



카르다노 (ADA)

상장검토 보고서

2018.06.14

- 목 차 -

1. 개요

가. 카르다노(Cardano, ADA) 란?

나. 주요 스펙

1) 기본정보

2) 시장정보

2. 주요 팀 멤버 및 재단소개

3. 카르다노 컨셉 및 특징

- 확장성

4. 기술적 특징

- 우로보로스 PoS(Ouroboros Proof-of-Stake) 프로토콜

- KMZ 사이드체인

- 카르다노 세틀먼트 레이어 (CSL)

- 카르다노 연산 레이어 (CCL)

- 하스켈 언어 (Haskell Language)

- Daedalus 지갑

5. 로드맵

6. 종합검토의견

1. 개요

가. 카르다노(Cardano, ADA) 란?

카르다노는 단순히 암호화폐가 아닌 이더리움처럼 스마트 컨트랙트를 지원하는 플랫폼으로, 기존 플랫폼들이 지니고 있던 확장성과 트랜잭션 속도 문제를 해결하고자 개발을 시작하였다. 카르다노의 주요 핵심 기술로는 우로보로스 PoS(Ouroboros Proof-of-Stake) 프로토콜, 하스켈 프로그래밍 언어, KMZ Sidechains, 그리고 Daedalus Wallet 등이 있다. 또한, 해당 플랫폼은 Kiayias, Miller, Zindros 교수들이 개발한 새로운 사이드 체인 프로토콜을 활용해 두개의 분리된 계층 레이어에서 비대화형 방식으로 값을 안전하게 이동할 수 있도록 한다.

현재 해당 블록체인 프로젝트는 암호화폐 중 최초로 과학적 철학과 학술 연구를 함께 접목하여 개발되고 있으며, 향후 전세계의 국가기관, 기업, 개인이 일상에서 금융 어플리케이션을 빠르고 쉽게 이용할 수 있도록 하는 것을 목표로 2020년 까지 개발이 진행될 예정이다.

나. 주요 스펙

1) 기본정보

암호화폐명	Cardano (ADA)
최초발행일	2015.09
홈페이지	https://www.cardano.org/
합의알고리즘	PoS

2) 시장정보

총발행량	31,112,483,745 ADA
시장유통량	25,927,070,538 ADA
시가총액	\$4,073,842,000 (약 4 조 4,160 억)
거래량(24h)	\$85,181,000 (약 920 억)
거래가격	0.157 (약 170 원)

* 2018.06.14 코인마켓캡 기준

2. 주요 팀 멤버 및 재단소개

Charles Hoskinson은 현재 카르다노의 CEO이며, 블록체인 연구 회사 Input Output Hong Kong(IOHK)의 CEO직을 겸하고있는 블록체인 사업가이자 수학자이다. 그는 Invictus Innovations과 이더리움의 스타트업 창업 경험을 가지고 있으며, 다양한 공공 및 민간 기관에서 활동하는 등 풍부한 블록체인 산업 관련 지식과 경험을 보유하고 있다.

그는 또한, 비트코인 파운데이션의 교육 위원회의 창립 의장으로 활동하기도 하였다.

카르다노 프로젝트는 카르다노 재단, Input Output Hong Kong(IOHK), Emurgo가 공동으로 개발하고 있는 프로젝트로 총 3 개의 독립된 기관이 각각 법규 및 커머스, 암호화폐 리서치 및 개발, 그리고 스타트업 및 벤처 투자 지원의 역할을 분담하고 있다.

카르다노는 2018년 3월, 스마트 기기의 이용자 보안 솔루션 회사인 SIRIN LABS와 제휴를 맺으며 오픈소스 시스템의 보안을 더욱 강화하게 되었으며, 최근에는 한국 블록체인 핀테크 기업 미탭스플러스(Metaps Plus)와 파트너십을 체결하여 향후 미탭스플러스와 계약되어 있는 약 3만개 오프라인 매장에서도 활용이 가능해질 예정이다.

3. 카르다노 컨셉 및 특징

■ 확장성

PoS 프로토콜은 기본적으로 샤딩(sharding)이라는 방법을 통해 블록 시간 간격을 단축하고 네트워크를 훨씬 효율적으로 만들기 때문에 PoW 프로토콜 보다 훨씬 빠르고 비용이 적게 든다. 우로보로스는 카르다노의 PoS 프로토콜로 카르다노의 핵심 기술이며, 또한 PoS 프로토콜 중 최초로 과학적으로 입증된 PoS 프로토콜이다. 우로보로스 PoS는 동시에 여러 체인을 병렬로 유지할 수 있기 때문에 뛰어난 확장성을 보유하고 있다.

4. 기술적 특징

■ 우로보로스 PoS (Ouroboros Proof-of-Stake) 프로토콜

카르다노의 합의 프로토콜은 우로보로스라고 불리며 이 프로토콜은 에딘버러 대학의 아겔로스 키아이아스(Kiayias)교수가 이끌고 있는 다섯 개의 학술 기관에서 모인 재능 있는 암호 학자 팀에 의해 설계되었다. 해당 프로토콜의 특징으로는 엄격한 암호학적 모델을 통한 안전성과, 다양한 프로토콜들이 플랫폼에 구성되어 기능할 수 있도록 하는 모듈식의 유연한 디자인이다. 즉, 카르다노는 확장성, 인센티브 방법, 안전한 투표라는 측면에서 우로보로스 PoS 프로토콜을 채택하게 되었다.

■ KMZ 사이드체인

카르다노 플랫폼은 Kayias, Miller, Zindros 교수들의 연구 결과인 "작업 증명의 증명" (Proofs of Proofs of works)을 기반으로 하여 개발된 KMZ 사이드체인(KMZ sidechains)을 지원한다. 그로 인해, 플랫폼의 카르다노 세틀먼트 레이어(CSL)에서 해당 프로토콜을 지원하는 다른 모든 블록체인으로 자금을 안전하고 상호작용없이 이동시킬 수 있다. KMZ 사이드체인은 플랫폼의 복잡한 요소들 예를 들어, 스크립트 언어, 법규, 비공개 거래 등 여러 제반 사항들을 효율적으로 요약하여 레저(Ledger)에 기록하게 되어 언제든 예기치 못한 상황에서 다시 확인이 가능하다.

■ 카르다노 세틀먼트 레이어 (Cardano Settlement Layer)

카르다노 세틀먼트 레이어(CSL)는 플랫폼의 첫번째 레이어로써 트랜잭션의 잔액을 확인 하는 원장 역할을 하며, PoS 합의 알고리즘을 이용해 새로운 블록을 생성하고 트랜잭션을 승인한다.

해당 레이어에서는 가치에 대한 회계 처리를 담당하게 되며, 목표는 다음과 같다.

- i. 두가지 스크립트 언어 세트의 지원. 하나는 가치의 이동을 위한 것이며, 다른 하나는 오버레이 프로토콜에 대한 지원을 강화하기 위한 것
- ii. 다른 장부와 연결되는 KMZ 사이드 체인에 대한 지원을 제공함
- iii. 더 높은 보안을 위해 양자 저항 시그니처를 포함한 여러 유형의 시그니처 지원
- iv. 다중 사용자가 발행한 자산 지원
- v. 실제 확장성 달성, 더 많은 사용자가 가입 할 수록 시스템 기능이 향상됨을 의미함

■ 카르다노 연산 레이어 (Cardano Computation Layer)

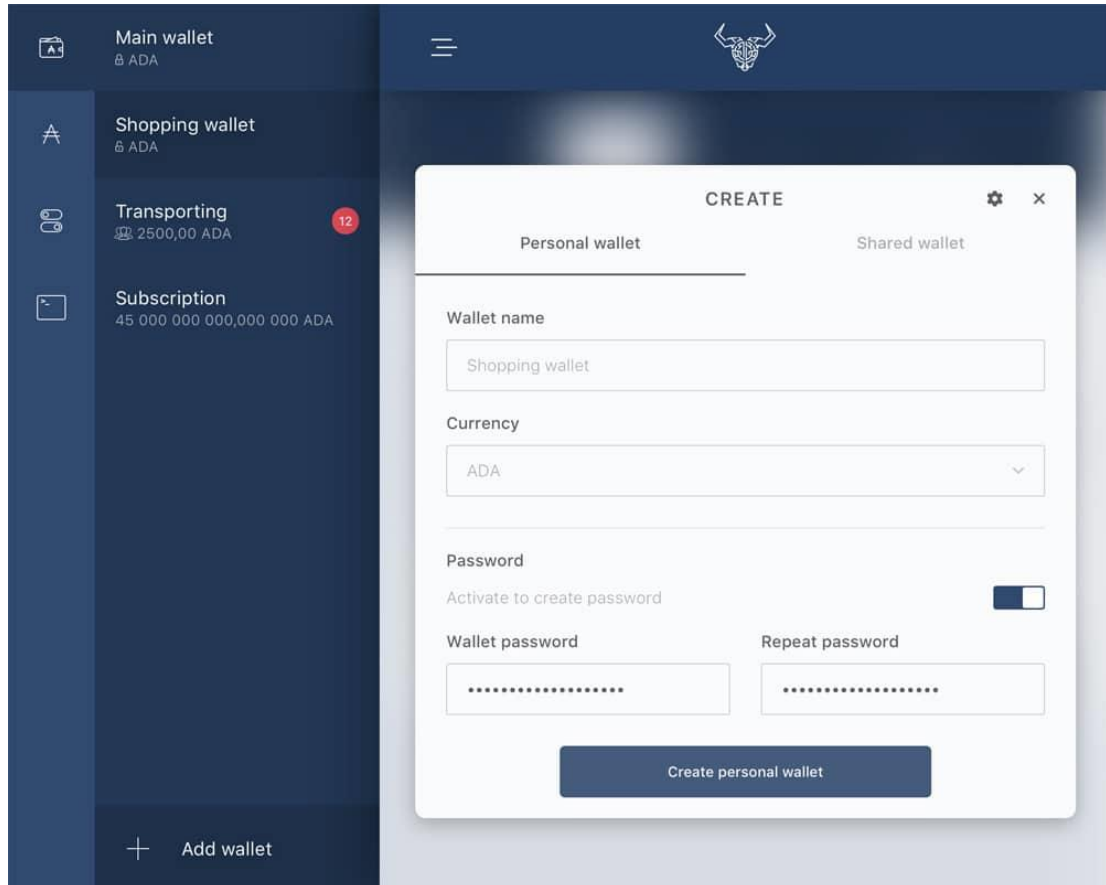
카르다노 연산 레이어(CCL)는 카르다노 플랫폼의 두번째 레이어로써 트랜잭션과 관련된 추상적인 정보들, 예를 들어 해당 거래가 생겨난 이유에 대한 정보 등을 저장하게 된다. 또한, CSL에서 분리되므로 CCL의 이용자들은 레이어 내에서 다른 규정들을 만들어 트랜잭션을 평가할 수 있다. 예를 들어, 트랜잭션 거래에서 AML / KYC 데이터가 포함되지 않은 거래를 의도적으로 제외하는 권한이 부여된 원장(Ledger)을 만들 수 있으며, 이는 사회적으로 블록체인 규정이 계속 증가함에 따라 더욱 중요한 요소가 될 수 있다. CCL은 카르다노가 자체 개발한 Plutus 프로그래밍 언어를 사용하게 되며, 이더리움의 스마트 컨트랙트에 사용되는 Solidarity 프로그래밍 언어도 함께 지원하고 있다.

■ 하스켈 언어 (Haskell Language)

하스켈은 뛰어난 모듈성과 조합성을 보유하고 있으며, 지난 몇년간 Galois, FP complete, Well-Typed 같은 기업들의 광범위한 활용 덕분에 많은 진화를 거듭하였다. 그로 인해, 하스켈은 상용 어플리케이션을 위한 언어로 사용될 수 있게 되었다. 하스켈 프로그래밍 언어는 뛰어난 프로그래밍 인재들 사이에서 이미 많이 사용되고 있으며, 하스켈 개발자는 컴퓨터 공학에 대한 많은 지식을 보유하고 있다고 여겨지기도 한다. 이때문에 어플리케이션을 개발하는 개발자의 역량을 평가하는 척도로 이용되기도 한다.

■ Daedalus 지갑

Daedalus 지갑의 1세대에서는 HD 전자지갑으로 기능할 것이며, 많은 회계 기능 및 지불 암호, 그리고 BIP39와 같이 산업 표준의 보안 기능을 보유하게 된다. 향후 2세대부터는 스토어, 일반적인 통합 APIs와 SDK를 가지는 응용프로그램 프레임워크로 개발될 예정이다. Daedalus는 프로그래머가 JavaScript, HTML5, CSS3 를 활용해 응용 프로그램과 프로그램 간 통신을 이어주는 브릿지를 개발할 수 있도록 하여 개발의 용이성이 매우 높다.



< Daedalus 지갑 화면 이미지 >

5. 로드맵

카르다노 로드맵 2018



< 카르다노 로드맵 도표 이미지 (홈페이지 참조: <https://cardanoroadmap.com/kr/>) >

- 카르다노 메인넷 공개, 거래소 성능 강화
- 로그 제출 매커니즘, 우로보로스 위임 시작
- 다중서명 트랜잭션, 백엔드 재설계
- 라이트 클라이언트 지원 등

카르다노는 2020년까지의 플랫폼 개발 로드맵을 최근 공개 하였으며, 각각 바이런, 셸리, 고겐, 바쇼, 볼테어의 총 5 단계로 나누고 있다. 현재 해당 프로젝트는 바이런에서 셸리의 단계로 이동중에 있으며, 이 단계에서는 탈 중앙화와 자동화 시스템 기술에 초점을 두어 개발이 진행될 예정이다.

6. 종합검토의견

카르다노는 스마트 컨트랙트를 지원하는 플랫폼으로 이더리움, EOS, Lisk, NEM 등 다른 유사한 플랫폼 프로젝트들과의 치열한 경쟁이 불가피해 보일 것으로 예상된다. 하지만 카르다노 팀은 우로보로스 PoS (Ouroboros Proof-of-Stake) 프로토콜, 하스켈 프로그래밍 언어, KMZ Sidechains, 그리고 Daedalus Wallet 등 확장성과 과학적 연구를 기반으로 개발된 고도의 코딩 구축을 통해 다른 경쟁 플랫폼들과 차별화를 시도하고 있다. 또한, 전 이더리움 CEO였던 Charles Hoskinson을 필두로한 카르다노 재단, 블록체인 연구 회사 Input Output Hong Kong (IOHK) 그리고 스타트업 벤처 투자회사 Emurgo의 협업이 가져오는 시너지 효과는 암호화폐 시장뿐만 아니라 교육기관 및 공공기관 등 다양한 분야에도 큰 파급력을 지니고있다.

카르다노는 스마트 기기의 이용자 보안 솔루션 회사인 SIRIN LABS와 제휴를 맺고 오픈소스 시스템 보안 기술을 발전 시키고 있으며, 한국 블록체인 핀테크 기업 메타스플러스 (Metaps Plus)와 파트너십을 체결하는 등 향후 오프라인 매장에서 해당 암호화폐 사용이 가능해질 예정이어서 더욱 귀추가 주목되고 있다.

본 검토의견보고서는 해당 암호화폐 재단의 의견을 일부 반영하였으며 공식 홈페이지, 백서 및 주요 관련 사이트 (Github, Slack 등)를 참고하여 작성되었음을 알려드립니다.

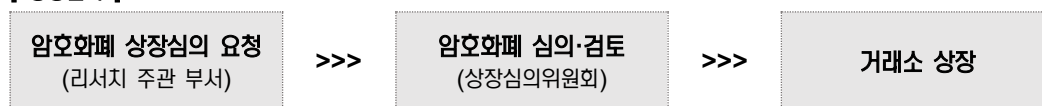
b 빗썸 상장심사기준

* 상장이란?

빗썸에서 정한 요건을 충족한 암호화폐가 거래소에서 거래할 수 있도록 허용하는 것으로, 전문가로 구성된 암호화폐 상장심의위원회의 엄격한 심의·검토를 통해 진행되고 있습니다.

또한, 원활한 유동성 유지와 시장의 공정한 가격 형성을 위하여 일정한 내부기준을 마련하여 운영함으로써 암호화폐 시장의 신뢰확보와 투자자 보호를 위해 노력하고 있습니다.

[상장절차]



* 상장심의위원회의 실질적 심사기준은,

1. 비즈니스 연속성

- 프로젝트(컨셉) 지속 가능성, 경쟁력, 안정적인 비즈니스, 수익구조, 장기적인 로드맵 등

2. 기술적 기반과 확장성

- 알고리즘 차별성, 기술의 적합성 및 확장성, 보안성, 완성도, 개발진의 신뢰도, 실현가능성 등

3. 시장성

- 시장수요,마켓쉐어,인지도(커뮤니티) 등

등으로 구성되어 있으며, 상장심사의 객관성을 확보하기 위한 상장심사기준을 구체화하고 있습니다.

i 투자유의사항

- 암호화폐의 가치 변동으로 인한 손실 발생 가능성 등을 유념하시어 무리한 투자는 지양하십시오.
 - 암호화폐는 정부가 보증하는 법정화폐가 아니며, 규제나 시장환경변화에 따라 암호화폐 가치에 부정적인 영향을 받을 수 있습니다.
 - 암호화폐에 대한 투자는 본인의 책임이오니 무리한 투자는 지양하시고, 신중한 투자를 부탁드립니다.
- 본 자료는 현재 시점의 암호화폐에 대한 투자자의 이해를 돕고자 작성된 것으로, 내용이 변경될 수 있습니다. 따라서, 본 자료가 제공하고 있는 정보에 기초한 투자결정과 투자결과에 관하여 당사가 이를 보장하지는 않습니다.