

Fiducia – 분산 블록체인 데이터 오라클 네트워크

Steve Chen*

Fiducia Network Project
Berkeley, California, USA
contact@fiducia.network

2019년 8월 18일

초록

Fiducia Network는 데이터 오라클 노드 분산 네트워크로 오프체인 데이터를 블록체인 애플리케이션에 제공합니다. Fiducia 노드는 핵심적으로 프록시 서버의 역할을 합니다. Fiducia 노드 소프트웨어는 사용자 요청을 받고, 블록체인 외부의 데이터를 검색하고, 그리고 중간 반응을 생성합니다. 데이터 진실성, 보안성, 그리고 기밀성을 확보하기 위해 P2P 네트워크 합의 메커니즘이 요청자에 대한 최종 반응을 처리하고 생성하는 데 적용됩니다. Fiducia 노드 소프트웨어는 산업 표준 보안 컴퓨팅 환경 내에서 작동되어 데이터가 노드 운영자에 의해 변경되지 않게 합니다.

Fiducia Network는 승인이 없는 방식으로 네트워크를 참여하고 떠나는 노드를 갖춘 P2P 네트워크로 작동됩니다. 네트워크의 기능이 효과적으로, 그리고 효율적으로 이루어질 수 있도록 노드 운영자는 요청을 하는 당사자에 의해 발생하는 수수료에 의해 참여를 하도록 인센티브를 받습니다.

데이터 소스 공급자는 데이터가 잘 알려진 API 종점을 통해 이용 가능하게 만들 수 있을 것입니다. 노드 소프트웨어는 잘 알려진 API 종점을 통해 데이터에 접근할 수 있을 것입니다. 혹은 데이터 공급자는 노드 소프트웨어를 운영하고 Fiducia Network에 직접 참여할 수도 있을 것입니다.

블록체인 애플리케이션(Dapp) 개발자인 데이터를 요청하는 당사자는 Fiducia Data Provision SDK를 블록체인 Dapp에 포함함으로써 노드 소프트웨어에 의해 공급되는 데이터를 활용할 수도 있을 것입니다.



도표 1: Fiducia – 신뢰, 믿음, 비밀 유지

* 대표 저자

목차

1 도입	4
1.1 블록체인 애플리케이션과 데이터 액세스	4
1.2 액세스 할 수 없는 문제	5
2 블록체인용 분산 데이터 오라클 네트워크	5
3 저희의 솔루션(Solution) - Fiducia 데이터 오라클 네트워크	6
3.1 Fiducia 네트워크 구성 요소	6
3.2 Fiducia 네트워크를 위한 신뢰 실행 환경	7
3.3 Fiducia 네트워크 운영	7
4 결론	8
4.1 앞으로의 계획	8
4.2 감사의 말	8
4.3 백서 버전 및 수정 정보	8

도표 목록

1	Fiducia – 신뢰, 믿음, 비밀 유지	1
2	Fiducia 네트워크	6

1 도입

비트코인 및 이더리움과 같은 블록체인은 체인 외부의 정보에 빠른 접근을 하지 못합니다. 스마트 계약은 조건 인증 절차에 필요한 다이렉트 액세스를 가지고 있지 않습니다. 데이터 처리 및 인증은 스마트 계약 기능에 있어서 필수적인 부분입니다. 하지만 현재 스마트 계약은 다이렉트 데이터 액세스 부재와 같은 문제로 인해 심각하게 그 기능이 제한적입니다. 블록체인 데이터 오라클은 간단히 말해서 외부 플랫폼에서 제공하는 정보를 위한 전달 매체에 해당합니다.

1.1 블록체인 애플리케이션과 데이터 액세스

사업자 및 개발자에게 있어서 블록체인의 가장 큰 이점은 신뢰할 수 있는 방법으로 데이터를 제시할 수 있는 블록체인의 능력입니다. 블록체인의 불역성 및 타임 스탬프 기능은 애플리케이션에서 신뢰성을 유지하는 데 중요한 역할을 합니다. 제대로 설계된 인프라를 통해 비즈니스 금고에 보관된 데이터 및 현재 접속이 불가능한 데이터를 신뢰할 수 있는 방법으로 공개할 수 있습니다. 이 모든 것이 블록체인이 없는 시스템보다 더 낮은 비용으로 가능합니다.

전 세계의 사업장, 여러 기관, 그리고 다양한 에이전시는 엄청난 양의 데이터를 보유하고 있습니다. 이렇게 많은 데이터는 대중이 사용할 수 있도록 되어 있습니다. 이러한 많은 공개 데이터를 대중이 활용할 수 없도록 막는 요인은 해당 서비스를 제공하는 데 드는 높은 비용입니다. 중앙화 된 애플리케이션은 설치 및 유지를 위해 다수의 인력을 필요로 합니다. 이와 달리 분산 블록체인 애플리케이션은 유지를 위해서 훨씬 더 적은 리소스만을 필요로 합니다. 블록체인 애플리케이션과 관련된 빌트인 경제 시스템은 주주에게 인센티브를 적절하게 부여할 수 있는 방법을 제공하고, 이를 통해 퍼블릭 액세스 시스템을 유지하는 데 필요한 비용을 급격하게 줄일 수 있습니다. 올바르게 설계된 블록체인 애플리케이션을 통해 딥 웹 또는 딥 데이터 애플리케이션이 실현 가능하게 되고 비용 면에서도 효과를 보이게 됩니다. 딥 데이터와 딥 웹 애플리케이션의 새로운 전체 카테고리가 블록체인 기술을 통해 효과적으로, 그리고 효율적으로 구축되고 배치될 수 있을 것입니다.

현재의 대부분의 블록체인 애플리케이션은 금융 결제에 중점을 두고 있습니다. 이것은 최초의 성공을 거둔 실용적인 결과가 P2P 디지털 현금 결제 시스템인 비트코인이라는 점에서 쉽게 이해할 수 있는 부분입니다. 다양한 기타 블록체인 결제 시스템들도 비트코인에 이어 널리 수용되게 되었습니다. 금융 서비스는 블록체인 기술이 성공적으로 적용된 첫 번째 분야입니다. 그렇다고 해서 이것이 블록체인 기술에 의해 긍정적인 방식으로 영향을 받을 수 있는 유일한 분야인 것은 아닙니다.

저희는 블록체인의 영향력을 바로 증명해 보일 수 있는 바로 다음 분야가 딥 웹과 딥 웹과 관련된 데이터라고 확신합니다. 오늘날의 검색 엔진은 표면 데이터를 위해 웹을 기어 다니고 있습니다. 표면 데이터는 검색 엔진의 지표가 될 수 있는 콘텐츠입니다. 표면 데이터의 대표적인 예는 바로 공공 웹 페이지입니다. 사업장 및 여러 기관들은 웹 페이지 형식으로 되어 있지 않은 수많은 양의 데이터와 콘텐츠를 보유하고 있습니다. 여기에는 프레젠테이션, PDF 파일, 그리고 데이터베이스에 저장된 여러 데이터 등이 포함됩니다.

많은 경우에 딥 웹 데이터는 일반 사람들이 사용할 수 있게 하고자 한 공개 정보에 해당합니다. 딥 웹 데이터는 전용 데이터 및 개인 데이터와는 다른 것입니다. 올바르게 설계된 블록체인 솔루션을 통해 딥 웹 데이터는 효율적인 저비용의 방식으로 일반 사람들에게 공개될 수 있습니다. Fiducia 블록체인 플랫폼의 주요 목표 중 하나는 딥 웹 데이터 액세스를 가능하게 만드는 것입니다. 딥 데이터가 이용 가능하도록 하기 위해서는 데이터 소유주 입장에서 적극적인 노력을 기울여야 합니다. 데이터 소유주가 딥 데이터를 이용 가능하게 만들지 못하게 하는 대표적인 문제점 중 하나는 바로 엄청난 양의 리소스가 필요하다는 점입니다.

저희는 블록체인 기술에 구축된 데이터 중심의 애플리케이션이 검색 애플리케이션의 완전히 새로운 형식을 가능하게 할 것이라고 확신합니다. 데이터 중심의 블록체인 애플리케이션은 금융 결제 솔루션에 이어 블록체인 애플리케이션이 영향을 크게 미칠 수 있는 다음 카테고리가 될 것입니다.

딥 웹 검색의 경우: 파플러 사이언스는 다음과 같이 기록하고 있습니다. “[딥 웹]에서는 온라인 정보가 암호로 보호되거나, 유료화 벽 뒤에 가두어 지거나, 또는 액세스를 위한 특별 소프트웨어를 필요로 하고, 그리고 딥 웹은 엄청나게 큼니다. 어떤 사람들은 이것이 대부분의 사람들이 매일 검색하는 표면 웹보다 500배 더 큰 것으로 보고 있습니다. 그런데 이것은 완전히 보이지 않는 곳에 있습니다. 네이처에서 발행한 연구에 따르면, 구글은 표면 웹의 16 퍼센트 이하를 기록하고 있고, 딥 웹의 모든 것을 놓치고 있다고 합니다. 모든 검색은 온라인에 존재하는 정보의 단지 0.03 퍼센트만 보여주고 있습니다 (3,000페이지에 하나). 이것은 마치 바다에서 겨우 표면 60 cm에서만 낚시를 하는 것과 같습니다. 그 아래에 있는 마리아나 해구는 완전히 놓치고 있는 것이죠.”

1.2 액세스 할 수 없는 문제

블록체인 기술의 이점에도 불구하고, 무엇 때문에 블록체인이 광범위하게 채택되지 않고, 또 블록체인 애플리케이션의 배치가 더 빠르게 이루어지지 않고 있을까요?

간단하게 답을 말해보자면 사실상 블록체인과 현재 존재하는 IT 데이터 인프라를 쉽게 연결하지 못합니다. 블록체인 애플리케이션은 웹과 현재 존재하는 IT 인프라의 모든 데이터에 액세스 할 수 있다는 “오해(misconception)”가 있습니다.

게다가 블록체인 애플리케이션을 개발하려면 개발자들은 낮은 레벨 블록체인 인터페이스를 직접 다루어야 합니다. 시장에 많은 경쟁 블록체인 플랫폼이 있기 때문에 낮은 레벨 블록체인 복잡성을 다루는 것은 개발자들에게 너무나도 힘든 과제가 되었습니다.

더 나아가 현재 블록체인 기술은 대규모 비즈니스 애플리케이션의 규모 및 성능 필요조건을 지원하고 있지 않습니다. 현재 존재하는 블록체인에서 처리하는데 요구되는 시간은 비즈니스 등급 애플리케이션의 필요를 충족시키지 못하고 있습니다. 블록체인 애플리케이션이 비즈니스 및 사용자의 기대를 충족시킬 수 있으면서 블록체인의 특별한 특징을 유용하게 활용하는 새로운 방법들이 필요합니다.

2 블록체인용 분산 데이터 오라클 네트워크

오라클은 스마트 계약을 처리하고 승인하는 데 필요한 데이터를 제공합니다. 이러한 작업은 스마트 계약의 핵심 기능입니다. 오프체인 데이터는 스마트 계약이 조건부 결정을 내릴 수 있는 기초를 형성합니다. 이러한 조건은 가격, 결제 완료, 기업 전용 데이터 등 스마트 계약과 관련되어 있는 모든 것이 될 수 있습니다. 이러한 오라클은 스마트 계약이 블록체인 환경 밖의 데이터와 상호 작용할 수 있는 유일한 길입니다.

블록체인 오라클은 중앙화 된 유형과 탈중앙화 된 유형으로 분류될 수 있습니다. 중앙화 된 오라클은 권한자에 의한 전통적인 기업 컴퓨팅 환경 내에서 작동합니다. 중앙화 된 오라클은 제한적이거나 오픈 소스일 수 있습니다. 중앙화 된 오라클 시스템의 세부 특징 중 하나는 시스템이 외부인들에게 닫혀 있다는 점입니다. 저희는 시스템의 무결성과 데이터 진실성, 보안성, 그리고 공정성을 보장하는 운용자의 무결성에 대해 신뢰를 가져야 합니다.

분산 블록체인 오라클은 데이터 공급 노드의 P2P 네트워크로 작동됩니다. 이것은 중앙화 된 오라클의 결점을 해결해 줍니다. 저희 팀은 블록체인의 개방성 하에서 허가를 요하지 않는 P2P 네트워크 기반의 블록체인 오라클 시스템이 블록체인 산업의 더 큰 발전을 위해 필요하다고 믿고 있습니다. 이로 인해 Fiducia 블록체인 플랫폼이 탄생하게 되었습니다.

3 저희의 솔루션 - Fiducia 데이터 오라클 네트워크

Fiducia 블록체인 플랫폼은 데이터 중심의 애플리케이션을 기반으로 하여 블록체인의 빠른 개발 및 배포를 제공하기 위해 노력하고 있고, 이를 통해 경제의 모든 분야에서 블록체인 기술이 더 광범위하고 빠르게 채택되게 하고자 노력하고 있습니다. 저희의 궁극적인 목표는 블록체인 기술을 통해 높은 신뢰 수준의 경제 시스템을 형성할 수 있도록 하는 것입니다.

Fiducia 네트워크를 통해 개발자들은 모든 소스로부터 데이터에 액세스 할 수 있는 모든 이점을 누릴 수 있고, 데이터 권한 설정과 관련된 낮은 레벨 문제에 봉착하지 않게 될 수 있습니다.

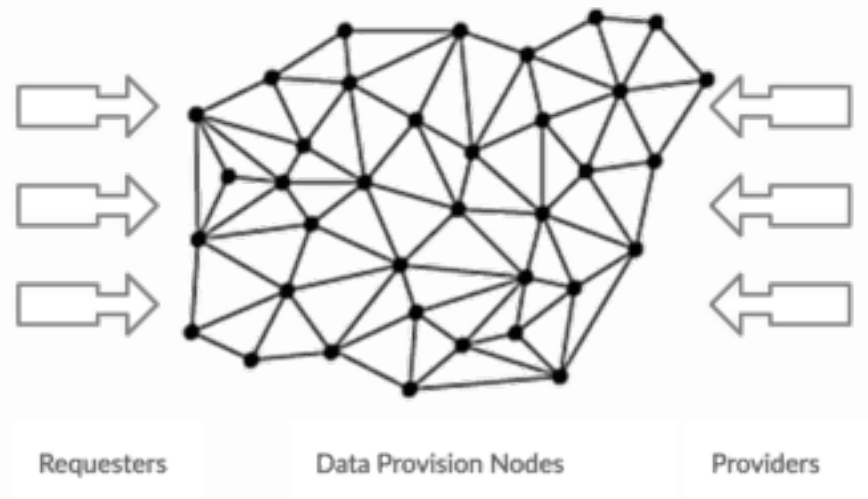


도표 2: Fiducia 네트워크

3.1 Fiducia 네트워크 구성 요소

Fiducia 데이터 공급 노드: 데이터 공급 노드는 Fiducia 생태계의 중심부를 형성합니다. 해당 노드 소프트웨어는 P2P 네트워크를 형성합니다. 네트워크는 총괄하여 사용자 요청을 처리하고, 태스크를 노드에 배정하고, 다양한 소스에서 데이터를 검색하고, 데이터를 처리하고, 요청 당사자에게 대한 반응을 생성합니다.

Fiducia 개발자 SDK: 블록체인 애플리케이션 개발자는 Fiducia 개발자 SDK를 자신들의 개발 환경으로 가져옵니다. 스마트 계약 내에서 개발자들은 SDK와 관련된 기능을 불러서 스마트 계약 기능을 위해 필요한 데이터를 검색하는 데 사용할 수 있습니다. SDK는 이더리움, 코스모스, 패리티, 또는 이오스와 같은 다양한 블록체인에 맞추어 조정될 수 있습니다. SDK는 P2P 방식을 통해 Fiducia 데이터 공급 노드와 연결됩니다. 데이터 요청은 데이터 요청 캐시를 통해 제출되고 수집됩니다. 요청은 랭킹 및 인센티브 제도에 기반하여 처리됩니다.

랜덤 노드는 데이터 검색 요청을 처리하기 위해 선택됩니다. 검색된 데이터는 요청자의 최종 반응을 형성하기 위해 인증되고, 결합되고, 그리고 처리됩니다.

Fiducia 데이터 공급자 SDK: 데이터 소스 소유자는 Fiducia 네트워크 액티브 공급자가 될 수 있습니다. 데이터 공급자 SDK는 데이터 소스 소유자가 자신들의 데이터를 데이터 공급 캐시에 제출하는 데 사용될 수 있습니다. 데이터 공급 캐시에 의해 관리되는 목록은 일반 사람들도 사용할 수 있습니다. 이것은 이용 가능한 데이터 유형 및 현재 Fiducia 네트워크를 통해 액세스가 가능한 소스의 목록의 역할을 합니다.

데이터 소스 소유자가 아닌 당사자들도 공개 API 종점을 통해 공개적으로 이용 가능한 데이터에 액세스를 하기 위해 데이터 공급 SDK를 사용할 수 있습니다. 어떠한 이유로 인해 데이터 소스 소유자가 적극적으로 Fiducia 네트워크에 참여하기를 원하는 않지만, 오픈 API 종점을 통해 공개적으로 데이터를 제공하는 경우, 모든 제삼자 개발자는 데이터 공급 노드를 사용하여 공개 데이터 API 종점과 연결될 수 있고, Fiducia 네트워크에 참여할 수 있습니다.

Fiducia P2P 네트워크 합의 메커니즘: P2P 데이터 공급 노드 네트워크의 중심이 되는 것은 랜덤 액티브 노드를 선택하여 어떤 데이터 요청을 처리하는 데 사용되는 랜덤 비컨(beacon)입니다. 몇 가지 랜덤 생성기 및 비컨은 독립적으로 또는 집합적으로 사용되어 네트워크 랜덤을 생성할 수 있습니다. 네트워크 랜덤에 기반하여 노드가 선택되어 태스크를 수행하게 됩니다. 싱글 데이터 요청의 경우, 몇 가지 노드가 무작위로 선택되어 데이터를 검색합니다. 검색된 데이터는 비교되고, 결합되고, 그리고 처리되어 최종 버전의 반응을 생성합니다. 이를 통해 어떤 노드도 잘못되거나 정확하지 않은 반응을 생성하도록 조작될 수 없습니다. 노드 소프트웨어는 랭킹 메커니즘에 기반한 요청 목록을 통해 작동합니다. 데이터 요청 당사자는 의도한 결과와 관련하여 긴급성, 데이터 유형, 소스, 그리고 기타 파라미터를 정의할 수 있습니다.

3.2 Fiducia 네트워크를 위한 신뢰 실행 환경

Fiducia 데이터 공급 노드는 신뢰 실행 환경 내에서 작동하도록 설계되어 있습니다. 신뢰 실행 환경(TEE)은 메인 프로세서의 보안 영역입니다. 이것은 내부에서 코드와 데이터가 불러지도록 함으로써 비밀보장 및 진실성과 관련된 보호가 이루어지게 합니다. TEE는 또한 노드 운용자가 노드 내에서 처리되는 데이터를 변경하지 못하게 합니다.

몇 가지 오픈 및 전용 신뢰 실행 환경은 현재 다양한 단계에서 이용 가능합니다.

- 인텔 SGX
- 암 트러스트존(ARM TrustZone)
- IBM 보안 서비스 컨테이너 (Secure Service Container)
- RISC V 멀티존

3.3 Fiducia 네트워크 운영

Fiducia 네트워크는 데이터 요청자와 공급자 사이에서 연결(매칭) 서비스 및 시장으로서 작동합니다. 데이터 공급 노드는 P2P 네트워크를 설정할 때 Fiducia 네트워크의 기반을 형성합니다. 데이터 요청자 및 공급자는 각각의 SDK를 통해 시장에 참여합니다. 요청 캐시 및 공급 캐시는 시장의 주문 대장의 역할을 하게 됩니다. 랭킹 및 요청과 공급의 연결은 집합적으로 데이터 공급 모드의 P2P 네트워크에서 발생합니다.

매우 중요한 점은 Fiducia 네트워크는 처리 비용 기반의 경제 시스템에서 작동한다는 점입니다. 요청자는 네트워크 토큰인 Fiducia 데이터 오라클 (FDO) 토큰으로 서비스 사용에 대한 지불을 하게 됩니다. 데이터 공급자와 노드 운용자는 요청자가 지불한 요금에 의해 자신들이 제공한 서비스에 대한 보상을 받게 됩니다.

Fiducia 네트워크는 다음과 같은 특별한 점을 제공합니다.

- 데이터 공급 노드에 대한 분산 및 P2P 네트워크
- 허가 조건이 없는 참여에 대한 개방성
- 무작위를 통한 데이터 진실성 및 보안성

4 결론

Fiducia 네트워크는 블록체인 프로젝트에 영향을 주는 데이터 이용 가능성 문제에 대해 개방된, 분산된, 보안성을 갖춘, 그리고 강력한 솔루션을 제공합니다. 블록체인과 블록체인 애플리케이션은 아직 초기 단계에 머물고 있는 가운데 저희는 Fiducia 네트워크가 블록체인 기술이 더 광범위하고 더 빠르게 채택될 수 있도록 추진할 수 있는 중요 기술이 될 것이라고 확신합니다.

4.1 앞으로의 계획

저희는 정기적으로 Fiducia 네트워크에 업데이트 정보와 세부 정보를 제공하려고 계획하고 있고 또한 새로운 버전을 준비하고 있습니다.

4.2 감사의 말

저희는 저희 프로젝트에 조언을 주신 산업 전문가 분들에게 감사의 마음을 전하고 싶습니다.

4.3 백서 버전 및 수정 정보

- v. 1.0 - 2019년 8월 최초 발행