THETA

NETWORK

Decentralized video streaming, powered by users and an innovative new blockchain.

WHITEPAPER

새로운 블록체인으로 동작하는
분산형 비디오 스트리밍 및 전송 네트워크

Last Updated: 2018년 11월 11일
Version 2.0

요약

이 백서는 분산 비디오 스트리밍과 전송 네트워크를 위한 인센티브 메커니즘인 새로운 블록체인과 토큰인 Theta네트워크를 소개합니다.

THETA 네트워크와 프로토콜은 오늘날 비디오 스트리밍 산업이 직면한 다양한 문제들을 해결합니다. 첫번째로, THETA 토큰은 각각의 유저들이 캐싱 노드로서 THETA 네트워크에 참여하도록 독려하는 역할을 합니다. 유저들은 그들의 기기에서 쓰이고 있지 않는 컴퓨팅 파워와 대역폭을 공유함으로써 THETA 네트워크의 캐싱 노드로 참여할 수 있습니다. 그 효과로 비디오 스트림의 질은 향상되고, 전통적인 스트림 전달 파이프라인에서의 병목문제인 "last-mile problem"이라고 불리는 문제가 해결됩니다. 특히 이러한 문제는 4K, 8K 그리고 다음 세대의 스트림 방식과 같은 높은 비트율을 가진 영상에서 더 두드러지는데 THETA네트워크는 이러한 문제를 해결할 수 있습니다. 두 번째로, 충분한 수의 캐시 노드가 있으면, 대다수의 시청자가 기존의 서버가 아닌 주변의 캐싱 노드로부터 스트림을 가져옵니다. 이것은 기존content delivery network (CDN)에서 대역폭을 위해 유지되는 비용을 획기적으로 감소시키는 효과를 가져옵니다. 더 중요하게는, 엔드 유저의 인센티브 메커니즘으로 토큰을 도입함으로써 Theta 네트워크는 비디오 플랫폼들이 더 깊은 시청자 참여를 유도하고, 더 많은 수익을 이끌어내고, 그들의 경쟁자들과는 차별화된 시청자 경험과 컨텐츠를 이끌어내도록 해줍니다.

Theta 블록체인의 세가지의 새로운 개념을 소개합니다:

- **Multi-Level BFT:** 수정된 BFT 합의 메커니즘은 매우 높은 처리량을 유지하는 동시에(TPS 1000이상), 수천개의 노드가 합의 프로세스에 참가할 수 있도록 허용합니다. 핵심 아이디어는 검증자 위원회(validator committee)를 생성하는 노드들의 작은 집합을 갖는 것입니다. 검증자 위원회는 PBFT와 유사한 프로세스를 이용하여 블록들의 체인을 가능한 한 빨리 생성합니다. Multi-level BFT 합의 메커니즘의 이름은 검증자/가디언이 여러 수준의 보안 보증(security guarantee)을 제공하는 것을 반영합니다. 검증자 위원회— 10에서 20의 검증자들로— 는 첫번째 보호 수준을 제공합니다. 이 위원회는 빠르게 합의에 도달할 수 있습니다. 가디언 풀은 두번째 방어선을 생성합니다. 수천개의 노드들을 사용하기 때문에, 악의적인 공격자가 공격하기 상당히 어렵고, 이는 상당히 높은 수준의 보안 레벨을 제공합니다. 우리는 이 메커니즘이 "impossible triangle"이라고 불리는 문제의 세 고민인 트랜잭션 처리량(transaction output), 일관성(consistency), 그리고 탈중앙화 수준(level of decentralization) 사이에서 적절한 균형을 이루고 있다고 믿습니다.

- **통합된 서명 가십 스킴 (Aggregated Signature Gossip Scheme):** 기본적인 All-to-All 브로드캐스팅을 통해 가디언 노드들 간에 체크포인트 블록 해시 값을 전달할 수 있습니다. 하지만 이는 지수적인 커뮤니케이션 오버헤드를 만들어내고, 결국 1000개 이상의 노드로 확장할 수 없도록 합니다. 우리는 메시지 복잡도를 상당히 줄여주는 통합된 서명 가십 스킴을 제안합니다. 각 가디언 노드는 그들의 이웃

노드로부터 부분적으로 통합된 서명을 결합하여 유지하고, 이를 가십 (gossip) 프로토콜로 내보냅니다. 추가로, 서명 통합은 노드와 노드 간의 메시지의 사이즈를 작게 유지하고, 커뮤니케이션 오버헤드를 추가적으로 감소시킵니다.

- **리소스 중심의 소액결제 풀:** 오프-체인 "리소스 중심의 소액결제 풀"은 비디오 스트리밍을 위해 만들어졌습니다. 이는 유저가 오프체인 소액결제 풀을 만들 수 있도록 해줍니다. 오프체인 소액결제 풀안에서 다른 사용자들은 오프체인 트랜잭션을 이용하여 출금할 수 있고, 이중 지불을 막을 수 있습니다. 이는 오프체인 결제 채널보다 훨씬 유동적입니다.

이 백서는 Theta 블록체인과 위의 개념들을 자세히 설명합니다. Theta 네트워크는 ERC20 토큰으로 출시했으며 SLIVER.tv 플랫폼에 2017년 12월에 통합되었습니다. Theta 블록체인 메인넷 코드가 공개되었으며, 첫번째 라이브 메인넷 구현은 2019년 3월 15일로 예정되어 있습니다. 메인넷 시 ERC20 Theta 토큰은 메인넷의 Theta 토큰과 1:1로 교환될 예정입니다.

TABLE OF CONTENTS

Vision

소개

비디오 스트리밍 시장

시스코의 2016년 6월 비쥬얼 네트워크 지수 리포트(Visual Networking Index report)에 따르면, 오늘날 라이브 비디오 스트리밍은 모든 인터넷 트래픽의 2/3 이상 차지하고 있고 2020년까지 82%로 급상승할 것으로 예상됩니다. 미국에서는, 18살에서 34살 사이인 밀레니얼 세대가 비디오 스트리밍의 성장을 이끌고 있고, 인스타그램, 스냅챗(Snapchat), 스포티파이(Sportify) 와 같은 서비스를 많이 사용합니다. SSRS Media and Technology 조사에 따르면, 이 밀레니엄 그룹의 스트리밍 비디오 시청시간은 주당 평균 1.6 시간에서 주당 5.7시간으로 256% 증가했으며, 모바일 기기가 2015 년에 44 %, 2016 년에 35 %의 비디오 소비를 차지하고 있습니다. 미국 시장에서의 Top 5 스트리밍 플레이어로는 페이스북, 구글/유튜브, 트위터 및 Live.ly와 트위치가 있습니다.

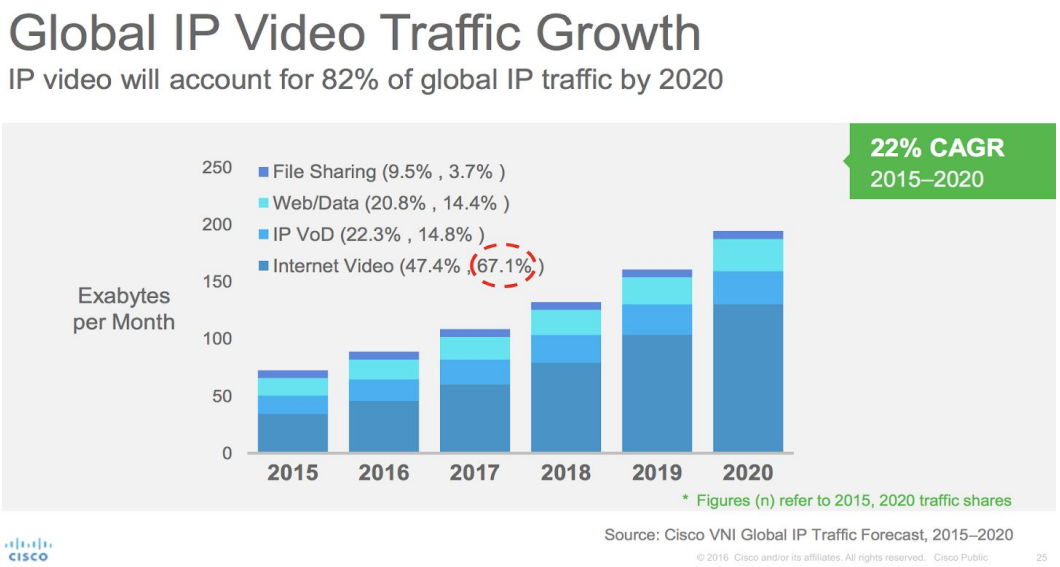

***Figure 1**. 글로벌 IP비디오 트래픽 성장률*

그와 동시에, 동일한 시스코 보고서에 따르면 360° 비디오 스트리밍 컨텐츠를 포함한 글로벌 VR 트래픽은 2020년까지 61배 성장할 것으로 추산되며, 연평균 127% 성장률을 가질 것으로 추산됩니다.

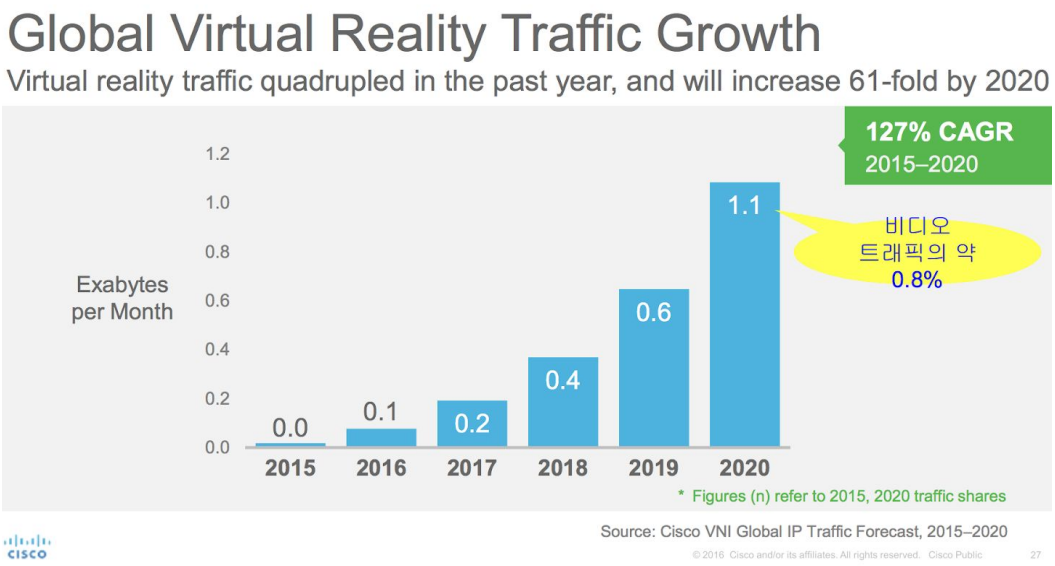

***Figure 2**. 글로벌 가상 현실 트래픽 성장률*[1]

비디오 스트리밍의 도전과제

컨텐츠 전달 네트워크 (CDN)는 비디오 스트리밍 에코시스템에서 중요한 역할을 하고 있습니다. 이 것은 최종 시청자들에게 비디오 스트림을 전달하기 위한 중추적인 기반시설입니다. 오늘날 CDN 네트워크의 주요한 한계는 "last-mile" 전달 문제라고 불립니다.

[1] https://www.cisco.com/c/dam/global/ko_kr/assets/pdf/2016-VNI-Complete-Forecast-PT.pdf

일반적으로 CDN 제공자는 POPs(Point-of-Presences)라고 불리는 데이터 센터를 전세계에 구축합니다. 그러면서 POPs가 시청자들과 지리학적으로 가까운 곳에 있기를 기대합니다. 그러나, POPs의 숫자는 한계가 있고 따라서 많은 시청자들은 충분하게 가까운 거리를 갖지 못합니다. 이 문제는 개발 도상국에서 더 심각하게 나타납니다. 이러한 "last-mile" 링크는 일반적으로 파이프라인을 통한 스트리밍 전달의 병목 지점이 되고, 고르지 못한 스트림과 빈번한 재 버퍼링을 포함하여 사용자에게 종종 안 좋은 경험을 전달합니다.

스트리밍 사이트들과 플랫폼들에게 있어서, 또다른 중요한 문제는 CDN 대역폭의 비용입니다. 유명한 사이트들은, CDN 대역폭에 소모되는 비용이 연간 수천만 달러에 쉽게 도달할 수 있습니다. 플랫폼이 자신의 CDN을 소유하고 있다고 하더라도, 유지비용 또한 너무 높습니다.

이 문제는 향후4K, 8K, 360° VR 스트리밍 및 light filed 스트리밍과 같은 향후 기술에서 더욱 더 두드러지는 문제입니다. 테이블1은 오늘날의 주된 기준인 720p/HD 스트림을 4k, 360° VR 그리고 미래의 lightfield 스트림과 대역폭 요구량을 비교한 것이다. 대역폭 요구량은 규모가 커짐에 따라 매우 빠르게 높아집니다

기준	해상도	대역폭 Mbps	규모
720p HD	1080x720	5 to 7.5	1x
1080p HD	1920x1080	8 to 12	1.6x
4K UHD	3920x2160	32 to 48	6.4x
8K 360° VR	7840x4320	128 to 192	25x
16K 360° VR	15680x8640	512 to 768	100x
Lightfield	---	5000+	1000x

***Table 1**. 대역폭 비교: 오늘날의 720p/1080p 비디오 vs 4K, 360° VR 스트리밍, vs 미래의 volumetric/lightfield 스트리밍*

VR과 light filed 비디오 전달 문제를 해결하기 위해서, 비디오 업계는 "foveated streaming" 기술을 탐구하고 있습니다. 이 기술은 전체 비디오를 최대 해상도로 스트리밍하는 대신 대역폭 요구사항을 줄이기 위해서 주변 시야의 영역 (중요하지 않은 영역)의 이미지 품질을 줄입니다. 시청자가 다른 방향을 보기 위해서 머리를 돌리면, 시스템은 서버로부터 시청 방향의 영상에 대한 고해상도 비디오 패킷을 가져와서 그에 따라 공간 비디오 해상도를 조절합니다. 실제로 foveated streaming 기술이 잘 동작하기 위해서는, 서버와 시청자 간의 패킷 왕복시간이 충분히 작아야 합니다. CDN POPS와 지리학적으로 먼 시청자들에게는, foveated 스트리밍 기술을 사용한다고 하더라도 VR 스트리밍 시청경험이 좋지 않을 것입니다.

배경

SLIVER.tv (이하 "회사")는 2015 년 이후 VR 및 구형 360 ° 비디오 스트림을 위한 차세대 비디오 스트리밍 기술 개발의 선두 주자이고, THETA 네트워크를 설립하였습니다. SLIVER.tv는 실리콘 벨리의 유명한 벤처 캐피털인 Danhua, DCM, Sierra ventures, Creative Artists Agency를 포함한 할리우드 미디어를 이끄는 투자자들, BDMI, Advancit Capital,

Greycroft Gaming Track Fund 그리고 가장 유명한 기업 투자자들인 GREE, Colopl, Samsung Next, Sony Innovation funds가 투자하였습니다. 추가적으로, 회사는 Heuristic Capital Partners, ZP Capital, Green Pine Capital Partners, 그리고 Sparkland를 포함한 강력한 중국 투자자들과 파트너가 있습니다.

"포버티드 스트리밍(foveated streaming)" 기술에서 파생되어 SLIVER.tv에서 특허 출원중인 최신 기술 #62/522,505, "다중 해상도 시청을 위한 비 중심적 원형 투영 방법 및 시스템(METHODS AND SYSTEMS FOR NON-CONCENTRIC SPHERICAL PROJECTION FOR MULTI-RESOLUTION VIEW)"은 특히 VR 스트리밍, 하이라이트 및 리플레이를 위한 고효율 구형 비디오 생성 문제를 해결합니다. 이 기술은 중요한 게임 행동들을 선택적으로 고해상도 디스플레이로 이끌어내기 위해서 비 집중적인 구형 투영(non-concentric spherical projection)을 수행합니다. 동시에, 변화가 없는 게임 배경들은 저해상도로 내보냄으로써 시각적 정확도 와 데이터 전송 부하 간에 트레이드오프를 최적화합니다.

SLIVER.tv는 오늘 2018 년 3 월에 순 방문자가 500 만회가 넘는 최고의 차세대 라이브 e-스포츠 스트리밍 플랫폼으로서 e-스포츠의 사용자 경험을 변화시킬 비전을 갖고 있습니다.
비디오 게임이 할리우드와 볼리우드(Bollywood)를 합친 것보다 더 큰 40 억 달러 규모의 시장으로 성장하면서, 멀티 플레이어 경쟁 비디오 게임의 증가는 관람 스포츠로서 e-스포츠라고 불리는 새로운 주요 산업이 되었습니다. E-스포츠는 유럽, 아시아, 북미지역의 주요 토너먼트들과 경쟁 팀들 그리고 주요 팬들에 의해서 구성된 세계적인 현상입니다. 온라인 게임과 e-스포츠 에코시스템은 과거 5년 동안 폭발적으로 성장했습니다.

최근의 2017 SuperData 연구 결과, YouTube 및 트위치의 게임 비디오 컨텐츠의 시청자를 합친 숫자가 미국 인구의 2 배인 6 억 6,500 만 명에 달했습니다. 이는 HBO 및 Netflix를 시청자 수를 합친 2 억 2 천 7 백만명을 능가합니다. 오늘날, e-스포츠와 게이밍 비디오 컨텐츠는 인터넷의 위에서 스트리밍 되는 비디오 컨텐츠의 상당한 부분을 차지합니다.

SLIVER.tv의 추가적인 핵심 특허들과 기술들은 최첨단 라이브 스트리밍을 통한 다양한 e-스포츠 컨텐츠에 초점이 맞춰져 있습니다. 회사의 미국 특허인 #9,573,062 "가상 현실 스트리밍 및 컴퓨터 비디오 게임의 다시 보기를 위한 방법 및 시스템 (METHODS AND SYSTEMS FOR VIRTUAL REALITY STREAMING AND REPLAY OF COMPUTER VIDEO GAMES)" 그리고 #9,473,758인 "가상 현실 다시 보기 및 게임 비디오 레코딩을 위한 방법 및 시스템 (METHODS AND SYSTEMS FOR GAME VIDEO RECORDING AND VIRTUAL REALITY REPLAY)" 는 완전히 몰입되는 360°VR 구형 비디오 스트림에서 가장 인기있는 PC e-스포츠 게임(LoL, Dota2, Counter-Strike 등)의 캡처 및 라이브 렌더링을 개척하고, 라이브 비디오 스트림을 통해 시청자와 청중을 효과적으로 3D 게임 내에 배치합니다.

작년에 출시된 이후로, SLIVER.tv는 수많은 글로벌 e-스포츠 토너먼트들을 360 ° VR 환경에서 방송하였고, 프리미엄 브랜드인 ESL One, DreamHack and Intel Extreme Masters 들과 함께 하였습니다.
미국과 유럽의 주요 행사로, SLIVER.tv는 Top e-스포츠 게임인 카운트 스트라이크 (CS:GO) 와 리그 오브 레전드(LoL)의 수백만명의 팬들에게 라이브 스트림을 제공했습니다.

SLIVER.tv는 2017 년 7 월에 Watch & Win esports 플랫폼을 출시했으며 e-스포츠 컨텐츠 스트리밍과 팬 참여를 중심으로 설계된 최초의 가상 토큰을 출시했습니다. 출시한 이후로, 회사는 실제 e-스포츠 경기에 적극적으로 참여하고 사로잡음으로써 10 억 개 이상의 가상 토큰을 돌리는 수백만 명의 e-스포츠 팬들을 확보했습니다. 이 사용자들은 출시 후 몇 주 동안 거의 100 년 분량인 5,000만 분(minute)동안 라이브 e-스포츠 스트리밍으로 시청했습니다. 이로써 회사는 오늘날 가상 커뮤니티를 중심으로 구축된 최대 e-스포츠 스트리밍 사이트 중 하나로 자리 매김하고 있습니다.

SLIVER.tv 플랫폼은 입소문, 추천 및 소셜 채널을 통해서 계속해서 빠르게 성장하고 있습니다.

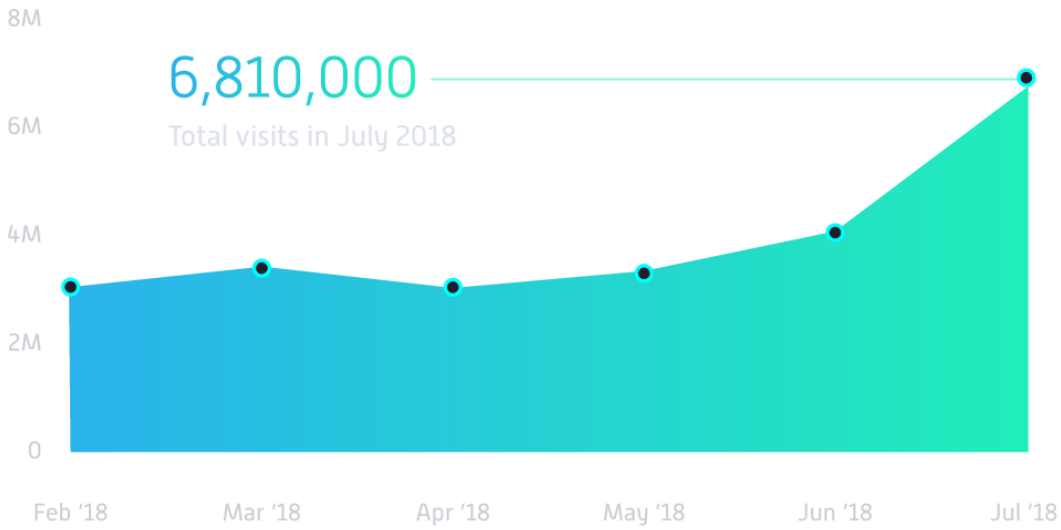

***Figure 3**. 최근6개월간 데스크탑과 모바일 웹에서의 총 방문자*

기회

우리의 도전과제는 블록체인 기술을 활용하여 첫번째 분산형 비디오 스트리밍 및 전달 네트워크를 구축하는 것이고, 비디오 시청자들이 자신들의 남는 컴퓨팅 리소스와 대역폭을 공유함으로써 정당한 보상을 받도록 함으로써 오늘날의 비디오 스트리밍 산업의 문제를 해결하도록 하는 것입니다. 이더리움의 EVM을 "월드 컴퓨터(World Computer)"라고 은유해서 부르는 것처럼, THETA 네트워크는 시청자들의 메모리와 대역폭 공유로 형성된 "월드 캐시(World Cache)"로 볼 수 있습니다.

특히, 전세계에 있는 시청자들은 그들의 컴퓨터를 "캐싱 노드"처럼 기여할 수 있습니다. 이를 통해, 전 세계 어디에서든 시청자들에게 주어진 비디오 스트림을 전달할 수 있도록 하는 비디오 전달 메쉬 네트워크(video delivery mesh network)가 만들어집니다. THETA 네트워크는 이전 섹션에서 논의된 여러 기술적 문제점들을 효과적으로 다룰 수 있습니다. 첫번째로, 시청자들의 디바이스는CDN POPs와의 거리가 매우 먼 반면에, 시청자들의 디바이스들 간에는 지리적으로 서로 매우 가깝습니다. 이러한 지리적 이점은 패킷의 왕복 시간을 줄이고 스트림 전달의 질을 향상시킵니다. 따라서 이전에 언급한 "last-mile" 전달 이슈를 해결할 수 있습니다. 두번째로, 충분한 수의 캐싱 노드가 있으면, 대다수의 시청자가 기존의 서버가 아닌 주변의 캐싱 노드로부터 스트림을 가져옵니다. 따라서 스트리밍 사이트들은 그들의 CDN 대역폭을 위한 비용이 감소하는 효과를 얻을 수 잇습니다. 세번째로, 캐싱 노드는 패킷의 왕복 시간을 줄여 foveated(포버티드) 기술 및 다음 세대의 스트리밍 기술을 실용적으로 만듭니다.

시청자들이 그들의 컴퓨팅 리소스와 대역폭을 공유하도록 독려하기 위해서, 우리는 인센티브 메커니즘으로 THETA 프로토콜을 도입합니다. 캐싱 노드는 다른 시청자들에게 비디오 스트림들을 전달함으로써 보상으로 토큰을 얻을 수 있습니다. THETA 토큰은 시청자들이 네트워크에 참여하게 하기 위한 동기가 될 뿐만 아니라, 비디오 전달 프로세스를 간소화하여 스트리밍 시장의 효율성을 효과적으로 증가시킵니다. 자세한 내용은 뒤에서 다루겠지만, THETA 네트워크안에서 광고주는 적은 비용으로 시청자들을 직접적으로 타겟팅 할 수 있고, 시청자들은 그들이 좋아하는 컨텐츠에 대한 관심과 참여에 대한 보상으로 THETA 토큰을 얻고, 스트리머와 같은 영향력 있는 사람들은 시청자들로부터 THETA 토큰을 선물 받을 수 있습니다. 스트리밍 플랫폼들은 THETA 토큰을 통해CDN 비용을 줄이고 새로운 수익 기회를 열 수 있습니다.

THETA 프로토콜이 완전히 런칭 되면 새로운 블록체인과 고유의 토큰이 도입됩니다:

- 캐싱 노드는 비디오 스트림을 캐싱하고 다른 시청자에게 전달함으로써 토큰을 얻을 수 있습니다.
- 시청자들은 광고주들로부터 참여에 대한 보상으로 선택적으로 토큰을 얻을 수 있고, 자신이 좋아하는 인플루언서나 컨텐츠 제작자에게 선물을 돌릴 수 있습니다.
- 스트리밍 사이트들과 플랫폼들은 프리미엄 상품과 서비스를 판매함으로써 새로운 수익을 이끌어 낼 수 있으며, Theta를 통해 사용자들의 더 깊은 참여를 이끌 수 있습니다.
- 광고주들은 인플루언서, 스트리밍 사이트들과 시청자를 지원하기 위해 토큰을 통해 광고 캠페인을 조성할 수 있습니다.
- 스트리밍 사이트와 플랫폼들은 CDN 비용을 최대 80%까지 줄일 수 있습니다.

THETA 프로토콜은 다음과 같은 개념들에 의해 만들어집니다:

- **Multi-Level BFT:** 수정된 BFT 합의 메커니즘은 매우 높은 처리량을 유지하는 동시에(TPS 1000이상), 수천개의 노드가 합의 프로세스에 참가할 수 있도록 허용합니다. 핵심 아이디어는 검증자 위원회(validator committee)를 생성하는 노드들의 작은 집합을 갖는 것입니다. 검증자 위원회는 PBFT와 유사한 프로세스를 이용하여 블록들의 체인을 가능한 한 빨리 생성합니다. Multi-level BFT 합의 메커니즘의 이름은 검증자/가디언이 여러 수준의 보안 보증(security guarantee)을 제공하는 것을 반영합니다. 검증자 위원회— 10에서 20의 검증자들로— 는 첫번째 보호 수준을 제공합니다. 이 위원회는 빠르게 합의에 도달할 수 있습니다. 가디언 풀은 두번째 방어선을 생성합니다. 수천개의 노드들을 사용하기 때문에, 악의적인 공격자가 공격하기 상당히 어렵고, 이는 상당히 높은 수준의 보안 레벨을 제공합니다. 우리는 이 메커니즘이 "impossible triangle"이라고 불리는 문제의 세 고민인 트랜잭션 처리량(transaction output), 일관성(consistency), 그리고 탈중앙화 수준(level of decentralization) 사이에서 적절한 균형을 이루고 있다고 믿습니다.

- **통합된 서명 가십 스킴 (Aggregated Signature Gossip Scheme):** 기본적인 All-to-All 브로드캐스팅을 통해 가디언 노드들 간에 체크포인트 블록 해시 값을 전달할 수 있습니다. 하지만 이는 지수적인 커뮤니케이션 오버헤드를 만들어내고, 결국 1000개 이상의 노드로 확장할 수 없도록 합니다. 우리는 메시지 복잡도를 상당히 줄여주는 통합된 서명 가십 스킴을 제안합니다. 각 가디언 노드는 그들의 이웃 노드로부터 부분적으로 통합된 서명을 결합하여 유지하고, 이를 가십 (gossip) 프로토콜로 내보냅니다. 추가로, 서명 통합은 노드와 노드 간의 메시지의 사이즈를 작게 유지하고, 커뮤니케이션 오버헤드를 추가적으로 감소시킵니다.

- **리소스 중심의 소액결제 풀:** 오프-체인 "리소스 중심의 소액결제 풀"은 비디오 스트리밍을 위해 만들어졌습니다. 이는 유저가 오프체인 소액결제 풀을 만들 수

있도록 해줍니다. 오프체인 소액결제 풀안에서 다른 사용자들은 오프체인 트랜잭션을 이용하여 출금할 수 있고, 이중 지불을 막을 수 있습니다. 이는 오프체인 결제 채널보다 훨씬 유동적입니다

Theta 메쉬(Mesh) 전송 네트워크

피어-투-피어 스트리밍은 거의 실시간에 가까운 엄격한 실시간 파라미터에 의해 오디오와 비디오 컨텐츠를 전송하는 것에 초점이 맞춰져 있습니다. 피어-투-피어 라이브스트림 전송은 많은 사람들이 같은 스트림을 동시에 사용할 때 가장 좋은 효과를 나타냅니다. 높은 동시 유저들의 수는 더 많은 피어링 리소스가 사용하다는 것을 의미하고 이는 피어 노드들이 서로 다른 각 노드에게서 더 효과적으로 스트림을 가져올 수 있다는 것을 나타냅니다. 전체 시스템의 수용력은 더 많은 피어 노드들이 사용 가능할수록 증가합니다. 더욱더, 노드가 컨텐츠를 받아 오기 위해 중앙화된 서버에 의존하지 않아도 되므로 피어-투-피어 네트워크에서 시스템의 강건함은 더 증가합니다. 이는 특히 서버 실패의 경우 더 중요합니다. 앞서 피어-투-피어 구조와는 반대로, 중앙화된 CDN 기반의 전송에선, 높은 동시 사용자 수는 CDN 서버에 확장성에 대한 압력을 가합니다.

그러나, 순수한 피어-투-피어 스트리밍의 단점은 사용성입니다. 피어들은 언제나 들어오고 떠날 수 있습니다. 이는 어떠한 피어 노드가 사용 가능할지 예측하는데 어려움을 줍니다. 또한 업로드와 다운로드 능력과 같은 노드 간의 차이는 제어할 수 없습니다. 반면에 CDN 서비스는 보다 안정적이고 견고하며, 따라서 다른 피어 노드에게서 스트림을 받아올 수 없는 경우 CDN 서비스가 신뢰할 수 있는 "백업" 역할을 할 수 있습니다.

우리의 목적은 넷플릭스, 유튜브, 트위치, 페이스북과 같은 스트리밍 플랫폼에서 매우 중요하게 작용하는 “QoS (quality of service)”의 희생없이 CDN 필요 대역폭을 최대로 감소시키는 것을 달성하는 것입니다. 이는 가능할 때마다 피어 노드가 CDN으로부터 스트림을 받아오는 것 대신, 다른 피어 노드로부터 스트림을 가져 오기를 원한다는 것을 의미합니다. 이러한 목표를 달성하기 위해, 피어 노드들이 자신의 주변에 있는 노드들을 효과적으로 식별하는 것이 매우 중요합니다. 만약 노드가 근접한 여러 피어를 식별할 수 있으면, 비디오 스트림 세그먼트를 훨씬 더 일관성 있게 제공해 줄 수 있는 피어들을 찾을 수 있습니다. 반대로, 식별된 피어가 네트워크 홉의 측면에서 “멀리 떨어져 있는” 경우, 노드는 식별된 피어에서 일관되게 스트림을 가져오지 못할 수 있으며, 빈번한 중단, 빈번한 재버퍼링 등과 같이 사용자의 경험을 저하시킬 수 있습니다.

이러한 문제를 해결하기 위해서, Theta는 지능적인 플레이어 클라이언트과 최적화된 추적 서버 모두를 결합하여 설계되었습니다. 기본적으로, 추적 서버는 플레이어 클라이언트를 위해 높은 수준의 지도(예시: 후보 피어 리스트)를 제공합니다. 플레이어 클라이언트는 여러 변수를 기반으로 보다 세분화된 피어 필터링 알고리즘을 구현하여 최상의 서비스를 제공할 수 있는 이웃 노드를 찾습니다.

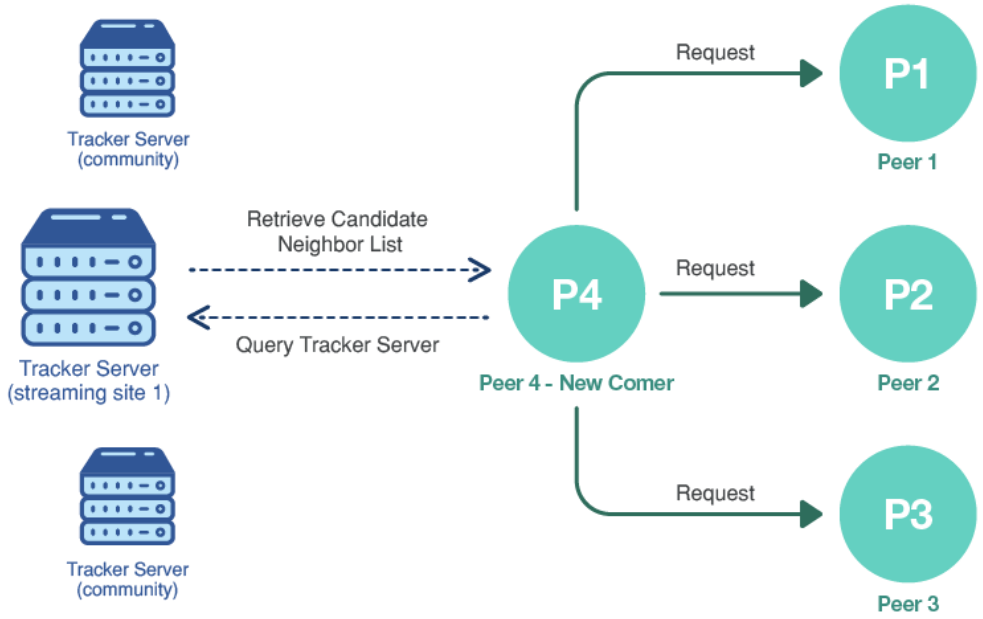

***Figure 4**. 플레이어 클라이언트와 추적 서버 간의 상호작용*

지리적으로-최적화된 추적 서버

각 클라이언트에게 피어 노드 후보 리스트를 제공하기 위해서, 추적 서버는 새로운 피어가 네트워크에 접속할 때마다 IP 주소, 위도/경도, 다른 성능 파라미터를 포함하여 지역 정보를 기록합니다. 이 정보로 서버는 공간 데이터베이스에서 노드를 구성 할 수 있습니다. Theta의 "최대로 최적화된" 공간 데이터베이스는 지리학적 공간에 정의된 객체를 나타내는 데이터 저장 및 쿼리에 최적화되어 있습니다. 피어 노드가 네트워크에 들어올 때, Figure4처럼 서버는 공간 쿼리를 수행하여 이 피어와 매우 근접한 후보자 피어 리스트들을 매우 빠르고 효율적으로 찾아낼 수 있습니다. 추적 서버와 공간 데이터베이스는 Theta 네트워크를 사용하는 비디오 스트리밍 사이트 혹은 컨텐츠 전송을 위한 커뮤니티 피어들에 의해 유지될 수 있습니다.

우리가 앞서 말한 것처럼, 피어 노드는 언제든지 네트워크를 떠날 수 있습니다. 그렇기 때문에 추적 서버는 어떠한 노드들이 활동하고 있는지 인식해야 할 필요가 있습니다. 이를 위해서, 활동하고 있는 피어 노드는 서버와 소켓 연결을 유지해야 할 필요가 있고 주기적으로 heartbeat 신호를 보내야 합니다. 만약 서버가 heartbeat를 일정 시간동안 받지 못했다면, 서버는 피어 노드가 네트워크를 떠난 것으로 간주하고 공간 데이터베이스를 업데이트 합니다.

중요한 차이점은 두 피어 노드간의 "거리"는 지리학적인 거리 대신 두 노드 간의 라우터 홉 수로 계산됩니다. 일반적으로 네트워크 거리와 지리학적 거리는 매우 높은 상관관계를 가지고 있지만, 완전히 동일하지는 않습니다. 예를 들어, 두 개의 컴퓨터는 물리적으로 바로 옆에 위치할 수 있지만, 두 개의 컴퓨터는 서로 다른 ISP에 연결되어 중간에 많은 홉이 존재할 수 있습니다. 따라서, 지리 정보 외에, 추적 서버는 과거에 수집된 IP 주소들 사이의 연결을 이용하여 이웃 후보를 분석하고 선택합니다. 예를 들어, 공간 쿼리에 의해 반환된 후보자들은 시청자의 것과 동일한 ISP에 연결되지 않은 후보자들을 제외하기 위해 다른 필터를 통과할 수 있습니다.

지능적인 사용자 클라이언트

각 피어 노드는 시청자와 캐싱 노드 혹은 두개의 역할을 동시에 할 수도 있습니다. 노드가 시작되고 나서, 헨드세이크 단계 동안, 라이브스트림을 위해 추적 서버로부터 후보 피어들의 리스트를 구합니다. 그런 다음, 스피드와 사용성 테스트를 수행하여 최적화된 성능, 연결성 그리고 안정적으로 비디오 스트림 세그먼트를 제공가능한 작은 집합을 선택합니다. 이 클라이언트는 라이브 스트림 세션 동안 정기적으로 스피드와 사용성 테스트를 수행하고 지속적으로 이웃 리스트를 갱신합니다.

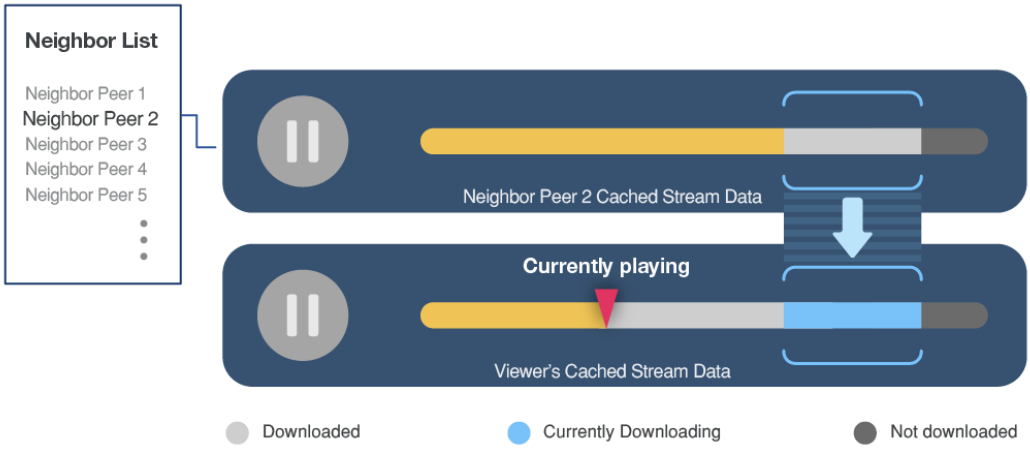

***Figure 5**. 플레이어 스트림 데이터 버퍼 핸들링*

QoS 저하를 피하기 위해, 로컬 버퍼의 관리는 매우 중요합니다. Figure5처럼 클라이언트 플레이어는 로컬 캐시를 다운로드된 스트림 데이터를 저장하기 위해 유지합니다. 캐시된 스트림 데이터의 지속 시간이 특정 임계 값보다 작은 경우, 플레이어는 주변 피어를 확인하여 그들이 플레이어가 원하는 비디오 스트림 세그먼트를 갖고 있는지 확인합니다. 비디오 세그먼트를 갖고 있는 어떠한 이웃 피어도 없는 사건이 발생했을 때, 플레이어는 지능적으로 CDN으로부터 세그먼트를 받아오도록 변경합니다. 가능한 최고의 QoS를 달성하기 위해서, 플레이어는 스트림 세션동안 정기적으로 추적 서버로부터 업데이트된 후보 리스트를 갱신합니다.
첫번째 클라이언트 비디오 플레이어 버전은 web/HTML5 기반의 플레이어로 WebRTC 프로토콜을 피어들간의 스트림 전송을 위해 사용합니다. Web 기반의 플레이어를 배치하는 것은 최소한의 노력만을 요구합니다. 스트리밍 사이트들과 플랫폼들은 간단히 이 플레이어를 그들의 웹페이지에 적용할 수 있고, 즉각적으로 Theta의 메쉬 네트워크의 수백만 사용자 노드들에게 접근하고 "실행"할 수 있습니다. 따라서, Theta의 메쉬 스트리밍 기술의 배치는 매우 경량화 되어 있고 마찰 없이 적용될 수 있습니다.

Theta는 또한 데스크탑과 모바일 클라이언트를 지원할 예정입니다. Web/HTML5 플레이어에 비해 데스크탑 클라이언트 앱이 가지는 이점은 비디오 스트림 전송을 백그라운드에서 실행시켜, 사용자가 비디오 스트림을 시청하고 있지 않을 때에도 실행시킬 수 있다는 점입니다. 또한 Theta는 스트림 전송 및 재방송을 위해 특별히 설계된 전용 하드웨어, IoT 장치, SmartTV 및 관련 접근 방법을 조사하고 있습니다. 이러한 장치는 잠재적으로 더 나은 사용성과 대역폭을 제공할 수 있습니다.

Theta Blockchain Ledger

Theta렛져(원장, ledger)는 비디오 스트리밍 산업을 위해 설계된 분산 원장입니다. 이는 사용자들이 자신의 기기에서 사용하지 않는 대역폭과 저장공간을 공유하도록 Theta 토큰 경제에 동기를 부여하며, 사용자들이 더욱더 비디오 플랫폼과 컨텐츠 제작자와 보다 활발히 참여하게끔 독려합니다. 이러한 목표를 실현하기 위해서는 비디오 스트리밍 어플리케이션만의 고유한 많은 도전 과제들을 해결해야 합니다.

많은 문제 중 하나는 엄청나게 높은 트랜잭션 처리량을 지원하는 것입니다. 많은 블록체인 프로젝트들이 트랜잭션 처리량 문제에 직면함에도 불구하고, 라이브 비디오 스트리밍의 스케일링 문제는 좀 더 어렵고 복잡합니다. 전통적으로, 비디오 세그먼트의 길이는 2초입니다. 약 1만 명의 동시 시청자가 있는 라이브 스트리밍에서는 초당 수천개의 마이크로 트랜잭션이 생성될 수 있습니다. 이런 상황에서 세분화된 토큰 보상을 —비디오 세그먼트 당 하나의 소액 지불(micropayment) — 주기 위해서는 비트코인과 이더리움 같은 오늘날의 퍼블릭 체인의 최대 처리량을 훨씬 초과하는 트랜잭션 처리량이 필요합니다. 메이저 e-스포츠 토너먼트와 같이 인기있는 라이브 스트리밍들은 하나의 라이브 스트리밍에 1만명이 넘는 동시 시청자들을 끌어들입니다. 이로 인해 잠재적으로 초당 트랜잭션 수만 건을 필요로 할 수 있습니다.

높은 처리량의 부정적인 면은 급속적으로 커지게 되는 저장공간의 소모입니다. 소액지불(micropayment)의 저장은 높은 저장공간을 요구합니다. 매초마다 수만개의 트랜잭션 들이 원장(ledger)으로 추가되기 때문에, 일반적인 컴퓨터의 저장 공간은 빠르게 고갈될 수 있습니다

비디오 스트리밍 어플리케이션은 전통적으로 빠른 합의를 필요로 합니다. 대역폭 공유 보상을 위해, 여분의 대역폭을 제공하는 사용자들은 당연히 다음 비디오 세그먼트를 보내기 전에 결제가 확인(confirm)되기를 원할 것입니다. 다른 유스케이스(use cases)로는, 라이브 스트리밍을 하는 스트리머에게 주는 도네이션이 있습니다. 도네이션은 시청자와 스트리머 간의 실시간 상호작용을 위해 짧은 확인 시간을 요구합니다.

마지막으로 하지만 최소한으로, 다른 블록체인들과 같이, 원장의 보안은 중요합니다. 보안은 탈중앙화의 레벨과 높은 연관성을 가지고 있습니다. 지분 증명(PoS)기반의 합의 알고리즘에서, 탈중앙화는 합의 참여자들 사이의 지분의 분포를 의미하기도 합니다. 이상적으로, 이러한 합의 알고리즘은 수천개의 독립적인 노드가 존재하며, 각 노드가 비슷한 양의 지분을 갖고 있고, 블록의 최종 완결(block finalization) 과정에 참여하며, 노드 각각이 로컬 블록체인 복사본을 갖고 있어야 합니다. 이러한 시스템을 손상시키기 위해서는 상당한 수의 독립적인 노드들이 공격자에 의해 제어되어야 하기 때문에 공격자가 이를 실현시키기는 매우 어렵습니다.

위의 여러 목적들을 달성하기 위해서, 우리는 원장(ledger) 소프트웨어를 실행시키는 노드들 중 2/3 이상이 정직할 경우 일관성(consistency, safety) 과 같은 확실한 보장을 제공하는 비잔티움 장애 허용(BFT) 기반의 PoS 합의 알고리즘을 디자인하였습니다. 그러나, 전통적인 BFT 알고리즘은 높은 수준의 탈중앙화를 허용하지 않습니다. 이는 일반적인 상황(정직한 제안자, non-faulty proposer)에서 조차 $O(n^2)$의 메시지 복잡도를 가지기 때문입니다. 여기서 n은 합의 프로토콜에 참여하는 노드의 숫자를 의미합니다. 우리가 수천개의 노드를 갖고 있을 때, 합의에 도달하기까지 상당한 시간이 소요됩니다. 이 문서에서, 우리는 새로운 **multi-level BFT 합의 메커니즘**을 소개합니다. 이 합의 메커니즘은 수많은 참여자들을

허용하며, 수초정도로 짧은 트랜잭션 승인 시간을 가지며 1000 TPS 이상의 처리량을 달성할 수 있습니다.

이러한 트랜잭션 처리량의 수준은, 이미 비트코인과 이더리움보다 훨씬 높은 처리량이긴 하지만, "바이트 당 지불(pay-per-byte)"과 같은 소액지불(micropayment)을 보장하기에는 충분치 않습니다. 처리량을 더욱더 증가시키기 위해서, Theta ledger는 지원 가능한 처리량을 몇배로 늘려주는 "리소스 중심의 소액지불 풀(resource oriented micropayment pool) "과 함께 오프-체인 스케일링을 기본 지원합니다.

오프-체인 지불은 처리량을 증가시킬 뿐만 아니라, 블록체인에 저장되어야 하는 트랜잭션의 수를 감소시켜야 한다는 것을 명심해야 합니다. 뿐만 아니라, 우리는 저장 공간 요구를 줄이기 위해서 상태와 블록 기록을 가지치기(pruning)하는 기술을 소개합니다. 또한, 다양한 머신 및 스토리지 백 엔드, 데이터 센터 또는 데스크탑 PC에서 실행되는 강력한 서버 클러스터에 적용할 수 있는 스토리지 시스템을 위해 마이크로서비스 아키텍처를 채택하였습니다.

합의 메커니즘

Multi-Level BFT

본 문서에서 우리는 수천개의 노드들이 합의 프로세스에 참가할 수 있으면서 매우 높은 트랜잭션 처리량을 지원하는 (1000+ TPS) multi-level BFT 합의 메커니즘을 제안합니다. 이 아이디어의 핵심은 검증자 위원회(validator committee)를 형성하는 작은 노드들의 집합을 갖는 것입니다. 이 검증자 위원회는 PBFT와 유사한 [2]프로세스를 사용하여 가능한 빨리 블록을 생성합니다. 충분한 수의 검증자(10에서 20)로 구성된 검증자 위원회는 블록들을 빠른 속도로 제공 가능하고, 공격자가 손상시키기에는 충분히 어렵습니다. 따라서, 위원회가 매우 높은 확률의 포크 없이 블록 체인을 생성하리라 기대하는 것은 충분히 합리적입니다. 가디언(guardians)이라고 불리는 수천 명의 합의 참여자들은 검증자 위원회로부터 생성된 체인을 완결(finalize)지을 수 있습니다. 여기서 완결(finalization)이란 "자기를 제외한 모든 가디언들의 2/3이상이 같은 블록체인을 본다는 것"을 각자의 정직한 가디언들에게 확신시키는 것을 의미합니다.

검증자보다 더 많은 가디언들이 존재하므로, 가디언들이 합의에 도달하는 것이 검증자 위원회가 도달하는 것보다 더 오래 걸릴 것입니다. 가디언들이 검증자 위원회가 새로운 블록들을 제공하는 속도에 맞춰서 블록들의 체인을 완결 짓기 위해, 가디언들은 블록들을 좀 더 큰 덩어리 나눠(at a much coarser grain) 처리할 수 있습니다. 좀 더 자세히 말하자면, 가디언들은 체크포인트 블록 — 어떤 정수T (예, T=100)의 배수의 높이를 가진 블록들 — 에 대한 해시(hash)만 동의하면 됩니다. 이러한 "립프로깅 (leapfrogging)" 완결 전략은 블록체인 데이터 구조의 불변성 특징을 활용합니다 – 두개의 가디언 노드가 어떤 한 블록의 해시에 동의하는 한, 두개의 노드는 압도적인 확률로 이 블록까지의 동일한 전체 블록체인을 갖게 됩니다. 체크포인트 블록만을 완결 짓는 것은 수천개의 가디언들이 합의에 이르기에 충분한 시간을 갖게 합니다. 따라서, 이 전략에서, 두가지의 독립적인 프로세스인 블록 생성(production)과 완결(finalization) 작업이 동일한 속도로 진행될 수 있습니다.

정상적인 조건에서, 체크포인트 블록을 완결(finalizing)짓는 것은BFT 알고리즘에서의 "커밋(commit)" 단계와 비슷합니다. 왜냐하면 각각의 가디언이 로컬 저장소에 체크 포인트

2

블록을 이미 저장했기 때문입니다. 또한, 체크포인트 블록은 검증자 위원회에 의해 서명되고, 결국엔 모든 정직한 가디언들이 같은 체크포인트를 가지게 될 확률이 높습니다. 따라서, 정직한 가디언들이 전체 가디언들의 2/3 이상이 같은 체크포인트 해시 값을 갖고 있다는 것을 확인하는 프로토콜만이 필요합니다.

단순히 체크 포인트 블록 해시 값을 전체 노드 대 전체 노드(all-to-all)로 브로드캐스팅(broadcasting)하는 것은 작동하긴 하지만, 이는 지수적인 오버헤드를 발생시키고, 많은 수의 가디언들로 확장시킬 수 없게 합니다. 대신 우리는 메시지 복잡도를 상당히 줄일 수 있는 aggregated signature gossip 스킴을 제안합니다. 핵심 아이디어는 간단합니다. 각각의 가디언 노드들은 주변 노드들로부터 통합된 서명(aggregated signature)들을 부분적으로 결합한 다음, 서명자들의 리스트들을 부호화(encode)한 압축 비트맵(compact bitmap)과 함께 통합된 서명들을 gossip프로토콜에 내보냅니다.
이렇게 하면 가십 프로토콜 덕분에 각 노드의 서명 공유가 기하 급수적으로 빠르게 다른 노드에 도달할 수 있습니다. 높은 확률로 $O(\log\ n)$ 회의 반복동안, 모든 정직한 가디언 노드들은 네트워크 분할(partition)이 없는 경우 다른 모든 정직한 노드들의 서명들을 통합하는 문자열(string)을 가지고 있어야 합니다. 한편으론, 서명 통합 (signature aggregation)은 노드 간 메시지들을 작은 사이즈로 유지하여 통신 오버헤드를 추가적으로 줄입니다.

위에서 언급한 것처럼, 검증자 위원회는 검증자 노드들의 제한된 집합(set)으로 구성됩니다 (일반적으로, 10에서 20개의 제한된 집합). 이들은 보안을 증가시키기 위해서 투표 과정을 통해 선출되거나, 랜덤한 과정, 혹은 교대로 선출될 수 있습니다. 검증자 위원회에 참여할 기회를 얻으려면, 노드는 특정한 양의 지분을 일정 기간 동안 락업(look up)하여야 합니다. 이렇게 락업한 지분은 노드가 악의적인 행동을 하여 발견될 시 삭감(slash) 될 수 있습니다. 위원회가 합의(consensus)에 도달한 블록들을 우리는 합의된 블록(settled blocks)이라고 부릅니다. 그리고 블록을 합의하기 위한 과정을 우리는 블록 합의 과정(block settlement process)이라고 부릅니다.

가디언 풀은 검증자 위원회의 *상위집합(super set)*입니다. 즉 하나의 검증자는 하나의 가디언입니다. 이 풀은 수천 개가 될 수 있는 많은 수의 노드를 포함하고 있습니다. 특정 기간 동안 특정한 양의 토큰 수를 락업 함으로써, 네트워크에 속한 어떠한 노드든 즉각적으로 가디언이 될 수 있습니다. 가디언들은 검증자 위원회로부터 생성된 블록들의 체인을 다운로드하고 검사합니다. 그리고 위에서 설명한 "립프로깅(leapfrogging)" 방식처럼 체크포인트에서 합의에 도달합니다. 많은 수의 참가자들을 허용함으로써, 우리는 트랜잭션 보안을 상당히 강화할 수 있습니다. 가디언 풀에서 합의에 도달한 블록들을 완결된 블록(finalized blocks)이라고 부릅니다. 그리고 블록을 완결(finalize) 시키기 위한 과정을 블록 완결 과정(block finalization process)이라고 부릅니다.

Multi-level BFT 합의 메커니즘의 이름은 검증자/가디언이 여러 수준의 보안 보증(security guarantee)을 제공하는 것을 반영합니다. 검증자 위원회— 10에서 20의 검증자들로— 는 첫번째 보호 수준을 제공합니다. 이 위원회는 빠르게 합의에 도달할 수 있습니다. 이것은 이미 악의적인 공격에 충분한 저항력이 있습니다. — 사실, 각각의 검증 노드가 개별적인 개체라면 이것은 이미 DPoS 메커니즘과 비슷한 수준의 보안 레벨을 제공합니다. 따라서, 트랜잭션은 합의된 블록에 포함될 때 이미 충분히 안전한 것으로 여겨질 수 있습니다 (특히 소액의 거래인 경우). 가디언 풀은 두번째 방어선을 생성합니다. 수천개의 노드들을 사용하기 때문에, 악의적인 공격자가 공격하기 상당히 어렵고, 이는 상당히 높은 수준의 보안 레벨을 제공합니다. 검증자 위원회가 완전히 공격자들에 의해 제어되는 희박한 경우에도, 가디언들은 검증자들을 다시 선별하고, 블록체인은 가디언들에 의해 완결된(finalized) 가장 최신 블록부터 다시 시작할 수 있습니다.
트랜잭션은 finalized block에 포함될 때 되돌릴 수 없는 것으로 간주됩니다. 우리는 이 메커니즘이 "impossible triangle"이라고 불리는 문제의 세 고민인 트랜잭션

처리량(transaction output), 일관성(consistency), 그리고 탈중앙화 수준(level of decentralization) 사이에서 적절한 균형을 이루고 있다고 믿습니다.

이 multi-level 보안 스킴은 비디오 스트리밍 어플리케이션에 적합합니다. 스트리밍 플랫폼애서는, 대다수의 트랜잭션들이 일반적으로 적은 가치를 지니고 있지만 빠른 확정(confirmation)이 필요한 소액지불(micropayment) —피어 대역폭, 스트리머에게 주는 도네이션들을 위한 결제 등—입니다. 이러한 낮은 지분(stake) 결제의 경우, 사용자들은 단 몇 초 만에 일어나는 매우 빠른 블록 합의(block settlement)만 기다리면 됩니다. 높은 지분(stake) 전송의 경우, 약간 더 많은 시간을 기다려야 할 필요가 있습니다. 하지만 이 또한 몇 분내로 처리됩니다.

시스템 모델

블록 합의(settlement)와 완결(finalization) 프로세스의 자세한 사항을 살펴보기 전에, 먼저 우리의 시스템에 대해 몇 가지 가정을 나열하겠습니다. 논의의 편의를 위해서, 각각의 노드들이(검증자 혹은 가디언) 같은 양의 지분을 갖고 있다고 가정하겠습니다. 알고리즘을 서로 다른 노드들이 서로 다른 양의 지분을 갖고 있는 일반적인 케이스로 확장하는 것은 간단합니다.

검증자 위원회 실패 모델: 총 m개의 검증자 노드들이 존재합니다. 대부분의 시간에서, 최대 3분의 1은 비잔티움 노드들입니다. 이들은 공격자들에 의해서 완전히 제어될 수도 있지만, 이는 가끔씩 발생되는 일입니다. 또한, 검증자 노드들의 어떠한 쌍이든 직접적인 메시지 교환 채널이 있다고 가정하겠습니다. (예: 직접적인 TCP 연결)

가디언 풀 실패 모델: 총 n개의 가디언 노드들이 존재합니다. 언제 어느 때나, 최대 3분의 1은 비잔티움 노드입니다.
두개의 가디언들 간의 직접적인 메시지 채널을 여기서는 가정하지 않습니다. 두개의 노드 간의 메시지는 다른 노드를 거쳐 전달되어야 합니다. 이렇게 메시지를 중간에서 전달해주는 노드 중 일부는 비잔티움 노드일 수도 있습니다.

타이밍 모델: 우리는 "약한 동기화" 모델을 가정합니다. 더 자세하게 설명하면, 네트워크는 비동기화 될 수 있고, 또는 한정된 시간동안 분할 될 수도 있습니다. 이러한 비동기 기간동안, 두개의 정직한 노드들 간의 모든 트랜잭션 메시지들이 시간 임계 값으로 알려진 Δ 안에 도착할 충분한 기간이 있습니다. 우리가 이 문서에서 나중에 논의할 것처럼, 비동기 기간 동안에는, 렛져(ledger)는 단순히 새로운 블록들을 생성하는 것을 멈춥니다. 네트워크가 분할되더라도 절대 충돌되는 블록들을 생성하지 않습니다. 동기화 단계 동안에는, 블록 생산이 자연스럽게 재개되고, 결국엔 생기성(liveness)을 얻을 수 있습니다.

공격자 모델: 우리는 막강한 공격자를 가정합니다. 그들은 많은 수의 목표한 노드들을 손상시킬 수 있지만, 동시에 가디언들의 3분의 1 이상을 손상시키지는 못합니다. 그들은 대규모로 네트워크를 조작할 수 있고, 한정된 기간 동안 네트워크를 분할시킬 수 있습니다. 하지만 그들은 계산적인 한계를 갖고 있습니다. 그들은 가짜 서명을 위조할 수 없고, 암호화 해시 값을 원래 값으로 되돌릴 수 없습니다.

블록 합의(Settlement) 프로세스

블록 합의(settlement)는 검증자 위원회가 가디언 풀이 finalize할 수 있도록 블록들의 체인을 생성하고 동의에 이르는 과정입니다. Tendermint[3], Casper FFG[4]및 Hot-Stuff[5]를 포함한 최근의 Proof-of-Stake 연구 작품에서 영감을 얻어, 아래에 설명된 블록 합의(settlement) 알고리즘을 설계하고 구현했습니다. 검증자가 차례대로 새로운 블록을 제안하는 회전 블록 제안자 전략(rotating block proposer)을 사용합니다. 그런 다음위원회는 Casper FFG 및 Hot-Stuff와 유사한 프로토콜을 사용하여 블록들의 순서를 결정하기 위해 블록에 투표합니다.

블록 제안(Block proposal)

검증자들은 블록 제안자(block proposer)의 역할을 수행하기 위해서 라운드 로빈(round robin) 방식에서 회전합니다. 블록 제안자는 검증자 위원회가 투표할 다음 블록을 제안해야 할 책임이 있습니다. 라운드 로빈 회전을 위해서, 각각의 제안자는 epoch이라고 불리는 지역 논리 클락(local logical clock)를 유지합니다. epoch t 동안 m 개의 검증자가 있다고 가정했을 때, ($t \bmod m$) 인덱스를 가진 검증자가 epoch을 위한 제안자로서 선출됩니다. 중요한 2가지 사항은 다음과 같습니다.

1) Epoch t는 멈추지 않아야 합니다. 이렇게 함으로써 제안자 회전의 생기성(liveness)이 보장됩니다.
2) 서로 다른 검증자들의 epoch t는 대부분 동기화 되어있어야 합니다. 즉, 모든 검증자들의 대부분의 시간은 같은 t 값을 가지고 있습니다. 따라서 그들은 어떤 노드가 다음 블록을 생성할지 동의할 수 있습니다.

아래는 제안자 선출 및 블록 제안을 위한 우리의 알고리즘입니다.

알고리즘1: 라운드 로빈(Round Robin) 블록 제안

[3] *Buchman et al*. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains

[4] *Buterin et al*. Casper the Friendly Finality Gadget

[5] *Yin et al*. HotStuff: BFT Consensus in the Lens of Blockchain

```
t ← 0,  proposer ← 0
voted ← false, received ← false, timeout ← false

loop begin
   proposer ← t mod m
   if (proposer == self.index) and (not proposed yet) begin // 노드가 제안자로서 선출됨
      propose one block
   end

   voted ← the node has proposed or voted for a block for epoch t
   received ← the node has received m/3 + 1 EpochChange(t + 1) messages
   timeout ← timeout reached
   if voted or received or timeout begin
      broadcast message EpochChange(t + 1)
   end

   if the node has received 2m/3 EpochChange(t + 1) messages begin
      t ← t + 1 // enters epoch t + 1
      voted ← false, received ← false, timeout ← false
   end

   sleep for some time
end
```

***Algorithm 1**. 라운드 로빈 블록 제안 프로토콜*

이 프로토콜은 메시지 $EpochChange(t + 1)$를 정의합니다. 이는 다음 epoch t + 1로 함께 진행하는 것을 돕기 위해 검증자들 사이에서 전달되는 동기화 메시지로서 간주될 수 있습니다. 기본적으로, 검증자는 다음과 같은 조건들을 만족할 때 $EpochChange(t + 1)$ 메시지를 다른 모든 검증자에게 브로드캐스트(broadcast) 합니다:

1) 노드가 epoch t 동안 블록을 제안하거나 투표한 경우. 또는
2) 노드가 다른 검증자들로부터 $m/3 + 1$ 개의 $EpochChange(t + 1)$를 수신한 경우. 또는
3) 노드가 에 epoch t 대해 시간이 초과(time out)된 경우 (timeout 은 4 Δ 로 설정)

한편, 검증자는 다른 노드들로부터 $2m/3$ 개의 $EpochChange(t + 1)$ 메시지를 받았을 때 epoch 로 진입(enters)합니다.

여기서 우리는 이 프로토콜이 위의 두가지 조건을 만족하는 것을 보여줍니다.

Eventual Progression: 모든 정직한 노드들은 결국(eventual)에 epoch $t + 1$에 진입합니다. 최악의 경우에, 모든 정직한 노드들은 (적어도 $2m/3 + 1$ 의 노드들)은 타임아웃에 도달하고 $EpochChange(t + 1)$ 메시지를 브로드캐스트 합니다. 타이밍 모델 가정 아래에서, 이러한 모든 메시지들은 전송되고 나서 시간 Δ 안에 전달됩니다. 따라서 각각의 정직한 노드는 적어도 $2m/3$ 개의 $EpochChange(t + 1)$ 메시지들을 받게 되고, 결국 epoch $t + 1$에 진입합니다.

Epoch 동기화: 직관적으로, 이것은 모든 정직한 노드들의 epoch의 "함께 움직임 (move together)"를 의미합니다. 더 정확히 말하자면, 우리는 정직한 노드가 epoch $t + 1$에 진입하는 것이 최대 2Δ 만큼 다르다는 것을 주장합니다. 이것을 증명하기 위해, 최대 f 개의 결함 노드가 있기 때문에, 첫번째 정직한 노드가 epoch $t + 1$에 진입하기 위해서는, 적어도 $m/3$ 개의 다른 정직한 노드들이 $EpochChange(t + 1)$ 메시지를 브로드캐스트 해야 합니다. 이 정직한 노드는 또한 프로토콜에 따라 $EpochChange(t + 1)$ 메시지를 브로드캐스트 합니다. 최대 Δ의 시간이 지난 후, 어떠한 정직한 노드든 적어도 $m/3 + 1$ 개의 $EpochChange(t + 1)$ 메시지를 수신하여야 합니다. 이 메시지를 수신함으로써 수신한 노드들이 $EpochChange(t +$

1)를 브로드캐스트하게 됩니다 (위의 조건2). Δ 의 시간이 지난 후, 모든 정직한 노드는 $2m/3$ 개의 $EpochChange(t+1)$ 메세지를 수신하고 epoch $t+1$에 진입합니다. 따라서, 첫번째 정직한 노드가 epoch $t+1$에 진입한 후에 최대 2Δ 시간이 지난 후 마지막 정직한 노드가 같은 epoch에 진입합니다.

실제로, 네트워크 지연이 충분히 작을 때, 모든 정직한 노드는 거의 동시에 epoch $t+1$에 진입합니다. 결과적으로, 검증자들은 누가 다음 제안자가 될지 동의할 수 있습니다. 또한 실제 구현을 위해서 주의할 점은, $EpochChange(t+1)$ 메시지들은 효율성을 위해 다른 타입의 메시지(예: 블록 투표)들과 결합될 수 있습니다. 따라서 일반적인 상황에서 (제안자 실패가 없을 때), epoch 변경을 위해 추가적인 동기화 오버헤드가 시스템에 추가되지 않습니다.

검증자 간 블록 합의(Consensus)

제안된 블록을 합의하기 위한 이 프로토콜은 Casper, FFG 그리고 Hot-Stuff와 비슷하게 모든 검증자 간의 PBFT-기반의 투표 절차를 포함합니다. Theta Ledger 블록체인에서는, 비트코인 및 이더리움과 유사하게 각각의 블록 헤더는 그들의 부모 블록(즉, 체인에서의 이전 블록)의 해시 포인터를 포함하고 있습니다. 블록이 다른 블록의 조상이 아니면 두개의 블록은 충돌합니다. 충돌하는 블록 제안(block proposal)이 같은 epoch 동안 여러 개가 존재한다면, 정직한 검증자는 하나의 블록이 합의될 때까지 여러 개 모두를 유지하고 있다가, 합의 된 블록이 생기면 나머지 충돌되는 블록 모두를 버립니다.

블록 합의 프로토콜은 epoch에서 epoch으로 작동합니다. 현재의 epoch를 위한 제안자는 모든 검증자들에게 블록 제안을 전송합니다. 검증자는 블록에 대한 투표를 브로드캐스팅 함으로써 응답합니다. 모든 메시지들은 보낸 노드에 의해서 서명됩니다. 제안된 블록의 헤더는 부모 블록에 대해 적어도 $2m/3+1$개 이상의 서명된 투표로 구성된 커밋(commit)-인증서(certificate)를 가질 수 있습니다. 결함이 있는 검증자들이 $m/3$을 넘지 않는다는 가정 하에, 높이(height) 당 최대 하나의 블록만이 커밋-인증서를 얻을 수 있습니다. 하나의 블록의 커밋-인증서는 이 블록과 모든 이전 블록들이 합의되었다는 것을 나타냅니다. 제안된 블록은 부모 블록이 $2m/3+1$ 개 이상의 서명된 투표를 얻지 못한다면 커밋-인증서를 가지고 있지 않을 수 잇습니다.

현재 제안자(proposer)가 아닌 검증자들의 경우, 그들의 일은 제안된 블록에 대해서 투표하는 것입니다. 검증자가 새로운 블록을 받자마자, 검증자는 서명된 투표를 다른 모든 검증자에게 브로드캐스트 합니다. 따라서 다음 epoch의 제안자가 커밋-인증서를 생성하기 위해 이를 수집할 있습니다. 두개의 연속적인 블록 A와 B 모두 커밋-인증을 받을 경우, 블록 A와 그 이전 블록 모두 합의(settled)된 것으로 여겨집니다. 안정성을 보장하기 위해, 정직한 노드들이 합의된 블록과 충돌되는 블록에 절대로 투표하지 않도록 하여야 합니다. 포크가 있을 때 (결함 있는 제안자 혹은 비동기화에 의해서), 정직한 노드들은 가장 긴 포크의 블록에 대해서 투표하여야 합니다.

아래의 그림은 블록 합의 과정을 나타냅니다. 높이 101의 제안자가 결함이 있고, 두개의 충돌되는 블록 X_{101}, Y_{101}를 제안했다고 가정했을 때, 이것은 두개의 분기를 이끕니다. 블록 X_{101}, Y_{101}둘 개 모두 $2m/3+1$ 이상의 투표를 받지 못한 다면, X_{102} 와 Y_{102}의 두개 헤더 모두 커밋-인증이 포함되어 있지 않습니다 (그림에서 nil 로 표시되었음). 하지만, 어느 지점에서 분기 X가 더 빠르게 커지고, 두개의 연속적인 블록 X_{102} 와 X_{103} 모두 $2m/3+1$ 이상의 투표를 얻습니다. 그런 다음 X_{102}블록까지의 위쪽 블록 분기 X는 합의된 것으로 간주됩니다. 그리고 아래 분기 Y는 버려집니다.

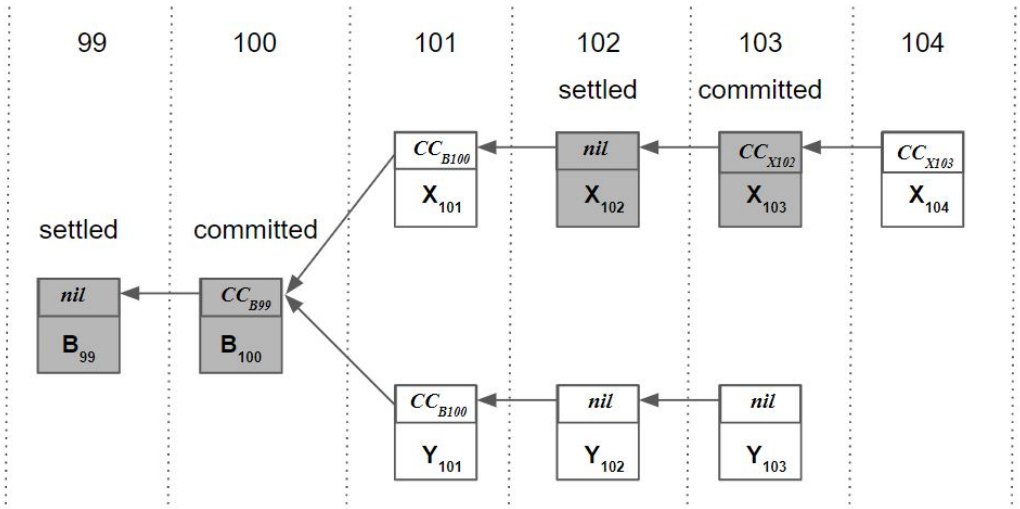

***Figure 6**. 블록 합의(settlement) 과정*

위의 예제는 텐더민트(Tendermint)와 같은 PBFT 기반의 프로토콜과 비교하여 우리의 구현의 강점이 무엇인지에 대해서 설명합니다 — 자식 블록들 중 하나가 합의(settled) 된다면, 커밋(commit)-인증서(certificate)를 받지 않은 하나의 블록 또한 합의된 체인에 포함될 수 있습니다. 예를 들어, 예제에 있는 블록 X_{101}는 커밋-인증을 받지 않았지만, 블록 X_{102}이 합의된 후, 블록 X_{101} 또한 합의된 것으로 여겨집니다. 이는 계산 파워의 낭비를 줄이고, 트랜잭션 처리량을 증가시키는데 도움을 줍니다.

분석

안전성(Safety): 안전성(safety)은 모든 정직한 검증자들이 같은 블록들의 체인에 대해 동의하는 것을 의미합니다. 더 정확하게는, 하나의 정직한 검증자가 블록 A를 받아들인다면, 다른 정직한 검증자들이 받아들인 이후의 블록들이 A 블록을 포함하고 있는 것을 의미합니다. 이러한 안정성에 대한 논의는 Casper FFG 그리고 Hot-Stuff와 유사하고 여기서는 생략되었습니다. 우리는 단지 정직한 노드가 합의된(settled) 블록과 충돌되는 블록에 절대 투표하지 않는다는 요구사항에서 비롯된 안정성에 대해 지적하고자 합니다.
생기성(Liveness): 생기성(liveness)는 검증자 위원회가 항상 진행되는 것을 의미합니다. 즉, 항상 새로운 블록들을 생성하고 동의할 수 있음을 의미합니다. 여기서 우리는 타이밍 모델 하에서 동기화 기간(synchronous period) 동안, 위원회가 언제나 생기성 목표(liveness goal)를 달성할 수 있다는 것을 보여줍니다. 첫번째로, "블록 제안" 섹션에서, epoch이 계속해서 증가하고, 모든 정직한 검증자들은 함께 다음 epoch으로 진행됨을 입증하였습니다. 제안자(proposer)가 정직한 검증자인 epoch에서, 제안자는 새로운 블록을 제안합니다. 블록 합의 과정에서, 생기성은 동기화 기간 동안, 연속해서 두개의 제안자들이 정직하고, 커밋(commit)-인증서(certificate)를 생성하기에 충분히 오래 기다리는 무수히 많은 epoch이 있다는 것에 달려있습니다. 우리는 이것이 적어도 2/3 이상의 검증자들이 정직하기 때문에, 라운드 로빈 회전과 함께 무수히 자주 발생하는 것을 보증합니다.

트랜잭션 처리량(Transaction throughput): 10에서 20개의 검증자들과 함께, 위원회는 보다 빠르게 블록들의 체인을 생성하고 합의할 수 잇습니다. 평균 블록 생성 및 합의 시간은 초 단위이고, 이것은 초당 1000+ 이상의 높은 처리량을 이끌어낼 수 있습니다.

블록 완결 (Finalization) 프로세스

이 섹션에선, "립프로깅 (leapfrogging)" 블록 완결 과정에 대해 자세히 논의할 것입니다. 위에서 말했던 것처럼, 가디언들은 체크포인트 블록의 해시에 대해서만 합의에 도달할 필요가 있습니다. 여기서 체크포인트 블록은 몇몇 정수 T(예: T=100)의 배수의 높이를 가지는 블록을 말합니다.

체크포인트 블록 만을 완결(finalize)짓는 것이 왜 충분한지 보여주기 위해서, 블록체인 소프트웨어의 트랜잭션 실행 엔진이 "결정론적 상태 기계 (deterministic state machine)" 로서 보일 수 있다는 것을 명심하여야 합니다. 트랜잭션은 결정론적 상태 전송 함수 (deterministic state transfer function)로 볼 수 있습니다. 만약 두 노드가 같은 상태 기계를 실행하고 동일한 초기 상태에서 시작한다면, 같은 트랜잭션 시퀀스(sequence)를 실행하고 나서, 그들은 결국 동일한 상태에 도달하게 됩니다. 이것은 몇몇 트랜잭션들이 유효하지 않을 때에도 상태 기계가 이러한 유효하지 않은 트랜잭션들을 감지하고 건너 띄는 한 결국에는 동일한 상태에 도달합니다. 예를 들어, 소스 계정이 갖고 있는 토큰 양보다 더 많은 토큰을 소비하는 트랜잭션이 있을 수 있습니다. 상태 기계는 세너티 체크(sanity check) 이 후에 간단히 이 트랜잭션을 건너 뛸 수 잇습니다. 이런 식으로 "나쁜(bad)" 트랜잭션들은 상태에 아무런 영향을 끼치지 못합니다.

블록체인의 문맥에서, 모든 정직한 노드들이 같은 블록체인 사본을 가진다면, 순서대로 모든 블록을 처리한 후 결국 같은 상태에 도달하게 된다는 것을 보장할 수 있습니다. 하지만 하나의 주의 할 점이 있습니다. — 블록체인은 막대한 양의 데이터를 포함할 수 있습니다. 어떻게 두 정직한 노드는 그들이 가진 체인이 동일한 것인지 효율적으로 비교할 수 있을까요?

여기에 블록체인의 데이터 구조의 불변성 특징이 이 문제를 구출할 수 있습니다. 각각의 블록의 헤더가 이전 블록의 해시 값을 포함하고 있기 때문에, 두개의 노드가 가진 각각의 체크포인트 블록의 해시 값이 같은 한, 압도적인 확률로 그들은 제네시스 블록부터 체크포인트 블록까지 동일한 블록들의 체인을 가지게 됩니다. 당연히, 각각의 가디언 노드들은 블록체인의 무결성을 확인해야 할 필요가 있습니다. 특히, 각각의 블록 헤더에 있는 블록 해시 값은 사실 이전 블록의 해시입니다. 노드는 자체적으로 다른 노드의 필요 없이 무결성 검사(integrity check)를 수행할 수 있습니다.

흥미롭게도, 불변성 특징은 네트워크 비동기 또는 분할에 대한 저항(tolerance)을 향상시킵니다. 네트워크 분할에서, 가디언들은 체크포인트의 해시 값에 대해 합의에 도달하지 못할 수도 있습니다. 그러나, 네트워크가 회복되고 나서, 다음 체크포인트에 대해 투표를 진행할 수 있습니다. 만약 그들이 합의에 도달한다면, 다음 체크포인트까지의 모든 블록이 현재 체크포인트에 대한 합의 여부와 관계없이 완결(finalized)됩니다.

비잔티움 장애 허용(byzantine fault tolerance)을 증명하기 위해서, 정직한 노드는 적어도 2/3의 가디언들이 같은 체크포인트 블록 해시를 갖고 있다는 것을 보장받아야 할 필요가 있습니다. 따라서 노드가 체크포인트에 대해 완결을 표시하기 전에, 이 체크포인트 해시에 대해서 모든 가디언 중 적어도 2/3에게서 서명을 받아야 할 필요가 있습니다. 이는 안정성(safety)를 보장하기 위한 것이며, 유명한 프로토콜인 PBFT 프로토콜의 "커밋(commit)" 단계와 유사합니다.

가디언들은 오직 T 블록마다 있는 체크포인트 해시 값에 대해서만 투표할 필요가 있으므로, 합의에 도달하기까지 더 많은 시간이 존재합니다. 체크포인트 완결의 간단한 구현은 PBFT "커밋" 단계를 따르므로 각 가디언은 다른 모든 보호자에게 서명을 브로드캐스트 합니다. 이것은 각 노드가 $O(n)$ 메시지들을 전송하고, 수신하고 처리하는 것을 요구하고, 각

메시지는 수 킬로바이트의 길이를 가질 수 있습니다 노드들이 합의에 이르기까지 T 블록 시간을 가지더라도, 이러한 접근법은 T 값을 크게 설정하지 않는 한 여전히 수백개의 가디언 노드들을 수용하도록 확장할 수 없습니다. T 값을 크게 설정하는 것은 블록 완결 지연을 증가시키므로 바람직하지 않습니다.

수천개의 가디언으로의 확장

통신 복잡도를 줄이고 수천개의 가디언으로 확장하기 위해서, 우리는 gossip 프로토콜과 BLS signature aggregation technique[6] 에서 영감을 받은 aggregated signature gossip 스킴을 디자인하였습니다. 이 스킴은 각각의 가디언 노드들이 합의에 도달하기 위해 실용적으로 더 작은 수의 메시지들을 처리하도록 요구합니다. 아래는 aggregated signature gossip 프로토콜의 단계를 보여줍니다. 이 프로토콜은 BLS 알고리즘을 서명 통합(aggregated signature)를 위하여 사용합니다.

Algorithm 2: Aggregated Signature Gossip

$finalized \leftarrow$ false, $\sigma_i \leftarrow$ **SignBLS**$(sk_i, height_{cp} \| hash_{cp})$, $c_i \leftarrow$ **InitSignerVector**(i)

for $t = 1$ to L **begin**

  send (σ_i, c_i) to all its neighboring guardians

  if *finalized* **break**

  wait for (σ_j, c_j) from all neighbors until timeout

  verify each (σ_j, c_j), discard if it is invalid

  aggregate valid signatures $\sigma_i \leftarrow \sigma_i \cdot \prod_j \sigma_j$, $c_i \leftarrow \left(c_i + \sum_j c_j\right) mod\ p$

  calculate the number of unique signers $s \leftarrow \sum^{n} I(c_i[k] > 0)$

  if $s \geq \frac{2}{3} n$ $finalized \leftarrow$ true

end

Algorithm 2. *The aggregated signature gossip 프로토콜*

핵심 아이디어는 간단합니다. 각각의 가디언 노드들은 주변 노드들로부터 통합된 서명(aggregated signature)들을 부분적으로 결합한 다음, 새롭게 통합된 서명을 gossip프로토콜에 내보냅니다. 이렇게 하면 가십 프로토콜 덕분에 각 노드의 서명 공유가 기하 급수적으로 빠르게 다른 노드에 도달할 수 있습니다. 한편으론, 서명 통합 (signature aggregation)는 노드 간 메시지들을 작은 사이즈로 유지하여 통신 오버헤드를 추가적으로 줄입니다.

위의 다이어그램에서, i는 현재 가디언 노드의 인덱스입니다. 프로토콜의 첫번째 줄에서 함수 **SignBLS**() 를 초기 통합된 서명 σ_i 을 생성하기 위해 사용합니다. 기본적으로 BLS 서명 알고리즘을 사용하여 체크포인트 블록의 해시와 높이를 결합한 메시지에 서명합니다. 곱셈 순환 그룹(multiplicative cyclic group) G, 초기 순서(prime order) p, 생성자(generator) g:

$$h_i \leftarrow H\left(pk_i,\ height_{cp} \| hash_{cp}\right)$$

[6] *Boneh et al.* A Survey of Two Signature Aggregation Techniques

$$\sigma_i \leftarrow (h_i)^{sk_i}$$

위의 첫번째 공식에서, 함수 $H : G \times \{0, 1\}^* \rightarrow G$ 는 퍼블릭 키 pk_i 와 메시지를 입력 값으로 하는 해시 함수입니다. 이것은 불법 공개키 공격(rogue public-key attack)을 막기 위한 것입니다[7].

이 프로토콜은 또한 서명자 벡터(signer vector) c_i 를 초기화 하기 위한 **InitSignerVector()** 함수를 사용합니다. 이 서명자 벡터(signer vector)는 j번째 가디언이 통합된 서명에 얼마나 많이 서명했는지를 나타내는 j번째 입력(entry)의 n 차원 정수 벡터입니다. 초기화 이후에, j 번째 입력(entry)은 1 로 설정되고, 남은 입력들은 모두 0으로 설정됩니다.

초기화 이후에, 가디언은 반복문 (loop)으로 진입합니다. 각각의 반복에서, 가디언은 먼저 현재 통합된 서명 과 서명자 벡터 c_i 를 모든 이웃 노드에게 보냅니다. 그런 다음 체크포인트가 완결된 것으로 간주되지 않으면, 이웃 노드로부터의 서명 및 서명자 벡터를 기다리거나 타임아웃까지 대기합니다. 모든 서명 및 서명자 벡터를 수신하고 나면, BLS 통합 서명 증명 (BLS aggregated signature verification) 알고리즘을 사용하여 (σ_j , c_j)의 유효성을 검사합니다.

$$h_u \leftarrow H(pk_u,\ height_{cp} \parallel hash_{cp})$$

$$\text{check if } e\left(\sigma_j,\ g\right) = \prod_u^n (e\,(h_u,\ pk_u))^{c_j[u]}$$

여기서 $e : G \times G \rightarrow G_T$ 는 $G \times G$ 에서 G_T까지의 쌍일차(bilinear) 매핑 함수이며, 또한 소수 p의 또다른 multiplicative cyclic 그룹입니다. 모든 유효하지 않은 서명 및 그와 연관된 서명자 벡터는 다음 통합 단계(aggregation step)에서 버려집니다. $height_{cp}$, $hash_{cp}$ 외에도 위의 검사는 관련 가디언의 퍼블릭 키 pk_u를 입력으로 요구한다는 점을 지적할 가치가 있습니다. 가디언이 지분을 락업 한 경우, 블록체인에 이미 기록된, 지분을 락하기 위한 트랜잭션에 해당 퍼블릭 키가 이미 첨부되어 있으므로 이러한 모든 정보는 로컬에서 사용가능해야 합니다. 따라서, 이러한 입력 값을 구하기 위한 다른 노드들과의 어떠한 통신도 필요하지 않습니다.

통합 과정(aggregation step)은 BLS 서명 σ_j 를 통합하고, 서명자 벡터 σ_j 를 업데이트합니다. 벡터 업데이트의 경우, 우리는 각 입력에 대해 $mod\ p$ 연산을 수행합니다. 우리는 $e(h_u,\ pk_u) \in G_T$ 가 소수 p의 multiplicative cyclic그룹이기 때문에 이 작업을 수행할 수 있습니다. 이것은 벡터 c_j 의 입력이 항상 제한된 수의 비트로 표현될 수 있음을 보장합니다.

$$\sigma_i \leftarrow \sigma_i \cdot \prod_j \sigma_j\ ,\ c_i \leftarrow \left(c_i + \sum_j c_j \right) mod\ p$$

그런 다음 알고리즘은 통합된 서명의 고유(unique)한 서명자들의 수를 계산합니다.

$$s \leftarrow \sum^n I\,(c_i\,[k] > 0)$$

여기서 함수 I: $\{\text{true, false}\} \rightarrow \{1, 0\}$ 은 참(true) 조건을 1로, 그리고 거짓(false0 은 0으로 매핑 시킵니다. 따라서 합계는 통합된 서명에 얼마나 많은 고유 서명자가 기여했는지를

[7] *Boneh et al.* BLS Multi-Signatures With Public-Key Aggregation

계산합니다. 모든 가디언들 중 2/3이상이 이 서명에 서명을 한 경우, 가디언은 이 체크포인트가 완결된 것이라고 간주합니다.

체크포인트가 완결된다면, 통합된 서명은 다음 반복문에 gossip 프로토콜로 내보내 집니다 (gossiped out). 따라서 $O(log(n))$ 반복 안에 모든 정직한 가디언들은 네트워크가 분할하지 않는다면, 전체 가디언의 2/3이상으로부터 서명된 통합된 서명을 갖게 됩니다.

이 반복문은 L 개의 반복을 가지고 있고, 서명이 네트워크를 통해 전파되도록 L 은 대략 $O(log(n))$이어야 합니다.

분석

안정성(Safety): 블록 완결의 안정성은 입증하기 쉽습니다. 2/3의 압도적인 수의 노드가 정직하다는 가정하에, 같은 높이의 두개의 체크포인트 둘다 모든 가디언의 2/3이상의 통합된 서명을 받으려면, 적어도 하나의 정직한 가디언이 같은 높이의 서로 다른 해시 값 두개 모두에 대해 서명하여야 합니다. 이는 불가능합니다.

생기성(Liveness): 네트워크 분할이 없고, L 이 충분히 큰 한, O(log(n)) 반복 이후 높은 확률로 모든 정직한 노드들은 모든 정직한 서명자들의 서명들이 합쳐진 통합된 서명을 볼 것입니다. 이것은 gossip 프로토콜이 최대 1/3의 비잔티움 노드들이 있는 경우에도 O(log(n)) 시간안에 네트워크를 통해 어떻게 메세지를 전달할 수 있는 지와 비슷합니다. 네트워크 분할이 있을 때, 체크포인트에 대해 합의를 도달하지 못할 수도 있습니다. 그러나, 네트워크가 분할이 끝나고 난 후, 가디언 풀은 다음 체크포인트 블록을 완결 짓는 것을 계속 할 수 있습니다. 그러고나서 합의에 도달한다면, 다음 체크포인트까지의 모든 블록들이 완결된 것으로 간주됩니다. 따라서 완결 과정은 계속해서 진행됩니다.

메시지 복잡도(Messaging Complexity): aggregated signature gossip 프로토콜은 대략 O(log(n)) 인 L번의 반복동안 실행됩니다. 각 반복 동안, 가디언은 메시지 - message(σ _i, c_i)를 모든 이웃 가디언들에게 전송해야 할 필요가 있습니다. 네트워크 토폴로지에 따라, 일반적으로 평균 노드에 대해, 이웃 노드들의 수는 일정하고 가정하는 것이 합리적입니다(즉, 노드의 총 수가 증가한다고 해도 어떤 노드의 이웃 노드의 수가 증가하지 않는다). 따라서 체크포인트를 완결(finalize)하기 위해 보내고 받는 메시지의 수는 대략 O(log(n))이며, O(n)의 복잡도를 가지는 순수한 전체 대 전체 (all-to-all) 서명 브로드캐스팅 구현보다 훨씬 낫습니다. 우리는 두 이웃 가디언들 간의 각각의 메시지들이 n 차원 서명 벡터 c_i 를 포함하고 있음을 압니다. 여기서 c_i는 소수 p 보다 작은 정수입니다. 그러나, 우리는 입력(entry)의 대부분이 실제로는 작은 정수이기 때문에 (p 보다 작은) 이 벡터가 다소 작게 표현될 수 있음을 주의해야 합니다.

메시지 복잡도에 대한 구체적인 아이디어를 얻기 위해서, 예시를 들어보도록 하겠습니다. 우리가 BLS 서명을 위해서 170 비트의 긴 소수 p 를 선택한다고 가정하면, 이는 1024 비트 RSA 서명과 비교할 만한 보안을 제공할 수 있습니다. 그리고 여기 총 1000개의 가디언 노드들이 있다고 가정하겠습니다. 이러한 설정 하에, c_i는 어떠한 압축도 없이 20 킬로바이트로 나타낼 수 있습니다. c_i의 대부분의 입력(entry)이 p 보다 상당히 작기 때문에, c_i는 2 킬로바이트로 상당히 압축될 수 있습니다. 또한 통합된 서명과 함께, 각 메시지의 크기는 일반적으로 수 킬로바이트의 범위를 가집니다. 게다가, 평균적으로 하나의 가디언이 20개의 다른 가디언들과 연결되어 있다고 가정하면, L 은 5보다 작아질 수 있습니다 (log20(1000) = 2.3의 두 배 이상). 즉 하나의 체크포인트를 완결 짓는 것은 하나의 가디언이 각 2킬로바이트의 길이를 가진 약 100개의 메시지를 이웃 가디언들에게 전송하거나 이웃 가디언들로부터 받는 것을 의미한다. 이는 통합 서명 가십 프로토콜(aggregated signature

gossip protocol)을 구현하는데 다소 실용적이며 수천 개의 가디언 노드로 쉽게 확장할 수 있습니다.

검증자와 가디언들의 보상과 페널티

토큰 보상 및 패널티 구조는 노드가 합의 프로세스에 참여하고 프로토콜에서 벗어나지 않도록 하는 데 필수적입니다. 검증자와 가디언 둘 다 토큰 보상을 얻을 수 있습니다. 각 블록은 새롭게 채굴되는 토큰을 검증자와 가디언의 주소로 이체하는 특별한 코인베이스(Coinbase) 트랜잭션을 포함하고 있습니다. 모든 검증자들은 각 블록마다 토큰 수익을 얻을 수 있습니다. 가디언의 경우에는, 각 블록마다 모든 가디언에게 보상을 주는 것은 가디언의 수가 너무 많기 때문에 실용적이지 않을 수 있습니다. 대신, 우리는 제한된 수의 가디언을 각 블록의 보상 수령인으로 무작위로 선택하는 다음 알고리즘을 제안합니다.

새로 제안된 블록의 높이를 l 로 표시하고 cp는 가장 최근에 완결된 체크포인트입니다. 제안자는 통합된 서명 σ_{cp} 과 체크포인트 cp에 대응되는 서명자 벡터 σ_{cp} 를 받아야 합니다. $(\sigma_{cp},\ c_{cp})$ 이 유효한지 확인하면서, 제안자는 벡터 c_{cp} 의 입력이 0이 아닌 각 가디언들에 대해 다음 조건들을 확인할 수 있습니다. (즉, 보호자가 체크포인트에 서명한 경우)

$$H(pk_i,\ \sigma_{cp} \parallel B_{l-1}) \leq \tau$$

여기서 B_{l-1} 은 높이가 $l-1$ 인 블록의 해시이고, $H : G \times \{0,\ 1\}^* \rightarrow G$ 는 BLS 서명 알고리즘에 사용된 것과 동일한 해시 함수입니다. 부등식이 성립하면, 제안자는 코인베이스 (Coinbase) 트랜잭션 수신자 목록에 가디언의 퍼블릭 키 pk_i를 추가합니다. Threshold τ 는 소수의 가디언만 포함되도록 적절하게 선택됩니다. 제안자는 보상에 대한 증명으로 코인베이스 트랜잭션에 $(\sigma_{cp},\ c_{cp})$ 를 첨부해야 합니다.

Theta ledger는 어떠한 악의적인 행동이 탐지되면 토큰 페널티를 적용합니다. 특히, 블록 제안자가 같은 높이의 충돌되는 블록들에 서명하거나, 검증자가 같은 높이의 서로 다른 블록에 대해서 투표하는 경우, 그들은 페널티를 받습니다. 이전에 언급한 것처럼 검증자 혹은 가디언은, 특정 기간 동안 특정한 양의 토큰을 락업 (look up) 할 필요가 있습니다. 페널티는 그들이 락업한 토큰에서 삭감됩니다. 악의적인 행동을 감지한 노드는 특별한 삭감 트랜잭션 (Slash transaction)을 블록체인에 제출할 수 있습니다. 악의적인 행동에 대한 증명 (예: 충돌되는 블록들에 대한 서명)은 삭감 트랜잭션에 첨부될 수 있습니다. 페널티 토큰은 악의적인 노드로부터 가져와 가장 먼저 삭감 트랜잭션을 제출한 노드에게 보상이 주어질 수 있습니다.

드물게 검증자의 3 분의 1 이상이 손상된 경우, 악의적인 검증자는 합의(settled)되었지만 아직 완결(finalized)되지 않은 블록에서 블록체인을 포킹(forking)하여 이중 지불 공격을 시도하는 것이 가능합니다. 그러나, 이는 가디언 풀에 의해 감지될 수 있습니다. 왜냐면 포킹(forking)은 같은 높이에서 여러 블록들을 만들어 내고, 검증자의 2분의 3이상이 서명해야 하기 때문입니다. 이 경우, 이중 서명을 수행한 검증자들은 페널티를 받게 되며, 전체 검증자 위원회가 재 선출됩니다. 검증자 위원회가 새로 구성된 후, 블록체인은 가장 최근의 완결된 체크포인트에서부터 계속 진행될 수 있습니다.

튜링-완전 스마트 컨트렉트 지원

이 Theta Ledger는 이더리움 가상 머신[8]과 완전히 호환되는 스마트 컨트렉트 실행 환경을 제공합니다. 이는 튜링-완전 스마트 계약을 위한 본격적인 지원을 제공합니다. 솔리디티 기반의 이더리움 스마트 계약은 Theta Ledger에 쉽게 포팅할 수 있습니다. 솔리디티[9]는 대규모 개발자 커뮤니티를 성장시켰고 이더리움 가상 머신의 호환성을 허용하여 재능 있는 개발자 풀이 바퀴부터 재개발할 필요 없이 Theta에 기여할 수 있도록 합니다.

스마트 계약은 Theta Ledger 위에 만들어진 비디오 플랫폼 DAPP을 위한 훌륭한 사용자 경험과 새로운 권한 모델을 허용합니다. 예를 들어, 비디오 플랫폼들은 사용자들을 사로잡기 위한 로열티 프로그램 스마트 계약을 작성할 수 있습니다. 사용자들의 활동 혹은 그들이 전송한 비디오 세그먼트/데이터 양에 기반하여, 플랫폼 DAPP은 사용자를 상위 계층으로 승격시켜 특정 권한 또는 단독 기능을 잠금 해제할 수 있습니다. 또 다른 예시로, 비디오 플랫폼들은 사용자들이 좋아하는 컨텐츠 제작자들을 위한 가상 아이템을 발행할 수 있습니다. 이러한 개념을 확장시키기 위해, "대체 불가능한 토큰" 기준으로 만들어진 가상 아이템은 희귀하고 유니크하며, 본질적으로 "암호 수집품"이 됩니다. 이는 제3자의 추가적인 승인을 필요로 하지 않고, 기념품으로 유지하거나 다른 수집품으로 교환할 수 있습니다.

또한, 비디오 플랫폼들은 사용량에 따라 지불하는 모델과 같은 더 유동적인 결제-소비 모델을 허용하는 스마트 계약을 작성할 수 있습니다. 전통적인 연간 혹은 월간 구독 대신, 사용자 소비량은 바이트-사이즈의 정밀도로서 가격을 매길 수 있습니다. 따라서 사용자들은 오직 그들이 사용한 만큼만 지불하면 됩니다. 이는 저가의 짧은 형식의 콘텐츠를 경제적이고 합리적으로 거래할 수 있는 실현가능한 방법으로 플랫폼과 사용자 모두에게 이득이 되는 방법입니다. Theta Ledger의 소액결제와 비디오 세그먼트의 추적 특성을 통해 이러한 스마트 계약이 실행될 수도 있습니다.

스마트 계약은 공정하고 투명하게 이익을 분배하기 위한 방법으로서 컨텐츠 제작자에게 이익을 주도록 설계될 수 있습니다. 전통적인 로열티 결제 프로세스는,
복잡성과 불명료함을 가지고 있는 전통적인 로열티 결제 프로세스 대신 제작자와 배포자가 상호 동의한 명확한 스마트 계약 조건을 수용할 수 있습니다.

Theta Ledger에서 스마트 계약을 이용하여 완전히 디지털화된 아이템 소유권, 혁신적인 결제-소비 모델, 그리고 투명한 로열티 분배를 사용할 수 있고, 이는 비디오/컨텐츠 전달의 핵심 기능을 보완하는 사회적 및 경제적 상호 작용 계층을 추가로 제공합니다.

---

8 https://github.com/ethereum/wiki/wiki/Ethereum-Virtual-Machine-(EVM)-Awesome-List

9 https://solidity.readthedocs.io/

Off-Chain Micropayment 지원

소개 섹션에서 설명한 것처럼, 비디오 스트리밍에 중점을 둔 블록체인은 높은 처리량을 지원해야 합니다. 우리는 많은 수의 트랜잭션 처리를 용이하게 하기 위해서 원장(ledger)에 직접 오프체인(off-chain) 결제를 지원합니다.

리소스 중심의 소액결제 풀(Resource Oriented Micropayment Pool)

우리는 "리소스 중심의 소액 결제 풀(Resource Oriented Micropayment Pool)"이라는 비디오 스트리밍 전용의 off-chain을 설계하고 구현하였습니다. 이 방법은 유저가 off-chain상에서 소액 결제 풀을 생성하도록 허용합니다. 이 소액 결제 풀로 다른 어떠한 유저든 off-chain의 트랜잭션을 이용해 돈을 인출할 수 있고, 이중 지불 문제를 방지합니다. 이러한 저희의 독자적인 솔루션은 기존 off-chain 결제 채널과 비교하여 더 유동성을 가집니다. 특히, 비디오 스트리밍의 사용 사례에서, 이 방법은 시청자가 여러 캐시 노드로부터 받아오는 비디오 컨텐츠에 대해 지불할 때 on-chain트랜잭션 없이도 지불이 가능하게 합니다. On-chain의 트랜잭션을 off-chain의 결제로 대체함으로써 "리소스 중심의 소액 결제 풀(Resource Oriented Micropayment Pool)"은 블록체인의 확장성을 상당히 개선할 수 있습니다.

다음의 시나리오와 다이어그램은 리소스 중심의 소액 결제 풀("Resource Oriented Micropayment Poo")이 어플리케이션에서 어떻게 작동하는지에 대한 종합적인 워크스루(walkthrough)를 보여줍니다

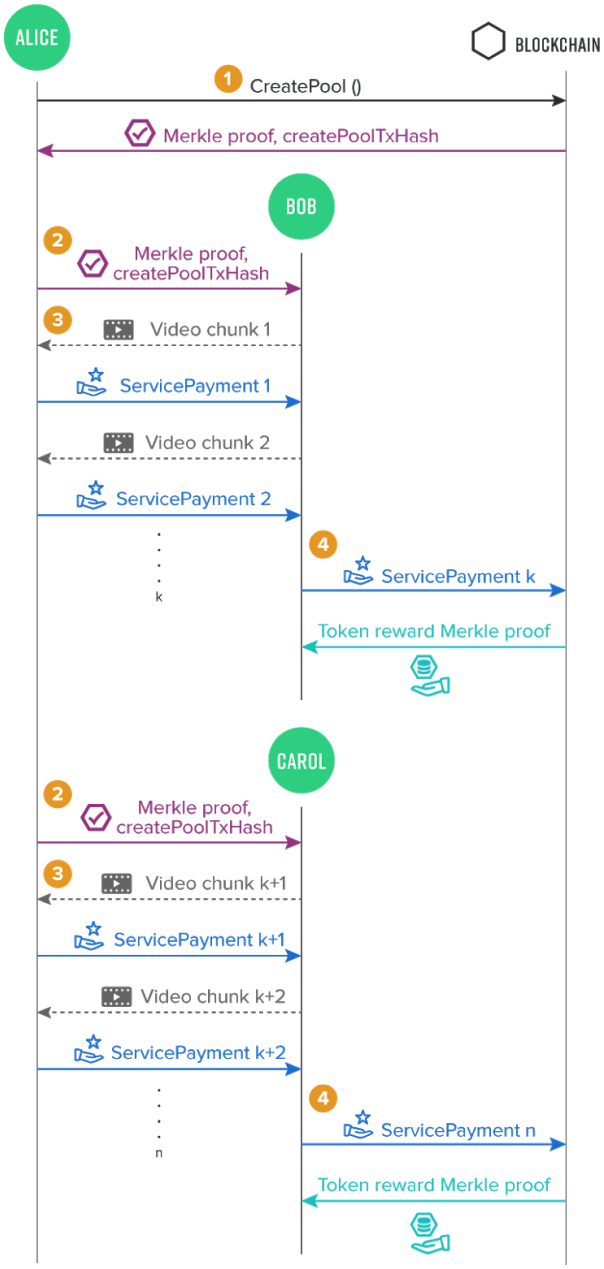

***Figure 7**. 이 그림은 시청자인 Alice가 비디오 청크(chunks)를 받아 오기 위해서 캐시 노드인 Bob과 Caro에게 off-chain 트랜잭션을 생성하는 것을 보여줍니다.*

- **Step 1. 소액결제 풀(Micropayment pool) 생성**: 첫번째 단계로서, Alice는 시간 제한 및 삭감 가능한 담보금이 있는 소액 결제 풀(Micropayment pool)을 생성하기 위해서 온-체인(on-chain) 트랜잭션을 게시(publish)합니다.

$$CreatePool(resourceId, deposit, collateral, duration)$$

여기에 주목해야 할 몇 가지가 있습니다. Pool을 생성하기 위해서, Alice는 "resource ID"를 구체적으로 명시해야 합니다. *resourceId*는 그녀가 찾고자 하는 디지털 컨텐츠를 고유하게 나타내는 ID입니다. 이 ID는 비디오 파일과 관련이 있을 수도 있고, 또는 라이브 스트림과 관련이 있을 수 있습니다.

"예금액(*deposit*)"은 적어도 찾고자 하는 리소스(resource)의 전체 가치보다 같거나 많아야 합니다. 예를 들어, 찾고자 하는 비디오 파일의 리소스가 10 토큰의 가치를 지닐 때, 입금액은 적어도 10 토큰이어야 합니다.

"담보금(*collateral*)"은 Alice의 이중지불(double spending)을 방지하기 위해서 필요합니다. 만약 Alice가 이중 지불을 시도하는 것이 블록체인의 검증자(validators)에 의해서 감지되면, 주어진 담보금이 깎이게 됩니다. 나중에 살펴볼 블로그 포스트에서 알 수 있지만 만약 담보금 > 예금액 일 때, 이중 지불에 대한 수익은 항상 마이너스일 것이므로 이성적인 사용자라면 이중 지불에 아무런 이득이 없다는 것을 알 수 있을 것입니다.

"*duration*" 은 시간 제한으로서 표준 결제 채널과 유사합니다. 시간 제한이 만료되기 전에 요청된 출금만이 유효합니다.

블록체인은 Alice의 *CreatePool*() 트랜잭션 요청이 블록체인에 커밋된 이후에 Alice에게 *CreatePool*() 트랜잭션에 대한 Merkle proof 값과 CreatePool() 트랜잭션의 트랜잭션 해시 값인 *createPoolTxHash*을 반환합니다.

Alice가 피어 (Bob, Carol, David 등)에게서 지정된 리소스를 찾기를 원할 때마다, 그녀는 온 체인 의 *CreatePool*() 트랜잭션의 Merkle proof 값을 피어에게 보냅니다. 수신자 피어는 Merkle proof 값을 확인하여 pool이 요청한 리소스에 대해서 충분한 예금액과 담보액을 갖고 있는지 확인하고, 확인이 되면 수신자 피어와 Alice는 다음 단계로 진행할 수 있습니다.

- **Step 2. 피어 들간 초기 핸드셰이크(handshake)**: Alice가 피어 (Bob, Carol, David 등)에게서 지정된 리소스를 찾기를 원할 때마다, 그녀는 온 체인의 *CreatePool*() 트랜잭션의 Merkle proof 값을 피어에게 보냅니다. 수신자 피어는 Merkle proof 값을 확인하여 pool이 요청한 리소스에 대해서 충분한 예금액과 담보액을 갖고 있는지 확인하고, 확인이 되면 수신자 피어와 Alice는 다음 단계로 진행할 수 있습니다.

- **Step 3. 오프체인 소액결제 (Off-chain micropayments)**: Alice는 지정된 리소스의 일부분(예, 비디오 파일의 일부분 또는 라이브 스트림 세그먼트)을 위해서 *ServicePayment* 트랜잭션들에 서명하고 이것들을 off-chain상에서 피어에게 보냅니다. *ServicePayment* 트랜잭션은 다음과 같은 데이터들을 포함합니다:

$$\begin{gathered} targetAddress,\ transferAmount,\ createPoolTxHash,\ targetSettlementSequence, \\ \mathbf{Sign}(SK_A,\ targetAddress \parallel transferAmount \parallel createPoolTxHash \parallel \\ targetSettlementSequence) \end{gathered}$$

"*targetAddress*"는 Alice가 자원을 찾고자 하는 피어의 주소이고, "*transferAmount*"는 Alice가 보내려고 하는 토큰의 수량입니다. "*targetSettlementSequence*"는 replay attack을 방지합니다. 이 값은 이더리움 트랜잭션의 "nonce" 값과 유사합니다. 만약 타겟이 ServicePayment 트랜잭션을 블록체인으로 게시한다면 (다음 단계에서 보게 될), *targetSettlementSequence* 는 1씩 증가해야 합니다.

수신자 피어는 이러한 오프 체인 트랜잭션들과 서명들을 확인해야 합니다. 유효성 검사가 끝나면, 피어는 *CreatePool*() 트랜잭션에서 지정된 리소스를 Alice에게 보낼 수 있습니다.

또한, 우리는 off-chain *ServicePayment*트랜잭션들이 두개의 피어 사이에서 직접적으로 전송되는 것을 알아야합니다. 따라서 이 단계에서는 확장성 병목 현상이 없습니다.

- **Step 4. 온-체인 합의 (On-chain settlement)**: Alice에게서 $ServicePayment$ 트랜잭션을 받은 어떠한 피어든 토큰을 인출하기 위해 블록체인으로 서명된 트랜잭션을 게시(publish)할 수 있습니다. 다만 시간이 만료되기 전이여야 합니다. 우리는 이렇게 게시(published)된 $ServicePayment$ 트랜잭션들에 대해서 "온 체인 합의(on-chain settlement)" 트랜잭션이라고 부릅니다. 수신자 피어는 "온 체인 합의(on-chain settlement)" 트랜잭션을 위해 가스비를 지불해야 한다는 것을 명심해야 합니다. 적은 트랜잭션 수수료를 지불하기 위해서, 피어들은 정말로 필요할 때만 온 체인 합의를 수행할 것이고, 이는 네트워크의 확장성에 도움이 됩니다.

Alice가 리소스를 찾기 위해 기존 피어에서 다른 피어로 변경할 때 어떠한 온 체인 트랜잭션도 필요하지 않다는 것을 알아야 합니다. 비디오 스트리밍에서, 시청자는 잠재적으로 비디오 스트림 전달을 지연시키거나 방해할 수 있는 온 체인의 트랜잭션 생성 없이, 언제든지 다른 캐시 노드로 리소스를 받아오도록 전환할 수 있습니다. 그림에 나와있듯이, Alice는 Bob에게서 k개의 청크(chuck)를 받아온 후에 Carol로 전환이 가능합니다. 전환 후에, 온 체인의 트랜잭션없이 계속해서 비디오 세그먼트를 받아옵니다.

또한, 소액 결제 풀을 생성하기 위해 총 토큰 양은 (담보금 + 예금)이며, Alice가 리소스를 얻기 위한 피어의 수와 상관없이 요청하려는 리소스 가치의 2배까지 낮아질 수 있습니다. 계산 복잡도 표현을 사용한다면, 단방향 결제 채널방식과 비교할 때 예약되는 토큰의 양은 $O(n)$에서 $O(n)$ 으로 감소합니다. 여기서 n 은 Alice가 자원을 검색하는 피어의 수입니다.

이중 지불 감지 및 페널티 분석

이중 지불을 소액 결제 풀에서 생성하는 Alice를 방지하려면, 우리는 1) 이중 지불을 감지할 수 있어야 하고, 2) 이중 지출로 인해 얻는 순 이익이 항상 마이너스라는 것을 보장해야 합니다.

이중 지불을 감지하는 것은 상대적으로 직관적입니다. THETA 네트워크의 검증자(validators)들은 모든 온 체인 트랜잭션을 확인합니다. 소액 결제 풀에 남아있는 예금액이 Alice와 다른 피어에 의해서 서명된 다음 통합 결제 트랜잭션을 처리할 수 없는 경우, 검증 노드는 Alice가 이중 지불을 시도했다고 판단합니다.

다음으로, 우리는 Alice 이중 지불을 시도한다면 그녀를 불행하게 만들어야 합니다. 이것은 담보금을 받아야 하는 이유입니다. 이전에, 우리는 담보액이 예금액보다 커야 한다고 언급한적이 있습니다. 여기에 그 이유가 있습니다.

아래 Figure 5 에서, Bob, Carol, 그리고 David는 정직합니다. Alice는 악의적인 공격자입니다. 더 나쁜 것은, 그녀는 다른 악의적인 행위자인 Edward와 결탁합니다. Alice는 지정된 리소스를 위해 Bob, Carol 그리고 David와 부분적으로 서명된 트랜잭션들을 교환합니다. Alice는 중복된 리소스에 대해서는 추가적인 가치를 얻을 수 없으므로, 그녀가 Bob, Carol 그리고 David에게서 얻는 최대 가치는 예금 액이 최대입니다. Alice는 Edward와 결탁함으로써 그녀는 Edward에게 총 예금액을 보낼 수 있습니다. 그런 다음 그녀는 다른 사람들이 커밋하기 전에 Edward에게 정산 트랜잭션(settlement transaction)을 블록체인에 커밋하도록 요청하고, 그 다음 다시 그녀에게 예금액을 반환하도록 합니다. 즉, Alice는 이중 지불이 감지되기 전에 최대 예금액만큼의 가치를 지닌 리소스를 무료로 얻습니다. 나중에 Bob, Carol 그리고 David가 정산 트랜잭션을 커밋할 때, 이중 지불은 감지됩니다. 그리고 모든 담보금액은 삭감됩니다. 따라서 Alice의 순 수익은 다음과 같습니다

$$\text{순수익}_{Alice} = \text{예금액}(deposit) - \text{담보금}(collateral)$$

그러므로, 이 시나리오에서 우리는 다음과 같은 결론을 낼 수 있습니다. 담보금이 예금액보다 큰 상황에서는, Alice의 순이익은 항상 마이너스입니다. 따라서 만약 Alice가 합리적이라면, 그녀는 이중 지불을 위해서 어떠한 행위도 하지 않을 것입니다.

우리는 다른 상황에 대해서도 비슷한 분석을 수행할 수 있습니다. 세부 사항은 여기서 생략됐지만, 그녀가 만약 이중 지불을 수행하는 모든 경우에 Alice의 순이익은 항상 마이너스임을 보여줄 수 있습니다.

다른 상황은 Alice가 정직하고, 그녀의 몇몇 피어가 악의적일 때입니다. Alice가 소액 결제를 악의적인 피어들 중 한명에게 보낸 후, 이 악의적인 피어는 그녀에게 리소스를 전달하지 않을 수 있습니다. 이러한 상황에서, Alice는 리소스를 얻기 위해서 다른 피어로 변경할 수 있습니다. 각각의 소액 결제의 금액은 이론상으로 극도로 작기 때문에, Alice의 손실을 임의적으로 매우 작게 만들 수 있습니다.

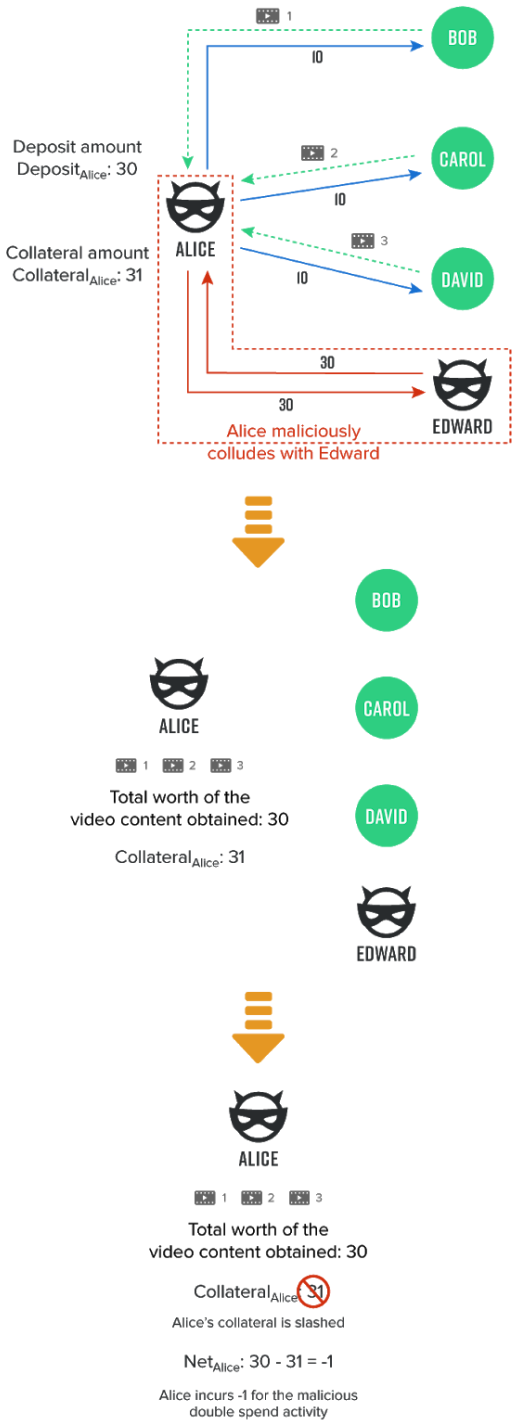

***Figure 8**. 위 그림은 악의적인 공격자인 Alice가 이중 지불을 시도하고 그 결과로 페널티를 받게 되는 것을 보여준다*

원장 스토리지 시스템 (Ledger Storage System)

스트리밍에서 소액 지불(micropayment)를 용이하게 하기 위해 공용 원장(public ledger)을 사용하는 것은 트랜잭션 처리량이 높아야 할 뿐만 아니라, 저장 공간 관리도 중요하기 때문에 까다로운 작업입니다. "바이트 당 지불(pay-per-byte)" 보장을 이루기 위해서, 각 시청자는 수 초마다 지불금 (payment)을 보냅니다. 보통 만명의 동시 사용자가 있을 때, 초당 수천개의 트랜잭션을 생성해 낼 수 있습니다. 오프 체인 결제 풀(off-chain payment pool)이 이미 상당한 양의 온 체인 트랜잭션을 줄여 주지만, 블록 및 상태 데이터는 여전히 풍선효과처럼 빠르게 커질 수 있습니다.

우리는 이 문제를 해결하고 데이터 센터에서 실행되는 강력한 서버 클러스터 또는 상용 데스크톱 PC 일지라도 여러 타입의 기계에 적응할 수 있는 스토리지 시스템을 설계했습니다.

스토리지 마이크로서비스 아키텍처

서버 클러스터의 프로세싱 및 스토리지 성능을 활용하기 위해, 주요 설계 결정은 장부의 다른 모듈을 다른 시스템에서 실행하도록 구성할 수있는 최신 웹 서비스 백엔드에서 흔히 볼 수있는 널리 사용되는 마이크로 서비스 아키텍처를 채택하는 것입니다.
특히, 합의 모듈과 스토리지 모듈은 분리될 수 있습니다. 잠재적으로 컨센서스 모듈은 MapReduce 프레임 워크를 사용하여 트랜잭션을 병렬로 처리하기 위해 여러 시스템에서 실행될 수 있습니다.

Theta Ledger는 이더리움과 비슷하게 트랜잭션 블록들과 계정의 상태 기록 둘다 저장합니다. 스토리지 모듈의 아래 레이어는 키 값을 저장하는 공간입니다. Theta Ledger는 단일 시스템 LevelDB에서 사실상 무제한 데이터를 저장할 수 있는 MongoDB와 같은 클라우드 기반 NoSQL 데이터베이스에 이르기까지 여러 데이터베이스에 대한 인터페이스를 구현합니다. 따라서 Ledger는 단일 컴퓨터에서 실행될 수 있으며, 또한 서버 클러스터에서 실행하도록 구성할 수도 있습니다.

History Pruning

마이크로서비스 아키텍처는 강력한 서버 클러스터에 잘 맞지만, 가정용PC에서 Ledger를 운영할 때 여전히 저장 공간 제약 문제를 직면하게 됩니다. 우리는 저장공간 소비를 줄이기 위한 여러 기술들을 설계하였습니다.

이더리움과 비슷하게, Theta Ledger는 각 블록의 전체 상태를 저장합니다. 그리고 상태 트리 루트 (state tree root)는 해당 블록의 헤더에 저장됩니다. 상태 기록에 의해 소모되는 저장 공간을 줄이기 위해서, Theta Ledger는 상태 기록 잘라내기(state history pruning)를 구현하였으며, 아래 그림에 나와있는 참조카운팅 (reference counting) 기법을 사용하였습니다.

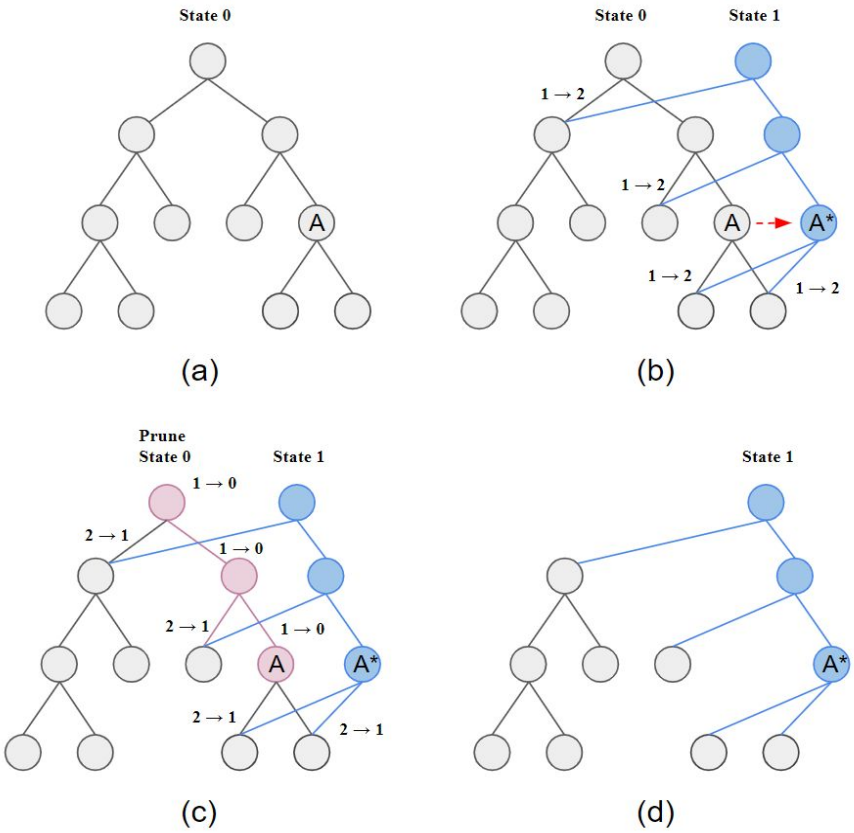

***Figure 9**. reference counting를 이용한 상태 기록 pruning*

Leger의 상태는 (즉, 각 계정의 토큰 잔액 등)은 Merkle-Patricia 트리를 이용하여 저장됩니다. Figure 6(a)는 루트의 State 0 으로 표시된 초기 상태 트리를 보여줍니다. 각 노드는 노드의 부모 수와 동일한 "참조 횟수(reference count)"라는 속성이 있는 트리입니다. 초기 상태 트리에서, 각 노드는 오직 하나의 부모를 갖고 있기 때문에, 모든 참조 횟수는 1로 설정되어 있습니다.

Figure 6(b) 에서, 계정 A는 새롭게 합의된 블록의 트랜잭션들을 적용하고나서 A* 로 업데이트 됩니다. 따라서 새로운 루트 State 1 과 A * (파란색 노드와 선)를 연결하는 Merkle 분기와 함께 새로운 Merkle 상태 루트 State 1 이 생성됩니다. 새로운 노드가 추가되었기 때문에, 새로운 노드와 직접적으로 연결된 자녀 노드의 참조 횟수를 1에서 2로 업데이트 합니다.

어떤 시점에 우리는 저장 공간을 절약하기 위해 State 0을 삭제하기로 결정할 수 있습니다. 이는 참조 횟수가 0인 노드를 루트 State 0에서부터 재귀적으로 삭제하여, 삭제가능한 노드가 남지 않을 때까지 수행함으로써 완료될 수 있습니다. 노드가 삭제될 때, 삭제된 노드의 모든 자녀들의 참조 횟수는 1만큼 줄어듭니다. Figure 6(c)는 이 과정을 보여줍니다. 그리고 Figure 6(d)는 pruning의 결과를 보여줍니다. 최대 수준의 상태 저장공간 소형화를 위해서, 가디언 풀에 의해 블록이 완결되면 해당 블록 이전의 모든 기록을 삭제할 수 있습니다. 또한 Ledger는 상태들의 제한된 기록만을 유지하도록 설정될 수 있습니다. 예를 들어, 사용가능한 저장 공간에 따라, 최신 1000개 블록의 상태 트리만을 유지할 수 있습니다.

참조 카운팅(reference counting) 기술을 사용하면 상태 트리를 정리 (pruning) 할 때 $O(k \log N)$의 시간 복잡도가 있음을 알 수 있습니다. 여기서 k는 한 블록의 트랜잭션에 의해 업데이트 된 계정 수이고 N 은 총 계정 수입니다. 일반적으로, k 는 2백개에서 천개의 범위를 가집니다.

따라서 상태 트리를 정리(pruning)하는 것은 매우 효율적이여야 하며 너무 많은 시간이 걸리면 안됩니다.

트랜잭션 블록들에 의해 소비되는 저장공간을 관리하는 것은 더 간단합니다. 블록이 완결되고 난 후, 우리는 단순히 모든 이전 블록들을 삭제하거나, 상태 트리와 비슷하게 제한된 기록만을 유지할 수 있습니다.

이러한 기술들로, 일반 PC와 랩탑들은 가디언 노드를 실행하기에 충분해질 수 있습니다.

상태 동기화 (State Synchronization)

이전 세대 블록 체인을 사용하는 문제점 중 하나는 상태 동기화 시간입니다. 새로운 노드를 회전시킨 후 일반적으로 창 블록으로부터 전체 블록 히스토리를 다운로드해야 합니다. 완료하는 데 며칠이 걸릴 수 있으며 이미 사용자 채택의 장애물이 됩니다.

폴 노드에 저장된 상태와 블록 기록은 동기화 시간을 극적으로 줄일 수 있습니다. 새로운 노드가 시작하고나서, 첫번째 단계는 모든 검증자와 가디언들의 join/leave 트랜잭션과 최근 완결된 블록까지의 이러한 특별 트랜잭션이 포함된 블록 헤더들을 다운받는 것입니다. 검증자와 가디언 서명이 포함된 헤더와 특별한 트랜잭션들로, 새로운 노드는 현재의 검증자 위원회와 가디언 풀을 얻어낼 수 있습니다. 검증자 및 가디언 집합 변경은 비교적 드물기 때문에, 이 단계에서 다운로드하고 확인해야하는 데이터의 양은 최소화되어야 할 필요가 있습니다

두번째 단계에서, 새로운 노드는 최신 완결된 블록에 대응되는 상태 트리를 다운받아야 합니다. 그리고 트리의 루트 해시가 최신 완결된 블록에 저장된 상태 해시와 동일한지 확인할 필요가 있습니다. 마지막으로, 새로운 노드는 상태 트리의 무결성을 확인합니다 (예: 머클 분기의 유효성). 모든 체크가 통과된다면, 새로운 노드는 새로운 블록을 들을 수 있고, 합의 프로세스에 참가할 수 있습니다.

이중 통화 시스템과 토큰 메커니즘

네트워크의 보안과 적절한 거버넌스의 설치 그리고 네트워크의 경제환경을 관리하기 위해서, Theta는 이중 통화 시스템을 도입할 것입니다. 이미 많은 사람들이 소유하고 있고 원래 알고 있던 Theta 토큰은 Theta 네트워크의 보안을 유지하고, 관리하고, 스테이크(Stake, PoS에서의 채굴)하기 위해 사용됩니다. 반대로, 각각의 연산들 (비디오 세그먼트 트랜잭션, 스마트 컨트랙트 연산 등)은 추가적인 토큰인 감마(Gamma)에 의해서 지불됩니다.

두번째 토큰을 도입한 주요한 두가지의 이유는 다음과 같습니다:

첫번째로, 이렇게 함으로써 각 토큰의 유틸리티와 목적을 분리시킬 수 있습니다. Theta는 네트워크의 스테이킹(Staking, PoS에서의 채굴)과 보안을 위해서 엄격하게 사용되고, Gamma는 유틸리티 기반의 네트워크 작업을 위해서 사용됩니다. 스테이킹은 본질적으로 토큰의 유통량을 감소시키지만, 비디오 세그먼트 트랜잭션들과 스마트 컨트랙트는 매일 수백만 건의 높은 트랜잭션을 원활하게 할 수 있는 높은 유동성을 가진 토큰을 필요로 하기 때문에 이러한 분리작업은 필수 적입니다.

두번째로, 같은 토큰을 스테이킹과 연산에 사용할 때 발생하는 여러 거버넌스 문제들을 해결하기 위해 두개의 토큰이 필요합니다. 토큰이 연산에 사용되기 위해서는 반드시 높은 유동성을 갖고 있어야 합니다. 따라서 악의적인 공격자가 높은 유동성을 가진 토큰을 오픈

마켓에서 상당량을 축적할 수 있습니다. 만약 이렇게 악의적인 공격자가 축적한 토큰이 스테이킹에도 사용이 된다면, 악의적인 공격자들은 잠재적으로 Theta 네트워크의 보안을 위협할 수 있습니다. 두가지의 기능을 두 개의 토큰으로 분리함으로써 (스테이킹과 연산), 위험 부담이 상당히 감소합니다.

쎄타 토큰 공급 및 메커니즘

ERC20 토큰으로서, 쎄타 토큰의 공급량은 현재 10억개로 고정되어 있습니다. 메인넷 런칭 시, 각 홀더들이 보유한 ERC20 쎄타 토큰은 새로운 블록체인의 쎄타 토큰으로 1:1 교환됩니다. 새로운 블록체인의 고유한 Theta의 공급량은 10억개로 고정되고, 이는 더 이상 새로운 쎄타 토큰이 만들어지지 않는다는 것을 의미합니다.

쎄타 토큰의 공급량이 고정된 주요 이유는 악의적인 공격자가 네트워크를 위협하기 위해 충분한 토큰을 얻는 것이 엄청나게 비용이 많이 들도록 하기 위해서입니다. 새로운 쎄타 토큰이 절대 생성되지 않기 때문에, 쎄타 토큰을 얻기 위한 유일한 방법은 존재하는 토큰을 구입하는 것이고 이는 시간이 지남에 따라 토큰의 가격을 더욱 비싸게 만들어 네트워크를 컨트롤할 만큼의 쎄타 토큰을 모으는 것을 더욱 비싸게 만듭니다.

감마(Gamma) 토큰 공급 및 메커니즘

감마는 Theta 블록체인의 추가적인 토큰으로, 비디오 세그먼트 소액결제와 스마트 계약 연산을 위한 "가스"로서 지불되는데 사용됩니다. 감마 토큰은 Theta blockchain위에 만들어지며 50억개의 감마가 메인넷이 출시되는 시점에 생성될 것입니다. 이러한 감마의 초기 공급은 모든 쎄타 토큰 홀더들에게 토큰 스왑 시 분배될 것이며, 이러한 충분한 양의 감마는 네트워크가 효과적으로 동작하기 위한 씨앗으로 작동할 것입니다.

토큰 스왑 시, Theta 토큰 홀더는 각 쎄타 토큰 당 5개의 감마를 얻게 될 것입니다. 초기에는, multi-level BFT 합의 메커니즘이 출시되고 가디언 풀이 구성되기 전까지는 감마 토큰이 증가하지 않을 것입니다. 이후에는, 검증자와 가디언 노드들은 그들이 각각의 기능을 수행하기 위해서 쎄타 토큰을 스테이킹해야 합니다. 검증자와 가디언 노드들 모두 감마를 그들이 스테이킹한 쎄타 토큰의 양에 비례해 얻을 수 있으며, 총 보상은 감마 공급량의 증가량과 동일합니다. 감마의 공급의 목표 증가량은 연간 5%로 초기에 설정됩니다. 이 비율은 비디오 플랫폼들의 감마의 수요에 따라 동적으로 조정될 수 있습니다. 즉, 감마의 공급량은 연간 5%씩 증가합니다. 만약 당신이 가디언 노드를 동작시키고 Theta 토큰을 스테이킹 한다면, 얻게 되는 감마 토큰의 양은 다음과 같습니다.

$$\text{받게 되는 감마 토큰 양} = \text{새롭게 생성되는 감마 토큰 양} \times \frac{\text{사용자가 } Staking \text{ 한 } Theta \text{ 토큰 양}}{\text{총 } Staking \text{ 된 } Theta \text{ 토큰 양}}$$

적절한 수의 감마 유통량을 유지하기 위해서, 스마트 계약을 배포하거나 상호작용하기 위해 사용되는 모든 감마는 소각됩니다. 감마의 생성과 소각을 네트워크 사용/채택에 연관시킴으로써, 감마의 토큰 양은 수요와 연관되어 건전한 균형을 유지할 것입니다.

검증자와 가디언 노드들

검증자 집합은 초기에 Theta Labs에서 운영하는 노드들로 구성되며 추가적으로 주요 전략 파트너사들이 운영하는 검증 노드들이 따라옵니다. 궁극적으로 높은 표준 (노드 가용성,

하드웨어 및 대역폭 요구 사항 등)을 수행하고 충분한 수의 쎄타 토큰을 스테이킹하는 가디언 노드는 검증 노드로서 참여할 수 있습니다. 우리의 최종 목적은 Theta Labs, 비디오 플랫폼 파트너들, 그리고 커뮤니티 멤버들로 구성된 검증자 집합을 만들어 어떠한 하나의 객체 혹은 그룹이 악의적으로 행동 가능할 만큼 네트워크를 컨트롤 할 수 없게 만드는 것입니다. 어떠한 검증자가 악의적으로 행동한다면, 가디언 풀이 악의적인 행위를 방지하고 악의적인 검증자를 제거하기위한 두 번째 방어선 역할을 할 정도로 충분히 다양하게 구성되어야 합니다. 네트워크에 위해를 끼치는 행동을 하는 악의적인 행동자의 Staking한 Theta는 삭감되어 사라집니다 (몰수).

우리는 가디언 노드의 주요 기능이 메인넷 출시 이후 메이저 업그레이드에서 출시될 것으로 예상하고 있습니다. 사용자들이 가디언 노드로 동작하고 그들의 Theta 토큰을 스테이킹 할 수 있도록 도와주는 독립적인 클라이언트가 출시될 예정입니다. 현재 구축된 프로토콜은 트랜잭션 처리량을 희생시키지 않으면서 최대 1,000 개의 가디언 노드를 지원할 수 있습니다. 가디언 노드들의 최적의 집합을 성취하기 위해서, 우리는 약 10 만 – 100만 Theta 토큰의 범위를 가디언 노드 당 스테이크가 허용되도록 설정할 것입니다. 이 수치는 메인넷 출시 전까지 이후 테스팅과 커뮤니티의 피드백을 반영하여 변경될 수 있습니다.

Future Work

이 백서에서는 분산형 비디오 스트리밍 네트워크를 위한 인센티브 메커니즘인 새로운 블록체인과 토큰인 Theta 프로토콜을 소개하였습니다. 쎄타 네트워크는 시청자들이 그들의 컴퓨팅과 대역폭 리소스를 공유하도록 격려하고 수 많은 기술과 비즈니스 문제들을 해결합니다.

여기에 고유한 Theta 네트워크의 초기 출시 이후에, 우리가 미래 과제로 분류해 놓은 프로토콜과 네트워크의 여러 기술적 측면이 있습니다.

- **불법 복제 방지**. 네트워크는 불법 복제 방지를 포함하도록 확장될 수 있습니다. 토큰은 특정 컨텐츠를 스트리밍하고 캐시하기 위해 사용될 수 있기 때문에, 컨텐츠는 "토큰이 요구되는" 또는 "프리미엄 컨텐츠"로 태그 됨으로써 토큰은 네트워크 내에서 "불이익(disincentive)" 역할을 합니다.

- **범용 목적의 서비스 플랫폼**. 쎄타 프로토콜은 사실 스트리밍과 독립적입니다. 쎄타 프로토콜은 다른 종류의 서비스(예: 컴퓨팅 리소스 공유)를 다루기 위해 확장되어 엔드 유저들이 무료로 이러한 서비스를 제공받도록 할 수 있습니다.

- **"무한한 트랜잭션 처리량"을 위한 사이드체인/플라즈마**. 튜링-완전 스마트 컨트렉트, 사이드체인과 같은2-레이어 구조, 상태(state) 채널[10], 플라즈마[11]를 Theta 블록체인 위에 구축하여 제한되지 않는 트랜잭션 처리량을 달성할 수 있습니다.

[10] https://www.jeffcoleman.ca/state-channels/

[11] *Poon et al*. Plasma: Scalable Autonomous Smart Contracts

창립 & 자문 팀

Theta 네트워크의 창립 멤버

Mitch Liu - Liu는 Theta Labs와 SLIVER.tv의 CEO이자 공동 창립자입니다. SIIVER.tv는 360° VR 환경에서 e-스포츠 이벤트들을 실시간 스트리밍하여 볼 수 있도록 해주는 특허기술들을 보유하고 있고 인텔 Extreme Masters, Turner ELEAGUE, ESL ONE 그리고 글로벌 토너먼트 운영업체 중 하나인 Dreamhack와 파트너쉽을 맺고 있는 엔터테인먼트 플랫폼입니다. 또다른 공동 창립자인 Jieyi Long과 함께 가상 현실 360° 비디오 스트리밍을 위한 2개의 특허를 보유하고 있고, 2개의 추가 특허 출원, 그리고 효율이 높은 360° 라이브 비디오 스트림 생성을 위한 새로운 알고리즘을 보유하고 있습니다.

2010년에, Liu는 거의 1억회 다운로드를 달성한 Tap Fish 모바일 게임 프랜차이즈로 유명한 Gameview Studios를 공동 창립하였습니다. 이 회사는 출시 6개월만에 일본의 선도적인 모바일 게임 회사인 DeNA에 의해서 인수되었습니다. 이 전에는 소셜 및 모바일 비디오 광고 보상의 선구자로서 2007년에 Tapjoy의 공동 창립자였습니다. 그리고 이 회사를 매출 1억 달러의 회사로 성장시켰습니다. 그는 MIT에서 컴퓨터 사이언스 & 엔지니어링 학사 학위를 받았으며, MIT Media Lab-"Interactive Cinema" 비디오 그룹에서 논문 연구를 마쳤고, 스탠포드 경영 대학원에서 MBA를 받았습니다.

Jieyi Long - Jieyi Long은 SLIVER.tv의 공동 창업자이자 CTO(최고 기술 책임자) 입니다. 그는 기술팀을 이끌어 오며 가상현실 라이브 스트리밍과 비디오 게임에 쓰이는 순간 전달 기술 관련 특허를 개발했습니다. 그는 중국 북경대에서 초소형 전자과를 졸업하였으며 Northwestern 대에서 컴퓨터 엔지니어링 박사 학위를 취득하였습니다. 그곳에서 그는 대규모 전자 시스템과 암호 열성을 최적화하는 수학적 모델과 알고리즘에 관해 연구하였습니다

Ryan Nichols - Nichols는 SLIVER.tv에서 제품과 플랫폼 관련 부서를 이끌고 있습니다. 그가 이끄는 e-스포츠 엔터테인먼트 플렛폼은 론칭 두 달 만에 10억이 넘는 가상화폐가 유통되는 e-스포츠 가상 경제를 만들었습니다. 과거에 그는 수백개의 타사 게임 개발자와 수천만명의 유져들이 사용하고 있는 게임간 가상 화폐 API를 디자인하고 론칭 한 바 있습니다.
그는 세계적으로 유명한 위쳇 앱을 탄생시킨 Tencent사에서 디렉터로 근무하였고 라이브 스트리밍 앱인 Foodies를 공동 창업하였습니다.

Rizwan Virk - Virk은 SLIVER.tv의 자문위원이며 투자자인 동시에 임시로 기업 개발부서를 이끌고 있습니다. 그는 전에 연구를 담당했던 MIT대의 Play Lab에서 디렉터를 역임하고 있습니다. Virk은 암호화폐와 BitPagos, CoinMkr, Bex.io 와 같은 블록체인 회사들의 초기 투자자이며 2013년부터 BitAngels에서 활동 해 왔습니다. Virk은 'Bitcoin Over-The-Counter Trading(2015)', 'Creating a Peer to Peer System for Buying and Selling Bitcoin Online(2013)'과 같은 여러 암호화폐 관련 논문의 공동 저자이고, 비트코인의 직거래를 위한 최초의 peer-to-peer 모바일 어플리케이션 중 하나인 Bitcoin Bazaar의 디자이너였습니다. Virk은 MIT에서 컴퓨터 사이언스 & 엔지니어링으로 학사 학위를 수여하였으며 스탠포드 경영 대학원에서 경영학 석사 학위를 수여하였습니다

Theta의 고문 팀:

MEDIA ADVISORS

STEVE CHEN
Cofounder, YouTube

YouTube

JUSTIN KAN
Cofounder, Twitch

twitch

KYLE OKAMOTO
Chief Network Officer,
Verizon Digital Media

verizon

SAM WICK
Head of Ventures,
United Talent Agency

UNITED TALENT AGENCY

KAREN HUH
Senior Vice President,
CJ Hello

CJ HELLO

JOOSANG LEE
CEO, SBS Digital News Lab

SBS

BLOCKCHAIN ADVISORS

STEVE DAKH
CTO, SmartWallet
Founding developer, Ethereum

ETHEREUM

MA HAOBO
CEO, aelf

aelf.

SHOUCHENG ZHANG
Chairman, DHVC

DHVC

FAN ZHANG
Founder, Sequoia Capital China

SEQUOIA

TRAVIS SKWERES
Founder, CoinMkt

CoinMkt

DOVEY WAN
Founding Partner,
Primitive Ventures

PRIMITIVE