밴드 프로토콜(Band Protocol)

탈 중앙화 데이터 거버넌스(Decentralized Data Governance)

# 개요

탈 중앙화 애플리케이션(이하 디앱)은 기존에 존재하던 중간 관리자를, 자동으로 실행되는 스마트 컨트랙트로 대체하여 기존 비즈니스에 대한 새로운 대안을 마련할 수 있는 큰 잠재력을 가지고 있다. 기존 웹 2.0에서는, 중앙화 되어있는 기업들이 문지기 역할을 해왔고, 그들은 그들에게 가장 이익이 되는 방법으로 데이터를 관리하고 저장하고 배포해왔다. 하지만 웹 3.0, 즉 분산화 되어있는 웹에서는 데이터의 소유권이 회복되고 인터넷에 대한 권리를 다시금 유저들에게 돌려주는 패러다임 전환을 약속하였다.

그러나 탈 중앙화 애플리케이션은 신뢰가 없이도 작동하고 기능하기 위해 여전히 데이터에 의존할 필요가 있다. 스마트 컨트랙트는 현재 신뢰할 수 있는 실제 정보에 쉽게 접근할 수 있는 방법이 없기 때문에 활용 사례는 다소 제한적이다. 지금 존재하는 분산형 애플리케이션들은 중앙화 되어있는 데이터 제공자에 의존하고 있어서 단일 장애 지점을 가지고 있을 뿐만 아니라 애초에 분산화 되어야 하는 목적을 상실한 것이 현실이다.

밴드 프로토콜(이하 밴드)은 분산형 블록체인 시스템에서 사용되는 데이터의 거버넌스를 용이하게 하 개방형 프로토콜이다. 프로토콜은 데이터 처리 및 데이터 관리를 위한 표준으로서 작동한다. 이 백서에서는 밴드가 완전히 분산화된 방식으로 데이터 접근성과 데이터 신뢰성을 어떻게 해결하고자 하는지에 대해 개략적으로 설명한다. 여기에는 밴드가 데이터 무결성을 보장하기 위해 실제 데이터 및 데이터 거버넌스 메커니즘을 쉽게 사용할 수 있도록 데이터 엔드포인트를 제공하는 방법이 포함된다.

처음엔 밴드가 이더리움 위에 구축이 되지만, 이더리움 외에도 다양한 블록체인 플랫폼을 사용할 수 있으며, 궁극적으로 코스모스 네트워크와 EOS를 포함한 모든 주요 스마트 컨트랙트 플랫폼에서 지원될 것이다. 밴드의 비전은 밴드가 분산형 프로그램이나 애플리케이션이 신뢰할 수 있는 데이터에 의존하는 것을 가능하게 하는 분산형 데이터베이스가 되는 것이다.

# 컨텐츠


1. 소개
   1.1 데이터 가용성의 문제
   1.2 신뢰할 수 있는 데이터에 대한 니즈.
   1.3 스마트 컨트랙트 컴포넌트 레이어 솔루션
2. 밴드 프로토콜 개요
   2.1 분산 어플리케이션을 위한 간단한 데이터 레이어
   2.2 데이터 거버넌스 집단들의 컨소시엄
   2.3 밴드 네이티브 토큰
   2.4 프로토콜 경제 구조
3. 데이터셋 거버넌스 그룹
   3.1 데이터셋 토큰
   3.2 본딩 되어있는 토큰 발행
   3.3 거버넌스 매개변수
4. 토큰 보상을 기반으로 한 데이터 선정
   4.1 토큰 보상을 기반으로 한 데이터 소스 선정
   4.2 토큰 보상을 기반으로 한 리스트 큐레이팅
5. 추후에 문제가 될 수 있는 부분과 한계점들
   5.1 기생하는 데이터 소스들
   5.2 온 체인 투표
6. 앞으로 사용 가능한 실 사용처들
   6.1 탈 중앙 금융
   6.2 탈 중앙 상업
   6.3 아이덴티티 레이어
   6.4 게이밍, 도박, 그리고 예측 시장
   6.5 공급망 추적
   6.6 실세계 API 연동

## 7. 앞으로 달성할 목표들

### 7.1 대용량 데이터에 대한 큐레이션 서비스

### 7.2 인터체인 커뮤니케이션

### 7.3 온 체인 데이터 프라이버시

# 1. 소개

스마트 컨트랙트에서 신뢰성 확인의 필요가 없이 코드를 작동하고 실행하는 모든 블록체인 플랫폼은 외부 데이터 포인트를 사용해야 할 때 발생하는 동일한 중앙 집중화 문제를 겪는다(블록체인 외부에 있는 곳에서 데이터를 가져와야 하기 때문이다). 거의 대부분의 분산형 시스템은 자산 가격, 체인 간 통신, 실제 이벤트 및 외부 웹 API 상호 작용과 같은 외부 데이터 공급을 필요로 하는 기본적인 작업과 계산을 수행할 수 있는 능력들에 의존할 수 밖에 없다.

## 1.1 데이터 가용성의 문제

스마트 컨트랙트 자체로는 데이터에 액세스할 수 없다 – 분산형 애플리케이션이 외부의 데이터를 받기 위한 간단하고 직관적인 쿼리 인터페이스가 없기 때문이다. 분산형 애플리케이션이 실제 외부 데이터 입력을 단순한 함수 호출(Function Call)에 접속시킬 수 있을 때까지, 기술의 채택적인 부분과 개발자들이 새로운 애플리케이션을 실현하는 부분에 있어서 상당한 장벽이 있을 것이다.

블록체인 스마트 컨트랙트를 위한 기존 데이터 가용성 솔루션은 매우 중요한 중앙 실패 지점들에 의존하거나 비동기식 상호작용의 영향을 받으므로 지연이 발생하고 스마트 컨트랙트 논리가 복잡해진다.

## 1.2 신뢰할 수 있는 데이터에 대한 니즈

분권형 시스템의 무허가성(Permissionless)적인 환경에서는 중요한 데이터 출처를 공격하려는 경제적 동기와 유혹이 상당할 수 있다. 높은 품질과 신뢰성 있는 데이터 제공을 보장하기 위한 강력한 인센티브 메커니즘이 없다면, 분산형 애플리케이션은 이러한 보안 위험을 지속적으로 겪을 것이다.

예를 들어, 오라클이 제공하는 외부 데이터 소스가 스마트 컨트랙트에 대한 데이터 입력을 제어하는 경우, 그것은 그 스마트 컨트랙트가 하는 응답과 행동을 결정할 수 있는 유일한 권한을 갖는다. 데이터 소스는 기본적으로 스마트 컨트랙트를 제어하는데, 오라클 그 자체가 손상되면 스마트 컨트랙트와 그것에 의존하는 모든 시스템도 마찬가지가 되어버리기 때문에 블록체인들의 보안 및 검열 저항 특성에 심각한 취약점을 만들게 된다.

분산형 애플리케이션들이 점점 더 정교해지고 유용해지려면, 그들은 분산형 애플리케이션을 위해 기존 중앙화 되어있는 DB에서 사용되는 동등한 도구를 사용하고 복제할 수 있어야 한다. 이렇게만 된다면, 개발자들은 사람들의 삶을 개선할 수 있는 매우 유용한 분산형 어플리케이션들을 만들 수 있을 것이다.

## 1.3 스마트 컨트랙트 컴포넌트 레이어 솔루션

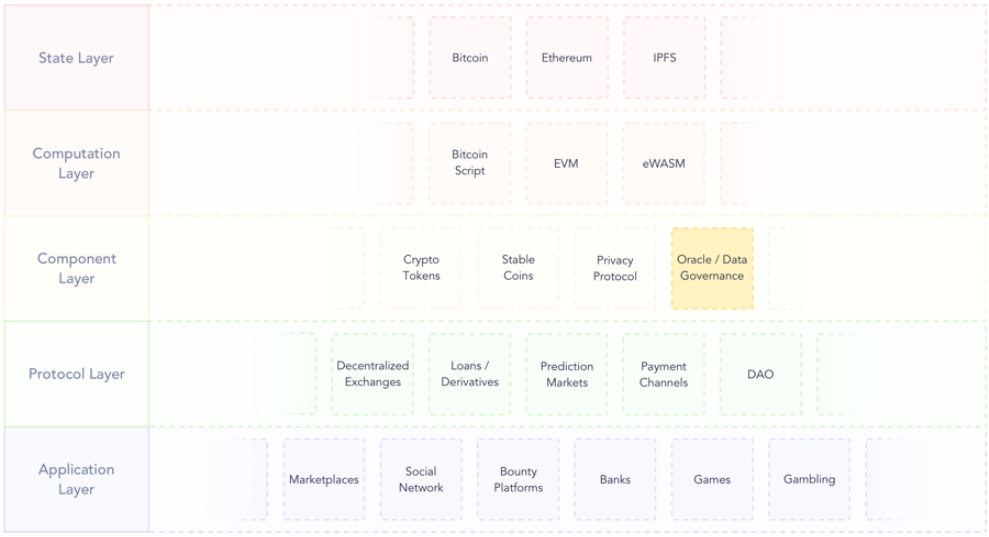


**그림1**: Web 3.0 기술 스택 개요이다. 밴드 프로토콜은 여기에서 Component Layer에 속하며, 다른 탈 중앙화 프로토콜에 믿을 수 있는 데이터를 제공하는 역할을 한다.

그림 1에서 알 수 있듯이, 밴드 프로토콜은 Web 3.0 기술 스택에서, 블록체인들에 대한 데이터 가용성 및 신뢰성 문제를 해결하는 데이터들을 관리하기 위한 Web 3.0 컴포넌트 레이어 솔루션이다. 밴드를 사용하는 분산 어플리케이션들은 블록체인 외부에 있는 오라클들이 아닌 밴드의 퍼블릭 스마트 컨트랙트 데이터 포인트를 통해 데이터를 소비한다. 밴드의 데이터 피드는 커뮤니티에 의해 선정되는 데이터 소스로, 분산 어플리케이션 사용자와 개발자가 의도한 목적을 달성하기 위해 필요한 데이터들이 신뢰할 수 있는지에 대해서 스스로 관리하고 선정하는 것을 가능하게 하는 프레임워크를 제공한다.

밴드는 모든 분산 어플리케이션들이 활용할 수 있는 신뢰 가능한 데이터들의 광범위한 채택과 통합을 위해 사회적으로 확장 가능한 방법을 데이터의 커뮤니티 관리를 위한 표준 프레임워크를 통해 만들어낼 수 있다.

밴드 데이터 인터페이스들은 소스와 애플리케이션에 대해 불가지론적이며, 데이터를 통제하고 규제하는 커뮤니티가 적합하다고 판단한다면, 어떤 목적에도 적용할 수 있다. 소스는 평균값, 중앙값 또는 다수 값을 사용하여 집계할 수 있으며 중앙화 되어있는 외부 피드 또는 체인상에 있는 데이터 집계기와 같은 여러 소스에서 조달해올 수 있다. 사용 사례의 예:

**자산 가격 피드**는 크립토/크립토 가격(ETH/BTC 같은), 크립토/법정화폐 가격, 그리고 전통적으로 사용되었던 증권 및 상품 가격을 포함한다. 분산형 금융 애플리케이션은 분산형 P2P 대출, 스테이블 코인, 파생상품 거래 등을 구축하기 위해 이러한 외부 가격 공급에 의존한다.

**실제 일어나는 이벤트 피드** 에는 스포츠 이벤트, IoT 데이터 출력, 실제 결제 등이 포함된다. 많은 스마트 컨트랙트들은 거래들을 처리하기 위해 이 정보들에 의존할 필요가 있다. 예를 들어, 예측 시장은 토큰 홀더들에게 의존하지 않아도 우리가 만들어내는 스포츠 이벤트 피드를 사용하여 쉽게 구축할 수 있다.

**신원 데이터는** 인증된 상태, 신용 점수, 학력 및 커리어 같은 정보를 포함한다. 탈 중앙 거래소와 시장은 그러한 데이터에 의존할 필요가 있는 잠재적인 분산 어플리케이션 중 하나이다.

**위치 데이터는** GPS상 기록되는 위치를 포함한다. 지도나 위치 정보를 활용해야 하는 분산형 애플리케이션은 이러한 위치 데이터에 의존할 수 있다.

가장 중요한 것은, 밴드는 데이터가 어떻게 처리되는지를 직접 정의하지 않고, 오히려 그것이 어떻게 사용되고 선정될지를 밴드 커뮤니티가 집단적으로 결정할 수 있는 수단을 제공한다는 점이다. 데이터가 어떻게 관리되고 처리되어야 하는지에 대해서, 밴드는 어떠한 가정도 하지 않는다.

이러한 권리들은 분산 애플리케이션에서 해당 데이터를 사용하고자 하는 커뮤니티 구성원의 손에 전적으로 놓이게 되며, 분산형 애플리케이션을 사용하는데 있어서 신뢰할 수 있는 데이터 소스를 만드는 공통의 목표에 부합하는 최적의 인센티브 참여자를 만들어낸다.

진정으로 탈 중앙화 되어있는 세계를 구현하고자 하는 것 외에도, 밴드는 민간 기업들이 사적인 데이터를 교류할 수 있는 생태계를 구축하고 있기도 하다. 많은 데이터들은 굉장히 민감할 수 있기 때문에 이해당사자들 간에 데이터를 자유롭고 안전하게 공유하기가 어렵다. 밴드는 신원 및 신용 점수와 같은 중요하고 유용한 정보를 포함하는 월드 데이터베이스를 만들 수 있도록 그러한 개인 정보 공유를 포함하는 웹 3.0 지원을 확장한다.

## 2. 밴드 프로토콜 개요

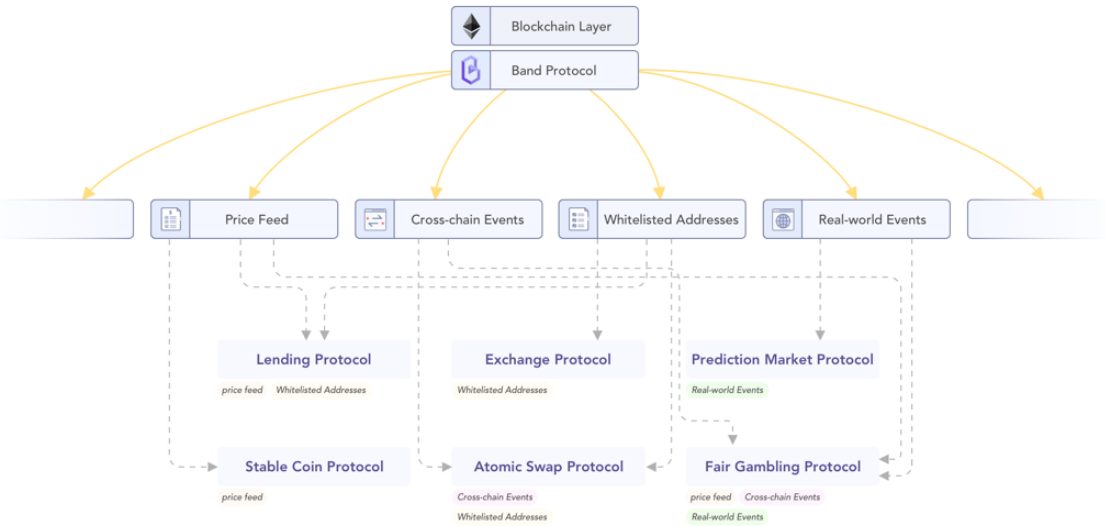


**그림2:** 밴드 프로토콜을 개략적으로 설명한 것이다. 커뮤니티가 선정하는 데이터 셋들이 블록체인 내에서 공존하는 구조이다. 그리고 이 데이터 셋들은 여러 탈 중앙 애플리케이션에 의해서 사용된다.

밴드 프로토콜(이하 밴드)의 주요 역할은 분산된 애플리케이션과 실제 오프체인 데이터의 갭 차이를 메우는 동시에 경제적 인센티브를 통해 정확하고 신뢰할 수 있는 데이터를 보장하는 것이다. 밴드 프로토콜은 처음에 이더리움 네트워크에 구축될 것이지만, 밴드의 사용은 이더리움 인프라로 제한되지 않는다. 이 프로토콜이 점점 더 널리 사용됨에 따라서 이더리움 외에 존재하는 다양하고 혁신적인 스마트 컨트랙트 플랫폼을 지원하고 새로운 세대의 분산형 애플리케이션을 발전시킬 것이다.

### 2.1 분산 어플리케이션을 위한 간단한 데이터 레이어

체인링크 또는 오라클라이즈와 같은 기존 데이터 공급자 서비스들은 스마트 컨트랙트와 데이터 계층 간의 비동기적 상호작용을 요구한다. 이러한 방식은 스마트 컨트랙트 구현을 복잡하게 할 뿐만 아니라 블록체인 트랜잭션을 두 건이나 순차적으로 실행하고 확인해야 하므로 상당한 지연을 야기한다. 데이터를 얻기 위해, 스마트 컨트랙트는 그림 3에 표시된 흐름을 따른다.

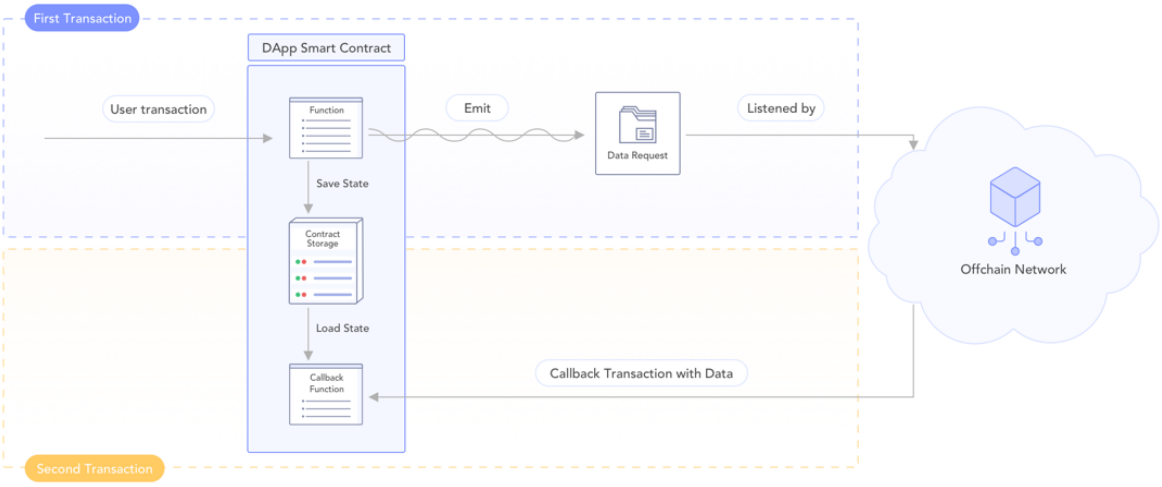


**그림3**: 스마트 컨트랙트와 기존에 존재하는 오라클 네트워크가 소통(상호작용) 하는 것을 보여주고 있다. 그림에서 나타나듯 정보를 획득하기 위해선 두 번의 트랜잭션이 필요하다.

1. 컨트랙트는 현재의 거래 상태를 컨트랙트의 보관소에 저장한다.
2. 컨트랙트는 데이터 조회를 요청하는 이벤트를 내보내고 현재 거래를 중지한다.
3. 오프체인 네트워크는 충분한 트랜잭션 확인이 이루어질 때까지 기다린다.
4. 오프체인 네트워크는 제공된 쿼리 결과를 가진 콜백 트랜잭션을 호출한다.
5. 컨트랙트는 거래를 검증하고 상태를 복구하며 실행을 계속한다.

밴드는 패러다임을 바꾸고 분권형 애플리케이션을 위한 직관적인 쿼리 인터페이스를 제공하여 스마트 컨트랙트에 대한 단순한 함수 호출로(Function Call)서 실제 데이터를 수신한다. 데이터 공급자는 블록 체인에 데이터를 입력하고 큐레이팅하여 탈 중앙 어플리케이션에서 동시에 소비할 수 있도록 하는 역할을 담당한다

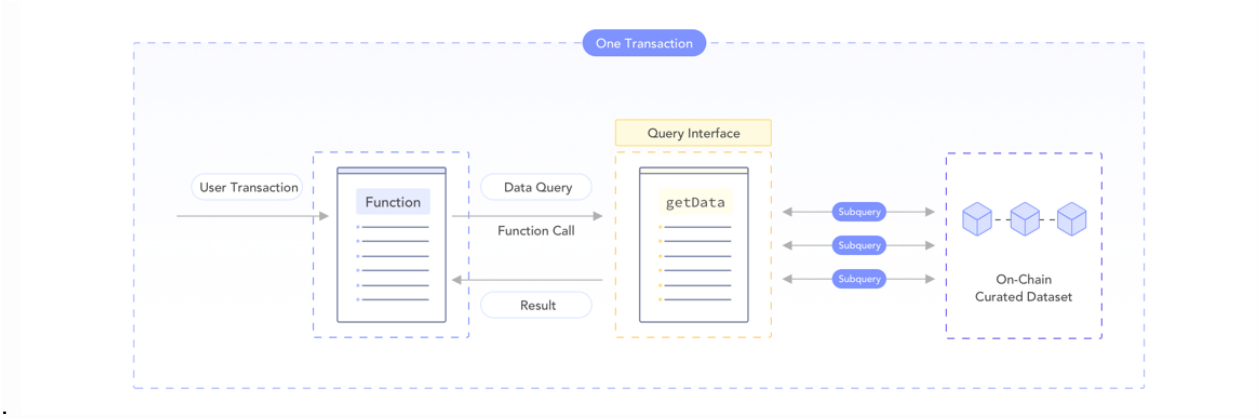


**그림4**: 이 그림은 스마트 컨트랙트와 밴드가 소통(상호작용) 하는 모습을 보여준다. 모든 요청이 하나의 트랜잭션에서 발생한다.

그림 4에서 알 수 있듯이, 결과적으로 밴드에 대한 데이터를 조회하는 것은 구현이 간단할 뿐만 아니라 적은 가스 비용만 발생시킨다. 또한 기존 솔루션에서는 모든 애플리케이션이 중복된 데이터 쿼리를 수행해야 하는 반면, 밴드에서는 데이터를 여러 당사자가 쉽게 사용할 수 있기 때문에 동일한 데이터셋을 사용하더라도 더 많은 애플리케이션으로 확장할 수 있다.

### 2.2. 데이터 거버넌스 집단들의 컨소시엄.

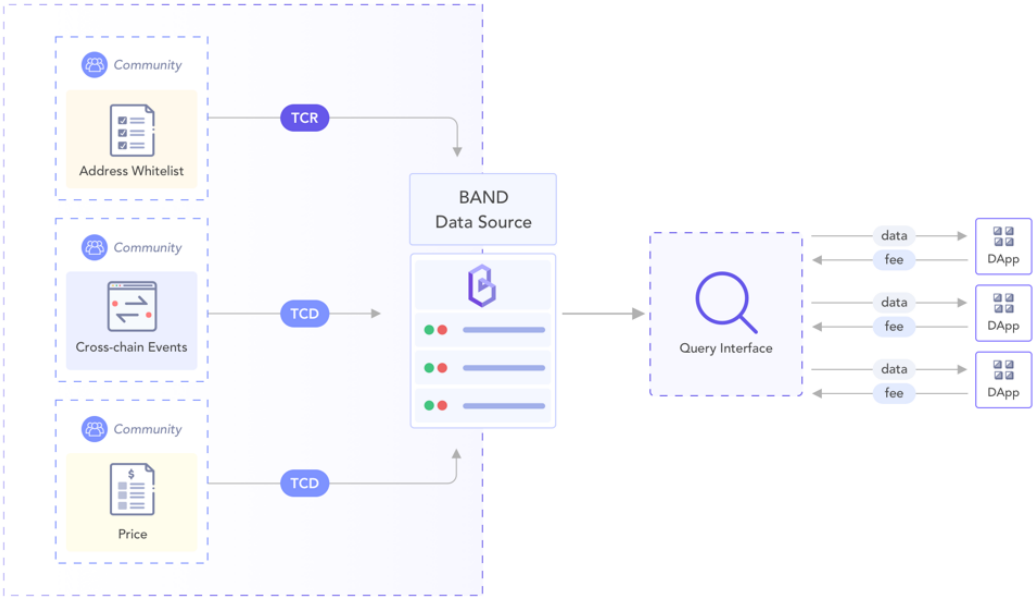


**그림5**: 밴드 프로토콜 구조에 대한 요약이다. 다양한 종류의 커뮤니티가 모여서 데이터를 제공해주는 것을 볼 수 있다.

밴드 내부의 데이터셋은 여러 데이터셋 거버넌스 그룹으로 나뉘는데, 각각 고유한 "데이터셋" 토큰을 활용하여 토큰 기반 큐레이션 리스트 제공 또는 토큰 기반 큐레이팅 데이터소스 제공 같은 메커니즘을 통해 데이터셋을 보유, 큐레이션 및 관리한다. 데이터 거버넌스 그룹은 독립적이며 동일한 토큰을 공유하지

않지만, 모두 본딩 커브 작동 방식을 통한 밴드 네이티브 토큰에 의해 보안된다. 이는 모든 유형의 큐레이션에 하나의 토큰을 독점적으로 사용하는 DIRT 프로토콜과 같은 데이터 큐레이션 프로토콜과는 근본적으로 다르다. 그룹당 하나의 토큰을 갖는 것은 두 가지 장점이 있다:

**토큰 보유자는 좋은 데이터를 선정하는 것에 대한 직접적인 동기를 가지고 있다**. 토큰의 가치는 이 그룹 내에서 관리되는 특정 데이터셋에 직접 연결되기 때문에, 좋은 데이터를 큐레이팅하면 토큰 보유자에게만 이익이 된다. 그렇지 않으면 토큰이 하나만 있는 경우, 특정 데이터셋에 기여하는 것이 얼마나 큰 가치 증가를 가져올지 명확하지 않으며, 따라서 데이터의 보안 및 신뢰성에 대한 모델은 더 취약해질 것이다. 이것은 쉽게 공유지의 비극과 낮은 투표 결과로 이어질 수 있다.

**토큰 소유자를 매수하는 행위가 더 어려워진다**. 반대로 토큰이 하나 있는 경우, 하나의 잘못된 데이터셋이 있다고 해서 토큰 가치의 큰 하락을 야기하지 않을 수는 있다. 따라서 토큰이 하나 있는 경우에서 토큰 소유자가 데이터셋을 조작하도록 매수될 가능성은 상대적으로 높다. 왜냐하면 데이터셋을 한 번 조작하더라도 토큰 가치의 하락에 크게 반영되지 않을 수 있기 때문이다. 반면에 데이터셋마다 토큰의 종류도 나눠서 관리하게 된다면, 토큰 홀더들이 데이터셋을 조작할 때 토큰의 가치가 크게 하락할 수 있음을 감수해야 하므로, 데이터셋마다 토큰을 두는 모델을 사용했을 때 토큰 소유자를 매수하는 행위가 더 어려워진다.

### 2.3 밴드 네이티브 토큰

밴드 프로토콜 자체 토큰인 밴드 토큰(심볼:BAND)을 중심으로 구축된다. 밴드는 처음에 이더리움 블록체인에서 ERC-20[16] 토큰으로 출시된다. 블록체인 플랫폼들이 더 다양해짐에 따라서 지원되는 블록체인 간에 토큰을 교환할 수 있는 기능을 갖춘 BAND도 여러 플랫폼에서 자유롭게 사용할 수 있게 될 것이다. 토큰은 프로토콜 생태계에 4가지 주요 유틸리티를 제공한다.

- **데이터 거버넌스 그룹에 유동성을 제공하고 토큰 값을 보장한다.** 밴드 토큰은 데이터셋 토큰을 발행하는데 담보로 사용된다. 데이터 거버넌스 그룹의 본딩곡선 스마트 컨트랙트에 BAND를 보내면 누구나 데이터셋 토큰을 구입할 수 있다. 반대로 데이터셋 토큰은 본딩 곡선으로 판매되어 BAND를 반환 받을 수 있다. BAND는 데이터셋 토큰들 사이에 전반적인 유동성을 제공하는 네트워크 토큰 역할을 하므로 누구나 즉각적으로 데이터셋 토큰을 구입, 판매 또는 교환할 수 있다.
- **데이터셋들의 가치를 보존해준다**. 데이터셋 토큰을 발행하기 위해선, 밴드 토큰을 담보로 해야 한다. 따라서 데이터셋 토큰 수요가 증가함에 따라 BAND의 수요도 증가할 것이다. 이것은 두 개의 효과가 있다. 첫째, BAND의 가격과 토큰 값이 증가하여 모든 데이터 거버넌스 그룹에 걸쳐 그 가치를 효과적으로 반영하게 될 것이다. 둘째, 데이터셋 토큰이 BAND를 기준으로 평가되므

로, BAND의 가격 상승으로 모든 데이터 거버넌스 그룹에 대한 보안이 강화된다.

- **향후 프로토콜 업그레이드를 위한 거버넌스.** ZRX 토큰이나 0x와 같이, BAND는 향후 프로토콜 개선을 제안하고 투표하는 데 사용될 수 있다. BAND Protocol이 구축되면 업그레이드가 시스템의 보안과 사용성에 영향을 미칠 수 있기 때문에 내부 로직을 쉽게 변경할 수 없다.

  BAND Token은 모든 데이터 거버넌스 그룹의 이해관계자들이 투표 계획 변경이나 새로운 큐레이션 방법 추가와 같은 향후 분산된 업그레이드 및 거버넌스 문제에 투표하는 거버넌스 토큰 역할을 할 것이다.

- **TCR을 통해 데이터셋 품질 관리** 처음에는 첫 번째 데이터셋은 엄격하게 큐레이팅 할 것이다. 그러나, 밴드가 탈 중앙화 됨에 따라 데이터셋을 만들고 큐레이팅하는 것은 허가가 없이도 진행이 될 것이다. BAND 토큰 소유자는 생태계 내부의 데이터셋의 품질을 관리하기 위해 정해진 기준에 따라 정당한 데이터셋의 규제된 레지스트리를 함께 유지한다. 악의를 가진 유저들로부터 TCR을 보호하는 투표권 자로 밴드 토큰이 사용될 것이다.

### 2.4 프로토콜 경제구조

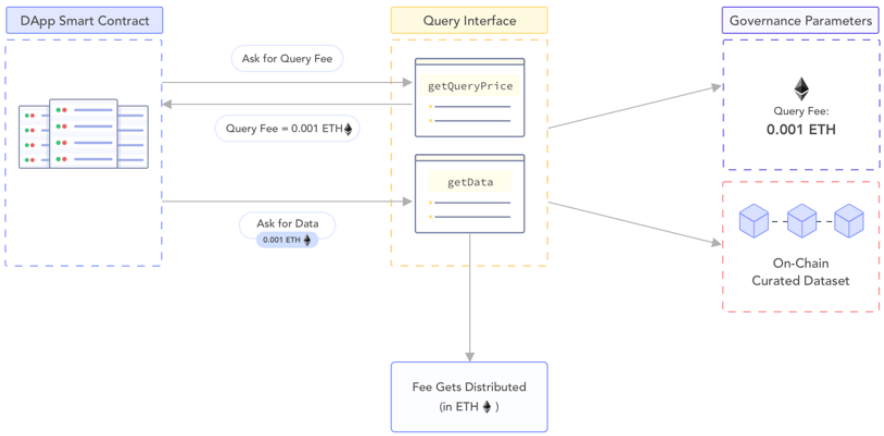


**그림6**: 디앱들은 기존에 표준화 되어있는 쿼리 인터페이스를 통해서 정보 요청 비용을 요청할 수 있다. 그러면 해당 요청은 데이터셋의 거버넌스 매개변수 컨트랙트로 넘어가게 된다.

프로토콜은 적절한 경제적 인센티브 없이는 살아남을 수 없다. 밴드는 데이터 제공자의 비용을 부담하고 정직한 데이터 큐레이션을 장려하기 위해 쿼리 수수료에 의존한다. 스마트 컨트랙트에서 데이터 조회 기능 호출을 할 때마다, 해당 블록체인이 사용하는 화폐로(이더리움의 경우 ETH)쿼리에 대한 수수료를 지불해야 한다. 지불된 쿼리 수수료는 데이터 거버넌스 그룹의 거버넌스 매개변수에 의해 설정된 수수료 일정에 따라 데이터셋의 데이터 공급자와 토큰 스테이커 간에 분할된다.

모든 디앱이 데이터셋 토큰 또는 밴드 토큰을 보유하고 사용할 의사가 있다고 가정하는 것은 비합리적이기 때문에 각각의 블록체인마다 유통되는 전용 통화들을 수락하는 결정은 주로 온 보드 및 통합 프로세스를 단순화하기 위한 것이다. 구현하는 과정 중에서 밴드는 Uniswap[20]과 같은 분산형 교환 프로토콜을 활용하여 즉시 플랫폼 전용 통화를 밴드 토큰으로 변환한 다음, 동일한 거래에서 본딩 곡선을 통해 데이터셋 토큰으로 변환된다. 따라서, 비록 앱이 고유 통화로 지불하지만, 데이터 공급자와 토큰 스테이커는 여전히 데이터셋 토큰으로 수익 몫을 받는다. 이 과정을 통해 더 많은 BAND가 본딩 곡선에 고정되고 데이터셋 토큰의 공급이 증가하여 두 토큰의 가격이 상승한다.

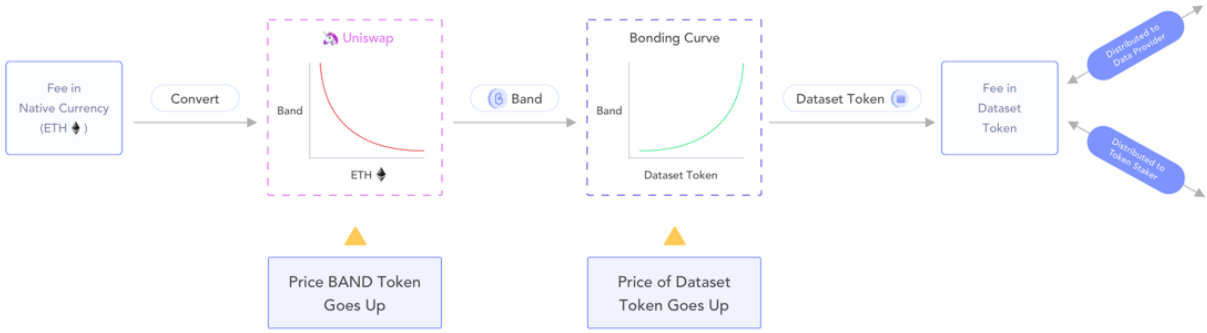


**그림7**: 디앱이 속한 네이티브 토큰(ERC20 기준으론 ETH)로 정보 요청 비용을 지불하면 본딩 커브와 유니스왑을 통해서 데이터셋 토큰으로 교환할 수 있다.

TCR 같은 일부 교육 방법이 참가자들에게 경제적 이익을 주기 위해 반드시 수익이 필요한 것은 아니라는 점에 유의할 필요가 있다. 이 경우 데이터셋 커뮤니티는 쿼리에 대한 수수료를 0으로 설정하기로 집단적으로 결정할 수 있다.

## 3. 데이터셋 거버넌스 그룹

데이터셋 데이터 거버넌스 그룹은 가장 기본적인 밴드 프로토콜 단위다. 밴드는 여러 데이터 그룹으로 구성되어 있으며, 각각 고유한 토큰을 가지고 있다. 데이터셋 토큰 소유자는 커뮤니티 거버넌스 및 데이터 큐레이션에 참여한다. 그 대가로, 그들은 데이터를 소비하는 것으로부터 수집된 수수료를 받고, 토큰 가치 상승으로부터 이익을 얻는다.

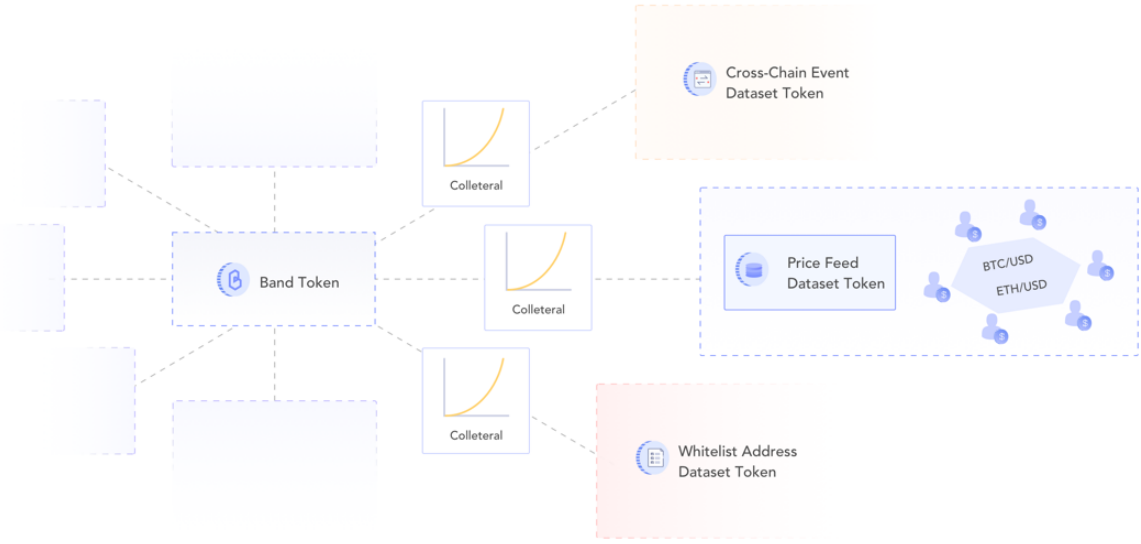


**그림8:** 밴드 프로토콜 내에서 데이터 고버넌스 그룹은 각자만의 거버넌스를 담당할 데이터셋 토큰을 발행한다. 하지만 모든 토큰들은 본드를 담보와 해야한다. 이러한 담보 시스템은 데이터셋 토큰이 가치 없이 허공에서 발행된 것이 아니고 항상 경제적 가치를 가지고 있음을 나타낸다.

### 3.1 데이터셋 토큰

Dataset Token은 ERC-20 [16] 토큰으로, 생성 시 거버넌스 그룹과 함께 배포된다. 토큰 공급은 데이터셋 토큰을 발행하고 소각할 수 있는 유일한 권한을 가진 본딩 곡선 계약에 의해 제어된다. 데이터셋 토큰은 토큰 인센티브를 통한 데이터 선출 방법을 통해 데이터를 선출하고 조절하는 데 사용된다. 밴드는 사용자 경험을 개선하기 위해 ERC-20 계약에 3가지 기능을 추가한다:

• Transfer-and-Call은 단일 트랜잭션 내에서 계약에 의해 토큰을 수신하고 처리할 수 있도록 하는 반면, 기존 네트워크에선 두 가지의 독립적인 트랜잭션이 필요했었다.

• Minimi의 Balance Snapshot을 통해 계약에서 모든 계정의 과거 잔액을 조회할 수 있다. 이것은 주로 투표권을 결정하고 이중 투표를 없애는 데 유용하다.

• 이전 동결로 인가된 계약은 토큰 전송을 비활성화할 수 있다. 하지만 그래도 토큰을 스테이킹 한 사람들이 토큰에 대한 권리는 허용된다. 이러한 기능은 주로 스테이킹 메커니즘을 구현하는 데 유용하다.

### 3.2 본딩 토큰 발행

데이터셋 토큰 발행은 데이터 거버넌스 그룹의 본딩 커브에 의해 제어된다. 본딩 커브의 개념은 원래 Simon de la Rouviere에 의해 제안되었다. 본딩 커브는 (1) 데이터셋 토큰의 가격이 공급량이 증가함에 따라 항상 상승하고 (2) 토큰 보유자는 데이터셋 토큰의 판매를 통해 "퇴장"할 수 있는 선택권을 갖는다. 따라서 데이터셋 토큰이 항상 유동적이고 어떠한 상황에서도 유용하게 유지되어 성공적인 운영에 중요한

인센티브 메커니즘을 보호한다.

### 3.2.1 가치 공급 공식

이 볼록하고 단조롭게 증가하는 그래프 공식은 데이터셋 토큰의 총 공급량과 그 총 가치 사이의 관계를 담보된 밴드 토큰의 관점에서 설명한다. 즉, 현재 공급 s를 감안하면 V(s)는 본딩 곡선 계약에서 담보된 총 BAND 수를 산출한다. 이 가치-공급 기능을 정의하면 특정 공급가치의 가치-공급 방정식의 파생상품으로 주어진 총공급 P(s)에서 데이터셋 토큰의 현물가를 쉽게 도출할 수 있다.

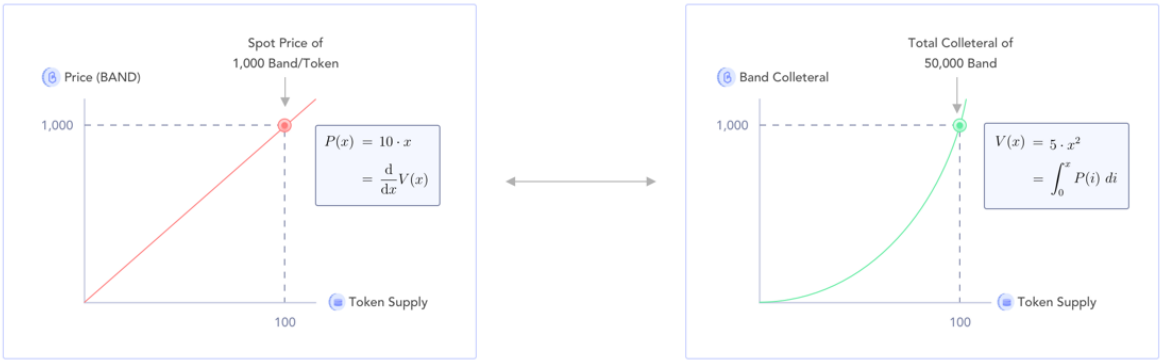


**그림9**: 본딩 커브의 예시로. 토큰 가격을 1차 방정식(선형 그래프)으로 나타낸 것과 담보가치를 2차 방정식으로 나타낸 것이다. 이 두 개의 그래프가 나타내는 바는 사실상 같다.

어떤 사람이 데이터셋 토큰을 살 때마다, 구매자는 본딩 곡선 계약으로 BAND 토큰을 보낸다. 계약은 조정된 데이터셋 토큰의 공급을 계산하고 구매자에게 토큰을 발행해줌으로써 추가적인 공급을 제공한다. 데이터셋 토큰을 판매하기로 결정할 땐 위에서 말한 것과 정 반대의 절차가 이루어진다.

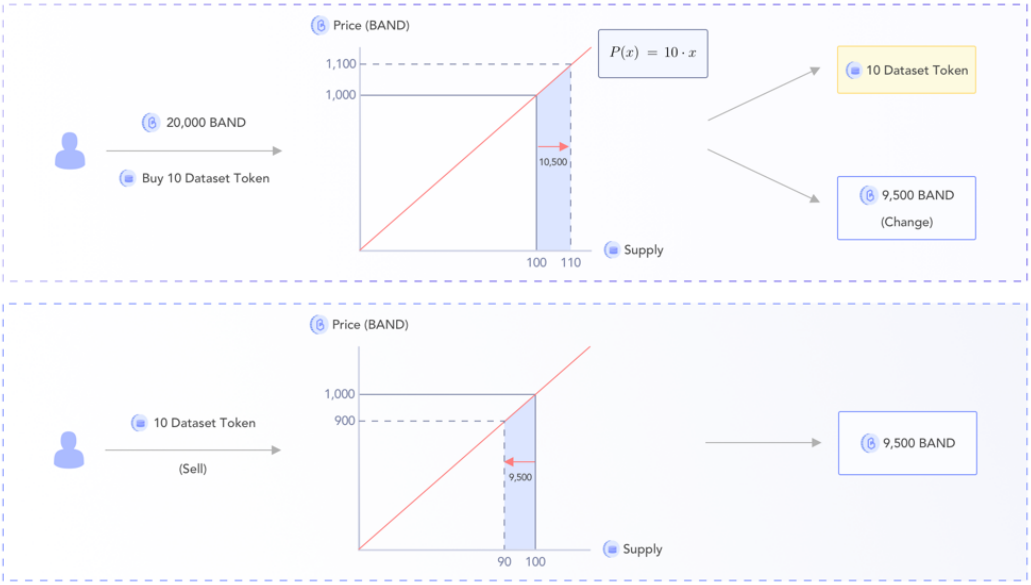


**그림10:** 실제로 유저가 밴드를 팔아서 데이터셋 토큰을 사고 파는 것을 형상화 한 것이다.

선행매매에 대항하기 위해, 본딩 커브 계약은 사용자들이 기존의 한계 주문을 시뮬레이션 하면서 가격 제한을 지정할 수 있도록 한다. 거래는 제한 조건을 위반하여 사용자가 잘못된 주문을 실행하지 못하게 할 경우 되돌릴 수 있다.

### 3.2.2 방정식 라이브러리

Band Protocol은 Solidity에서 임의적인 수학적 공식을 구성하기 위한 일반적인 스마트 컨트랙트 라이브러리[14]를 제공한다(자세한 내용은 비디오 설명 참조). 현재 공급 및 숫자 상수에 대한 공통의 일절, 이항 및 임시 작업의 재귀적 적용 측면에서 설명할 수 있는 표현식은 인코딩 할 수 있다.

### 3.3.3 유동성 스프레드

유동성 스프레드는 데이터셋 토큰의 매입가격과 판매가격의 차이를 통제한다. 매개 변수는 bonding:liquidity spread. 로 거버넌스 매개변수를 통해 설정할 수 있다. 유동성 확산이 심하면 악의적인 유저들이 전방위 공격을 감행하기가 더욱 어려워진다. 그러나, 높은 스프레드는 또한 토큰 소유자가 데이터셋 토큰을 현금으로 바꿀 때 더 적은 이득을 취하는 것으로 이어진다

### 3.3 거버넌스 매개변수

데이터 거버넌스 그룹 내부의 거버넌스 매개변수는 그룹의 다른 스마트 컨트랙트들이 어떻게 그들의 계약을 수행하는지를 지시한다. 형식적으로 거버넌스 매개변수는 32바이트 키와 32바이트 값 쌍을 포함한다. 32바이트 값은 키에 따라 정수, 백분율 값, 블록체인 주소 또는 IPFS 해시로 해석할 수 있다. 예를 들어, 파라미터 Bonding:liquidity-spread맵은 본딩 곡선 구매와 현물 판매 사이의 스프레드 비율을 제어하는

정수로 확산된다. 데이터셋 토큰 보유자는 다음 프로세스를 통해 매개변수의 변경을 수행할 수 있다:

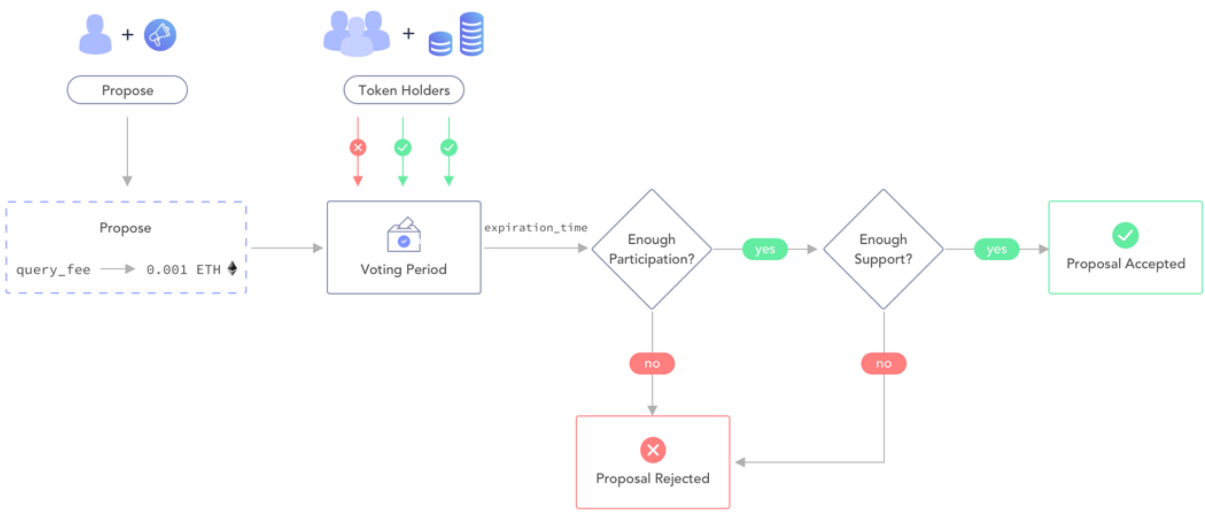


**그림11**: 매개변수 변경 요청을 하는 과정을 형상화 한 것이다.

1. 데이터셋 토큰 보유자는 거버넌스 계약에 "제안" 거래를 전송하여 하나 이상의 매개변수에 대한 변경을 제안하여 제안서를 작성한다. 일단 제안이 만들어지면, 제안은 params:expiration_time 동안 공개된다.
2. 제안서가 공개되어 있는 동안 토큰 소유자는 제안서에 대한 승인이나 거절에 투표할 수 있다.
3. 투표 기간이 종료된 후 (1) 모든 토큰의 Params: Min_paricipation_pct % 가 투표에 참여했고 (2) params: supportrequired_pct %의 참여된 토큰들이 승인에 투표하면, 요구하면 제안이 승인되고 변경 사항이 적용된다.
4. 또한 만장일치 매개변수 변경을 용이하게 하기 위해, 제안서가 모든 토큰의 params:support_required-pct 이상일 경우, 제안서 만료 전에 해결될 수 있다.

본딩 커브 및 거버넌스 계약의 초기 매개변수는 데이터 거버넌스 그룹이 작성하는 동안 설정될 것이다. 지배구조 계약 자체의 3가지 매개 변수 역시 동일한 제안 투표 과정을 통해 변경할 수 있다는 점에 유의해야 한다.

## 4. 토큰 인센티브를 기반으로 한 데이터 선정

첫 번째 메인넷 출시 동안, 밴드는 데이터 거버넌스 그룹이 데이터 셋 토큰을 활용하여 데이터를 집단적으로 통제하고 큐레이팅 할 수 있는 두 가지 기본 모델을 제공한다. 우리는 더 많은 큐레이션 모델에 대

해 적극적으로 연구하고 있으며, 향후 프로토콜 업그레이드 시 이를 프로토콜에 추가할 계획이다. 데이터 거버넌스 그룹은 반드시 하나의 큐레이션 방법만을 사용하도록 제한되는 것은 아니며, 동일한 데이터 거버넌스 그룹 내에서는 여러 데이터셋에서 동일한 데이터셋 토큰을 사용할 수 있다. 이 섹션에서는 주로 기술적 토큰 메커니즘에 대해 논한다. 더 구체적인 예는 잠재적으로 밴드가 사용될 수 있는 사례 부분에서 다룰 것이다.

### 4.1 토큰 보상을 기반으로 한 데이터 소스 선정.

TCD라 불리는 토큰 보상을 기반으로 한 데이터 소스 선정 방법은 객관적인 데이터들을 큐레이팅 하는 방법이다. 어쩌면 많은 사람들이 알고 있는 Delegated Proof-of-Stake 합의 알고리즘과 비슷하다고 생각될 수 있다. 토큰을 가지고 있는 홀더들은 자신의 토큰을 원하는 후보의 이름에 스테이킹하고 자신들의 대변해줄 수 있는 데이터 제공자들을 선출한다. 데이터 제공자들은 특정 조건하에서 데이터를 제공해줄 수 있는 권한을 갖게 되며 데이터 요청으로부터 발생하는 수수료를 일부 획득할 수 있게 된다.

- **데이터 제공자:** 데이터셋에 데이터를 제공해줄 권한을 얻기 위해 데이터 제공자로 지원한다. 그리고 홀더들이 가장 많이 스테이킹한 상위 후보들은 데이터를 제공할 수 있는 권한을 얻게 된다. 이들은 데이터 요청으로부터 발생하는 수수료의 과반 이상을 이들이 제공하는 서비스에 대한 대가로 얻게 된다.
- **토큰 홀더:** 자신이 신뢰하는 데이터 제공자의 이름에 자신들의 토큰을 스테이킹한다. 이들은 물론 데이터 제공자가 받아가는 수수료보다 적은 수수료를 획득하게 된다.

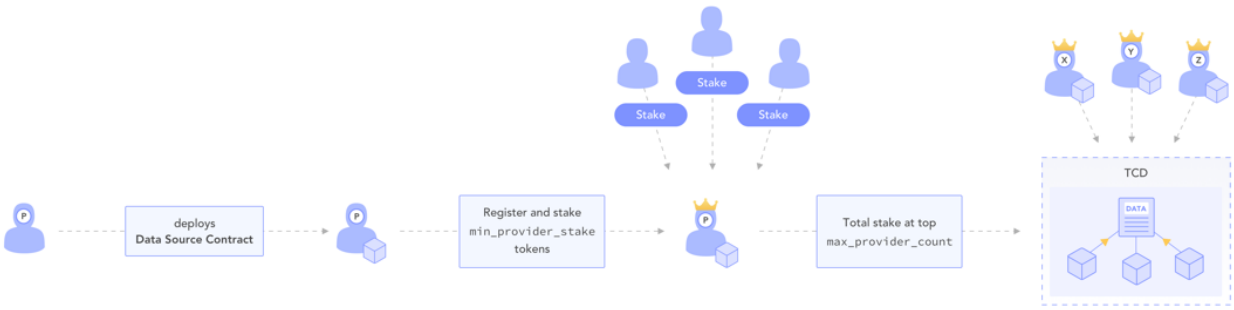


**그림 12:** TCD 제공자가 어떻게 선정되는지를 보여주는 플로우 차트이다.

#### 4.1.1 TCD는 어떤 방식으로 작동을 하는가?

- 데이터 제공자가 되고 싶은 토큰 홀더들은 데이터 소스 계약을 구축한다. 그 후 데이터 제공자 후보로 등록하기 위해서 min_provider_stake 정도의 토큰을 스테이킹한다.
- 다른 토큰 홀더들은 자신이 신뢰하는 데이터 제공자에게 토큰을 스테키이킹한다. Max_provider_count(최대 수량의 스테이킹 토큰)을 받은 상위 후보들은 Active Data Provider가 된다.
- 데이터 요청이 들어올 때 마다, TCD 계약은 활성화 되어있는 데이터 제공자의 모든 데이터 소스

들에 대한 하위개념의 쿼리를 발행한다. 쿼리 결과는 데이터 쿼리의 최종 결과가 되도록 집계된다.

- 탈 중앙 어플리케이션은 데이터 요청에 대한 수수료를 ETH(이더리움 플랫폼에 한해서)를 지불하고, 그것은 커뮤니티 토큰으로 전환이 된다. Owner_revenue_pct 부분에 해당되는 수익은 활동하고 있는 데이터 제공자에게 지급이 되며, 나머지는 커뮤니티 구성원들에게 할당된다.

- 토큰 홀더들은 언제든지 자신의 스테이킹 되어있는 토큰을 인출할 수 있으며, 데이터 제공을 통해서 발생한 수익을 포함한 양의 토큰을 다시 함께 스테이킹 할 수 있다. 토큰 인출이 발생하게 되면 데이터 제공자 리스트 순위는 다시 계산이 된다.

- 데이터 제공자 역시 자신의 스테이킹 되어있는 토큰을 인출할 수 있다. 하지만, TCD 스마트 컨트랙트에 그들의 의도를 먼저 알림으로써 토큰 홀더들이 제공자보다 앞서서 자신들의 토큰을 인출할 수 있어야 한다. 이러한 방식은 데이터 제공자가 악의적으로 활동을 하였을 때 발생할 수 있다.

#### 4.1.2. 쿼리 인터페이스

외부 데이터 소비자는 현재 활동하는 데이터 공급자 간에 데이터 포인트를 집계하는 쿼리 인터페이스를 사용하여 데이터를 쿼리한다. 데이터 포인트는 데이터 제공자의 2/3 이상이 그러한 데이터를 제공하는 경우에만 유효하다. 이는 시스템이 악의적인 데이터 제공자의 3분의 1까지 허용할 수 있음을 보장한다. 프로토콜 영역에서, 밴드는 특정한 집계 방법을 강요하지 않지만, 데이터 제공자는 다음과 같이 이용 가능한 절반 이하의 데이터 포인트들로 조작할 수 있는 것에 대한 내성을 가진 방법을 사용하여 데이터를 집계해야 한다.

- 주어진 키의 모든 결과 중 중간 값.
- 주어진 키의 모든 결과 중 다수 값 그렇지 않을 경우(다수 값이 없을 경우) 실패한다.

#### 4.1.3. 경제적 분석

이 섹션에선 TCD 의 경제적인 부분을 분석한다.

**데이터 공급자가 드는 비용이 적다.** 데이터 포인트를 업데이트 하는 것은 데이터 공급자에게 적은 비용이 든다. 예를 들어, 공급자가 이더리움 블록체인에서 키-값 쌍을 업데이트하는 경우, 가스 비용은 약 26000 가스(저장 단어 업데이트의 경우 5000, 고정 거래 비용의 경우 21000)이다. 따라서 매시간 이 데이터 포인트를 업데이트하는 것은 26000·24·5·109 = 0.00312 ETH 또는 200 USD/ETH의 Ether 가격이라

가정했을 때 하루 0.624 달러의 비용이 드는 것이다. 실제 가격 피드나 다른 블록체인 블록 해시 등과 같은 중요한 데이터 포인트의 경우 데이터 포인트당 하루에 1달러 미만의 비용은 상당히 저렴한 것이다. 더욱이, 향후의 밴드 에서 데이터 제공이 반복되면, 데이터 제공자들은 모든 개별 데이터 포인트 대신에 데이터셋의 Merkle 해시만을 제공함으로써 추가적인 비용을 절감할 수 있다. 자세한 내용은 섹션 7.1을 참조하십시오.

**데이터를 소비하는 사람들에게도 적은 비용이 든다.** 데이터 소비자는 거래를 네트워크에 통신할 때 이미 가스 요금을 지불한다. 복잡한 거래의 평균 크기가 5Gwei의 가스 가격에서 20,000개라고 가정했을 때, 거래 수수료만 이미 20센트(200ETH/USD)이다. 따라서, 데이터의 보안을 보장하기 위해 10센트를 추가로 지불하는 것은 사용자 경험을 침해하지 않아야 한다. 데이터의 보안 정도에 따라 요금을 조정할 수 있다는 점에 유의하기는 해야한다.

**건전한 이득과 긍정적 평판을 동시에 얻을 수 있다.** 앞에 언급한 두 부분을 종합하면 데이터 공급자가 균등점에 도달하기 위해서는 소량의 쿼리만 필요하다는 것을 알 수 있다. 위의 숫자를 사용해서 계산해 보면, 데이터 제공자가 10명일 경우, 데이터 제공자를 지원하기 위해 하루에 $10 \cdot 0.624/0.1 \approx 60$개의 쿼리에만 필요하다. 그 이상의 것은 데이터 제공자들에겐 경제적 순이익이다. 데이터 제공자들은 경제적 이익 외에도 밴드를 채택함으로써 명성을 얻는다. 예를 들어, 암호화폐 거래소는 네트워크에 유효하고 최신의 가격 정보를 제공함으로써 분산된 생태계를 지원한다는 긍정적 평판을 얻을 수 있다.

**시장의 확장성.** 더 많은 분산형 애플리케이션이 Band Protocol에 가입함에 따라, 데이터 공급자에게 어떠한 한계 비용도 부담하지 않고 데이터를 소비하고 수수료를 지불하는 것을 시작할 수 있다. 이는 데이터셋의 시가총액이 직접 증가하여 데이터 공급자와 토큰 보유자가 모두 이득을 얻는 것을 의미하며, 데이터 거버넌스 그룹은 다른 데이터셋 토큰을 발행하지 않고도 더 많은 TCD를 지원하기 위해 다양한 시장으로 확장할 수 있다.

#### 4.1.4. 보안성 분석과 가능한 공격 벡터들

**데이터 제공자의 1/3 미만이 결탁하는 경우**: 소수의 데이터 제공자가 데이터 결과를 조작하기 위해 공모할 수 있음 – 소수의 악의적인 공격자는 네트워크의 전체 데이터 무결성에 영향을 미치지 않으며. 아래의 사례가 이를 보여준다:

**데이터 제공자의 2/3만 데이터를 제공하는 경우**: 이러한 경우엔 데이터 제공자들이 제공하는 절반 이상의 데이터는 솔직한 것이므로 절반 이하의 악의적인 데이터 포인트들로 조작할 수 있는 것에 대한 내성을 가자고 있는 방법을 사용하여 데이터를 집계하는 밴드의 경우엔 여전히 신뢰할 수 있는 데이터를 얻을 수 있을 것이다.

**데이터 제공자의 2/3 미만만 데이터를 제공하는 경우:** 이러한 경우엔 밴드는 유저들에게 데이터를 제공하지 않는다. 다른 말로 하면, 밴드 자체의 운영보다 안전성을 더 중요하게 여긴다는 것이다. 밴드는 데이터 제공자의 2/3 이상이 다시 데이터를 제공할 때야 비로소 작동하게 될 것이다.

**데이터 제공자의 1/3이상이 결탁하는 경우:** 더 많은 수의 데이터 공급자가 데이터 결과를 조작하기 위해 공모할 수 있다. 제공자의 3분의 1 이상이 잘못된 데이터를 제공한다면, 밴드는 필연적으로 디앱에 나쁜 데이터를 제공할 것이다. 그러나, 그러한 공격이 발생하고 데이터가 덜 유용해지면, 그러한 데이터에 대해 더 이상 지불할 의향이 있는 디앱이 없기 때문에 토큰의 가치는 본질적으로 파괴된다. "탈퇴 지연" 메커니즘은 데이터 공급자가 일반 토큰 소유자보다 먼저 데이터 토큰을 BAND로 변환하는 것을 방지한다. 이것은 데이터 제공자들이 지배집단의 붕괴로 가장 큰 피해를 보게 한다. 신뢰할 수 있는 경제적 손실의 위협은 데이터 공급자의 커뮤니티 전반의 유착을 억제하기에 충분해야 한다. 또한, 유착으로 인한 실제적인 평판 손실은 데이터 제공자들이 악의적으로 행동하는 것을 막는 동기가 되기도 한다. 앞으로 우리는 부정직한 행동을 더욱 자극하지 않기 위해 토큰을 없애버리는 패널티를 부과하는 것도 고려하고 있다.

**부유한 공격자:** 부유한 공격자는 토큰을 구입하고 상당한 힘을 얻기 위해 많은 자본을 사용할 수 있으며, TCD에 1/3 + $\epsilon$의 공격을 감행한다 – 토큰을 구입하여 기존 토큰 소유자를 제압하는 것은 엄청나게 비싸다. 토큰 발행의 본딩 커브가 가진 특성 때문에, 새롭게 제공되는 토큰은 점점 더 비싸지는 구조다. 구체적인 예로, 20% 미만 지급 준비율을 가지고 있는 상태의 본딩 커브 토큰 공급의 1/3 수준을 달성하려면 현재 공급되는 토큰양의 50%를 발행해야 한다. 그 비용은 1.5 (100%/20%) ≈ 현 담보물의 7.6배정도가 발생하며, 시장의 총액이 충분히 높은 거버넌스 그룹의 경우 극히 비싸다. 미래엔 데이터 공급자가 되기 위한 자격으로 토큰 보유를 일정 기간 동안 해야 한다는 기간이 포함될 수 있다. 즉 이러한 딜레이는 거버넌스 그룹으로 하여금 갑작스런 가격 인상에 반응하게 할 수 있다.

**서비스 거부:** 데이터 제공자는 블록체인과의 건전한 연결을 유지할 책임이 있지만, 데이터 제공자의 신원이 알려질 가능성이 높기 때문에 악의적인 공격자는 이러한 제공자를 직접 공격하여 데이터를 제공할 수 없게 할 수 있다. 그러나 데이터 사용자에게 데이터가 직접 제공되는 기존의 데이터 API와 달리, 밴드는 데이터 배포를 돕기 위해 블록체인 인프라를 활용하기 때문에, 전체 블록체인 생태계를 폐쇄하지 않는 한 공격자가 Band Protocol의 데이터 서비스를 종료하는 것은 거의 불가능하다.

### 4.2 토큰 보상을 통한 리스트 큐레이팅

토큰 홀더들은 TCR이라 불리는 방법을 통해서 집단적으로 퍼블릭 데이터셋을 구성할 수 있다. TCR은 주소 숫자 또는 해시를 포함한 32바이트 항목으로 구성된 온 체인 데이터 리스트다. TCR, 어플리케이션 후보, 토큰 홀더, 데이터 소비자 구축에 세 집단이 참여하게 된다:

- 애플리케이션 후보들은 데이터 토큰을 시스템에 포함시키기 위해 자신의 데이터 토큰을 걸고,

본질적으로 데이터 제공자 역할을 한다. TCR의 지침에 맞지 않으면 토큰을 잃을 위험을 감수해야한다. .

- 토큰 홀더는 TCR의 품질을 모니터링 한다. 그들은 낮은 질의 응답에 대항하고, 투표한다. 그들은 큐레이션 작업을 수행하면서 토큰 보상을 받는다.
- 데이터 소비자는 TCR의 입력에 관한 정보를 읽고 활용한다. 소비자가 지불하지 않지만, 그들은 TCR 입력에 관한 정보를 가지고 있는 소유주들에게 내재가치를 제공한다.

TCR로 잠재적으로 크라우드 소싱 및 큐레이팅 할 수 있는 데이터의 예시로는 특정 기준을 충족하는 검증된 크립토 프로젝트 목록, 커뮤니티 표준을 충족하는 뉴스 및 연구 목록 또는 신뢰할 수 있는 제3자가 검증한 고유한 ID 목록이 포함된다. TCR은 투명성과 규모적인 측면에서 중앙화 되어있는 데이터 큐레이션에 비해 잠재적인 이점을 가지고 있다.

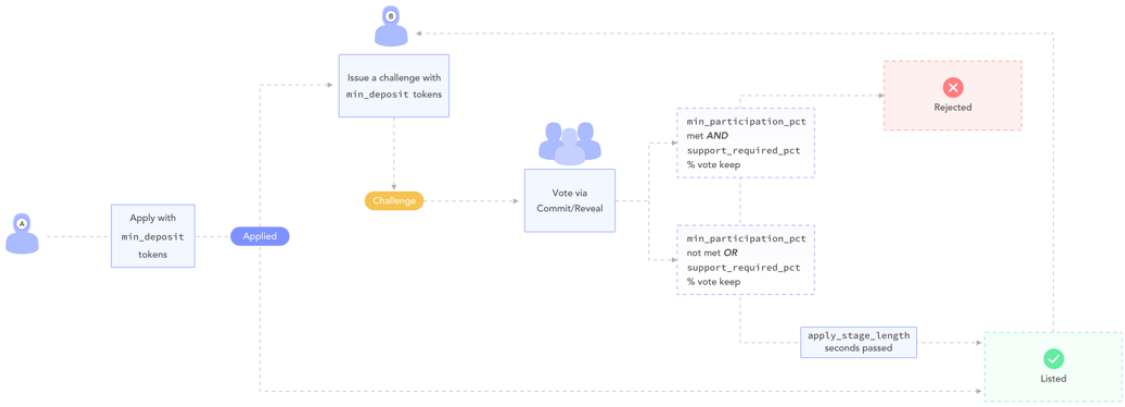


**그림 13**: TCR에 들어와서 의의제기를 하는 순서를 보여주는 차트다.

#### 4.2.1. TCR 큐레이션은 어떻게 이루어지는가?

1. 지원자는 최소 입금 데이터셋 토큰을 스테이킹해서 TCR에 등록할 수 있도록 신청한다. 신청 단계 기간 동안 누군가가 이의를 제기하지 않으면 해당 엔트리는 자동으로 등록된다.

2. 토큰 보유자는 지원자가 스테이킹한 토큰의 양과 일치하는 양의 예금을 걸어 참가 신청에 이의를 제기할 수 있다. 그렇게 되면 참가 신청은 투표를 거치게 된다. 토큰 소유자는 커밋-리빌 투표를 사용하여 엔트리를 유지하거나 제거하기 위해 투표한다.

3. 토큰이 최소 참가 수량보다 적으면, 의의제기는 의미 없는 것으로 간주한다. 일치하는 보증금은 의의를 제기한 자에게 돌려주고, 엔트리는 TCR에 남는다.

4. 토큰이 충분히 참가하고, 엔트리 제거를 위해 필요한 지지를 얻으면, 엔트리는 제거되고, 엔트리의 보증금은 도전자에게 주는 보상이 된다. 도전자는Dispensation_percentage에 해당하는 %의 보상을 받고, 이긴 유권자는 나머지를 갖는다. .

5. 한편, 도전이 실패하면 도전자의 지분을 몰수하여 엔트리를 지키기 위해서 투표했던 지원자와 유권자에게 분할한다. 엔트리 소유자는 Dispensation_percentage %를 받고, 이긴 유권자는 나머지를 얻는다.

밴드는 엔트리 예금의 감가상각 스테이킹 모델을 적극적으로 실험하고 있는데, 이 모델은 시간이 흐르고 엔트리의 실제 가치가 하락할수록 엔트리의 예금이 감소할 수 있다[7].

#### 4.2.2 경제와 보안 분석

TCR모델에 대한 경제적 그리고 보안적 분석은 2017년 TCR이란 개념이 소개되고 나서부터 지금까지 활발하게 이루어지고 있다. TCR과 TCR 분석에 대해서 관심이 있는 독자들은 TCR Reading List를 참고하면 될 거 같다. 통상적으로 알려진 사실을 배제하더라도, 2.2 섹션에서 언급했던, 밴드가 거너번스 그룹별로 데이터셋 토큰을 분리하여 독립적으로 사용한다는 사실 또한 시스템에 더 강력한 인센티브와 보안적 요소를 제공한다.

## 5. 추후에 문제가 될 수 있는 점들과 한계점들.

### 5.1 기생하는 데이터 소스들

기생적 스마트 컨트랙트는 데이터 셋의 데이터를 소비하여 더 낮은 비용으로 다른 디앱에 재 배포한다. 요약하자면, 그것은 본래의 사실에 대한 캐싱 레이어 역할을 하므로 원래 큐레이션된 데이터셋에 대한 수익 손실이 발생한다. 기존 중앙화 기업들은 법 집행을 이용해 데이터 재판매를 막을 수 있지만 자율적인 데이터 거버넌스 그룹의 스마트 컨트랙트에는 그러한 특권이 없다.

안타깝게도, 퍼블릭 프로토콜로서의 밴드는 이러한 존재들(기생하는 데이터 소스들, 스마트 컨트랙트들)을 막을 수 없다. 그러나 기생하는 스마트 컨트랙트에 의존하기로 선택한 어플리케이션들은 최신 데이터나 악성 데이터를 수신할 위험이 있다. 탈 중앙 어플리케이션의 규모가 커질수록 신뢰와 명성이 매우 중요해지기 때문에 공식 데이터 출처의 데이터를 소비해야 할 것이다.

### 5.2 온 체인 투표

뇌물, 투표 매수와 관련하여 토큰 기반 투표의 가능성은 아직 완전히 입증되진 않았다. 이 주제는 여러 팀에서 활발한 연구를 하고 있다. 그러나 현재 토큰 기반 투표는 가장 널리 채택되고 있으며 시빌 공격(Sybil Attack, 어떠한 목적을 달성하기 위해서 한 사람의 행위를 여러 사람의 행위인 것처럼 속이는 공격을 말한다)에 대항하는 최선의 방법이다. 밴드는 공격의 동기를 낮추기 위해 다음과 같은 추가 계층을 구현한다.

- 데이터셋 토큰은 연속적인 본딩 곡선을 통해 자유롭게 구매하거나 판매할 수 있지만, 계약은 매수와 매도가격 사이에 작은 유동성 스프레드(유동성을 공급하는 사람에게 부여하는 프리미엄)를 부여한다. 이것은 특정 투표에 영향을 주기 위해서 토큰을 구입하는 경우에 비용이 많이 들게 한다.

- 평판은 또 다른 중요한 자원이다. 일반적으로 데이터 제공자는 커뮤니티로부터 신뢰를 얻기 위해 자신의 ID를 제출할 필요가 있다. 따라서, 모든 데이터 제공자는 금전적 가치와 평판 둘 다 걸고서 데이터를 제공하는 것이고, 이는 그들이 악의적으로 행동할 동기를 빼앗을 것이다.

- Band Protocol 내부의 모든 투표 기반 결정을 다시 고려할 수 있다. 이전에 하였던 의의제기가 불리하게 끝났을 경우 TCR 의의제기는 다시 시작될 수 있다. 거버넌스 제안도 마찬가지로 다시 제안할 수 있다.

밴드는 온 체인 투표에 관해서 꾸준히 리서치 할 것이며, 더 나은 메커니즘과 방법론들이 있다면 꾸준히 업데이트 할 것이다.

## 6. 앞으로 가능한 실 사용처들.

### 6.1. 탈 중앙 금융

대부분의 기존 탈 중앙 금융(DeFi) 애플리케이션들은 치명적인 위험 요소가 될 수 있는 가격 피드 Oracle을 공유한다. MakerDAO, Compound, Dharma, dYdX 또는 SET와 같은 명성 있는 프로젝트는 상대적으로 적은 수의 신뢰할 수 있는 개발자들에만 의존하여 프로토콜에 블록체인 외부 가격 정보를 제공한다. 밴드는 격차를 메우고 그와 같은 중요한 정보를 제공함으로써 프로젝트가 그들이 가장 잘 하는 측면에 초점을 맞출 수 있게 하는 동시에 밴드의 데이터 제공자들의 데이터 보안성을 함께 누릴 수 있다. 이는 금리, 환율, 주식, 채권, 상품 등 실물 데이터의 지식을 필요로 하는 실물 자산의 파생상품 거래와 같은 미래 분권형 금융 적용에도 확대 가능하다.

### 6.2 탈 중앙 상업

많은 분산형 어플리케이션은 토큰을 지불 수단으로 활용하는데, 토큰은 토큰을 토큰을 기준으로 가격이 매겨져야 한다. 그러나 이러한 어플리케이션은 가격을 비교적 안정적인 법정 화폐로 메기고 있고, 토큰은 가격 변동성이 높기 때문에 이것은 어렵다. 따라서, 그들은 그들이 메기는 법정화폐 가치를 지속적으로 토큰의 가치로 변환할 수 있도록 꾸준한 Crypto-Fiat 가격 피드를 제공해줘야 한다.

### 6.3 아이덴티티 레이어

많은 분산된 어플리케이션들은 가짜 계정과 시빌 공격의 문제를 해결하기 위해서 정말로 고군분투 하고 있다. 비탈릭이 시사하는 바와 같이, 아이덴티티 레이어는 담합을 저항할 수 있는 토큰 시스템을 구축하는 데 있어 가장 중요한 부분 중 하나이다[6]. 밴드는 밴드가 가지고 있는 단순한 쿼리 인터페이스를 통해 애플리케이션에 의해 소비될 수 있는 다양한 ID 서비스들과 함께 ID 정보를 큐레이팅하는 플랫폼 역

할을 할 수 있다.

### 6.4 게이밍, 도박, 그리고 예측시장.

게임과 도박은 블록체인 생태계에서 가장 큰 분야 중 하나이다. 밴드를 활용함으로써 탈 중앙 어플리케이션은 하나의 데이터 소스에만 의해 제어되지 않는 신뢰할 수 있는 현실 정보에 접근할 수 있다. 이는 DeFi와 유사하게 개발자들이 핵심 제품에 집중하는 동시에 밴드가 가진 보안성을 동시에 활용할 수 있게 해준다.

### 6.5 공급망 추적

암호화폐를 이용해 실제 제품을 상대방을 신뢰할 필요가 없이 사고 파는 것은 현재 기술로는 거의 불가능하다. 밴드는 품목 발송 또는 블록체인을 통하지 않은 지불과 같은 공급망 관련 데이터를 포용한다. 스마트 컨트랙트는 이러한 정보를 온 체인 방식으로 검증하고 그에 따라 재무적인 일들을 수행할 수 있다.

### 6.6 현실세계 API 연동

스마트 컨트랙트는 디지털 세계와 현실 세계를 연결하지 못하기 때문에 매우 제한적이다. 밴드는 실제 세계 API 연결을 지원할 수 있으므로 스마트 컨트랙트는 실제 세계 이벤트를 충분히 인지하고 특정 이벤트를 작동시키기 위해 API에 입력(input)을 제공할 수 있다. 예를 들어, 은행 API를 연결하여 스마트 컨트랙트에서 오프 체인 거래가 있거나 스마트 컨트랙트 자체로 오프 체인 거래가 자동으로 작동될 수 있음을 스마트 컨트랙트에서 정확히 알 수 있다.

## 7. 앞으로 달성할 기술적 목표들

### 7.1 대용량 데이터에 대한 큐레이션 서비스

Band Protocol이 기존의 웹의 위키피디아나 Wikidata와 같은 데이터 질의의 장이 되기 위해서는 대규모 데이터 셋을 지원할 수 있어야 한다. 현재의 TCD 설계로 데이터 공급자는 데이터셋의 모든 데이터를 블록체인(blockchain)에 제출해야 하는데, 이것은 엄청난 비용 때문에 실현 불가능한 일이다. 가공되지 않은 데이터는 토큰 소유자들이 데이터를 집단적으로 검증하는 오프체인 네트워크를 통하여 배포될 것이다. 온 체인 스마트 컨트랙트는 동일한 쿼리 인터페이스를 통해 데이터 유효성을 확인할 수 있다.

### 7.2 인터체인 커뮤니케이션

다른 블록체인의 해시 체인(hash-chain)을 큐레이팅하는 것을 목표로 하는 데이터셋 데이터 거버넌스 그

룹을 이용할 수 있게 된다. 위에서 언급한 Merkle-hash 압축과 결합하여, 이더리움 스마트 컨트랙트는 비트코인이나 EOS와 같은 다른 블록체인에서 일어나는 일을 검사할 수 있을 것이다.

우리는 Cosmos Network와 EOS를 포함하여 스마트 컨트랙트가 지원되는 모든 블록체인에서 밴드 토큰을 사용할 수 있는 블록체인(blockchain agnostic protocol)으로써의 밴드를 꿈꾼다. 이를 가능하게 하기 위해서 밴드 토큰은 밴드 프로토콜 자체에 의해 구동되는 분산형 데이터 oracle임에도 불구하고 BancorX[5]와 유사하게 블록체인 간의 인터체인 아토믹 스왑을 지원해야만 한다. 이를 통해 여러 블록 체인을 효과적으로 상호 연결하여 광범위한 분산형 애플리케이션을 구축할 수 있다.

### 7.3 온 체인 데이터 프라이버시

일부 데이터는 일반 텍스트로 저장하여 게시할 수 없다. 이름, 나이, 신용 점수와 같은 개인 정보는 매우 사적인 영역이다. 그러나 그러한 정보는 분산형 애플리케이션의 가능성을 여는 데 중요하다. 예를 들어, 무담보 대출 신청은 올바른 대출 결정을 하기 위해 개인 정보를 요구해야만 한다. 향후 밴드에서 반복적으로 데이터를 검증하는데 있어, 사용자의 프라이버시를 훼손하지 않고 신뢰가 불필요한 정보 주장을 허용하는 신뢰된 실행 환경(TEE)과 영 지식 증명 등 최첨단의 암호 기법을 통합하여 개인적인 정보를 안전하게 다룰 계획이다.