공정한 고속의 퍼블릭 블록체인 : 앤드어스체인(version 0.71)
(부제 : 안전하고 공정한 고속 차세대 이더리움)

블록체인이 제4차 산업혁명의 핵심 기반기술 또는 제2의 인터넷(가치의 인터넷)이라는 것을 대부분의 사람들은 인지하고 있다. 이는 현재 사이버 세상의 인프라가 컴퓨터와 인터넷인 것처럼 미래 세상의 인프라는 블록체인이 된다는 것을 의미한다.

사실 블록체인은 단순한 분산원장 기술 그 이상의 의미를 포함하고 있다. 블록체인은 우리에게 주어진 새로운 컴퓨터이자 네트워크이다. 이더리움의 정의가 글로벌 신뢰컴퓨터이다. 그리고 이러한 블록체인 기술을 기반으로 현재의 모든 생태계(정치, 경제, 금융, 의료, 에너지, 물류, 교육 등)를 재구성한 세상이 블록체인 세상이다.

블록체인의 기본적인 철학과 사상은 탈중앙화된 P2P 기반 세상을 꿈꾸는 것이다. 즉, 신뢰성을 가정하는 제3의 신뢰기관이나 중개자 없이 P2P 기반으로 세상을 혁신하고자 하는 시도이다. 이러한 철학과 사상을 반영한 블록체인이 퍼블릭 블록체인이다.

대표적인 퍼블릭 블록체인 이더리움이야 말로 이러한 블록체인의 철학과 사상을 달성하고자 만든 블록체인이다. 우리가 제안하는 앤드어스체인을 공정한 고속 차세대 이더리움이라 명명하는 것은 이러한 연유 때문이다.

앤드어스체인은 이더리움에 기반한 퍼블릭 블록체인이다. 그러나 이더리움이 원래 추구하고자 했던 탈중앙화 특성이 작업증명 또는 지분증명 방식의 중앙화 특성으로 인해 지속가능성에 대한 많은 논쟁이 벌어지고 있다. 물론 이러한 논쟁 속에는 성능 및 정보보호 등 많은 이슈도 있다.

한편으로는 합의 알고리즘의 지속가능한 탈중앙화 특성을 제외한 다른 문제들의 경우 현재 많은 연구가 진행되어 해결 가능성을 보여주고 있다. 그러나 지속가능한 탈중앙화 특성이 유지되는 합의 알고리즘의 연구는 미진한 상태이다.

앤드어스체인은 지속가능한 탈중앙화 특성이 유지되는 새로운 합의 알고리즘인 deb 합의 알고리즘을 개발하고 적용한 퍼블릭 블록체인이다. deb 합의 알고리즘성의 목적은 지속가능한 탈중앙화 특성을 유지하면서도, 이더리움보다 고속의 퍼블릭 블록체인을 개발하고자 하는 것이다.

목차

1. 개요

2008년 분산원장(distributed ledger) 개념과 합의 알고리즘인 작업증명(PoW:Proof of Work)을 사용하여 사토시 나까모도가 탈중앙화된(decentralized) P2P 암호화폐 시스템인 비트코인(Bitcoin)을 개발하였다. 이후, 2014년 부탈린은 비트코인의 튜링 불완전성 등 한계를 극복한 "글로벌 신뢰컴퓨터(A trust world computer)"인 이더리움(Ethereum)을 개발하였다.

블록체인(blockchain)의 가장 중요한 핵심 기술은 상호 신뢰하지 않는 노드(Node)들 간의 합의(consensus) 알고리즘이다. 비트코인과 이더리움 모두 합의 알고리즘으로 작업증명 방식을 사용한다. 그러나 작업증명 방식을 사용하는 합의 알고리즘의 경우 노드가 보유한 컴퓨팅 파워(computing power)에 의해 채굴(mining) 확률이 결정된다. 이러한 특성으로 인해 블록체인이 추구하고자 하는 탈중앙화 특성이 약화되는 단점을 가지게 되고, 비트코인의 중앙화 문제가 현실적으로 대두되고 있는 실정이다. 이러한 연유로 이더리움은 현재 합의 알고리즘을 작업증명에서 지분증명(PoS:Proof of Stake) 방식으로 전환하고 있는 실정이다. 그러나 지분증명 방식도 노드들이 보유한 지분에 의해 채굴 확률이 결정되기 때문에 탈중앙화 특성이 지속가능한지에 대해 의문이 제기되고 있다. 본질적으로 지분증명 방식이 자본주의 문제점을 가지게 될 것이라는 논쟁도 이러한 이유에서 출발한다.

우리는 먼저 블록체인의 핵심 원천기술인 합의 알고리즘에 대한 탈중앙화 특성을 공정성(fairness) 개념으로 정의하여 분석하고자 한다. 간단히 설명하면 합의 알고리즘의 공정성은 채굴을 원하는 노드들의 조건(컴퓨팅 파워, 보유 지분 등)에 따른 채굴 확률의 비례성을 의미한다고 생각할 수 있다.

그리고 공정성을 극대화한 deb 합의 알고리즘을 제안하여 지속가능한 탈중앙화 특성이 유지되는 퍼블릭 블록체인 앤드어스체인(AndUschain)을 개발하고자 한다.

앤드어스체인은 기본적으로 이더리움에 기반한다. 즉, 앤드어스체인은 대표적인 퍼블릭 블록체인(public blockchain)인 이더리움의 구조를 유지하면서, 지속가능한 탈중앙화를 유지하고 속도를 대폭 향상한 퍼블릭 블록체인이다. 현재까지 퍼블릭 블록체인 및 프라이빗 또는 컨소시움 블록체인(private or consortium blockchain) 등 많은 블록체인이 제안되고 있으나, 원래 블록체인의 철학과 사상을 만족하는 것은 이더리움 블록체인이라고 생각하기 때문이다. 특히, 이더리움의 기본 목적인 탈중앙화 P2P 비즈니스 생태계(ecosystem)를 창출하는 인프라로서의 역할이 가장 중요하고 본질적인 블록체인의 철학과 사상이기 때문이다.

한편으로는 deb 합의 알고리즘과 기존의 퍼블릭 블록체인에서 사용하는 작업증명 및 지분증명 방식과의 차별성으로 채굴과 암호화폐(cryptocurrency) 발행과의 연관성을 말할 수 있다. 기존의 합의 알고리즘들은 노드들의 채굴 참여를 지속적으로

유지하기 위하여 채굴에 성공한 노드들에게 보상으로 암호화폐 발행 권한을 주는 방식이다.

그러나 deb 합의 알고리즘의 경우, 채굴과 암호화폐 발행과는 연관성이 없다. 즉, 채굴과 암호화폐 발행이 상호 무관한 최초의 퍼블릭 블록체인을 개발하기 위한 합의 알고리즘이다. 채굴자들에게 필요한 보상금을 암호화폐 발행 권한으로 주는 것이 아니고, 채굴에 참여하고자 하는 노드들로 구성될 유료 채굴리그의 참가비의 일부와 거래수수료로 보상해주는 방식이다. 이렇게 구성해야 하는 본질적인 이유는 지속가능한 탈중앙화를 위해서 노드들의 채굴 조건과 무관하게 만드는 것과도 연계된다. 즉, 채굴작업의 공정성을 확보하기 위하여 채굴과정이 모든 노드들에게 공정할 수 있도록 매우 저비용이기 때문에 고액의 보상체계가 필요하지 않다는 것이다.

특히, deb 합의 알고리즘의 경우 기존의 퍼블릭 블록체인과는 달리 포크(fork)가 발생하지 않는 장점 또한 지니고 있다. 이는 블록 생성이 바로 블록의 최종성(finality)을 보장하는 것이다.

2. 앤드어스체인의 비전과 목표

앤드어스체인의 비전과 목표는 원칙적으로 블록체인의 철학과 사상을 실현하는 퍼블릭 블록체인 이더리움의 비전과 목표와 동일하다. 그러나 합의 알고리즘의 원론적인 탈중앙화 문제를 해결하고 고성능의 차세대 이더리움을 실현하였다.

□ **비전**

√ 우리들이 만드는 공정한 고속 퍼블릭 블록체인 플랫폼

√ 공정하고 신뢰할 수 있는 세상 실현

□ **목표**

√ 암호경제 또는 블록체인 경제 실현

√ 편의성이 극대화된 dapp 생태계 구축 인프라

앤드어스체인 또한 이더리움과 같이 탈중앙화된 P2P 비즈니스 생태계를 위한 오픈된 블록체인 플랫폼이다. 즉, 이더리움이 가지고 있는 토큰 발행 기능, 스마트계약 기능, 스마트자산 기능 및 DAO 기능들을 모두 가지고 있다.

특히, 앤드어스 체인은 블록체인 기반 탈중앙화된 P2P 오픈생태계(dapp 생태계) 활성화를 위해 사용자들을 위한 편리한 생태계 지원 기능을 강화하였다.

□ **이더리움과의 차별화된 특징**

① 지속가능한 탈중앙화 특성이 유지되는 공정한 합의 알고리즘인 deb 합의 알고리즘 적용

② 채굴과 암호화폐 발행의 무 연계(즉, 채굴 기능에 암호화폐 발행 기능 없음)

③ 퍼블릭 블록체인 중 최고의 성능 : 1,000 TPS 이상

④ 포크가 발생하지 않아 블록 생성과 동시에 최종성이 보장

⑤ Dapp 서비스 생태계 지원 기능 강화

3. 합의 알고리즘의 공정성

앤드어스체인의 지속가능한 탈중앙화 특성을 설명하기 전에 먼저 합의 알고리즘의 공정성에 대해 설명하고자 한다.

deb 합의 알고리즘의 목적은 채굴을 원하는 노드들의 조건(컴퓨팅 파워, 보유 지분 등)과 상관없이 모든 노드들에게 공정한 채굴 확률을 보장함으로서 지속가능한 탈중앙화 특성을 유지하는 것이다.

이를 위해 먼저 합의 알고리즘의 공정성(fairness)을 정의하고 기존 퍼블릭 블록체인들의 공정성을 분석한다.

정의 : 합의 알고리즘의 공정성

> 합의 알고리즘의 공정성이란 노드들의 채굴 확률과 노드들이 가지고 있는 조건(컴퓨팅 파워, 지분 등)들과의 상관관계로 정의 한다.

예를 들어 비트코인과 이더리움에서 사용하는 작업증명 방식의 경우, 노드들의 채굴 확률은 노드가 보유한 컴퓨팅 파워에 위해 결정된다. 즉,

$$\text{노드의 채굴 성공 확률} = \frac{\text{자신이 보유한 컴퓨팅 파워}}{\text{전체 노드들이 보유한 컴퓨팅 파워의 합}}$$

작업증명 방식을 채택하고 있는 비트코인의 경우, 채굴공장 및 그룹의 탄생 등에 따라 일반적인 노드가 채굴에 성공할 확률은 거의 0에 가깝다. 이로 인해 비트코인은 중앙화되고 있다는 논쟁이 일고 있다.

그리고 이더리움에서 사용하게 될 지분증명 방식의 경우, 노드들의 채굴 확률은 노드가 보유한 지분에 의해 결정된다. 즉,

$$\text{노드의 채굴 성공 확률} = \frac{\text{자신이 보유한 지분}}{\text{암호화폐 총 발행량}}$$

지분증명 방식의 경우는 보유지분에 따른 채굴 확률이 결정됨으로 전형적인 자본의 논리가 적용된다는 문제점이 지적되고 있는 실정이다.

4. deb 합의 알고리즘

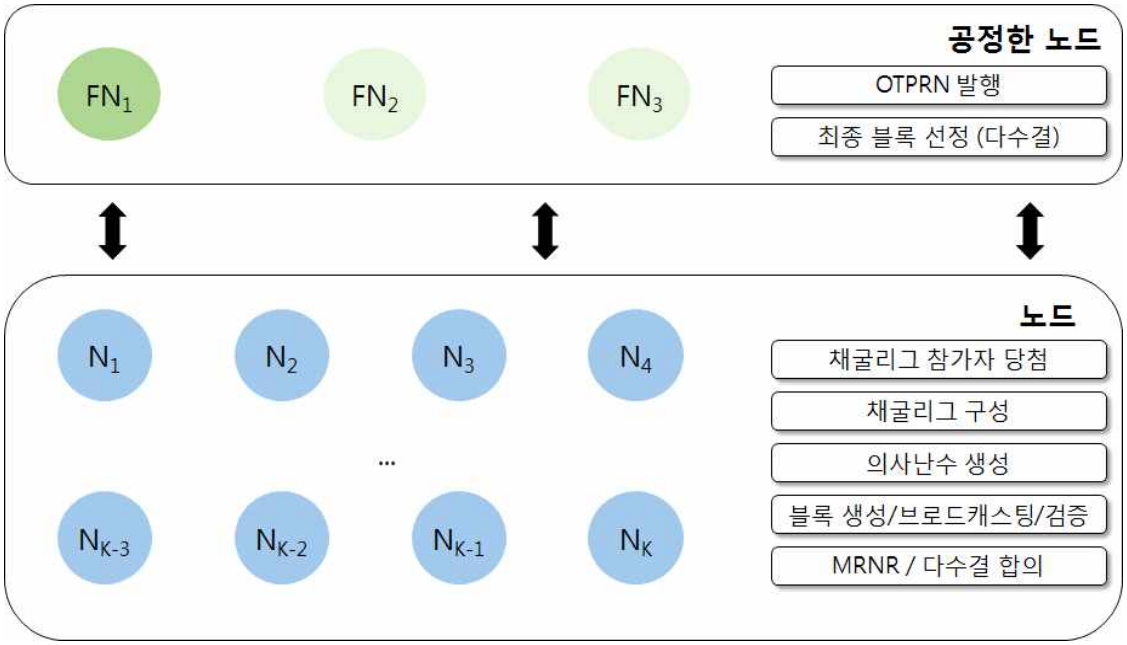
기존의 작업증명 및 지분증명 합의 알고리즘의 경우 채굴 노드가 가지고 있는 컴퓨팅 파워와 보유한 지분에 따라 채굴 노드의 채굴 확률이 비례하는 특성을 가지고 있으며, 이는 채굴 관점에서 블록체인에 참여를 원하는 채굴자들에게 공정(fairness)하지 않다는 것을 말해주고 있다.

deb 합의 알고리즘은 바로 이러한 공정하지 못한 문제점을 해결하여 공정한 채굴 기회를 보장하기 위한 합의 알고리즘이다. 먼저 공정한 채굴 기회를 보장하기 위해서는 채굴을 원하는 모든 노드들에게 주어진 조건(컴퓨팅 파워, 보유 지분 등)에 상관없이 공정한 채굴 기회를 주어야 한다.

이를 위해 deb 합의 알고리즘은 작업증명과 지분증명 방식과는 달리 공정한 노드(fairnode, 이하 혼용하여 사용)라는 개념을 도입한다. 물론 P2P 기반의 deb 합의 알고리즘의 특성을 유지하기 위해 공정한 노드의 신뢰성을 가정하지는 않는다. 즉, 공정한 노드는 제3의 신뢰기관(TTP:Trusted Third Party)은 아닌, 단지 P2P 네트워크의 노들들과 협력하여 합의 알고리즘을 지원하는 단순한 특별한 노드라고 생각하면 된다. 공정한 노드의 역할 및 안전성에 대해서는 추후 설명하기로 한다.

deb 합의 알고리즘은 유료 채굴 리그, 최대 난수 규칙(MRNR : Maximum Random Number Rule, 가장 큰 랜덤 넘버) 및 다수결 원칙 등 3가지 기본 원리로 작동된다. 유료 채굴 리그란 채굴을 원하는 노드들 중 특정 수(예, 100명)의 노드들로 구성된 채굴 노드들의 그룹이다. 물론 채굴 리그에 참여를 원하는 노드들은 채굴 리그에 참여하기 위해 현실적으로 충분히 가능한 적은 금액(예, 100원)인 참가비를 지불해야 한다. 그리고 유료 채굴 리그에 참여한 노드들로 구성된 그룹에서 각 노드가 블록을 생성하는 규칙이 최대 난수 규칙이다. 그리고 최종 채굴자를 결정하는 방식, 즉 최종 블록을 결정하는 방식은 공정한 노드와 채굴리그에 참여한 노드들간의 협력을 통한 다수결 원칙으로 이루어진다.

deb 합의 알고리즘의 전체 구성도는 다음과 같다.



(그림 4-1) 합의 체계 구성도

공정한 노드는 클러스터로 구성할 수 있다.

4.1 deb 합의 알고리즘 전체 프로세스

deb 합의 알고리즘의 전체 프로세스는 유료 채굴리그 구성, 블록 생성(채굴), 최종 블록 합의 등 크게 3단계로 구성된다.

□ 유료 채굴리그 구성

① 채굴을 원하는 노드는 공정한 노드에게 자신의 접속 정보를 제공한다.

② 공정한 노드는 채굴리그 구성을 위해 모든 노드들에게 $OTPRN$을 배포한다.

③ 채굴리그에 참여를 희망하는 노드는 공정한 노드가 배포한 $OTPRN$을 참조하여 본인이 채굴리그 참여 대상자인지를 판단한다.

④ 채굴리그 참여자로 선정된 채굴노드는 채굴리그 구성을 위해 $OTPRN$을 포함한 $JoinTx$를 생성한다.

⑤ 모든 노드들에게 $JoinTx$를 브로드캐스팅한다.

⑥ 채굴리그 참여자로 선정된 채굴노드들만 $JoinTx$를 참조한다.

□ **블록 생성 (채굴)**

① 채굴리그에 참여한 채굴 노드는 최종 블록 선정의 기준이 되는 $difficulty$를 생성한다.

- $difficulty = \{0 \le n \le JoinNonce \mid MAX(CSPRNG(n, OTPRN{\cdot}rand, coinbase, P\_BlockHash))\}$
  ※ 채굴 확률을 균등하게 하기 위해 채굴리그에 신청하였으나, 채굴자로 선정되지 못한 경우 선정되지 못한 경우만큼 복수의 $difficulty$ 생성

② 채굴 노드는 블록 헤더에 $difficulty$를 포함하여 블록을 생성한다.

③ 모든 노드에게 생성된 블록을 브로드캐스팅한다.

□ **합의 알고리즘**

블록 합의의 기본 원칙은 가장 큰 수($MRNR: Maximum\ Random\ Number\ Rule$, 가장 큰 랜덤 넘버) 규칙과 노드와 공정한 노드가 협력하여 다수결에 의한 최종 블록 합의 절차이다.

① 노드는 자신이 수신한 블록 중 $difficulty$가 가장 큰 블록을 선택한 뒤 서명하여 공정한 노드에 전송한다.

② 공정한 노드는 다수결 원칙에 따라 전송 받은 블록 중 가장 많은 선택된 블록을 최종 블록으로 결정하여 서명한 후 노드들에게 전송한다.

③ 채굴 노드는 공정한 노드로부터 수신한 블록이 다수에 의해 선택된 블록인지 검증한 뒤 전체 노드들에게 브로드캐스팅한다.

④ 각 노드들은 공정한 노드와 다수가 서명한 블록을 최종 블록으로 인지하고 블록체인에 추가한다.

4.2 유료 채굴 리그 구성 세부 프로세스

안전성 및 효율성을 위해 유료 채굴리그를 구성하는 방법은 공정한 노드와 노드들의 자체적인 인원 조정과 채굴리그 참여 신청으로 진행된다.

□ **유료 채굴리그 참여자 선정**

① 채굴을 원하는 노드는 공정한 노드에게 노드 정보를 제공한다.

<표 4-1> enodeCoinbase 구조체

필드명	설명
$enode$	채굴 노드의 enode 값
$coinbase$	채굴에 참여할 계정의 주소
$port$	공정한 노드와 통신할 포트 번호

② 공정한 노드는 블록 생성 주기에 따라 transOTPRN 구조체를 모든 노드에게 배포한다.

<표 4-2> transOTPRN 구조체

필드명	설명
$OTPRN$	채굴 노드들이 채굴 시 참조하는 구조체
Sig	$OTPRN$에 대한 공정한 노드의 서명

<표 4-3> OTPRN 구조체

필드명	설명
num	OTPRN 발행 번호
$rand$	공정한 노드가 주기적으로 배포하는 일회성 의사 난수
$CMiners$	채굴을 수행하기 위해 공정한 노드와 연결을 유지하고 있는 노드의 수
$Timestamp$	공정한 노드의 로컬 시간

③ 채굴 후보 노드들은 공정한 노드가 배포한 $OTPRN$ 구조체를 참조하여 자신이 참가할 수 있는지 파악한다.

(ㄱ) 최대 채굴 참여 인원수를 정의한 시스템 설정 변수 $MMiners$를 제수로 설정

(ㄴ) 채굴 노드는 공정한 노드가 전파한 $OTPRN$ 구조체 중 채굴 의사를 밝힌 전체 채굴 노드 수를 나타내는 $CMiners$를 피제수로 설정

(ㄷ) 두 값을 연산하여 얻은 몫을 Div로 설정

$$Div = CMiners \div MMiners$$

(ㄹ) $enodeCoinbase.coinbase$와 $OPTRN.rand$의 XOR 연산의 합을 랜덤 함수의 시드(SEED)로 사용하여 랜덤 값 도출

$$rand = RAND(\sum_{i=0}^{19}(enodeCoinbase.coinbase[i] \oplus OPTRN.rand[i]))$$

※ $RAND$는 랜덤 함수

(ㅁ) $rand$를 div와 모듈러 연산하여 다음과 같은 조건이 충족될 때 채굴 참여가 가능하다고 판단함

$rand \ \% \ div \ == \ 0$ → 가능

□ **유료 채굴 리그 구성**

① 채굴리그에 참가 가능한 채굴노드는 $OTPRN$ 구조체를 포함한 $JoinTx$를 생성하여 모든 노드들에게 브로드캐스팅 한다.

※ $JoinTx$: 노드가 채굴리그에 참여하고자 할 때 발생시키는 채굴리그 참여 신청 트랜잭션

<표 4-4> JoinTx 구조체

필드명	설명
Tx	아래의 필드를 제외하고 이더리움 트랜잭션 구조체와 동일 · $to : Fairnode's\ address$ · $data : JoinTxData$

<표 4-5> JoinTxData 구조체

필드명	설명
$JoinNonce$	계정의 $JoinNonce$에 1을 더한 값
$OtprnHash$	공정한 노드로부터 수신한 $OTPRN$의 해시 값
$FairNodeSig$	$transOTPRN.sig$
$Timestamp$	채굴 노드의 로컬 시간
$NextBlockNum$	채굴할 블록의 번호

② 채굴리그에 참여한 채굴노드들만 $JoinTx$를 수집한다.

③ 채굴노드는 수집한 $JoinTx$를 목록화하여 각자의 채굴리그를 구성한다.

4.3 블록 생성 프로세스 : 채굴 프로세스

공정하고 효율적인 채굴을 위해 공정한 노드와 의사난수($difficulty$)를 활용한다.

□ **Difficulty 생성**

① 채굴 노드는 참여자 선정 과정에서 공정한 노드로부터 받은 OTPRN 구조체를 참조하여 $difficulty$를 생성한다.

$$difficulty = \{0 \le n \le JoinNonce \mid MAX(CSPRNG(n, OTPRN.rand, coinbase, P\_BlockHash))\}$$

※ $JoinNonce$: $JoinNonce$의 다른 목적으로, 채굴노드가 채굴리그에 참여한 만큼 채굴 확률을 높여주는 기능을 수행함. 이와 같은 목적을 달성하기 위해 $JoinNonce$ 수만큼 다른 $difficulty$를 생성할 수 있고 그 중 가장 큰 값을 블록 생성에 사용할 수 있음.

※ $OTPRN.rand$: 공정한 노드가 배포한 일회성 의사난수로 채굴노드가 $difficulty$를 생성함에 있어 채굴에 유리한 값을 임의로 생성할 수 없도록 함

※ $coinbase$: 채굴노드가 채굴할 때 사용하는 주소로 채굴 노드별로

$difficulty$를 다르게 생성하게 하기 위함

※ $P\_BlockHash$: 이전 블록의 해시 값으로 (i) 공정한 노드가 특정 채굴 노드에게 유리한 $OTPRN.rand$를 배포할 때를 대비하고 (ii) 채굴 노드가 특정 블록에 종속된 하나의 $difficulty$를 생성하도록 하기 위함

② 채굴노드는 자신이 생성한 $difficulty$ 중 가장 큰 $difficulty$를 선택하여 트랜잭션을 생성한다.

$difficulty = MAX(\{difficulty_n\}\ _{0 \le n \le JoinNonce})$

□ 블록 생성 및 브로드캐스팅

① 채굴 노드는 자신의 블록 헤더에 $OTPRN.rand$와 기타 데이터를 참조하여 난수를 생성한 뒤 해당 난수와 자신의 $JoinNonce$를 블록 헤더에 기록한다. 블록 내에 존재하는 $FairNodeSig$와 $Voters$는 향후 공정한 노드에 의해 기록된다.

<표 4-6> 블록 구조체 (아래 필드를 제외하고 이더리움과 동일)

구분	필드명	설명
$Header$	$UncleHash$	제거
	$JoinTxHash$	$JoinTx$ 리스트 해시 값
	$GenTxHash$	Tx 리스트 해시 값
	$JoinReceipt Hash$	$JoinTx$의 receipt 해시 값
	$GenReceipt Hash$	Tx의 receipt 해시 값
	$Difficulty$	채굴 노드가 공정한 노드로부터 수신한 $OTPRN.rand$을 활용하여 생성한 난수 값
	$nonce$	채굴 노드의 $JoinNonce$ 값
	$FairNodeSig$	공정한 노드가 다수의 채굴 노드들이 선택한 블록과 증명 데이터를 포함하여 서명한 값
	$VoterHash$	$Voters$ 해시 값
$Body$	$JoinTxs$	Tx 목록
	$GenTxs$	$JoinTx$ 목록
	$Voters$	해당 블록에 투표한 노드들의 주소와 서명 (복수)

<표 4-7> Voters 구조체

필드명	설명
$addr$	해당 블록에 투표한 채굴 노드의 주소
sig	채굴 노드의 서명
$difficulty$	채굴 노드 자신이 생성한 $difficulty$ 값으로 향후 다수결에 의해 선택된 $difficulty$가 올바른지 검증할 때 사용

② 채굴노드가 수집한 각종 트랜잭션을 블록에 포함한 뒤 블록 생성한다.

③ 채굴노드는 생성된 블록을 다른 채굴 노드들에게 브로드캐스팅한다.

4.4 합의 알고리즘

블록 합의는 기본적으로 $MRNR$과 다수결 원칙에 기반한다. 즉, 최초에 채굴 노드들끼리 각자 생성한 블록을 브로드캐스팅 한 뒤, 자신에게 수신된 블록 중 가장 큰 $Difficulty$가 지정된 블록을 선택($MRNR$)한 뒤 서명하여 공정한 노드에게 전송한다.

공정한 노드는 자신이 수신한 블록 중 다수의 채굴 노드들이 선택한 블록을 선정(다수결 원칙)하여 채굴 노드들의 주소와 서명을 블록 내에 포함시킨 뒤 자체 서명한다. 그리고 공정한 노드가 해당 블록을 채굴 노드들에게 전파하면 채굴 노드들은 해당 블록이 다수결 원칙에 부합하는지, 공정한 노드가 서명했는지 등을 검증한 뒤 원장에 추가한다. 이로써 해당 블록은 최종 블록으로 결정되고, 채굴 노드들은 해당 블록을 네트워크에 전파한다.

□ 유효성 검증 단계

① $OTPRN$ 전파 주기와 블록 생성 주기가 일치하는지 확인한다.

② $OTPRN$ 무결성 및 공정한 노드의 서명을 검증한다.

③ 채굴한 노드가 채굴 리그 참가 가능 대상자인지 확인한다.

④ 채굴 노드가 채굴 리그 참가비를 지불할 수 있는 지 확인한다.

⑤ $Difficulty$가 올바르게 생성되었는지 확인한다.

□ 블록 합의

① 채굴 노드는 수신한 블록 중 $Difficulty$가 가장 큰 블록을 선택($MRNR$)하여 서명한 뒤 공정한 노드에 전송한다.

② 공정한 노드는 전송 받은 블록 중 다수결 원칙에 따라 다수에 의해 선택된 블록을 최종 블록으로 결정하여 서명한 후 노드들에게 전송한다. 향후 검증을 위해 공정한 노드는 해당 블록에 투표한 채굴 노드들의 주소와 서명을 블록에 포함시킨 뒤 서명한다.

③ 공정한 노드는 해당 블록을 채굴 노드들에게 브로드캐스팅한다. 채굴 노드들은 수신한 블록이 다수결 원칙에 부합하는지, 공정한 노드의 서명이 포함되었는지를 검증한 뒤 자신의 원장에 추가하고 해당 블록을 브로드캐스팅한다.

④ 마찬가지로, 위 블록을 수신한 일반 노드들(채굴에 참여하지 않은 노드들)도 채굴 노드들이 수행한 방식과 동일한 검증 절차를 거친 뒤 해당

블록을 원장에 추가한다.

⑤ 채굴자는 아래와 같이 인센티브를 제공받는다.
인센티브 = 트랜잭션 수수료 + 채굴리그 참가자 전체 참가비

⑥ 채굴리그 참가자들의 채굴 확률을 조정한다.
- 채굴 성공 노드 : $Tx.Join\_Nonce = 0$
- 채굴 실패 노드 : $Tx.Join\_Nonce = Tx.Join\_Nonce + 1$

4.5 공정한 노드의 역할 및 공정성

비트코인 및 이더리움의 합의 알고리즘은 공정한 노드 개념을 사용하지 않는다. 그러나 deb 합의 알고리즘의 경우 지속가능한 탈중앙화 특성을 유지하기 위해 공정한 노드 개념을 도입하였다. 물론 deb 합의 알고리즘이 동작하기 위해서 공정한 노드의 신뢰성을 가정하지 않는다.

공정한 노드는 유료 채굴리그 구성의 효율성, 블록 합의 및 최종성 협력을 위한 역할만을 담당한다.

□ **공정한 노드의 역할**

① 유료 채굴리그 참여자의 랜덤한 선정

② 노드들과의 상호 견제를 통한 최종 블록 합의 협력

가장 중요한 것은 deb 합의 알고리즘은 공정한 노드의 신뢰성에 의존하지 않는다. 공정한 노드와 블록체인 노드들간의 상호 견제를 통해 공정한 노드의 신뢰성 보장 없이도 블록체인의 안전성을 확보할 수 있다.

공정한 노드를 이용하여 deb 합의 알고리즘의 공정성은 다음과 같이 생각할 수 있다.

$$\text{노드의 채굴 확률} = \frac{1}{\text{채굴 희망 전체 노드수}}$$

4.6 성능

deb 합의 알고리즘의 성능은 유료 채굴리그 구성 수와 블록생성 주기 등에 따라 동적으로 결정될 수 있다.

예를 들어, 채굴 리그 인원 수 100명인 경우 예상되는 성능은 다음과 같다.

<표 4-8> deb 합의 알고리즘의 성능

	deb 합의 알고리즘
Block Size	4.5MB ~ 9MB
TPS	1000 TPS
생성주기	10초 ~ 1분

특히, 블록 생성 시간을 줄이기 위해 공정한 노드와 유료 채굴 리그 노드들 간의 네트워크 접속부하를 줄이면 블록 생성 시간을 더욱 단축할 수 있다. 일례로 한번 구성된 유료 채굴 리그의 블록 생성 숫자를 10개로 한다면 블록 생성 시간은 10초 이내로 단축할 수 있을 것이다.

4.7 deb 합의 알고리즘 특징

deb 합의 알고리즘의 목적은 현재의 합의 알고리즘의 불공정성으로 인해 발생할 수 있는 블록체인 합의 알고리즘의 중앙화 문제를 해결하는 것이다. 즉, 기존의 합의 알고리즘인 작업증명 방식, 지분증명 방식과 deb 합의 알고리즘의 가장 큰 차이점은 지속가능한 탈중앙화를 유지할 수 있다는 것이다. 이는 채굴을 원하는 노드들의 조건들에 의존하지 않는 공정한 합의 알고리즘이라는 것을 의미한다.

또한 기존의 퍼블릭 블록체인의 합의알고리즘의 경우 블록을 생성하는 채굴과 암호화폐 발행이 연계되어 있으나, deb 합의 알고리즘의 경우 채굴과 암호화폐 발행이 무관하다는 것이다. 즉, 초기 발행한 암호화폐 발행량이 바로 총 통화량이 된다는 것을 의미한다.

이는 암호화폐 발행 권한을 독점하면서도 퍼블릭 블록체인을 구성할 수 있게 하는 최초의 합의 알고리즘이다.

한편으로 deb 합의 알고리즘의 장점으로는 포크(fork)가 일어나지 않아 최종성이 1블록이면 달성되는 장점이 있다.

□ deb 합의 알고리즘 특징

① 지속가능한 탈중앙화 특성 유지 (공정성)

② 채굴과 암호화폐 발행 무관 (암호화폐 발행 독점 가능)

③ 포크 없는 1블록의 최종성 보증

④ 1,000 TPS 이상의 고속 성능

5. 앤드어스체인(AndUschain)

앤드어스체인은 본질적으로 이더리움에 기반하기 때문에 이더리움의 아키텍쳐 등 대부분은 이더리움과 동일하며, 지속가능한 탈중앙화 특성을 유지하기 위해 합의 알고리즘을 개선하였다고 보면 된다. 본 장에서는 기존 이더리움에서 수정된 부분과 개인정보보호 측면을 주로 다룬다.

5.1 이더리움 수정 영역

deb 합의 알고리즘을 적용하기 위하여 수정된 부분들을 정리하면 다음과 같다.

□ 계정(Account) 상태

○ $JoinNonce$ 추가
√ 채굴 리그에 참여할 때마다 증가되는 값으로 증가된 값만큼 채굴 확률을 높여주어 자발적인 채굴 리그 참여를 유도

□ 거래(Transaction) 구조체 : JoinTx 타입

○ to 수정
√ $JoinTx$는 to필드를 공정한 노드의 주소로 대체함

○ $JoinNonce$ 추가
√ 채굴 노드가 전송한 $JoinTx$의 수 (채굴 성공 시 초기화)

○ $OtprnHash$ 추가
√ 공정한 노드로부터 수신한 $OTPRN$의 해시 값

○ $FairNodeSig$ 추가
√ 공정한 노드가 전송한 transOTPRN 구조체에 포함된 서명 값

○ $Timestamp$ 추가
√ 채굴 노드의 채굴 시 로컬 시간

○ $NextBlockNum$ 추가
√ 채굴할 블록 번호

□ 블록(Block) 구조체

○ $JoinTxHash$ 추가
√ $JoinTx$ 리스트의 해시 값

○ $JoinReceiptHash$ 추가
√ $JoinTx$의 receipt 해시 값

○ $difficulty$ 수정
√ 공정한 노드가 배포한 OTPRN 구조체로 채굴 리그에

필요한 정보를 포함

○ $nonce$ 수정

√ 채굴 노드의 $JoinNonce$ 값

○ $FairNodeSig$ 추가

√ 공정한 노드가 다수의 채굴 노드들이 선택한 블록과 증명 데이터를 포함하여 서명한 값

○ $votersHash$ 추가

√ $voters$ 해시 값

○ $uncleHash$ 제거

√ 포크가 발생하지 않기 때문에 $uncle$ 블록이 생성되지 않으므로 해당 필드는 불필요함

○ $mixHash$ 제거

√ Pow 합의 알고리즘을 사용하지 않기 때문에 해당 필드는 불필요함

○ $voters$ 추가

√ 블록에 투표한 노드들의 주소와 서명

○ $JoinTxList$ 추가

√ $JoinTx$ 목록

특히, 앤드어스체인은 deb 합의 알고리즘을 활용함으로서 현재까지 제안된 퍼블릭 블록체인 중 지속가능한 탈중앙화를 유지하면서도 성능이 가장 우수하다.

<표 5-1> 주요 퍼블릭 블록체인 성능 비교

	비트코인	이더리움	앤드어스 블록체인
합의 알고리즘	작업증명	작업증명	deb 합의 알고리즘
TPS	7	12~15	1,000 이상
최종성	10분	약 3분	10초 ~ 1분

결론적으로 앤드어스체인은 deb 합의 알고리즘을 기반으로 진정한 의미의 우리 모두가 공정한 조건에서 모두 동일한 채굴 확률을 갖게 되는 지속가능한 탈중앙화를 유지하는 우리가 함께 만드는 고속 퍼블릭 블록체인이이라 할 수 있다.

5.2 개인정보보호 등 정보보호 기능

정보보호 기능은 이더리움에 내장된 기능을 사용한다. 이더리움 내에 존재하는 정보보호 기능은 크게 P2P 암호화 통신과 영 지식 증명 데이터를 검증할 수 있는 내장된 스마트 컨트랙트를 통해 이루어진다.

□ 전송 구간 암호화

이더리움의 P2P 네트워크를 구성하는 프로토콜 집합을 "devp2p"라고 한다. Devp2p는 블록체인에서만 사용되는 것이 아닌 이더리움과 관련된 모든 네트워크 응용 프로그램에서 사용될 수 있도록 고안되었다. 이는 네트워크에 존재하는 다른 노드들을 탐지하고 트랜잭션과 블록 등을 교환할 때 사용된다.

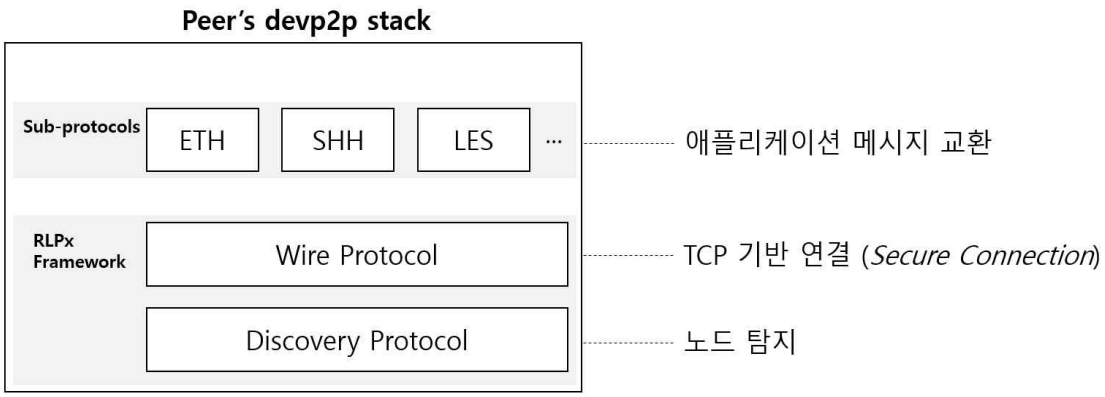
Devp2p는 아래와 같이 두 계층으로 구성되어 있다.

○ RLPx 프레임워크

√ 노드 간 통신을 가능하게 한다. 해당 프레임워크는 다른 노드를 탐지하는 Discovery 프로토콜과 각 노드들이 서로 암호화되고 인증된 연결을 맺을 수 있도록 해주는 Wire 프로토콜로 나뉠 수 있다.

○ 사용자 영역의 하위 프로토콜

√ Ethereum(ETH), Whisper(SHH), Swarm(BZZ), Light Client Protocol(LES) 등이 포함된다.

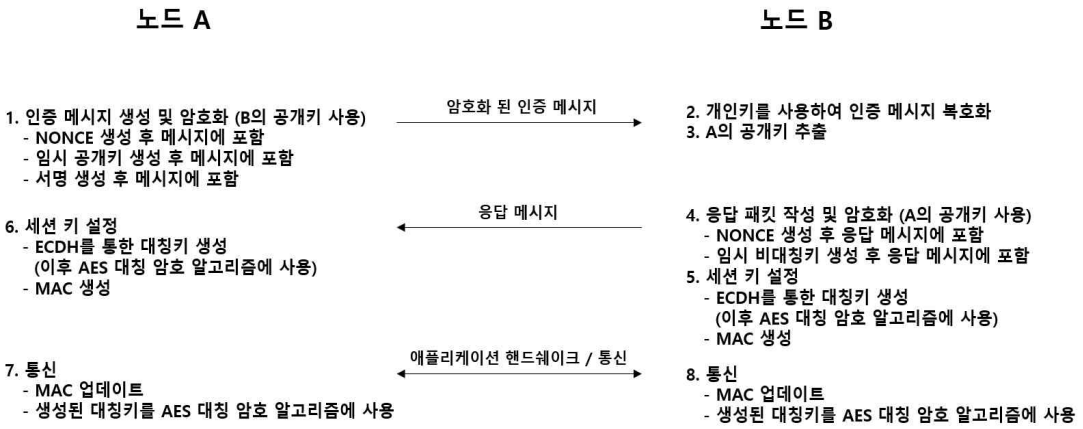


(그림 5-1) DEVP2P STACK

여기서 우리가 다룰 부분은 devp2p 프로토콜이 제공하는 통신구간 암호화 방법이다. Devp2p 프로토콜은 통신구간 암호화를 위해 핸드쉐이크 과정에서 "Elliptic Curve Diffie Hellman(ECDH)" 키 교환 프로토콜을 사용하여 데이터 암호화에 사용될 키를 생성한다. (그림 5-2)를 간략히 설명하자면 다음과 같다.

최초 세션을 연결하고자 하는 노드 A는 인증 메시지(수신자인 노드 B의 공개키를 사용하여 인증 데이터를 암호화 함)를 생성한다. 인증 메시지에는 노드 A의 개인키와 노드 B의 공개키를 통해 생성된 공유 비밀 데이터와 논스의 XOR 연산 데이터, 임시 공개키 등을 포함한다. 이를 수신한 노드 B는 자신의 개인키로 데이터를 복호화 한 뒤 A의 임시 공개키를 추출한다. 노드 B는 수신한 인증 데이터에 대한 응답 메시지(노드 A의 공개키를 사용하여 응답 메시지를 암호화 함)를 생성한다. 응

답 메시지에는 노드 B의 임시 공개키와 논스 등이 포함되어 있다. 메시지 교환이 완료되면 노드 A와 노드 B는 서로의 임시키를 기반으로 ECDH 알고리즘을 통해 새로운 비밀 공유 데이터를 생성하고, 해당 값에 추가 연산을 진행하여 대칭키를 추출하게 된다. 이렇게 생성된 대칭키는 통신 과정에서 데이터를 암호화하는 데 사용된다. 추가로 상대방이 생성한 논스와 자신이 생성한 논스, MAC 용 비밀 데이터 등의 연산을 통해 MAC(Message Authentication Code)을 생성한 뒤 데이터를 교환할 때마다 추가하여 메시지 인증을 동시에 진행한다.



(그림 5-2) 통신 구간 암호화

앤드어스 체인 역시 devp2p 프로토콜을 사용하여 안전한 통신구간 암호화를 가능하게 한다.

□ 개인정보보호 (영 지식 증명)

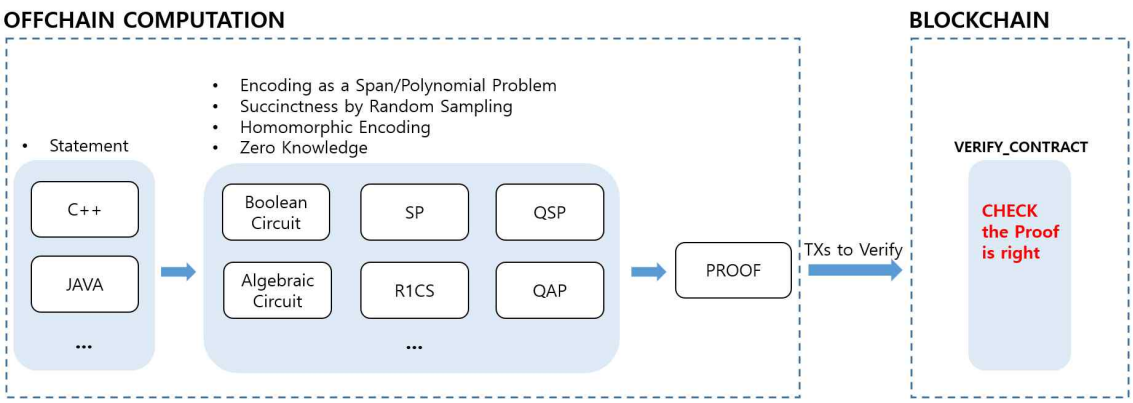
블록체인 원장에 기록된 정보는 일반적으로 삭제가 불가능하고 모두 공유되기 때문에 개인정보를 평문으로 저장하는 것은 바람직하지 않다. 이더리움은 블록체인의 이와 같은 특성 때문에 특별한 컨트랙트를 제공한다. 해당 컨트랙트는 이러한 특성을 보완하여 개인정보보호 기능을 블록체인 네트워크 내에서 제공하기 위해 미리 컴파일되어 제공된다.

이더리움에서 사용되는 개인정보보호 기법은 영 지식 증명의 한 방식인 zk-SNARKs를 사용한다. 이는 특정 정보를 원장에 직접적으로 저장하는 대신 증명할 수 있는 방식으로 변환하여 저장한다. 이렇게 변환된 데이터(증명 데이터)로부터 원본 데이터를 추출하는 것은 현실적으로 매우 어렵기 때문에 증명 데이터를 원장에 기입해도 특정 정보의 기밀성을 보장할 수 있다(물론 새로운 기술과 알고리즘의 발전 가능성으로 인해 먼 미래에도 동일한 수준으로 기밀성이 보장된다고 장담할 순 없다). 검증자는 이렇게 생성된 증명 데이터를 이더리움에서 제공하는 컴파일된 컨트랙트

를 사용하여 검증할 수 있다.

단, 증명 데이터를 생성하는 과정은 계산 집약적이며 개인 정보를 노출할 수 있는 위험을 가지고 있기 때문에 블록체인 상에서 수행하지 않는다. 오직 생성된 데이터를 검증하는 절차만 블록체인 상에서 진행된다. (그림 5-3) 이러한 과정을 설명한다.

간략히 (그림 5-3)에 대해 설명하자면 다음과 같다. C와 같은 상위 수준의 언어를 분해/재조립하여 zk-SNARK에 적합하게 표현한다. 해당 표현식이 참임을 증명하고자 하는 증명자는 zk-SNARK에 적합하게 표현된 식(계산/조건 등)을 참으로 만들 수 있는 데이터로 증명 데이터를 생성한다. 증명 데이터를 생성할 때에는 이더리움에서 제공한 공개 파라미터를 활용한다. 이렇게 생성된 증명 데이터는 검증 컨트랙트(VERIFY_CONTRACT)에 증명 데이터를 전송하여 검증을 수행한다(OFFCHAIN으로도 검증은 가능함). 검증 컨트랙트는 이더리움에서 제공하는 컴파일된 컨트랙트를 활용하여 구현된다.

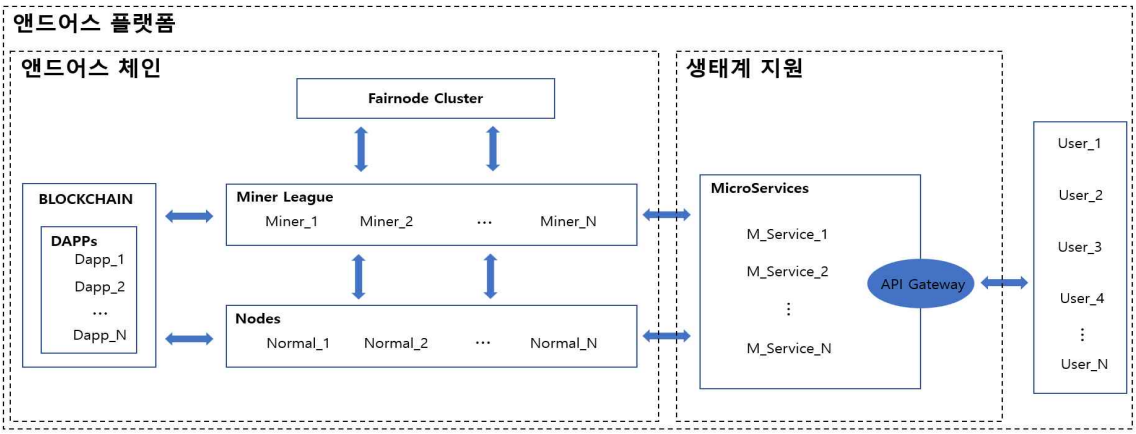


(그림 5-3) zk-SNARK 진행 과정

앤드어스 체인 역시 위와 같은 형태로 사용자의 개인정보를 보호한다.

6. 앤드어스 생태계 지원을 위한 주요 기능 제공

앤드어스 체인은 사용자들이 다양한 측면에서 서비스를 누릴 수 있도록 하기 위해 생태계 지원 계층을 마련하였다. 우리는 앤드어스 체인과 생태계 지원 계층을 혼합한 형태를 앤드어스 플랫폼이라 한다. 즉, 앤드어스 플랫폼 사용자는 블록체인에 국한된 서비스만을 받는 것이 아닌 여러 기술이 융합된 서비스를 제공받을 수 있을 것이다.



(그림 6-1) 앤드어스 플랫폼 구성도

물론 서비스 제공자의 역할을 앤드어스가 독점하는 것은 아니다. 원하는 사용자는 누구나 앤드어스 플랫폼에서 서비스 제공자로서 역할을 수 있다. 서비스 제공자는 크게 Dapp과 마이크로 서비스 형태로 서비스를 제공할 수 있다. 그 뿐만 아니라 한 서비스 제공자는 다른 서비스 제공자가 제공한 Dapp과 마이크로 서비스를 자신이 제공하고자 하는 서비스에 혼합하여 보다 풍부한 기능을 가진 서비스를 제공할 수 있다. 서비스 제공자는 자신이 제공한 서비스의 이용 요금을 제시하고 이에 따른 수익을 얻을 수 있을 것이다.

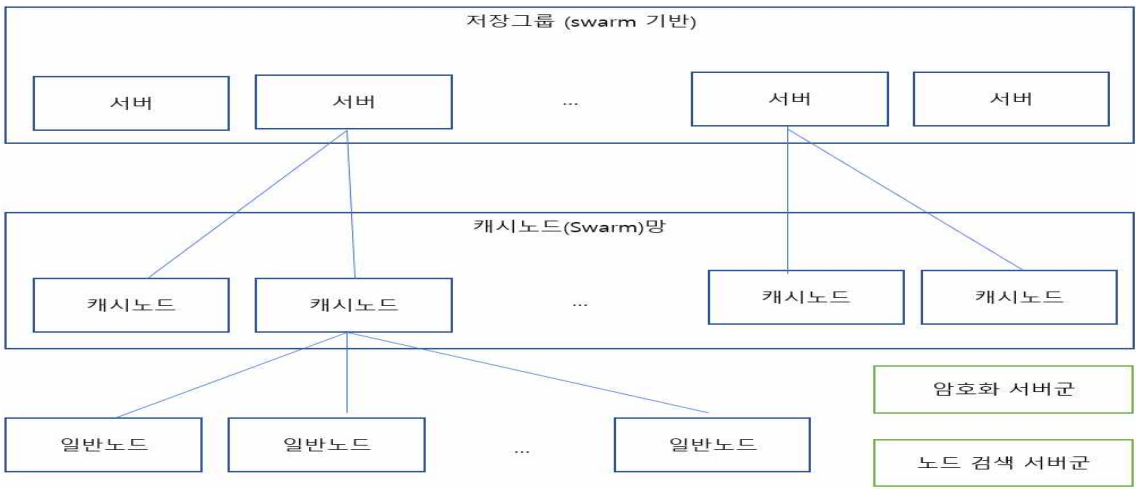
여기에서는 앤드어스에서 제공하는 빅데이터를 통해 생태계를 지원하는 방식을 설명하고자 한다.

6.1 빅데이터

기존 이더리움은 데이터 저장소로 Swarm을 제안하였고, 그 외 분산 저장소로는 IPFS가 인기를 끌고 있다. 하지만 두 저장소는 자료를 저장 및 관리하는 것에 따른 인센티브 규정이 미흡하다. 이 뿐 아니라 공유 유지, 안정성, 보안성, 삭제 방법 등 다양한 분야에서 실제 서비스로 사용할만큼 충분치 않다. 따라서 우리 앤드어스 체

인은 자료 저장을 위한 새로운 저장 메커니즘을 제안하고자 한다.

제안된 저장 메커니즘은 이더리움 Swarm을 기반으로 하여 저장소와 암호 전용 서버, 동작하고 있는 노드를 효율적으로 검색할 수 있는 노드 검색 서버가 추가된 구조를 가진다. 또한 별도의 삭제 풀(pool)을 관리하여, 해당 풀에 해시가 등록되면 삭제된 것으로 판단하여 다운로드가 중지된다. 삭제 풀에 해시를 등록할 수 있는 사용자는 최초 자료를 업로드한 사용자만 가능하다.



(그림 6-2) 생태계 지원 : 빅데이터 서비스 구성도

□ 빅데이터 서비스 구성도 설명

- 일반 노드는 노드 검색 서버를 통하여 자신과 인접한 캐시 노드를 찾고, 캐시 노드를 사용하여 자료를 저장 및 조회한다.
- 노드 검색 서버는 활성화된 캐시 노드들을 관리하며, 일반 노드가 요청시 Kademlia 알고리즘을 이용하여 요청 노드와 가장 근접한 캐시 노드를 알려준다.
- 캐시 노드는 일반 노드의 요청을 자신이 직접 처리할 수 있는 경우 직접 처리함(요청받은 캐시 노드가 자료를 관리하는 경우)
- 캐시 노드는 일반 노드의 요청을 자신이 직접 처리할 수 없는 경우 이웃한 캐시 노드에 요청하여 일반 노드의 요청을 처리한다(요청받은 캐시 노드가 자료를 직접 관리하지 않은 경우).
- 저장 그룹의 서버는 자료 저장을 책임지며, 저장 그룹 내 서버들 간에는 Swarm 프로토콜을 이용하여 자료를 관리한다.
- 암호화 서버는 일반 노드에서 자료를 저장 및 조회하는 경우, 자료의 암·복호화를 담당한다.

- 삭제 풀은 머클트리 형태로 구성되며, 삭제할 자료의 해시를 기록하여 풀에 등록된 자료의 경우 다운로드가 중지시키며, 중지가 완료되면 가비지 컬렉터에 의해 저장된 자료는 자동 삭제된다.

□ 저장소 구조

- 기존 Swarm 데이터 구조

<표 6-1> 기존 Swarm 데이터 구조체

필드	설명
Chunk	최대 4KB 크기의 데이터로 구성되며, 자료를 저장하거나 조회하기 위한 기본 단위임
Reference	저장된 파일을 조회하기 위해 유일하게 할당된 값. 기본적으로 Swarm은 암호화 된 파일 형태로 저장되기 때문에 32바이트의 컨텐츠 주소와 32바이트의 복호화 키를 포함한 128바이트로 구성됨. 생성되는 암·복호화 키는 시스템에서 자동으로 생성되어 해당 필드에 복호화키를 저장시킴.
Manifest	파일 저장소를 나타내기 위한 데이터 구조체로서 URL 형태로 자료를 검색하기 위한 용도로 사용됨(파일명과 실제 위치를 표시하는 해시로 구성).

- 파일 저장 시 "manifest"를 생성하고 해당 위치를 지정하는 해시를 블록체인에 저장하는 트랜잭션을 생성한다.

- 트랜잭션 구조체

<표 6-2> Swarm 용 트랜잭션 구조체

필드	설명
Receiver	저장소
ExData	Manifest의 해시가 기록됨

- 개인용 파일의 경우 Manifest의 내용을 저장 노드의 개인키로 복호화할 수 있게 저장한다.

- 자료의 공개 정책(공개용, 개인용, 허가용)에 따라 자료의 암호화는 Swarm 자체 암호화와 관계없이 별도 암호화 서버군을 사용하여 일반 노드에서 암·복호화를 진행한다.

- 자료가 저장소로 업로드되면 해당 자료는 "chunk" 단위로 분해되며, 각 chunk는 chunk 해시를 통해 접근할 수 있다.

- Chunk 해시를 사용하여 머클 트리를 구성한다.

- 캐시노드 검색시 전달되는 컨텐츠를 캐싱하여 요청 빈도가 높은 컨텐츠의

접속 시간을 최소화한다.

- 이더리움의 Swarm과 가장 큰 차이점은 자료의 보관 기간과 별도의 암호화 서버군이 존재하는 것으로 이더리움의 경우 접근 빈도가 낮은 자료는 Swarm에서 자동으로 삭제되지만 본 서비스는 보관 기간이 만료될 때까지 유지하며 별도의 암호화 서버군이 자료의 암호화를 책임지는 역할을 한다.

□ 캐시노드 및 저장서버

- 기본적으로 이더리움의 Swarm 프로토콜을 사용한다.
- 업로드된 자료는 캐시노드에서 chunk 단위로 분해되어, chunk 해시를 기준으로 동일한 주소공간에 있는 다른 노드에 배포된다.
- 캐시노드는 저장서버 한 대 이상과 상시 연결되어 있으며, chunk로 분해된 자료는 chunk 단위로 캐시노드 간 동기화되는 것 이외에 저장서버로 전송된다.
- 저장서버는 캐시노드와 달리 모든 청크를 저장하며 저장서버들끼리 서로 동기화함으로써 자료를 유지/보관한다.
- 업로드된 자료는 캐시노드에서 chunk 단위로 분해되어, chunk 해시를 기준으로 동일한 주소공간에 있는 다른 노드에 배포된다.

□ 자료 보안

- 일반 노드는 자료를 저장할 때 공개 정책(공개용/허가용/개인용)을 설정할 수 있다. 일반 노드는 저장된 자료를 조회할 수 있도록 해시를 트랜잭션에 포함하여 블록체인에 저장하고 해당 트랜잭션의 해시를 통해 자료를 조회할 수 있도록 한다.
- 개인용으로 지정된 경우에는 저장 시 자료를 저장한 노드의 공개키로 암호화하여 개인키를 소유한 노드만이 조회할 수 있도록 한다.
- 허가용의 경우에는 암호화 서버에서 임의의 키를 생성한 후 자료를 암호화하고 해당 내용을 조회할 수 있는 API를 제공한다. 해당 API 정보는 저장 노드의 공개키로 암호화하여 블록에 저장하는 방식으로 제공한다. 해당 노드는 개인키로 해당 정보를 복호화하여 API 정보를 확인한 후 정보를 조회할 수 있다.
- 공개용의 경우 별도의 암호화 처리 없으 그대로 저장한다.

□ 가상 네트워크의 거리

- P2P 환경에서는 노드 간 물리적 거리를 측정할 수 없기 때문에, 가상의 네트워크를 상정하고 거리를 측정한다. 본 서비스는 이와 같은 방식으로 거리를 측정하는 알고리즘 중 하나인 Kademlia 알고리즘을 사용하여 계산한다.
- 가상 네트워크의 거리 계산은 노드의 주소를 기반으로 비트 단위 XOR 연산을 하여 나온 값을 빅 엔디언으로 변환하여 얻을 수 있다.
  - ✓ 최대 거리(M) : 주소의 자리수가 N인 경우 최대 N
  - ✓ 노드 간의 거리(D) : 두 노드의 주소 값을 XOR 나온 값의 로그 값 ($\log_2 D$)
  - ✓ 근접도 : 최대 거리에서 노드 간 거리를 뺀 값 (M-D)

□ 인센티브(수수료) 규정

- 사용자가 빅데이터 서비스를 사용하고자 할 때, 저장 파일의 크기에 비례하여 수수료를 지불한다. 해당 수수료는 캐시 노드에 일정 비율로 분배되고 나머지는 주기적으로 저장 그룹의 서버들에게 분배된다.
- 사용자가 서비스를 사용하는 기간은 기본 1년으로 설정되며 저장 서버 그룹은 해당 기간 동안 책임지고 보관한다. 기본으로 설정된 기간을 초과할 경우 1년 단위로 갱신 가능하며 그 때마다 추가 수수료를 지불해야 한다. 해당 수수료 역시 저장 서버 그룹에 분배된다.
- 사용자는 자료 저장 시, 해당 자료에 접근하는 다른 사용자에 대해 조회 수수료(유/무료)를 설정할 수 있다. 만약 조회 수수료가 유료로 설정되면, 자료 조회시 지불되는 수수료는 캐시 노드에 일정 비율로 분배하고, 남은 금액은 자료를 업로드한 사용자에게 분배한다.
- 캐시노드에 분배되는 조회 수수료는 자료의 저장 위치와 관계없이 요청에 응답한 캐시노드에게 지급된다.

6.2 인공지능

※ 백서 0.8 버전에서 공개 예정

7. 양질의 일자리 창출을 위한 저비용 창업생태계

앤드어스체인의 가장 중요한 목적은 지속가능한 탈중앙화된 P2P 기반 서비스를 구축할 수 있는 플랫폼을 제공하는 것이다. 그렇기 때문에 현재의 모든 서비스를 블록체인 기반으로 전환할 때 사용가능한 일반적인 플랫폼이다(사실 이더리움의 본질이기도 하다). 따라서 앤드어스체인 생태계는 모든 분야를 포함한다. 결론적으로 앤드어스체인은 블록체인 관련 산업육성을 위한 기반 인프라이다.

현재 우리나라의 경우 가장 중요한 정책 중 하나가 양질의 일자리 창출이다. 그리고 이와 관련한 청년 실업문제 해소이다. 정부는 이를 위해 수많은 예산을 투입하여 일자리 창출을 위한 창업생태계를 지원하고 있다. 그러나 기존의 창업생태계는 제4차 산업혁명 생태계를 실질적으로 반영하는데 실패했으며, 고비용의 창업생태계이다. 즉, 기조의 창업생태계의 경우 청년들은 좋은 사업 아이디어가 있다하더라도 그것을 현실화하기에는 창업비용, 사전 검증이 어려운 상황에서 자금조달의 문제, 실패 시 경제적 안전망이 미비한 상황에서 높은 실패 확률의 문제 등으로 도전적인 창업 경험을 갖추기 어려운 환경에 있었다. 결론적으로 기존의 창업생태계는 고비용 구조로 인한 일자리 창출의 경직성에 놓여있었다는 결론에 다다를 수 있다.

앤드어스체인은 바로 이러한 고비용 창업생태계 구조를 제4차 산업혁명 및 미래 세상에 적극적으로 대응하기 위한 저비용의 창업생태계 구조로 전환 할 수 있게 해준다. 즉, 앤드어스체인 플랫폼의 공유를 통해 창업비용 및 운영비용 등을 혁신적으로 절감시켜 줄 수 있다.

앤드어스체인 플랫폼을 활용하여 많은 청년들은 P2P 기반의 비즈니스 서비스를 통하여 창업에 대한 사전 검증을 시도할 수 있으며, 설사 실패한다 하더라도 비용절감을 통하여 보다 안전한 재기가 가능한 상황으로 전환된다.

블록체인 창업생태계가 가지는 장점에도 불구하고 국내의 경우 블록체인 기반의 창업생태계가 전무한 상황이다. 현재 많은 스타트업이나 대기업들이 블록체인 사업을 진행하지만 대부분은 블록체인 기반의 서비스 개발 용역에 그치고 있다.

앤드어스체인 플랫폼은 오픈된 플랫폼으로 누구나 저비용으로 쉽게 사용할 수 있다.

□ 기본 창업생태계 문제

- 창업비용 문제 : 실제 자신의 아이디어를 사업화하기 위해서는 시스템 구축 등 자금이 필요함
  ※ IT 산업 관련 평균 창업비용은 약 3억[8]
- 자금 조달 문제 : 사전 검증이 미비한 상태에서 자금 조달 어려움

- 높은 실패 확률 : 실패 했을 경우 재기할 수 있는 안전망 구축 미비로 자금 조달 시 창업자의 금전적 부담(보증 등)

□ 앤드어스체인 플랫폼 기반 저비용 창업생태계

- 창업비용 문제 해결 : 블록체인플랫폼을 활용함으로서 시스템 구축 등의 비용 절감
- 자금 조달 문제 해결 : 공개적인 사전 검증이 이루어짐으로서 자금 조달이 용이함
- 낮은 실패 확률 : 저비용 구조를 유지함으로서 혁신의 안전망 구축 효과

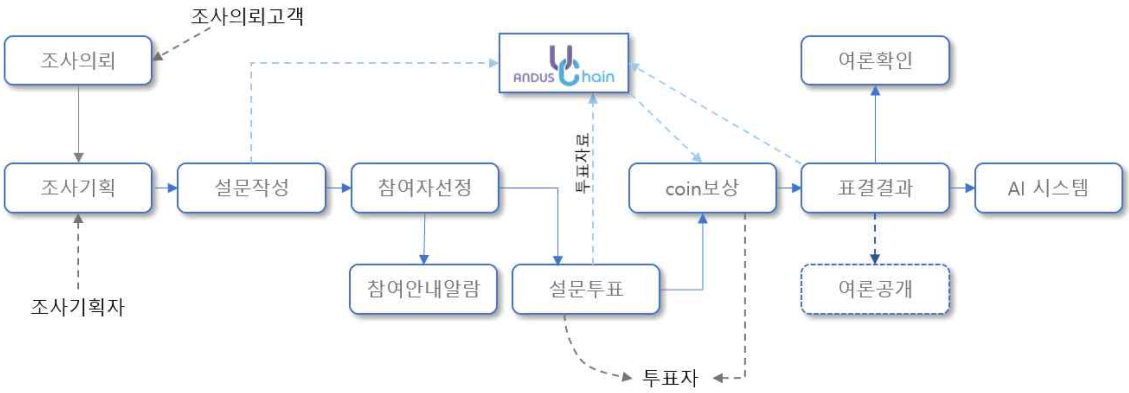
현재 대표적인 블록체인 기반 오픈 창업생태계 모델은 이더리움이다. 누구든지 이더리움 플랫폼 위에 P2P 비즈니스 서비스를 구축할 수 있으며, 2019년 4월 기준 2,670여개의 블록체인 기반 서비스가 구축 또는 개발 중에 있다.

앤드어스체인은 이더리움보다 사용자 편리성을 극대화하여 이더리움보다 용이하게 생태계를 국축할 수 있도록 하여 양질의 일자리 창출을 위한 저비용 창업생태계 역할을 담당하게 된다.

8. 추진 프로젝트

8.1 여론 조사 (Survey)

여론조사 프로세스를 블록체인에 구축하여 조사 결과의 신뢰성을 혁신적으로 높일 수 있다. 또한 여론조사에 참여한 모든 사용자에게 적절한 보상을 지급하여 여론조사 시스템의 활성화를 극대화시킬 수 있다. 우리가 추진하는 여론 조사 프로젝트는 이러한 장점을 극대화한 오픈형 여론조사 서비스이다.



(그림 8-1) 여론 조사 서비스 구성도

□ **주요 프로세스**

- 조사 의뢰
  조사목적, 조사대상, 조사기간 등 정보를 등록하여 조사진행 및 여론수집을 위탁한다.
- 조사기획
  소정의 절차를 통하여 누구나 조사기획자의 권한을 획득할 수 있으며, 조사에 대한 전반적인 기획과 진행을 수행하고 최종 결과를 수집한다.
- 설문작성
  조사 질의 문항을 등록하면 블록체인에 기록되면서 자동으로 표결할 수 있는 웹 페이지가 생성된다.
- 참여자 선정
  임의의 불특정 다수 또는 특정 요구조건에 따른 조사 참여자의 목록을 생성한다.
- 참여 안내 알람
  조사 참여자 목록에 따라 참여자에게 조사 안내문을 전송하여 표결을 유

도한다.

- 설문 투표
  참여자는 이메일, SMS 및 사이트 로그인을 통하여 설문지에 직접 접근할 수 있으며 각 질의 문항별 표결 정보는 블록체인에 기록한다. 경우에 따라, 인터뷰 조사자를 참여시켜 전화설문조사를 수행할 수도 있다.

- 표결 결과
  참여자의 표결 데이터를 집계하고 오차범위와 유효의미를 분석하여 최종 결과를 도출한다.

- 여론 확인 및 공개
  조사 의뢰자는 언제든 투표결과를 조회할 수 있으며, 경우에 따라 투표 참여자 및 제 3자에게 여론을 공개할 수도 있고 기타 시스템(AI, 빅데이터 등)에서 활용할 수 있도록 정보를 제공할 수도 있다.

- AI 시스템
  유사한 조사 문항별 표결 결과를 지속적으로 누적하여 간접적으로 이와 관련된 여론 형성을 인공지능을 통하여 추론하여 예측한다.

- 인센티브 정책
  설문 참여자, 인터뷰 조사자, 참여 추천자 및 서비스 평가자에게 코인 보상을 제공한다.

□ 기대효과

- 투표 시스템을 블록체인에 적용함으로써 투표 데이터의 위변조 위험성을 원천적으로 차단하여 결과에 대한 불신을 최소화한다.

- 각 참여자(설문 참여자, 인터뷰 조사자, 참여 추천자 등)에게 코인으로 보상을 제공함으로써 오픈형 투표 시스템의 활성화를 유도할 수 있다.

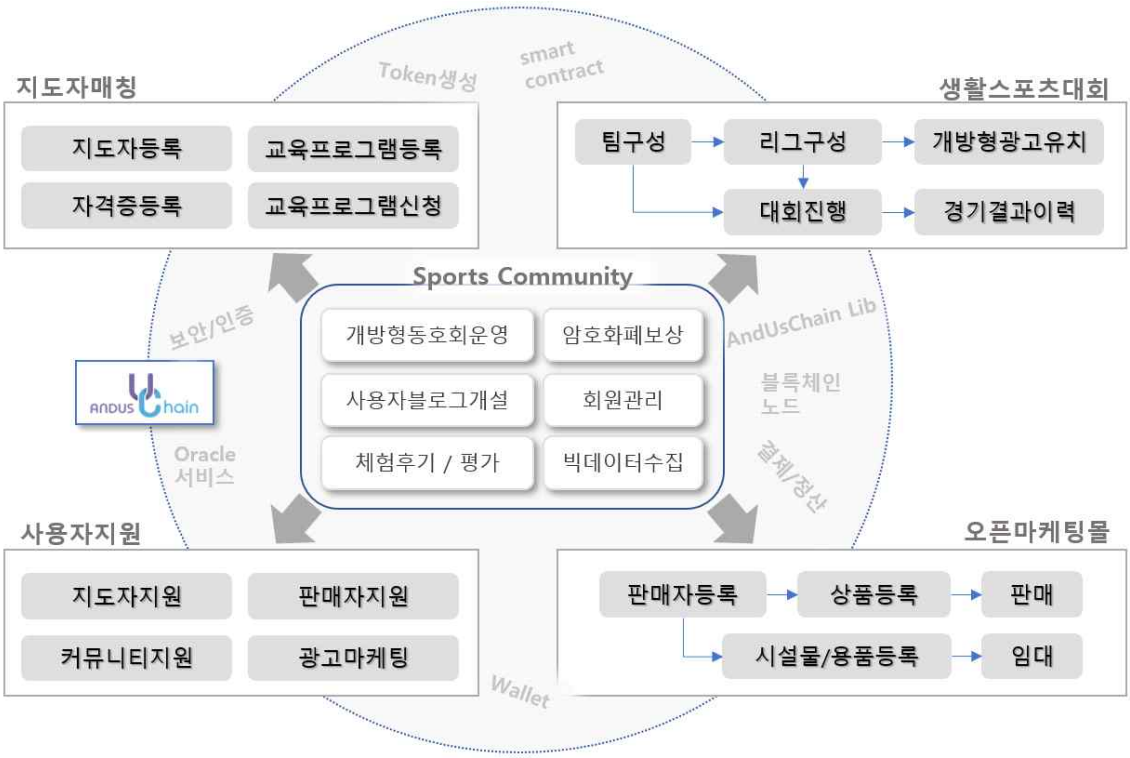
- 원천적으로 위변조를 방지하기 때문에 신뢰성을 높일 수 있고, 누구나 조사를 의뢰하거나 투표에 참여할 수 있는 오픈 시스템으로 구축되어 활성화에 이점이 있다. 이와 같은 이점은 다양한 의사결정사안에 대하여 공정하고 민주적인 신뢰 사회 발전에 기여할 것이다.

8.2 ATA Club

ATA Club 서비스는 생활 스포츠 시장을 확장하고자 스포츠와 관련된 다양한 서비스를 블록체인 시스템에서 제공하고자 한다. 본 서비스는 스포츠 동호회 및 블로그

등 다양한 커뮤니티를 중심으로 우수한 스포츠 지도자와 교육 희망자를 연결시켜주는 매칭 서비스, 스포츠 시설물 및 용품을 임대 또는 판매하는 오픈 마켓, 경기팀 구성과 아마추어 대회 진행을 지원하는 대회 운영 서비스 등으로 구성될 것이다.

ATA Club 서비스는 블록체인 상에서 구축되어 신뢰도와 공정성을 보장하고 생활 스포츠 시장의 확장을 견인할 것이다.



(그림 8-2) ATA Club 서비스 구성도 (생활 스포츠 관련 서비스)

□ 주요 프로세스

- 개방형 동호회 운영
  회원이면 누구나 동호회를 만들고 동호회원을 유치할 수 있다. 또한 동호회 활동을 지원하는 프로그램을 편리하게 사용할 수 있다.

- 사용자 블로그 개설
  모든 회원은 자신의 블로그를 개설하여 운영할 수 있으며, 소정의 조건에 따라 다양한 의견을 블로그에 올려서 여러 회원들과 의견을 나눌 수 있다.

- 체험후기/평가
  교육 프로그램, 쇼핑, 동호회 등 회원들의 다양한 체험에 대하여 의견을

작성하고 여러 채널의 평가 시스템을 통하여 대상을 평가함으로써 양질의 서비스를 선별할 수 있다.

- 인센티브 정책
  회원들은 모든 활동과 참여에 대해 암호화폐로 보상을 받는다.

- 회원관리
  지도사, 수강생, 팀 구성원, 동호회원 및 일반 회원 등 다양한 참가자를 등록하여 인증을 수행하고 각 역할에 대한 권한을 부여할 수 있다.

- 빅데이터 수집
  회원들이 체험한 다양한 서비스에 대한 의견 및 서비스 자체에서 생성되는 자료(경기 결과, 평가 등)를 수시로 수집 및 분석하여 보다 나은 서비스를 제공하고자 한다.

- 지도자 등록
  스포츠에 역량을 갖춘 사람이면 누구나 지도자로 등록하여 교육 프로그램을 타인에게 제공하거나 모두에게 공유할 수 있다.

- 교육 프로그램 등록
  지도자 권한이 있는 사용자는 교육 프로그램을 공지하여 수강생을 모집할 수 있다.

- 교육 프로그램 신청
  회원은 원하는 교육 프로그램을 신청할 때 지도자의 프로필 등을 확인할 수 있다. 이와 별도로 회원이 등록한 요구조건과 교육이수조건 등에 따라 자동으로 지도자의 교육 프로그램을 추천받을 수도 있다.

- 팀 구성
  스포츠 종목에 따라 팀을 구성(팀원 초청, 팀원 신청)할 수 있고, 팀이 구성되면 대회 참가 등 팀 단위 활동(팀 게시판 접근 등) 권한이 제공된다.

- 리그 구성
  팀들이 모여 대회를 만들 수 있고 이에 따른 부가 기능(경기대진표 구성 등)을 편리하게 활용할 수 있어 편리하게 대회를 즐길 수 있다.

- 개방형 광고 유치
  경기할 팀들과 리그 구성이 완료되면 대회 홈페이지가 자동으로 만들어지고 해당 홈페이지에 광고를 올려 광고 유치 수입을 암호화폐로 받을 수 있다.

- 대회 진행
  대진표와 경기일정에 따라 시설물 및 용품을 임대할 수 있고, 심판진 구성

등 대회 진행에 필요한 후속 처리와 경기별 결과를 등록한다.

- 경기 결과 이력
  매 경기 결과, 진행됨에 따라 발생되는 의견 및 특이사항 등은 블록체인에 기록되어 팀원들 간에 공유가 가능하며 이후에 이루어지는 대회에서도 참조할 수 있다.

- 판매자 등록
  회원이 판매자로 등록되면 쇼핑몰 페이지를 개설할 수 있는 권한이 부여된다.

- 상품 등록
  판매자로 등록된 회원은 자신이 개설한 쇼핑몰 페이지에 판매할 상품 정보를 등록할 수 있다.

- 시설물 / 용품 등록
  임대할 스포츠 시설물 또는 용품 정보를 등록한다.

- 판매 / 임대
  판매자는 스포츠 상품 판매, 시설물 사용 예약, 용품 임대 등을 통하여 수익을 올릴 수 있다.

- 지도자 지원
  일반 지도자 및 프리미엄 지도자가 교육 프로그램 운영, 교육 신청 접수, 수납, 정산, 체험후기, 게시판 및 홍보 등 지도자의 활동을 지원하는 지도자용 서비스이다.

- 판매자 지원
  판매자가 입점 매장 홍보, 상품 진열 및 관리, 주문 접수 및 시설물 예약, 결제 및 정산 등 판매자의 제반 활동을 지원하는 입점 매장용 운영 서비스이다.

- 커뮤니티 지원
  블로그 운영 또는 동호회 운영 및 활동을 지원하는 커뮤니티 관리용 서비스이다.

- 광고 마케팅
  교육 프로그램, 상품, 시설물 및 용품의 홍보 배너 설정, 광고 신청 및 접수, 고아고 콘텐츠 등록 등 광고 관리에 필요한 서비스 모듈이다.

□ 기대 효과

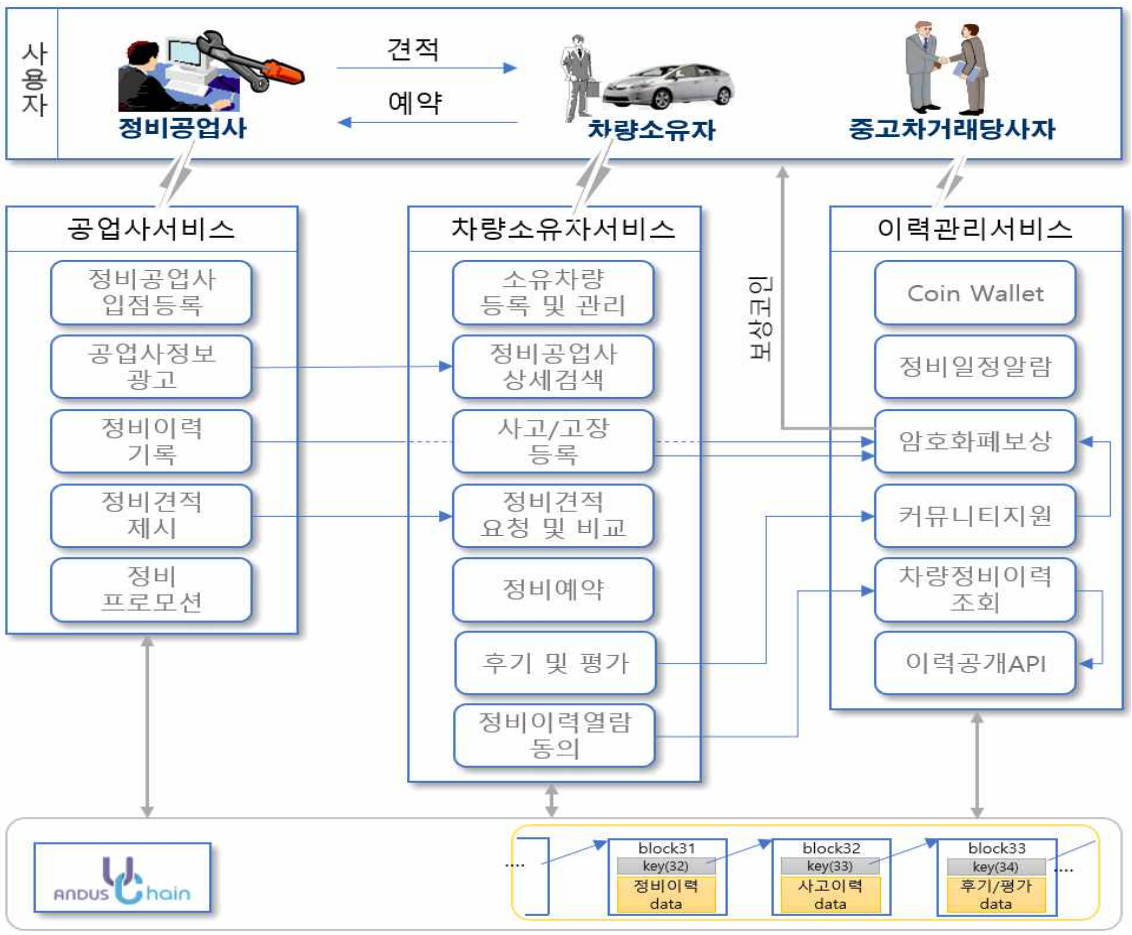
- 블록체인에서 생활 스포츠를 위한 다양한 서비스가 제공되기 때문에 관리

의 투명성이 보장된다.

- 자율적인 커뮤니티를 통한 창의적인 의견 표출, 평가 및 생활 스포츠 데이터 등을 지속적으로 축적하고 분석하여 생활 스포츠 서비스의 품질을 향상시키고 사용자의 만족도를 강화할 수 있다.

8.3 중고 자동차 매매

중고자동차 매매의 신뢰성 확보를 위해 블록체인 기반의 자동차 이력관리 기능을 중심으로 자동차 중고매매 서비스 또한 추진하고 있다.



(그림 8-3) 중고 자동차 매매 서비스 구성도

※ 세부 내용은 백서 0.8 버전에서 공개 예정

9. 암호화폐 다온

앤드어스체인은 플랫폼 운영을 위해 암호화폐 "다온(단위 DEB)"를 발행한다.

□ 암호화폐 다온 총 발행량 : 100억개

□ 암호화폐 분배 정책 (예정)

<표 9-1> 암호화폐 분배 정책 (예정)

구분	비율(%)	사용처
창안자	10	인센티브
개발자 및 어드바이저	10	인센티브
회사 보유	20	앤드어스 플랫폼 운영
개발비	20	√ 앤드어스 생태계 지원 기능 강화 √ 분산화 프로토콜과 개발도구를 세계에 제공하기 위해 연구 및 개발
생태계 지원	25	√ 교육센터 운영 √ 앤드어스 기반 차세대 분산 응용 프로그램인 (dapps)을 개발 할 수 있도록 지원 √ 창업비 지원 등
마켓팅	10	√ 홍보 및 마케팅
보상 프로그램	5	√ 버그 발견 및 주요 개선 시 보상
합계	100	

10. 로드맵

앤드어스체인 개발 및 생태계 확보 로드맵은 다음의 일정대로 추진할 계획이다.

<표 10-1> 앤드어스체인 로드맵

일정	주요 결과
2019년 4월	백서(version 0.7)
2019년 4월 5일	테스트넷 공개
2019년 9월	빅데이터 기능 융합
2019년 11월	인공지능 융합
2019년 12월	백서(version 1.0)
2020년 1월	메인넷 공개
2020년 1월 ~	√ 교육센터 운영 √ 앤드어스 기반 차세대 분산 응용 프로그램인 (dapps)을 개발 할 수 있도록 지원 √ 창업비 지원 등
2020년 6월	√ 5개의 생태계 확보(자체) √ 10개의 생태계 확보(공동) √ Dapp 생태계 활성화 지원
2020년 12월	√ 10개의 생태계 확보(자체) √ 30개의 생태계 확보(외부) √ Dapp 생태계 활성화 지원

11. 결론

앤드어스체인은 미래 블록체인 세상의 인프라이다. 미래 암호경제(블록체인 경제) 활성화의 핵심 기반 구조의 역할을 담당할 것이며, 특히 양질의 일자리 창출을 위한 저비용 창업생태계 구축이 일차적인 목적이다.

그러나 앤드어스체인의 궁극적인 목적은 현재 가장 많은 생태계를 확보한 이더리움을 능가하는 차세대 이더리움이다. 앤드어스을 한마디로 정의하면 공정하고 고속의 차세대 이더리움(A fair&fast&secure next ethereum)이라 할 수 있다. 앤드어스체인을 통해 우리나라가 블록체인 강국이 되는 초석을 마련하고 싶다.

무엇보다도 암호화폐에 극단적으로 부정적인 정부 관계자들에게 건전한 암호화폐 및 블록체인 생태계를 창출할 수 있다는 것을 현실적인 실증프로젝트를 통해 보여주고 싶다.

앤드어스체인이 우리 모두가 함께 잘사는 미래의 블록체인 강국을 실현하는데 충분한 역할을 할 수 있도록 최선을 다하고자 한다.

참고자료

[1] 이더리움 공식 사이트, https://ethereum.org/

[2] 이더리움 백서, A Next-Generation Smart Contract and Decentralized Application Platform, 2018.08.

[3] 이더리움 황서, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BYZANTIUM VERSION e94ebda, 2018.06.

[4] 비트코인 백서, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[5] V. Buterin, On Settlement Finality, https://blog.ethereum.org/2016/05/09/on-settlement-finality, 2016.09.

[6] V. Buterin, On Slow and Fast Block Times, https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times, 2015.09.

[7] C. Decker, R. Wattenhofer, Information Propagation in the Bitcoin Network, In IEEE International Conference on Peer-to-peer Computing, 2013.

[8] 중소기업청, 창업진흥원, 2016년 창업기업 실태조사, 2016.

변경 내역

2019.05.31. - 백서 버전 0.71

· 변경 원인 : 채굴 참여 트랜잭션은 수수료가 부과되지 않기 때문에 일반 트랜잭션 대비 블록 포함 우선순위가 낮아 블록에 포함되지 않음

· 해결 방안 : 채굴 참여 트랜잭션의 처리 우선순위를 최우선으로 지정

· 변경 위치 : 블록 구조체