# XY Oracle Network: 원천증명 기반암호화 위치 네트워크

Arie Trouw*, Markus Levin†, Scott Scheper‡

January 2018


## 요약

연결되고 위치에 기반한 기술이 점차로 도래함에 따라 우리의 사생활과 안전은 더욱 위치 정보의 정확성 및 합법성에 의존하게 되었다. 위치 데이터 흐름을 관장하는 중앙화된 주체에 대한 필요성을 없애려는 다양한 시도들이 있어 왔으나 그러나 각각의 시도들은 실세계에서 이러한 데이터를 수집하는 기기들의 완전성에 의존해왔다. 위치 정보에 관한 높은 수준의 데이터 확실성을 수립하기 위하여 우리는 영지식 증명(zero-knowledge proof) 체인을 기반으로 하는 혁신적 형태를 이용하는 무신뢰성(trustless)의 암호화 위치 네트워크를 제안한다. **XYO Network(XY Oracle Network)**는 다양한 기기 등급과 프로토콜에 걸쳐 계층화된 위치 검증을 가능케하는 존재이다. 그 중심에는 블록체인 기술의 힘과 실제 세계의 데이터 수집을 오늘날의 직접적 애플리케이션으로 시스템에 연결하는 **원천증명(Proof of Origin)** 및 **연결 증인(Bound Witness)**이라 불리는 일련의 혁신적 암호화된 메커니즘이 자리잡고 있다.


# 1 서론

블록체인 기반의 무신뢰성 스마트 계약의 도래와 함께 계약의 결과를 조정하는 오러클 서비스에 대한 필요성도 그만큼 증가한다. 오늘날의 대부분의 스마트 계약의 실행은 단일하거나 또는 누적된 일련의 권위 있는 오러클에 의존하여 계약 결과에 대한 정산을 한다. 당사자 쌍방이 그러한 구체적 오러클의 권위와 무결성에 대하여 합의하는 경우 이는 충분한 조건이 된다. 그러한 많은 경우 적절한 오러클이 존재하지 않거나 또는 해당 오러클이 오류 또는 결점의 가능성으로 인하여 권위 있는 것을 간주되지 못하고 있다.

위치 오러클은 다음과 같은 범주에 속한다. 실세계의 대상에 대한 위치는 일정한 오러클의 보고, 전달, 저장 및 처리 요소들을 통하여 처리되며 이러한 모든 것들은 오류를 야기할 수 있고 또한 오염이 될 수 있다. 이와 같은 위험 요소들에는 데이터 조작, 데이터 오염, 데이터 손실 및 결탁이 있다.

이에 따라 **위치의 확실성과 정확성이 무신뢰성의 분산화된 위치 오러클의 부재로 인하여 부정적으로 영향을 받을 수 있다**는 문제점이 존재한다. 이더리움(Ethereum) 및 EOS와 같은 플랫폼들은 ICO 형태의 자금 조달 에스크로와 관계된 주요 이용 사례와 관련하여 온라인으로 안전하게 상호 활동을 중재할 수 있는 기능으로 폭넓게 사용이 되어 왔다. 그러나 현재까지 모든 플랫폼들은 현재 정보 채널의 데이터 무결성의 오염 가능성 등으로 인하여 실세계 대신에 전적으로 온라인 세계에만 집중해왔다.

XYO Network는 블록체인 플랫폼을 작성하는 이들을 포함한 개발자들로 하여금 마치 API와도 같이 실세계와 상호 작용할 수 있도록 하는 개념을 위하여 노력을 경주해왔다. XYO Network는 2개의 주체가 중앙화된 제3자 없이 실제 세계에서 거래를 진행할 수 있도록 해주는 세계 최초의 오러클 프로토콜이다. 이러한 개념으로 위치 검증이 개발자들에게 무신뢰성으로 지원됨으로써 현재까지는 불가능하였던 혁신적 이용 사례들을 위한 프로토콜이 제공된다.

XYO Network는 우리의 대고객 비즈니스인 XY Findables를 통하여 전세계에 걸쳐 배포된 100만개의 기기들로 구성된 기존의 인프라를 토대로 구축이 된다. XY의 블루투스 및 GPS 기기들을 통하여 일상적인 고객들은 자신들이 계속적으로 추적하고자 하는 사물(열쇠, 가방, 자전거 및 심지어는 애완동물 등)에 물리적 추적 비콘을 부여할 수 있다. 만일 그러한 사물들이 다른 곳에 놓이거나 또는 분실했을 경우에는 스마트폰 애플리케이션을 통하여 위치를 확인함으로써 그 정확한 위치를 알 수 있다. XY는 단 6년만에 세계에서 가장 방대한 수준의 고객 블루투스 및 GPS 네트워크를 갖추게 되었다.

*XYO Network, **arie.trouw@xyo.network**

[†]XYO Network, **markus.levin@xyo.network**
[‡]XYO Network, **scott.scheper@xyo.network**

# 2 역사적 배경 및 기존의 접근법

## 2.1 위치증명

증명 가능한 위치에 대한 개념은 1960년대부터 제시되어 왔으며, LORAN[1] 등 1940년대의 지상 기반 전파 항법 시스템까지 거슬러 올라 갈 수 있다. 현재는 여러 가지의 검증 매체를 서로 간에 쌓아 삼각화(triangularization) 및 GPS 서비스를 통해 위치증명을 만들어 내는 위치 서비스들이 있다. 하지만 이러한 접근법들은 오늘날 위치 기술에 있어서 우리가 직면하고 있는 가장 중요한 요소 즉, 사기 신호를 감지하고 위치 데이터의 스푸핑(spoofing)을 무력화시키는 시스템의 구축 문제를 제대로 해결해주지 못하고 있다. 이러한 연유로 오늘날의 암호화-위치 플랫폼은 물리적 위치 신호의 원천을 증명하는데 집중하는 것이 되어야 할 것이다

놀라운 것은 위치 검증의 개념을 블록체인 기술에 적용하는 개념은 2016년 9월에 개최된 이더리움의 DevCon 2에서 처음으로 제시되었다는 사실로, 베를린 출신의 이더리움 개발자인 Lefteris Karapetsas가 제기했다. 그의 프로젝트인 Sikorka는 그가 칭하는 소위 실재증명(Proof of Presence)을 사용하여 스마트 계약들이 실제 세계의 현장에 배치될 수 있도록 하였다. 그가 위치와 블록체인 세계를 연결한 시도는 주로 증강 현실의 사용 사례에 초점을 맞추었으며, 위치의 증명에 있어서 그는 파악 질문과 같은 신개념을 선보였다[2].

2016년 9월 17일에는 "위치증명"이라는 용어가 이더리움의 커뮤니티에 공식적으로 등장하였으며[3], 이후에는 Ethereum Foundation의 개발자 Matt Di Ferrante가 다음과 같이 추가적으로 언급하였다:

> *"여러분이 신뢰할 수 있는 위치증명이란 솔직히 말해 가장 실행이 어려운 것 중 하나입니다. 다수 참여자들에 대한 각각의 위치를 검증할 수 있다고 하더라도 향후 그 언제든 어렵게 되지 않을 것이란 보장이 없고, 또한 다수자 보고에만 의존한다는 것은 큰 약점이라고 할 수 있습니다. 만일 누군가가 기기를 열거나 또는 그 펌웨어를 바꾸려고 시도할 경우 개인 키가 파괴되는 것과 같은 조작 방지 기술을 갖춘 특수한 종류의 하드웨어 기기를 갖추게 된다면 보다 보안성이 강화되겠지만, 그럼에도 불구하고 GPS 신호를 속이기가 불가능한 것과 같지는 않을 것입니다. 이를 제대로 시행하여 정확성을 기하려면 많은 대비책과 함께 많은 다양한 데이터 소스들이 필요하기 때문에 아주 충분한 자금의 프로젝트가 되어야 할 것입니다." [3]*
>
> *—Matt Di Ferrante, (Ethereum Foundation 개발자)*

## 2.2 위치증명: 단점

위치증명은 요약하자면 타임스탬핑(time-stamping) 및 탈중앙화(decentralization)와 같은 블록체인의 강력한 자산들을 활용하여 이들을 조작이 어려운 오프 체인(off-chain)의 위치 인식 기기들에 결합하는 것으로 이해될 수 있을 것이다. 암호화 위치 기술의 영역을 우리는 "암호화-위치(crypto-location)"이라고 부른다. 아울러 스마트 계약의 취약성이 단일한 데이터 소스를 사용하는 (따라서 단일한 문제 발생원을 갖는) 오러클과 연관되는 것과 유사하게, 암호화-위치 시스템 역시 동일한 문제에 직면한다. 현재의 암호화-위치 기술의 취약점은 개체의 위치에 대하여 보고를 하는 오프 체인 기기들과 연관이 있다. 스마트 계약에 있어서 이러한 오프 체인 데이터 소스는 오러클이다. XYO Network에 있어서 오프 체인 데이터 소스는 소위 Sentinel이라 칭하는 하나의 특별한 형태의 오러클로 실제 세계를 돌아 다닌다. XYO Network의 중심에 있어서 진정한 혁신은 안전한 암호화-위치 프로토콜의 생성을 위해 우리의 시스템의 구성요소들의 토대를 이루고 있는 무신원(identityless)의 위치 기반 증명을 기반으로 한다.

# 3 XY Oracle Network

"GPS를 받쳐줄 튼튼한 시스템에 대한 필요성은 이미 오래전부터 잘 알려져 왔다. GPS는 대단히 정확하고 신뢰성이 있으나 재밍 (jamming), 스푸핑(spoofing), 사이버 공격 및 기타 형태의 간섭 행위들이 그 빈도와 강도에 있어서 점점 더 심해지고 있다. 이로 인하여 우리의 생활과 경제 활동이 크게 타격을 입게 될 가능성이 있다." [4]

—Dana Goward (RNT Foundation 이사장)

## 3.1 서론

XYO Network의 목표는 공격에 견디고 가능한 데이터에 대한 쿼리가 있을 경우 최고 수준의 확실성을 제공하는 무신뢰성의 분산화된 위치 오러클 시스템을 구축하는 것이다. 우리는 이러한 목표를 영지식 증명 체인을 통하여 시스템의 구성요소에서 위치 스푸핑의 위험을 크게 줄이는 일련의 추상화를 통하여 달성한다.

## 3.2 네트워크 개관

우리의 시스템은 암호화 증명들의 체인을 통하여 위치 데이터에 대한 높은 확실성을 제공하는 연결 기기들의 프로토콜에 대한 진입점을 제공한다. 사용자는 "쿼리(query)"라 부르는 거래의 발급을 통해 스마트 계약 기능[1]을 보유한 제반 블록체인 플랫폼상에서 일련의 위치 데이터를 불러올 수 있다. 이후 XYO Network로부터의 집합자(aggregator)는 계약에 대하여 제기된 이러한 쿼리에 주목하고, 암호화 증명을 이러한 집합자들에게 다시 전달하는 분산화된 기기 집합으로부터 가장 높은 정확성을 지닌 답변을 이끌어 낸다. 이러한 집합자들은 이후 가장 높은 점수의 답변에 대한 합의에 도달한 후 해당 스마트 계약에 답변을 제공한다. 이와 같은 구성요소의 네트워크로 그 어떠한 개체가 특정 시간에 특정 XY 좌표에 있는지를 가장 가능성이 높은 무신뢰성의 확실성으로 확인할 수 있다.

XYO Network는 4가지 주요 구성요소 즉, **Sentinel**(데이터 수집자), **Bridge**(데이터 전달자), **Archivist**(데이터 보관자) 및 **Diviner**(답변 집합자)로 구성된다. Sentinel은 센서, 무선기기 및 기타 수단을 통하여 위치 정보를 수집한다. Bridge는 Sentinel로부터 이러한 데이터를 받아 Archivist에 제공한다. Archivist는 Diviner가 이러한 정보를 분석할 수 있도록 정보를 저장한다. Diviner는 Archivist로부터의 위치 휴리스틱(heuristic)을 분석하여 쿼리에 대한 답변을 생성하고 그에 대한 정확성 점수를 부여한다. 이후 Diviner는 이러한 답변들을 다시금 스마트 계약으로 전달한다(따라서 Diviner가 오러클의 역할을 함). 정확성 점수("**원천 체인 점수**(**Origin Chain Score**)"라고 함)는 일련의 영지식 증명("**원천증명 체인**(**Proof of Origin Chain**)"이라고 함)을 통하여 결정된다. 이러한 체인을 통하여 그 어떠한 기본 정보의 공개 없이 동일 소스로부터 나온 두가지 이상의 데이터가 보장된다. 쿼리 경로 상의 각 구성요소는 그 자체의 원천증명(Proof of Origin)을 생성하며, 이는 이후에 그것이 데이터를 전달하는 각 구성요소에 연결된다. 원천증명은 실제 세계의 데이터에 대한 높은 수준의 신뢰성을 제공하기 위하여 네트워크상에서 전달자의 경로를 따라 암호화 보증을 구축하는 고유 정보이다. 이러한 **원천증명 체인**은 데이터를 수집한 가장 최초의 기기까지 위치 데이터에서 우리가 가질 수 있는 신뢰성을 내포한다. 원천증명의 기능 방식에 대하여는 다음의 섹션에서 살펴보기로 한다.

Diviner 간에 분산화된 합의 메커니즘을 구축하기 위해서 XYO Network는 Diviner로부터 수집된 데이터 및 그 관련된 원천 점수에 따라 쿼리 거래를 저장하는, **XYOMainChain** 이라는 명칭의 공개적이고 변경 불가능한 블록체인에 의존해야 한다. 전체 시스템의 기능에 대한 세부 내용을 살펴보기에 앞서 우선 우리 네트워크의 각 구성요소들의 역할에 대하여 정의해보기로 한다.

[1] Ethereum, Bitcoin + RSK, Stellar, Cardano, IOTA, EOS, NEO, Dragonchain, Lisk, RChain, Counter- party, Monax 및 기타

### 3.2.1 Sentinel

Sentinel은 위치 증인이다. 이들은 데이터 휴리스틱을 관찰하며 임시적 장부를 생산함으로써 휴리스틱의 확실성과 정확성을 보증한다. Sentinel의 가장 중요한 측면은 동일한 소스로부터 온 것이라는 점을 다른 구성요소들이 확신할 수 있는 장부를 Sentinel이 생산한다는 점이다. Sentinel은 원천증명을 암호화 증명의 릴레이 체인에 추가함으로써 이러한 기능을 수행한다. XYO Network는 무신뢰성의 시스템이기 때문에 Sentinel은 정직한 위치 정보를 제공하도록 유도가 되어야 한다. 이는 명성 요소를 지급 요소와 결합함으로써 수행된다. Sentinel은 그 정보가 쿼리의 답변에 사용될 때 XYO Network Token(XYO)으로 보상을 받는다. 보상 수령의 가능성을 높이기 위해서 Sentinel은 그와 동등한 존재들의 것과 부합하는 장부를 생성하고 원천증명을 제공하여 자신들을 위치 정보의 소스임을 확인시켜 주어야 한다.

### 3.2.2 Archivist

Bridge는 위치 데이터 트랜스크라이버(transcriber)로, Sentinel로부터 Diviner로 안전하게 위치 장부를 전달하는 역할을 한다. Bridge의 가장 주요한 측면은 Archivist는 Bridge로부터 받은 휴리스틱 장부가 그 어떠한 식으로든 변경되지 않았다는 안심을 할 수 있다는 점이다. Bridge의 두번째로 중요한 측면은 오리진 메타데이터(metadata)의 추가적인 증명을 더해준다는 점이다. XYO Network는 하나의 무신뢰성 시스템이기 때문에 Bridge가 정직한 휴리스틱을 전달할 수 있도록 유도되어야 한다. 이 기능은 명성 요소를 지급 요소와 결합함으로써 수행된다. Bridge는 자신이 전달한 정보가 쿼리의 답변에 사용될 때 XYO Network Token(XYO)으로 보상을 받는다. 보상 수령의 가능성을 높이기 위해서 Bridge는 그와 동등한 존재들의 것과 부합하는 장부를 생성하고 원천증명을 제공하여 자신들을 휴리스틱의 전달자임을 확인시켜 주어야 한다

### 3.2.3 Archivist

Archivist는 모든 이력 장부들을 저장하기 위하여 분산화된 데이터 세트의 일환으로 위치 정보를 저장한다. 일부 데이터가 소실되거나 또는 일시적으로 이용 불가능할 경우에도 시스템은 정확도만 약간 낮아질 뿐 기능을 지속한다. Archivist는 또한 장부들을 색인화하여 필요 시 장부 데이터 열을 쉽게 반환할 수 있다. Archivist는 로우 데이터(raw data)만을 저장하며 데이터의 검색 및 그와 관련된 이용에 대하여만 XYO Network Token으로 지불을 받는다. 저장은 항상 무료이다

Archivist는 네트워크화되어 있기 때문에 하나의 Archivist 에게 질의를 할 경우 해당 데이터를 포함하고 있지 않은 다른 Archivist들에 대하여도 질의를 하는 결과가 된다. Archivist는 자신에게 반환된 모든 장부 정보를 선택적으로 저장할 수 있다. 이로 인하여 두가지 타입의 Archivist가 나타나는데, 하나는 “클라우드(cloud)”의 데이터 생산 측에 있는 것이고 또 다른 타입은 “클라우드”의 데이터 소비 측에 있는 타입이다. 중간의 Archivist는 하이브리드 타입이다. 데이터 저장의 선택은 강제되지 않으나 IPFS 또는 또 다른 분산화된 저장 솔루션을 통하여 간단하게 이뤄질 수 있다. 데이터가 한 Archivist로부터 다른 Archivist로 이전되는 매 시점마다 추가적인 원천증명이 추가되어 지불에 대한 추적이 이뤄진다 (모든 Archivist에게 지급이 되기 때문). 검색의 경우 유효성을 높이기 위하여 최소 원천증명 수준을 설정할 수 있다. 데이터의 과장을 방지하기 위하여 Sentinel, Bridge 및 Archivist의 비율이 조절되어야 한다.

### 3.2.4 Diviner

Diviner는 XYO Network 중 가장 복잡한 부분이다. Diviner의 전반적 목적은 쿼리에 대한 가장 정확한 데이터를 XYO Network로부터 도출하여 그 데이터를 해당 쿼리의 제기자로 다시 전달하는 것이다. Diviner는 XYO 스마트 계약에 대하여 제기된 쿼리들에 대하여 적절한 블록체인 플랫폼(Ethereum, Stellar, Cardano, IOTA 등)을 찾으며, 이후 Archivist 네트워크와의 직접적인 상호 작용을 통하여 쿼리에 대한 가장 높은 정확도와 신뢰도 점수를 갖는 답변을 찾는다. 이러한 작업은 증인을 최적의 원천증명 체인으로 판단함으로써 이뤄진다. 가장 짧은 시간에 최고 점수의 답변을 도출한 Diviner는 작업증명(Proof of Work)을 통하여 주 XYO 블록체인(XYOMainChain)상에 블록을 생성할 수 있게 된다. 쿼리들은 보상 크기 및 복잡성에 따라 우선순위가 정해지는 관계로 답변에 대하여 제공된 XYO가 많을수록 해당 쿼리의 우선순위는 높아진다.

기타 Diviner들은 블록의 유효성에 대한 합의에 도달한 후 블록에 디지털적으로 서명을 한다. 해당 블록에서 코인베이스(coinbase) 어드레스였던 Diviner는 이후에 거래를 그 정확도 점수와 함께 답변을 담고 있는 스마트

계약으로 보내게 된다. 또한 공격자가 Diviner인척하여 가짜 정보를 블록체인으로 발급하는 것을 방지하기 위해 기타 Diviner들의 서명 목록을 보낸다. 이후 스마트 계약은 페이로드(payload)의 서명 목록을 확인함으로써 이 정보의 완전성을 검증하게 된다.

## 3.3 엔드투엔드(End-to-End) 기능

각 구성요소의 역할에 대하여 설명하였으므로 이제는 시스템 기능의 엔드투엔드(end-to-end) 예를 살펴보기로 한다:

1. **Sentinel의 데이터 수집**
    - Sentinel은 실제 세계 위치 휴리스틱을 수집하여 자기 자신의 원천증명(Proof of Origin)이 그 위의 노드에 연결되도록 준비한다.
2. **Bridge의 Sentinel로부터의 데이터 수집**
    - Bridge는 온라인 Sentinel로부터 필요한 데이터를 수집하여 원천증명을 그들의 체인에 추가한다. 이후 Bridge는 Network상에서 자신들이 Archivist에게 이용될 수 있도록 한다.
3. **Archivist의 Bridge로부터의 데이터 색인화/조합**
    - Bridge는 Archivist에게 지속적으로 정보를 보내며, 이후 Archivist는 위치 휴리스틱 색인과 함께 분산화된 저장소에 유지된다.
4. **Diviner의 사용자 쿼리의 도출**
    - Diviner는 이더리움 스마트 계약에 보내진 쿼리를 찾아 답변 구성 절차의 개시를 결정한다.
5. **Diviner의 Archivist로부터의 데이터 수집**
    - Diviner는 이후 Archivist 네트워크로부터 필요한 적절한 정보를 가져와 쿼리에 대응한다.
6. **Diviner의 답변 구성**
    - Diviner는 Archivist Network로부터 최적의 Origin Chain Score를 갖는, 쿼리에 대한 최적의 답변을 선택한다.
7. **Diviner의 블록 제시**
    - Diviner는 이후에 답변 내용, 쿼리 및 작업증명(Proof of Work)을 통해 지급된 XYO Token(XYO)을 포함하는 XYOMainChain 상에서 블록을 제시한다. 네트워크상의 기타 Diviner들은 블록의 내용을 디지털적으로 서명하고, 이후에 코인베이스 Diviner의 계정이 업데이트되어 유효한 블록에 대한 합의가 도출된 후에 시스템에서 작업증명을 보여주게 된다.
8. **Diviner의 쿼리 개시자에게로의 결과 반송**
    - Diviner는 답변, Origin Chain Score 및 그 디지털 서명 세트를 묶어 XYO 스마트 게약에 안전하게 연결되는 어댑터 구성요소로 보낸다. 어댑터는 Diviner의 완전성이 훼손되지 않도록 하는 역할을 수행하여 디지털적으로 서명된 답변 세트를 스마트 계약으로 보낸다. 이 과정은 블록 생산 과정 바로 이후에 진행된다. 이후 코인베이스 Diviner는 그 노력에 대한 보상을 받는다.
9. **XYO Network 구성요소들의 작업에 대한 보상**
    - 원천증명 체인(Proof of Origin Chain)상의 구성요소들은 쿼리 답변 도출에 대한 그 참여에 대하여 보상을 받게 된다. Sentinel, Bridge, Archivist 및 Diviner 모두가 그 작업에 대하여 보상을 받는다.

같은 쿼리가 2회 이상 질의될 경우에는 특정 시점에 생산된 답변이 당시에 시스템이 제공할 수 있는 가능한 휴리스틱을 토대로 하기 때문에 2개 이상의 답변이 생산될 수 있다. 블록체인에 대한 답변의 제출은 2단계로 진행된다. 먼저, 쿼리에 대한 최적의 답변(Best Answer)을 결정하기 위하여 분석이 실시되어야 한다. 둘째, 시스템에 의해 다수의

답변들이 생성되는 경우, 노드는 답변들을 비교하여 항상 보다 나은 답변을 찾아내게 된다. 간단한 쿼리로 “과거 특정 시간 중 네트워크에서의 노드의 위치는”을 한 예로 들 수 있다.

## 3.4 단일 데이터 소스로서의 블록체인

Diviner들은 그 중심에서 상대 데이터(relative data)를 절대 데이터(absolute data)로 단순하게 변환시킨다. 전체 Archivist 네트워크를 검색하여 XYO Network상에서 쿼리에 대한 절대 답변을 구체화시킨다. Diviner들은 또한 XYOMainChain에 블록을 제시하고 더하는 노드이며, 그들의 작업증명(Proof of Work)에 대하여 보상을 받는다. Archivist 네트워크는 비처리된 데이터의 저장소이며 블록체인은 절대적이고 처리 완료된 데이터의 저장소인 관계로 네트워크는 XYOMainChain에서 최신의 정보를 사용함으로써 Archivist Network을 통한 비싼 전산 처리에 의존하는 대신에 향후의 쿼리에 궁극적으로 답변을 할 수 있다.

XYOMainChain상의 블록들은 쿼리의 답변에 사용된 원천증명 체인(Proof of Origin Chain) 및 구성요소들의 그래프를 저장하기 때문에 향후의 Diviner들은 이러한 절대적인 데이터를 검색하여 낮은 대역폭의 사용으로도 정확한 결과를 도출할 수 있다. 이에 따라 XYOMainChain은 점차적으로 시스템 중에서 가장 중요한 데이터 소스가 된다. 그러나 Sentinel이 수집한 위치 휴리스틱에 관한 최신 정보의 유지를 위하여는 Archivist 네트워크가 여전히 요구된다.

## 3.5 최적의 후보 답변의 선택을 위한 XYO Network의 프레임워크

우리는 최적의 답변(Best Answer)를 일련의 후보 답변(Answer Candidate)들 중에서 최고 수준의 유효성 점수를 제공하고 최저 요구 정확성보다 높은 정확성을 갖는 단일 답변이라고 정의한다. 유효성 점수는 원천 체인 점수(Origin Chain Score)를 토대로 한다. 시스템은 가장 높은 기록의 원천 점수가 어떤 것인지, 보다 높은 점수가 달성될 때까지는 어떤 것이 100%인지, 그리고 어떤 것이 새로운 100%가 되는지를 알고 있다. XYO Network 은 최적의 답변 결정을 위한 최적의 답변 알고리즘(Best Answer Algorithm)의 선택을 허용한다. 이를 통하여 대체 알고리즘을 위한 향후 조사를 위한 확대가 이뤄진다.

데이터가 적절치 못하거나 부정확하다는 이유로 답변으로부터 배제될 경우, 해당 데이터는 Archivist로 순환되어 그 분산화된 저장소로부터 제거가 된다.

## 3.6 퍼블릭 블록체인과의 첫 통합

XYO Network은 Ethereum, Bitcoin + RSK, EOS, NEO, Stellar, Cardano 등과 같은 스마트 계약의 능력을 가진 퍼블릭 블록체인(public blockchain)과 상호 작용을 하도록 설계가 되었다. XYO Network와의 상호 작용을 위해 이를테면 Ethereum의 사용자는 우리의 XYO 스마트 계약에 쿼리를 제기하고 XYO Token(ERC20)으로 지급을 할 수 있다. 우리의 XYO 블록체인인 Diviner의 노드는 이러한 쿼리들에 대하여 지속적으로 Ethereum을 폴링(polling)하고 우리 자신의 XYO 블록체인(XYO Token이라고도 불림) 고유 화폐로 보상을 받는다. 향후 우리는 ERC20의 보유자들로부터 우리의 블록체인의 고유 화폐로 1:1 전환을 함으로써 확장 가능 IoT 용도에 필요한 소액지불 요구기준을 지원하는 거래 수수료를 우리의 플랫폼에 제공할 것이다. 이러한 용도에서 우리는 사용자들로 하여금 퍼블릭 스마트 계약을 통하여 상호 작용을 하는 대신에 우리의 블록체인에 직접적으로 퉈리를 제기하도록 허용할 것이다.

---

# 4 원천증명 (Proof of Origin)

**비신뢰 노드로 구성된 물리적 네트워크에서는 두개 이상의 데이터가 동일 소스로부터 나온 영지식(zero-knowledge proof) 증명을 기반으로 에지 노드(edge node)에 의하여 제공된 데이터의 확실성을 결정할 수 있다.** 이러한 데이터 세트의 사용 및 다수의 유사한 데이터 세트와 최소 한 개 노드의 절대적 위치에 대한 지식과의 결합을 통하여 그 상대 노드의 절대적 위치를 확인할 수 있다.

## 4.1 원천증명 소개

기존의 무신뢰성 시스템은 시스템에서 거래 또는 계약의 서명을 위하여 프라이비트 키(private key)에 의존했다. 이느 해당 데이터에 서명을 하는 네트워크상의 노드가 물리적 및 가상적으로 안전하다는 가정과 잘 매칭된다. 그러나 만일 프라이비트 키가 오염될 경우에는 원천 증명의 능력은 훼손된다.

무신뢰성 개념을 사물인터넷(IoT)에 적용할 때에는 네트워크 상의 에지 노드가 물리적 또는 가상적으로 안전하지 못하다는 가정을 해야 한다. 이로 인하여 고유 ID 사용의 필요 없이 에지 노드를 확인하고 네트워크 외부로부터의 그 어떠한 지식도 필요 없이 그에 의하여 생산된 데이터를 정직하고 유효한 것으로 판단해야 할 필요성이 대두된다.

## 4.2 원천증명의 핵심: 연결 증인

원천증명(Proof of Origin)은 연결 증인(Bound Witness)의 개념에 의존한다. 디지털 계약의 해결을 위하여 사용된 비신뢰성 데이터 소스(오러클)은 유용하지 못하기 때문에 우리는 양방향 위치증명의 존재를 먼저 구축함으로써 제공된 데이터의 확실성을 크게 증대시킬 수 있다. 기본적 양방향 위치 휴리스틱은 접근성인데, 이는 양 당사자 상호 작용에 공동 서명을 함으로써 상호 작용의 발생 및 범위를 검증할 수 있기 때문이다. 이를 통하여 양 노드가 서로간에 근접하였다는 영지식 증명이 이뤄진다.

이후 우리는 무신뢰성 시스템에서의 오러클 증인 노드가 그것이 공유하는 데이터를 수집하였다는 확실성을 결정해야 한다. 무신뢰성 시스템에서는 증인 노드가 결함 또는 오염에 의하여 거짓 데이터를 생산할 수 있다. 비실효 데이터는 해당 휴리스틱의 허용된 범위 밖으로 떨어질 경우 간단하게 감지 및 제거가 될 수 있다. 유효하지만 부정확한 데이터(거짓 데이터 등)는 감지가 보다 어렵다.

## 4.3 단방향 vs. 양방향 위치 휴리스틱

실세계와 관련된 대부분의 데이터(휴리스틱)는 단방향이다. 이는 곧 측정된 요소를 재측정하기가 불가능함을 의미하여 단방향 휴리스틱 데이터의 검증을 매우 어렵게 만든다. 양방향 휴리스틱은 측정된 요소가 그 자신의 측정치를 다른 당사자에게 다시 보고할 수 있는 휴리스틱이며, 이로 인하여 검증이 가능해진다. 위치는 2개의 에지 노드가 상호 간에 보고를 할 수 있는 양방향이라는 점에서 드문 휴리스틱이다. **이에 대한 실제 세계의 사례로는 두 명이 서로 가까이서 셀프카메라를 찍고, 상대방을 위하여 사본을 인쇄한 후 각자가 셀프카메라에 서명을 하는 경우를 들 수 있다. 이러한 과정을 통하여 양자에게는 접근성증명(Proof of Proximity)이 부여된다. 이 두 사람이 이러한 "데이터"를 얻는 유일한 길은 양자가 같은 위치에 함께 있는 것이다.**

이제 네트워크의 효과에 대하여 살펴보자. 모든 에지 노드가 돌아 다니면서 이러한 "셀프카메라"를 지속적으로 생산하고 바인더에서 이들을 저장하는 시스템을 가정해보자. 이들은 또한 그 바인더를 시간 순차적 순서로 저장할 것으로 예상되고 그 어느 것도 삭제가 허용되지 않는다. 이를 통하여 상대방 에지 노드에 대한 기록기로 상호 참조가 가능한, 각 에지 노드를 위한 접근성 기록기가 구축된다.

## 4.4 비 에지 노드

모든 노드들은 브리지, 릴레이, 저장소 및 분석 노드를 포함하여 "증인(witness)"으로 간주된다. 이를 통하여 한 노드로부터 다음 노드로 전달된 모든 데이터가 연결이 된다. 이것이 **연결 증인(Bound Witness)**의 개념이다.

## 4.5 상호 참조 (Cross Reference)

각 에지 노드에 의하여 생산 및 함께 묶인 모든 “셀프카메라” 세트의 분석을 통하여 시스템은 네트워크 내의 모든 노드의 상대적 접근성으로부터 최적의 답변(Best Answer)을 얻게 된다. 만일 모든 노드가 정직 및 정확하게 보고를 한다면, 에지 노드의 모든 상대 포지션들의 맵핑은 가능한 최대한의 확실성과 정확성(즉, 100%)을 달성하게 된다. 이와는 반대로 만일 모든 노드가 부정직 또는 결함이 있는 경우에는 확실성 및 정확성 모두가 최소한인 0%가 된다.

보고된 데이터 세트 및 에지 노드 중 하나의 상대 포지션에 대한 쿼리를 기반으로 확실성 및 정확성 계수와 더불어 해당 포지션에 대한 근사치가 생성된다.

동일한 데이터 세트와 동일한 분석 알고리즘을 기반으로 모든 계산은 동일한 포지션 근사치 및 확실성과 정확성의 동일한 계수에 도착해야 한다.

## 4.6 다이어그램

S’ 및 S”(Figure 1 참조)는 휴리스틱을 수집하는 각각 하나의 Sentinel(에지 노드)이다. 이들은 서로 접촉하게 되면 휴리스틱 데이터와 퍼블릭 키를 교환한다. 양자는 상호 작용에 대한 완전한 기록을 구축한 후 그 결과의 상호 작용에 서명한다. 이러한 서명된 기록은 이후에 그들의 로컬 장부 모두에서 다음의 엔트리가 된다 (S’에 대하여 16 및S”에 대하여 3). 이러한 액션을 통하여 이 두 증인들이 서로 근접한 존재처럼 서로 묶게 된다.

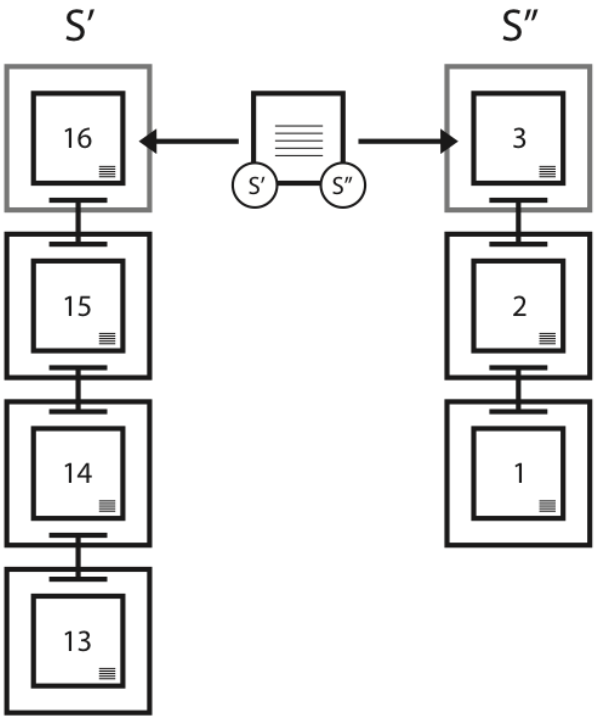


*Figure 1. 두 Sentinel 간의 증인 바인딩의 예*

## 4.7 원천 체인 (Origin Chain)

각 원천(origin)은 그 자체의 장부를 유지하며 그것에 서명하여 하나의 원천증명 체인(Proof of Origin Chain)을 만든다. 이 원천증명 체인에 관한 정보가 공유되면 그것은 사실상 항구적으로 유지된다. 이는 그 공유 이후에 발생하는 포크(fork)가 체인을 종료시키고 증인으로부터의 모든 미래의 데이터가 새로운 증인으로부터 온 것처럼 처리되도록 하기 때문이다. 원천증명 체인에서 링크를 생성하기 위하여 원천은 퍼블릭/프라이비트 키 페어를 생성한다. 이후에는 양 블록 모두에 퍼블릭 키를 포함시킨 다음 동일한 페어로 이전 및 다음의 블록 모두에 서명을 한다. 서명이 완료된 후 즉시 프라이비트 키는 삭제된다. 프라이비트 키의 즉각적 삭제로 키가 도난 또는 재사용될 위험이 크게 줄어든다.

각 원천(origin)은 그 자체의 장부를 유지하며 그것에 서명하여 하나의 원천증명 체인(Proof of Origin Chain)을 만든다. 이 원천증명 체인에 관한 정보가 공유되면 그것은 사실상 항구적으로 유지된다. 이는 그 공유 이후에 발생하는 포크(fork)가 체인을 종료시키고 증인으로부터의 모든 미래의 데이터가 새로운 증인으로부터 온 것처럼 처리되도록 하기 때문이다. 원천증명 체인에서 링크를 생성하기 위하여 원천은 퍼블릭/프라이비트 키 페어를 생성한다. 이후에는 양 블록 모두에 퍼블릭 키를 포함시킨 다음 동일한 페어로 이전 및 다음의 블록 모두에 서명을 한다. 서명이 완료된 후 즉시 프라이비트 키는 삭제된다. 프라이비트 키의 즉각적 삭제로 키가 도난 또는 재사용될 위험이 크게 줄어든다.

원천증명 체인은 XYO Network으로 흘러 들어가는 장부들이 유효한지 확인하기 위한 열쇠가 된다. 데이터 소스에 대한 고유 ID는 위조가 될 수 있기 때문에 실효성이 부족하다. 프라이비트 키 서명은 XYO Network의 대부분이 물리적 보안의 확보가 어렵거나 불가능하며 따라서 나쁜 의도를 가진 자가 프라이비트 키를 훔칠 수 있는 가능성이 있기 때문에 역시 실질적이지 못하다. 이를 해결하기 위하여 XYO Network는 잠정 키 체인(Transient Key Chain)을 이용한다. 이것의 효용성은 데이터의 원천 체인을 조작하기가 불가능하다는 점이다. 그러나 일단 체인이 파손이 되면 항구적으로 파손된 상태가 되며 따라서 하나의 섬이 되고 만다.

휴리스틱 장부가 XYO Network에서 보내지면 수신기(receiver)는 그 자체의 원천증명을 추가하며, 이를 통하여 원천증명이 길어지고 원천증명 인터섹션(Proof of Origin Intersection)을 생성한다. 원천증명 체인(Proof of Origin Chain) 및 원천증명 인터섹션(Proof of Origin Intersection)은 Diviner가 장부의 유효성을 검증하기 위하여 사용하는 기본적 지표이다. 장부 평판(Ledger Reputation)을 위한 등식은 실질적으로 몇 퍼센트의 XYO Network이 그와 연계된 원천증명 볼(Proof of Origin Ball)의 만들기에 참여했는가이다. 이론적으로 만일 XYO Network 기록의 100퍼센트가 원천증명과 링크가 되고 이후에 완전히 분석이 되면, 그것이 유효하게 될 가능성은 100퍼센트이다. 만일 XYO Network 기록의 0%가 분석에 이용 가능하다면 유효성은 0퍼센트로 떨어진다.

추가적인 보안을 위하여 체인 링크(Chain Link)에 대한 퍼블릭 키는 그에 대한 2차 엔트리가 이용 가능할 때까지는 제공되지 않는다. 이를 통하여 엔트리 및 이전 또는 다음 링크에서 저장될 기타 데이터 간에 시간 간격이 생긴다.

## 4.8 원천 체인 점수 (Origin Chain Score)

원천 체인 점수는 다음과 같이 계산한다 (디폴트 알고리즘):

- PcL = 원천증명 체인의 길이
- PcD = 원천증명 체인의 난이도
- Pc' Pc" O = Pc' 및 Pc"에 대한 원천증명 체인 오버랩

$$Score = \prod_{i=0}^{i=n} \frac{PcL * PcD}{Pc' Pc'' O}$$

## 4.9 원천 트리 (Origin Tree)

원천 트리는 답변의 개략적 유효성을 계산하기 위하여 사용된다. 이는 특정한 단언적인 답변을 위한 데이터에 가장 잘 맞는 트리인 이상적 트리(Ideal Tree)를 생성하기 위하여 수집된 데이터를 사용한다. 만일 노드 N이 X,Y,Z,T 위치에 위치할 경우, 데이터 세트 내의 전체 데이터에 걸친 오차는 일정한 가치를 갖는다. 이러한 오차를 계산하기 위해서 우리는 MIN, MAX, MEAN, MEDIAN 및 AVERAGE DISTANCE FROM THE MEAN를 계산한다.

모든 점수 s의 세트 S, 원천증명 체인 난이도 PcD 및 오차율 error를 기준으로 하여 결정된 최적의 답변(Best Answer)은 다음과 같다:

$$BestAnswerScore = \max_{\forall s \in S_j} [PcD * (1 - error)]$$

즉, 가장 높은 최적의 답변 점수(Best Answer Score)를 획득한 단언적 답변이 최적의 답변(Best Answer)이다. 우리는 원천증명 트리를 이용하여 불가능한 가지(이상점)들을 확인하고 제거할 수 있다.

## 4.10 잠정 키 체인화 (Transient Key Chaining)

임시적인 프라이비트 키를 사용하여 일련의 데이터 패킷을 체인화하여 두개의 연속적인 패킷에 서명을 할 수 있다. 프라이비트 키와 쌍을 이룬 퍼블릭 키가 데이터 패킷에 포함될 경우, 수신기는 양 패킷이 동일한 프라이비트 키에

의하여 서명이 된 것을 확인할 수 있다. 패킷 내의 데이터는 서명을 파기하지 않고는 수정이 불가능한 관계로 서명된 패킷이 Bridge 또는 저장 노드와 같은 제3자에 의하여 변경되지 않았음을 확신할 수 있다.

## 4.11 링크의 깊이

최소한의 경우, 노드는 원천증명 체인(Proof of Origin Chain) 내의 모든 링크에 대해 새로운 퍼블릭/프라이비트 키 페어를 생성하며, 이 링크는 1의 링크 깊이(Link Depth)를 갖는다. 하나의 Ledger Entry에 대한 링크 테이블 내에는 N 엔트리가 있을 수 있으며, 각 엔트리는 링크의 파트 2가 추가 추가될 때 거리를 명시하게 된다. 그 어떠한 두개의 링크도 베이스 2 척도에서 동일한 등급 순서를 갖지 않는다. 예를 들어 엔트리 [1,3,7,12,39]는 허용되나 [1,3,7,12,15]는 허용되지 않는다.

이전 블록이 발행될 경우 깊이 1 링크가 생성, 사용 및 삭제가 된다. 그러나 1보다 큰 깊이의 링크는 이전의 블록이 서명됨에 따라 그 페어가 생성이 되며, 두번째의 서명은 추후 n 블록 이후에야 발생하며, 이 이후에 프라이비트 키는 삭제된다. 이러한 연유로 1보다 큰 깊이의 링크는 깊이 1의 링크보다 항상 덜 안전한 것으로 간주되나 그러한 링크는 낮은 안전 대신에 기능 개선과 데이터 손실을 줄이는데 사용될 수 있다.

## 4.12 고정된 순서

장부 순서의 결정에 있어서의 핵심적 요소는 그 보고 순서이다. 기기가 원천증명이 서명된 장부의 순서를 변경할 수 없으므로 모든 장부들을 포괄적으로 검토함으로써 절대적 순서가 수립될 수 있다.

## 4.13 마지막에서 두번째의 발행

원천증명의 수립을 위한 기본적 방법은 Sentinel이 항상 그 마지막에서 두번째의 블록을 최종 블록에 대한 보고 없이 보고한다는 사실을 바탕으로 하고 있다. 이를 통하여 최종 블록은 그 이전에 대한 서명된 링크를 링크의 증빙으로 가질 수 있게 된다.

## 4.14 빈 링크(Empty Link)

원천증명 체인을 보다 안전하게 만들기 위해서는 체인이 최대 매 10초당 1회~최소 매 6초당 1회 업데이트되도록 하는 것이 필요하다. 새로운 데이터가 없을 경우, 빈 블록이 체인에 추가된다.

## 4.15 다이어그램

시간이 좌측에서 우측으로 진행됨에 따라 (Figure 2), 구축되는 원천증명 체인도 길어진다. 그 어느 시점이든 체인의 생산자는 짙은 경계를 가진 엔트리를 콜러에 제공함으로써 사용 가능하기 전에 엔트리의 두번째 서명을 기다리게 된다. 예를 들어 3번째 컬럼에서 엔트리 2와 1만이 체인의 일부로 반환이 된다.

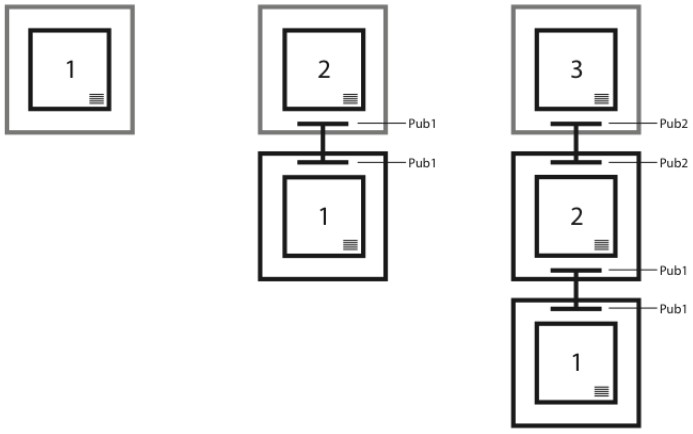


*Figure 2. 원천증명 체인에서의 링크 포함의 예*

### 4.16 요약

잠정적 프라이비트 키로 순차적 페어에 서명되고 페어를 이룬 퍼블릭 키를 포함하는 일련의 데이터 패킷을 기반으로, 패킷이 동일한 원천으로부터 왔다는 사실이 절대적 확실성으로 결정될 수 있다.

---

# 5 보안 관련 사항

## 5.1 가짜 Diviner 공격

디지털 서명 세트는 XYO 스마트 계약으로 보내지는데, 이는 계약이 답변을 보낸 Diviner의 완전성을 확인할 필요가 있기 때문이다. 이후 계약은 높은 신뢰도 간격으로 이 목록에 서명한 다른 Diviner들을 확인할 수 있다. 이것이 없이는 전달 오러클이 시스템 내에서 유일한 이상 및 위험 원천이 될 것이다.

## 5.2 Sentinel DDoS 공격

생각해보아야 할 또 다른 공격은 특정 지역 내에서의 Sentinel 노드 사이에서의 '분산 서비스 거부 공격'(Distributed Denial of Service: DDoS)이다. 공격자는 Sentinel에 대한 수많은 연결을 시도함으로써 Sentinel이 정확한 정보를 전달하거나 또는 그 어떠한 정보든 Bridge에게 전달하는 것을 방해하려는 시도를 한다. 우리는 이러한 문제를 Sentinel에 연결하려는 모든 시도에 작은 암호화된 퍼즐을 요구함으로써 해결할 수 있다. 쿼리는 Sentinel에 많은 수의 연결을 하지 않으므로 이는 XYO 릴레이 시스템에 커다란 부담을 주지 않으며, 공격자로 하여금 우리 네트워크에 대한 성공적인 DDoS 공격을 하려면 많은 리소스를 사용해야만 하도록 요구를 한다. 그 어떠한 시점이든 원천증명 체인은 XYOMainChain 상에 저장된 모든 이에 의하여 확인될 수 있다. 이를 통하여 만일 체인상의 단일 주체가 손상되었을 경우 쿼리 답변의 정확성(원천 제인 점수)은 0로 떨어지게 된다.

---

# 6 XYO Token 경제

오러클은 분산화된 애플리케이션을 위한 파워 및 인프라 니즈의 중요한 부분으로, 그 주요 초점이 권위를 가진 오러클들의 연결성 및 집합성에 맞춰진다. 우리는 오러클에 대한 완전히 분산화되고 무신뢰성인 시스템은 분산화된 애플리케이션이 그들의 최대한의 잠재력을 발휘하기 위하여 필요하다고 생각한다.

## 6.1 XYO Network 암호경제학

우리는 XYO Network의 사용을 통하여 정확하고 신뢰성 있는 위치 휴리스틱을 제공하기 위한 바람직한 활동을 유도하기 위하여 XYO Token을 사용한다. XYO Token은 특정 사물의 XY 좌표에 대한 검증을 위하여 실제 세계와의 연결에 필요한 "가스(Gag)"로 생각할 수 있다.

그 과정은 다음과 같이 진행된다: 토큰 보유자가 우선 쿼리(query)를 가지고 XYO Network에 질의를 한다 (예: "XYO 어드레스 0x123456789를 갖는 전자상거래 주문 패키지의 위치는?"). 이후 쿼리는 큐(queue)로 보내져 처리 및 답변을 기다리게 된다. 사용자는 각 쿼리 생성 시 원하는 신뢰도 수준과 XYO 가스 가격을 설정할 수 있다. 쿼리의 비용(XYO Token 단위)은 해당 쿼리에 대한 답변 제공을 위한 데이터의 양과 시장 상황에 의거하여 결정된다. 데이터가 더욱 많이 필요할수록 쿼리는 더욱 비싸지게 되고 XYO 가스 가격이 올라간다. XYO Network에 대한 쿼리들은 매우 광범위하고 고가가 될 잠재력이 있다. 이를테면 운송 및 물류 회사는 XYO Network에게 "우리 차량들의 각각의 위치는?"이라는 질의를 할 수 있을 것이다

일단 XYO Token 보유자가 XYO Network에 질의를 하고 요청된 가스를 지불하게 되면 해당 작업의 모든 Diviner(데이터를 분석하여 쿼리에 답변을 함)가 관련 Archivists로 호출하여 쿼리에 답변하기 위하여 필요한 관련 데이터를 검색한다. 반환된 데이터는 본래 Sentinel로부터 데이터를 수집하였던 Bridge로부터 오는 것이다. Sentinel은 기본적으로 개체의 위치를 확인하는 기기 또는 신호이다. Sentinel에는 블루투스 트래커(tracker), GPS 트래커, IoT 기기에 내장된 지오로케이션(geo-location) 추적, 위성 추적 기술, QR- 코드 스캐너, RFID 스캐닝 및 기타 많은 기능들이 포함된다. XY Findables는 실제 세계의 위치 휴리스틱을 테스트 및 처리를 가능케 한 소비자용 블루투스 및 GPS 비즈니스를 시작하고 이끌어 왔다. XY Findables의 소비자 비즈니스 구축을 위한 모든 노력들은 XYO Network Blockchain Protocol를 설계하는데 커다란 역할을 하였다.

만일 Sentinel 기기가 제공한 데이터(블루투스 비콘 등)가 커리의 답변에 사용될 경우, 거래와 관련된 4가지의 모든 구성요소들이 토큰 보유자가 지불한 XYO 가스의 일부를 받으며, 그 4 구성요소는 다음과 같다: Diviner (답변을 찾음), Archiver (데이터를 저장), Bridge (데이터를 전송) 및 Sentinel (위치 데이터를 기록). XYO Network의 4개 구성요소 중 3개 사이의 가스의 배분은 항상 같은 비율이다. 예외는 Diviner의 것으로, 이것에 의한 답변 제공 과정에서의 참여는 보다 광범위하다. 각 구성요소에 있어서 가스는 공평하게 배분이 된다.

## 6.2 독립성에 대한 보상

위치 수집 기기들은 네트워크의 원자 블록이며, 단일한 기기가 시스템의 하나 또는 그보다 많은 구성 요소로서의 역할을 할 수 있다. 그러나 특히, 대규모 XYO Network의 경우, 기기들이 이러한 구성요소들의 두 가지 이상의 역할을 하는 것은 드문 일이다. 또한 독립적인 원천증명을 갖는 블록체인 장부는 보다 높게 평가되므로 다수의 구성요소로 작용하는 기기에 대하여는 암호경제학적 패널티가 부여된다.

## 6.3 정상성 완전성에 대한 보상

XYO Network 내의 Sentinel에게는 그들의 수명 주기에 걸친 무브먼트의 질에 따라 정상성 계수(stationarity coefficient)가 부여된다. Sentinel이 그 어느 기간 동안 적게 이동할수록 그 데이터의 신뢰성은 높아진다. 어떠한 Sentinel로 쿼리를 라우팅할 것인가를 고려할 때 Archivist는 이러한 정상성 계수를 추적 및 분석한다.

## 6.4 Token 사용의 인센티브 제공

토큰 보유자에 의한 토큰 사용을 장려하지 않는 시스템은 기초 경제에 대한 장기적인 문제점을 초래한다. 이는 가치의 저장이 매우 희소한 생태계를 낳고, 또한 효용성 및 유동성의 진작 대신에 토큰을 사용치 않는 것에 대한 이유를 촉발시키게 된다.

오늘날의 다수의 암호화화폐들은 지나치게 토큰 마이너(miner)(Sentinel, Bridge, Archivists, Diviner 등)에 초점을 맞추고 있으며 토큰 사용자들에게는 집중하지 않고 있다. XYO Token은 이 두가지 모두에 집중한다.

XYO Token 모델은 마이너에 대한 인센티브 제공을 통하여 정확한 데이터의 제공뿐만 아니라 데이터 제공 시점에 대한 파악에 대하여도 주력한다. 네트워크 유동성이 높을 때 대비, 네트워크 유동성이 낮을 때에는 최종 사용자가 보다 많은 거래를 할수록 보상을 받는다. 따라서 XYO Token 생태계는 균형 있고 유동적이며 튼튼하다.

## 6.5 XYO Token의 스펙

일반 토큰 판매는 1 ETH: 100,000 XYO부터 시작하여 최대 1 ETH: 33,333 EYO까지의 계층적 가격 결정 구조를 갖고 있다. 우리의 수량 및 시간 기반의 가격 결정 구조와 관련한 상세한 내용은 추후 발표할 예정이다.

- 스마트 계약 플랫폼: Ethereum
- 계약 타입: ERC20
- Token: XYO
- Token 명: XYO Network Utility Token
- Token 어드레스: 0x55296f69f40ea6d20e478533c15a6b08b654e758
- 총 생성: Token 본격 판매 이후에 도달한 양으로 한정
- 예상 XYO 토큰 캡: 4800만 달러
- 판매 및 분배되지 못한 Token: token 판매 행사 후에 번(burn)됨. 본격 판매의 종료 후에는 그 어떠한 XYO token도 생성되지 않음

# 7 XYO Network 용례

XYO Network는 여러 산업에 걸쳐 광범위하게 활용이 가능하다. 이를테면 그 주요 고객에게 배송 후 지불 서비스를 제공하는 전자상거래 회사를 예를 들 수 있을 것이다. 전자상거래 회사가 XYO Network 및 XYO Platform(XYO Token을 사용)을 활용하여 스마트 계약을 (이더리움의 플랫폼 등에) 작성함으로써 이러한 서비스를 제공할 수 있다. 이후에 XYO Network는 고객에게 전달될 물품의 위치와 함께 창고 선반으로부터 배송업체, 그리고 고객의 집과 그 중간의 모든 이행 단계에 대한 추적을 할 수 있게 된다. 이를 통하여 전자상거래 소매업체 및 웹사이트는 물품이 고객의 집 현관뿐만 아니라 집 안으로 안전하게 전달되었음을 무신뢰성의 방식으로 확인을 할 수 있게 된다. 물품이 고객의 집에 도착한 것으로 확인되면(구체적인 XY 좌표로 정의 및 확인), 해당 배송은 완료된 것으로 간주되며 판매자에 대한 지급도 이뤄진다. 이에 따라 XYO Network의 전자상거래와의 통합을 통하여 판매업체가 사기 행위로부터 보호가 되고 고객도 물품이 자신의 집에 도착한 이후에야 지불을 할 수 있다.

위의 경우와 완전히 달리, 호텔 리뷰 사이트에 XYO Network를 결합하는 사례를 생각해보자. 이 사이트의 현재의 문제점은 그 리뷰의 내용들이 신뢰를 얻지 못하는 경우가 많다는 점이다. 호텔 소유주들은 많은 비용을 들여서라도 그들에 대한 리뷰를 개선시키려하기 마련이다. 한 예를 들어 미국 샌디에이고에 거주하는 사람이 인도네시아 발리의 한 호텔로 가서 2주일간 숙박한 뒤 다시 샌디에이고로 돌아와 호텔에 대한 후기를 작성했다면 어떠할까? 이러한 리뷰는 높은 신뢰도를 얻었을 것이고 특히 그 작성자가 검증된 위치 데이터를 가지고 많은 리뷰를 작성해온 사람이라면 더욱 그러할 것이다.

---

# 8 XYO Network의 확장

우리들은 전세계에 걸쳐 100만개 이상의 블루투스 및 GPS 기기로 구성된 실제 세계의 네트워크를 성공적으로 구축해왔다. 대부분의 위치 네트워크는 아직 이러한 단계에 이르지 못했으며 또한 광대한 네트워크의 구축에 필요한 임계 수준을 확보하지 못했다. 그러나 XY가 구축한 Sentinel 네트워크는 단지 시작점에 불과하다. XYO Network는 모든 위치 기기 운영자들이 접속하여 XYO Token의 확보를 시작할 수 있는 개방형 시스템이다.

일반적으로 XYO Network상에 Sentinel의 수가 많을수록 네트워크의 신뢰성은 높아진다. 네트워크의 확대를 위하여 XYO Network는 다른 기업들과 제휴하여 자체적인 XY 비콘 네트워크를 초월하는 Sentinel 네트워크로 확대하고 있다.

---

# 9 감사의 말씀

본 백서(white paper)는 다음과 같은 분들로부터 우리의 비전에 대한 신념을 통하여 가능할 수 있었던 탁월한 팀 노력의 산물이다: 백서를 보다 간결하게 정리하고 그 기술적 내용을 세상에 제대로 전하는데 도움을 주신 Raul Jordan (Harvard College, Thiel Fellow 및 XYO Network 어드바이저); 탁월한 세부적 검토 작업을 해주신 Christine Sako (특히 구성과 모범적 사례에 대한 도움을 제공); 관련 용례에 대한 조사와 편집을 해주신 Johnny Kolasinski. 끝으로 면밀한 검토와 창조적인 의견을 주신 John Arana.

# 참조문헌

[1] Blanchard, Walter. Hyperbolic Airborne Radio Navigation Aids. Journal of Navigation, 44(3), September 1991.

[ 2 ] Karapetsas, Lefteris. Sikorka.io.
http://sikorka.io/files/devcon2.pdf. Shanghai, September 29, 2016.

[3] Di Ferrante, Matt. Proof of Location. https://www.reddit.com/r/ethereum/comments/539o9c/proof of location/. September 17, 2016.

[ 4 ] Goward, Dana. RNT Foundation Testifies Before Congress. US House of Representatives Hearing: “Finding Your Way: The Future of Federal Aids to Navigation,” Washington, DC, February 4, 2014.

# 용어 설명

**정확도(accuracy)**
어떠한 데이터 포인트 또는 휴리스틱(heuristic)이 구체적인 오차 한계 내에 있음에 대한 신뢰성 척도.

**Archivist**
Archivist는 모든 이력 장부들을 저장하기 위하여 분산화된 데이터 세트의 일환으로 휴리스틱을 저장한다. 일부 데이터가 소실되거나 또는 일시적으로 이용 불가능할 경우에도 시스템은 정확도만 약간 낮아질 뿐 기능을 지속한다. Archivist는 또한 장부들을 색인화하여 필요 시 장부 데이터 열을 반환할 수 있다. Archivist는 로우 데이터(raw data)만을 저장하며 데이터의 검색에 대하여만 지불을 받는다. 저장은 항상 무료이다.

**최적의 답변(Best Answer)**
후보 답변(Answer Candidate) 목록 중에서 가장 높은 유효성 점수를 제시하고 최소 요구 정확성보다 높은 정확도 점수를 제공하는 단일 답변.

**최적의 답변 알고리즘(Best Answer Algorithm)**
Diviner가 답변을 선택할 때 최적의 답변 점수를 생성하기 위하여 사용되는 알고리즘. XYO Network는 특화된 알고리즘의 추가를 허용하며, 사용자로 하여금 어떠한 알고리즘을 사용할 것인지 구체화할 수 있도록 허용한다. 동일한 데이터 세트가 주어진 Diviner 에서 작동 시 이 알고리즘은 동일한 점수가 되어야 한다.

**연결 증인(Bound Witness)**
연결 증인은 양방향 휴리스틱의 존재로 인하여 달성된 개념이다. 디지털 계약 해결을 위한 비신뢰성의 데이터 소스는 유용성이 없기 때문에 그러한 휴리스틱의 구축에 의하여 제공된 데이터의 확실성이 크게 증가한다. 기본적 양방향 휴리스틱은 근접성(proximity)인데, 이는 양 당사자가 상호작용에 공동 서명을 함으로써 상호작용의 발생 및 범위에 대하여 확인할 수 있기 때문이다. 이를 통하여 두 노드가 서로 근접하였다는 영지식 증명(zero-knowledge proof)이 가능하다.

**Bridge**
Bridge는 휴리스틱 트랜스크라이버(transcriber)이다. 이는Sentinel로부터 Diviner로 안전하게 휴리스틱 장부를 전달한다. Bridge의 가장 주요한 측면은 Diviner는 Bridge로부터 받은 휴리스틱 장부가 그 어떠한 식으로든 변경되지

않았다는 안심을 할 수 있다는 점이다. Bridge의 두번째로 중요한 측면은 오리진 메타데이터(metadata)의 추가적인 증명을 더해준다는 점이다.

**확실성(certainty)**
어떠한 데이터 포인트 또는 휴리스틱(heuristic)이 오염이나 조작으로부터 안전할 것이라는 가능성의 척도.

**암호화-위치(crypto-location)**
암호학적 위치 기술의 영역.

**암호경제학(cryptoeconomics)**
분산화된 디지털 경제에서 재화와 서비스의 생산, 분배 및 소비를 관장하는 프로토콜에 대하여 연구하는 공식적 분야. 암호경제학은 이러한 프로토콜의 설계 및 특징화에 집중하는 실제 과학이다.

**Diviner**
Diviner는 XYO Network에 의하여 저장된 이력 데이터를 분석함으로써 주어진 쿼리에 대하여 답변을 한다. XYO Network에 저장된 휴리스틱은 해당 휴리스틱의 타당성과 정확도를 결정하기 위한 높은 원천증명 수준을 갖추어야 한다. Diviner는 그 원천증명을 토대로 증인을 판단함으로써 답변을 확보 및 전달한다. XYO Network는 무신뢰성 시스템이기 때문에 Diviner는 정직한 휴리스틱 분석을 제공하도록 유도되어야 한다. Sentinel 및 Bridge와는 달리 Diviner는 작업 증명을 이용하여 블록체인에 대한 답변을 추가한다.

**휴리스틱(heuristic)**
Sentinel의 포지션(근접성, 온도, 빛, 동작 등…)과 관련된 실제 세계에 대한 데이터 포인트.

**오러클(oracle)**
정확도와 확실성을 가진 답변을 제공함으로써 디지털 계약을 해결하는 디앱(DApp: 분산화된 애플리케이션) 시스템의 일부. 암호학에서 유래하는 “오러클”이라는 용어는 암호학에서 진정한 랜덤 소스(예: 랜덤 번호의 것)를 의미한다. 오러클은 암호화 등식으로부터 그 이상의 세계로 필요한 게이트(gate)를 제공한다. 오러클은 스마트 계약에 대하여 체인 이상(실제 세계 또는 오프 체인)으로부터의 정보를 제공한다. 오러클은 디지털 세계로부터 실제 세계로의 인터페이스이다. 하나의 음산한 예를 들어, Last Will & Testament(유언 및 유언장)를 예로 들어 보자. 유언의 조건들은 해당 유언자가 사망했다는 확인과 함께 실행이 된다. 이에 공식적 소스로부터 관련 데이터를 편집 및 축적함으로써 유언을 실행하기 위한 오러클 서비스가 구축이 된다. 이후 오러클은 해당자의 사망 여부를 확인하기 위하여 스마트 계약이 호출하게되는 피드(feed) 또는 엔드 포인트로서 사용이 될 수 있다.

**원천 체인 점수(Origin Chain Score)**
T원천 체인에 대하여 그 신뢰성을 결정하기 위하여 배정된 점수. 이 평가는 길이, 얽힘, 오버랩, 및 중복을 고려한다.

**원천 트리(Origin Tree)**
휴리스틱 장부의 원천을 구체적인 확실성 수준으로 구축하기 위한, 다양한 원천 체인(Origin Chain)을부터 얻어진 장부 엔트리 데이터 세트.

**원천증명(Proof of Origin)**
원천증명은 XYO Network로 흘러 들어오는 장부들이 유효한 것인지를 검증하기 위한 키(key)이다. 데이터 소스에 대한 고유 ID는 조작이 될 수 있기 때문에 실효성이 없다. 개인 키 서명도 XYO Network의 대부분이 물리적으로 확보하기가 어렵거나 또는 불가능하기 때문에 역시 실질적이지 못하며, 따라서 나쁜 의도를 가진 이에 의해 개인 키가 도난 당할 위험성이 있다. 이러한 문제를 해결하기 위해서 XYO Network는 ‘일시적 키 체인화’(Transient Key Chaining) 기능을 이용한다. 이 기능의 이점은 데이터에 대한 원천 체인을 조작하기가 불가능하다는 점이다. 그러나 일단 체인이 파손되면 영원한 파손 상태가 되어 유지될 수가 없기 때문에 하나의 독립적 섬이 된다.

**작업증명 체인(Proof of Origin Chain)**
일련의 연결 증인(Bound Witness) 휴리스틱 장부 엔트리를 함께 연결하는 잠정 키 체인(Transient Key Chain).

**작업증명(Proof of Work)**

작업증명은 일정한 요구기준을 충족시키는 데이터 부분으로, 생산은 어려우나(특히, 고비용 및 많은 시간 소비), 다른 것들의 의한 확인은 용이하다. 작업증명의 생산은 생산의 가능성이 낮은 랜덤한 과정이기 때문에 유효한 작업증명이 생산되기 전까지는 평균에 대한 부단한 시행 착오가 요구된다.

**Sentinel**
Sentinel은 하나의 휴리스틱 증인이다. Sentinel은 휴리스틱을 관찰하며 잠정적 장부를 생산함으로써 그 확실성과 정확성을 보증한다. Sentinel의 가장 중요한 측면은 Diviner들이 원천증명을 더함으로써 동일한 소스로부터 온 것이라는 점을 확신할 수 있는 장부를 Sentinel이 생산한다는 점이다.

**스마트 계약(smart contract)**
비트코인 이전에 아마도 1994년쯤(이 때문에 일부에서는 그가 비트코인의 전설적인 개발자인 Satoshi Nakamoto일 것이라고 추정한다)에 Nick Szabo가 만든 프로토콜. 스마트 계약의 기본적 개념은 법적 계약을 프로그램을 코드화하고, 사람이 계약을 해석 및 실행하는 대신에 분산화된 컴퓨터들로 하여금 그 조건들을 실행하도록 만드는 것이다. 스마트 계약은 금전(예: Ether) 및 계약을 동일한 개념으로 분류한다. 스마트 계약은 (컴퓨터 프로그램처럼) 결정적인 것이며 완전히 투명하고 확인이 가능한 것이기 때문에 중개자 및 브로커를 대체할 수 있는 강력한 수단으로서 작용을 한다.

**잠정 키 체인(Transient Key Chain)**
잠정 키 암호학(Transient Key Cryptography)을 사용하여 일련의 데이터 패킷을 링크하는 잠정적 키 체인.

**무신뢰성(trustless)**
시스템 내의 모든 당사자들이 정규적(canonical) 사실이 무엇인가에 대한 합의에 도달할 수 있는 특성. 파워 및 신뢰가 그 어느 개인이나 주체(예: 은행, 정부, 금융기관 등)에 집중되기 보다 네트워크의 관련 당사자(예: 개발자, 마이너, 소비자 등) 사이에 배분이 된다. 이 개념은 매우 오해하기 쉬운 일반 용어이다. 블록체인은 사실상 신뢰를 배제하지 않으며, 대신에 시스템 내의 제반 단일 행위자로부터 요구되는 신뢰의 양을 최소화하는 것이다. 이는 행위자들이 프로토콜에 의하여 정의된 규칙에 협조하도록 장려하는 경제적 게임을 통하여 시스템 내에서 여러 행위자들 간에 신뢰를 배분함으로써 이뤄진다.

**XY Oracle Network**
XYO Network.

**XYO Network**
XYO Network은 “XY Oracle Network”를 의미한다. 이 네트워크는 Sentinel, Bridge, Archivist 및 Diviner가 포함된 XYO 실행 구성요소/노드의 전체 시스템으로 구성된다. XYO Network의 주요 기능은 디지털 스마트 계약이 실제 세계의 지형 위치(geo-location) 검증을 통하여 실행될 수 있는 포털로서 기능을 하는 것이다.

**XYOMainChain**
쿼리 거래 및 Diviner로부터 수집한 데이터와 그들의 관련 원천 점수를 저장하는 XYO Network 내의 변경 불가능한 블록체인.