비트코인 사용 가이드

개인 지갑 · 결제 · 풀 노드 · 라이트닝 노드 · 노스터 · 홈 채굴 가이드

2판
2025. 9. 1. 기준

필레몬 지음
HYPE 감수
익스토스 출판

비트코인 사용 가이드

개인 지갑 • 결제 • 풀 노드 • 라이트닝 노드 • 노스터 • 홈 채굴 가이드

비트코인 사용 가이드: 개인 지갑, 결제, 풀 노드, 라이트닝 노드, 노스터, 홈 채굴 가이드, 제2판

저작권 없음 🅭 ⓪ 필레몬, 2025
필레몬은 2025년 『비트코인 사용 가이드』 제2판을 CC0 1.0 Universal에 따라 퍼블릭 도메인에 헌정합니다.

| 필레몬의 퍼블릭 도메인 선언 |

지식과 문화는 인류 모두의 자산입니다. 정보는 희소하지 않으며, 따라서 희소한 재화에 적용하는 재산권이 정보에는 적용될 수 없습니다. 정보에 대한 독점적 재산권 부여는 오히려 정보를 정당하게 취득한 소비자의 물리적 재산권을 침해합니다.
소비자 각각의 재산권 보호가 훨씬 중요하므로 저자는 본 저작물(비트코인 사용 가이드 제2판)에 대한 모든 저작재산권을 최대한도로 포기합니다. 이에 따라 소비자는 일반적으로 저작재산권에 따라 제한되는 복제, 전시, 배포, 전송, 수정, 상업적 이용을 자유롭게 할 수 있습니다. 본 선언은 크리에이티브 커먼즈 CC0 1.0 Universal에 따라 이루어집니다.

선언문 해시값: `45046C4A0858AD664122B30974353D46580D7F107A68CF761724A4E30170BA0D`
비트코인 메시지 서명: `H9gTJUOT1JIYQGVxsDd89AOTgiE1by7bdk4EDXf7arjFDg3gqP/wdqoRclSiwXwp/rNNSen3t/pxK2AFDDxmkjE=`

서명 검증을 위한 저자의 공개된 비트코인 주소는 keybase.io/philemon21에서 확인할 수 있습니다.

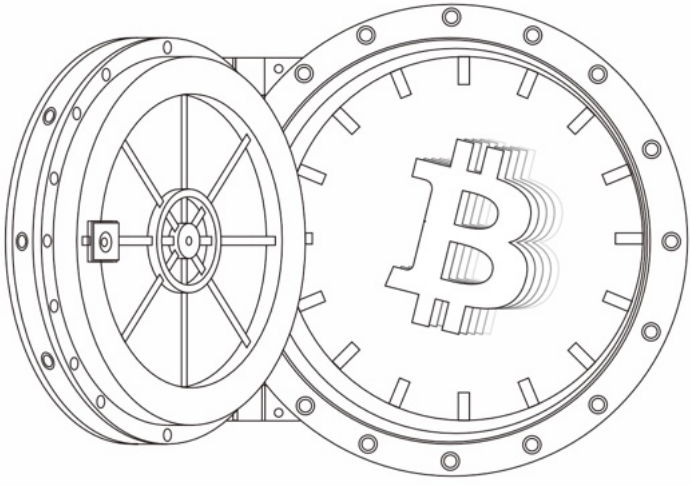
저자의 저작재산권 포기가 상표권, 저작인격권, 퍼블리시티권, 프라이버시권, 저자에게 귀속되지 않는 제3자의 권리 등의 포기를 의미하지 않습니다. 이를 무시하여 발생하는 문제에 대한 책임은 전적으로 사용자에게 있습니다.

본 전자 파일은 배포용으로 제작되었습니다. 본 전자 파일에 표시된 출판사명이나 로고는 원전 출처 확인을 돕기 위한 것으로, 전자 파일의 배포는 해당 출판사와 무관하게 진행되었습니다.

파일의 무결성을 확인하기 위해서는 해시값, 저자 서명이 올바른지 검증해 보십시오.

비트코인 사용 가이드

개인 지갑 · 결제 · 풀 노드 · 라이트닝 노드 · 노스터 · 홈 채굴 가이드



2판
2025. 9. 1. 기준

필레몬 지음
HYPE 감수
익스토스 출판

| 목차 |

서문. 당신의 돈을 통제하라 7
감수의 글 12

1부. 셀프 커스터디 가이드

■ 비트코인 지갑 사용을 위한 지식 26

셀프 커스터디 • 26 | 비트코인의 소유권과 셀프 커스터디의 필요성, 책임 • 27 | BTC와 sats 단위 • 28 | 잔고 모델과 UTXO 모델 • 28 | 에어-갭 지갑과 워치-온리 지갑 • 31 | PSBT • 33 | 개인키와 주소 • 34 | 니모닉과 개인키, 주소 • 35 | 확장 공개키 • 37 | 주사위를 굴릴 때 주의할 점 • 38 | 거래 데이터(트랜잭션) • 39 | UTXO에 대한 비유 • 40 | 거래 데이터와 블록 • 41 | 수수료 • 43 | 멤풀 웹사이트 • 43 | UTXO 정리 • 45 | 주소 재사용 주의 • 46 | 파생 경로 • 46 | 갭 리밋과 주소 순차 사용 • 47 | 패스프레이즈 • 48 | 니모닉 체크섬과 MFP • 49 | 5달러 렌치 공격과 수량 발설 주의 • 52 | KYC (고객 확인) 제도와 트래블 룰 • 54 | 라이트닝 네트워크와 인보이스, 라이트닝 주소 • 55

■ 키스톤 지갑 57

필수 준비물 • 57 | 권장 준비물 • 59 | 업데이트를 위한 마이크로SD카드 준비 • 60 | 기기 검증 • 63 | 펌웨어 2.0.4 검증 및 업그레이드 • 66 | 최신 펌웨어 업데이트 • 70 | 지갑 생성 • 77 | 키스톤 사전 설정 • 85 | 블루월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 • 88 | 넌척에 확장 공개키 내보내 워치-온리 지갑 만들기 • 94 | 코코넛 월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 • 101 | 블루월렛으로 서명 연습 • 105 | 넌척으로 서명 연습 • 111 | 코코넛 월렛으로 서명 연습 • 116 | 복구 연습 • 119

■ 시드사이너 지갑 125

필수 준비물 • 125 | 권장 준비물 • 128 | 이미지 파일 다운로드 • 129 | 소프트웨어 변조 여부 확인(윈도우OS) • 130 | 소프트웨어 변조 여부 확인(맥OS) • 141 | 부팅 마이크로SD카드 만들기 • 150 | 발레나에처로 시드사이너 이미지 파일 플래싱이 안 될 경우 해결 방법 • 156 | 무선 통신 모듈 제거(라즈베리파이 제로 W 보드만 해당) • 164 | 시드사이너 조립 • 166 | 시드사이너 케이스까지 조립 • 174 | 지갑 생성 • 182 | 시드 QR 제작 • 188 | 니모닉 입력하기 or 시드 QR 스캔하기 • 194 | 블루월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 • 196 | 넌척에 확장 공개키 내보내 워치-온리 지갑 만들기 • 204 | 코코넛 월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 • 212 | 블루월렛으로 서명 연습 • 218 | 넌척으로 서명 연습 • 224 | 코코넛 월렛으로 서명 연습 • 231 | 시드사이너를 게임기로 만들기 • 236

■ 공기계 지갑 247
스마트폰 공기계를 콜드월렛으로 사용해 지갑 생성하기 • 247 | 블루월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 • 256 | 넌척에 확장 공개키 내보내 워치-온리 지갑 만들기 • 262 | 블루월렛으로 서명 연습 • 269 | 넌척으로 서명 연습 • 274 | 공기계 블루월렛에서 간접 복구 테스트 • 279
■ 거래소에서 지갑으로 비트코인 옮기기 282
거래소에서 비트코인으로 환전하는 방법 • 282 | 빗썸 가입 및 KYC 인증 • 285 | 바이낸스 가입 및 KYC 인증 • 298 | 빗썸에서 원화 입금하고 테더 구매하기 • 304 | 빗썸에서 바이낸스로 테더 보내기 • 307 | 바이낸스에서 테더로 비트코인 구매하기 1: Convert 사용 • 310 | 바이낸스에서 테더로 비트코인 구매하기 2: 시장가 매수 • 312 | 바이낸스에서 온-체인을 통해 바로 개인 지갑으로 전송하기 • 316 | 바이낸스에서 라이트닝 네트워크와 볼츠 스와프 서비스를 통해 개인 지갑으로 전송하기 • 317
■ 지갑에서 거래소로 비트코인 옮겨 원화 출금하기 322
전송 경로 • 322 | 개인 지갑에서 해외 거래소로 전송 • 323 | 해외 거래소에서 국내 거래소로 전송 • 324 | 국내 거래소에서 원화 환전 후 은행 계좌로 출금 • 330
■ 스패로우 지갑 사용 방법 및 UTXO 정리하기 334
준비물 • 334 | 스패로우 설치 • 335 | 풀 노드 서버 설정 • 337 | 워치-온리 연동하기 • 340 | UTXO 정리 • 345 | 앨리스의 UTXO 정리 • 346 | 스패로우에서 UTXO 정리하기 • 348 | 넌척에서 UTXO 정리하기 • 368
■ 수수료율 설정, RBF와 CPFP 376
온-체인 수수료 • 376 | 멤풀 웹사이트 보는 방법 • 379 | 적정 수수료율 설정하기 • 382 | RBF • 386 | CPFP • 401
■ 패스프레이즈 418
패스프레이즈와 주의 사항 • 418 | 키스톤에서 패스프레이즈 설정하기 • 420 | 시드사이너에서 패스프레이즈 설정하기 • 424 | 공기계 콜드월렛에서 패스프레이즈 설정하기 • 425 | 서명 기기에서 서명이 안 될 때 • 430
■ 멀티시그 431
멀티시그(다중서명) • 431 | 블루월렛에서 멀티시그 지갑 생성 • 434 | 넌척에서 멀티시그 지갑 생성 • 446 | 스패로우 지갑에서 멀티시그 지갑 생성 • 461 | 블루월렛 멀티시그 지갑에서 서명하기 • 478 | 넌척 멀티시그 지갑에서 서명하기 • 487 | 스패로우 멀티시그 지갑에서 서명하기 • 495 | 멀티시그 워치-온리 지갑 삭제 후 복구하기 • 505

2부. 비트코인 스탠다드 가이드

■ **비트코인은 돈이다** 524

비트코인은 돈이다 • 524 | 교환 매개 • 525 | 구매력 보존 • 529 | 회계 단위 • 534 | 비트코인의 레이어 구조 • 536 | 라이트닝 네트워크를 사용하는 방법 • 539 | 비트코인 결제 체험이 중요한 이유 • 539

■ **라이트닝 수탁 지갑 이용 방법** 541

라이트닝 수탁 지갑 설치 • 541 | 커스텀 라이트닝 주소 발급 • 544 | 온-체인으로 라이트닝 수탁 지갑에 비트코인 입금하기 • 549 | 라이트닝 수탁 지갑에서 온-체인으로 비트코인 출금하기 • 553 | 원화 환전을 위해 라이트닝 수탁 지갑에서 해외 거래소로 비트코인 송금하기 • 556

■ **오프라인 매장에서 라이트닝 결제하기** 561

비트코인으로 커피 사 마시기 • 561

■ **온라인 매장에서 라이트닝 결제하기** 565

비트코인으로 물건 구매하고 택배 받기 • 565

■ **1분 만에 비트코인 결제 매장 되기** 571

매장에서 라이트닝 결제받는 방법 • 571

3부. 풀 노드 운영 가이드

■ **풀 노드 운영을 위한 지식** 574

풀 노드와 풀 노드 운영의 중요성 • 574 | 풀 노드가 수행하는 검증 작업 • 575 | 풀 노드가 보관하는 데이터 • 576 | 가지치기 풀 노드 • 579 | 비트코인 클라이언트: 비트코인 코어와 노츠 • 579 | 초기 블록 다운로드(IBD) • 580 | 아웃바운드 연결과 인바운드 연결, 인바운드 허용 노드 • 581 | 일렉트럼 서버 • 584 | RPC 인터페이스 • 585 | 진정한 금융 주권의 실천 • 586

■ **엄브렐 홈 구매 및 세팅** 587

풀 노드 구축 방법 • 587 | 엄브렐 홈 구매 방법 • 588 | 엄브렐 홈 세팅 • 596

■ **미니 PC 조립하고 엄브렐OS 설치하기** 598

미니 PC 준비물 • 598 | 미니 PC 조립하기 • 603 | 바이오스에서 램 설정하기 • 609 | OS 설치용 USB 만들기 • 611 | 엄브렐OS 설치하기 • 618

■ **라즈베리파이5 조립하고 엄브렐OS 설치하기** 623

라즈베리파이5 준비물 • 623 | SSD에 엄브렐OS 설치하기 • 630 | 라즈베리파이5 조립 • 639 | 부팅이 안 될 경우 • 650 | 케이스 조립 • 660

■ **노트북에 엄브렐OS 설치하기** 664

남는 노트북에 엄브렐OS 설치하기 • 664 | OS 설치용 USB 만들기 • 665 | 노트북에 엄브렐OS 설치하기 • 673 | 노트북에서 엄브렐 화면 띄우기 • 677

■ **엄브렐 설정 및 풀 노드 동기화** 685

엄브렐 설정 및 업데이트 • 685 | 비트코인 노드(코어) 또는 노츠 설치 • 690 | 가지치기(프루닝) 설정 • 694 | 노츠의 사용자 정책 설정 • 696

■ **외부에서 엄브렐 접속하기** 704

테일스케일 설치 및 연결 • 704

■ **워치-온리 지갑과 자신의 풀 노드 연동하기** 710

일렉터스(Electrs) 설치 • 710 | 블루월렛과 자신의 풀 노드 연결하기 • 712 | 넌척과 자신의 풀 노드 연결하기 • 714 | 코코넛 월렛과 자신의 풀 노드 연결하기 • 716 | 스패로우와 자신의 풀 노드 연결하기 • 718 | 토르를 이용해 자신의 풀 노드와 워치-온리 지갑 연결하기 • 722 | 블루월렛에서 토르를 이용해 워치-온리 지갑 연결하기 • 728 | 넌척에서 토르를 이용해 워치-온리 지갑 연결하기 • 730

■ **멤풀과 RPC 명령어** 733

멤풀 앱 연결하기 • 733 | RPC 익스플로러 사용하기 • 734 | 터미널에서 RPC 명령어 사용하기 • 745

■ **도달 가능한 노드 되기** 752

자기 노드가 도달 가능한 노드인지 확인해 보기 • 753 | 익명 네트워크에서 도달 가능한 노드 되기 • 755 | 클리어넷에서 도달 가능한 노드 되기 • 757 | TP링크 공유기: DHCP 서버 설정, 포트 포워딩 • 758 | IP타임 공유기: DHCP 서버 설정, 포트 포워딩 • 763 | 인터넷 서비스 업체의 공유기를 사용하는 경우 • 768 | 엄브렐 인바운드 연결 허용 및 방화벽 해제 • 770 | 도달 가능한 노드가 되었는지 확인하기 • 774

■ **윈도우OS에서 풀 노드 운영하기** 775

윈도우OS에 비트코인 코어 설치하고 동기화하기 • 775 | 윈도우OS에 비트코인 노츠 설치하고 동기화하기 • 784 | 같은 기기에서 스패로우 지갑 연결하기 • 793

■ **맥OS에서 풀 노드 운영하기** 800

맥OS에 비트코인 코어 설치하고 동기화하기 • 800 | 맥OS에 비트코인 노츠 설치하고 동기화하기 • 810 | 같은 기기에서 스패로우 지갑 연결하기 • 822

■ **로컬 네트워크에서 스패로우 지갑과 비트코인 코어, 노츠 연결하기** 828

코어, 노츠가 설치된 기기의 로컬 IP 주소 알아내기 • 828 | bitcoin.conf 파일 설정하기 • 830 | 윈도우OS에 코어, 노츠가 설치되어 있는 경우 방화벽 해제 • 833 | 맥OS에 코어, 노츠가 설치되어 있는 경우 방화벽 해제 • 836 | 로컬 네트워크에서 스패로우 지갑 연결하기 • 837

4부. 라이트닝 노드 운영 가이드

■ **라이트닝 노드 운영을 위한 지식** 842

라이트닝 네트워크 • 842 | 라이트닝 채널의 원리 • 843 | 인바운드 유동성과 아웃바운드 유동성 • 847 | 다중 경로 결제 • 852 | HTLC • 854 | 협력적 종료와 비협력적 종료, CSV, 페널티 • 855 | 라이트닝 노드의 유형 • 857

■ **라이트닝 노드 설치, 복구, RTL 설치** 859

라이트닝 노드(LND) 설치 • 859 | 라이트닝 노드 제거 후 복구 • 863 | CLN을 설치하는 경우 • 866 | RTL 설치 • 873

■ **일상적인 지갑 목적으로 라이트닝 노드 운영하기** 876

라이트닝 노드 온-체인 지갑에 자금 전송 • 878 | 라이트닝 노드 검색 및 피어 추가, 채널 개설 • 880 | 두 번째 채널 개설 • 889 | 세 번째 채널 개설 • 892 | 네 번째 채널 개설 • 894 | 다섯 번째 채널 개설 • 896 | 인바운드 유동성 확보 • 898 | 여섯 번째 채널 개설 • 908 | 일곱 번째 채널 개설 • 910 | 여덟 번째 채널 개설 • 912 | 채널 추천 목록 • 914

■ **외부에서 라이트닝 노드 사용하기** 917

토르를 통해 라이트닝 노드와 제우스 앱 연동하기 • 917 | 테일스케일을 통해 라이트닝 노드와 제우스 앱 연동하기 • 920 | 제우스 앱 사용 방법 • 925

■ **라이트닝 노드 설정하기** 931

라이트닝 노드 네트워크 설정과 개인 맞춤 설정 • 931 | 채널 설정 • 935 | 라우팅 설정 • 938 | 워치타워 설정 • 946

■ **채널 관리 가이드** 953

라우팅 수수료 부과 원리 • 953 | 특정 노드가 유동성을 다 흡수할 때 • 955 | 채널별 라우팅 수수료, 최대/최소 HTLC 금액 조정하기 • 957 | 수수료 조정보다는 적절한 노드 찾고 채널 맺기 • 959 | 채널 닫기 • 961 | 라이트닝 노드 SCB 파일 백업과 복구 • 963

■ **라이트닝 주소 설정, 자신의 노드 알리기** 969

알비 허브로 라이트닝 주소 연결하기 • 969 | 알비 유료 결제하고 커스텀 라이트닝 주소 만들기 • 978 | 앰보스에서 노드 정보 입력하기 • 984

■ **라이트닝 노드로 온라인 비트코인 결제 매장 구축하기** 990

워드프레스에 BTCPay Server, 우커머스 플러그인 설치 • 990 | 우커머스 기본 설정 및 테마 선택 • 992 | 우커머스 상품 올리기 • 996 | 엄브렐에서 BTCPay Server 다운로드하고 설정하기 • 1001 | 클라우드플레어 회원가입 • 1009 | 클라우드플레어 터널 연결 • 1016 | 도메인 연결 • 1020 | SSL 적용 • 1025 | 워드프레스 우커머스와 자신의 BTCPay Server 연결 • 1029 | 기타 설정 • 1033 | 법률 문제, 세금 문제 • 1034

5부. 노스터 가이드

■ **노스터 사용을 위한 지식** 1038

기존 소셜 미디어의 문제점과 노스터 • 1038 | 노스터 클라이언트 • 1041 | 노스터 릴레이와 이벤트, 작동 원리 • 1042 | 노스터 구현 제안(NIP) • 1044 | 개인키(nsec)와 공개키(npub), 노스터 주소 • 1045 | 노스터의 DM과 종단간 암호화 • 1046 | 잽(Zaps)과 NWC (노스터 지갑 연결) • 1047 | 노스터의 단점과 광고 필터, 리스트 구독 • 1049

■ **프라이멀 사용 방법** 1051

프라이멀 앱 설치 및 개인키-공개키 쌍 생성 • 1052 | 다른 사람들에게 npub 알려주기 • 1056 | 팔로우 추가 • 1057 | 잽을 위한 지갑 추가 • 1058

■ **다무스 사용 방법** 1062

다무스 앱 설치 및 개인키-공개키 쌍 생성 • 1062 | 다른 사람들에게 npub 알려주기 • 1065 | 팔로우 추가 • 1066 | 잽을 받기 위한 라이트닝 주소 연결 • 1068 | 다른 사람에게 잽 보내기 • 1070

■ **피닉스 사용 방법** 1073

피닉스에서 개인키-공개키 쌍 생성 • 1073 | 다른 사람들에게 npub 알려주기 • 1079 | 팔로우 추가 • 1081 | 잽을 받기 위한 라이트닝 주소 연결 • 1083

■ **노스터 서명 확장 프로그램** 1084

서명 확장 프로그램을 쓰는 이유 • 1084 | 크롬에서 알비 익스텐션 사용 방법 • 1085 | 알비에서 노스터 주소 사용하기 • 1092 | 웹 클라이언트에서 알비 익스텐션으로 로그인하기 • 1094

■ **노스터에서 기사, 칼럼 등의 긴 글 쓰기** 1098

하블라에서 긴 글 쓰기 • 1098 | 마크다운 문법 간략히 알아보기 • 1103

■ **엄브렐에서 노스터 릴레이 서버 운영하고 연결하기** 1112

프라이빗 릴레이 서버 운영하기 • 1112 | 로컬 네트워크에서 자신의 릴레이 서버에 연결하기 • 1114 | 테일스케일을 이용해 원격으로 자신의 릴레이 서버에 연결하기 • 1117 | 도메인을 연결해 퍼블릭 릴레이 서버로 만들기 • 1119

■ **NWC를 이용해 자신의 라이트닝 노드에서 잽 보내기** 1124

알비 허브를 통해 NWC 지갑 생성하기 • 1124 | 다무스에서 NWC 지갑 연결하기 • 1126 | 피닉스에서 NWC 지갑 연결하기 • 1129

■ **NWC를 이용해 제우스에서 라이트닝 주소 발급하기** 1132

제우스에서 라이트닝 주소 발급하기 • 1132

6부. 홈 채굴 가이드

■ **홈 채굴을 위한 지식** 1136

비트코인 채굴 • 1136 | 채굴 방식의 분류 • 1139 | 채산성 계산하기 • 1141 | 채굴 풀 보상 방식 • 1144 | 스트라텀 프로토콜 • 1151 | 채굴 풀의 한계 • 1153 | 다텀과 채굴 주권 • 1155 | 홈 채굴의 의미 • 1157

■ **비트엑스 감마 601로 솔로 채굴하기, 채굴 풀 참여하기** 1159

준비물 • 1159 | 비트엑스 스탠드 조립 및 전원 연결 • 1161 | 비트엑스 네트워크 연결 • 1162 | 비트엑스 펌웨어 업데이트 • 1164 | 솔로 채굴 설정하기(ckpool) • 1167 | 채굴 풀 참여하기(브레인스 풀) • 1170 | 라이트닝 네트워크로 보상 받기(브레인스 풀) • 1176

■ **아발론 나노 3로 솔로 채굴하기, 채굴 풀 참여하기** 1179

준비물 • 1179 | 아발론 나노 3 전원 연결 • 1181 | 아발론 나노 3 설정하기 • 1182 | 솔로 채굴 설정하기(ckpool) • 1186 | 채굴 풀 참여하기(브레인스 풀) • 1190 | 라이트닝 네트워크로 보상 받기(브레인스 풀) • 1197

■ **다텀으로 풀 노드와 채굴기 연결하기** 1200

비트코인 노츠 설치 • 1200 | 다텀 설치 • 1202 | 다텀에서 솔로 채굴 설정하기 • 1204 | 비트엑스를 다텀에 연결하기 • 1208 | 아발론 나노 3를 다텀에 연결하기 • 1210 | 채굴이 잘 되는지 확인하기 • 1211 | 다텀을 이용하여 채굴 풀(오션 풀) 참여하기 • 1213 | 블루월렛에서 생성된 지갑 주소 사용 • 1214 | 라이트닝 노드에서 생성된 온-체인 주소 사용 • 1216 | 다텀 설정하기 • 1216 | 비트엑스를 다텀에 연결하기 • 1220 | 아발론 나노 3를 다텀에 연결하기 • 1222 | 채굴이 잘 되는지 확인하기 • 1223 | 라이트닝 지갑으로 채굴 보상 받기 • 1228 | 코어 라이트닝(CLN)으로 Offer 생성하기 • 1231 | 메시지 서명하기 • 1236 | 마무리하며 • 1246

부록

■ **부록 1. 기기별 니모닉 생성 알고리즘** 1248

니모닉 생성 알고리즘 검증 • 1248 | 키스톤 3 프로 기기의 니모닉 생성 알고리즘 • 1249 | 시드사이너 기기의 니모닉 생성 알고리즘 • 1251 | 블루월렛에서의 니모닉 생성 알고리즘 • 1253

■ **부록 2. 니모닉 복구 방법 및 니모닉 목록** 1256

BIP-39 목록 설명 • 1256 | 니모닉 복구 전 주의 사항 • 1256 | ① 영단어 4자리로 백업되어 있는 경우 • 1258 | ② 이진법(비트)으로 백업되어 있는 경우 • 1260 | ③ 영단어 4자리 순서로 백업되어 있는 경우 • 1263 | BIP-39 니모닉 목록 • 1267

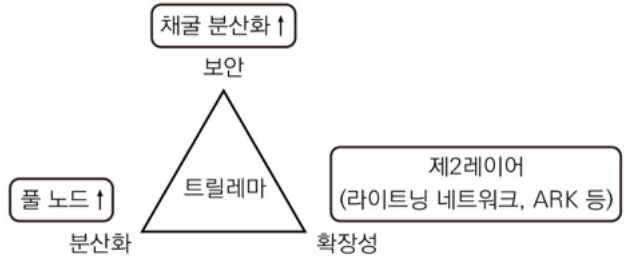
비트코인 사용 가이드

6. 홈 채굴 가이드

| 홈 채굴을 위한 지식

비트코인 채굴

채굴은 단순히 새로운 비트코인을 얻는 방식이 아니라 네트워크의 보안을 책임지는 핵심이다. 풀 노드가 분산화, 라이트닝 네트워크가 확장성을 담당한다면 채굴은 비트코인의 보안을 담당한다.

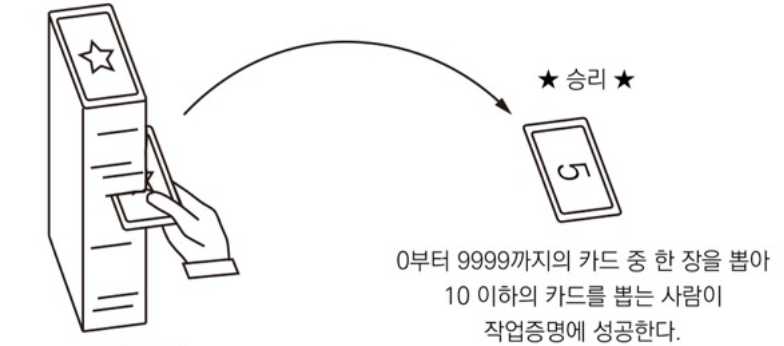


비트코인에서 채굴은 작업증명과 인센티브를 합친 것을 말한다. 따라서 채굴이 무엇인지 이해하고 싶다면 작업증명PoW, proof-of-work과 인센티브 시스템에 대해 알아야 한다.

비트코인 네트워크에는 거래들을 모아서 새로운 블록을 만들려는 노드들이 있다. 풀 노드들은 유효한 거래들을 자신들의 거래 바구니인 멤풀에 넣고 전파한다. 이렇게 멤풀에 들어있는 거래들을 수수료가 높은

순서대로 모아 블록을 만드는 노드들이 바로 채굴자다. 그런데 이런 블록을 구성하려는 사람들이 매우 많으니, 이들이 올린 블록 중 어떤 블록을 참인 것으로 인정할지 합의하는 시스템이 필요하다. 이를 해결하는 것이 작업증명이다.

작업증명은 일종의 제비뽑기 같은 것이다. 정확히는 논스값을 바꿔보며 목푯값보다 작은 해시값이 나오게 하는 것이 작업증명이다. 좀 더 쉽게 이해하기 위해 예시를 들어보겠다. 0부터 9999까지 적혀있는 카드들이 있다고 해보자. 블록을 올리려는 사람들은 계속 카드를 뽑는다. 카드를 계속 뽑고 섞다가 10 이하의 카드를 뽑은 사람이 있으면 그 사람이 만든 블록을 참으로 인정하기로 하는 것이다. 내가 만든 블록이 참으로 인정되려면 카드를 계속 섞고 뽑아보면서 다른 채굴자들보다 더 빨리 10 이하의 카드를 뽑아야 한다. 더 빨리 뽑아야 자신이 만든 블록이 참으로 인정받기 때문이다. 카드에 적힌 숫자는 비트코인 채굴에서 블록 해시값이고, 카드를 뽑는 행위는 추가 논스값을 포함하여 논스값을 바꿔보는 행위이다.



작업증명이 단순한 무작위 게임이 아닌 이유는 많은 연산 능력이 들어가야만 블록을 생성할 수 있기 때문이다. 카드를 계속 뽑으려면 에너지와 시간이라는 비용이 들어간다. 따라서 작업증명에 대한 보상으로 새로 발행된 비트코인과, 사람들이 각각의 거래에서 지불한 수수료가 지급된다. 그 보상은 채굴자가 직접 블록에 넣고, 풀 노드들이 규칙에 맞는지 검증한다. 이 인센티브 구조는 채굴자들이 네트워크 보안 유지에 자발적으로 참여하도록 유도하는 원동력이다.

만약 어떤 공격자가 과거 블록을 조작하려면 변조하려는 블록 이후의 모든 블록을 다시 채굴해야 한다. 이는 엄청난 비용이 들어가기 때문에 사실상 불가능하다. 블록 생성에 들어가는 에너지 비용은 네트워크를 공격하려고 할 때도 전부 지불해야 하는 비용이 되기 때문이다. 평상시에는 여러 채굴자들이 모여 각자의 이익을 위해 이 에너지 비용을 지불하지만, 공격자가 비트코인을 공격하려고 할 때는 혼자서 이 비용을 전부 지불해야 한다.

따라서 채굴은 비트코인을 안전한 상태로 유지하는 방패다. 수많은 채굴자들의 연산 능력이 합쳐진 방어막이 비트코인의 보안을 보장한다. 이러한 연산 능력을 해시레이트hashrate라고 한다. 앞에서 이야기한 비유로 돌아가자면 해시는 카드를 한 번 뽑는 것과 같다. 해시레이트는 1초에 몇 번 해시 함수를 돌릴 수 있는지, 즉 카드를 몇 번 뽑을 수 있는지를 나타내는 것이다. 쉽게 이해하기 위해 이러한 예시를 들었지만, 개념이 잘못 잡힐 수 있으므로 정확히 이해하기 위해서는 사토시 나카모토가 쓴 비트코인 백서를 읽어보는 것을 추천한다.

채굴 방식의 분류

비트코인을 채굴하는 방식은 크게 두 가지로 나눌 수 있다. 하나는 채굴자가 독립적으로 연산을 수행하고 보상도 단독으로 받는 솔로 채굴이고, 다른 하나는 여러 채굴자들이 힘을 합쳐 블록을 찾고 보상을 나누는 채굴 풀 참여 방식이다.

솔로 채굴은 비트코인 초창기에는 일반적인 방식이었다. 초창기에는 개인용 컴퓨터나 GPU 카드만으로도 채굴이 가능했기 때문이다. 하지만 지금은 채굴 난도가 매우 높아지면서 솔로 채굴의 현실적인 성공 가능성은 희박하게 되었다. 솔로 채굴자는 블록을 발견했을 때 모든 보상을 온전히 가져간다. 2025년 기준, 보상은 3.125 BTC에 수수료 인센티브를 더한 값이다. 수수료 인센티브를 제외한 채굴 보상은 약 4년마다 절반으로 줄어드는데, 그래서 약 4년(정확히는 21만 블록)을 반감기라고 한다.

채굴 난도가 매우 높은 현재 상황에서는 개인이 블록을 찾는 데 수년 동안 운이 따라주지 않을 수도 있다. 그럼에도 불구하고 솔로 채굴은 기술적으로 매우 중요한 의미를 가진다. 특정 풀이나 제3자의 통제를 받지 않고도 완전히 독립적으로 채굴에 참여할 수 있기 때문이다.

채굴을 할 때는 채굴 과정에서 들어가는 에너지 비용을 보상받는 인센티브를 통해 개인적인 이익을 꿈꿀 수 있다. 하지만 채굴의 의미는 검증된 거래들을 모아 유효한 새 블록을 만들고, 이 과정에서 비트코인의 보안에 기여하는 것이기도 하다. 따라서 채굴을 로또 추첨에 비유하는 것은 좋지 않은 생각이지만, 그래도 이만큼 이해하기 좋은 비유가 없어 한 번 비유를 해보도록 하겠다. 솔로 채굴은 혼자서 로또를 사는 것과 같다.

채굴 풀 참여는 다수의 채굴자가 해시 파워(해시레이트)를 모아 블록을 찾고, 블록을 찾았을 때 받는 채굴 보상(인센티브)을 나누어 갖는 구조다. 여러 사람이 돈을 모아 로또를 사고, 당첨이 되면 당첨금을 나누어 갖는 방식이 채굴 풀 방식인 것이다. 각각의 채굴자는 셰어share라는 단위를 제출함으로써 자신이 얼마나 작업에 기여했는지를 증명한다. 셰어를 발견하여 제출하는 것은 일반적인 채굴보다 훨씬 쉽다(난도가 낮다).

예를 들어보자. 여러 명이 함께 0부터 9999까지 있는 카드를 뽑는데, 10 이하의 카드를 뽑으면 당첨되는 것이라고 해보자. 채굴 풀은 만약 카드를 뽑았는데 100 이하면 카드를 전부 내라고 한다. 채굴 풀 참여자들은 100 이하의 카드를 내는데, 이 100 이하의 카드가 셰어다. 그러다 보면 100 이하의 카드 중에 10 이하의 카드도 있을 것이다. 그러면 이 채굴 풀에서 작업증명에 성공한 것이다. 이때 만약 제출된 셰어가

총 100장인데, 내가 그중에 5장의 셰어를 제출했었다면 나는 총채굴 보상의 5%를 가져가는 방식이다(채굴 풀 운영자가 가져가는 수수료는 제외한다). 채굴 풀이 채굴 보상을 분배하는 방식에는 여러 가지가 있는데 이에 대해서는 잠시 뒤에 알아보겠다.

채산성 계산하기

채굴은 에너지 비용을 들여서 비트코인을 얻는 것이기 때문에 수익을 바라보고 한다면 채산성 계산이 필수다. 채산성 계산은 비용 대비 보상을 계산했을 때 이익이 되는지 계산하는 것이다.

채산성을 판단하기 위해 고려해야 할 요소들에는 네트워크 총 해시레이트, 내 해시레이트, 소모 전력, 비트코인 대비 원화 환율, 현재 채굴 보상, 전기료, 장비 비용과 수명 등이 있다. 총 해시레이트와 내 해시레이트는 기댓값을 계산하기 위해 필요하다. [내 해시레이트] / [총 해시레이트]는 내가 블록을 발견할 확률을 의미하며, 채굴 풀에 참여할 때는 내 기여도를 판단할 수 있는 지표가 된다. 블록은 평균적으로 1시간에 6개 정도 발견되므로, 자신이 블록을 발견할 확률에 '6 (블록) × 24 (시간) × 30 (일)'을 곱하면 한 달 동안 채굴을 해서 블록을 찾을 확률, 또는 한 달 동안의 나의 기여도를 계산할 수 있다.

비트코인 대비 원화 환율이 필요한 이유는 전기료를 원화로 내기 때문이다. 현재 채굴 보상과 비용을 비교하기 위해서는 채굴 보상을 원화로 환산하거나 전기료를 비트코인으로 환산하는 작업이 필요하다. 예상 소모 전력에 전기료를 곱하면 채굴 비용을 계산할 수 있을 것이다.

예시를 들어 계산해 보자. 계산을 단순화하기 위해 난이도 조정이나 장비 가격, 수명은 고려하지 않겠다. 하지만 정말 진심으로 이익을 위해

서 채굴을 한다면 이런 변수도 함께 계산해야 한다. 현재 비트코인 네트워크의 총 해시레이트가 1 ZH/s라고 하고, 내 기기의 해시레이트는 1 TH/s라고 하자. 채굴 보상은 3.125 BTC, 소모 전력은 18 W, 비트코인 대 원화 환율은 1억 5천만 원/BTC, 전기료는 대한민국 가정용 1단계 누진세 전기료인 120원/kWh라고 하고 채산성이 있는지 계산해 보자.

한 달 보상의 기댓값부터 계산해 보자. 내 네트워크 기여도는 1 TH/s를 1 ZH/s로 나누면 계산할 수 있다. T (테라)는 10^12를 의미하고, Z (제타)는 10^21을 의미하니 기여도는 10억 분의 1이 된다. 여기에 '6 (블록) × 24 (시간) × 30 (일)'을 곱하면 0.00000432가 된다. 그러면 솔로 채굴을 할 때 성공 확률은 0.00000432, 즉 약 23만 분의 1이다. 여기에 채굴 보상인 3.125 BTC와 비트코인 환율인 1.5억 원/BTC를 곱하면 한 달 기댓값이 나온다. 만약 채굴 풀에 참여하여 기댓값만큼 채굴 보상을 받는다면 한 달에 약 2,025원을 받는 셈이 된다.

이제 비용을 계산해 보자. 소모 전력이 18 W이고, 전기료가 120원/kWh니 두 값을 곱하면 전기료가 나온다. 참고로 1 kWh는 1,000 Wh이므로 전기료와 소모 전력을 곱하고 1,000으로 나눠주면 1시간당 전기료가 나온다. 계산하면 2.16 원/시가 된다. 이제 여기에 24 (시간) × 30 (일)을 곱하면 한 달 예상 전기료인 1,555원이 나온다.

그러면 보상에서 비용을 빼면 한 달에 약 500원 정도가 이익인 것을 알 수 있다. 하지만 보통 이 정도 홈 채굴 장비는 2025년 기준 20만 원 정도로 가격이 형성되어 있다. 손익분기점을 넘기 위해서는 30년이 넘게 걸리는 셈이다.

만약 솔로 채굴을 한다면 매달 1,500원 정도를 들여 작업증명 성공 확률이 약 23만 분의 1이고, 채굴 보상이 3.125 BTC인 게임에 참여하는 것과 같다는 계산이 나온다.

한 달 수익 계산식:

$$\text{보상: } \frac{\text{내 해시레이트}}{\text{총 해시레이트}} \times \text{블록 보상} \times 6 \times 24 \times 30 \times \text{비트코인 환율}$$

$$\text{비용: } \frac{\text{채굴기 소모 전력(W)} \times \text{전기료(원/kWh)}}{1000} \times 24 \times 30$$

순수익: 보상 – 비용

채산성이 있는지 계산해 보니 채굴은 이익으로 접근하면 안 된다는 생각이 들지 않는가? 채굴은 에너지 산업이다. 즉, 에너지 생산을 더 저렴하고 효율적으로 할 수 있는 에너지 기업이어야 더 큰 이익을 남길 수 있다. 에너지 생산에 비교우위가 없다면 수익을 얻기 힘들다. 이러한 이유로 비트코인 채굴은 효율적인 에너지 산업이 성장할 수 있도록 장려한다.

그렇다면 홈 채굴은 개인에게 아무런 이익이 없는 것일까? 그렇지 않다. 채굴은 비트코인이 생성되는 일이므로 채굴 풀에 참여하면서 신상정보를 입력하지 않는 한 완전한 non-KYC 비트코인을 얻을 수 있는 일이다. 세계 각국의 정부는 사람들의 자유로운 거래를 추적하고 제한하기 위해 거래소에서 열심히 KYC를 하도록 추진하고 있다. 하지만 채굴 보상으로 받는 비트코인은 처음 만들어지는 비트코인이므로 KYC가 될 수가 없다. 이런 순수한 비트코인을 얻을 수 있는 것은 영세한 홈 채굴자들에게 더 매력적으로 다가오는데, 거대한 규모로 채굴을 하는

기업들은 적어도 사업 신고를 해야 하기 때문이다. 따라서 일정 주기로 조금씩 비트코인을 환전하기를 원하는 개인들에게는 홈 채굴이 매력적으로 다가올 수 있다.

채굴 풀 보상 방식

채굴 풀이 보상을 분배하는 방식은 매우 다양하다. 여기서는 가장 흔한 분배 방식인 PPS, FPPS, PPLNS를 함께 알아보고, 오션 풀에서 새롭게 내놓은 TIDES 채굴 보상 분배 방식도 알아볼 것이다.

PPS는 Pay-Per-Share의 약자로 '셰어당 지급'을 말한다. 이는 셰어를 지급하면 그에 해당하는 보상을 바로 주는 것을 의미한다. 만약 내 채굴기가 유효 셰어를 1개 제출하면 고정된 보상을 즉시 받는다. 앞의 예시를 생각해 보자. 10 이하의 카드를 뽑으면 3 BTC를 보상으로 주는 게임에서 채굴 풀이 일반 목푯값의 10배인 100 이하의 카드(셰어)를 다 내라고 했다고 해보자. 그러면 어떤 채굴자가 100 이하의 카드를 채굴 풀에 낼 때마다, 채굴 풀은 3 BTC의 10분의 1인 0.3 BTC를 채굴자에게 즉시 지급한다(이 예시에서는 셰어 제출 난이도가 일반 채굴 난이도의 10분의 1이기 때문이다). 물론 수수료를 제외하기 때문에 채굴자가 받는 보상은 카드당(셰어당) 0.29 BTC 정도가 될 것이다. 만약 현재 채굴 보상이 3.125 BTC인데 셰어 제출 가변 난이도가 일반 채굴 난이도보다 500만 배 더 쉽다고 해보자. 그러면 채굴자는 셰어를 제출할 때마다 3.125 BTC / 500만 ≒ 63 sats를 즉시 지급받는다. 여기서 수수료를 제외하고 받으므로 실제로 받는 금액은 약 61 sats가 될 것이다.

PPS에서 주목할 것이 몇 가지 있다. PPS 보상 방식은 보상을 분배할 때 수수료 인센티브는 분배하지 않는다. 채굴 보상은 새롭게 발행되는

비트코인 블록 보상에 수수료 인센티브가 더해져 있다고 했다. 하지만 PPS 보상 분배 방식은 수수료 인센티브는 분배하지 않고 블록 보상만 분배한다.

PPS 방식은 또한 채굴 풀에서 실제로 블록이 채굴되든 안 되든 셰어당 보상을 지급하는 구조다. 따라서 채굴 풀이 운이 안 좋아서 채굴 풀에 참여하고 있는 채굴자들이 블록 채굴에 계속 성공하지 못하고 있으면 채굴 풀은 손해를 본다. 앞의 예시에서 실제로 10 이하의 카드를 뽑는 사람은 별로 없다고 해보자. 채굴자들이 11 이상 100 이하의 카드만 잔뜩 뽑으면 채굴 풀은 보상은 없는 채로 채굴자들에게 계속 0.3 BTC씩 줘야 한다. 만약 11 이상 100 이하의 카드를 뽑은 채굴자가 연속으로 11번 이상 나온다면 채굴 풀은 손실 상태로 들어간다. 채굴자는 안정적으로 수익을 얻을 수 있지만, 채굴 풀 입장에서는 이런 리스크가 있으므로 PPS 보상 방식의 채굴 풀은 일반적으로 수수료가 높은 편이다.

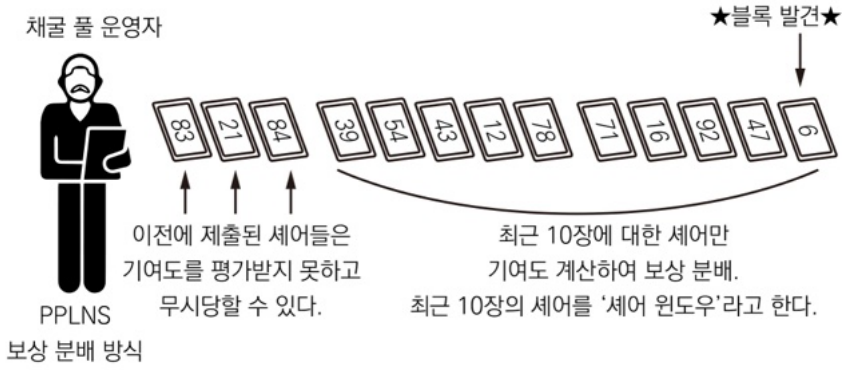
PPS를 이해했다면 FPPS(또는 PPS+) 보상 방식은 이해하기 쉽다. FPPS는 Full Pay-Per-Share의 약자로, '셰어당 전부 지급'이라는 뜻이다. PPS 보상 방식은 분배에서 수수료 인센티브는 제외하고, 블록 보상만 분배한다고 했다. FPPS는 수수료 인센티브까지 분배하는 것이다. 블록당 수수료 인센티브를 통계 내, 셰어당 수수료 인센티브 예상치까지 계산한다. 만약 블록 보상이 3.125 BTC고, 수수료 인센티브가 평균적으로 0.075 BTC라고 해보자. 그러면 총채굴 보상은 3.2 BTC가 된다. 셰어 제출 가변 난이도가 일반 채굴 난이도보다 500만 배 쉽다면 FPPS에서 셰어당 보상은 64 sats가 될 것이다(3.2 BTC / 500만). 여기서 수수료를 제외하면 셰어당 62 sats 정도를 받게 될 것이다. FPPS

는 채굴 풀이 수수료까지 분배하므로 채굴자는 매우 안정적으로 수익을 얻을 수 있지만, 채굴 풀 운영의 리스크는 더 커진다. 그러므로 수수료가 더 높은 편이다.

PPLNS는 Pay-Per-Last N Shares의 약자로, '마지막 N개의 셰어당 지급'의 약자다. 앞에서 PPS나 FPPS는 채굴 풀에서 블록이 발견되든 안 되든 셰어를 제출하면 무조건 보상을 주기 때문에 운이 없는 경우 채굴 풀이 단기적으로 손실을 볼 수도 있는 구조라고 했다. PPLNS는 채굴 풀에서 블록이 실제로 발견될 때만 보상을 분배한다. 따라서 채굴 풀은 좀 더 안정적으로 운영할 수 있고, 채굴자들은 반대로 보상 주기가 조금 안정적이지 않을 수 있다. 채굴 풀의 운이 안 좋아서 채굴 풀에서 블록이 잘 발견되지 않으면 채굴자들은 보상을 긴 주기로 받게 될 수도 있다. 거꾸로 채굴 풀의 운이 좋아서 채굴 풀에서 블록 발견이 잘 되면 비교적 짧은 주기로 계속 보상을 받을 수 있다. PPLNS는 블록이 발견될 때 최근에 N개의 셰어를 제출한 채굴자들에게만 보상을 분배한다. 앞의 예시로 돌아와 0부터 9999까지의 카드를 뽑는 게임에서 10 이하의 카드를 뽑으면 작업증명에 성공하는 게임이 있다고 해보자. 채굴 풀

은 100 이하의 카드를 뽑으면 그 셰어를 전부 다 내라고 했다. 만약 이 채굴 풀의 참여자 중 누군가 10 이하의 카드를 뽑으면 그 셰어를 포함해 최근에 채굴 풀에 제출된 10개의 셰어를 기준으로 보상을 분배한다. 만약 내가 셰어를 찾지 못해 제출 못 하고 있다가 최근에 2개의 셰어를 제출했다면 채굴 보상의 20%를 가져가는 것이다.

PPLNS 보상 방식은 채굴 풀이 손해를 볼 가능성이 없이 안정적으로 운영이 가능하므로 수수료가 낮다. 그러나 채굴자들에게는 리스크가 있다. 만약에 계속 셰어를 많이 제출해도 이 채굴 풀에서 블록이 발견 안 되면 계속 보상을 못 받을 수도 있다. 그러다가 내가 셰어를 발견 못 하는 때에 채굴 풀에서 블록이 채굴된다면 내가 제출한 셰어에 대한 보상을 못 받을 수도 있다. 만약 내가 셰어(100 이하의 카드)를 제출했는데 채굴 풀에서 계속 10 이하의 카드를 못 찾고 11 이상 100 이하의 셰어만 제출되고 있다고 해보자. 그 뒤로 14개의 셰어가 더 제출되었을 때 비로소 채굴 풀의 누군가가 10 이하의 카드를 제출했다고 해보자. 그러면 그 카드를 포함해서 10개의 셰어만을 바탕으로 기여도를 평가하므로 마지막으로부터 15번째에 있는 내 셰어는 기여도를 평가받지 못하고 보상을 못 받게 된다. 현실적인 예시로 돌아와서, 현재 비트코인 채굴 보상이 수수료 인센티브를 합했을 때 3.2 BTC라고 해보자. 셰어 제출 가변 난이도가 일반 채굴 난이도보다 500만 배 낮다면 채굴 풀에서 블록이 발견되었을 때 최근 500만 개의 셰어에 보상이 분배된다. 이때 기여도가 평가되는 마지막 N개의 셰어(방금 예시에서는 500만 개)를 '셰어 윈도우'라고 한다.

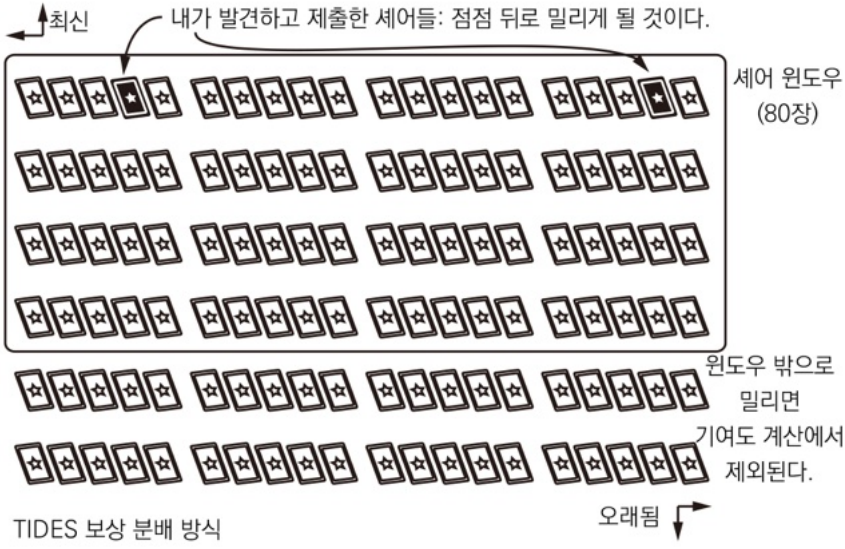


오션 풀이 최초로 도입한 TIDES 보상 방식은 채굴 풀이 운이 안 좋을 경우 채굴자들의 기여도가 사라질 수도 있는 PPLNS 보상 방식의 단점을 해결한 방식이다. TIDES는 Transparent Index of Distinct Extended Shares의 약자로, 번역하면 '각각의 확장된 셰어의 투명한 지표'이다. 좀 더 풀어쓰면 개별 셰어의 기여도를 투명하게 평가하는 보상 구조라고 할 수 있겠다.

TIDES 보상 방식은 일반적인 셰어 윈도우의 크기를 8배로 늘린 방식이다. 따라서 내가 제출한 셰어는 평균적으로 8번에 걸쳐 보상을 나누어 받게 된다.

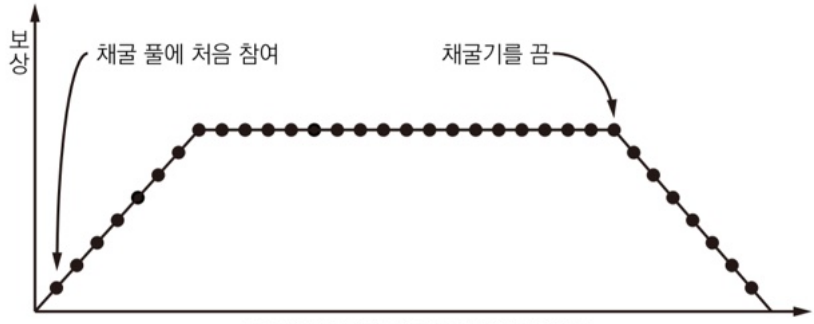
앞의 예시로 돌아와서 0부터 9999의 카드를 뽑는데, 10 이하의 카드를 뽑으면 작업증명에 성공하는 것이고, 채굴 풀은 100 이하의 카드(셰어)를 뽑으면 전부 다 내라고 했다고 해보자. 이런 상황에서는 셰어 난이도가 채굴 난이도보다 10배 더 쉬우므로 보통 셰어가 10장 제출되면 평균적으로 1번 채굴에 성공한다. PPLNS는 최근 셰어 10개에 대해 분배를 하지만, TIDES 방식은 최근 80개 셰어에 대해 분배를 한다. 만약 작업증명에 성공하면 3 BTC를 받는데, 내가 처음 이 채굴 풀에 참여해

셰어를 1개 발견했다고 해보자. 그러다가 이 채굴 풀에서 블록이 발견되면 나는 3 BTC의 80분의 1인 0.0375 BTC를 보상으로 받게 된다. 여기서 수수료를 제외하면 보통 0.037 BTC 정도를 받게 될 것이다. 그런데 이 보상을 받았다고 끝이 아니다. 셰어 윈도우의 크기가 8배이기 때문에 채굴 풀에서 다음 블록이 발견되었을 때 내가 제출한 셰어에 대한 보상 0.037 BTC를 또 받을 수 있다. 즉, 1번 제출한 셰어를 평균적으로 8번에 걸쳐 나누어 받는 것이다.



만약 내 기여도가 10%라고 해보자. 채굴 풀에 10개의 셰어가 제출될 때 그중에는 평균적으로 내 셰어가 평균적으로 1개 포함되어 있는 것이다. 주기적으로 딱딱 다른 사람들이 9개의 셰어를 제출할 때마다 내가 1개의 셰어를 제출한다고 해보자. 그러면 처음에는 채굴 풀에서 블록이 발견되면 나는 3 BTC의 80분의 1인 0.037 BTC (수수료 제외)를 받게 된다. 그런데 채굴 풀에서 다음 블록을 발견할 때는 내 셰어가

80개 중에 2개 포함되어 있다(다른 사람들이 9개의 셰어를 제출할 때 나는 1개를 제출하기 때문이다). 그러면 나는 0.074 BTC를 받게 된다. 그다음 블록을 발견할 때 나는 또 1개의 셰어를 더 제출한 상황이므로 80개 중에 내 셰어는 3개가 있다. 이런 식으로 TIDES 방식은 처음에는 보상을 적게 받다가 점점 보상을 많이 받아 일정한 수준에 이르게 된다.



TIDES 방식의 채굴 풀에 참여했을 때
시간에 따른 보상 그래프
(각각의 점은 채굴 풀에서 블록이 발견된 순간을 의미한다.)

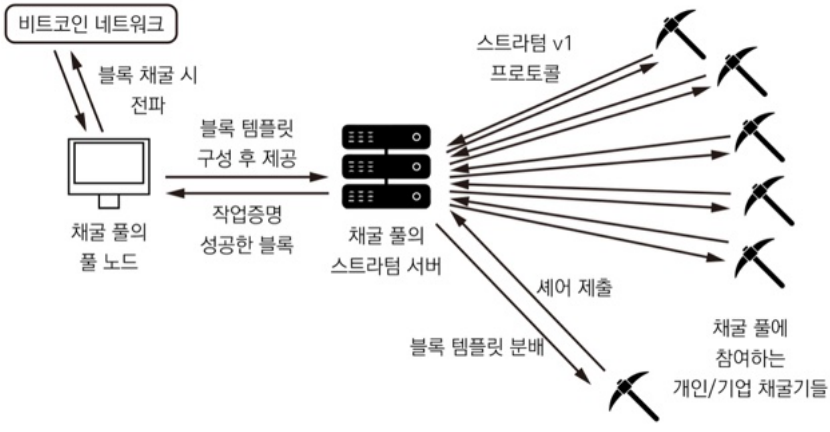
채굴 풀은 평균적으로 10개의 셰어가 제출될 때마다 한 개의 블록을 발견해야 한다. 그러나 채굴 풀이 정말 몹시 운이 안 좋으면 셰어가 80개 제출되었는데도 작업증명에 성공(10 이하의 카드를 찾는 것)을 못 할 수도 있다. 하지만 이럴 확률은 매우 희박할 것이라고 예상할 수 있다. 따라서 TIDES 방식은 PPLNS 방식과 달리 내 셰어에 대한 기여도가 사라질 가능성이 매우 낮다. 실제로 TIDES 보상 방식을 쓰는 오션 풀의 경우 내가 제출한 셰어에 대한 보상을 한 번도 못 받을 확률은 0.0335%다. TIDES 보상 방식에서 윈도우의 크기는 PPLNS의 셰어 윈

도우 크기의 8배라고 했지만, 이 크기는 비트코인의 난이도 조정 메커니즘에 따라 조금씩 변한다.

스트라텀 프로토콜

채굴 풀에 참여하려면 내 채굴기가 채굴 풀과 통신을 해야 한다. 이때 채굴기는 채굴 풀에서 지속적으로 갱신되는 블록 템플릿을 받아와야 하고, 그러면서 셰어를 계속 제출해야 한다. 블록 템플릿은 논스값이 비어 있는 아직 완성되지 않은 블록의 구조를 말한다.

비트코인 초창기에는 채굴기가 풀 노드와 직접 JSON-RPC를 통해 통신했다. 하지만 이 방식은 실시간 대량 통신에 적합하지 않다. 따라서 채굴 풀의 요구에 맞는 전용 프로토콜이 필요했다. 이 문제를 해결하기 위해 개발된 것이 스트라텀 프로토콜stratum protocol이다.

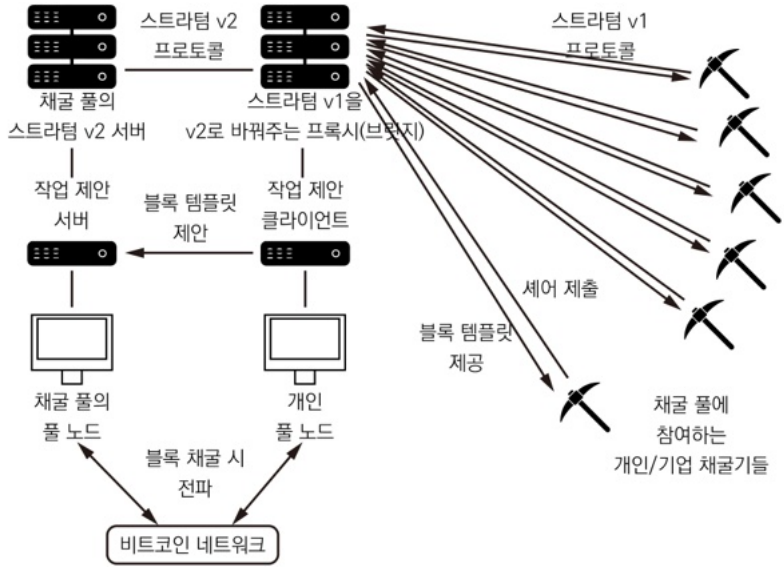


스트라텀 프로토콜은 TCP 연결을 통해 채굴기와 채굴 풀 서버가 실시간으로 데이터를 주고받는 구조다. 간단하게 설명하자면, 채굴기가 채굴 서버에 구독 요청을 보낸다. 채굴기 계정이 인증되면 채굴 풀 서버

가 채굴기에게 블록 템플릿을 계속 전송한다. 그러면 채굴기는 유효한 셰어를 제출한다.

이 과정에서 서버는 채굴기의 해시레이트에 따라 적절한 셰어 난이도를 자동으로 조절한다. 이를 가변 난이도Vardiff라고 한다. 셰어 난이도를 조절하지 않는 경우를 생각해 보자. 채굴기의 해시레이트에 비해 셰어 제출 난도가 너무 낮으면(쉬우면) 셰어를 너무 자주 제출해서 서버에 과부하가 걸릴 수 있고, 셰어 제출 난도가 너무 높으면(어려우면) 셰어를 거의 못 내서 기여도 측정이 제대로 안 될 것이다. 그래서 기본 난도부터 시작해서 셰어 제출 빈도를 기반으로, 가변 난도를 점진적으로 조절한다.

처음 등장한 스트라텀 프로토콜을 스트라텀 v1이라 하는데, 여기에는 몇 가지 문제점이 있다. 먼저 TCP 통신 과정이 암호화되어 있지 않다. 따라서 중간자 공격에 취약하다. 또한 채굴자에게 블록 템플릿 구성 권한이 없으므로 채굴 중앙화 문제가 있다. 스트라텀 v1은 BIP 제안 없이 비공개적으로 개발되었기 때문에 이러한 문제점들이 있었던 것이다. 그래서 스트라텀 v2가 등장했는데 DEMAND 풀에서 최초로 스트라텀 v2 방식을 도입했다. 스트라텀 v2부터는 암호화된 통신을 지원한다. 채굴자가 풀 노드를 운영할 경우 블록 템플릿 구성 권한을 직접 가져올 수도 있고, 다른 노드에게서 블록 템플릿을 받아올 수도 있다. 하지만 스트라텀 v2는 기존에 중앙화 채굴 모델이었던 스트라텀 v1을 개선하여 나온 것이기 때문에 비효율이 존재했고, 이 때문에 처음부터 채굴 분산화를 위해 설계된 다텀 프로토콜이 등장했다. 이에 대해서는 바로 다음 절에서 자세히 알아보자.



채굴 풀의 한계

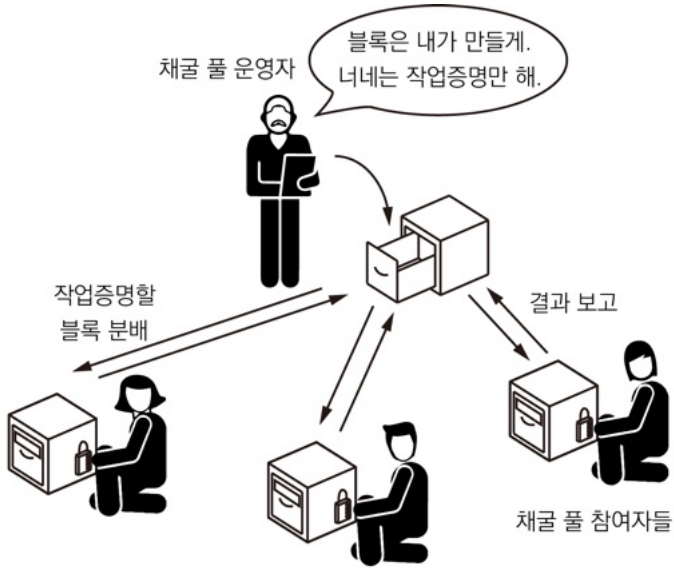
채굴 풀은 간접민주주의(대의민주주의)와도 같다. 간접민주주의는 개인들이 선거를 통해 입법자를 뽑으면, 입법자가 법을 제정하는 권한을 갖는 형태를 말한다. 간접민주주의의 단점은 명확하다. 일단 선출된 입법자가 시민들의 의지에 반하는 법들을 마구 입법할 수 있기 때문이다. 따라서 간접민주주의는 진정한 민주주의라기 보다는 효율성과 어느 정도 타협한 민주주의라고 할 수 있다. 역사 속에서 많은 선출자들이 간접민주주의의 한계를 이용하여 독재로 전환했다. 로마의 카이사르나 나치의 히틀러 모두 정당한 선출 과정을 통해 선출된 뒤, 자신들의 독재를 위한 법을 입법하여 민주주의를 훼손하였다.

채굴 풀도 간접민주주의 형태와 같다. 채굴자들은 어떤 채굴 풀에 참여할지 선택할 수 있다. 그러나 일단 채굴 풀에 참여하고 나면 블록의

구성 권한은 채굴 풀 운영자가 모두 갖게 된다. 채굴 풀에 참여한 채굴자는 채굴 풀 운영자가 만든 블록 템플릿을 수동적으로 받을 수밖에 없다. 그 블록 템플릿에서 논스값만을 변경해 보며 작업증명을 한다.

만약 채굴 풀 운영자가 비트코인 네트워크에 해가 되는 블록을 구성했다고 해보자. 그러면 해당 채굴 풀에 참여한 채굴자들은 그 블록을 채굴할 것이다. 그런 사실이 밝혀지면 해당 채굴 풀에 참여하고 있는 채굴자들은 다른 채굴 풀로 옮기고, 풀 노드들은 그 블록을 거부할 수 있다. 그렇다고는 해도 일단 이런 일이 일어나면 네트워크 분리가 일어나는 등 네트워크 불안이 야기될 수 있다. 채굴자들의 소중한 해시레이트가 악의적인 블록 생성에 쓰일 수도 있는 것이다.

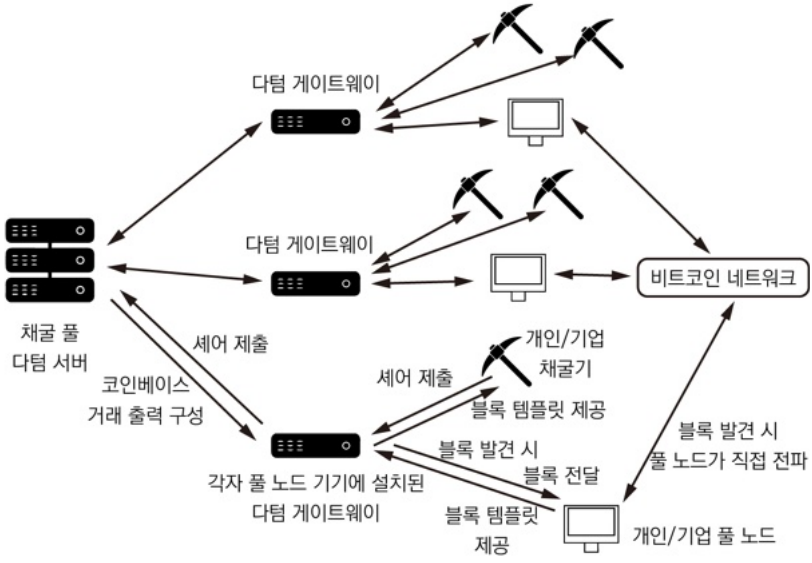
솔로 채굴도 마찬가지다. 대부분의 솔로 채굴자들은 CK풀이나 퍼블릭 풀에 참여하는데, 이것도 채굴 풀이다. 블록을 채굴한 당사자가 보상의 대부분을 가져가는 솔로 채굴 보상 방식일 뿐이다. 보상의 '전부'가 아니라 '대부분'이라고 한 이유는 채굴 풀이 수수료 명목으로 전체 블록 보상의 1-3% 정도를 가져가기 때문이다. 당연히 블록의 구성 권한은 CK풀이나 퍼블릭 풀에게 있다. CK풀이나 퍼블릭 풀에 참여하는 솔로 채굴자들은 채굴 풀 운영자가 악의적인 블록을 생성하지 않을 것이라는 신뢰에 기대야 한다. 물론 이런 방식이 아니라 자신의 풀 노드가 직접 블록 템플릿을 구성하고 솔로 채굴을 할 수 있게 해주는 퍼블릭 풀의 오픈 소스 소프트웨어도 있다.



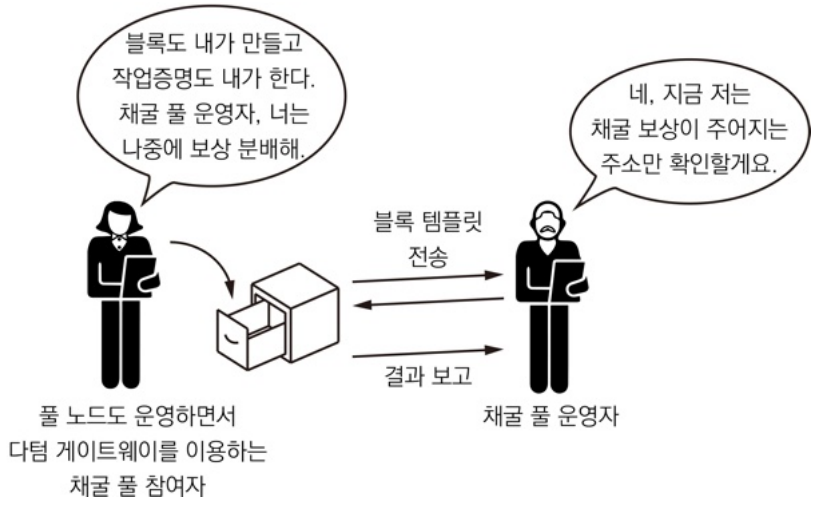
다텀과 채굴 주권

그렇다면 채굴 주권을 지키기 위해서는 직접 풀 노드를 돌려 퍼블릭 풀 소프트웨어를 이용해 자신의 채굴기와 연결하고, 솔로 마이닝을 하는 방법밖에 없을까? 보상을 분배하는 채굴 풀에 참여하고 싶다면 채굴 주권을 포기해야 할까? 이 문제를 해결하기 위해 다텀DATUM이 나왔다.

다텀은 자신의 풀 노드가 직접 블록 템플릿을 구성할 수 있게 해준다. 채굴기는 다텀을 이용해 풀 노드와 연결된다. 그러면 채굴기는 풀 노드가 만든 블록 템플릿을 이용해 채굴할 수 있게 된다. 만약 다텀의 개념이 여기서 끝났다면 보상을 분배하는 채굴 풀은 불가능하고, 솔로 채굴만 가능했을 것이다.



보통 채굴 풀이 블록 템플릿의 구성 권한을 갖는 이유는 채굴 보상이 지급될 주소 설정 때문이다. 일단 채굴 보상이 채굴 풀에게 주어져야 채굴 풀이 채굴자들에게 보상을 분배할 수 있다. 따라서 다텀은 채굴 풀이 코인베이스 거래(채굴 보상이 주어지는 거래)를 구성할 수 있는 권리를 갖게 할 수 있다. 채굴자들이 돌리는 풀 노드에서 블록 템플릿이 만들어지면, 그 블록 템플릿은 먼저 오션 풀이라는 채굴 풀로 간다. 오션 풀은 채굴 보상이 주어지는 코인베이스 보상 주소만 수정하고 다시 풀 노드의 다텀 앱으로 보낸다. 그러면 다텀은 비로소 채굴기에게 블록 템플릿을 보내주고, 채굴기가 그 블록 템플릿으로 채굴하게 되는 것이다. 채굴기가 채굴하면서 얻은 결과는 다시 다텀을 이용해 채굴 풀에게 보내진다. 정리하면, 다텀은 블록의 구성 권한을 채굴자(채굴자가 돌리는 풀 노드)가 갖되, 채굴 보상 주소만 채굴 풀이 바꿀 수 있도록 허용한다.



홈 채굴의 의미

공장처럼 거대한 규모로 돌아가는 대형 채굴장을 생각해 보자. 냉각 설비를 갖춘 데이터 센터, 저렴한 전력 공급 계약, 대규모 장비 투자. 이와 비교하여 가정에서의 소규모 채굴은 상대적으로 이익이 적다. 홈 채굴은 산업용 전기보다 비싼 전기 요금을 지불해야 하고 냉각 환경도 열악하며, 장비의 유지·보수에도 어려움이 따른다. 따라서 수익을 내는 것은 노하우가 필요한 일이다.

수익을 기대하기보다 손해를 최소화하며 채굴하는 것으로 관점을 바꿔볼 수도 있다. 겨울철 난방 대용으로 채굴기를 이용하거나, 재생 에너지를 이용한 자가발전 설비와 연계할 수도 있다. 이러한 자가발전은 특히 중요한데, 에너지 생산도 개인이 자율적으로 하는 첫걸음이 되기 때문이다. 또한 다텀을 통해 자신의 풀 노드와 채굴기를 연결하여 좀 더 독립적으로 채굴할 수도 있다. 이러한 홈 채굴자들은 비트코인 네트워

크에서 매우 중요하다. 이들 각각의 해시레이트가 미약하다고 하더라도, 이들이 네트워크에 기여하는 것은 무시할 수가 없다. 이들은 채굴 풀이 비트코인 사용자에게 도움이 되지 않는 내용들을 지지하거나 거래들을 검열할 경우 얼마든지 다른 채굴 풀로 이동할 수가 있다. 따라서 채굴 풀의 중앙화를 견제한다. 게다가 다텀을 통해 자신의 풀 노드와 채굴기를 연결하는 경우 채굴이 분산화되어 네트워크 전체의 자율성이 올라간다.

채굴은 비트코인 네트워크를 보호하는 행위다. 따라서 홈 채굴자들은 자신이 직접 에너지를 써서 네트워크를 보호하는 사람들이다. 또한, 중앙화된 권력 없이 비트코인이 만들어지는 데 기여한다. 이러한 행위는 단순한 이윤 논리를 넘어선 진정한 금융 주권의 실천이다.

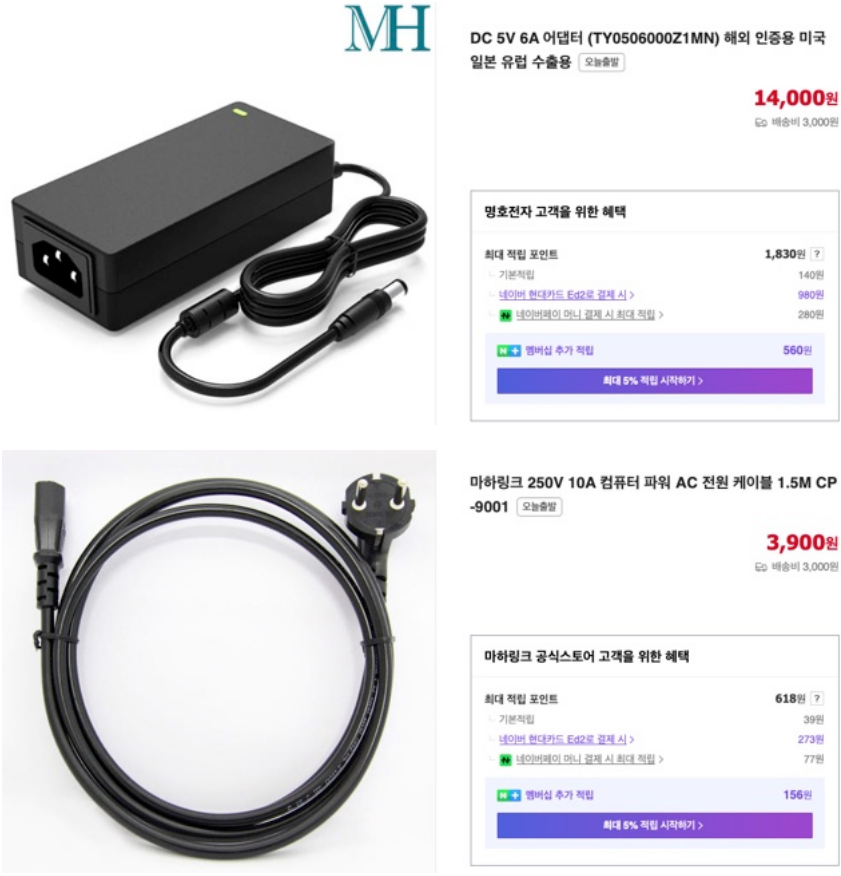
| 비트엑스 감마 601로 솔로 채굴하기, 채굴 풀 참여하기

준비물

1. 비트엑스 감마 601 (스탠드 포함)

2. 5V 30W 이상 전원선

비트엑스 감마 601은 전압 5V에 20W 이상 안정적인 전력 공급이 필요하다. 따라서 5V에 6A 정도 되는 어댑터가 필요하다. 멀티플러그 어댑터(돼지코)를 쓰는 것은 개인적으로 추천하지 않는다. 채굴기는 무엇보다 안정적인 전력 공급이 중요한데 멀티플러그 어댑터가 헐거운 경우 전력이 안정적으로 공급되지 않을 수 있다. 그러면 채굴기까지 망가질 수 있다. 따라서 한국형 플러그에 사용 가능한 5V 6A 어댑터를 따로 구해서 사용하는 것을 추천한다. 다음 사진을 참고하라.

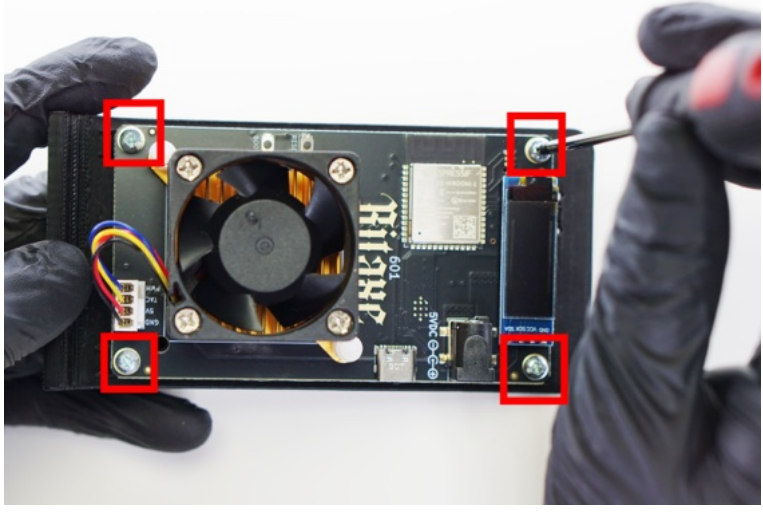


3. 스마트폰, PC

비트엑스를 설정할 때 스마트폰이 필요하다. 펌웨어 업데이트 등을 할 때는 PC가 있는 것이 편하다.

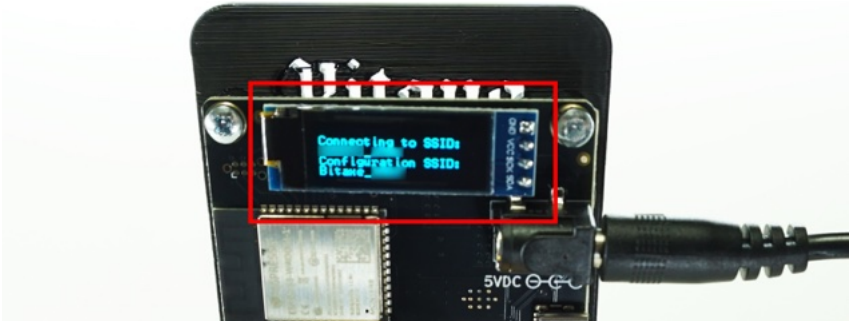
비트엑스 스탠드 조립 및 전원 연결

스탠드가 있다면 먼저 스탠드 조립을 해주자. 다음 사진에 보이는 네 귀퉁이에 나사를 돌려 연결해 주면 된다.



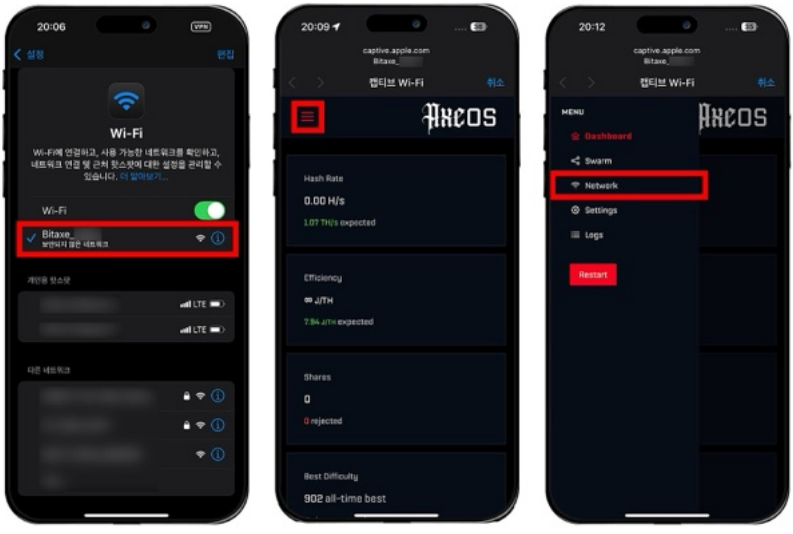
이제 전원을 연결한다.

처음에 전원을 연결하면 LCD 화면에 여러 가지 정보들이 뜨며 지나갈 것이다.



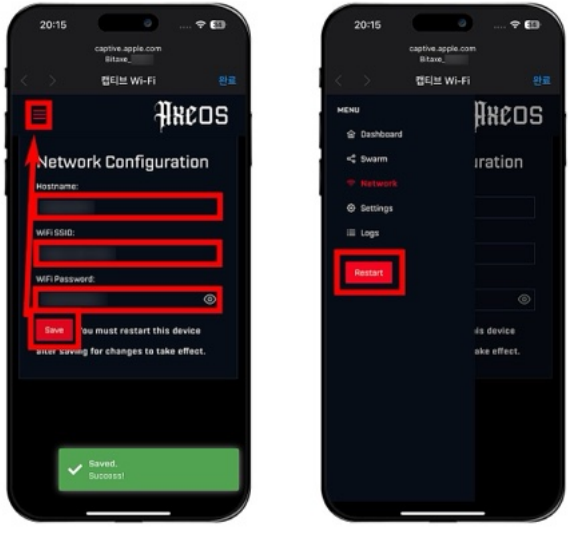
비트엑스 네트워크 연결

비트엑스를 와이파이에 연결해 보자. 연결할 와이파이는 2.4GHz여야 하고, 5GHz와 통합되어 있는 스마트 와이파이면 안 된다. 스마트폰의 와이파이 설정 창에서 Bitaxe_???? 로 되어 있는 와이파이를 연결한다. 그러고 왼쪽 위 메뉴 버튼 → [Network]를 누른다.



'Hostname'은 아무거나 입력해도 된다. 'WiFi SSID'는 연결할 와이파이 이름을 입력하면 된다. 집에서 쓰는 2.4GHz 와이파이 이름을 입력한다. 이때 대소문자, 공백 등 오타에 주의하여 입력한다. 'WiFi Password'에는 입력한 와이파이의 비밀번호를 입력하면 된다.

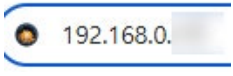
그다음 [Save]를 누르고 왼쪽 위 메뉴 버튼 → [Restart]를 누른다. 비트엑스는 항상 설정 변경 후 [Restart]까지 눌러야 변경한 설정이 저장된다.



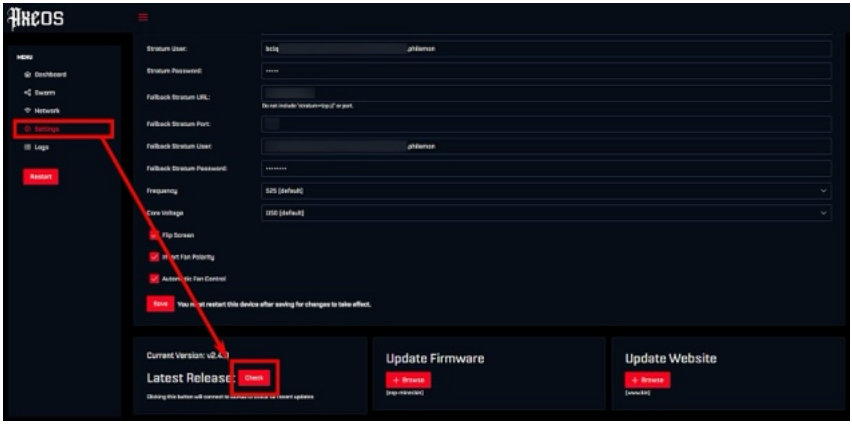
비트엑스 펌웨어 업데이트

와이파이에 성공적으로 연결되면 로컬 IP 주소가 할당된다. 비트엑스의 LCD 화면을 보면 로컬 IP 주소가 나온다. 이것을 먼저 확인한다.

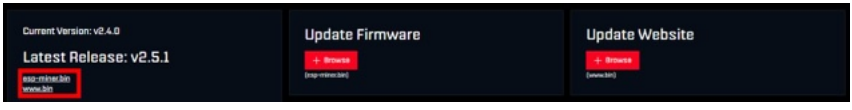
인터넷 주소창에 로컬 IP 주소를 입력한다.



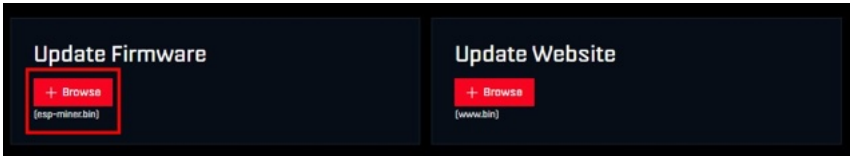
왼쪽의 [Settings] 탭으로 들어가 스크롤을 맨 아래로 내린다. 'Latest Release' 옆에 있는 [Check]를 누른다. (2.5.0보다 최신 버전일 경우 왼쪽의 [Update] 탭을 누르고 똑같이 진행하면 된다.)



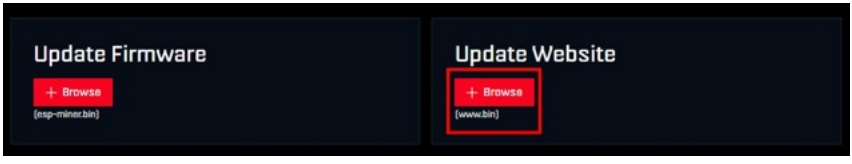
최신 버전이 아니라면 아래 펌웨어 파일을 다운로드할 수 있는 링크가 나타난다. esp-miner.bin 파일과 www.bin 파일 둘 다 다운로드한다.



'Update Firmware' 아래 있는 [Browse]를 누른다. 그다음 esp-miner.bin 파일을 선택한다.



'Update Website' 아래 있는 [Browse]도 누른다. 그다음 www.bin 파일을 선택한다.



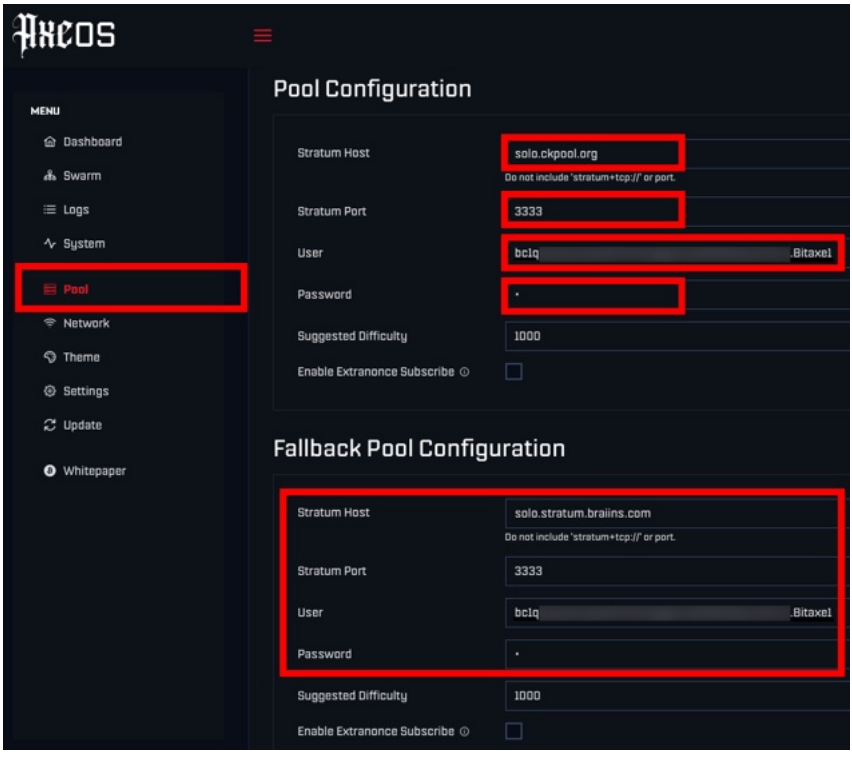
다 되었으면 [Save]를 누르고 [Restart]를 누른다.

솔로 채굴 설정하기(ckpool)

풀 노드가 없는데 솔로 채굴을 하려는 경우 '솔로 풀'을 이용해야 한다. 솔로 풀에는 대표적으로 'ckpool'과 '퍼블릭 풀'이 있다. 여기서는 ckpool을 이용해 솔로 채굴 설정하는 방법을 알아보자.

[Pool] 탭에 들어간다. 'Stratum Host'에는 solo.ckpool.org를 입력한다. 'Stratum Port'에는 3333을 입력한다. 'User'에는 '보상을 받을 비트코인 주소.채굴기 이름(자기 마음대로)'을 입력하면 된다. 채굴기 이름 없이 비트코인 주소만 입력해도 된다. 여기서 비트코인 주소에 오타가 나면 블록을 채굴해도 보상이 엉뚱한 곳으로 갈 수 있으니 꼭 잘 확인하자. 'Password'에는 영어 소문자 'x' 한 글자를 입력하면 된다.

그 아래에 'Fallback Pool Configuration'으로 똑같은 입력창이 있다. 이 부분은 만약 입력한 풀과 제대로 연결이 안 될 경우에 대비해 다른 연결할 곳을 입력하는 칸이다.



입력했다면 스크롤을 내려 [Save]를 누르고 [Restart]를 누른다. 꼭 [Restart]까지 누르자.

이전에는 ckpool이 솔로 풀 중 네트워크 연결이 안정적이라는 평이 많았다. 그런데 최근 ckpool 네트워크 연결이 안정적이지 못해 다른 풀

에 연결해야 했던 사례가 있었다. 그럴 경우 다음 솔로 풀 중 선택해서 연결하면 된다.

ck풀

Stratum Host: solo.ckpool.org

Stratum Port: 3333

User: 보상받을 비트코인 주소(.채굴기 이름-선택사항)

Password: x (영어 소문자)

다음 링크에서 확인: https://solo.ckpool.org/

퍼블릭 풀

Stratum Host: public-pool.io

Stratum Port: 21496

User: 보상받을 비트코인 주소(.채굴기 이름-선택사항)

Password: x (영어 소문자)

다음 링크에서 확인: https://web.public-pool.io/#/

브레인스 솔로 풀

Stratum Host: solo.stratum.braiins.com

Stratum Port: 3333

User: 보상받을 비트코인 주소(.채굴기 이름-선택사항)

Password: x (영어 소문자)

다음 링크에서 확인: https://solo.braiins.com/stats

익명 솔로 풀

Stratum Host: stratum.solomining.io

Stratum Port: 7777

User: 보상받을 비트코인 주소(.채굴기 이름-선택사항)

Password: x (영어 소문자)

다음 링크에서 확인:

https://btc.solomining.io/#statMining

채굴 풀 참여하기(브레인스 풀)

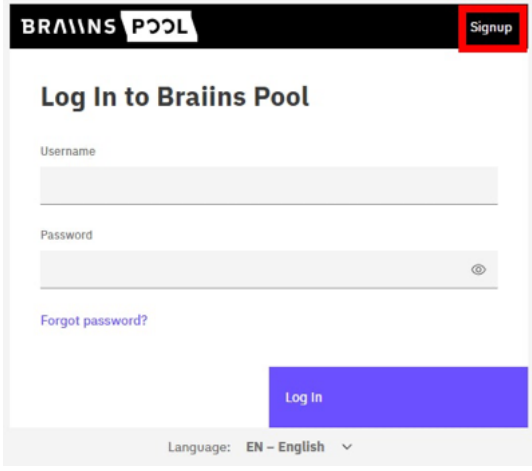
솔로 채굴보다는 꾸준히 비트코인이 들어오는 것을 원하는 사람도 있을 것이다. 그런 경우 채굴 풀에 참여하면 된다. 채굴 풀은 여러 사람이 모여 블록을 채굴하고, 기여도에 따라 보상을 나눠 갖는 구조다.

이번에는 브레인스 풀에 참여하는 방법을 알아보자. 브레인스 풀은 비트코인 최초의 채굴 풀이다. 예전에 처음 등장했을 때는 이름이 슬러시 풀이었는데 브레인스 풀로 이름을 바꿨다. 브레인스 풀은 라이트닝 네트워크로 비트코인 보상을 받는 것도 가능하다.

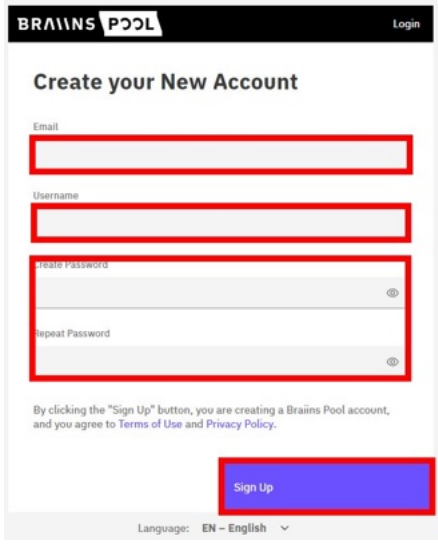
먼저 브레인스 풀에 가입해 보자. 이메일을 이용해 가입할 것이다. 다음 링크에 접속한다.

https://pool.braiins.com/login

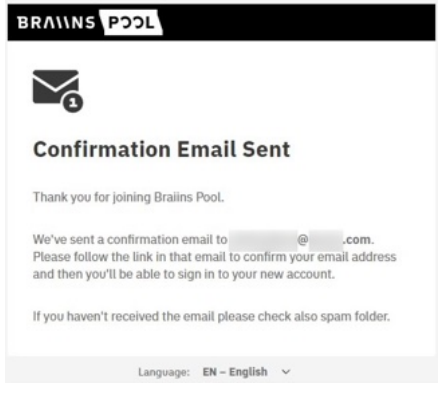
오른쪽 위 [Signup(회원가입)] 버튼을 누른다.



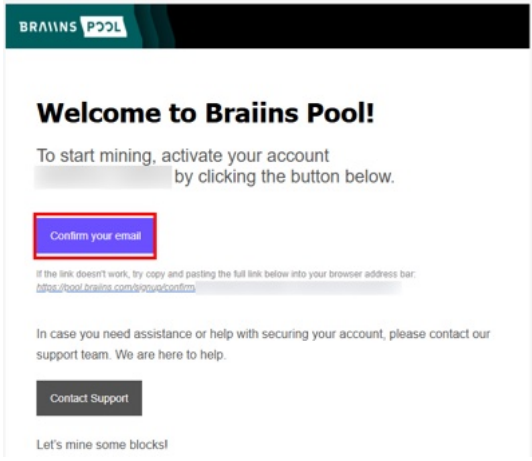
'Email'에는 인증을 받을 이메일을 입력한다. 'Username'에는 닉네임을 입력하면 된다(참고로 브레인스 풀은 로그인할 때 이메일이 아니라 유저네임과 비밀번호로 로그인한다). 'Create Password'와 'Repeat Password'에는 똑같은 비밀번호를 입력하면 된다.



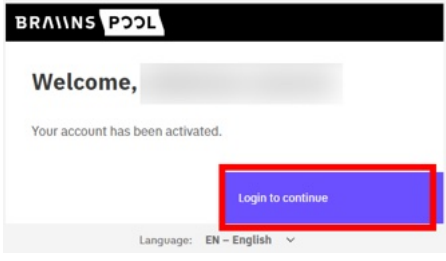
그러면 인증 이메일이 발송되었다는 안내창이 뜬다.



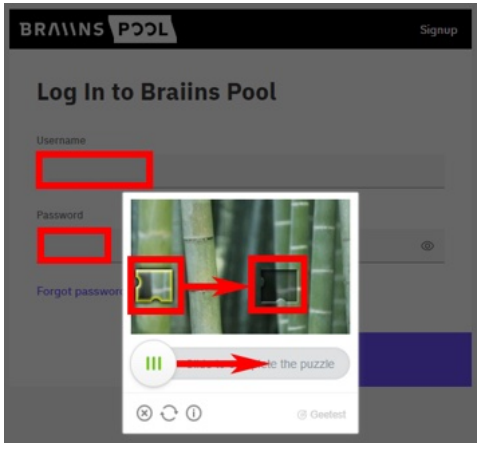
이메일에 로그인하고 메일함을 보면 다음과 같은 이메일이 와있는 것을 볼 수 있다. [Confirm your email]을 누른다.



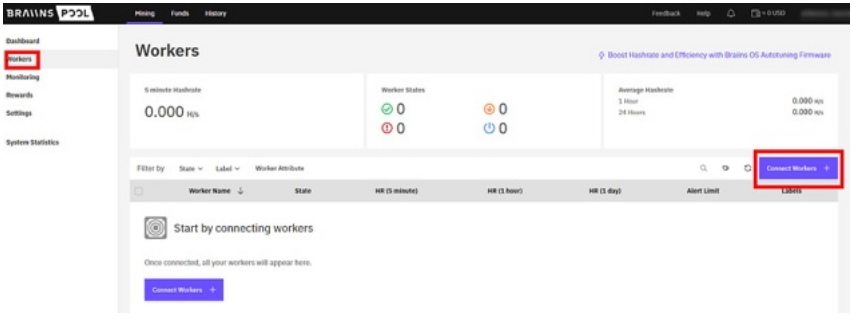
그러면 브레인스풀 웹사이트로 이동될 것이다. [Login to continue]를 누른다.



로그인 정보를 입력한다. 이때 이메일이 아니라 Username (닉네임)을 입력해야 한다. 퍼즐을 풀라는 창이 뜨면 슬라이드 버튼을 움직여 퍼즐을 푼다.



왼쪽 탭에서 [Workers]를 누르고 [Connect Workers]를 누른다.



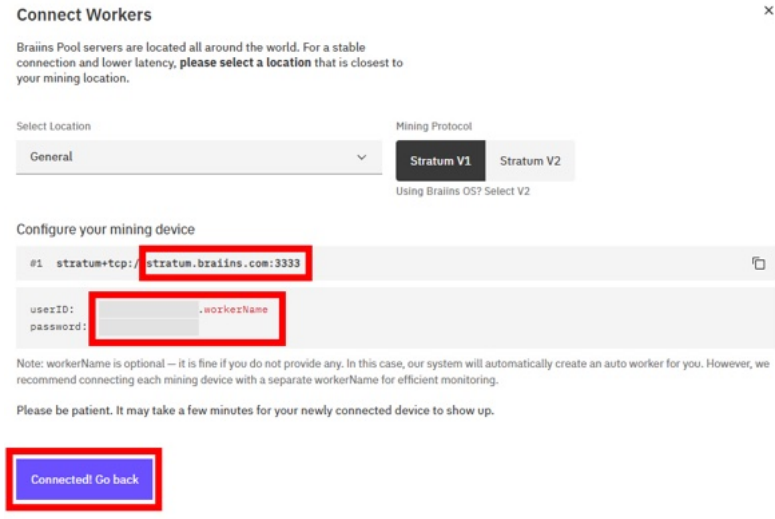
그러면 입력해야 하는 정보들이 뜰 것이다. 다음 정보들을 비트엑스 설정 창에 그대로 입력한다.

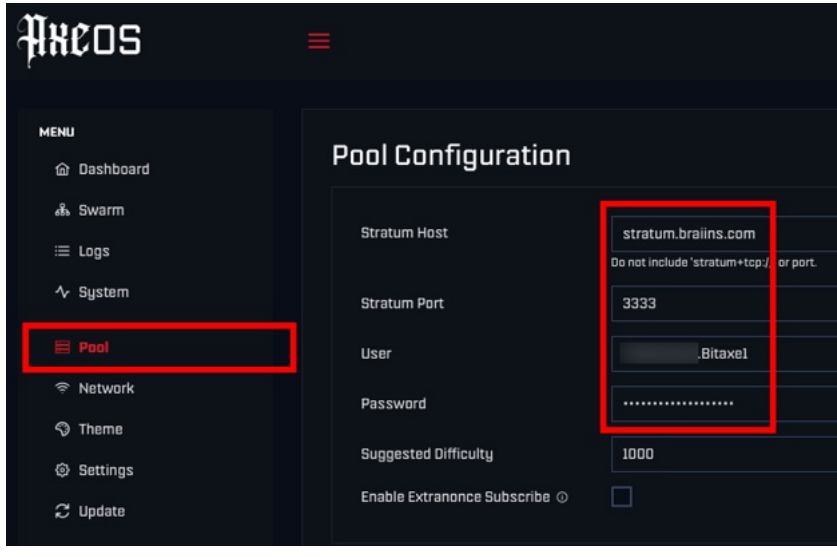
Stratum Host: stratum.braiins.com

Stratum Port: 3333

User: 브레인스 풀 userID에 쓰여 있는 내용(.채굴기 이름-선택사항)

Password: 브레인스 풀 password에 쓰여 있는 비밀번호





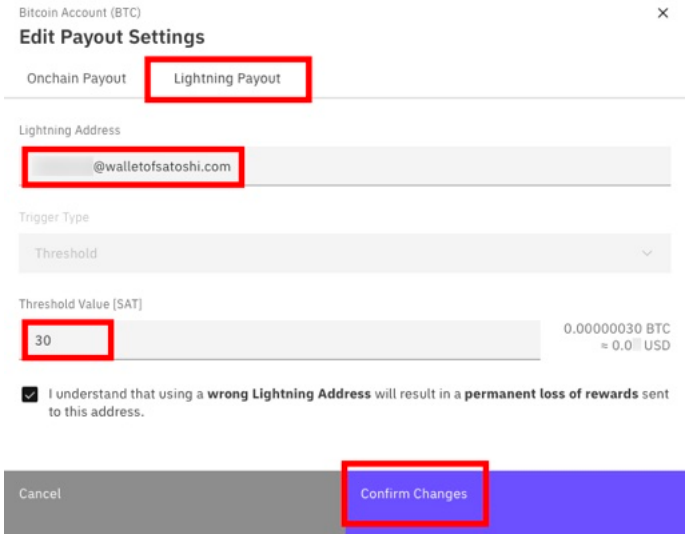
다 되었으면 [Save]를 누르고 [Restart]를 누른다.

이제 시간이 좀 지나 채굴기가 셰어를 제출하면 브레인스 채굴 풀에 채굴기가 연결되었을 것이다.

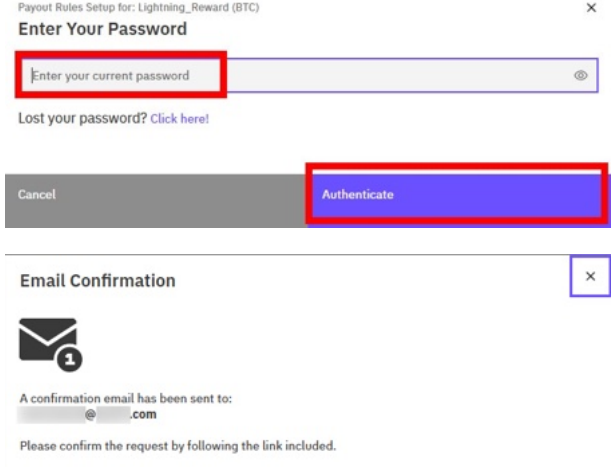
라이트닝 네트워크로 보상받기(브레인스 풀)

이제 보상받는 방식을 설정해 보자. 상단 [Funds] 탭을 누르고 'Payout rule' 아래에 있는 [Set up]을 누른다.

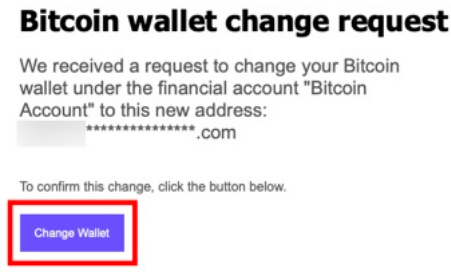
그러면 보상받는 방법을 설정하는 창이 나온다. 여기서 [Lightning Payout]을 누른다. 'Lightning Address'에는 보상을 받을 라이트닝 주소를 입력한다. 'Threshold Value'는 해당 금액(sats) 이상이 쌓이면 라이트닝 주소로 보상을 받겠다는 뜻이다. 너무 적은 금액으로 설정하면 너무 자주 라이트닝 보상을 받게 될 것이고, 너무 큰 금액으로 설정하면 보상을 너무 느리게 받게 되니 적당한 금액을 설정하자.



[Confirm Changes]를 누르면 비밀번호를 입력하는 창이 뜬다. 비밀번호를 입력하고 [Authenticate]를 누르면 이메일 인증을 위해 이메일을 보냈다는 안내문이 뜬다.



이메일을 확인하면 인증 이메일이 와있을 것이다. [Change Wallet]을 누르면 인증이 완료된다.



이메일 인증까지 마쳤다면 이제 설정한 사토시가 쌓일 때마다 채굴 보상이 들어올 것이다.

| 아발론 나노 3로 솔로 채굴하기, 채굴 풀 참여하기

준비물

1. 아발론 나노 3

2. 28V 5A C타입 한국형 플러그 어댑터

아발론 나노 3의 전원 규격은 28V에 최대 140W (5A)다. 보통 유럽형 플러그 어댑터가 함께 오는데 이것을 사용하는 것은 추천하지 않는다. 채굴기는 무엇보다 안정적인 전력 공급이 중요한데 플러그가 헐거운 경우 전력이 안정적으로 공급되지 않을 수 있다. 그러면 채굴기까지 망가질 수 있다. 따라서 한국형 플러그에 사용 가능한 28V 5A 어댑터를 따로 구해서 사용하는 것을 추천한다. 140W C타입 어댑터는 노트북 어댑터 중에 많이 있다. 다음 사진을 참고하라.

3. 스마트폰, PC

아발론 나노 3를 설정할 때 앱을 설치해야 하므로 스마트폰이 필요하다.

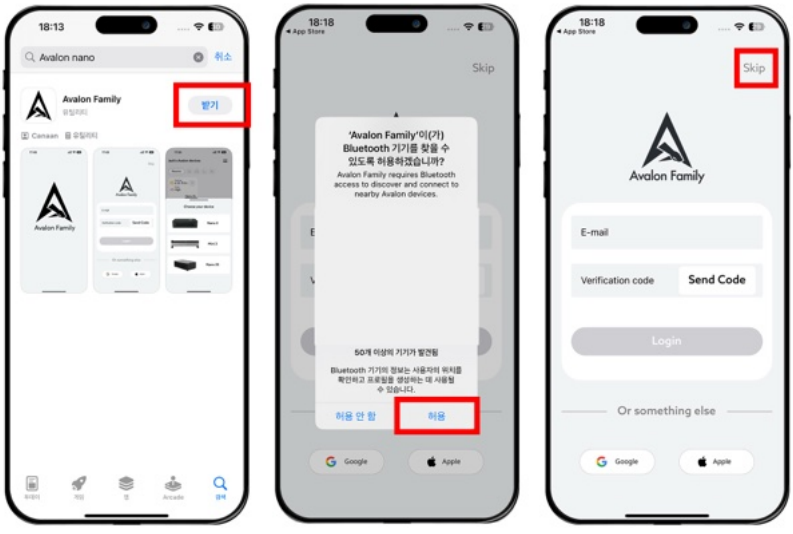
아발론 나노 3 전원 연결

어댑터에는 Type-C1 선을 꽂는다. 반대쪽은 아발론 나노 3에 선을 꽂는다.

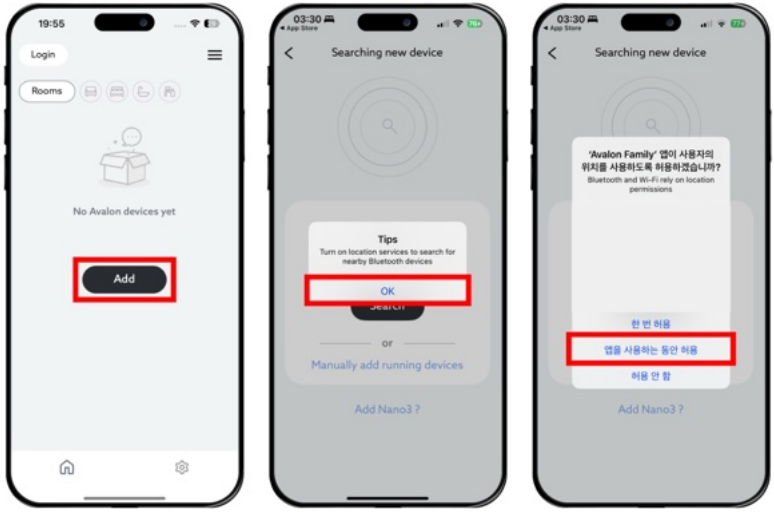
그러면 전원이 들어온다.

아발론 나노 3 설정하기

아발론 나노 3는 앱을 이용하면 쉽게 설정할 수 있다. 앱스토어에서 'Avalon Family'를 검색해 앱을 다운로드한다. 블루투스 연결을 [허용]한다. 오른쪽 위에 있는 [Skip]을 누른다.

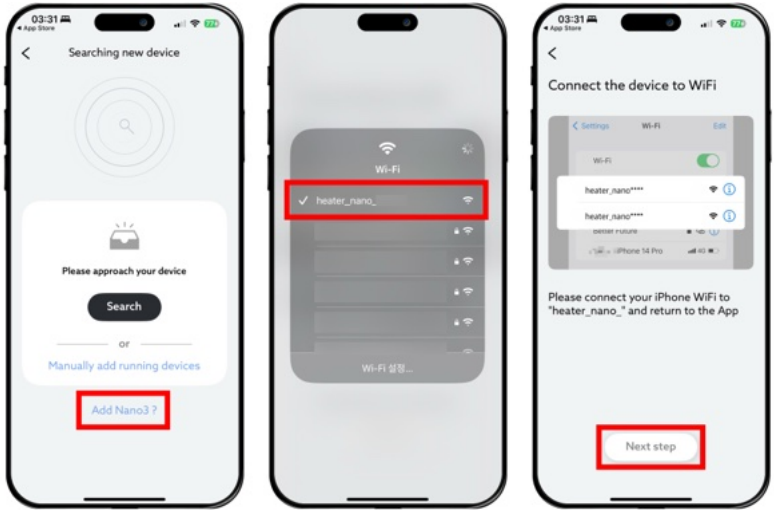


[Add]를 누른다. 앱이 위치 사용 권한을 요청하면 허용한다.

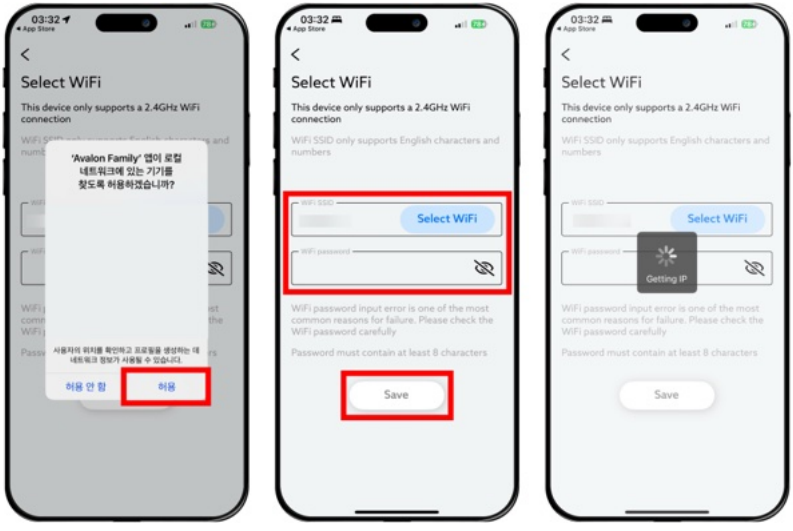


우리는 나노 3를 연결할 것이므로 [Add Nano3?]를 누른다. 다른 모델인 경우 [Search]를 누르면 된다.

그다음에 와이파이 설정에 들어가서 [heater_nano_????]를 누른다. 선택했으면 앱으로 돌아와 [Next step]을 누른다.

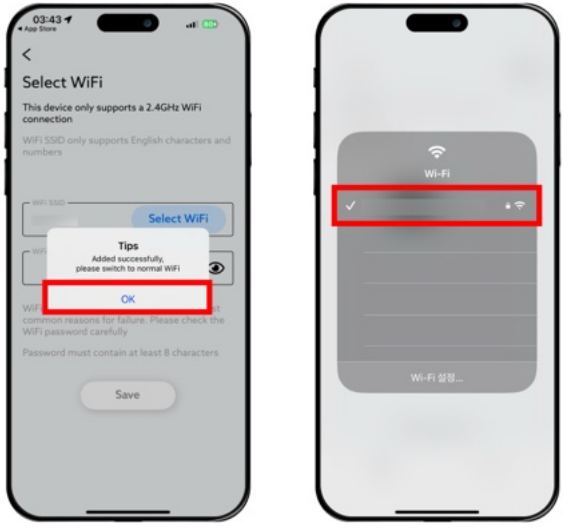


[Select WiFi]를 누르고 집에서 사용하는 와이파이를 선택한다. 로컬 네트워크 기기 검색 권한을 요청하면 허용한다. 이때 와이파이는 2.4GHz여야 하고, 5GHz와 통합되어 있는 스마트 와이파이면 안 된다. 와이파이를 선택하고 와이파이 비밀번호까지 입력했으면 [Save]를 누른다.

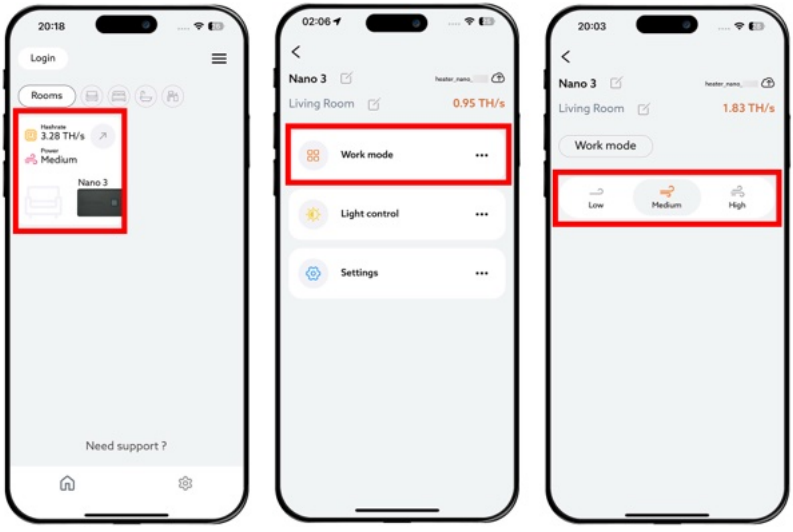


잘 연결되었다는 안내문이 뜰 것이다. 만약 연결에 실패하면 스마트폰의 와이파이가 [heater_nano_????]로 연결되었는지 확인해 보고, 처음부터 다시 시도해 보자. 연결이 되었다면 다시 원래 집에서 사용하는 와이파이를 연결한다.

잘 연결되었다면 아발론 기기를 선택할 수 있다. 앱에서 기기를 선택하고 [Work mode]에 들어간다. 여기서 채굴 모드를 설정할 수 있다. [High]는 기기 온도를 정말 차갑게 관리하지 않으면 기기가 금방 망가진다. 아발론 나노 3의 경우 특히 이런 사례가 많으니 조심하자. [Medium]이나 [Low]를 선택하는 것이 좋다. [High]는 전력을 많이 쓰며 비트코인 해시레이트가 올라가고, 반대로 [Low]는 전력을 적게 쓰며 해시레이트가 내려간다.



참고로 'Light control'에서 불빛 색상도 변경 가능하다. 은은하고 따듯한 주황색 조명으로 해놓으면 기분이 좋아진다.

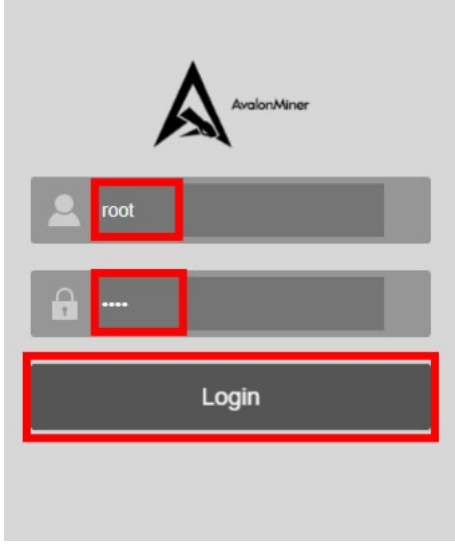


솔로 채굴 설정하기(ckpool)

지금부터는 컴퓨터에서 설정을 해보도록 하겠다. 모바일 앱에서 계속 설정하는 것도 가능하다(모바일의 경우 [Settings] → [Pool Config]에 들어가면 된다).

와이파이에 성공적으로 연결되었다면 아발론 기기에 로컬 IP 주소가 할당되었을 것이다. 아발론의 LCD 화면을 보면 화면이 넘어가다가 이 로컬 IP 주소가 나올 것이다. 컴퓨터에서 로컬 IP 주소를 인터넷 주소창에 입력한다.

처음에 어떤 입력창이 나타난다. 초기에는 ID와 비밀번호 둘 다 'root'이다.

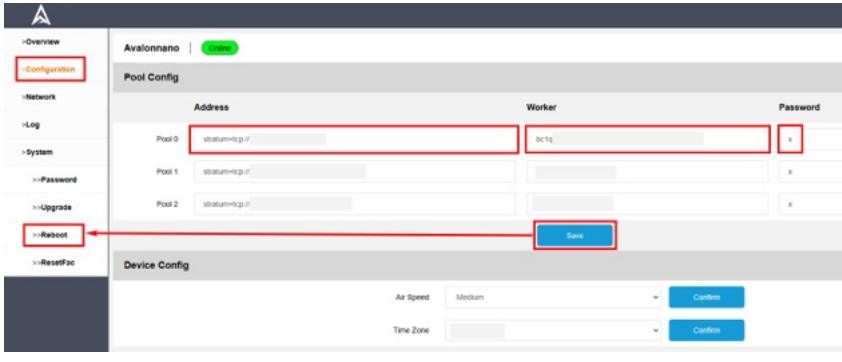


왼쪽 탭에서 [Configuration]을 선택한다. Pool 0과 Pool 1, Pool 2가 있다. 기본적으로는 Pool 0에 입력하면 된다. Pool 1은 Pool 0과의 연결에 실패했을 때 연결하는 것이고, Pool 1도 연결에 실패하면 Pool 2와 연결을 시도한다.

풀 노드를 돌리지 않는 경우 솔로 채굴을 하기 위해서는 솔로 풀에 참여해야 한다. 대표적인 솔로 풀인 'ckpool'에 참여하는 방법을 알아보겠다.

'Address'에는 stratum+tcp://solo.ckpool.org:3333을 입력한다. 'Worker'에는 '채굴 보상받을 주소(.채굴기 이름-선택 사항)'를 입력한다. 이때 보상받을 주소에 오타가 나지 않도록 주의하자. 오타가 나면 채굴에 성공했는데도 엉뚱한 주소로 보상이 갈 수 있다. 'Password'는 영어 소문자로 'x' 한 글자 입력하면 된다.

입력했다면 [Save]를 누르고 [Reboot]를 누른다. 꼭 [Reboot]까지 눌러야 설정이 저장된다.



이전에는 ckpool이 솔로 풀 중 네트워크 연결이 안정적이라는 평이 많았다. 그런데 최근 ckpool 네트워크 연결이 안정적이지 못해 다른 풀

에 연결해야 했던 사례가 있었다. 그럴 경우 다음 솔로 풀 중 선택해서 연결하면 된다.

ck풀

Address: stratum+tcp://solo.ckpool.org:3333
Worker: 보상받을 비트코인 주소(.채굴기 이름-선택사항)
Password: x (영어 소문자)
다음 링크에서 확인: https://solo.ckpool.org/

퍼블릭 풀

Address: stratum+tcp://public-pool.io:21496
Worker: 보상받을 비트코인 주소(.채굴기 이름-선택사항)
Password: x (영어 소문자)
다음 링크에서 확인: https://web.public-pool.io/

브레인스 솔로 풀

Address: stratum+tcp://solo.stratum.braiins.com:3333
Worker: 보상받을 비트코인 주소(.채굴기 이름-선택사항)
Password: x (영어 소문자)
다음 링크에서 확인: https://solo.braiins.com/stats

익명 솔로 풀

Address: stratum+tcp://stratum.solomining.io:7777

Worker: 보상받을 비트코인 주소(.채굴기 이름-선택사항)

Password: x (영어 소문자)

다음 링크에서 확인:

https://btc.solomining.io/#statMining

채굴 풀 참여하기(브레인스 풀)

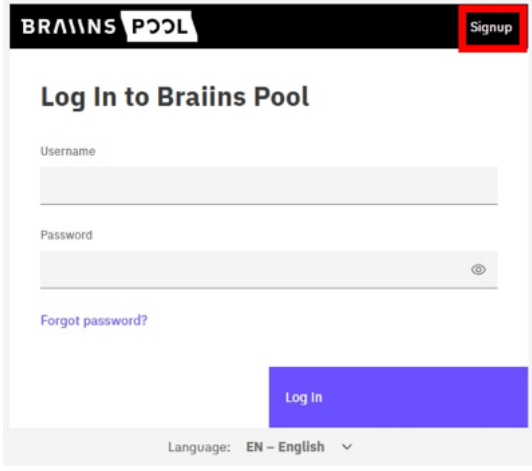
솔로 채굴보다는 꾸준히 비트코인이 들어오는 것을 원하는 사람도 있을 것이다. 그런 경우 채굴 풀에 참여하면 된다. 채굴 풀은 여러 사람이 모여 블록을 채굴하고, 기여도에 따라 보상을 나눠 갖는 구조다.

이번에는 브레인스 풀에 참여하는 방법을 알아보자. 브레인스 풀은 비트코인 최초의 채굴 풀이다. 예전에 처음 등장했을 때는 이름이 슬러시 풀이었는데 브레인스 풀로 이름을 바꿨다. 브레인스 풀은 라이트닝 네트워크로 비트코인 보상을 받는 것도 가능하다.

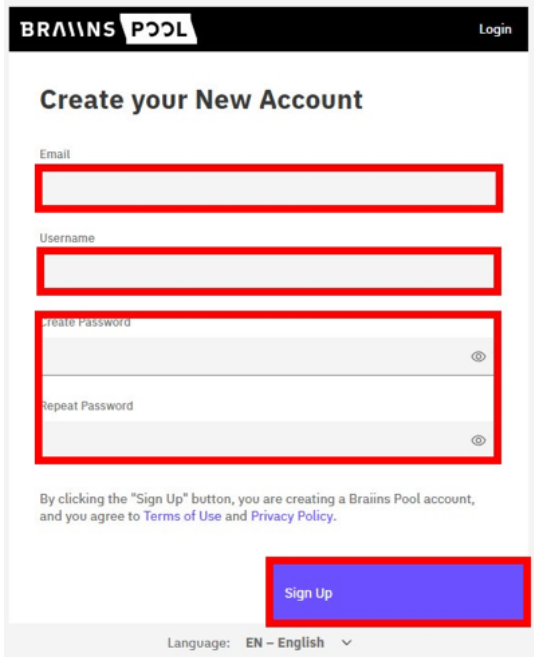
먼저 브레인스 풀에 가입해 보자. 이메일을 이용해 가입할 것이다. 다음 링크에 접속한다.

https://pool.braiins.com/login

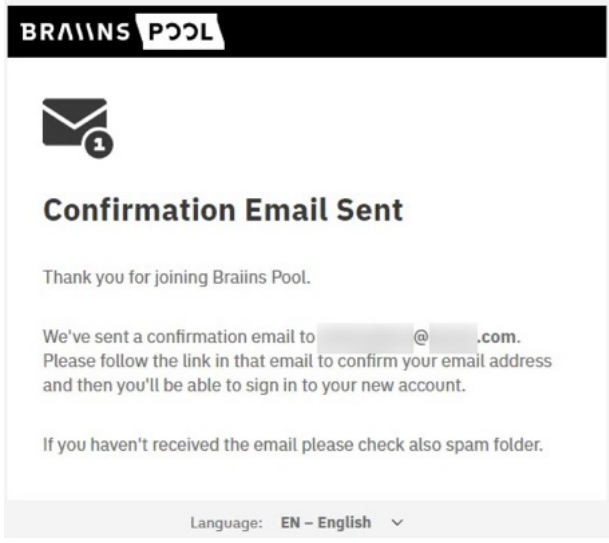
오른쪽 위 [Signup(회원가입)] 버튼을 누른다.



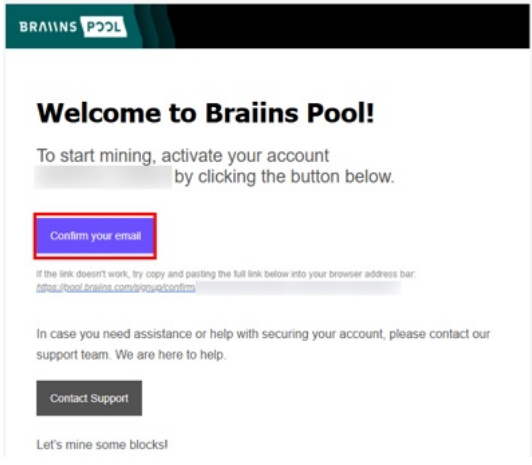
'Email'에는 인증을 받을 이메일을 입력한다. 'Username'에는 닉네임을 입력하면 된다(참고로 브레인스 풀은 로그인할 때 이메일이 아니라 유저네임과 비밀번호로 로그인한다). 'Create Password'와 'Repeat Password'에는 똑같은 비밀번호를 입력하면 된다.



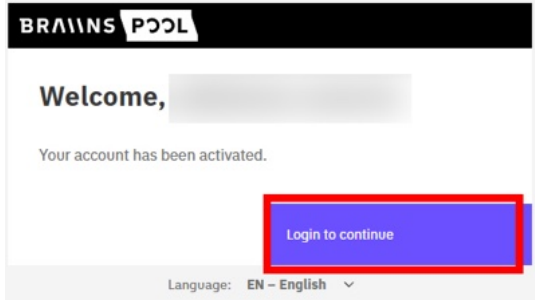
그러면 인증 이메일이 발송되었다는 안내창이 뜬다.



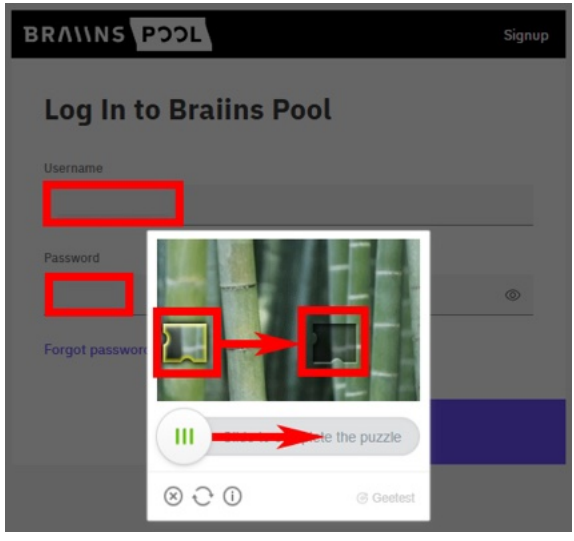
이메일에 로그인하고 메일함을 보면 다음과 같은 이메일이 와있는 것을 볼 수 있다. [Confirm your email]을 누른다.



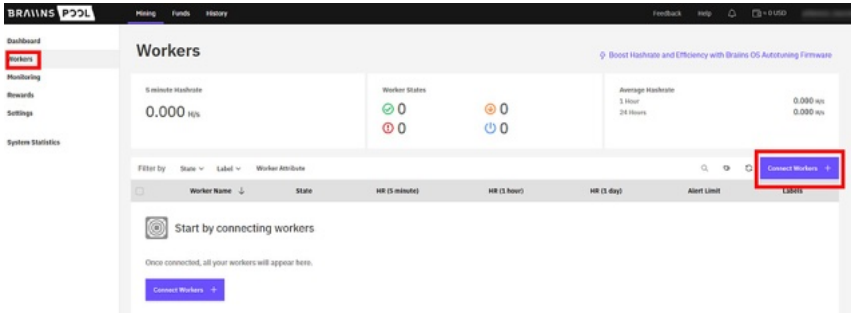
그러면 브레인스풀 웹사이트로 이동될 것이다. [Login to continue]를 누른다.



로그인 정보를 입력한다. 이때 이메일이 아니라 Username (닉네임)을 입력해야 한다. 퍼즐을 풀라는 창이 뜨면 슬라이드 버튼을 움직여 퍼즐을 푼다.



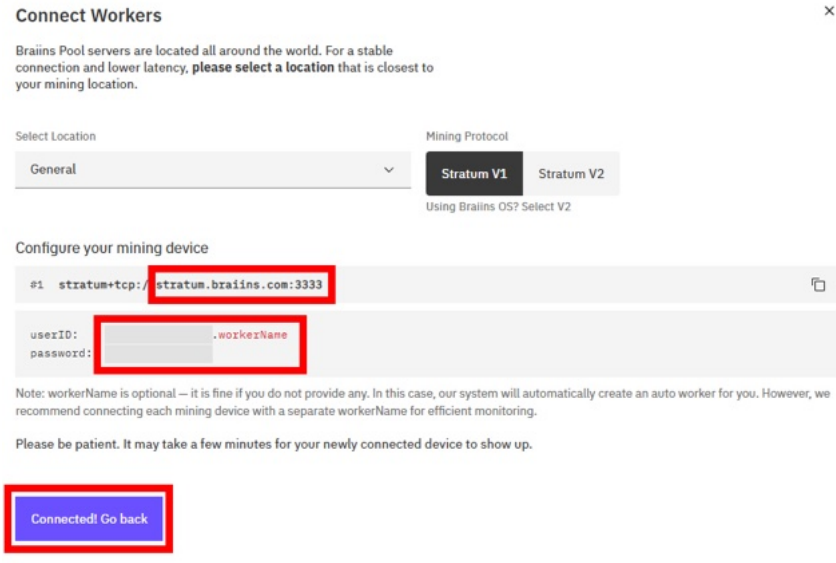
왼쪽 탭에서 [Workers]를 누르고 [Connect Workers]를 누른다.

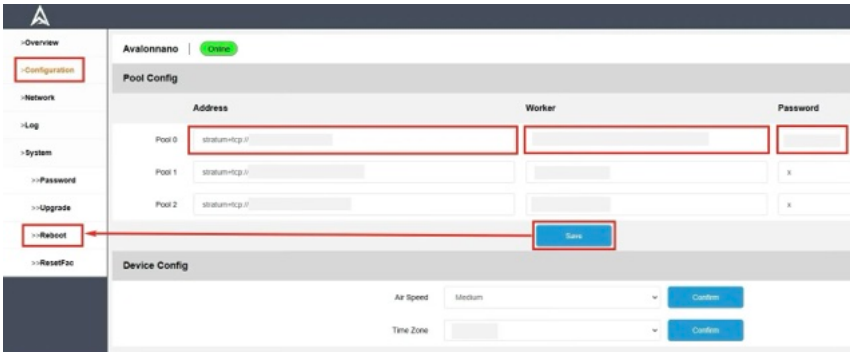


그러면 입력해야 하는 정보들이 뜰 것이다. 다음 정보들을 아발론 설정 창에 그대로 입력한다.

Address: stratum+tcp://stratum.braiins.com:3333
Worker: 브레인스 풀 userID에 쓰여 있는 내용(.채굴기 이름-선택 사항)
Password: 브레인스 풀 password에 쓰여 있는 비밀번호

다 되었으면 [Save]를 누르고 꼭 [Reboot]를 누르자.

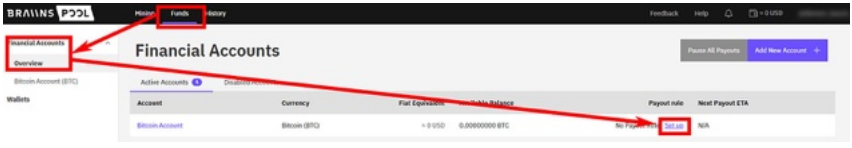




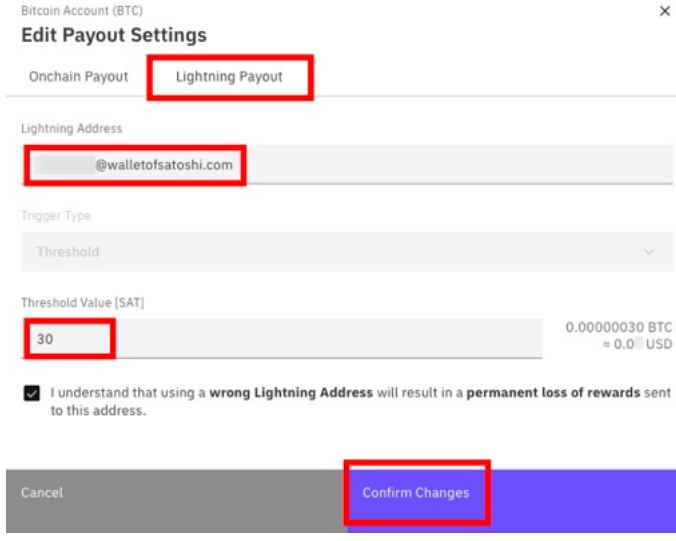
이제 브레인스 풀 채굴 풀에 연결되었을 것이다.

라이트닝 네트워크로 보상 받기(브레인스 풀)

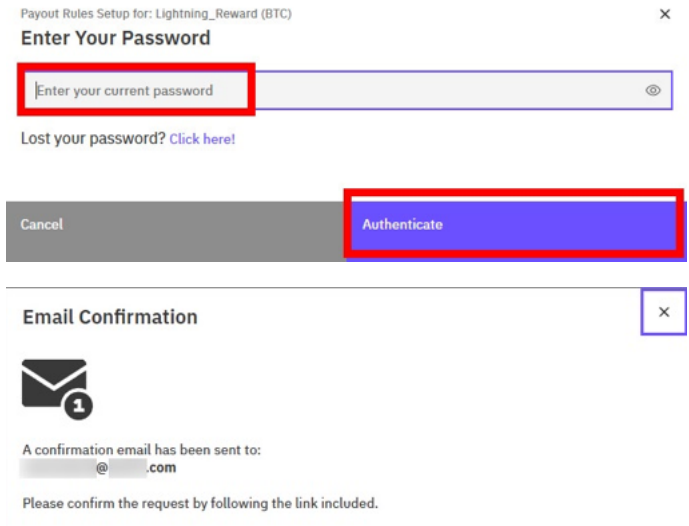
이제 보상받는 방식을 설정해 보자. 상단 [Funds] 탭을 누르고 'Payout rule' 아래에 있는 [Set up]을 누른다.



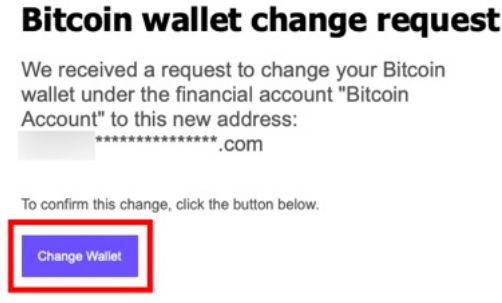
그러면 보상받는 방법을 설정하는 창이 나온다. 여기서 [Lightning Payout]을 누른다. 'Lightning Address'에는 보상을 받을 라이트닝 주소를 입력한다. 'Threshold Value'는 해당 금액(sats) 이상이 쌓이면 라이트닝 주소로 보상을 받겠다는 뜻이다. 너무 적은 금액으로 설정하면 너무 자주 라이트닝 보상을 받게 될 것이고, 너무 큰 금액으로 설정하면 보상을 너무 느리게 받게 되니 적당한 금액을 설정하자.



[Confirm Changes]를 누르면 비밀번호를 입력하는 창이 뜬다. 비밀번호를 입력하고 [Authenticate]를 누르면 이메일 인증을 위해 이메일을 보냈다는 안내문이 뜬다.



이메일을 확인하면 인증 이메일이 와있을 것이다. [Change Wallet]을 누르면 인증이 완료된다.



이메일 인증까지 마쳤다면 이제 설정한 사토시가 쌓일 때마다 채굴 보상이 들어올 것이다.

| 다텀으로 풀 노드와 채굴기 연결하기

비트코인 노츠 설치

엄브렐OS에서는 다텀 설정을 쉽게 할 수 있다. 지금부터는 다텀 설정을 하고 솔로 마이닝과 풀 채굴을 하는 방법을 각각 알아보자.

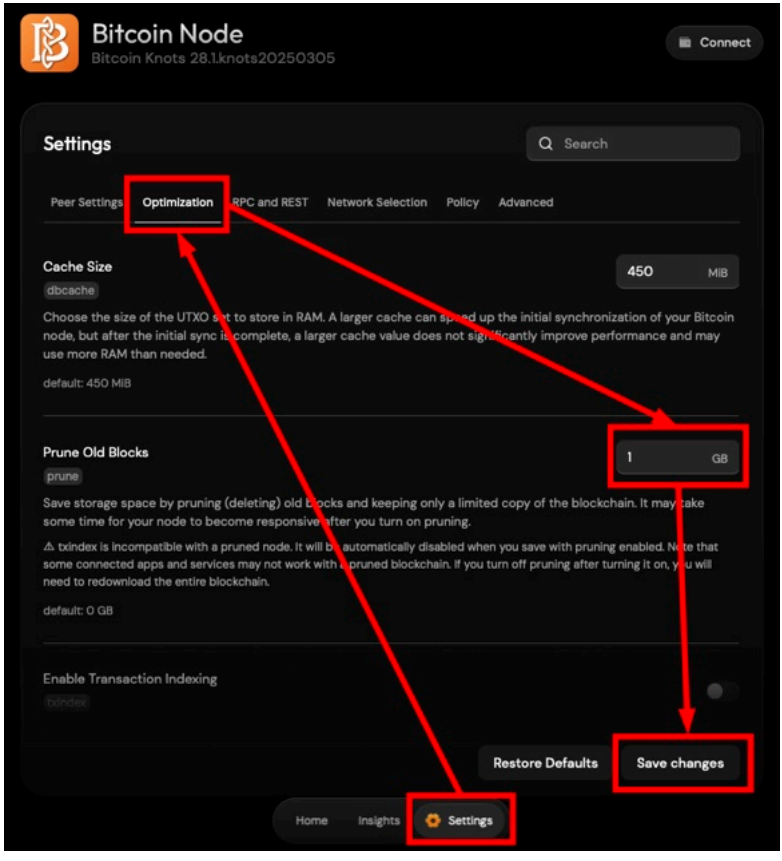
다텀을 설치하려면 비트코인 노츠Bitcoin Knots가 먼저 깔려있어야 한다. 엄브렐을 설치하면 풀 노드가 되기 위해 비트코인 노드Bitcoin Node(비트코인 코어) 혹은 비트코인 노츠를 설치했을 것이다.

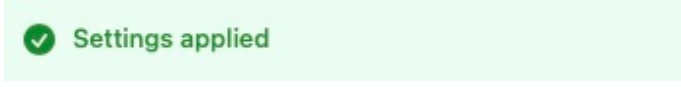
비트코인 노츠를 설치했다면 이번 단계는 건너뛰어도 된다. 비트코인 노드를 설치했던 경우에는 다텀을 설정하기 위해 노츠를 또 깔아야 한다. 그런데 비트코인 노드와 노츠는 블록 데이터 디렉토리를 공유하지 않는다. 무슨 뜻이냐면 블록 용량이 700GB를 초과하는 현재, 비트코인 노드와 노츠를 둘 다 다운로드하면 블록 용량이 총 1.4TB가 넘어가게 된다는 뜻이다. 이를 막기 위해서는 노츠에서 가지치기pruning 설정을 해야 한다. 하나씩 차근차근 해보자.

엄브렐OS에서 노츠를 먼저 설치하자.

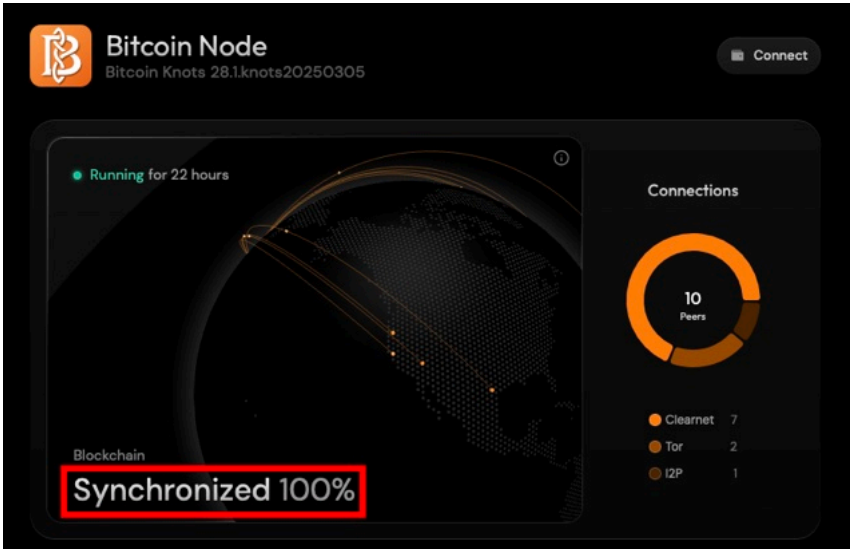
설치가 다 되었다면 [열기]를 누른다.

이제 노츠에서 가지치기 설정을 해줄 것이다. 하단 [Settings] → 상단 [Optimization]을 누르고, 'Prune Old Blocks'를 1GB로 설정한다. 그러고 [Save changes]를 누르면 블록 크기가 1GB 이상으로 올라가지 않는다.





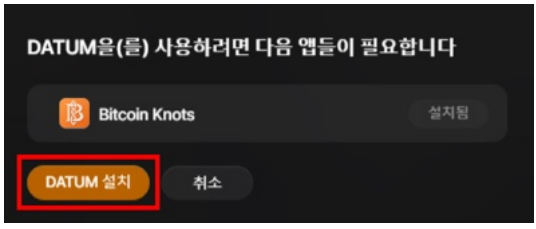
이제 블록 데이터가 100% 동기화될 때까지 기다리자. IBD (초기 블록 다운로드)를 해봤다면 알겠지만, 이 과정은 하루에서 길게는 일주일까지도 걸릴 수 있다.



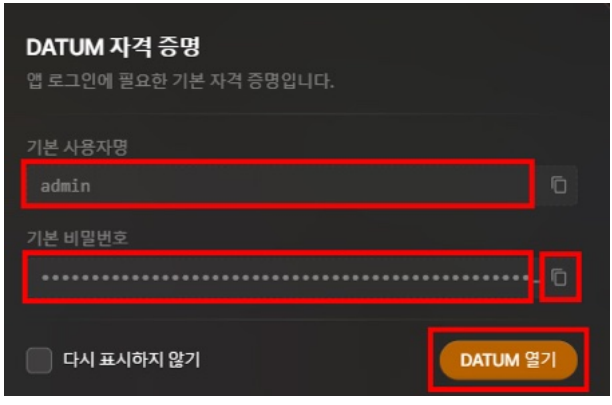
그런데 왜 비트코인 코어가 아니라 노츠를 사용할까? 노츠가 어떤 거래를 블록에 포함시킬지, 블록 템플릿을 사용자의 입맛에 따라 구성하기가 비트코인 노드(코어)보다 훨씬 쉽기 때문이다. 자세한 이유는 '3부. 풀 노드 운영 가이드'에서 '비트코인 노드(코어) 또는 노츠 설치' 절과 '노츠의 사용자 정책 설정' 절을 참고하라.

다텀 설치

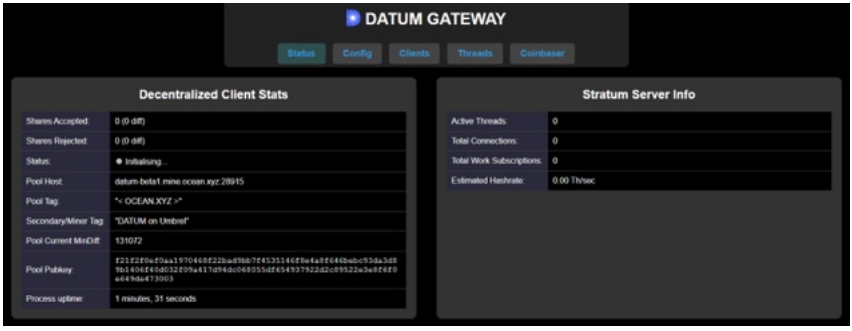
노츠가 100% 동기화되었다면 이제 설레는 마음으로 다텀을 다운로드하자. 노츠를 설치해야 한다는 안내문이 뜰 것이다. 우리는 이미 노츠를 설치했으니 계속 진행하면 된다.



이제 다텀을 실행해 보면 사용자명과 비밀번호 창이 뜬다. 이 비밀번호는 설정을 변경할 때 필요할 수도 있으니 미리 복사 버튼을 눌러 복사해 놓는다. 그다음에 [DATUM 열기]를 누른다.



그러면 다음과 같은 화면이 나온다.



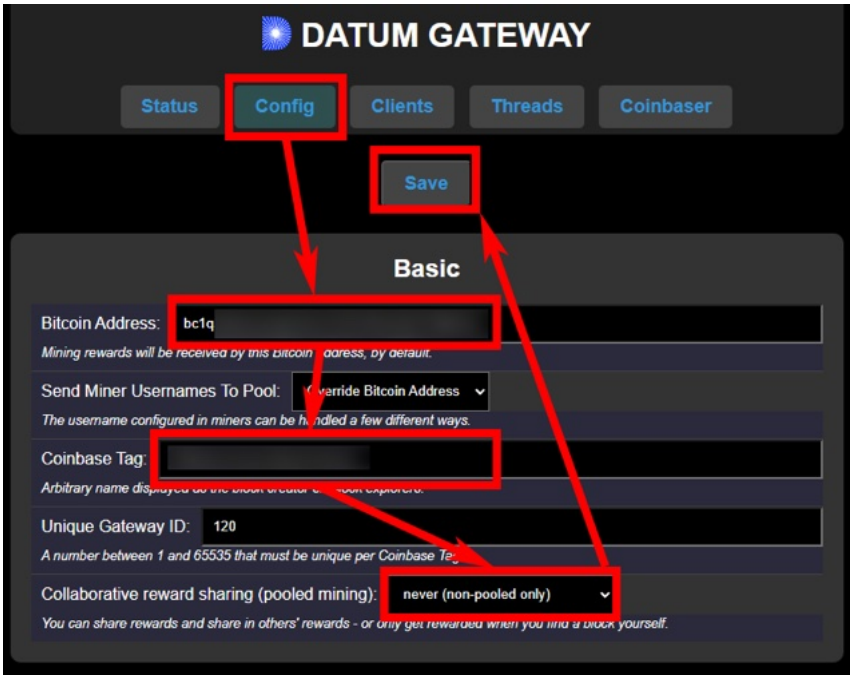
다텀에서 솔로 채굴 설정하기

솔로 채굴을 하기 위한 다텀 설정 방법에 대해 알아보자. 위의 탭에서 [Config]를 눌러 설정 창으로 들어온다.

'Bitcoin Address'에는 보상을 받을 비트코인 온-체인 주소를 입력한다. 이때 오타가 나지 않도록 주의하자.

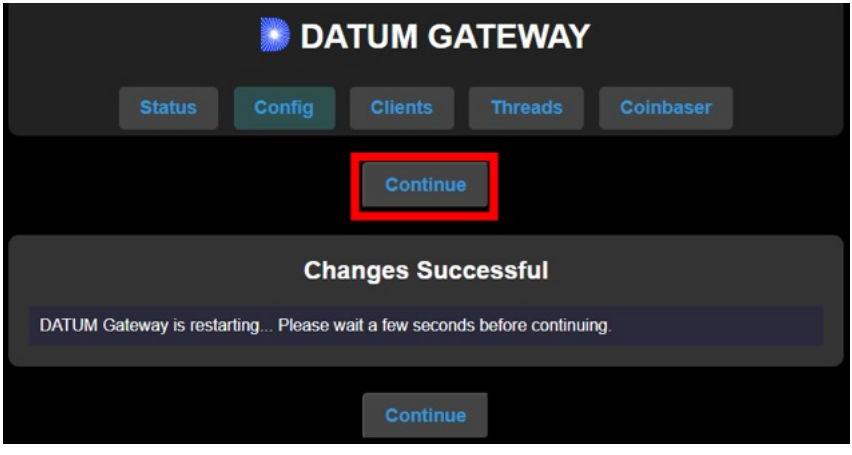
'Coinbase Tag'에는 자신이 설정하고 싶은 문구를 설정하면 된다. 사토시 나카모토가 제네시스 블록에 심었던 문구도 이 코인베이스 태그에 심겨 있던 것이다.

솔로 채굴로 설정하려면 'Collaborative reward sharing'을 [never (non-pooled only)]로 설정한다. 다 입력했으면 [Save]를 누른다.


DATUM GATEWAY
Status
Config
Clients
Threads
Coinbaser
Save
Basic
Bitcoin Address:
bc1q
Send Miner Usernames To Pool:
Coinbase Tag:
Unique Gateway ID:
120
Collaborative reward sharing (pooled mining):
never (non-pooled only)

만약 로그인하라는 창이 뜨면 앞에서 복사했던 사용자명과 비밀번호를 붙여넣는다. (※ 주의: 참고로 현재 애플의 사파리 브라우저에서는 다텀의 사용자명과 비밀번호 입력이 안 되는 것으로 확인되고 있다. 아무래도 http 접속이라 암호화된 전송이 아니기 때문에 데이터 전송이 막히는 것으로 추측된다. 따라서 다텀 설정 변경을 위해서는 크롬이나 파이어폭스 같은 다른 웹 브라우저에서 시도하길 바란다.)

성공적으로 변경됐다는 창이 나오면 [Continue]를 누른다. (이 화면이 안 나오기도 한다. 그러면 바로 다텀 재시작을 하면 된다.)



다텀을 재시작해야 한다. 엄브렐 홈에서 다텀 아이콘에 우클릭을 하고 [다시 시작]을 누른다.

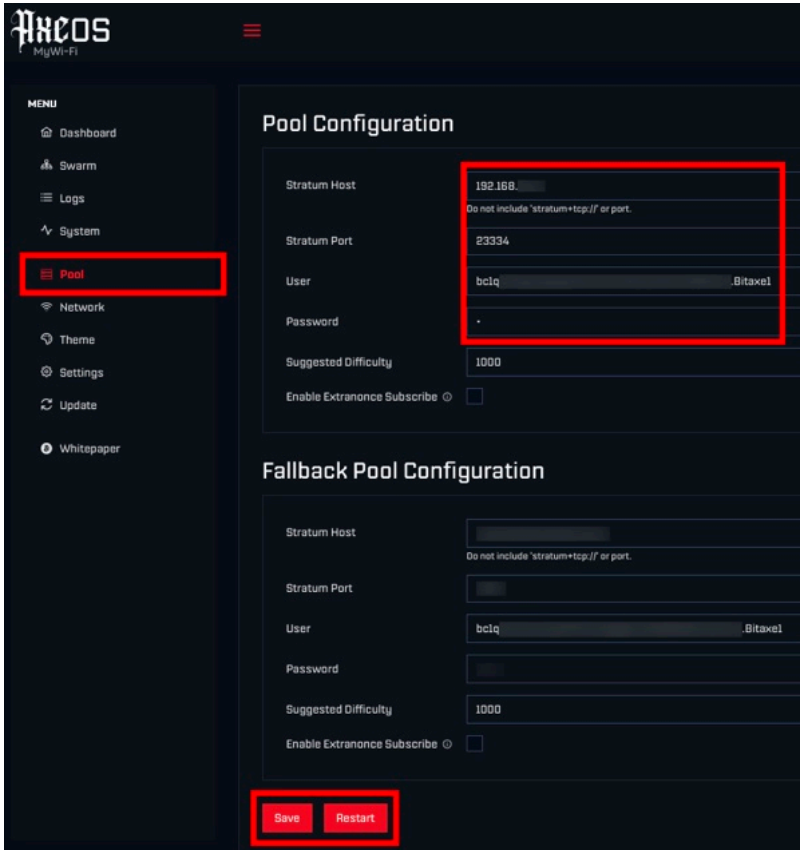
비트엑스를 다텀에 연결하기

이제 비트엑스를 다텀에 연결하기 위해서는 풀 노드의 로컬 IP 주소를 알기만 하면 된다. 주소창에 입력했을 때 엄브렐 접속이 되는 IP 주소(192.168.???.???)를 뜻한다. 'Stratum Host'에 자신의 엄브렐 풀 노드 로컬 IP 주소를 입력한다. 'Stratum Port'에는 23334를 입력한다. 'User'에는 'Bitcoin Address'에 입력한, 채굴 보상을 받을 주소를 입력한다. 'Password'에는 'x'를 입력한다.

그 아래에 'Fallback Pool Configuration'으로 똑같은 입력창이 있다. 이 부분은 만약 입력한 풀과 제대로 연결이 안 될 경우에 대비해 다른 연결할 곳을 입력하는 칸이다.

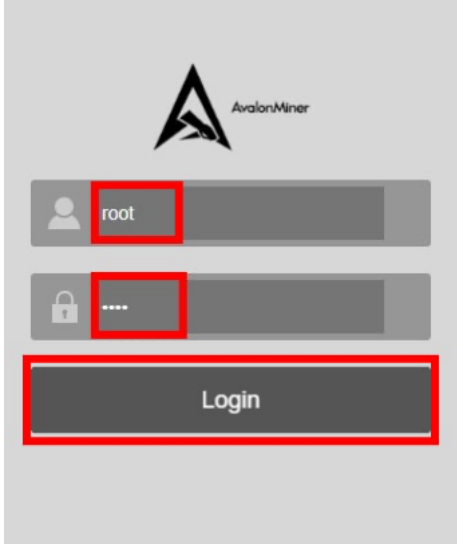
Stratum Host: 192.168.???.???
Stratum Port: 23334
User: Bitcoin Address에 입력한 비트코인 주소(.채굴기 이름-선택사항)
Password: x

입력했으면 [Save]를 누르고 [Restart]를 눌러 비트엑스를 재시작한다.


AXCOS
MyWi-Fi
MENU
Dashboard
Swarm
Logs
System
Pool
Network
Theme
Settings
Update
Whitepaper
Pool Configuration
Stratum Host
192.168.
Do not include 'stratum+tcp://' or port.
Stratum Port
23334
User
bc1q
.Bitaxe1
Password
x
Suggested Difficulty
1000
Enable Extranonce Subscribe
Fallback Pool Configuration
Stratum Host
Do not include 'stratum+tcp://' or port.
Stratum Port
User
bc1q
.Bitaxe1
Password
Suggested Difficulty
1000
Enable Extranonce Subscribe
Save
Restart

아발론 나노 3를 다텀에 연결하기

아발론 나노 3를 내 다텀 게이트웨이로 연결하는 것도 비트엑스 설정 방법과 똑같다. 웹 인터페이스에서 초기 ID와 비밀번호는 둘 다 'root'이다.



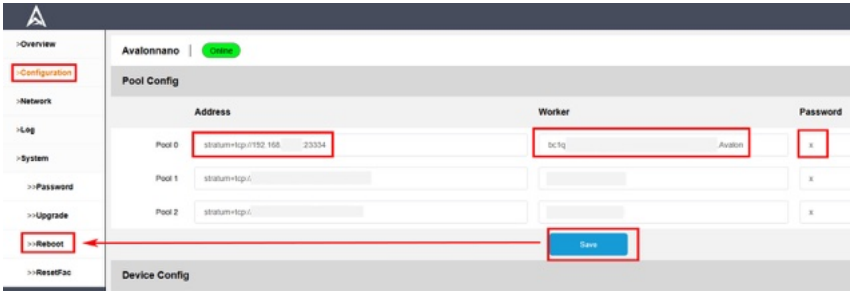
Pool 0에 있는 설정만 하면 된다. 'Address'에는 'stratum+tcp://' 다음에 내 풀 노드의 로컬 IP 주소를 입력하고 뒤에 ':23334'를 붙인다. 'Worker'에는 'Bitcoin Address'에 입력한, 채굴 보상을 받을 주소를 입력한다. 마지막으로 'Password'는 'x'를 입력한다.

Address: stratum+tcp://192.168.???.???:23334

Worker: Bitcoin Address에 입력한 비트코인 주소(.채굴기 이름-선택 사항)

Password: x

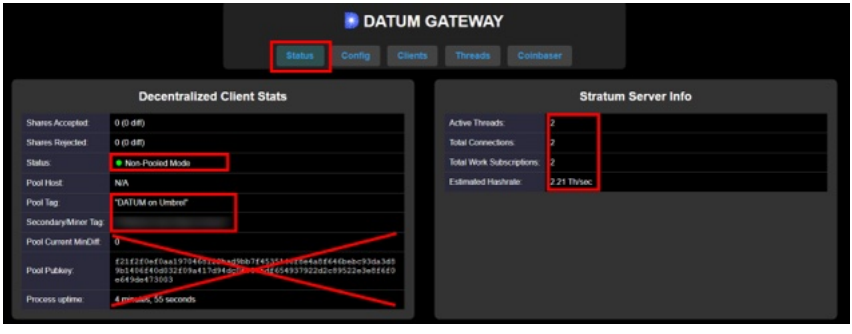
그다음에 [Save]를 누르고 [Reboot]를 눌러 아발론 나노 3를 재시작한다.



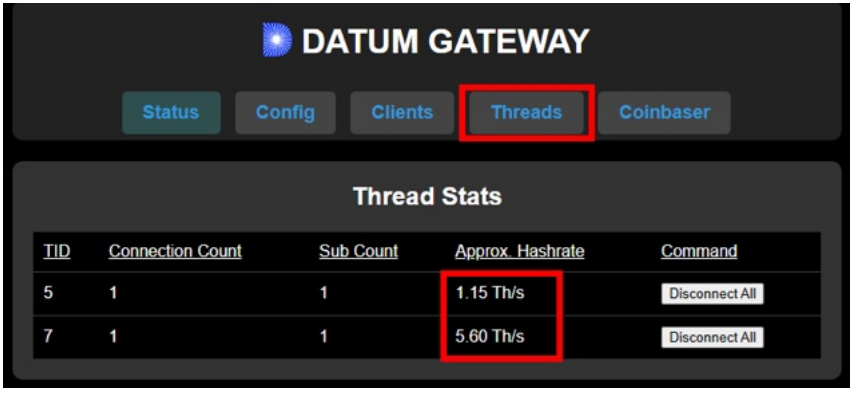
채굴이 잘 되는지 확인하기

이제 다시 엄브렐에서 다텀에 접속해 보고 채굴기들이 다텀 게이트웨이에 잘 연결됐는지, 잘 돌아가고 있는지 확인해 보자.

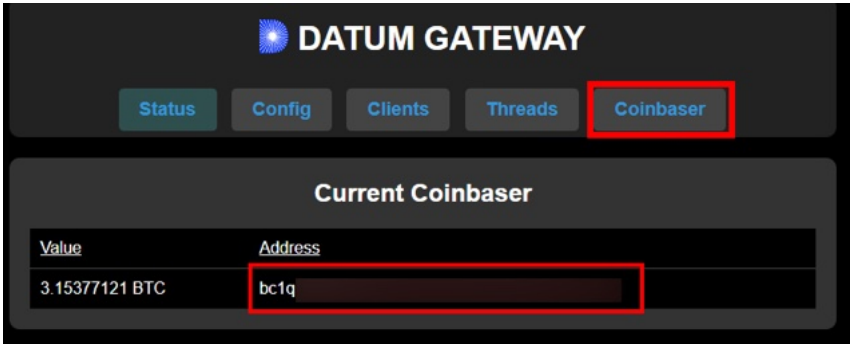
[Status] 창에서 전체적인 내용을 확인할 수 있다. 솔로 채굴로 설정했다면 'Status'는 Non Pooled Mode가 되어 있어야 한다. 'Pool Host'는 N/A로 되어있는지 확인하자. 그리고 코인베이스 태그가 잘 설정되었는지 확인하자. 'Pool Pubkey'는 채굴 풀 모드에서만 사용되는 정보이므로 무시해도 된다.



'Clients' 창과 'Threads' 창에서 다텀 게이트웨이에 연결된 채굴기들의 상태를 확인할 수 있다. 참고로 다텀에서 표시하는 채굴기들의 해시레이트는 Share 제출 빈도로 판단하기 때문에 정확하지는 않고, 계속 변하는 것을 알 수 있다.



마지막으로 제일 중요한 부분을 확인하자. 'Coinbaser' 창에서 채굴 보상이 주어질 주소를 확인하자. 이 부분이 잘못되면 작업증명에 성공해도 보상이 엉뚱한 곳으로 갈 수 있다.



이렇게 해서 다텀을 이용해 솔로 채굴 모드로 설정하는 것이 완료되었다.

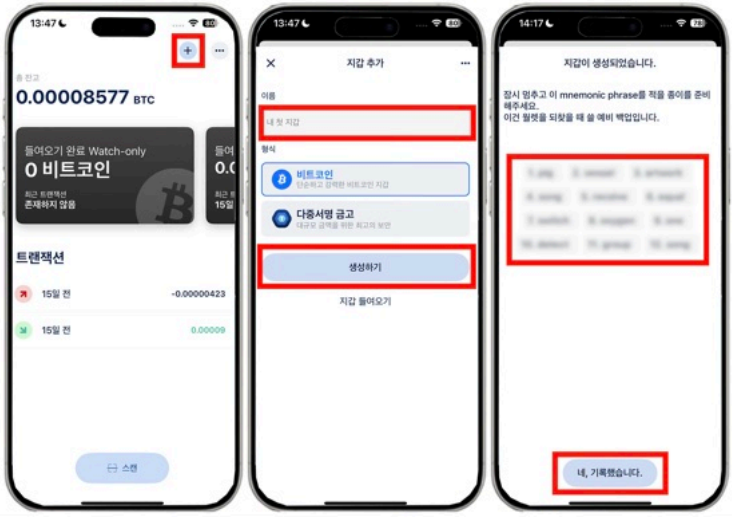
다텀을 이용하여 채굴 풀(오션 풀) 참여하기

다텀의 매력은 자신이 블록 구성 권한을 가지면서 보상을 나눠 갖는 채굴 풀에 참여할 수 있게 하는 데 있다. 다텀을 통해 오션 풀OCEAN POOL에 참여하는 방법에 대해 알아보자.

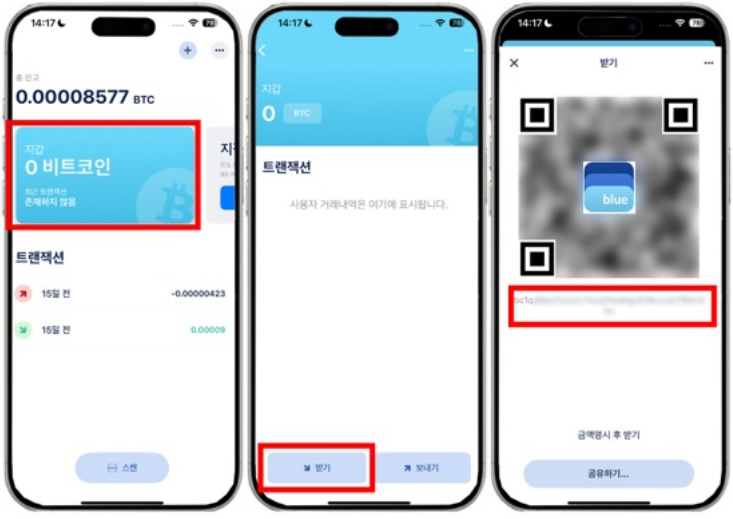
뒤에서 살펴보겠지만 만약 채굴 보상을 라이트닝 네트워크로, 오션 풀에서 블록을 채굴할 때마다 받고 싶다면 메시지 서명을 해야 한다. 에어-갭 지갑 중에서는 시드사이너가 메시지 서명을 하기에 편하다(2025년 8월 기준, 키스톤은 오션 풀에서 보여주는 메시지에 서명하는 것에 실패했다. 콜론(:) 문자를 제대로 인식 못 하기 때문인 것으로 보인다). 모바일 핫월렛에서는 블루월렛 지갑(워치-온리 말고 블루월렛에서 생성한 핫월렛 지갑)을 이용하는 것이 편하고, 엄브렐에서 하려면 라이트닝 노드(온-체인 주소)로 하는 것이 편하다.

블루월렛에서 생성된 지갑 주소 사용

블루월렛을 이용한 방법부터 설명하겠다. 블루월렛에 들어가 오른쪽 위 [+] 버튼을 누른다. 지갑 이름을 설정하고(채굴 보상받는 용도 등) [생성하기]를 누른다. 이때 오른쪽 위 점 세 개를 누르면 직접 주사위를 굴려서 생성할 수도 있다. 니모닉을 백업하고 아래에 있는 [네, 기록했습니다.]를 누른다.

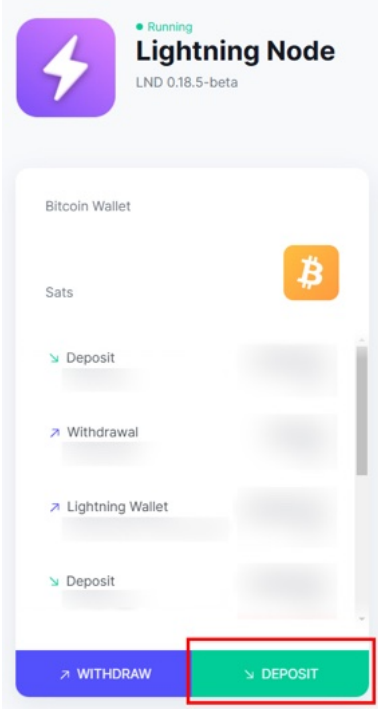


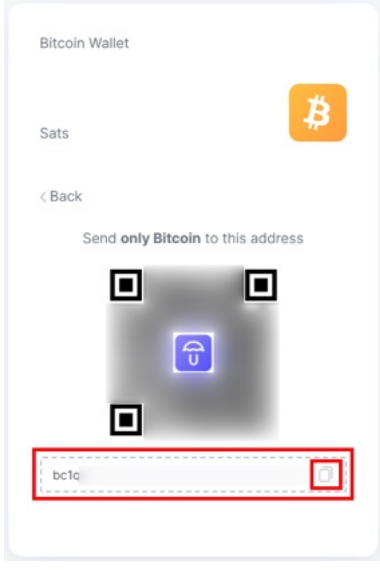
블루월렛에서 생성된 지갑은 파란색이다. 지갑을 누르고 [받기]를 누른다. 여기 나오는 주소를 'Bitcoin Address'로 설정한다. (오타를 방지하기 위해 주소를 복사한 뒤 붙여넣는 것을 추천한다. 블루월렛에서는 주소를 누르면 자동으로 복사가 된다.)



라이트닝 노드에서 생성된 온-체인 주소 사용

엄브렐에서 라이트닝 노드(LND)를 이용하는 방법도 있다. 라이트닝 노드를 운영 중이라면 라이트닝 노드의 온-체인 주소를 채굴 보상을 받을 주소로 설정하면 된다.





다텀 설정하기

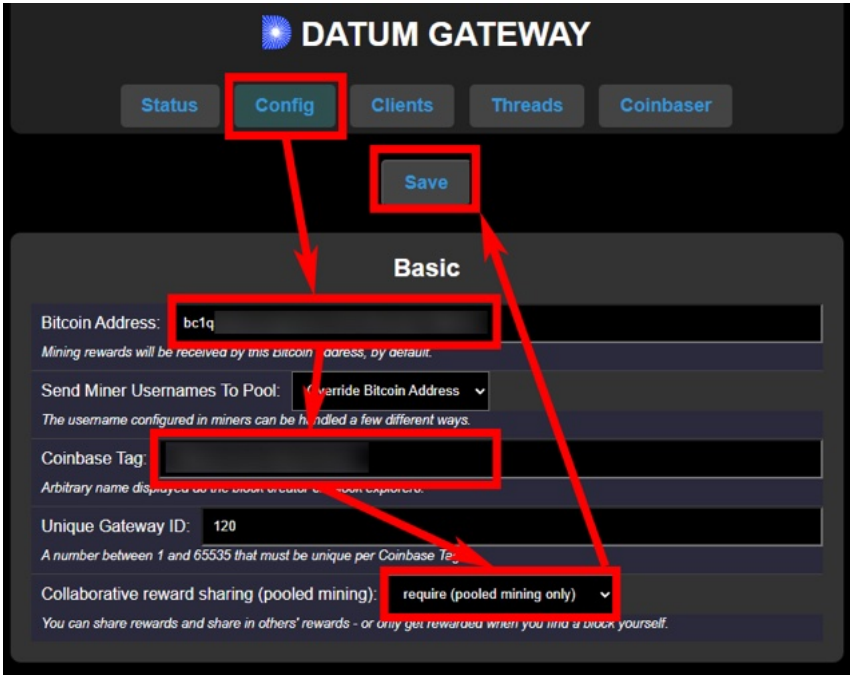
이제 다텀 앱으로 들어온다. 맨 위의 탭에서 [Config]를 눌러 설정 창으로 들어온다.

'Bitcoin Address'에는 보상을 받을 비트코인 온-체인 주소를 입력한다. 이때 오타가 나지 않도록 주의하자. 메시지 서명 기능을 이용하려

면 앞서 블루월렛이나 라이트닝 노드에서 생성한 주소를 이용하는 것이 좋다.

'Coinbase Tag'는 자신이 설정하고 싶은 문구를 설정하면 된다. 사토시 나카모토가 제네시스 블록에 심었던 문구도 이 코인베이스 태그에 심겨 있던 것이다.

오션 채굴 풀에 참여하려면 'Collaborative reward sharing'을 [require (pooled mining only)]로 설정한다. 다 입력했으면 [Save]를 누른다.



만약 로그인하라는 창이 뜨면 앞에서 복사했던 사용자명과 비밀번호를 붙여넣는다. (※ 주의: 참고로 현재 애플의 사파리 브라우저에서는 다텀의 사용자명과 비밀번호 입력이 안 되는 것으로 확인되고 있다. 아무래도 http 접속이라 암호화된 전송이 아니기 때문에 데이터 전송이 막히는 것으로 추측된다. 따라서 다텀 설정 변경을 위해서는 크롬이나 파이어폭스 같은 다른 웹 브라우저에서 시도하길 바란다.)

다텀을 재시작해야 한다. 엄브렐 홈에서 다텀 아이콘에 우클릭을 하고 [다시 시작]을 누른다.

오션 풀에서 채굴할 때 자신이 설정한 코인베이스 태그는 어떻게 삽입되는 것일까? 다음 사진은 멤풀 웹사이트에서 오션 풀을 검색했을 때 나오는 오션 풀에서 채굴된 블록 정보 화면이다. 여기서 코인베이스 태그 부분을 보면 풀 태그Pool Tag인 〈OCEAN.XYZ〉 다음에 사용자들이 각자 입력한 보조 태그Secondary Tag가 있는 것을 볼 수 있다. 만약 자신이 블록을 채굴하면 자신이 설정했던 코인베이스 태그가 이런 방식으로 블록에 영원히 실리는 것이다.

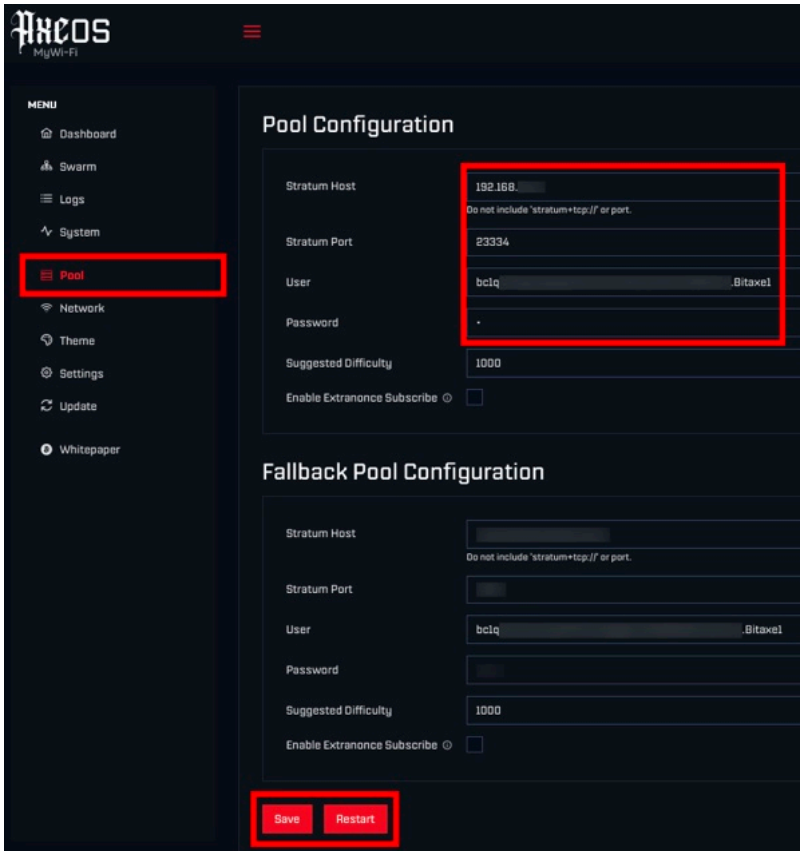
비트엑스를 다텀에 연결하기

이제 비트엑스를 다텀에 연결하기 위해서는 풀 노드의 로컬 IP 주소를 알기만 하면 된다. 주소창에 입력했을 때 엄브렐 접속이 되는 IP 주소(192.168.???.???)를 뜻한다. 'Stratum Host'에 자신의 엄브렐 풀 노드 로컬 IP 주소를 입력한다. 'Stratum Port'에는 23334를 입력한다. 'User'에는 'Bitcoin Address'에 입력한, 채굴 보상을 받을 주소를 입력한다. 'Password'에는 'x'를 입력한다.

그 아래에 'Fallback Pool Configuration'으로 똑같은 입력창이 있다. 이 부분은 만약 입력한 풀과 제대로 연결이 안 될 경우에 대비해 다른 연결할 곳을 입력하는 칸이다.

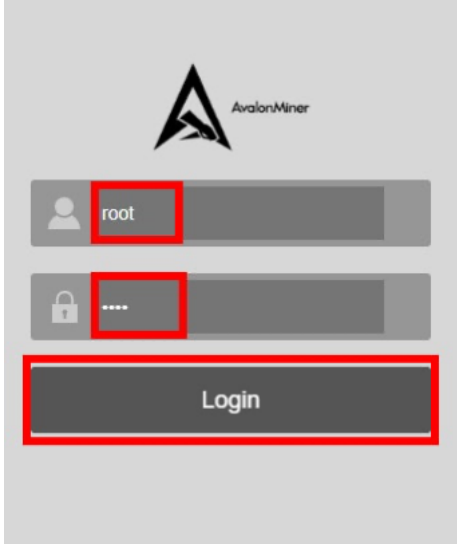
Stratum Host: 192.168.???.???
Stratum Port: 23334
User: Bitcoin Address에 입력한 비트코인 주소(.채굴기 이름-선택사항)
Password: x

입력했으면 [Save]를 누르고 [Restart]를 눌러 비트엑스를 재시작한다.


AXCOS
MyWi-Fi
MENU
Dashboard
Swarm
Logs
System
Pool
Network
Theme
Settings
Update
Whitepaper
Pool Configuration
Stratum Host
192.168.
Do not include 'stratum+tcp://' or port.
Stratum Port
23334
User
bc1q
.Bitaxe1
Password
x
Suggested Difficulty
1000
Enable Extranonce Subscribe
Fallback Pool Configuration
Stratum Host
Do not include 'stratum+tcp://' or port.
Stratum Port
User
bc1q
.Bitaxe1
Password
Suggested Difficulty
1000
Enable Extranonce Subscribe
Save
Restart

아발론 나노 3를 다텀에 연결하기

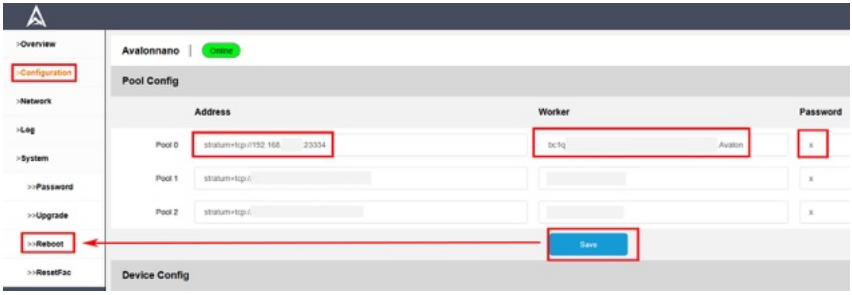
아발론 나노 3를 내 다텀 게이트웨이로 연결하는 것도 비트엑스 설정 방법과 똑같다. 웹 인터페이스에서 초기 ID와 비밀번호는 둘 다 'root'이다.



Pool 0에 있는 설정만 하면 된다. 'Address'에는 stratum+tcp:// 다음에 내 풀 노드의 로컬 IP 주소를 입력하고 뒤에 :23334를 붙인다. 'Worker'에는 'Bitcoin Address'에 입력한, 채굴 보상을 받을 주소를 입력한다. 마지막으로 'Password'는 'x'를 입력한다.

Address: stratum+tcp://192.168.???.???:23334
Worker: Bitcoin Address에 입력한 비트코인 주소(.채굴기 이름-선택사항)
Password: x

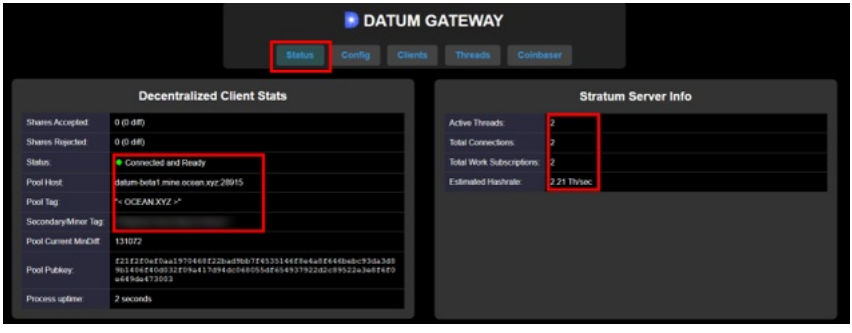
그다음에 [Save]를 누르고 [Reboot]를 눌러 아발론 나노 3를 재시작한다.



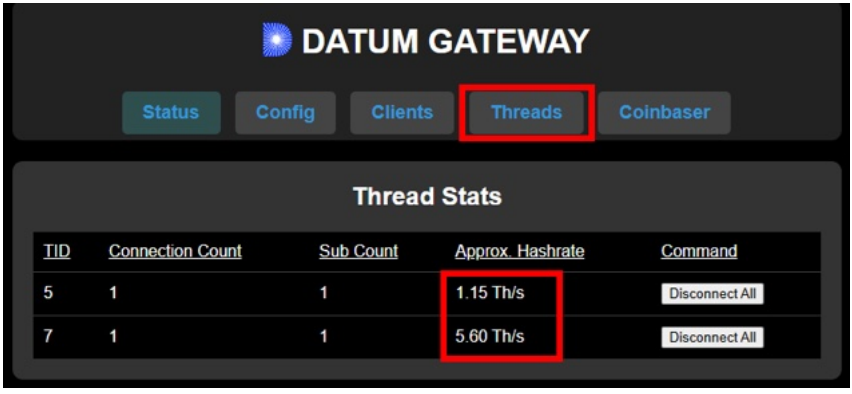
채굴이 잘 되는지 확인하기

지금부터는 채굴기들이 다텀 게이트웨이에 잘 연결됐는지 확인하고, 오션 풀 웹사이트에서 채굴 풀에 잘 참여하고 있는지 확인해 볼 것이다.

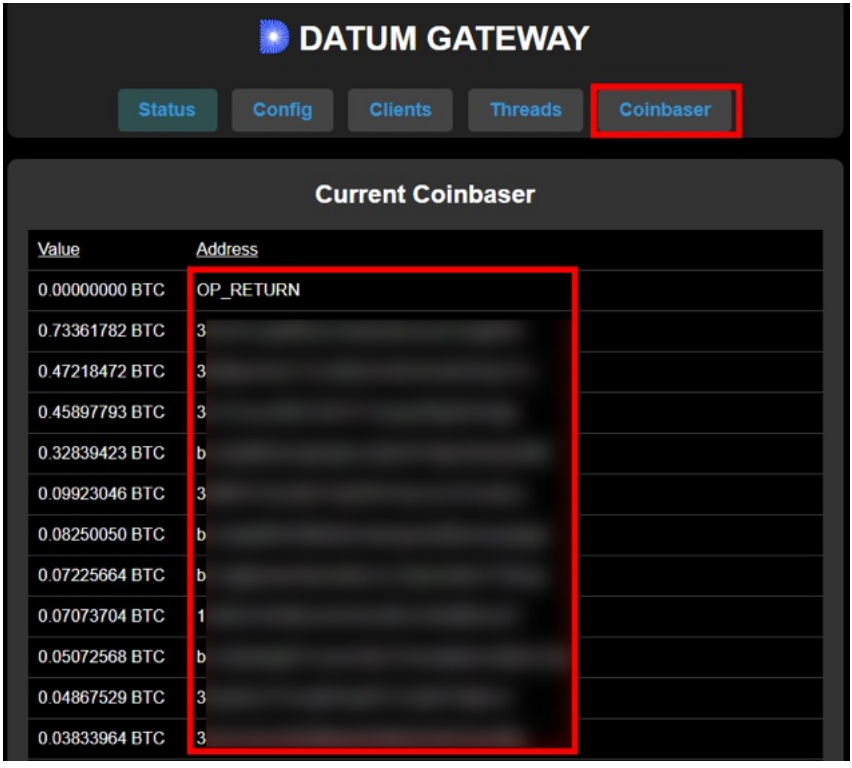
먼저 엄브렐 다텀 앱에 접속해 보자. [Status] 창에서 전체적인 내용을 확인할 수 있다. 'Status'는 초록색 점과 함께 'Connected and Ready'가 되어 있어야 한다. 코인베이스 태그도 잘 설정되었는지 확인하자.



'Clients' 창과 'Threads' 창에서 다텀 게이트웨이에 연결된 채굴기들의 상태를 확인할 수 있다. 참고로 다텀에서 표시하는 채굴기들의 해시레이트는 셰어 제출 빈도로 판단하기 때문에 정확하지는 않고, 계속 변하는 것을 알 수 있다.



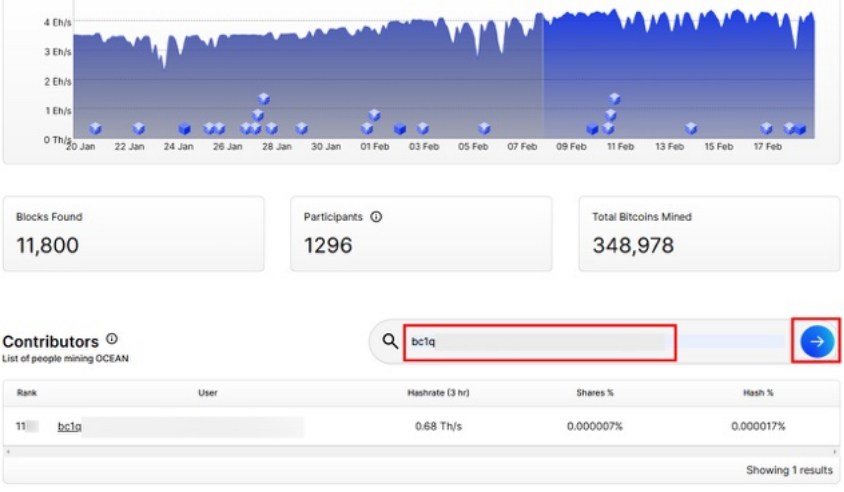
마지막으로 블록의 코인베이스 보상의 출력 부분을 확인해 보자. 이 출력은 채굴 풀인 오션 풀이 구성 권한을 갖는다.



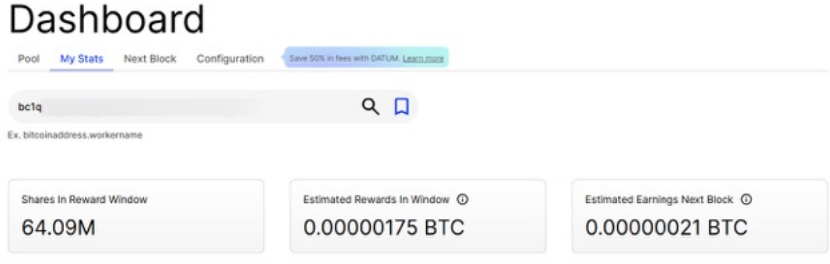
이제 오션풀 웹사이트에 들어가서 채굴 풀에 잘 참여가 되고 있는 건지 확인해 보자. 다음 링크에 들어간다.

https://ocean.xyz/dashboard

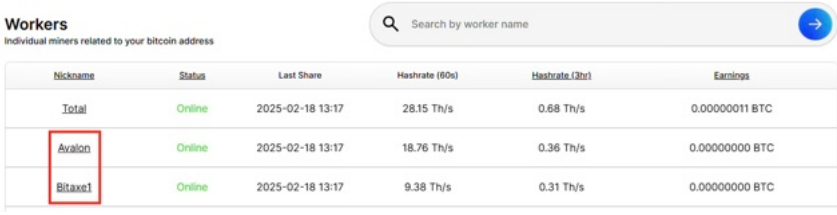
스크롤을 조금만 내려보면 'Contributors'를 검색할 수 있는 창이 나온다. 여기에 자신이 채굴 보상을 받기로 설정했던 비트코인 주소를 입력한다. 그리고 옆의 화살표 버튼을 눌러보자.



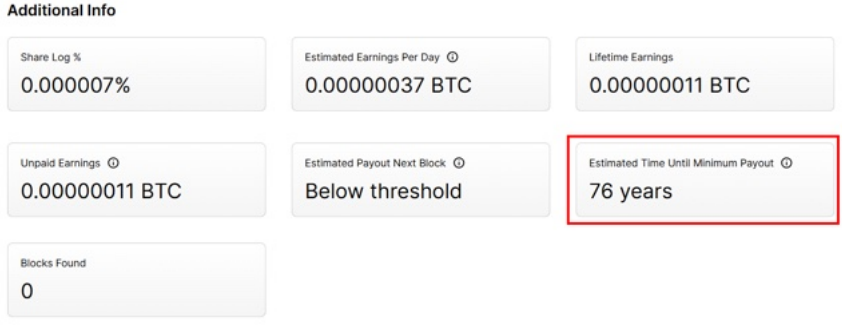
그러면 대시보드가 나온다.



스크롤을 조금만 아래로 내려보자. ‘Workers’에서 채굴기들이 잘 연결되었는지 확인할 수 있다. ‘Nickname’에 내가 설정한 채굴기 이름이 잘 뜬다면 된 것이다. ‘Status’가 Offline이라면 조금 기다려보면 된다. Share가 제출되어야 Online으로 바뀌기 때문이다. 해시레이트도 정확하지는 않다는 것을 알 수 있다. ‘Nickname’에 채굴기가 추가됐다면 연결된 것으로 보아도 된다.



스크롤을 조금 더 내려보자. 문제가 있다. ‘Estimated Time Until Minimum Payout’을 보자. 이것은 최소 보상을 받기까지 걸리는 예상 시간이다. 그런데 지금 이 칸이 76년으로 표시된다. 채굴 보상을 76년 뒤에나 받을 수 있다니 이건 너무하지 않은가?



라이트닝 지갑으로 채굴 보상 받기

홈 마이닝의 경우 하루에 채굴되는 양이 기껏해야 수십-수백 sats이므로 온-체인으로 보상을 받기에는 금액이 너무 적다. 따라서 라이트닝 네트워크로 받는 것이 좋다. 라이트닝 네트워크로는 오션 풀에서 블록을 채굴할 때마다 sats를 전송받을 수 있기 때문이다.

참고로 오션 풀의 온-체인 지급 기준은 다음과 같다. 일단 오션 풀이 가져가는 수수료는 1%다. 보통 수수료는 2%지만, 오션 풀은 다텀 이용을 장려하기 위해 다텀 게이트웨이를 통해 채굴 풀에 연결된 경우 수수료를 1%만 가져간다.

만약 쌓인 보상이 1,048,560 sats가 넘으면 오션 풀에서 다음 블록이 채굴될 때 내가 설정한 온-체인 주소로 보상이 즉시 전송된다. 내가 설정한 온-체인 주소가 코인베이스 출력에 포함되어 직접적으로 보내지는 것이다.

쌓인 보상이 65,535 sats를 넘은 경우 채굴 풀과 연결이 끊긴 지 일주일이 지나면 내가 설정했던 온-체인 주소로 보상이 전송된다. 그러나 하루에 몇백 sats가 쌓이는 홈 마이닝의 경우 65,535 sats를 쌓기도 쉬운 일이 아니다. 따라서 지금부터는 라이트닝 네트워크로 채굴 보상을 받는 방법에 대해 알아볼 것이다.

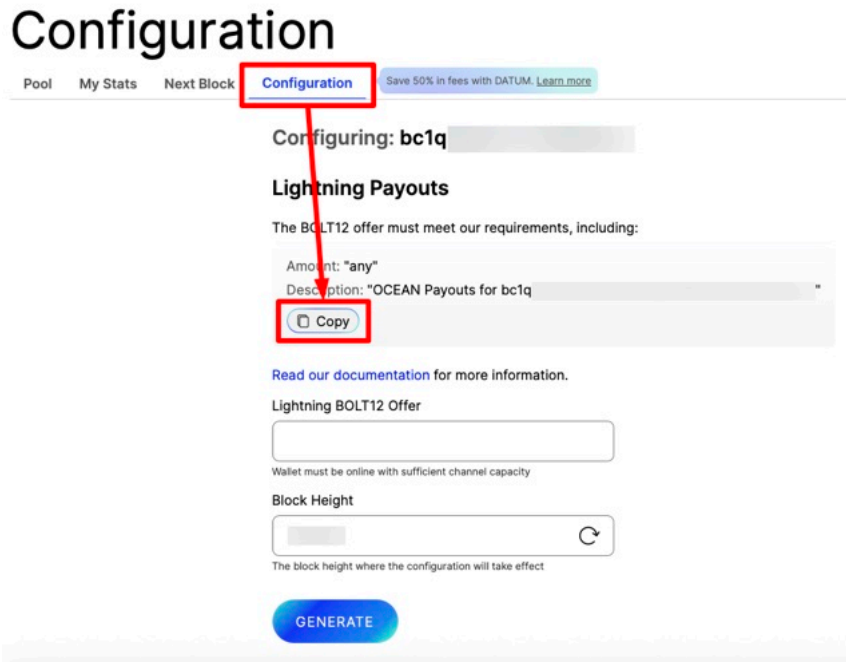
오션 풀에서 라이트닝 네트워크로 채굴 보상을 받으려면 이용하는 라이트닝 노드가 Bolt12 오퍼Offer 기능을 지원해야 한다. 오퍼 기능이란 보통 1시간이면 만료되는 인보이스와 다르게 시간이 지나도 계속 받을 수 있는 결제 요청이다. 그런데 2025년 8월 기준 LND는 이 오퍼 생성 기능을 지원하지 않는다. 라이트닝 수탁 서비스인 월렛 오브 사토시 앱도 오퍼 생성 기능을 지원하지 않는다.

따라서 현재는 오퍼 생성 기능을 지원하는 코어 라이트닝CLN, Core Lightning(이하 CLN)을 이용하여 직접 라이트닝 노드를 운영하는 수밖에 없다. 라이트닝 지갑인 피닉스 지갑은 오퍼 생성 기능을 지원하기는 하지만, Description 설정이 불가능해서 오션 풀에서 라이트닝 지갑 주소로 전송받을 수 없다. 하지만 점차 Bolt12 오퍼 기능을 지원하는 라이트닝 서비스들이 많아질 것이다.

또한 오션 풀은 이메일을 포함한 일체의 개인정보를 받지 않기 때문에 라이트닝 네트워크로 받는 설정을 하는 과정에서 메시지 서명이 필요하다. 블루월렛에서 생성한 지갑이나 LND 라이트닝 노드에서는 메시지 서명을 쉽게 할 수 있다. 에어-갭 지갑의 경우 스패로우 워치-온리 지갑의 [Tools] → [Sign/Verify Message] 기능을 이용하여 메시지 서명을 할 수 있다. 2025년 8월 기준으로 키스톤은 스패로우 지갑이 생성하는 메시지를 읽기는 하지만 제대로 읽지는 못했다. 시드사이너는 메시지 서명 기능이 제대로 작동했다.

메시지 서명은 시드사이너와 스패로우를 사용하는 방법, 블루월렛(핫 월렛)으로 생성한 지갑 주소를 사용하는 방법, 라이트닝 노드의 온체인 주소를 사용하는 방법을 서술하겠다. 또한, 다음 가이드는 '4부. 라이트닝 노드 운영 가이드'가 어느 정도 숙지된 사람들을 대상으로 쓰였다.

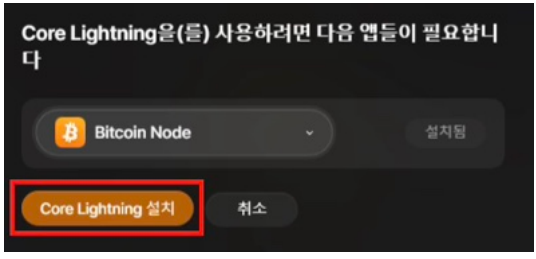
오션 풀 웹사이트의 대시보드에서 내 비트코인 주소를 검색하고, [Configuration]을 누른다. 'Lightning Payouts' 밑에 'Amount: -', 'Description: -' 부분이 보일 것이다. 그 밑의 문서 모양 버튼을 눌러 복사한다.



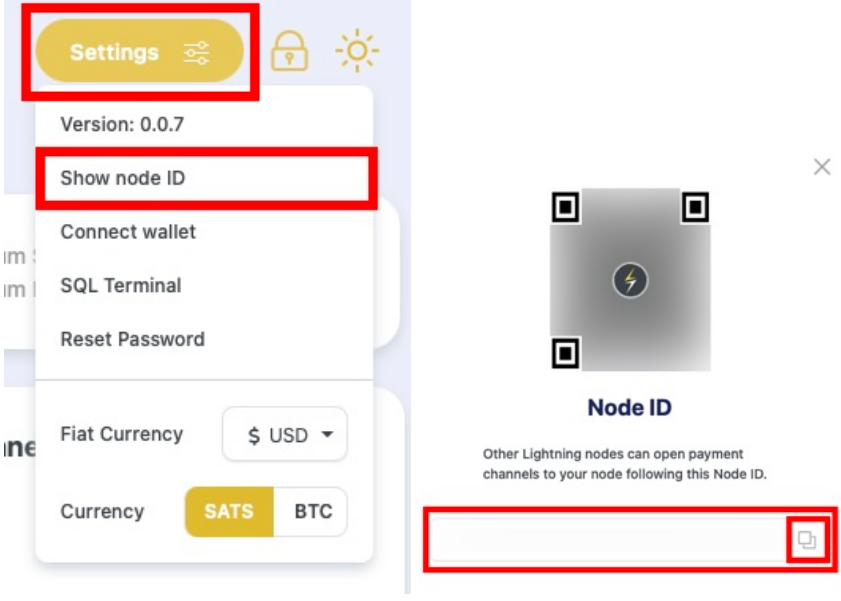
코어 라이트닝(CLN)으로 Offer 생성하기

이제 라이트닝 노드인 CLN을 이용해 Offer를 생성해야 한다. 따라서 CLN을 운영해야 한다. CLN은 백업이 까다로우므로 LND를 중점으로 해서 라이트닝 노드를 운영하고, 자신이 운영하는 CLN과 LND를 채널로 연결하는 것도 하나의 방법이다. CLN의 백업 방법은 4부의 'CLN을 설치하는 경우' 절을 참고하라.

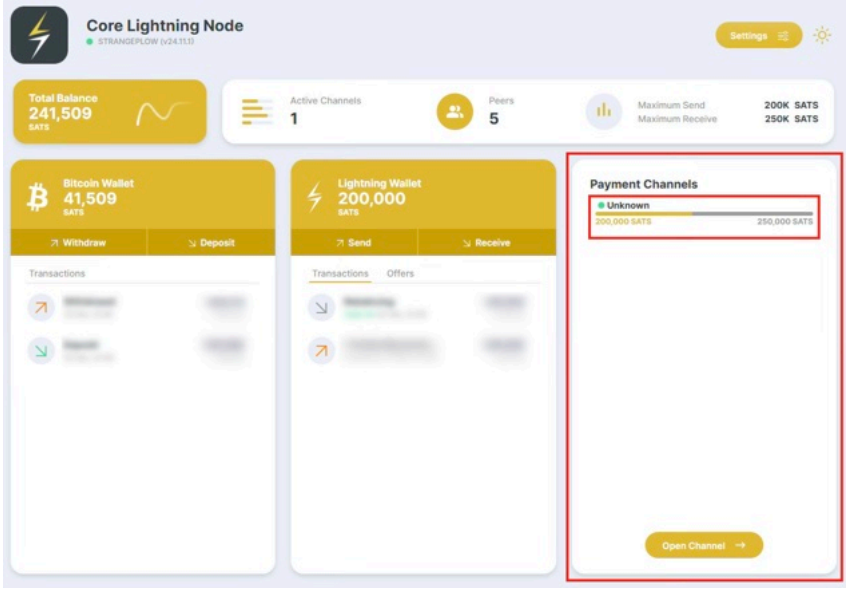
필자는 미리 운영 중인 라이트닝 노드(LND) 측에서 새로 개설한 CLN과 채널을 열고 CLN의 인바운드 유동성을 확보해 놓았다. 과정은 다음과 같다. 먼저 CLN을 설치한다.



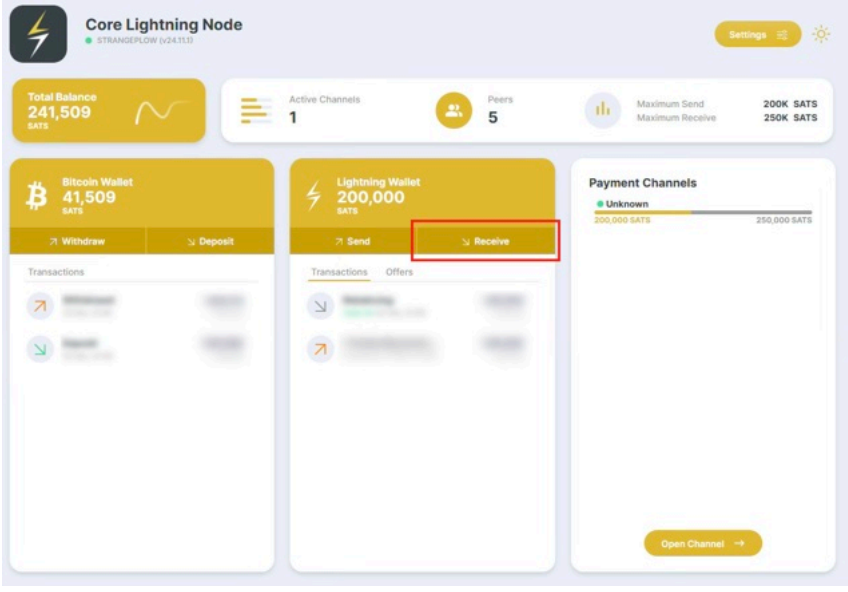
CLN과 비트코인 풀 노드 동기화가 다 될 때까지 시간이 조금 걸릴 수 있다. 동기화가 다 되면 CLN에서 우측 상단의 [Settings] → [Show node ID]를 누르고 노드 ID 옆 문서 모양의 복사 버튼을 눌러 노드 ID를 복사한다.



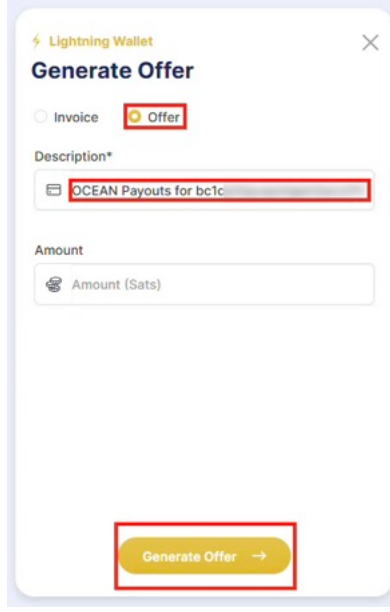
이제 자신이 운영하는 LND에서 이 CLN 노드를 피어로 추가하고, 채널을 개설하면 된다. LND 노드에서 피어를 추가하고 채널을 개설하는 방법은 '4부. 라이트닝 노드 운영 가이드'를 참고하라. CLN 측의 인바운드 유동성이 있어야 채굴 보상을 받을 수 있다. 또한, 지금처럼 오션 풀에서 라이트닝 네트워크로 채굴 보상을 받기 원하는 경우에는 LND에서 bfx-lnd0 혹은 bfx-lnd1 등의 노드와 채널을 맺으면 좋다. 해당 노드를 통해 채굴 보상이 전송되기 때문이다. 그러나 bfx 채널은 라우팅 시 아웃바운드가 안 차는 경향이 있고, 어차피 다른 채널의 라우팅을 통해 채굴 보상을 받을 수도 있으므로 잘 선택하길 바란다. bfx 노드들의 채널 개설 최소 용량은 약 100만 sats이다.



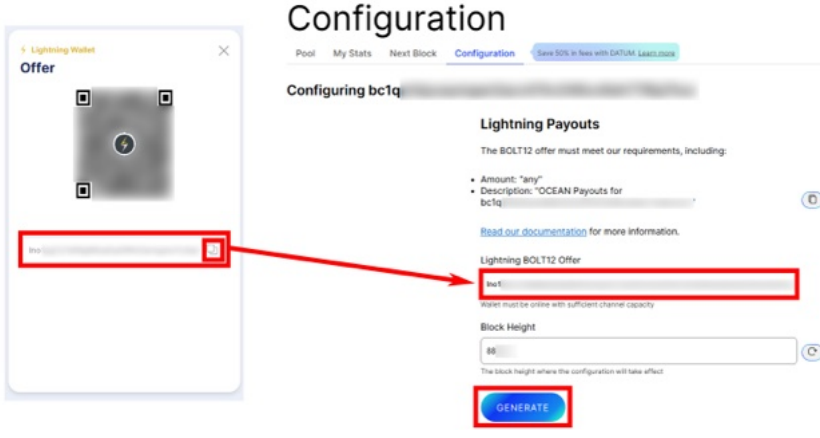
이제 CLN에서 가운데 있는 'Lightning Wallet' 아래의 [Receive]를 누른다.



[Offer]를 선택하고, 'Desciption'에 앞에서 오션 풀 웹사이트에서 복사했던 Description 데이터를 붙여넣기 한다. 그다음 아래에 있는 [Generate Offer]를 누른다.



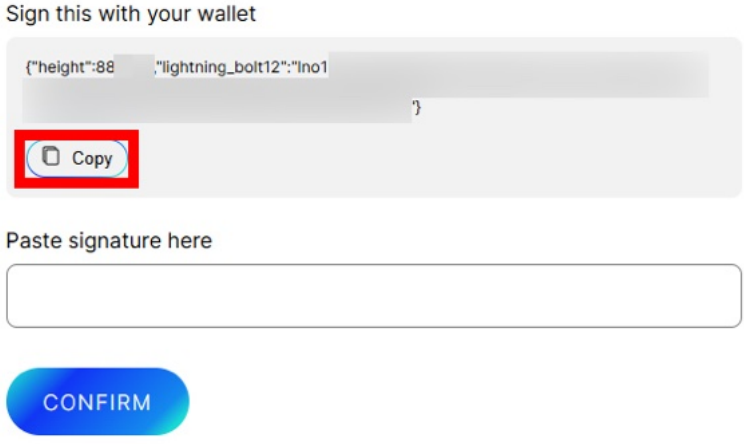
밑에 뜨는 Offer를 복사한 뒤 오션 풀 웹사이트의 'Lightning BOLT12 Offer' 칸에 붙여넣기 한다. 그 밑에 있는 [GENERATE]를 누른다.



메시지 서명하기

이제 메시지 서명만 하면 설정이 끝난다. 메시지 서명이란 메시지를 개인키로 서명한 것을 제시함으로써 내가 해당 주소의 개인키를 갖고 있다는 것을 증명하는 방법이다.

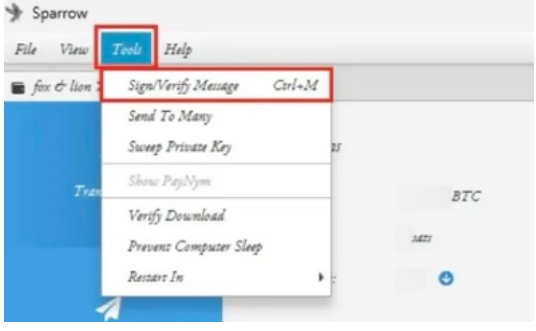
[GENERATE]를 눌렀다면 아래 어떤 문구가 나올 것이다. [Copy]를 눌러 이 텍스트를 복사한다.



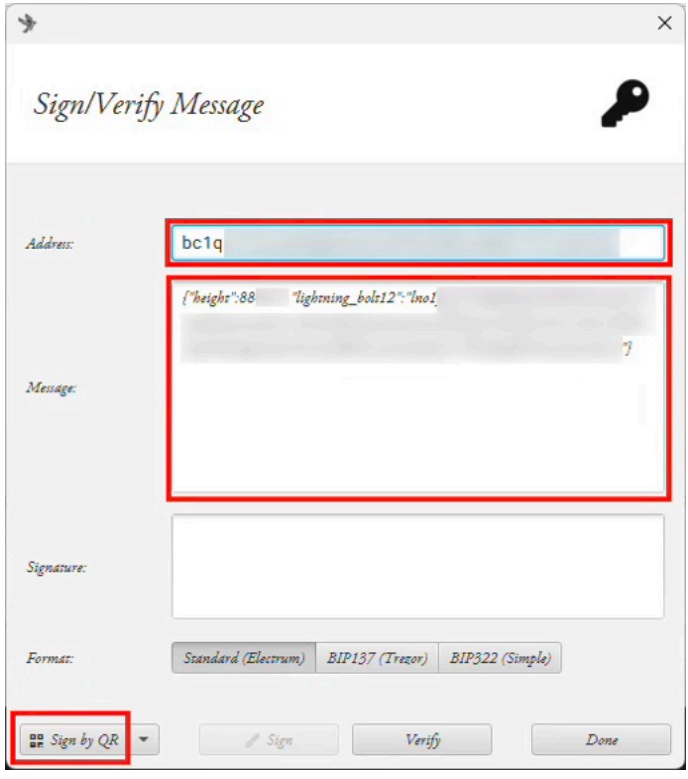
이제 에어-갭 지갑의 주소를 사용할 때(스패로우 워치-온리), 블루월렛(핫월렛)에서 생성한 주소를 사용할 때, 라이트닝 노드(LND)의 온-체인 주소를 사용할 때, 각각 어떻게 서명하는지 살펴볼 것이다.

에어-갭 지갑에 있는 주소를 보상 주소로 설정한 경우 PC에서 스패로우 워치-온리 지갑을 이용해 서명할 수 있다. 그러나 일부 에어-갭 지갑은 ':' 문자를 인식하지 못해 서명이 제대로 안 되니 참고하자. 키스톤은 홑따옴표를 붙이든 \를 이용하든 메시지 서명에 실패했다. 시드사이너는 제대로 작동되는 것을 확인했다. 시드사이너는 스패로우에서 보여주는 QR 코드를 스캔하면 바로 메시지 서명 창이 뜨며 니모닉을 입력하면 서명이 생성된다. 이를 웹캠으로 읽어오면 된다. 당연히 스패로우와 연동된 에어-갭 지갑에 속하는 비트코인 주소가 보상 주소로 설정되어 있어야 한다.

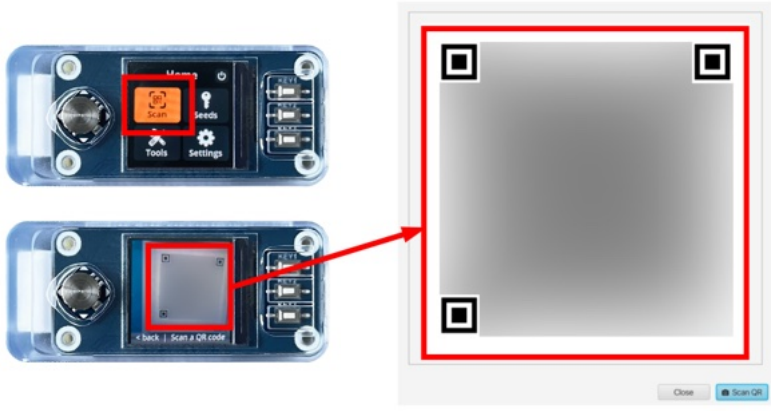
스패로우 상단의 [Tools] → [Sign/Verify Message]를 누른다.



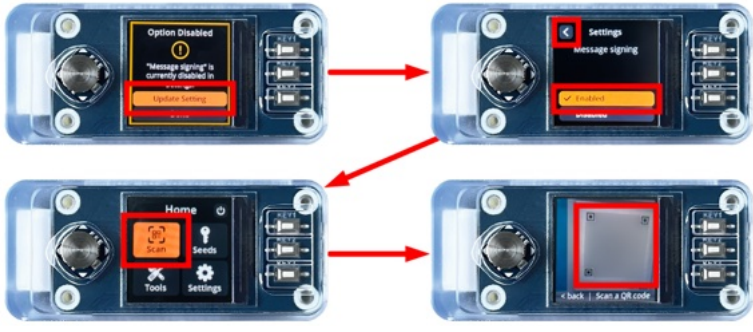
보상 주소를 설정하고, 메시지에 오션 풀 웹사이트에서 복사했던 메시지인 {height: …} 데이터를 붙여넣는다. 그다음 왼쪽 아래에 있는 [Sign by QR]을 누른다.



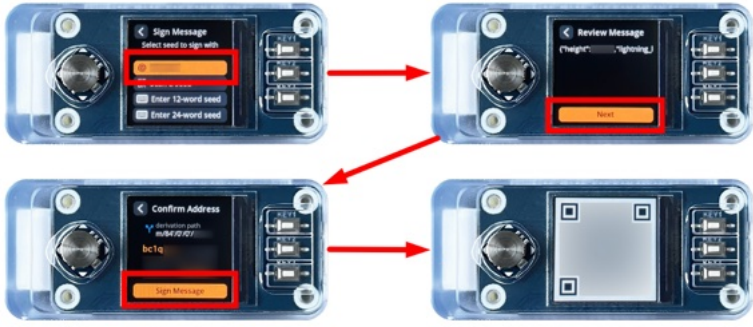
이 QR 코드를 에어-갭 지갑(시드사이너 등)으로 읽고 에어-갭 지갑에서 표시하는 서명을 읽어오면 된다. 시드사이너의 경우 니모닉을 입력하거나 시드 QR을 스캔한 뒤 바로 스캔하면 된다.



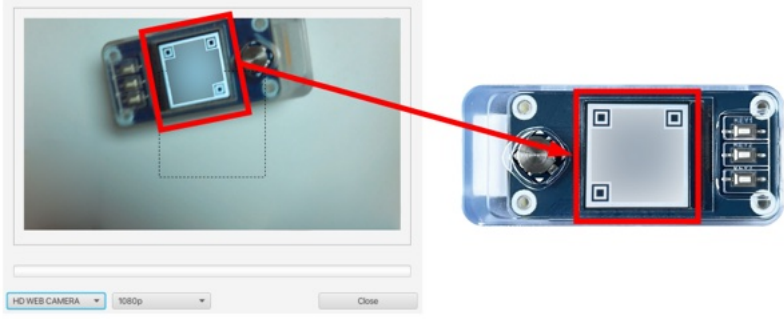
만약 메시지 서명 기능을 안 켰다는 안내문이 나올 때는 고급 설정에서 메시지 서명 기능을 켜고 다시 스캔하면 된다.



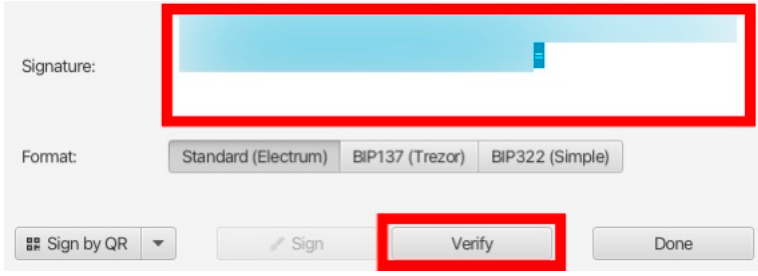
스캔이 제대로 되었다면 MFP가 나온다. 계속 다음을 누르면 서명 정보가 담긴 QR 코드가 나온다.



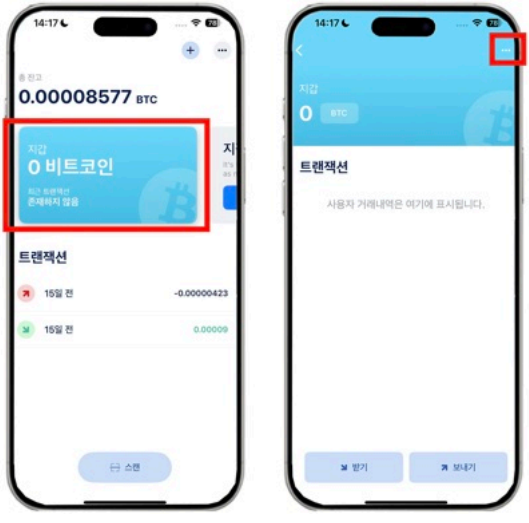
그다음에 스패로우에서 QR 코드 화면 아래에 있는 [Scan QR]을 눌러 웹캠을 통해 읽어오면 된다.



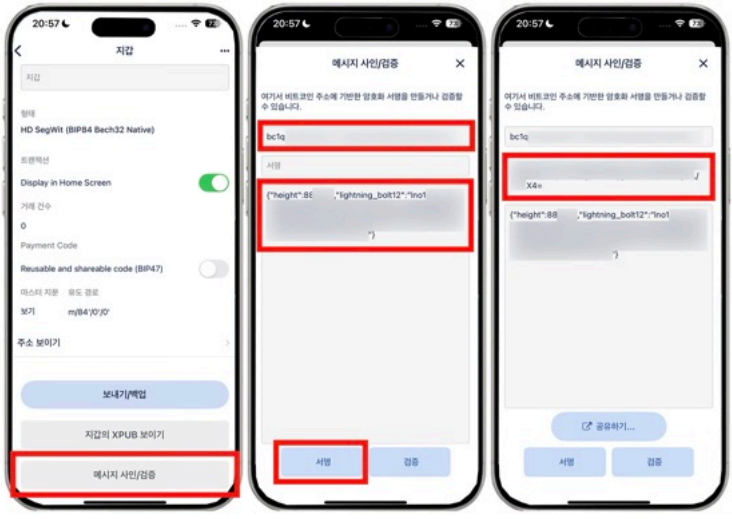
그다음 서명 부분을 복사한다. 참고로 아래에 있는 [Verify]를 누르면 서명이 올바른지 검증할 수 있다. 복사한 서명을 오션 풀 웹사이트에 붙여넣으면 된다.



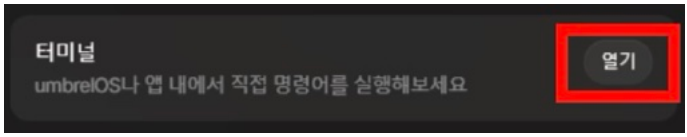
이제 블루월렛에서 생성한 주소를 사용한 경우를 살펴보자. 보상을 받을 곳으로 설정한 주소가 당연히 블루월렛 지갑에 속해 있어야 한다. 블루월렛에서 생성했던 지갑을 누르고 오른쪽 위 점 세 개를 누른다.

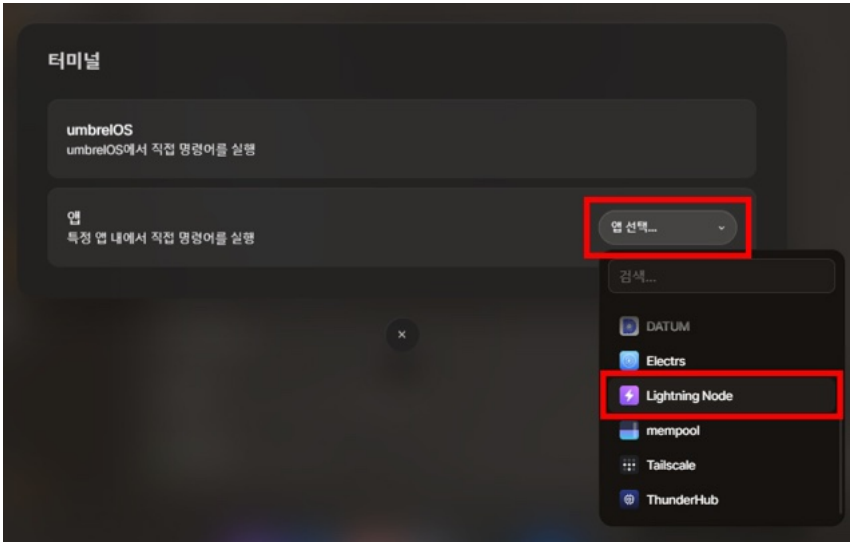


아래로 스크롤하여 [메시지 사인/검증]을 누르고, 맨 위에 보상받을 것으로 설정했던 주소를 입력한다. 그리고 서명은 비우고 그다음 칸에 오션 풀 웹사이트에서 복사했던 메시지인 데이터 {height: … }를 붙여넣는다. 그다음 [서명]을 누른다. 서명이 나오면 서명을 복사하여 오션 풀 웹사이트에 붙여넣으면 된다.



라이트닝 노드에서는 메시지 서명 기능을 이용하기 위해 터미널로 들어가야 한다. 엄브렐 홈 → 설정 → 고급 설정: [열기] → 터미널: [열기] → [앱 선택] → [Lightning Node]에 들어간다.





이제 터미널에 명령어를 쳐야 한다. 명령어는 다음과 같다.

```
lncli wallet addresses signmessage --address
  [보상 설정한 비트코인 주소] --msg '[메시지{"height":…}]'
```

주의할 점이 있다. 메시지인 {height: …}를 홑따옴표로 감싸야 한다. 따라서 명령어는 아래와 같은 형태가 될 것이다.

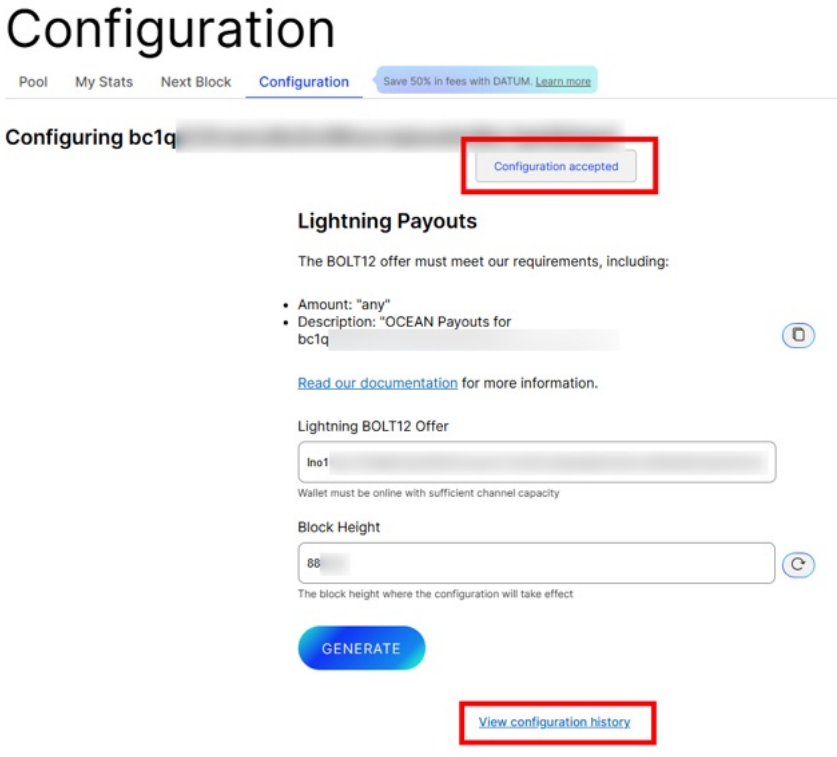
```
lncli wallet addresses signmessage --address
  bc1q…… --msg '{"height":……}'
```

명령어를 치고 엔터를 누른다.

그러면 서명이 나올 것이다. 서명 부분을 드래그하여 복사한다. 컴퓨터에서는 Ctrl + C 버튼이 안 먹히므로 마우스 오른쪽 클릭을 하고 복사를 눌러야 한다. 이렇게 나온 서명을 오션 풀 웹사이트에 붙여넣으면 된다.

오션 풀 웹사이트에 서명을 붙여넣은 뒤 [CONFIRM]을 누른다.

서명이 올바르다면 아래와 같은 화면이 나온다. 'Configuration accepted'가 뜨면 올바르게 설정된 것이다. 제대로 설정되었는지 확인하고 싶다면 아래 [View configuration history]를 눌러서 확인할 수 있다.



이렇게 해서 다텀으로 채굴 풀(오션 풀)에 참여하고, 라이트닝 네트워크로 보상을 받는 방법까지 설정했다. 보상은 오션 풀에서 블록을 채굴할 때마다 주어진다.

마무리하며

여기까지 따라오면서 당신은 돈을 저축해 보기도, 사용해 보기도 했다. 네트워크에 직접 참여하고, 전 세계에서 일어나는 모든 비트코인의 거래 장부를 직접 보유하고 업데이트했다. 누구도 신뢰하지 않고 스스로 잔액을 조회했다. 거래와 블록을 독립적으로 검증하고 전파했다. 네트워크를 직접 확장하고 보호했다.

이 책과 함께한 시간과 경험이 당신을 진정한 자유로 이끄는 데 도움이 되었기를 진심으로 바란다.