헬륨

분산된 무선 네트워크

Amir Haleem Andrew Allen Andrew Thompson Marc Nijdam Rahul Garg Helium Systems, Inc.

릴리스 0.4.2 (2018-11-14)

추상적인

사물 인터넷은 8000억 달러 규모의 산업으로 84억 개 이상의 온라인 연결된 장치 가 있으며 2021년까지 지출이 거의 1조 4000억 달러에 이를 것으로 예상됩니다[1]. 이러한 장치의 대부분은 작동하려면 인터넷에 연결해야 합니다. 그러나 셀룰러, WiFi 및 Bluetooth와 같은 현재 솔루션은 최적이 아닙니다. 너무 비싸고, 너무 전력 소모가 많거나, 범위가 너무 제한되어 있습니다.

Helium 네트워크는 전력을 많이 소모하는 위성 위치 하드웨어나 값비싼 셀룰러 요금제 없이도 전 세계 어디에서나 무선으로 인터넷에 연결하고 위치를 파악할 수 있는 분산형 무선 네트워크입니다. 헬륨 네트워크를 구동하는 것은 커버리지 제공자와 커버리지 소비자 간의 양면 시장을 장려하는 기본 프로토콜 토큰이 있는 블록체인입니다 . 블록체인의 도입으로 우리는 현재 독점에 의해 통제되는 산업에 탈중앙화를 주입합니다. 그 결과 무선 네트워크 범위는 경쟁에 힘입어 현재 비용의 일부만으로 전 세계 어디에서나 사용할 수 있는 상품이 되었습니다.

당사의 안전한 오픈 소스 프리미티브를 통해 개발자 는 저전력 인터넷 연결 장치를 빠르고 비용 효율적으로 구축할 수 있습니다. Helium 네트워크는 산업 전반에 걸쳐 다양한 애플리케이션을 갖고 있으며 이러한 종류의 최초의 분산형 무선 네트워크입니다.

1. 소개

세상은 탈중앙화되고 있습니다. 수많은 플랫폼, 기술 및 서비스가 중앙 집중식 독점 시스템에서 분산된 개방형 시스템으로 이동하고 있습니다. Napster(창립자 중 한 명인 Shawn Fanning에 의해 생성됨)[2] 및 BitTorrent와 같은 피어 투 피어 네트워크 는 블록체인 네트워크와 암호화폐가 구축될 수 있는 길 을 열었습니다.

이제 비트코인, 이더리움 및 기타 블록체인 네트워크는 분산 트랜잭션 원장의 가치를 보여주었습니다. 파일 저장, 신원 확인 및 도메인 이름 시스템과 같은 기존 인터넷 서비스 는 현대적인 블록체인 기반 버전 으로 대체되고 있습니다. 소프트웨어 수준의 탈 중앙화가 빠르게 진행되고 있지만 물리적 네트워크는 더 오래 걸립니다. 관련되는. 이러한 네트워크는 종종 특수 하드웨어가 작동해야 하므로 분산화하기가 더 복잡 합니다.

헬륨 네트워크는 광역 무선 네트워킹 시스템, 블록체인 및 프로토콜 토큰입니다. 블록체인은 Helium Consensus Protocol이라고 하는 새로운 합의 프로토콜과 Proof-of-Coverage라고 하는 새로운 종류의 증명에서 실행됩니다.
암호학적으로 검증된 물리적 위치와 시간 에서 무선 네트워크 커버리지를 제공하는 광부 는 헬륨 네트워크에 증명을 제출하고 가장 좋은 증명을 제출한 광부 는 고정된 에포크에서 비동기식 비잔틴 결함 허용 합의 그룹에 선출됩니다 . 합의 그룹 의 구성원은 다른 채굴자가 제출한 암호화된 트랜잭션을 수신하여 매우 높은 트랜잭션 속도 로 블록으로 형성합니다 . 블록체인 프로토콜 외에도 Helium Wireless 프로토콜인 WHIP는 단일 조정자에 의존 하지 않는 독립 공급자 네트워크를 통해 무선 장치와 인터넷 사이에 양방향 데이터 전송 시스템을 제공합니다. 인터넷으로 데이터 를 보내고 받고 비용을 지불하고 자신의 위치를 파악합니다. (2)

광부는 네트워크 범위를 제공하기 위해 토큰을 얻습니다. (3)
광부는 거래 및 헬륨 네트워크의 무결성 검증을 통해 수수료를 받습니다 .

참고: 이 백서는 진행 중인 지속적인 작업을 나타냅니다. 우리는 이 문서를 최신 개발 진행 상황과 함께 최신 상태로 유지하기 위해 노력할 것입니다. 지속적이고 반복적인 개발 프로세스의 결과로 결과 코드 및 구현은 이 백서에 나와 있는 것과 다를 수 있습니다.

관심 있는 독자가 https://github.com/helium 에서 GitHub 리포지토리를 정독하도록 초대합니다. 시간이 지남에 따라 시스템의 다양한 구성 요소를 계속해서 공개 합니다.

1.1 주요 구성 요소

Helium 네트워크는 다음과 같은 주요 구성 요소를 중심으로 구축됩니다 .

커버리지 증명 우리는 채굴자 들이 무선 네트워크 커버리지를 제공 하고 있음을 증명할 수 있게 해주는 계산적으로 저렴한 커버리지 증명을 제시합니다. 우리 는 광부가 허용하는 직렬화 증명을 사용하여 이러한 증명을 고정합니다.

암호학적으로 안전한 방식으로 네트워크의 다른 사람과 관련된 시간을 정확하게 표시하고 있음을 증명합니다 .

헬륨 네트워크 우리는 WHIP 서비스를 위해 구축 된 완전히 새로운 목적의 블록체인 네트워크를 시연하고 장치 인증 및 식별을 위한 시스템을 제공하고 데이터 전송 및 신뢰성에 대한 암호화 보장을 제공 하며 WHIP를 중심으로 설계된 트랜잭션 프리미티브를 제공하는 등 의 작업을 수행합니다.

Helium Consensus Protocol 우리는 Proof-of-Coverage를 통해 제공된 ID와 비동기식 비잔틴 결함 허용 프로토콜을 결합하여 무허가 , 높은 처리량, 검열 방지 시스템 을 생성 하는 새로운 합의 프로토콜 구성을 제시합니다.

WHIP 광대한 영역의 저전력 장치용으로 설계된 WHIP라는 새로운 오픈 소스 및 표준 호환 무선 네트워크 프로토콜을 소개합니다. 이 프로토콜은 독점 기술이나 변조 체계가 필요 하지 않은 수십 개의 제조업체에서 제공하는 기존 상용 무선 칩에서 실행되도록 설계되었습니다 .

Proof-of-Location 우리는 값비싸고 전력을 많이 소모하는 위성 위치 하드웨어 없이 WHIP를 사용하여 장치 의 물리적 지리적 위치를 해석하는 시스템을 설명합니다 . 장치 는 블록체인에 기록된 주어진 순간에 자신의 위치에 대해 변경 불가능하고 안전하며 검증 가능한 주장을 할 수 있습니다 .

DWN 우리 는 여러 독립 광부를 통해 장치에 대한 인터넷에 대한 무선 액세스를 제공 하고 Helium 네트워크 의 참가자가 준수해야 하는 Helium 네트워크 및 WHIP 사양을 간략하게 설명 하는 분산형 무선 네트워크(DWN) 를 제시합니다. 라우터 는 인터넷 과 데이터를 주고받는 대가로 이 광부 네트워크에 비용을 지불 하고 광부는 네트워크 범위를 제공 하고 인터넷에 장치 데이터를 전달하기 위해 새로 발행된 토큰으로 보상을 받습니다 .

1.2 시스템 개요

- Helium 네트워크는 고유 토큰 을 사용하여 특별히 제작된 블록체인에서 WHIP를 중심으로 구축된 분산형 무선 네트워크 입니다.
- 장치는 WHIP와 호환되는 무선 칩 및 펌웨어가 포함된 하드웨어의 형태를 취하고 인터넷과 데이터를 주고받기 위해 광부에게 지불하여 토큰을 사용합니다.
- 채굴 자는 WHIP와 인터넷 애플리케이션인 라우터 사이에 다리를 제공하는 전용 하드웨어를 통해 무선 네트워크 커버리지를 제공함으로써 토큰을 얻습니다 .
- 장치는 개인 키를 상용 키 저장 하드웨어에 저장하고 공개 키를 블록체인에 저장합니다.
- 채굴자는 위성에서 파생된 위치, 블록체인의 특별한 유형의 거래를 주장하고 토큰 보증금을 스테이킹 하여 네트워크에 합류합니다 .
- 광부는 데이터 전송 및 위치 증명 서비스에 대해 수락할 가격을 지정하고 라우터 는 장치 데이터 에 대해 지불할 가격을 지정합니다 . 광부는 장치의 지정된 라우터에 데이터를 전달했음을 증명하면 지불 됩니다.
- 채굴자는 비동기식 비잔틴 결함 허용 합의 그룹 에 선출되어 블록체인 의 새로운 블록 생성에 참여합니다 .
- 채굴자는 합의 그룹 에 속해 있는 동안 생성된 블록에 대해 새로 생성된 프로토콜 토큰으로 보상을 받습니다 .
- 주어진 에포크에서 합의 그룹으로 선출될 광부의 확률은 그들이 제공하는 무선 네트워크 커버리지의 품질을 기반으로 합니다.
- 블록체인은 광부가 만들고 있는 무선 네트워크 범위를 정직하게 대표 하도록 보장하기 위해 범위 증명을 사용 합니다.

[그림 1]은 헬륨 네트워크를 시각적으로 나타낸 것이다.

2. 헬륨 DWN

DWN의 핵심 구성요소를 소개합니다.

2.1 참가자

헬륨 네트워크에는 장치, 광부 또는 라우터 의 세 가지 유형의 참가자가 있습니다 .

장치 는 WHIP[섹션 2.4]와 호환되는 하드웨어를 사용 하여 인터넷에서 암호화된 데이터를 보내고 받습니다 . 디바이스에서 전송된 데이터 는 핑거프린트되며, 해당 핑거프린트 는 블록체인에 저장됩니다.

광부 는 WHIP 장치와 인터넷 사이의 장거리 브리지를 제공하는 핫스팟[섹션 2.5]이라고 하는 특수 제작된 하드웨어를 통해 헬륨 네트워크에 무선 네트워크 범위를 제공합니다. 사용자 는 WHIP를 준수하는 핫스팟을 구매하거나 구축하고 해당 지역에서 작동하는 다른 광부의 밀도에 비례하여 토큰 보증금을 스테이킹하여 헬륨 네트워크에 광부로 가입합니다 [섹션 5.3.3]. 광부 는 장치가 사용할 수 있는 무선 네트워크 범위를 지속적으로 제공하고 있음을 증명하기 위해 범위 증명[섹션 3] 프로세스에 참여 합니다. 채굴자는 유효한 증명을 제출하지 않고 블록이 통과함에 따라 감소하는 점수[섹션 3.3.4]로 헬륨 네트워크에 합류합니다. 주어진 에포크에서 새로운 채굴자 그룹이 블록체인에서 새로운 블록 을 채굴하고 블록을 받는 합의 그룹에 선출됩니다.

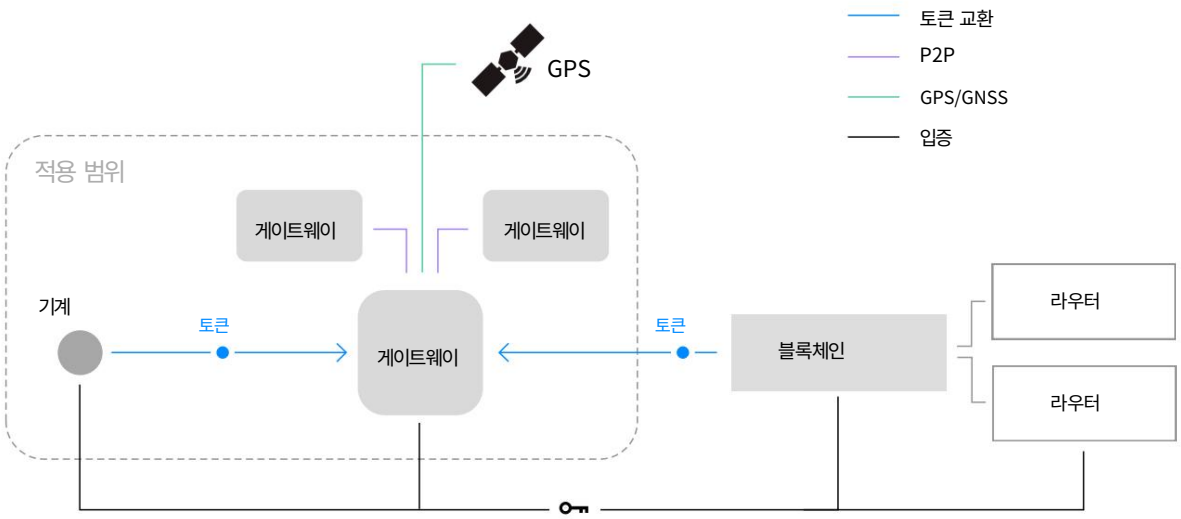

그림 1. 시스템 개요

일단 채굴된 블록에 포함된 모든 거래에 대한 보상 및 거래 수수료 . 광부의 점수가 떨어지면 합의 그룹에 선출될 확률이 떨어지고 채굴 블록이 감소합니다.

라우터 는 채굴자로부터 암호화된 장치 데이터를 구매하는 인터넷 응용 프로그램입니다. 충분한 수의 광부가 있는 위치에서 라우터는 우리가 위치 증명 이라고 하는 위성 위치 하드웨어 없이 장치를 지리적으로 찾기 위해 충분한 패킷 사본을 얻기 위해 여러 광부에게 비용을 지불할 수 있습니다 . 라우터는 장치 데이터 암호화의 종료 지점입니다. 장치 는 주어진 광부가 라우터로 데이터를 보내야 하는 블록체인에 기록 하므로 Helium 네트워크의 모든 핫스팟이 장치 데이터를 적절한 라우터로 보낼 수 있습니다. 라우터는 장치 데이터 가 올바른 목적지로 전달되었고 광부 가 해당 서비스에 대해 지불해야 함을 핫스팟에 확인할 책임이 있습니다.

2.2 블록체인

Helium 네트워크는 DWN 의 운영에 애플리케이션 로직 코어를 실행하고 , 변경할 수 없는 장치 데이터 지문을 저장 하고, 트랜잭션 시스템을 제공하는 비용 효율적인 방법을 제공 하도록 설계된 분산 원장입니다 . Helium 네트워크는 Helium Consensus Protocol[섹션 6]을 사용하여 합의를 달성하는 변경 불가능한 추가 전용 트랜잭션 목록입니다 .

DWN 의 내부 및 외부 사용자는 DWN 을 위해 처음부터 새로 구축된 새로운 프로토콜인 블록체인에 액세스할 수 있습니다 .

블록체인은 헤더와 트랜잭션 목록을 포함하는 블록으로 구성됩니다. [섹션 5]에 설명된 여러 종류의 거래가 있습니다.

주어진 에포크에서 주어진 블록은 다음으로 구성됩니다.

블록 버전
블록 높이 이전 블
록 해시 트랜잭션 1..n 머클
해시
현재 합의 그룹의 임계값 서명

커버리지 증명[섹션 3]은 네트워크에 가치가 있으므로 광부는 정기적으로 증명을 제출해야 합니다. 모든 광부에는 시간이 지남에 따라 감소하는 점수가 있으며 블록체인에 적용 범위 증명을 제출하면 향상됩니다. 고정된 에포크에서 가장 높은 점수를 받은 채굴자들의 HoneyBadgerBFT [4] 합의 그룹이 선출됩니다. 그 시대 동안 모든 거래는 암호화 되어 블록체인에 포함하기 위해 합의 그룹에 제출됩니다 . 합의 그룹은 임계값 복호화를 사용하여 트랜잭션을 해독하고, 트랜잭션의 유효성과 순서에 동의하고, 블록으로 만들고, 합의 그룹의 구성원이 보상을 받는 블록체인에 추가하는 역할을 합니다.

합의 그룹은 관련 블록 증거(임계 서명 이상)를 제공할 필요 없이 트랜잭션을 검증하기 때문에 실제로 결제 시간이 없고 트랜잭션 처리량이 비트코인 또는

이더 리움. 헬륨 합의 프로토콜은 [섹션 6]에 자세히 설명되어 있습니다.

2.3 물리적 구현

Helium 네트워크는 또한 물리적 무선 네트워크 인스턴스화입니다. 헬륨 네트워크의 참가자는 다음과 같이 생각할 수 있습니다.

WHIP 헬륨 네트워크는 WHIP라고 하는 새로운 개방형 무선 프로토콜을 사용합니다. WHIP은 범용 개방형 표준 하드웨어 와 함께 사용하기에 적합한 장거리, 저전력, 무선 네트워크 프로토콜입니다. WHIP 호환 하드웨어 는 밀집된 도시 환경에서 수 평방 마일 또는 시골 환경에서 수백 평방 마일 이상에서 통신할 수 있습니다.

WHIP 호환 하드웨어는 표준 배터리를 사용하여 몇 년 동안 사용할 수도 있습니다. WHIP은 강력한 공개 키 암호화를 사용하고 인증은 Helium 블록체인을 사용하여 발생 하며 데이터는 장치와 해당 인터넷 호스팅 라우터 간에 종단 간 암호화됩니다 .

핫스팟 은 광역 무선 범위를 제공하고 헬륨 네트워크에 참여 하는 물리적 네트워크 장치입니다 . 핫스팟은 Helium 네트워크[섹션 3]에 대한 커버리지 증명을 생성하는 동안 인터넷의 라우터와 장치 간에 데이터를 주고 받습니다. 핫스팟은 독점 하드웨어가 없는 범용 개방형 표준 구성 요소를 사용하여 제조됩니다.

핫스팟은 추가로 필요한 하드웨어 없이 헬륨 네트워크를 사용하여 장치를 협력하고 지리적 위치를 찾을 수 있습니다 . 각 핫스팟은 수천 개의 연결된 장치를 지원할 수 있으며 수 평방 마일에 걸쳐 적용 범위를 제공할 수 있습니다.
핫스팟을 운영하는 광부는 장치 에 대한 운송 및 위치 증명 서비스에 대해 수락 할 가격을 지정합니다 .

장치 는 WHIP 호환 무선 송수신기 를 포함 하고 Helium 네트워크의 핫스팟 과 통신하는 하드웨어 제품 형태로 존재 합니다. WHIP는 저전력 데이터 전송 및 수신을 용이하게 하도록 설계되었으므로 일반적으로 장치는 표준 배터리를 사용하여 몇 년 동안 작동할 수 있는 배터리 구동 센서 형태로 존재합니다 (주 전원 장치도 꽤 잘 작동함). 장치는 제품이나 사용 사례에 따라 다양한 형태로 존재할 수 있으며 다양한 송수신 전략을 사용하여 송수신 주파수 또는 배터리 수명 을 최적화할 수 있습니다 . 장치 제조업체는 개인 키를 누출하지 않고 공개/개인 키 쌍을 안전하게 생성, 저장 및 인증할 수 있는 하드웨어 기반 키 저장소를 사용하는 것이 좋습니다 .

이 섹션에서는 무선 네트워크의 구성 요소를 확장합니다.

2.4 무선 프로토콜(WHIP)

2.4.1 동기 부여

오늘날 여러 가지 저전력 광역 네트워크(LPWAN) 기술 을 사용할 수 있습니다. 이러한 무선 기술 은 센서 및 기타 스마트 장치를 위한 장거리 저전력 인터넷 통신을 만드는 데 중점을 둡니다. 일반적으로 이러한 기술은 18bps(초당 비트 수)의 낮은 데이터 속도와 마일 단위로 측정되는 범위로 처리량을 범위로 교환합니다.

이에 비해 일반적인 WiFi 네트워크는 데이터 속도가 훨씬 더 높지만 범위는 수십 피트로 제한됩니다. LoRa[6] 및 RPMA[7]와 같은 이러한 새로운 기술 중 일부는 좋은 관심을 얻었으며 이러한 시스템 과 호환되는 상용 제품이 많이 있습니다. 그러나 우리는 분산형 무선 네트워크가 비독점 프로토콜과 변조 방식을 사용해야 하며 헬륨 네트워크의 참가자가 경쟁 하드웨어 공급업체 중에서 선택할 자유가 있어야 한다고 믿습니다 . 우리는 독점 하드웨어 위에 구축된 공개 동맹을 수용 가능한 타협으로 간주하지 않습니다 . 1세대 무선 제품에 사용된 IEEE 802.15.4[8]와 같은 많은 개방형 표준 무선 네트워킹 스택이 있지만 어느 것도 당사의 초장거리 및 저전력 기준을 충족하지 않습니다. 새로운 프로토콜의 생성 을 주도한 것은 이러한 개방형 솔루션의 부족입니다 .

2.4.2 개요

WHIP을 소개합니다. WHIP는 GHz 미만의 비면허 주파수 스펙트럼에서 작동 하는 다양한 기존 무선 송수신기와 호환되는 매우 안전한 장거리 저전력 양방향 무선 네트워크 프로토콜입니다 .

무선 네트워크를 통한 인증은 최신 공개 키 암호화와 NIST P-256 ECC 키 쌍을 사용하며 모든 참가자의 공개 키가 블록체인에 저장됩니다.

변조 형식은 간단하고 널리 지원 되며 구현하기 쉽고 RF 노이즈에 대한 내성이 뛰어납니다. Texas Instruments, Microchip 및 Silicon Labs 와 같이 WHIP와 호환되는 무선 송수신기를 구현하는 수십 개의 공급업체 가 있습니다 .

WHIP는 비허가 스펙트럼 내에서 여러 채널 을 생성하고 주파수 호핑을 사용하여 채널 간에 전환 하는 협대역 무선 프로토콜입니다 . 일반적으로 주파수 호핑에는 용량이 제한된 복잡한 시간 동기화 시스템이 필요합니다. 그러나 WHIP를 사용하는 장치는 핫스팟이 언제든지 사용 가능한 스펙트럼 내의 모든 채널을 들을 수 있으므로 채널 선택 시 핫스팟과 조정할 필요가 없습니다 . 다음 목표를 달성하기 위해 협대역을 선택합니다 .

스펙트럼 효율성 비인가 RF 스펙트럼 내에서 매우 효율적으로 작동하는 것이 필요합니다 . RF는 공유, 임

따라서 용량을 늘리고 견고성을 향상시키기 위해 효율성에 중점을 두어야 합니다.

공존 성능 장치와 네트워크의 수가 증가함에 따라 간섭 없이 잡음이 많은 RF 환경에서 작동하는 능력 이 중요한 고려 사항입니다.

범위 협대역 은 핫스팟의 밀도에 따라 확장 및 축소되는 데이터 속도를 사용하여 매우 장거리 통신을 허용합니다.

2.4.3 구현

WHIP는 여러 데이터 속도, 채널 대역폭 및 오류 수정 기술을 지원합니다. 핫스팟 및 장치 는 초기 통신을 위한 최대 범위를 보장하기 위해 가장 낮은 대역폭과 기호 속도로 전달되는 신호 패킷 을 사용하여 이러한 옵션의 조합을 동적으로 협상합니다 .

전체 WHIP 사양은 분산 장치 네트워크 연합에서 제공합니다.

2.5 핫스팟

핫스팟은 광역에서 무선 RF 범위를 생성 하는 광부가 운영하는 물리적 네트워크 장치 입니다. 그들은 인터넷의 라우터와 네트워크의 장치 간에 데이터를 주고받고 , 블록체인 트랜잭션을 처리 하고, 헬륨 네트워크에 대한 커버리지 증명을 생성합니다[섹션 3]. 핫스팟은 이더넷, WiFi 또는 셀룰러와 같은 TCP/IP 가능 백홀을 사용하여 인터넷에 연결할 수 있습니다 . 각 핫스팟에는 한 번에 몇 MHz의 무선 스펙트럼을 수신할 수 있는 무선 프론트엔드 칩이 포함되어 있으며 해당 스펙트럼 내에서 전송되는 모든 무선 트래픽을 들을 수 있습니다. 이 구성 에서 변조 및 복조는 일반적으로 소프트웨어 정의 무선 (SDR)이라고 하는 소프트웨어에서 수행됩니다. 이 구조의 이점은 핫스팟이 주파수 범위 내에서 전송된 모든 장치 트래픽 을 들을 수 있고 핫스팟과 장치 간에 동기화가 발생할 필요가 없다는 것입니다. 이를 통해 장치는 저렴하고 비교적 단순하게 유지되며 무선 프로토콜 오버헤드를 줄일 수 있습니다. 광부가 핫스팟 하드웨어 비용을 최소화하려는 경우 더 비싼 무선 프론트엔드 에 대한 더 저렴한 대안으로 사양 내에서 동기화된 주파수 도약 방식도 허용 됩니다.

핫스팟은 정확한 위치 및 날짜/시간 정보 를 얻기 위해 GPS 또는 GNSS 수신기가 필요합니다 . 이 위성에서 파생된 위치는 핫스팟이 주장하는 위치 에서 실제로 무선 네트워크 범위를 제공하는지 확인하기 위해 다른 기술과 함께 사용됩니다 . 위성 위치 메시지 는 조작하기 쉽고 무선 RF 커버리지가 생성되고 있음을 반드시 증명하지 않기 때문에 [섹션 3]에 자세히 설명된 대로 이 작업을 검증하기 위해 여러 메커니즘이 필요합니다 .

위성 위치 정보는 또한 여러 핫스팟이 동일한 패킷을 관찰하는 경우 장치에 대한 위치 증명을 제공하기 위해 패킷 도착 이벤트와 상관 관계가 있습니다. 이를 통해 장치는 GPS/GNSS 트랜시버를 물리적으로 요구하지 않고 스스로 위치를 찾을 수 있으므로 경쟁 방법 보다 훨씬 적은 배터리 수명과 비용으로 정확한 위치 데이터를 제공할 수 있습니다. 이 방법은 [섹션 4]에서 자세히 설명합니다.

Heilum 네트워크 출시와 함께 완전한 오픈 소스 참조 디자인 과 완제품을 모두 사용할 수 있도록 할 것입니다.

2.6 장치

장치는 WHIP를 통해 핫스팟 과 통신할 수 있는 모든 무선 하드웨어 입니다. WHIP는 저전력 데이터 전송 및 수신을 용이하게 하도록 설계 되었으므로 일반적으로 장치는 표준 배터리를 사용하여 몇 년 동안 작동 할 수 있는 배터리 구동 센서의 형태로 존재합니다 .

WHIP는 매우 저렴한 BOM(Bill of Material)으로 다양한 공급업체에서 제공하는 상용 하드웨어를 사용하여 장치를 제조할 수 있도록 설계되었습니다.
Texas Instruments CC1125 또는 STMicroelectronics S2-LP와 같은 최신 무선 트랜시버의 기술은 독점 변조 방식 이나 물리적 계층 없이 구축 할 수 있는 매우 장거리 네트워크 시스템을 가능 하게 합니다. 이러한 라디오 중 일부는 합리적인 볼륨에서 약 $1에 사용할 수 있습니다.

각 장치 는 개인 키 누출 없이 공개/개인 NIST P-256 ECC[3] 키 쌍을 안전하게 생성, 저장 및 인증할 수 있는 Microchip ECC508A 또는 이에 상응하는 하드웨어 기반 키 저장 장치를 사용하는 것이 좋습니다. 또한 다양한 방어 메커니즘 이 보안 장치 자체에 대한 물리적 보호와 함께 키 저장 장치와 호스트 MacDevicehine 간의 암호화된 데이터에 대한 논리적 공격을 방지 합니다. 사용자는 정의된 API 를 사용하여 WHIP 무선 사양에 정의된 온보딩 프로세스의 일부로 키 저장 장치를 프로그래밍합니다 .

2.7 라우터

라우터는 핫스팟을 통해 장치에서 패킷을 수신 하고 HTTP 또는 MQTT 끝점과 같은 적절한 대상으로 라우팅 하는 인터넷 배포 응용 프로그램입니다 .

라우터는 다음을 포함 하여 Helium 네트워크에서 여러 기능을 제공합니다 .

- 헬륨 네트워크로 장치를 인증합니다.
- 핫스팟에서 패킷을 수신하고 이를 인터넷;
- OTA 업데이트를 포함한 다운링크 메시지 를 핫스팟을 통해 장치에 전달합니다.

- 운송 거래가 정직하도록 배송 확인을 제공합니다.

- Google Cloud Platform 또는

  마이크로소프트 애저; 그리고

- 전체 노드 역할을 하여 블록체인 원장 의 전체 사본을 저장하고 사용 가능하게 하는 것 [섹션 5.5]

핫스팟이 Helium 네트워크의 장치에서 데이터 패킷을 수신하면 블록체인에 쿼리하여 장치의 Helium 네트워크 주소가 지정된 경우 사용할 라우터를 결정합니다.
누구나 자유롭게 자신의 라우터를 호스팅하고 Helium 네트워크 의 핫스팟에서 전달될 장치의 트래픽을 정의할 수 있습니다. 이 기능을 통해 Helium 네트워크 사용자는 VPN과 유사한 기능을 생성할 수 있으므로 암호화된 데이터가 자신이 지정하고 선택적으로 자체적으로 호스팅할 수 있는 라우터(또는 라우터 세트)에만 전달됩니다 .

라우터는 Google Cloud Platform IoT Core 와 같은 특정 타사 인터넷 애플리케이션에 대한 인증 및 데이터 라우팅을 처리 하는 채널이라는 시스템을 구현할 수 있습니다 . 이러한 채널 구현은 장치의 온보드 하드웨어 보안을 활용하여 임베디드 마이크로컨트롤러 에서 직접 구현하기 어려운 타사에 대한 안전한 하드웨어 인증 연결을 생성할 수 있습니다 . 우리는 인터넷 서비스에 대한 추가 인터페이스를 구축하는 데 사용할 수 있는 채널의 오픈 소스 참조 구현을 제공할 것입니다.

또한 누구나 사용할 수 있는 고가용성 클라우드 라우터를 호스팅하고 다양한 운영 체제 및 배포에 대한 소스 코드 또는 바이너리 패키지로 사용할 수 있는 오픈 소스 라우터를 제공 및 유지 관리합니다 .

라우터 구현에 필요한 프로토콜 사양 은 WHIP 무선 사양 문서에 정의되어 있으며 이 문서 는 분산 장치 네트워크 연합에서 제공합니다.

3. 적용 범위 증명 및 일련 번호 증명

Helium 네트워크에서 광부는 장치가 인터넷과 통신하는 데 사용할 수 있는 무선 네트워크 범위를 제공하고 있음을 증명해야 합니다 . 채굴자는 Helium 네트워크 및 기타 채굴자가 감사 및 확인 하는 Proof-of-Coverage 프로토콜을 준수하여 이를 수행 합니다. 우리는 Proof-of- Serialization을 사용하여 광부가 네트워크의 다른 사람들과 관련하여 시간을 올바르게 표시 하고 부정직한 행동에 대한 암호학적 증거를 얻도록 합니다. Proof-of-Coverage와 같은 Helium 네트워크의 여러 구성 요소는 Proof-of-Serialization을 암호화 시간 증명으로 이러한 발생 을 근간으로 하는 암호화 "앵커"로 사용합니다. 커버리지 증명과 직렬화 증명의 조합 으로 헬륨 네트워크 내에서 발생하는 이벤트 의 대략적인 위치와 시간에 대한 암호 증명을 얻을 수 있습니다 .

3.1 동기 부여

비트코인[9] 및 이더리움[5]과 같은 대부분의 기존 블록체인 네트워크 는 본질적으로 비대칭인 알고리즘 퍼즐 에 의존하는 작업 증명 시스템을 사용합니다 . 이러한 증명 은 생성하기가 매우 어렵지만 제3자가 확인하기에는 간단합니다. 이러한 네트워크의 보안 은 유효한 증거를 생성하는 데 필요한 컴퓨팅 성능의 양이 위조하기 어렵고 후속 블록이 블록체인에 추가됨에 따라 체인의 누적 난이도 가 조작하기 엄청나게 어려워진 다는 네트워크 전체의 합의에 의해 달성됩니다. .

그러나 이러한 계산이 많은 증명은 블록체인 네트워크에 유용 하지 않습니다 . 우리는 유용성을 원장 보안을 넘어 블록체인 네트워크에 가치 있는 작업으로 정의합니다. 다른 네트워크에서 이더리움 이 스마트 계약이라는 작은 프로그램을 실행하는 것과 같이 채굴 능력을 유용한 것으로 바꾸려 는 시도가 있었지만 대부분의 작업은 유용하거나 재사용할 수 없습니다. 작업의 결정 요소는 일반적으로 엄청난 양의 전기를 소비하고 실행하는 데 상당한 하드웨어가 필요한 계산 능력이기 때문에 마이닝 프로세스 도 매우 낭비 입니다.

헬륨 네트워크에 사용된 증명은 부정직한 광부가 가명 ID를 생성하고 이를 사용하여 헬륨 네트워크를 전복하고 자격이 없어야 하는 보상을 차단하는 데 액세스하는 Sybil 공격에 저항해야 합니다 . 이것은 헬륨 네트워크와 같은 물리적 네트워크에서 관리하기 특히 어려운 공격 벡터입니다. 우리는 또한 새로운 공격 벡터인 대체 현실 공격에 저항 해야 합니다. 이 공격 은 부정직한 광부 그룹이 실제로는 존재하지 않는 물리적 세계에 무선 네트워크 범위가 존재한다고 시뮬레이션 할 수 있는 곳에 존재합니다. 이에 대한 예는 단일 컴퓨터에서 마이닝 소프트웨어를 실행하고 GPS 좌표 및 RF 네트워킹을 시뮬레이션 하는 것입니다.

우리는 나중에 Proof-of-Coverage를 사용하여 블록체인을 보호하고 Helium 네트워크에 매우 유용한 서비스를 제공하는 헬륨 합의 프로토콜[섹션 6]을 제안합니다. 이 프로토콜 은 장치가 데이터를 주고받는 데 사용할 수 있는 무선 네트워크 범위를 제공합니다 . 인터넷.

3.2 영감

커버리지 증명은 채굴 자가 특정 지역의 무선 네트워크 커버리지 W 를 도전자 C 에게 제공하고 있음을 증명할 수 있도록 하는 혁신적인 증거입니다 . 커버리지 증명은 목표 세트 Tn 이 W 를 주장 하는 대화형 프로토콜입니다. 특정 GPS 위치 L 에 존재하고 Tn 이 실제로 W 를 생성 하고 해당 커버리지가 반드시

무선 RF 네트워크를 사용하여 생성되었습니다. 커버리지 증명 은 물리적 공간에서 채굴자의 진실성 을 증명 하고 블록체인 네트워크에서 합의를 달성하는 데 사용하는 최초의 프로토콜입니다.

Proof-of-Coverage를 통해 다음을 해결하는 것을 목표로 합니다.

- 채굴자가 WHIP와 호환되는 RF 하드웨어 및 펌웨어를 운영하고 있음을 증명 하십시오.
- RF를 통해 통신하도록 하여 광부가 주장하는 지리적 위치에 있음을 증명합니다 . 그리고
- 갈등이 있을 때 어떤 버전의 현실이 올바른지 정확하게 식별

Proof-of-Coverage는 GTP(Guided Tour Protocol)[13]에서 영감을 받아 클라이언트 c 가 다양한 "투어 가이드" 컴퓨터 Gn 에 요청을 요청하여 서비스 거부 방지 시스템을 고안했습니다. 서버에 대한 액세스 s. 투어 가이드는 특정 순서로 방문해야 하며 다음 Gn 의 위치를 순서대로 나타내는 데이터 해시를 교환 해야 합니다. 모든 Gn 을 방문한 후에만 c는 s에 액세스 할 수 있습니다.

c 가 투어의 마지막 정류장에 도착 하면 Gn 에 연락 할 필요 없이 투어의 첫 번째 및 마지막 정류장이 올바른지 확인할 수 있고 c 만 알 수 있는 첫 번째 및 마지막 정류장의 증거를 s 에게 제출합니다 . 투어를 올바르게 완료한 경우 첫 번째 및 마지막 정류장 입니다.

매우 영리하고 혁신적인 시스템이지만 GTP는 RF 네트워킹의 범위가 제한되어 있으므로 헬륨 네트워크의 어느 곳에서도 피어와 통신할 수 없기 때문에 헬륨 네트워크의 증거로 직접 적합하지 않습니다.

우리는 GTP에 제시된 아이디어를 기반으로 느슨하게 증명을 구성하는 것을 목표로 하지만 우리 프로토콜에 적용할 수 있습니다.

우리는 Proof-of-Serialization과 Proof-of-Serialization을 결합 합니다. 이 증명은 Helium 네트워크의 광부가 탈 중앙화된 클라이언트 간에 암호화 시간 합의를 달성할 수 있도록 합니다.
우리는 특정 시간 서버에 의존하지 않는 안전한 방식으로 대략적인 시간 동기화를 달성하는 것을 목표로 하며 , 시간 서버가 오작동하는 경우 클라이언트 가 해당 동작에 대한 암호학적 증거를 얻게 됩니다.

3.3 적용 범위 증명 구성

Proof-of-Coverage 프로토콜을 사용 하여 인터넷 통신 과 다른 고유하고 다른 무선 주파수(RF) 통신 의 다음 특성을 활용하는 증거 를 구성하는 것을 목표로 합니다.

1. RF는 물리적 전파가 제한되어 있으므로
   탄스;
2. 수신된 RF 신호의 강도 는 송신기로부터의 거리의 제곱에 반비례 합니다. 그리고
3. RF는 (효과적으로) 아니오로 빛의 속도로 이동합니다.
   지연 시간

우리의 목표는 물리적 지역의 채굴자가 정직하게 행동 하고 WHIP와 호환되는 무선 네트워크 범위를 생성 하는지 확인하는 것 입니다. 이를 위해 챌린저 C 는 초기 타겟 T1 에서 시작 하여 일련의 순차적 타겟 Tn 에 무선으로 브로드캐스트 되는 다중 계층 데이터 패킷 O 를 결정적 으로 구성합니다. 의도된 수신자인 경우 O 의 대부분의 레이어 .

각 대상은 영수증 Ks에 서명하고 C에 전달하고 O 계층을 제거 하고 다음 대상을 위해 이를 브로드캐스트합니다. 기본적 으로 의도된 수신자만 해독할 수 있는 "봉투 봉투" 입니다.

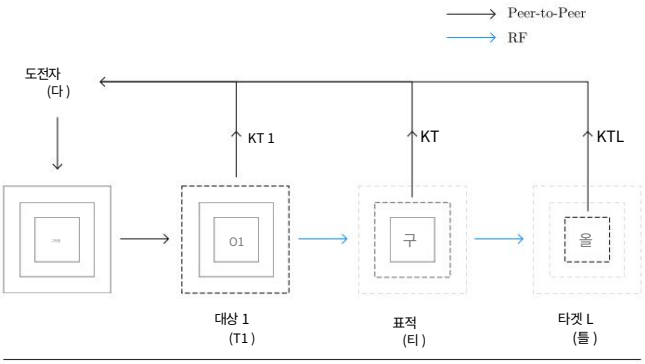

그림 2. 다계층 데이터 패킷 분해

3.3.1 초기 대상 선택

우리 는 도전자 C에 대한 지리적 참조 대상 T를 결정론적으로 찾는 것을 목표로 합니다 . C 와 T 는 모두 헬륨 네트워크의 광부입니다. T 는 지리적으로 C에 근접할 필요가 없습니다 . T 를 찾기 위해 C 는 처음 에 개인 키로 현재 블록 해시에 서명하여 검증 가능한 엔트로피 η 를 선택 프로세스에 시드합니다. 각 채굴자와 관련된 확률 은 이산 확률 분포를 형성하기 때문에[수학식 1], C 는 각 적격 채굴자와 관련된 확률을 사용하여 T 를 찾고 η 를 통해 생성된 균일한 난수를 사용하여 역 누적 분포 함수를 적용합니다 . 이를 통해 우리는 잠재적으로 부정직한 광부가 점수가 낮기 때문에 항상 표적으로 삼을 수 있으므로 C의 표적이 될 가능성이 높아 집니다 . 광부 점수가 시간이 지남에 따라 선형적으로 감소 한다는 점을 감안할 때[섹션 3.3.4], 다음이 필요합니다. 이 역 관계를 생성하여 점수가 낮은 광부 에게 프로세스에 참여하고 점수를 높일 수 있는 기회를 제공합니다. 이 감소 점수는 또한 모든 참가자가 C 에 영수증을 보내고 나머지 O 를 브로드캐스트하도록 장려합니다 .

3.3.2 다계층 챌린지 구성

T 가 선택되면 C 는 다층 챌린지를 구성해야 합니다 . O. O 는 Helium 네트워크를 통해 브로드캐스트되고 지리적으로 가까운 타겟 Tn에 의해 수신되는 데이터 패킷입니다.

지리적 근접성 은 네트워크 값 Tradius 인 T의 반경 내로 정의됩니다 . O, Ol 의 각 레이어는 E(S, ψ, R) 의 3개의 튜플로 구성되며 , ECDHE(Elliptic-Curve Diffie-Hellman) 파생 대칭 키를 사용 하는 보안 암호화 기능 이고, S 는 nonce, ψ 는 챌린지의 다음 레이어를 브로드캐스트할 시간이고 R 은 재귀적 3-튜플로 구성된 O 의 나머지 부분입니다 . Ol 의 최대 수 는 네트워크 값 Omax 에 의해 제한됩니다 .

O by C의 구성 논리는 다음과 같습니다.

1. 후보 노드 세트 Tn 은 Tn 의 모든 구성원이 T를 포함 하는 인접 무선 네트워크 내에 있도록 선택됩니다 .

2. T에서 가장 멀리 떨어진 Tn 에서 가장 높은 득점 목표를 찾아 두 개의 목표 T1 과 TL 을 선택합니다.

3. 가중 그래프 Tg 는 Tn 에서 구성 되어 서로의 무선 범위에 있는 Tg 의 구성원이 1 - score(Ta) - score(Tb) 의 값으로 가중치가 부여된 가장자리로 연결됩니다 .

4. T1 에서 T , TL 사이의 최단 경로 는 이전 단계 의 에지 가중치를 사용하여 Dijkstra의 알고리즘[10]을 사용하여 계산됩니다 .

5. 임시 공개/개인 키 쌍 Ek 및 Ek-1 은 다음 과 같습니다.
생성됨;

6. 계층 O 가 생성되어 O에 추가되고 S 는 TL 의 공개 키 조합으로 암호화되며 블록체인에서 TLk로 검색 되고 Ek - 1 은 ECDH 교환으로 검색되어 공유 비밀을 계산합니다. 당사자 C 및 TL ; 그리고

7. 모든 TL → T1 이 O에 포함된 레이어 O1 을 가질 때까지 이전 단계를 O에 추가 레이어로 반복합니다 .

결과 O 는 [그림 3] 과 같이 시각적으로 나타낼 수 있습니다 .

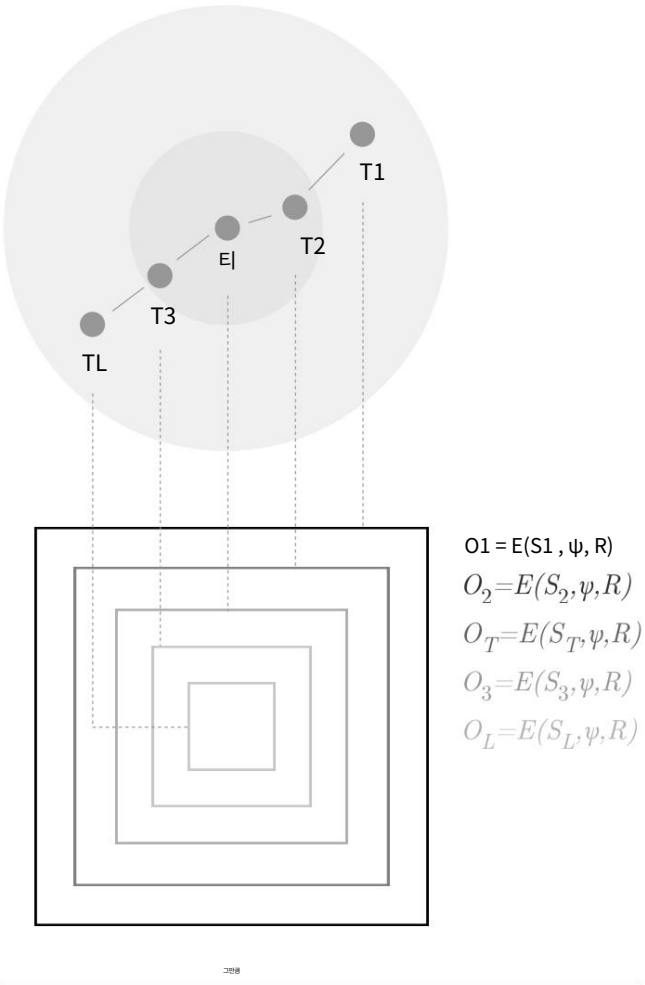

그림 3. O의 구성

3.3.3 증명 생성

O 가 구성 되면 헬륨 네트워크를 통해 T1 에 전달되고 헬륨 네트워크를 통해 T1 에 의해 즉시 브로드캐스트됩니다 . WHIP은 지점 간 시스템이 아니므로 T1 에 근접한 여러 광부가 O 를 듣게 됩니다 . 이 예에서 특정 대상 T 만이 E 를 해독 하고 유효한 영수증을 도전자 C에게 보낼 수 있습니다.

다음과 같이 Proof-of-Coverage 생성의 대략적인 흐름을 설명합니다.

1. T1 은 헬륨 네트워크를 통해 C 로부터 O 를 수신 하고 가장 바깥쪽 레이어 를 해독 하고 즉시 헬륨 네트워크 를 통해 R 을 브로드캐스트합니다 .

2. T 는 O 를 듣고 개인 키 를 사용하여 E 의 값을 해독하려고 시도합니다 .
여기서 pk: Epk (S, ψ, R);

3. T 는 도달 시간 β 와 신호 강도 를 모두 기록합니다.
O의 υ;

4. 성공하면 T는 서명된 영수증 Ks 를 생성합니다. 여기서 Ks = (S||β||υ)
T의 개인 키로 서명됩니다.

5. T 는 Helium 네트워크를 통해 C 에 K 를 제출 하고 가장 바깥쪽 레이어를 제거하고 나머지 O를 무선으로 브로드캐스트합니다. 그리고

6. 이 단계는 T1..T..TL에 대해 반복되며, TL 은 그래프 의 마지막 대상입니다.

C 는 시간 임계값 λ 내 에서 Tg 의 응답을 들을 것으로 예상합니다 . 그렇지 않으면 커버리지 증명이 완료된 것으로 간주합니다 . C 는 O에 대한 완전한 지식 을 가진 유일한 당사자 이기 때문에 β 및 υ 값의 상한은 O 의 각 레이어가 예상했던 장소와 시간에 대략적으로 전송 되었는지 확인하는 데 사용되는 C 에 의해 할당됩니다 . β 의 상한 은 Tn 과 Tn 1 사이 의 빛의 속도 τ 에 의해 제한됩니다 . 따라서 반사 또는 다중 경로로 인한 약간의 지연이 있지만 패킷은 τ 에 지리적 거리를 곱한 것보다 늦게 Tg 에 도착해서는 안 됩니다.

tance D + 약간의 작은 에피실론 값, υ = τ × D + .
υ의 경우 역제곱 법칙 때문에 Tg 1 에서 Tg 까지 전송된 패킷에 대해 가능한 최대 RSSI(Received Signal Strength Indication) μ 를 D2 로 계산할 수 있습니다 . 예상보다 가깝거나 μ = 위치 불일치를 가리기 위해 더 정되는 [illegible] 가

TL 이 C에 영수증을 전달 했거나 λ 가 경과 하면 적용 범위 증명이 완료됩니다. 서명된 영수증 모음 Ks 는 C 가 Helium 네트워크에 제출할 보증을 구성합니다 .

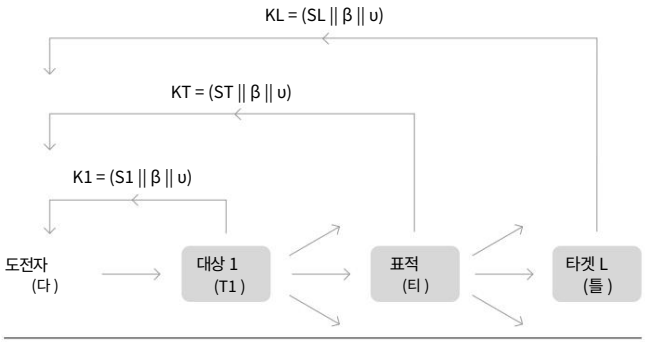

그림 4. Proof-of-Coverage 흐름

3.3.4 채점

채굴자에게 할당된 점수, 따라서 Proof-of-Coverage의 결과 점수는 [섹션 6]에 설명된 헬륨 합의 프로토콜의 필수적인 부분입니다. 광부가 헬륨 네트워크에 가입하면 점수 ϕm이 할당 됩니다 . 우리는 ϕm 이상의 점수를 가진 모든 광부를 정직한 광부 로 간주합니다. 이 점수 는 광부가 마지막으로 성공한 검증 이후 키와 함께 검증 횟수에 따라 감가상각됩니다 . ϕm 이 감소함에 따라 채굴자 M 이 C 의 표적이 될 확률이 증가 하여 헬륨 네트워크는 지속적으로 가장 낮은 점수를 받은 채굴자가 정직하게 행동하고 있다는 것을 증명하고 채굴자들에게 점수를 향상시킬 수 있는 합리적인 기회를 제공합니다.

이 동작을 달성하기 위해 다음과 같은 불변량을 정의합니다.

M, Miner v, M
에 대한 성공적인 검증 수 - M에 대한 마지막 성공적인 검증 이후
M 높이에 대한 실패한 검증 수

시간,

모든 광부에 대한 이상적인 검증 간격이 240블록에 가깝다고 가정하면(60초 블록 시간을 가정할 경우 4시간) 점수 함수에 맞게 이러한 불변량을 조정합니다.

, v/10.0 , h/
480

위의 내용을 사용하여 이제 Miner M 의 점수를 결정하는 데 사용되는 staleness-factor, δ를 구성할 수 있습니다.

$$m = \begin{cases} -(8.h0)^{2} & v = 0 \\ .(1 - \frac{시^{02}}{(0.25, v0)}) 분 & > 0 \\ (1 - 10.v0 .h02) & < 0 \end{cases}$$

위의 조건은 다음 원칙 을 엄격히 준수합니다 .

1. 음수 v 는 광부가 지속적으로 검증에 실패하고 있음을 나타냅니다.

2. v = 0 이면 신뢰 정보가 없으므로 h에 의존 하는 감쇠에 대해 가파른 포물선 곡선을 사용합니다.
.

3. v > 0 이면 Miner가 일관되게 성공적으로 검증되었음을 의미하므로 1에서 Y 축을 가로지르는 역포물선 곡선을 사용합니다. 여기서 포물선의 너비는 최대 v 의 계수로 증가합니다. 0.25. 이는 채굴자가 더 많은 긍정적인 검증[섹션 3]을 획득할수록 점수 가 h의 요소로 더 느리게 감소 한다는 것을 의미합니다.

.

4. 마지막으로 v < 0이면 위의 경우와 반대입니다. 여기서 광부는 지속적으로 검증에 실패했습니다.
따라서 위와 유사한 포물선을 사용합니다. 그러나 포물선의 너비는 v 의 계수 로 감소하여 h의 계수로서 Miner에 대한 더 높은 점수 감소로 이어집니다. .

[그림 5]는 위의 각 기능에 대한 경향을 보여준다.

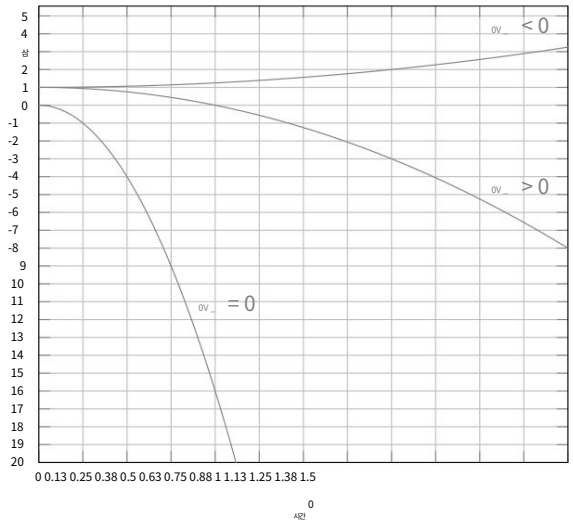

그림 5. 스코어링 기능의 추세선

위의 규칙 집합을 준수하여 기본적으로 값(0, 1) 사이에서 변동 하는 시그모이드 곡선의 변형인 다음 점수 함수 를 정의합니다.

$$\phi m = 3.16 \frac{\text{아크탄}(2.\delta m) + 1.58}{}$$

이 스코어링 함수는 [그림 6]을 생성하며, 이는 staleness-factor에 따른 스코어의 변화를 보여줍니다.

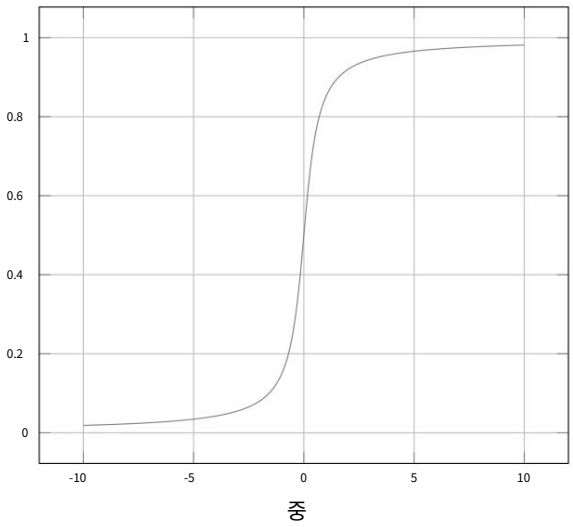

그림 6. 스코어링 알고리즘과 그에 따른 staleness factor

[그림 7]은 임의의 블록체인 높이 h에서 헬륨 네트워크의 임의 하위 집합의 스냅샷을 보여줍니다. 광부는 그림으로 표시된 점수로 임의의 위치를 나타내고 가장자리 는 Dijkstra의 알고리즘을 사용하여 계산됩니다[10].

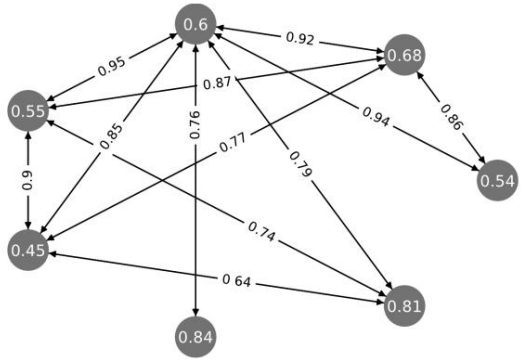

그림 7. 초기 네트워크의 임의 하위 집합의 스냅샷

10,000번의 반복 후에 [그림 8] 과 같이 헬륨 네트워크가 나타납니다 .

이 시스템의 목표는 채점 알고리즘 이 일부 광부가 부정직하게 행동할 수 있음을 고려하도록 하는 것입니다.
그러나 계산된 edge-weights(Dijkstra의 알고리즘을 통해)와 대상 선택 메커니즘 은 다른 고득점 광부 가 검증할 때만 광부의 점수를 높이 도록 보장하기 때문에 시스템이 합법적인 광부를 선호하고 억제 할 것이라고 믿습니다. 부정직한 것들.

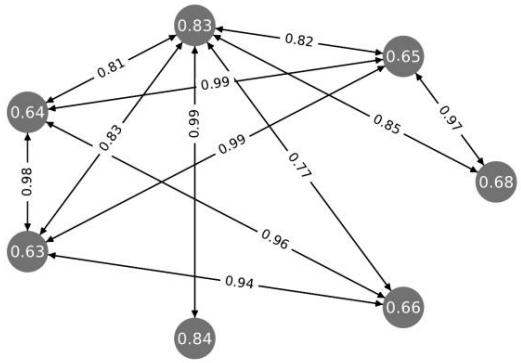

그림 8. 10000번의 반복 후 네트워크의 임의 하위 집합의 스냅샷

3.3.5 대상 선택

점수가 감소하는 방식으로 인해 해당 광부가 합리적인 간격 내에 검증되지 않을 수 있으므로 주어진 광부의 점수가 부실해질 가능성이 있습니다. 따라서 우리는 목표 선택 메커니즘을 구조화하여 채굴자들이 점수가 감소함에 따라 목표로 선택되어 점수를 높일 수 있는 통계적으로 더 큰 기회를 제공합니다. 이것은 개별 점수를 기반으로 광부가 잠재적인 목표로 선택될 확률을 편향함으로써 달성됩니다.

광부 집합을 다음과 같이 정의합니다.

$$N = \{m1, m2, m3 \ldots \text{미네소타} \mid n > 1\}$$

광부 점수 세트를 다음과 같이 정의합니다.

$$S = \{\phi m, m \in N\}$$

다음과 같은 방식으로 각 채굴자에게 목표 선택 확률을 할당합니다 .

$$P(m) = \frac{1 - \phi m}{n - X_{\text{나는=1}}^{n} \phi mi} \quad (1)$$

위의 방정식은 가장 낮은 점수를 가진 광부가 잠재적인 목표로 선택될 가장 높은 확률을 할당받는 반면 , 가장 높은 점수 를 받은 광부는 반대 임을 보장합니다.

또한 확률은 개별 Miner의 점수에 반비례한다고 주장합니다. 이를 통해 잠재적으로 점수가 낮은 광부를 성공적으로 타겟팅 하고 점수 시스템의 전반적인 균형을 개선할 수 있습니다.

위에 표시된 것처럼 확률을 할당하는 또 다른 중요한 측면은 모든 확률이 함께 이산 확률 분포를 형성한다는 것입니다. 이산 확률 분포 는 다음 방정식을 충족합니다.

$$\text{엑스}_{\text{나}} P(M = \text{나}) = 1$$

3.3.6 증명 확인

TL 이 Ks 를 전달 하거나 λ 가 경과하면 적용 범위 증명이 완료된 것으로 간주됩니다 . C 가 특별한 유형의 거래를 통해 이 증명을 제출하면 T1 ...TL 의 모든 영수증 K 가 Helium 네트워크에 게시된 거래에 포함됩니다. C 가 원래 완료한 모든 단계 는 검증 가능하고 재생성 가능한 무작위성을 지닌 본질적으로 결정적 이므로 Miner, V를 검증하는 것은 원래 단계와 증명이 합법적인지 확인하는 것이 간단합니다.

, 재창조하다

증명 트랜잭션 을 보는 합의 그룹 [섹션 6]의 광부 확인 다음 단계를 다시 생성하여 커버리지 증명을 확인할 수 있습니다.

1. 검증하는 채굴자 V , Miners N 세트를 재구성합니다 .
2. 랜덤 시드 η 는 C의 개인 키에 의해 거의 정확한 시간에 생성 된 것으로 V 에 의해 검증될 수 있습니다 .
3. V 는 N에서 T 를 선택합니다 . η 로 시딩 하면 동일한 대상이 선택 되기 때문입니다 .
4. T1 및 TL 이 결정 되는 후보 Tn 세트 가 재구성됩니다 .
5. Dijkstra의 알고리즘은 그래프 Tg를 재구성하는 데 사용됩니다.
   그리고
6. BC 에 포함 된 Ks 영수증 은
   T1..T..TL 의 개인 키로 서명 됨

이러한 단계가 성공적으로 완료되었다고 가정하면, Proof of Coverage는 C 의 점수 가 적절하게 조정 되었음을 확인 합니다.

3.4 직렬화 증명 구성

분산 클라이언트 간의 암호화 시간 합의를 달성하기 위해 Google의 Roughtime[12]을 단순화한 형태로 구현합니다. Roughtime은 특정 시간 서버에 의존 하지 않는 안전한 방식으로 대략적인 시간 동기화 를 달성하는 것을 목표로 하는 프로토콜이며, 이러한 방식 으로 시간 서버가 오작동할 경우 클라이언트는 해당 동작에 대한 암호 그래픽 증거를 얻게 됩니다.

이 섹션에서는 Proof-of- Serialization 프로토콜의 구성에 대해 설명합니다.

3.4.1 증명 생성

암호화 보안 시간 을 달성하기 위한 대략적인 프로세스 는 다음과 같습니다.

1. 먼저 Miner M 은 연락처 직렬화를 증명할 두 명의 Miner M1 과 M2를 무작위로 선택 합니다.
2. M 이 M1 과 M2에 대한 공개 키를 가지고 있다고 가정 합니다. 그렇지 않으면 M이 블록체인에서 가져와야 합니다.
3. M 은 M이 부분적으로 구성한 Proof-of-Coverage 의 SHA512 해시인 논스 R을 생성합니다 .
4. 그런 다음 M 은 증명 커널 이라고 하는 솔티드 해시 커밋 K를 생성합니다 . 여기서 K = H (R||M1||M2)입니다.
5. M은 K를 M1에게 보냅니다. M1 은 현재 시간 T1 및 K를 포함하는 서명된 메시지인 T로 응답합니다. 그리고
6. M 은 M이 생성한 nonce R이 포함되어 있기 때문에 M1 의 응답 이 미리 생성되지 않았음 을 알고 있습니다.

M 은 M1을 신뢰할 수 없기 때문에 M2 에서 다른 시간 을 요청할 것입니다.

1. 두 번째 요청의 경우, 무작위로 생성된 512비트 숫자 를 XOR하여 블라인드 처리된 T를 사용하여 512비트로 절단된 T 를 사용하여 새로운 논스 R 이 생성됩니다 .
2. M 은 그런 다음 하위 증거 커널, L = H(R||T||K)를 생성합니다. M2 로 보냅니다 .
3. M2 는 현재를 포함하는 서명된 메시지인 U로 응답합니다 .
   시간 T2 및 L; 그리고
4. U 는 이제 M 이 원하는 것을 보여주고 M1 과 M2 사이의 직렬화를 증명하는 증명 아티팩트입니다.

서버가 두 개뿐인 경우 M 은 문제가 있다는 증거로 끝날 수 있지만 정확한 시간은 알 수 없습니다. 그러나 6개 이상의 독립 서버가 있는 경우 M 은 여러 서버가 서명한 모든 서버의 오작동에 대한 증거 체인으로 끝납니다. 다른 사람, 정확한 시간 Tt 를 설정하기에 충분한 정확한 답변 .

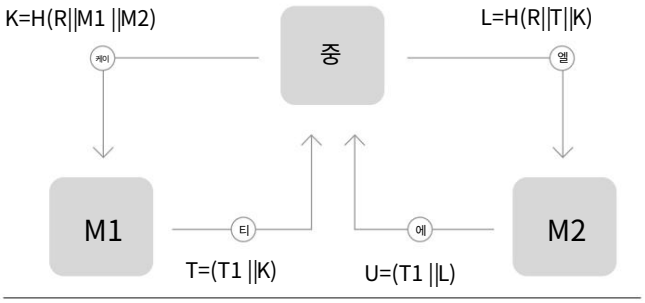

그림 9. 직렬화 증명 생성

3.4.2 증명 확인

M1 과 M2 의 시간 이 크게 다르고 M2 의 시간이 M1 이전 이라고 가정하면 M 은 오작동 의 증거를 갖습니다. M2 의 응답은 M 이 nonce 를 구성한 방식 때문에 나중에 생성되었음을 암시적으로 보여줍니다 . M2 로부터의 시간이 M1 이후 이면 M 은 M1 과 M2 의 역할을 반대로 하고 프로세스를 반복하여 시계가 일정하다고 가정할 때 다른 경우와 같이 잘못된 증명을 얻을 수 있습니다.

정확한 시간을 확인하려면 M 이 정확한 시간에 대한 합의 를 얻기 위해 충분한 광부와 시간 동기화 프로세스 를 반복 해야 합니다.

1. A 광부 M 이 다시 의사 무작위로 n 광부 를 선택합니다.
   M1...Mn;

2. M 은 솔티드 해시 커밋 K를 생성하고 전달 합니다.
   M1으로, 여기서 K = H (R||M1||M2);

3. M1 은 현재 시간 T1 및 K 를 포함하는 서명된 메시지인 T로 다시 응답합니다 .

4. M 은 sub-proof-kernel, L = H(R||T||K)를 생성 하고,
   다음 Miner Mn 에게 보냅니다 .

5. 다음 광부 는 현재 시간과 L을 포함하는 서명된 메시지인 U로 응답 합니다.

6. 이 단계 는 최소 3번의 응답 Tn 이 단조로워질 때까지 Mn 을 통해 반복됩니다 . 그리고

7. Tn 은 정확한 시간 인 Tt 로 확인할 수 있습니다 .

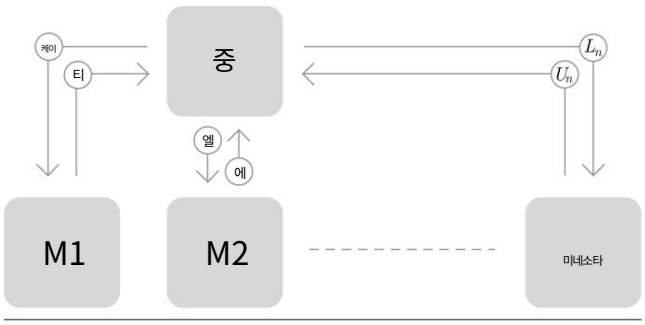

그림 10. 직렬화 증명 확인

3.4.3 검증된 시간 활용

올바른 시간 Tt 가 Proof of Serialization을 통해 결정되면 M 에서 사용되며 [2.2절]에 설명된 대로 Proof 구성 중에 포함됩니다 . O 를 계산 하여 적용 범위 증명을 얻는 데 사용되는 임의성 η은 Tt 를 포함하는 이전 블록에 연결됩니다 . 이를 통해 우리 는 이전 블록 bt 와 Tt 사이에 데이터 D 의 일부가 생성되었음을 비교적 확실하게 증명할 수 있습니다. 이 경우 D 는 적용 범위 증명입니다. 따라서 우리 는 D 가 b 와 Tt 사이에 구성되어야 함을 압니다 . 이렇게 하면 적용 범위 증명을 미리 계산할 수 없습니다.

4. 위치 증명

Proof-of-Coverage 및 Proof-of-Serialization을 사용 하여 채굴자 위치에 대한 암호화 증명 및 채굴 자 간의 암호화 시간 합의를 달성합니다. 우리는 이러한 증명을 활용하여 WHIP 호환 장치의 물리적 지리적 위치를 결정하고 장치 지리적 위치를 기반으로 하는 새로운 유형의 증거를 생성할 수 있습니다. 우리는 이것을 위치 증명이라고 부릅니다 .

4.1 동기 부여

위치 추적은 저전력 장치의 가장 가치 있는 사용 사례 중 하나입니다. 2022년까지 최소 7천만 대의 자산 추적 장치가 출하 될 것으로 예상됩니다 [14].

오늘날 GNSS(Global Navigation Satellite System)는 위치 정보 서비스가 필요한 대부분의 장치에서 사용되며 GPS가 가장 널리 사용됩니다.

GPS 시스템은 도착 시간(TOA)이라는 기술을 사용하여 지구를 도는 20개 정도의 위성과 관련하여 수신기의 위치를 결정합니다. GPS 위성 은 고정밀 온보드 시계를 사용하여 시간을 동기화하고 지상의 제어 서버와 정기적으로 동기화합니다. GPS 수신기는 머리 위의 여러 위성에서 정확하게 타임스탬프가 찍힌 데이터를 수신하고 삼각 측량이라는 기술을 사용하여 지구상의 정확한 위치를 제공합니다.

GPS는 위치 및 시간 서비스 를 모두 제공하기 위해 광범위한 애플리케이션에서 사용되는 매우 안정적인 서비스로 성숙했습니다 . 그러나 특히 헬륨 네트워크가 용이하도록 설계된 저전력 장치 영역에서 GPS 에는 상당한 단점이 있습니다. GPS 수신기가 충분한 위성으로 잠금을 달성하는 데 약 2분이 소요될 수 있으며 , 이는 배터리 수명을 크게 단축시키는 것으로 해석됩니다.

예를 들어, 하루에 25번 정도 자신의 위치를 전송하는 장치는 GPS 없이 같은 배터리로 몇 년 동안 수명을 유지하는 것에 비해 AA 배터리로 한 달만 사용할 수 있습니다. GPS 수신기는 일반적으로 정확한 위치 를 계산하는 데 필요한 3-4개의 위성을 보기 위해 하늘 과의 가시선이 필요하기 때문에 실내에서 GPS를 사용하는 것은 일반적으로 불가능합니다 . GPS 데이터는 암호화되지 않은 상태로 전달되기 때문에 시스템이 스푸핑, 전파 방해 및 기타 공격 벡터에 매우 취약합니다 .

우리는 변경할 수 없는 분산 원장과 함께 위치 및 시간을 확인하는 데 사용할 수 있는 위치 서비스의 저전력 구현에 관심이 있습니다. 위의 요소를 감안할 때 GPS는 이러한 요구 사항에 대해 수용할 수 없는 메커니즘이라는 결론을 내립니다.

4.2 위치 증명 구성

우리의 목표는 GNSS 하드웨어를 사용하지 않고 주어진 장치 D의 물리적 지리적 위치를 확인하는 것입니다 . 이를 위해 [섹션 3]에 설명된 Proof-of-Coverage 및 Proof of Serialization 프로토콜을 사용하여 주어진 Miner, M 의 물리적 지리적 위치 및 암호화 시간 합의 를 이미 결정하고 입증했다는 사실에 의존합니다 .

4.2.1 RF 데이터의 정확한 타임스탬프

RSSI(Received Signal Strength Indication), ToA(Time of Arrival), TDoA(Time Differential of Arrival) 등 GNSS를 사용하지 않고 포지셔닝 시스템에서 사용하는 몇 가지 기술이 있습니다. 이러한 기술은

일반적으로 하나 이상의 수신기에 의해 수신되는 무선 주파수 전송 은 해당 전송의 특성을 기반으로 하는 다양한 알고리즘과 결합됩니다 .

결론은 TDoA가 가장 정확하지만 구현하기 어려운 기술이라는 것입니다 [15], [16], [17], [18]. TDoA 는 간단히 말해서 송신기와 여러 수신기 간에 정확하게 동기화되고 기록된 타이밍 정보 간의 차이에 의존합니다 . 따라서 장치가 방출하는 RF 패킷을 정확하게 타임스탬프 하고 헬륨 네트워크에서 채굴자의 시계를 동기화하는 것이 중요합니다.

타임스탬프 흐름의 예는 다음과 같습니다.

1. 장치 D는 임의의 내용을 포함 하는 패킷 P 를 브로드캐스트합니다. 헬륨 네트워크를 통한 데이터
2. 여러 광부 Mn이 P를 듣고 P 의 수신 시간에 대한 타임스탬프 Tn 을 기록합니다.
3. Tn 은 GNSS를 통해 수신된 나노초 시간을 기반으로 생성 되고 Hotspot 무선 프론트엔드에서 수신한 원시 무선 샘플 데이터를 사용하여 스탬프 처리됩니다 .
4. P 와 Tn 을 포함하는 서명된 트랜잭션 은 Mn 에 의해 D에 속한 라우터 R 로 전달됩니다 . 그리고
5. R 은 이제 P 의 사본을 여러 개 받았습니다. Tn 값이 약간 다릅니다.

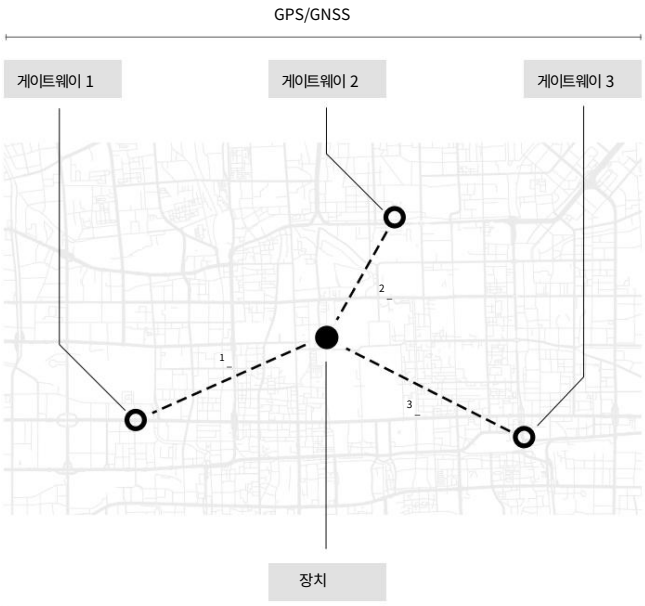

그림 11. TDoA를 통한 지리적 위치

일반적으로 타임스탬프의 나노초 수준 변동으로 인해 결과 위치 솔루션에 상당한 변동이 발생할 수 있으므로 이러한 타임스탬프 를 정확하게 기록하는 것은 어렵습니다 . 이러한 수준의 정밀도를 달성하려면 Miner의 무선 하드웨어에서 매우 높은 대역폭의 원시 동위상 및 직교 (I/Q) 데이터를 사용해야 하며 충분히 빠른 프로세서가 이 데이터를 샘플링하고 적절한 패킷을 식별하며 타임스탬프를 기록합니다. 일반적으로 FPGA(Field Programmable Gate Array)는 이러한 유형의 프로세서가 결정적인 방식으로 데이터를 처리할 수 있기 때문에 이 데이터의 프로세서로 사용됩니다. 그러나 FPGA는 상당히 비싸고 전력 소모가 많으며 상당한 열을 방출합니다. 대신, 우리의 핫스팟 마이닝 하드웨어는 I/Q 데이터를 처리하고 이 정밀도 수준에서 타임스탬프를 달성하기 위해 상용 저가 구성 요소를 사용하는 새로운 기술을 사용 합니다. 비교 예로서, 기존의 저가 LoRaWAN[23] 액세스 포인트는 몇 밀리초의 정확도 내에서만 정확한 타임스탬프 데이터를 제공 할 수 있습니다. 전파는 빛의 속도로 이동하기 때문에 각 밀리초 는 정확한 지리적 위치 에 대해 실질적으로 쓸모없는 것으로 간주되는 물리적 거리 . Hotspot에서 사용되는 기술, 구성 요소 및 회로도에 대한 추가 정보 는 Helium 네트워크 출시와 함께 오픈 소스 소프트웨어로 공개될 예정입니다 .

4.2.2 타임스탬프를 사용하여 위치 도출

이제 장치 라우터 R은 정확한 타임스탬프 Tn 을 포함하는 다양한 서명된 메시지를 소유하고 있으므로 장치 D 의 위치를 해결할 수 있습니다 .

[20], [21], [19], [22]와 같은 다양한 TDoA 알고리즘이 존재합니다 . 주어진 패킷에 대해 충분한 밀도의 Mn , 따라서 Tn 이 기록된다면, D 의 위치 는 다양한 요인에 따라 몇 미터까지 유도될 수 있다 . TDoA 알고리즘에 대한 자세한 내용 은 이 백서의 범위를 벗어나 므로 관심 있는 독자가 인용된 논문을 읽는 것이 좋습니다 .

4.2.3 위치 증명 확인

R 이 D 의 위치를 계산 하면 보고된 D의 위치 가 주어진 시간에 정확한지 확인하는 것이 필요할 수 있습니다. 위치 증명은 결정적이며 블록체인에서 공개적으로 사용할 수 있는 정보에서 파생 되므로 관련된 모든 단계를 재구성할 수 있습니다 .

- 타임스탬프 패킷 Tn에 포함된 서명에서 타임스탬프 제공에 관련된 모든 광부를 확인할 수 있습니다.
- assert_location [섹션 5.3.3] 트랜잭션 을 검사하여 해당 광부의 청구된 GPS 위치를 결정할 수 있습니다. 그리고
- 각 항목에 대한 범위 증명 및 점수 [섹션 3]
  채굴자는 블록체인에서 검색하고 검사할 수 있습니다.

위의 단계를 감사함으로써 라우터 운영자는 주어진 장치 D에 대한 위치 증명을 위한 구성 요소를 제공하는 것과 관련된 각 광부의 위치를 암호화 방식으로 증명(또는 반증)할 수 있습니다.

증명의 정확성은 관련된 Mn 의 수 와 따라서 수신 된 Tn 의 수 에 크게 의존합니다 . 반사 및 다중 경로와 같은 추가 RF 요인 은 위치 계산의 정확도에 상당한 영향을 미칠 수 있습니다.

5. 거래

Helium 네트워크의 트랜잭션은 기존의 많은 블록체인 네트워크와 유사하게 프로토콜 토큰의 주소 대 주소 전송을 가능하게 하는 기능을 제공하지만 DWN 작동에 중요한 핵심 기능을 가능하게 하는 기본 세트도 제공합니다 . 우리는 먼저 소액 거래에 대한 헬륨의 필요성 을 해결하고 새로운 솔루션을 제안할 것입니다.

5.1 소액 거래에 대한 헬륨 네트워크의 필요성

장치는 패킷당 지불 Helium 네트워크의 목표는 현재 이러한 유형의 서비스에 사용할 수 있는 것보다 훨씬 저렴한 인터넷 데이터 전송 요금(장치가 채굴자에게 지불하는 요금)을 제공하는 것입니다. 이 전송 요금은 최대한의 유연성을 허용하기 위해 패킷별로 측정되어야 합니다. 이러한 방식으로 장치 는 이전 에 해당 광부와 관계를 설정하지 않고 단일 패킷 을 보내거나 받기 위해 모든 광부와 거래할 수 있습니다 .

모든 트랜잭션은 온체인에서 발생 합니다. Helium 네트워크는 모든 트랜잭션이 온체인에서 발생해야 한다는 철학에 기반을 두고 있습니다 . 즉, Helium 네트워크 에서 발생하는 모든 트랜잭션이 블록체인에 저장되어야 하는 빈도로 블록의 크기를 조정하고 마이닝 해야 합니다.

이 목표를 달성하기 위해서는 마이닝 비용이 낮아야 하고, 많은 수의 트랜잭션을 캡슐화할 수 있을 만큼 블록이 커야 하며, 트랜잭션이 빠르게 처리될 수 있을 만큼 블록이 자주 생성되어야 합니다 .

장치가 블록체인에 데이터를 유지하도록 허용 Helium 네트워크는 특정 용도인 DWN을 서비스하기 때문에 블록은 트랜잭션과 함께 장치에서 보낸 데이터의 지문을 추가로 저장할 수 있어야 하며 , 이 경우 전송 서비스에 대해 광부가 지불합니다. 우리는 이 전체적인 변조 방지 데이터 추적이 센서 데이터의 신뢰성과 진실성이 중요한 완전히 새로운 사용 사례를 가능하게 할 것이라고 믿습니다 .

5.2 기존 솔루션의 한계

이제 Helium 네트워크 내 트랜잭션 요구 사항에 대해 논의 했으므로 블록체인의 소액 결제에 대한 기존 솔루션을 간략하게 설명하고 Helium 네트워크에 적용할 때의 단점을 해결합니다.

중량 거래 이 첫 번째 옵션은 지불보다 서비스 수수료가 적기 때문에 대규모 거래에만 적합합니다 . 이 방법은 거래 수수료를 지불하는 사람이 종료되기 때문에 매우 작은 거래에는 잘 작동하지 않습니다 .

잠재적 으로 교환되는 가치 보다 거래 수수료에 대해 더 많은 비용을 지불합니다 . 이것은 오늘날 신용 카드를 사용하여 소액 품목 을 사는 것과 유사한 문제 입니다. 판매자 는 각 신용 카드 거래에 대해 최소 수수료를 지불하고 일정 금액 이하에서는 거래에 대해 손실을 입습니다.

이러한 대규모 거래는 분명히 헬륨 네트워크 내에서 소액 거래 시스템으로 사용하기에 적합하지 않습니다 .

수수료 제로 거래 장치 관점에서 매우 바람직하지만 진정한 제로 수수료 블록체인은 스팸 거래로 가득 차 있습니다. 블록체인의 공간을 낭비하고 네트워크의 혼잡을 증가시키기 위한 트랜잭션으로 블록체인을 오염시키는 스크립트를 작성하는 것은 간단 합니다. 표면적으로 수수료가 없는 일부 블록체인 구현은 처리 작업과 트랜잭션 확인 작업을 거래자 자신에게 전가하는 것과 같은 영리한 방식으로 이 문제를 해결합니다. 그러나 이러한 구현에는 자체 문제가 있습니다. 예를 들어 IOTA[24]는 중앙 조정자 없이 이러한 유형의 시스템을 운영할 수 있다는 것을 아직 입증 하지 못했습니다.

상태 채널 상태 채널[31]을 통해 두 당사자는 일반적으로 매우 제한된 위험으로 한 번에 작은 증분으로 가치를 교환할 수 있습니다. 한 당사자가 다른 당사자가 부정직하게 행동하고 있다고 생각하면 상태 채널의 최종 트랜잭션을 블록체인에 게시하고 채널을 닫을 수 있습니다.

일반적으로 최대 한 번의 지불이 위험합니다. 그러나 몇 가지 단점이 있습니다. 지불 인은 국가 채널의 수명 동안 상당한 자금을 잠가야 합니다. 즉, 다른 당사자와 국가 채널을 개설 하거나 다른 회비를 지불하지 못할 수 있습니다. 상태 채널의 트랜잭션은 메인 체인에 전혀 나타나지 않습니다. 그리고 이러한 구현 은 비교적 복잡하여 잘 실행됩니다(Lightning [29]나 Raiden [30] 모두 아직 널리 사용 되지는 않았습니다).

후불 지불 서비스가 제공된 후 후불 지불은 분산된 의사 익명 시스템에서 매우 위험한 방법입니다. 거래하는 법인 의 의도나 정직성에 대한 확신을 얻을 수 있는 메커니즘 이 없으며 부채 만기가 도래했을 때 해당 법인 이 필요한 자금을 통제하는지 여부도 알 수 없습니다. 이 모델은 관련된 당사자들이 서로를 신뢰 하거나 자금 회수를 위한 다른 수단이 있는 경우에만 작동합니다.

5.3 헬륨의 수수료 유형

이 섹션에서는 헬륨 네트워크에 필요한 수수료 유형을 설명 하고 헬륨 합의 프로토콜 [섹션 6] 의 고유한 특성을 활용하는 솔루션을 제안합니다 .

5.3.1 운송비

Helium 네트워크를 사용하여 인터넷과 데이터를 주고받는 장치 는 광부에게 전송 요금 으로 알려진 금액을 지불해야 합니다 . 이 수수료 는 인터넷에서 장치와 의도된 라우터 사이에 데이터 패킷 을 전달하는 채굴자에 대한 보상 이며 , 블록체인 에 기록되는 블록의 일부로 채굴 거래에 대해 채굴자가 얻는 거래 수수료와 관련이 없습니다. 장치가 블록체인에 직접 연결되어 있지 않기 때문에 장치가 속한 라우터와 채굴자 간에 요금이 협상됩니다 .

광부 는 바이트 단위로 인터넷과 데이터를 주고받는 데 기꺼이 수락할 가격을 설정합니다 .

장치 라우터는 데이터를 송수신할 때 마이너에게 전송 요금을 지불합니다 . 즉, 채굴자는 거래가 블록에서 채굴 되어 블록체인에 기록 되기 전에 운송비를 받습니다 . 이것은 채굴자가 블록체인에서 확인 되기 전에 운송 지불이 악의적이거나 사기가 아니라고 믿어야 하기 때문에 약간의 위험을 수반합니다 . 그러나 바이트당 전송량이 얼마나 낮을지 감안할 때 이 위험은 견딜 수 있을 것 같습니다. 광부는 시스템을 지속적으로 남용하는 경우 장치 또는 조직 주소를 블랙리스트에 올릴 수 있습니다.

운송 수수료 프로세스의 예는 다음과 같습니다.

1. 광부 M은 장치 D가 브로드캐스트하는 패킷 P를 듣습니다.
2. M 은 P에 첨부된 D 의 주소 를 사용하여 라우터 R은 D의 소유자입니다.
3. M 은 P 의 서명 K(P) 와 R로의 전송을 위한 n개의 토큰 제안을 보냅니다.
4. R 은 K(P) 및 지불 제안을 수신하고 제안된 가격에 대한 패킷 수락 여부를 결정합니다.
5. R 이 제안된 가격으로 패킷을 수락 한다고 가정 하고 M 에게 지불해야 하는 n 값 의 트랜잭션 T 를 구성 하고 이를 채굴자 에게 보냅니다. 그리고
6. M 이 회신에서 트랜잭션을 확인하면 P를 R에 전달 하고 T 를 Helium 네트워크 에 포함하기 위해 합의 그룹에 제출 합니다.

5.3.2 거래 수수료

거래 수수료는 대부분의 블록체인 구현 에서 필수적인 부분입니다 . 그들은 채굴 자가 초안 블록에 트랜잭션 을 포함하도록 장려 하고 스팸 트랜잭션 이 Helium 네트워크를 오염시키지 않도록 합니다.

새로운 거래에 대한 적절한 수수료를 결정하기 위해 거래자는 약간의 오차 범위 내 에서 과거 δ 패킷 전송 수수료의 중앙값을 취합니다. Helium 네트워크에서 δ 패킷 전송 이 발생할 때까지 요금은 일정한 값 α로 고정됩니다. 거래 수수료를 헬륨 운송에 대해 부과되는 현재 수수료에 고정함으로써 네트워크, 우리는 그것들을 현실에 뿌리내립니다. Helium 네트워크의 주요 목적은 무선 인터넷 범위의 네트워크를 용이하게 하는 것입니다. 장기적으로 이를 달성하려면 시스템의 모든 경제성이 기본 사용자가 헬륨 네트워크에서 거래하는 것이 실용적이도록 조정되어야 합니다. 한 세트의 수수료가 다른 세트를 능가한다면 Helium 네트워크는 주요 사용자 세그먼트 에 대한 유용성을 빠르게 잃게 됩니다 .

광부 및 기타 라이트 클라이언트가 적절한 수수료를 결정할 수 있도록 전체 노드[섹션 5.5]는 수수료 제안 API를 노출합니다. 이러한 방식으로 블록체인의 완전한 사본을 유지하지 않는 리소스 제약이 있는 엔터티 는 가장 최근 거래에서 수수료를 계산할 필요가 없습니다.

블록 제출 프로세스 동안 합의 그룹[섹션 6]의 채굴자들은 블록의 정확성을 확인하고 수수료가 허용 가능한 임계값 δ를 초과하지 않았는지 확인합니다.

Helium Consensus Protocol[섹션 6]에 내장된 검열 복원력으로 인해 더 큰 거래 수수료를 포함할 인센티브가 없습니다. 채굴자가 블록 에 포함하기 위해 멤풀에서 가장 큰 수수료가 있는 거래를 체리픽하는 비트코인과 달리 헬륨 채굴 자는 합의 그룹의 다른 구성원과 협력하여 암호를 해독하지 않고는 거래 내용을 볼 수 없습니다 . 수수료가 너무 높거나 낮은 거래 는 블록이 블록체인에 추가되기 전에 거부됩니다.

5.3.3 스테이킹 수수료

아래 [섹션 5.4]에 언급된 주장 위치 트랜잭션에는 특별한 유형의 수수료 계산인 동적 수수료가 있습니다.
Helium 네트워크는 핫스팟의 특정 밀도에서 최대 유용성에 도달하기 때문에 수수료가 Helium 네트워크 밀도가 가능한 한 이상적인 밀도에 가까워지도록 장려하기를 원합니다. 이를 위해 위치 주장에 대한 거래 수수료는 다음 공식 을 사용하는 곡선의 y 좌표로 생각할 수 있습니다 .

$$y = (x \quad D)^{4} + \text{에프}$$

여기서 D 는 이상적인 핫스팟 밀도이고 F 는 위치 거래에 대한 단위 요금입니다. D = 3 및 F = 1 인 이 함수의 샘플 그래프는 다음과 같습니다.

알 수 있듯이 이상적인 네트워크 밀도 근처의 핫스팟은 추가 비용이 저렴하지만 새 네트워크를 설정하거나 네트워크를 과도하게 채우는 것은 매우 빠르게 비용이 듭니다. 이는 네트워크에 도움이 되지 않는 핫스팟 배포에 대한 인센티브를 제거하는 역할을 합니다. 특히 Alternate Reality Attacks 및 Miner로 가득 찬 창고는 엄청나게 비쌉니다.

위치를 주장하지 않아 스테이킹 비용을 지불하지 않은 광부 는 합의 그룹[섹션 6]에 포함되는 것으로 간주되지 않습니다.

물리적 위치를 이동하는 광부는 새 위치를 주장하고 새 스테이킹 비용을 지불해야 합니다.

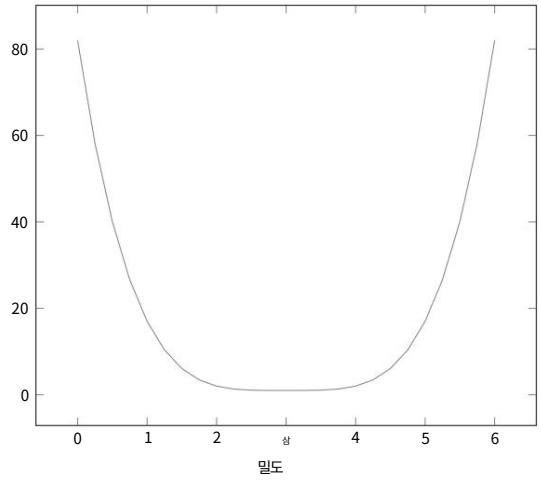

그림 12. 스테이킹 수수료와 채굴자 밀도

5.4 헬륨 네트워크의 기본 요소

거래 시스템의 철학에 대해 논의한 후
소액 거래를 촉진하기 위한 우리의 접근 방식을 제시했습니다.
Helium 네트워크에서 이제 트랜잭션을 설명합니다.
프리미티브와 그 속성.

핫스팟 추가 Helium 네트워크에 새로운 핫스팟을 등록하고 해당 지분
(채굴에 필요) 공급 을 담당할 기존 계정에 추가합니다.

채굴 보상[섹션 6] 및 수수료를 받습니다.
핫스팟

특성	설명
핫스팟 주소	핫스팟 의 공개 키 주소
	네트워크에 추가 중
소유자 주소	서명 소유자 계정의 주소
	소유자의 상호 서명 및
	핫스팟

assert·location 다음 형식으로 핫스팟의 위치를 주장합니다.
동적 지분이 필요한 지리적 좌표

특성	설명
핫스팟 주소	자신의 위치를 주장하는 주소
목하	단조 증가하는 정수
위도 경도	핫스팟의 위도
고도 서명	핫스팟의 경도
	핫스팟의 고도
	핫스팟의 서명

지불 인 한 계정에서 토큰을 다음으로 이동합니다.
필요한 수수료를 포함한 다른 계정, 수취인.

특성	설명
지불인	주소 발신인의 주소
수취인	주소 수취인의 주소
목하	단조 증가하는 정수
값	정수 기반 표현
	보낼 토큰
서명	보낸 사람의 서명

5.5 라이트 클라이언트와 풀 노드

지금까지 소액 거래를 비용 효율적으로 처리하는 방법에 대해 논의했지
만 아직
블록체인의 크기가 지속적으로 증가하는 불가피한 상황에 대처
하는 방법을 다루었습니다. 에 대한 한 가지 요구 사항
헬륨 네트워크는 모든 거래가 온체인에서 발생한다는 것입니다. 이것
전체 블록체인의 크기가 결국에는 커질 것임을 의미합니다.
꽤 크다. 이것은 모든 광부가
Helium 네트워크는 핫스팟 장치이며 상대적으로 제한적입니다.
연산 능력과 저장 공간.

마이닝 노드가 작동하도록 하여 이 제약을 해결합니다.
블록체인의 라이트 클라이언트로서 오래된 블록을 잘라내고
필요에 따라 거래하고 최신 원장만 유지
가치. P2P 네트워크를 통해 통신합니다.
전체 히스토리를 유지하는 풀 노드로
거래를 확인하는 블록체인.

이것은 다음과 같은 질문을 제기합니다.
노드, 그리고 그렇게 하는 동기는 무엇입니까? 라우터는
확장 가능한 클라우드 기반 스토리지에 액세스할 수 있는 소프트웨어 전
용 애플리케이션으로
목적을 달성하기 위해. 우리는 호스트된 세트를 운영할 것입니다
개발자가 자체 라우터를 배포할 필요 없이 제품 을 쉽게 출시할 수 있도
록 해주는 라우터입니다. 하지만,
유지 관리해야 하는 많은 엔터프라이즈 개발자
더 높은 수준의 개인 정보 보호를 위해 자신의 라우터를 호스팅하려고 합니다.
함께 이러한 라우터는 리소스가 제한된 핫스팟 및 지갑을 지원할 수
있는 전체 노드 네트워크를 형성합니다.
가벼운 클라이언트를 운영하고 있습니다.

6. 헬륨 합의 프로토콜

계산적으로 매우 비싸고 전력이 많이 소모되는 대신
배고픈 작업 증명, 광부가 커버리지 증명을 생성합니다.
[섹션 3]. 이 섹션에서는 이러한 유용한 증명이 어떻게
무허가 네트워크 합의를 생성하는 데 사용할 수 있습니다.

6.1 동기

많은 현재 세대 블록체인은 계산 동맹이 어려운 작업 증명 에 의존 하여
헬륨 네트워크를 보호합니다.
Nakamoto Consensus라고도 알려진 Sybil 공격에 대항합니다.
작업 증명이 계산적으로 비싸다는 사실
생성하지만 검증하는 데 비용이 적게 든다는 것은 제안하기 위해

Helium 네트워크에 대한 새로운 유효 블록 에는 상당한 양의 계산이 소비되었다는 증거 가 있습니다.
현대 기술의 하드웨어 비용, 전력 비용, 물리적 공간 및 계산 효율성에 의해 계산이 제한된다는 사실 때문에 Sybil 공격은 불가능합니다. 그러나 이 접근 방식은 블록체인 기술의 주류 채택에 기본적이지만 몇 가지 단점이 있습니다 .

가장 큰 단점은 전력 소비입니다. 비트코인 네트워크는 많은 소규모 국가보다 더 많은 전력을 소비하는 것으로 추정 됩니다. 비트코인의 작업증명(Proof-of-Work)은 너무 낭비적이어서 현재 세계에서 가장 많이 사용되는 전력 목록에 있으며 비트코인의 가치가 올라갈 때마다 채굴에 투입되는 자원도 함께 증가합니다.

전력 문제와 관련하여 마이닝 풀 문제가 있습니다.
많은 블록체인에는 사용자가 뭉쳐서 단일 블록을 동시에 채굴하고 풀의 주소를 지불받을 당사자로 나열하는 마이닝 풀이 있습니다. 그런 다음 풀 은 풀의 구성원과 블록 보상 을 공유 합니다. 이것은 비트코인과 이더리움이 각각 10개 미만의 마이닝 풀 에 의해 지배되기 때문에 분산화의 많은 이점을 무효화하게 됩니다 . 이러한 대규모 풀은 독립적인 당사자가 자체적으로 블록을 채굴하는 것을 효과적으로 방지합니다.

이는 이러한 블록체인에 대한 합의 프로토콜이 매우 적은 수의 마이닝 풀에 의해 효과적으로 제어되고 더 중앙 집중화될 위험이 있음을 의미합니다.

최근에는 블록체인 합의 프로토콜을 덜 낭비하고 네트워크에 더 유용하게 만드는 추진력이 증가했습니다. Filecoin[25]에는 시공간 증명이 있고 이더리움[5]은 지분 증명[26] 접근 방식으로 이동하고 있습니다.

Helium 네트워크 의 경우 다음 속성을 가진 합의 프로토콜이 필요합니다.

무허가 노드는 합의 규칙에 따라 작동하는 한 다른 주체의 허가 나 승인 없이 헬륨 네트워크에 자유롭게 참여할 수 있어야 합니다.

본질적으로 극도로 분산된 네트워크 합의는 특정 지역에서 전기에 대한 더 저렴한 액세스와 같은 거시 경제적 요인을 활용하는 데 사용할 수 있는 인센티브가 없고 동일한 위치에서 단순히 더 많은 하드웨어를 구입하는 것이 비효율적이거나 비용이 많이 들도록 설계되어야 합니다. 금지. 또한 마이닝 풀이 형성되고 그룹이 마이닝 블록에서 협력하는 것이 불가능해야 합니다 .

비잔틴 장애 허용 프로토콜은 행위자의 임계값이 정직하게 행동하는 한 합의에 도달할 수 있도록 비잔틴 장애[27]에 대해 내성이 있어야 합니다 .

유용한 작업 기반 네트워크 합의 달성 은 네트워크에서 유용하고 재사용할 수 있어야 합니다. Nakamoto Consensus 기반 시스템 에서 수행된 작업 은 채굴 중인 특정 블록은 네트워크에서 유용 하거나 재사용할 수 없습니다. 이상적인 합의 시스템 은 단순히 블록체인을 보호하는 것 이상 으로 네트워크에 유용하고 재사용 가능한 작업을 포함합니다 .

높은 확인된 거래율 우리의 이상적인 합의 프로토콜은 초당 매우 많은 수의 거래를 처리할 수 있으며, 한 블록에서 거래가 확인되면 확인된 것으로 간주됩니다. 기존의 많은 블록체인은 긴 결제 시간이 필요하지만 네트워크는 합의를 달성하는데 이는 헬륨 네트워크와 같은 시스템에서 이상적이지 않습니다. 이 시스템은 매우 많은 수의 트랜잭션을 경험할 수 있고 트랜잭션이 결제 되기를 기다리는 것이 견디기 힘든 곳 입니다.

거래는 검열에 강합니다 . 이상적으로는 채굴자가 검열을 하거나 채굴하기 전에 거래를 선택하고 선택할 수 없습니다. 이는 거래를 악의적으로 검열하려는 모든 시도를 무효화 할 뿐만 아니라 그렇지 않으면 매력적이지 않은 거래(예: 고정 수수료 거래)가 블록체인에 포함될 수 있습니다.

이 섹션의 나머지 부분에서는 헬륨 합의 프로토콜이라고 하는 이러한 설계 목표를 염두에 두고 합의 프로토콜을 구성하는 방법을 설명합니다.

6.2 헬륨 합의 프로토콜

우리 는 HBFT(HoneyBadgerBFT)[4] 비동기식 비잔틴 내결함성 프로토콜 의 변형 과 결합하여 작업 증명을 대체 하는 헬륨 네트워크를 검증하는 유용한 작업을 캡처하기 위해 커버리지 증명과 관련된 고유한 합의 프로토콜을 제안 합니다.

6.2.1 HBFT

HBFT는 최적의 점근적 효율성을 달성 하도록 설계된 비동기식 원자 브로드캐스트 프로토콜 로 2016년에 처음 제시되었습니다. HBFT에서 설정은 고유한 잘 알려진 ID (P0 ~ P N-1) 를 가진 N 개의 지정된 노드 네트워크를 가정합니다. 우리의 HCP 인스턴스화에서 이 노드 네트워크는 합의 그룹 C 로 알려져 있습니다 . 합의 그룹은 트랜잭션을 입력으로 수신하고, 그 목표는 이러한 트랜잭션의 순서에 대한 공통 합의에 도달 하고 블록체인에 추가할 블록으로 구성하는 것입니다. .

프로토콜은 라운드로 진행되며 각 라운드 후에 새로운 트랜잭션 배치가 블록체인에 추가됩니다. 각 라운드가 시작될 때 그룹은 버퍼에 있는 트랜잭션의 하위 집합을 선택 하고 무작위 합의 프로토콜의 인스턴스에 대한 입력으로 제공합니다. 합의 프로토콜 이 끝나면 이 라운드의 최종 거래 세트 가 선택됩니다.

HBFT는 공유된 공개 키를 사용하여 트랜잭션을 암호화해야 하는 임계값 암호화 방식[28]에 의존하므로 합의 그룹이 다음을 위해 함께 작업해야 합니다.

그것을 해독하십시오. 이는 개별 노드가 그룹의 대다수와 공모하지 않고 특정 트랜잭션을 해독하거나 검열 할 수 없음을 의미합니다.

6.2.2 HBFT에 적용 증명 적용

Helium 네트워크에서 채굴자는 epoch, Δp 에 Helium 네트워크에 커버리지 증명을 제출해야 합니다 . 이러한 증명은 특별한 유형의 트랜잭션으로 제출되고 이후에 블록체인에 기록됩니다. [섹션 3] 에 설명된 대로 채굴자 들은 헬륨 네트워크에 유효한 증명을 제출할 때 점수를 높 입니다. epoch, Δc 에서 가장 높은 점수를 받은 Miner N이 새로운 HBFT 합의 그룹 C 로 선출됩니다.

Proof-of-Coverage를 사용하여 C 의 구성원을 선택함으로써 우리는 본질적으로 HBFT 프로토콜 에서 잘 알려진 ID를 대체 합니다. 우리는 무허가 네트워크를 원하기 때문에 광부가 정직하게 행동하는지 여부를 확인 하고 HBFT 합의 그룹에 선출함으로써 주어진 시대에 가장 정직한 광부를 보상 하기 위해 커버리지 증명을 사용할 수 있습니다.

6.2.3 합의 그룹

Δc 동안 현재 선출된 합의 그룹은 블록을 생성하고 블록체인에 추가하는 책임이 있습니다.
Helium 네트워크의 모든 새로운 거래 는 현재 합의 그룹 구성원에게 제출됩니다. 고정된 간격 Δb 로 C 에 의해 새로운 블록 이 생성되어 블록체인 에 기록됩니다 . 토큰 블록 보상은 유효한 거래에 포함된 모든 수수료의 합계와 함께 제출된 모든 블록에 대해 C 의 구성원 에게 분할 됩니다. Δb 동안 트랜잭션이 없는 특이한 경우 에는 빈 블록이 블록체인에 추가됩니다.

6.2.4 채굴 과정

주어진 Δc 에포크에 대해 합의 그룹 C 가 선택되면 임계값 암호화 키 TPKE 를 부트스트랩하기 위해 분산 키 생성 단계가 발생합니다 . TPKE 는 모든 당사자가 마스터 공개 키 PK에 대한 트랜잭션을 암호화할 수 있도록 하는 암호화 프리미티브 입니다. 따라서 C 는 이를 해독하기 위해 함께 작업해야 합니다 . f + 11 C 의 올바른 구성원이 암호 해독 공유 σi 를 계산하고 공개 하면 트랜잭션을 복구할 수 있습니다.
TPKE.Setup 기능 을 통해 PK 가 생성 되면 PK 가 포함 된 블록 이 즉시 블록체인에 제출됩니다.
C 의 각 구성원 Nm 은 PK 의 비밀 키 공유 SKi 를 받습니다.

Helium 네트워크의 채굴자들은 새로운 트랜잭션 t 를 C에 제출합니다. C 의 각 구성원은 대기열에 있는 첫 번째 B 트랜잭션 의 임의 하위 집합을 선택하고 TPKE.Enc(PK, t) → e 함수를 적용하고 이를 다른 구성원에게 제출합니다. C. C 의 구성원이 최소한 N - fe 를 받으면

[1] f 는 허용 가능한 비잔틴 결함의 수와 동일한 프로토콜 매개변수입니다.

TPKE.DecShare(SKi , e) → σi 함수를 실행하여 암호 해독 공유를 생성합니다 . 구성원은 자신의 σi 를 C 의 다른 구성원 에게 브로드캐스트 하고 f + 1 구성원이 σi 공유를 본 후에는 PK, e 및 σi 공유를 사용하여 TPKE.Dec 기능 으로 진행할 수 있고 트랜잭션 암호 해독을 시도할 수 있습니다.
C 의 각 구성원은 복호화된 트랜잭션을 로컬 버퍼에 보관된 다음 블록의 자체 인스턴스화에 추가 합니다. 이중 지출 및 기타 잘못된 거래는 이 단계에서 이러한 블록에서 제거됩니다.

그룹의 구성원은 자체적으로 e 를 해독할 수 없으므로 지정된 구성원은 트랜잭션이 수신될 때 C 의 f + 1 구성원이 공모 하지 않고 후보 블록에 포함 되기 전에 트랜잭션을 검열할 수 없습니다. 트랜잭션 대기열 의 첫 번째 B 에 t 가 있는 정직한 C 구성원은 C 의 다른 구성원 이 동의 할 때까지 트랜잭션을 해독할 수 없으므로 결국 블록에 t 를 포함할 수 있습니다. 검열합니다. Δc 시대에 대한 C 의 구성원 은 제출된 커버리지 증명을 기반으로 선택 되어 구성원을 예측할 수 없게 하므로 이러한 유형의 담합은 실행하기가 매우 어려울 것입니다.

f + 1 노드가 블록에 대한 트랜잭션에 동의하면 블록 에 대해 TPKE 임계값 서명을 얻습니다.
이것은 비잔틴 장애 임계값을 초과하는 충분한 노드가 블록에 동의했음을 인증합니다. 블록의 내용을 검열하거나 동의하지 않는 C 의 구성원은 서명 임계값 계산에 사용할 수 없는 호환되지 않는 서명 공유를 생성합니다 . 그런 다음 이 블록은 헬륨 네트워크를 통해 모든 광부에게 가십을 주고 블록체인에 추가됩니다.

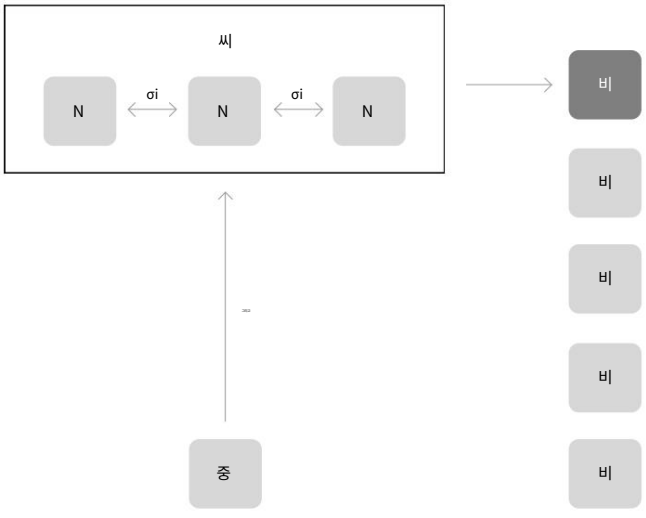

그림 13. 컨센서스 그룹 및 마이닝

6.2.5 결론

우리는 현대적이고 비동기적이며 효율적인 비잔틴 결함 허용 합의 프로토콜과 허가된 ID를 유용하고 효율적인 것으로 대체하기 위한 새로운 메커니즘을 결합한 헬륨 합의 프로토콜을 제시했습니다.

재사용 가능한 적용 범위 증명. 결과 프로토콜 은 유용한 작업을 기반으로 하는 무허가 , 분산화 , 비잔틴 내결함성 및 매우 높은 속도의 검열 증명 트랜잭션 메커니즘의 설계 요구 사항을 충족합니다.

HoneyBadgerBFT 프로토콜에 대한 자세한 분석 및 분석을 위해 관심 있는 독자를 [4] 참조하십시오 .

7. 향후 작업

이 문서는 헬륨 네트워크를 구축하기 위해 잘 설계된 설계를 제시합니다. 그러나 우리는 이것이 분산형 무선 네트워크의 엔지니어링, 연구 및 설계의 시작에 불과하다고 생각합니다. 우리는 블록체인 및 기본 토큰과 실제 하드웨어의 긴밀한 통합이 다른 종류의 네트워크 및 무선 물리 계층 에 적용될 수 있는 새롭고 가치 있는 혁신이라고 믿습니다. 우리는 블록체인의 미래가 누가 가장 많은 해싱 파워를 가지고 있거나 가장 저렴한 전력에 접근할 수 있느냐가 아니라, 채굴 증거가 가치 있고 검증 가능한 서비스를 제공하는 것과 연결된 블록체인에 관한 것이라고 믿습니다.

다음을 포함하여 우리가 착수 했거나 착수할 계획이 있는 몇 가지 이니셔티브가 있습니다 .

- 이러한 아이디어를 WiFi, Bluetooth 및 Cellular와 같은 다른 물리적 계층 에 적용할 수 있는지 조사합니다.
- 유사한 설계를 통한 5G 60GHz+ mmWave 연결 제공 가능성 탐색
- 더 많은 Proof-of-Coverage를 연구하고 구현합니다.
  헬륨 네트워크가 성장함에 따라 보안 유지
- 인센티브 시스템의 게임 이론 분석
- Proof of Coverage에 사용된 채점 알고리즘을 공식적으로 증명
- WHIP 무선 사양 생성 및 출시
- 가용성을 위한 핫스팟 및 장치 모듈 제조
  헬륨 네트워크 출시 시
- 기본 DWN 프리미티브를 넘어 스마트 계약 환경의 배포를 조사합니다.
- Forward Error Correc의 지속적인 작업과 진화
  기술

감사의 말

이 문서는 우리 팀 구성원들의 협력 작업의 결과이며 이사회, 고문, 투자자 및 협력자 의 도움, 피드백 및 검토 없이는 불가능했을 것 입니다. 관련된 모든 분들께 진심 으로 감사드립니다.

MIT Digital Currency Initiative 의 Jeremy Rubin에게도 감사의 인사를 전 합니다. 가장 빠른 피드백

그리고 방향은 이 프로젝트의 일부 설계 결정과 발전에 매우 중요했습니다. 또한 이 작업에 대한 자세한 검토와 도움을 주신 Berkeley 팀 의 Blockchain 에도 감사드립니다 .

우리는 또한 이 프로젝트를 만들 수 있었던 많은 이전 작업과 발명, 특히 Bitcoin[9]과 Ethereum[5]을 인정하고 싶습니다.

참고문헌

[1] 마커스 토키아, 모니카 쿠마르. IDC - 2017년 전 세계 반기 사물 인터넷 지출 가이드(문서)

[2] 숀 패닝. Napster - 독립적인 P2P 파일 공유, 1999년 1

[3] 메흐메트 아달리에. Curve P-256 2.6의 효율적이고 안전한 타원 곡선 암호화 구현

[4] Andrew Miller 및 Yu Xia 및 Kyle Croman 및 Elaine Shi 및 Dawn Song. BFT 프로토콜의 허니 오소리, 2016 2.2, 6.2, 6.2.5

[5] 비탈릭 부테린. 이더리움, 2014 3.1, 6.1, 7

[6] 로라 얼라이언스. LoRa Alliance - IoT용 광역 네트워크, 2013년 2.4.1

[7] Ingenu. RPMA 기술 2.4.1

[8] IEEE. 저속 무선 네트워크에 대한 IEEE 표준, 2015 2.4.1

[9] 나카모토 사토시. 비트코인: P2P 전자 현금 시스템, 2008 3.1, 7

[10] EW 다익스트라. 그래프 와 관련된 두 가지 문제에 대한 메모 , 1959 4, 3.3.4

[11] 데이비드 카거, 에릭 리먼, 톰 레이튼, 매튜 리바인, 다니엘 르윈, 리나 파니그레이. 일관된 해싱 및 랜덤 트리: 월드 와이드 웹에서 핫스팟 을 완화하기 위한 분산 캐싱 프로토콜 , 1997

[12] 아담 랭글리, 구글. 러프타임 - 안전한 시간 동기화 제공 을 목표로 하는 프로젝트 3.4

[13] Mehmud Abliz, Taieb Znati. 거부를 위한 가이드 투어 퍼즐 서비스 예방, 2009 3.2

[14] 모바일 전문가 자산 추적 IoT 장치, 2017 4.1

[15] Guofang Dong, Bin Yang. TDOA 기반 및 RSSI 기반 지하 무선 측위 방법 및 성능 분석 4.2.1

[16] Mohamed Laaraiedh, Lei Yu, Stephane Avrillon. RSSI, TOA 및 TDOA 를 사용한 하이브리드 현지화 방식 비교 , 2011 4.2.1

[17] 모하마드 야신, 엘리아스 라시드, 로니 나스랄라. 2014년 Wi-Fi 네트워크의 위치 확인 기술 성능 비교 4.2.1

[18] Muhammad Farooq-i-Azam, Muhammad Naeem Ayyaz. 무선 센서 네트워크의 위치 및 위치 추정, 2016 4.2.1

[19] 김상덕, 종화. 기지국 간 동기화가 없는 효율적인 TDOA 기반 현지화 알고리즘 , 2015 4.2.2

[20] Igor Olegovych Tovkach, Serhii Yakovych Zhuk. 센서 네트워크에서 TDOA 로컬라이제이션을 위한 순환 알고리즘, 2017 4.2.2

[21] Peter W. Boettcher, Gary A. Shaw. 음향 방위 추정을 위한 도달 알고리즘의 분산 시차 4.2.2

[22] Shuai He, Xiaodai Dong, Wu-Sheng Lu. 도착 측위 시스템의 비동기 시차, 2015 4.2.2

[23] 로라 얼라이언스. LoRaWAN - LoRa 연합 기술, 2014 4.2.1

[24] David Snsteb, Sergey Ivancheglo, Dominik Schiener 및 Serguei Popov. IOTA - 차세대 블록체인, 2015 5.2

[25] 프로토콜 연구소. Filecoin - 분산 스토리지 네트워크, 2017년 6.1

[26] 위키피디아. 지분 증명 6.1

[27] K Driscoll, B Hall, M Paulitsch, P Zumsteg, H Sivencrona. 레알 비잔틴 장군, 2004 6.1

[28] 백준상, 정위량. Gap Diffie-Hellman Group의 간단하고 효율적인 임계값 암호 시스템, 2003 6.2.1

[29] Joseph Poon, Thaddeus Dryja. 라이트닝 네트워크 - 확장 가능하고 즉각적인 비트코인/블록체인 거래, 2017 5.2

[30] 브레인봇. Raiden Network - 빠르고 저렴하며 확장 가능한 토큰 이더리움에 대한 전송, 2017 5.2

[31] 제프 콜먼. 상태 채널, 2015 5.2