자들은 이미 논의된 다양한 이유로 다른 참여자의 신뢰도를 정량화하고자 할 것입니다. 따라서 참여자의 신뢰도를 추적하고 이 정보를 제공해 거래 상대방 위험을 완화하는 평판 서비스가 등장할 가능성이 높습니다.

로드맵(Roadmap)

여기서는 폴리스웜 개발의 예비 마일스톤을 제시합니다. 각 마일스톤은 다음을 목표로 합니다:

1. 새로운 기능 제공.
2. 새로운 앰버서더, 전문가, 최종 사용자 트랜잭션을 가능하게 하는 문서와 테스트 제공.

폴리스웜은 모든 트랜잭션을 영구히 보관해야 하는 Bitcoin이나 Ethereum과 같은 네트워크에 비해 뚜렷한 개발적 이점을 가지고 있습니다. 일단 최종 결과값이 확정되거나 오퍼 채널이 체인에 정산되면, 앰버서더와 전문가들은 각각 아티팩트에 대한 인텔리전스와 NCT라는 자신들이 필요로 한 것을 이미 얻은 상태입니다. 이러한 원자성은 우리가 1.0 출시 전까지 비용과 합의 문제 없이 하위 호환되지 않는 변경을 가능하게 합니다.

V0.1 Alpha (2018년 4월 30일)

폴리스웜 Alpha는 토큰 세일 이후 바운티에 대한 프로토타입 엔드투엔드 워크플로우를 제공하는 데 집중할 것입니다. 이 초기 릴리스는 폴리스웜 팀이 본격적으로 부트스트래핑을 시작할 수 있게 합니다. 앰버서더와 전문가들은 폴리스웜 테스트 네트워크(“testnet”)를 통해 거래할 수 있습니다. 기본 바운티 스마트 계약이 폴리스웜 테스트넷에서 제공되어, 앰버서더는 바운티를 게시하고, 전문가들은 검사를 제출하며, 앰버서더는 평결을 산출할 수 있습니다.

우리는 폴리스웜 Alpha가 다음을 달성할 것으로 예상합니다:

- 바운티 금액과 수수료를 보관하고, 검사를 수락하며, 평결을 게시하고, 정확한 전문가들에게 보상을 지급하는 “바운티 매니저” 스마트 계약.
- 폴리스웜 외부 스토리지(e.g. S3, IPFS)를 통한 아티팩트 게시 및 검색.
- 바운티 만료 시 아비터를 선택하기 위한 프로토타입 알고리즘.

- 바운티 게시, 주장 응답, 아비터 최종 결과값 결정에 대한 참조 구현.

V0.2 Beta (2018년 5월 31일)

폴리스웜 Beta는 Raiden 스타일 채널을 통한 폴리스웜 오퍼 지원 제공에 집중할 것입니다. 오퍼는 바운티보다 더 높은 처리량의 아티팩트 평가를 용이하게 하도록 설계되었으며, 각 트랜잭션에 대해 더 효율적인 블록체인 정산을 요구합니다. 폴리스웜 Beta는 오퍼 스마트 계약을 구현할 것입니다. 우리는 이 기능을 앰버서더와 전문가 간에 설정된 Raiden 스타일의 직접 P2P 채널을 통해 testnet에서 구현할 것으로 예상합니다.

우리는 폴리스웜 Beta가 다음을 달성할 것으로 예상합니다:

- 오퍼 채널
 - 분산형 채널 설정
 - 단일 채널을 통한 다중 오퍼
 - 채널 종료 시 NCT 정산
- 오퍼 생성 및 응답에 대한 참조 구현
- 아비터 최종 결과값 통지 및 응답에 대한 참조 구현
- 수수료 징수 및 분배 스마트 계약
- 특정 아티팩트 볼륨에 필요한 신뢰(NCT) 연구 및 정량화
- 전문가와 앰버서더가 바운티 및 오퍼 처리를 자동화할 수 있는 오퍼/바운티 개발 툴킷

V0.3 Gamma (2018년 7월 31일)

폴리스웜 Gamma는 앰버서더, 전문가, 아비터 간의 협업을 촉진하는 매칭 기능을 제공하는 데 집중할 것입니다. 전문가들은 특정 유형의 아티팩트에 맞게 조율된 Workers에 자신의 전문성을 캡슐화할 수 있습니다. 이 Workers를 폴리스웜 레지스트리에 광고할 수 있을 것으로 기대합니다. Worker Registry는 앰버서더가 Stable 릴리스 이전에 위험 없이 Workers와 협업할 수 있도록 해야 합니다(Gamma는 계속 폴리스웜 testnet을 사용).

또한, Alpha와 Beta에서 얻은 피드백을 바탕으로 바운티 도구를 강화·확장하는 방안을 고려할 것입니다. 예를 들어, 바운티는 주장 마감 전까지 다른 전문가에게는 비공개로 유지되며, 마감 이후에만 공개되는 기능이 도움이 될 수 있습니다.

우리는 폴리스웜 Gamma가 다음을 달성할 것으로 예상합니다:

- 아티팩트 분석 기능 및 전문가 저작 Attribution(평판)을 설명하는 Worker Description Language(WDL).
- 분산형·검색 가능한 Workers 및 그 기능 레지스트리.
- 마감 전 바운티 주장의 기밀성 보장.

- 아비터 선택·응답 및 엔드투엔드 바운티 피드백 루프의 최종 확정.

Gamma는 기능적으로 완성될 것으로 예상합니다.

폴리스웜 1.0 (2018년 4분기)

폴리스웜 Stable은 폴리스웜 testnet(테스트 토큰)에서 실제 폴리스웜 마켓으로 이전하기 전에 폴리스웜 Gamma의 버그를 제거하는 데 집중할 것입니다.

Stretch Goal로, 시간과 자금이 허용된다면 Stable에서는 제한된 대상에게만 공개되는 바운티를 통해 아티팩트 기밀성을 일급 기능으로 도입할 수도 있습니다.

폴리스웜 2.0 (2019년 2분기)

폴리스웜의 두 번째 Stable 릴리스에는 두 가지 주요 목표가 있습니다: 오퍼와 바운티를 확장해 더 다양한 아티팩트 유형(e.g. URL, 네트워크 스트림)을 처리하는 것과, 기업 및 개인 사용자가 폴리스웜을 더 쉽게 활용할 수 있도록 하는 것입니다.

향후 폴리스웜 릴리스에서의 아티팩트 유형 확장은, 예를 들어 최종 사용자 URL에 대해 직접 바운티와 오퍼를 걸어 자동화된 피싱 시도 탐지를 가능하게 할 것입니다.

Stable 이후 개발의 우선순위는 폴리스웜의 보호를 엔드포인트에 직접 확장하는 것입니다. 우리는 폴리스웜 인텔리전스를 기반으로 악성 아티팩트를 자동 차단하는 오픈 소스 엔드포인트 보호 제품군의 참조 구현을 개발할 것으로 예상합니다. 우리는 이러한 오픈 에이전트 프레임워크가 최종 사용자의 광범위한 채택의 열쇠라고 봅니다.

향후 기능

폴리스웜의 미래 릴리스는 위협 환경의 진화와 네트워크의 실제 사용을 반영할 것입니다. 우리는 다음과 같은 기능이 네트워크와 최종 사용자 보호라는 궁극적 목표에 도움이 될 기회가 있다고 봅니다(폴리스웜 사용량에 따라 결정됨):

- 유연한 아티팩트 기밀성
 - **기본:** 특정 전문가 또는 SaaS 제공자에게만 아티팩트 공개
 - **고급:** SGX enclave나 완전동형 엔진 외부에는 아티팩트를 전혀 공개하지 않음
- 새로운 도구(e.g. 구독형 위협 피드)
- 오늘날의 엔드포인트 보호 제품군을 대체할 엔드포인트 상주 Worker 컨테이너 배포 지원.

토큰 세일(Token Sale)

폴리 Swarm 생태계의 기술 개발, 커뮤니티 참여, 그리고 참가자 유치는 폴리 Swarm Pte. Ltd.에 의해 진행되며, 이는 폴리 Swarm의 Nectar 유틸리티 토큰(NCT) 판매를 통해 자금을 조달합니다.

이 토큰은 참가자들 간 위협 인텔리전스 거래에 사용됩니다. NCT는 폴리 Swarm의 주요 상호작용을 모두 구동합니다: 바운티 게시, 오픈 채널 개설/종료/교환, 주장 등록, 최종 결과값 결정. 유틸리티 전용 NCT 토큰을 판매함으로써, NCT와 위협 인텔리전스 간 교환 비율은 더 큰 ETH 시장의 변동성에서 격리될 수 있으며, ETH의 가격 변동에 대한 걱정 없이 폴리 Swarm 참여를 활성화할 수 있습니다.

이 섹션은 폴리 Swarm의 토큰 이코노미에 대한 상위 개요를 제공합니다. 본 문서와 토큰 세일 계약 (“Agreement”) 간 상충이 발생할 경우, 계약이 우선합니다. **[토큰 세일 계약은 온라인에서 확인할 수 있습니다.]**

일정(Schedule)

PolySwarm Pte. Ltd., Inc는 현재 초대된 참가자들을 대상으로 토큰 프리세일을 운영하고 있습니다. NCT 공개 세일은 **2018년 2월 20일 19:00 UTC**에 자격을 갖춘 구매자들에게 열리며, **2018년 3월 22일 19:00 UTC**에 종료될 예정입니다.

구매 요건(Purchase Requirements)

NCT는 이더(Ether, ETH)로만 독점적으로 구매할 수 있습니다. 잠재적 구매자는 세일 전에 충분한 ETH를 확보해야 합니다.

토큰 세일은 KYC(Know Your Customer) 통제를 적용하며, 특정 구매를 국가, 이메일 주소, 전체 이름, IP 주소, 토큰 세일 계약 동의 등 KYC 데이터 포인트와 연결하는 독자적 기술 메커니즘을 사용할 것입니다.

캡 / 제한(Caps / Limits)

토큰 세일 기간 종료 후에는 새로운 토큰이 생성되지 않습니다.

NCT 토큰의 총 발행량은 토큰 세일 동안 결정됩니다.

토큰의 최대 발행량은 상한이 있으며, 이는 최대 자금 조달 USD 상한, NCT 가격(ETH 단위), 현재 ETH-USD 환율에 기반합니다. NCT 상한, 가격, 자금 트랜치 등 세부 사항은 토큰 세일 웹페이지를 참조하십시오.

배분(Allocation)

- **70%**의 NCT 토큰은 토큰 세일 기간 동안 판매됩니다.
- 나머지 **30% 중 15%**는 폴리 Swarm 생태계 부트스트래핑을 돕고자 하는 기업, 벤더, 보안 전문가에게 분배됩니다. 수혜자는 PolySwarm Pte. Ltd.의 단독 재량으로 결정됩니다.

- 마지막 **15%** 는 폴리스웜 생태계의 채택을 가속화하는 방식으로 PolySwarm Pte. Ltd.에 의해 사용됩니다. 예시로, 폴리스웜 “해커톤” 참여를 위한 인센티브로 제공될 수 있습니다. 이 배분 또한 PolySwarm Pte. Ltd.의 단독 재량에 따릅니다.

분배(Distribution)

폴리스웜의 Nectar 유틸리티 토큰(“NCT”) 판매로부터 확보된 ETH는 다음과 같이 배분될 예정입니다:



- **54.51%** – 프로토콜 및 소프트웨어 개발
- **3.00%** – 사무실 운영비
- **4.06%** – 운영 비용
- **14.49%** – 법률 비용
- **13.62%** – 마케팅
- **10.32%** – 세금

폴리스웜 팀은 FY19/20 기간 동안 법률 비용이 감소할 것으로 예상합니다. 남은 금액은 마케팅, 운영 비용, 개발자 급여로 재분배됩니다.

예상 세금 비율 10.32%는 낮지만, 비현실적이지 않습니다. 이는 참가자들에게 긍정적입니다. 더 많은 자금이 폴리스웜의 개발과 홍보에 직접 배정되기 때문입니다.

면책 고지(Disclaimer)

이 백서는 잠재적 토큰 구매자에게 기술적 배경을 제공하기 위한 것입니다. 폴리스웜 토큰 세일은 본 문서에 제시된 경제적 도구들의 초기 프로토타입 개발과 테스트에 자금을 지원할 것입니다. 사려 깊은 참가자라면 누구나 예상할 수 있듯, 본 문서에 제시된 세부사항은 Stable 이전 개발 및 테스트 기간 동안 변경될 수 있습니다. PolySwarm Pte. Ltd.와 토큰 구매자의 이해관계는 폴리스웜을 위협 인텔리전스 산업을 진정으로 교란하는 실현 가능한 마켓플레이스로 만드는 데 일치합니다.

결론(Conclusion)

폴리스웜은 보안 전문가, 벤더, 기업 간 새로운 상호작용 방식을 가능하게 하여 위협 인텔리전스 산업을 교란하려는 ERC20 토큰 NCT와 새로운 시장을 제안합니다. 폴리스웜 팀은 소프트웨어 개발 자금 조달과 이 새로운 마켓플레이스를 중심으로 커뮤니티를 육성하기 위해 토큰 론칭을 진행할 예정입니다.

여러분이 *All Angles™* 로부터 사용자를 보호하는 여정에 동참하시길 바랍니다.