Raptoreum:
선물, 자산 그리고 컨트랙트의 생성과 전송이 자유로운 유연한 시스템

랩토리움(Raptoreum)이라는 이름은, 레이븐코인(Ravencoin)과 이더리움(Ethereum)을 통합하여서 만들어졌습니다. 레이븐(큰까마귀)은 "명예로운" 맹금류로 불리어왔으며, 우리의 코인은 레이븐 코인을 포크하여 스마트 컨트랙트 기능을 덧붙였기 때문에 랩토리움이라는 이름이 가장 적당합니다. 비트코인과 레이븐코인 개발자들에게 깊은 감사를 드리며, 이들이 아니었으면 이렇게 훌륭한 코드 기반에서부터 우리의 것을 만들어내지 못했을 것입니다.

개요

랩토리움은 아주 간단한 아이디어에서 시작했습니다. 그것은 온-체인에서 사용 가능한 스마트 컨트랙트를 도입하고, 레이븐코인 코드 기반에서 신뢰할 필요가 없는 전송들이 가능하게 하는 동시에, 자산들과 RTM(랩토리움)의 자동화가 가능하도록 해보자는 것이었습니다. 프로젝트는 자산 레이어를 확장시키는 것뿐만 아니라, 다른 블록체인 프로젝트들을 도울 수 있는 혁신적인 기능들을 추가하면서 빠르게 발전되었습니다. 랩토리움은 누구나 빠르고 편리하게 자산을 만들 수 있게 디자인되었고, 온-체인에서 신뢰할 필요 없는 전송을 통해 안전하게 전송될 수 있도록 고안되었습니다.

랩토리움은 레이븐 코인 코드의 포크이기에, 레이븐 코인의 자산, 투표, 배당 그리고 메시지 기능을 상속받습니다. 그리고 우리는 다음의 기능들을 추가하여, 자산 범용 가능성을 늘리려 합니다:
첫 번째는, 특정 수량의 코인이나 자산을 동결시킬 수 있게 하는 것입니다. 그리고 이 동결된 자산은, 지정된 블록 높이나 특정한 시간에 풀리게 설정할 수 있습니다.
두 번째는 스마트 컨트랙트를 통해서, 자산과 네이티브 코인인 RTM(랩토리움)간의 신뢰하지 않아도 되는 온-체인 전송을 할 수 있게 하는 것입니다.

이러한 추가기능들은, 랩토리움의 자산 레이어의 사용에 대한 강력함과 용이성을 높이는 동시에, 분산화 어플리케이션 산업에 다양성을 줄 수 있게 될 것입니다. DAPP 은 다양한 분야에서 사용될 수 있는 매개체로, 랩토리움은 DAPP 개발자들을 위해 지속적으로 다양한 대안들과 가능성들을 제공할 것입니다.

랩토리움의 목표 중 하나는, 단순히 랩토리움을 위한 혁신적인 아이디어를 내는 데에 그치지 않고, 암호화폐 커뮤니티에 오픈 소스를 제공함으로써 누구나 그들의 블록체인 프로젝트가 성공하는데 도움을 받을 수 있도록 하는 것입니다. 51% 공격과 이중 지불 공격에 대한 방어 시스템인 Prysm 은 오픈 소스로 공개되어 누구나 사용할 수 있게 할 것입니다. 최근 암호화폐 시장을 보면 이러한 방어시스템이 얼마나 중요한지를 알 수 있습니다. 물론 그 어디에도 100% 완벽한 시스템 컨센서스는 없겠지만 말입니다.

랩토리움이 해결하려 하는 문제

대중적 수용(Mass Adoption): 암호화폐 업계에서 가장 큰 이슈 중에 하나는 대중적 수용(Mass adoption)입니다. 랩토리움은 쉽고 직관적인 방법으로, 누구나 그 어떤 것이든 토큰화 할 수 있게 함으로써 이 문제를 해결합니다. 뿐만 아니라, 우리는 스마트 컨트랙트의 유연성과 강력함을 제공함으로써 DAPP 개발자들이 도박에서 교육까지 넓은 분야를 아우르는 분산화 어플리케이션을 만들 수 있도록 합니다.

FPGA 와 ASIC 저항성: 랩토리움은 특별히 제작된 비싼 하드웨어 없이도, 누구나 채굴 가능하여 탈중앙화 정도를 높일 수 있도록 ASIC 과 FPGA 가 네트워크에 참여하지 못하게 만들어졌습니다.

이것이 가능하게 하기 위한 노력의 일환으로, 우리는 "GhostRider" [3]라 불리는 새로운 POW (작업증명방식) 알고리즘을 개발하였습니다. GhostRider 는 CNv1-8 과 x16r 랜덤화(randomizer)가 결합된 것으로써, ASIC 과 FPGA 를 사용 할 때 예상되는 보상에 비해 매우 높은 비용을 사용하게 만들어, 이들을 사용하지 않도록 유도하는 알고리즘입니다. 또한 이에 그치지 않고, 지속적으로 알고리즘의 능력을 향상시키기 위해 개발하고 있습니다. 이 기술을 사용하면, 랩토리움이 알고리즘의 특정 변수들을 바꾸는 것 만으로, 느리고 비싸고 보안에 취약한 포킹 과정 없이, 네트워크에서 발견되는 ASICS 와 FPGA 를 제외시킬 수 있습니다.

체인 포킹에 있어서, 많이 논의되지는 않았지만, 활성화된 체인이 포킹될 때마다, 기존 체인과 분리된 체인간에 연관된 정도를 분석할 수 있게 되어 보안성이 떨어지는 문제가 있습니다. 이는

스냅샷 시점에서부터 갈라진 두 개의 체인에서 같은 프라이빗 키가 사용되고, 이것이 여러 체인에서 같은 주소로 사용되기 때문입니다. 명심하건대, RTM 은 런칭 약 12 개월 이후 자산의 활성화를 위해 단 한번의 포크만 계획되어 있습니다.

51% 공격과 이중지불 방어: 2018 년부터 성공적인 51% 공격이 늘어나고 있고, 이러한 트렌드는 2019 년에도 지속되었습니다. 2018 년에는 총 약 24 억원어치가 51% 공격으로 도둑맞았고 [1], 이에 더해, 해당 프로젝트의 명성에 엄청난 타격을 입혔습니다. 51% 공격을 위한 비용은 생각보다 크지 않습니다[2]. 랩토리움은 "***Prysm***"이라는 방어 시스템을 개발 중이며, 누구나 혜택을 누릴 수 있도록 오픈 소스로 공개될 예정입니다. Prysm 은 서비스 노드들이 처리하게 될 것입니다.

- **하이퍼 인플레이션:** 마스터노드는 강력한 툴이지만, 하이퍼 인플레이션을 발생시켜, 시장에서 코인의 가격을 곤두박질 치게 만들 수 있고, 프로젝트에 돌이킬 수 없는 해를 입힐 수 있습니다. 랩토리움은 이러한 문제가 발생하지 않도록 단계별로 나누어진 담보금과 보상 시스템을 고안하였습니다. (**서비스 노드**를 참고하세요)

- **확장성 :** 랩토리움은 이더리움 같이 컨트랙트를 추가하지 않습니다, 대신 서비스 노드들이 이를 제공함으로써 현재 이더리움이 직면하고 있는 확장성 문제를 해결하고, 더 나은 확장성을 가질 수 있게 되었습니다.

서비스 노드

서비스 노드는 랩토리움 네트워크에서 여러 가지 중요한 역할을 합니다. 이들은 스마트 컨트랙트를 저장하고 실행하는 것뿐만 아니라, 51% 공격과 이중지불 방어를 시행하는 PRYSM 또한 구동합니다. 랩토리움은 단계별로 나누어진 서비스 노드 담보금과 보상 시스템과 함께, 최적화된 코인 발행 커브를 사용합니다. 이렇게 함으로써 마스터/서비스 노드를 사용하는 다른 많은 코인들이 피해를 입은 하이퍼인플레이션 문제를 해결 할 수 있습니다.

하드웨어:

이러한 다양한 기능을 수행하기 위해서는, 4 코어 8Gb 정도의 사양이 요구됩니다.

랩토리움 서비스 노드

우리는 노드 보상에 있어서 프로젝트의 장기적인 생존가능성을 약화시키는 것이 증명된 기존의

방식을 사용하지 않습니다. 즉, 얼마나 많은 코인이 발행되었는지에 따라 보상이 바뀌는 기존의 방식이 아니라, 네트워크에 서비스를 얼마나 제공했는지에 따라 보상하는 방식의 접근방법을 선택하였습니다. PRYSM 을 구동하고 있는 노드는, 전체블록 보상의 5% 와 함께 "자산 수수료(자산을 생성시 지불하는 수수료)"를 보상받습니다. 물론, 이는 소각되어야 할 "자산 수수료" 가 보상으로 지급되기 때문에 디플레이션적 요소를 없애는 것이기도 합니다. 하지만 동시에, 체인을 구동하면서 몇 개의 블록 만에 재편성을 못하게 막음으로써, 빠르지만 보안성이 뛰어난 전송이 가능하게 됩니다..
컨트랙트 레이어를 구동하는 노드는 블록보상의 15%를 받게 될 것입니다.

전반적인 서비스 노드의 보상과 ROI:
190 만개의 RTM 이 담보로 묶인 상태에서 4-6000 개의 서비스 노드가 구동될 때, 연간 ROI 는 네트워크의 전체 노드 수에 따라 변화는 있겠지만, 8-12%가 될 것 입니다. 이것은 노드를 구축하고 구동하는 비용과 비교하였을 때 충분히 타당한 수치라고 볼 수 있습니다.

보상 구조:

블록 높이 #	블록 보상	채굴 보상	컨트랙트 레이어 보상	PRYSM 보상	개발자 보상	서비스 노드 담보금
0-720	4	1	1	1	1	500.000
721- 5761	5000	4750	0	0	250	500.000
5762- 88720	5000	3750	750	250+ 자산 수수료	250	500.000
88.721- 132.720	5000	3750	750	250+ 자산 수수료	250	600.000
132.721- 176.720	5000	3750	750	250+ 자산 수수료	250	700.000
176.721- 220.720	5000	3750	750	250+ 자산 수수료	250	800.0000
220.721- 264.720	5000	3750	750	250+ 자산 수수료	250	900.000

264.721-308.720	5000	3750	750	250+ 자산 수수료	250	1.000.000
308.721-352.720	5000	3750	750	250+ 자산 수수료	250	1.150.000
352.721-396.720	5000	3750	750	250+ 자산 수수료	250	1.300.000
396.721-440.720	5000	3750	750	250+ 자산 수수료	250	1.450.000
440.721-484.720	5000	3750	750	250+ 자산 수수료	250	1.600.000
484.721-528.720	5000	3750	750	250+ 자산 수수료	250	1.750.000
528.721-572.720	5000	3750	750	250+ 자산 수수료	250	1.900.000
572.720-xxx.xxx	4500	3375	675	225+ 자산 수수료	225	1.900.000

문의

디스코드: https://discord.gg/2T8xG7e

텔레그램: https://t.me/raptoreumm

트위터: https://twitter.com/raptoreum

레딧: https://www.reddit.com/r/raptoreum/

참고문헌

[1] 2018 51% and double spend attacks:
https://thenextweb.com/hardfork/2018/10/23/cryptocurrency-51-percent-attacks/
[2] Cost to perform 51% attacks:
https://www.crypto51.app/
[3] Raptoreum GhostRider Explained:
https://medium.com/@kawwwoin/raptoreums-ghostrider-algorithm-explained-93f1f8070158