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.

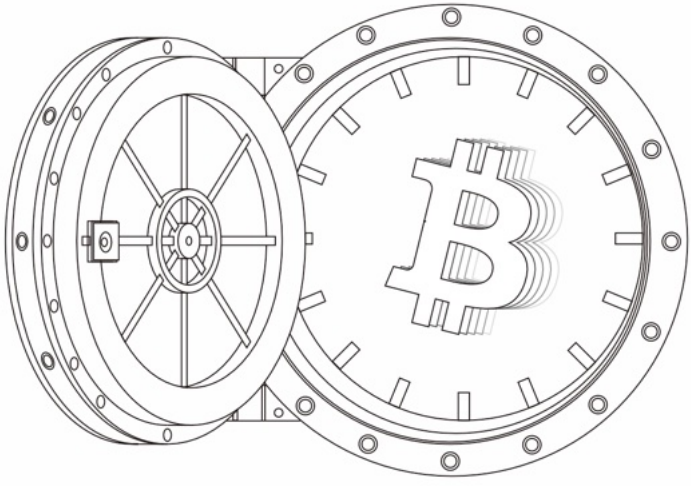
저자의 저작재산권 포기가 상표권, 저작인격권, 퍼블리시티권, 프라이버시권, 저자에게 귀속되지 않는 제3자의 권리 등의 포기를 의미하지 않습니다. 이를 무시하여 발생하는 문제에 대한 책임은 전적으로 사용자에게 있습니다.

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

5. 노스터 가이드

5. 노스터 가이드

| 노스터 사용을 위한 지식

기존 소셜 미디어의 문제점과 노스터

노스터Nostr, Notes and Other Stuff Transmitted by Relays(노스트르, 노스트라로도 종종 발음)는 탈중앙화된 소셜 네트워크 프로토콜이다. 기존 소셜 미디어들을 생각해 보자. 인스타그램을 사용하려면 인스타그램의 앱을 이용해야 하고, 개인정보와 포스트는 모두 인스타그램의 서버에 저장된다. 다른 소셜 미디어도 마찬가지다. 그러나 노스터는 중앙 서버 없이 누구나 참여할 수 있고, 심지어 자신이 서버 역할을 하는 릴레이를 운영할 수도 있다.

비트코인 사용 가이드에서 갑자기 소셜 미디어 프로토콜에 대한 이야기를 해서 당황할 수도 있다. 그러나 노스터는 소셜 미디어들의 문제를 해결하기 위해 나왔지만 그 이상의 의미를 지닌다. 표현의 자유를 위한 것이며, 현재는 비트코인, 라이트닝 네트워크와도 떼놓을 수가 없는 관계가 되었다. 예를 들어 노스터에서는 '잽' 기능을 통해 마음에 드는 글이나 콘텐츠에 소액의 비트코인을 전송할 수 있다. 이는 라이트닝 네트워크를 이용한다. 즉, 예술가나 창작자 등 콘텐츠를 생산하는 사람들에게 좀 더 쉽게 후원이 갈 수 있게 한다. 이 외에도 노스터와 라이트닝 지

갑을 연결하기 위한 '노스터 지갑 연결(NWC)' 프로토콜이 노스터 클라이언트가 아니더라도 라이트닝 지갑을 간편하게 이용할 수 있도록 해주기도 한다.

노스터의 필요성을 이해하려면 먼저 기존 소셜 미디어들의 문제점을 이해해야 한다. 크게 세 가지 문제가 있는데, 첫째로 기존 소셜 미디어들은 서버가 중앙화되어 있기 때문에 특정 발언을 검열할 수 있다. 여기에 국가가 중앙화된 소셜 미디어 운영자에게 압박을 가하면 우리는 표현의 자유를 잃게 된다. 각 소셜 미디어에는 감시, 검열 전담 부서가 있으며, 우리가 올리는 말과 콘텐츠들은 알고리즘과 사람들에 의해 실시간으로 감시되고 있다.

> 표현의 자유는 프라이버시보다도 더 중요한, 열린 사회의 핵심이다. 우리는 어떠한 표현도 제한하지 않기를 원한다. 여러 사람이 같은 공간에서 이야기한다면, 각자는 서로 지식을 공유하고 집단적으로 축적할 수 있다. 전자 통신의 힘은 이러한 집단적 소통을 가능하게 했으며, 우리가 이를 원치 않는다고 해서 사라지지 않을 것이다.
>
> 에릭 휴즈, 「사이퍼펑크 선언문」

두 번째 문제는 기존 소셜 미디어들이 방대한 양의 개인 데이터를 수집하고 있다는 사실이다. 이름, 성별, 나이, 연락처, 주소는 물론이고, 관심사와 소득까지 유추하여 보관한다. 어떤 포스트를 좋아하고, 어떤 포스트를 싫어하는지 수집하고, 심지어 어디서 스크롤을 내리고, 어디서 한참 머무르는지도 추적한다. 소셜 미디어들은 이렇게 수집한 데이터를 판매하여 막대한 수익을 올린다. 소셜 미디어의 타깃 광고는 사는 곳, 나이, 성별, 관심사, 소득, 자녀 유무 등에 따라 어떤 광고를 누구에게 보여줄지 정밀하게 설정할 수 있다. 즉, 소셜 미디어 이용자들은 무료로 소셜 미디어를 이용하는 소비자인 게 아니라, 진열장에 전시된 상품이 되는 것이다. 광고주가 와서 "나는 20대, 서울에 사는 소득이 낮지

만 돈을 벌고 싶은 사람들을 구매하고 싶다"라고 하면 소셜 미디어는 진열장에 전시된 사람들을 보여주는 셈이다. 암호학자인 브루스 슈나이어Bruce Schneier는 다음과 같이 말했다.

> 어떤 서비스가 무료라면, 당신은 고객이 아니라 상품이다.
>
> 브루스 슈나이어 지음, 이현주 옮김, 『당신은 데이터의 주인이 아니다』, 반비, 2016.

소셜 미디어는 진열된 상품들이 도망가지 않고 더 오래 머물도록 상품들을 더 자세히 파악하고, 알고리즘을 통해 묶어 놓을 수밖에 없다. 소셜 미디어들은 사용자들이 다른 사람들과 한 대화와 사진, 영상들뿐 아니라, 소셜 미디어 사용과 관계없는 음성이나 다른 앱 사용 방식까지 수집하는 것으로 의심받아 문제가 된 적도 있다. 사용자들의 개인정보와 대화, 사진, 영상은 AI가 학습하는 재료가 된다. AI는 사용자들에 대해 공부하고 사용자의 현재 상황에 적절한 광고를 끼워 넣는다. 사용자가 살이 찐 것에 대한 관심사를 보이거나 관련 키워드와 상호작용했을 경우 다이어트 식품을 광고에 올리는 것이다.

첫 번째 문제와 두 번째 문제가 결합하면 소셜 미디어는 사람들의 생각을 통제할 능력을 갖게 된다. 금지하고 싶은 생각들을 표현하는 사람들의 계정은 정지시키고, 그러한 포스트는 사람들에게 보이지 않게 하면서, 알고리즘을 통해 유도하고 싶은 생각의 포스트만 보여주는 것이 가능하다. 즉, 사용자의 표현의 자유를 막고 특정 사고방식을 강요할 수 있다는 뜻이다.

세 번째 문제는 개인정보와 민감한 정보들을 소셜 미디어가 수집하면서 이렇게 수집한 정보들이 정부나 해커들의 목표가 된다는 것이다. 정부는 안전을 위한다는 이유로 소셜 미디어 측에 사람들의 개인정보와

민감한 정보를 요구할 수 있고, 해커들은 이 정보를 가져다가 암시장에서 판매하거나 해킹, 사기에 이용한다.

노스터는 이러한 문제들을 해결하기 위해 나온 프로토콜이다.

노스터 클라이언트

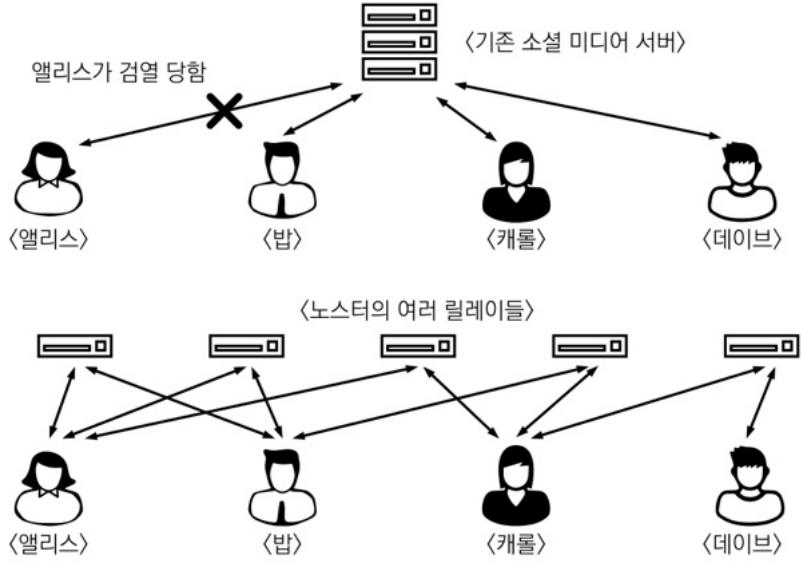
노스터는 프로토콜이기 때문에 노스터를 이용하기 위한 여러 클라이언트가 존재한다. 인스타그램을 이용하기 위해서는 인스타그램 앱을 이용해야 하고, X를 이용하기 위해서는 X 앱을 이용해야 하는 것과는 다르다. 그것보다는 인터넷 웹 브라우징을 위해서 웹 브라우저로 크롬을 사용할 수도 있고, 사파리를 사용할 수도 있고, 엣지를 사용할 수도 있는 것과 비슷하다. 노스터를 이용하기 위해서는 프라이멀, 다무스, 애머시스트, 피닉스, 노스트루델 등 엄청나게 많은 앱을 이용할 수 있다. 당연히 클라이언트들은 노스터 프로토콜 위에서 구축되므로 각각 호환된다. 프라이멀 앱에서 쓴 글이나 보낸 잽이 다무스 앱에서도 보이는 식이다.

각각의 클라이언트들은 서로 다른 기능에 특화되어 있기도 하다. 어떤 클라이언트는 일반적인 소셜 미디어 기능에 집중하고, 어떤 클라이언트는 대화, 블로그 형식의 포스트, 팟캐스트나 음악 스트리밍, 영상 스트리밍 기능 등에 각각 집중한다. 다양한 클라이언트들은 노스터 프로토콜과 호환되게 하면서 여러 기능들을 확장하고 있다. 엄청나게 다양한 클라이언트가 있으니 목적에 따라 다양하게 이용하면 된다.

노스터 릴레이와 이벤트, 작동 원리

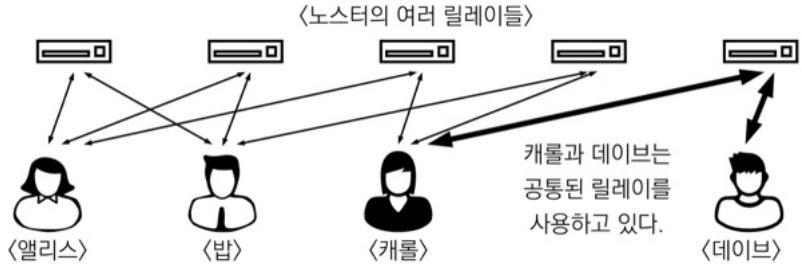
노스터에서 릴레이는 일반 소셜 미디어의 서버와 비슷하다. 그러나 누구나 릴레이를 운영할 수 있고, 훨씬 기능이 단순할 뿐이다. 사용자들은 보통 릴레이를 여러 개 연결하기 때문에 노스터의 검열 저항성은 극대화된다. 하나의 서버만 장악하면 사용자를 검열할 수 있는 기존 소셜 미디어와 다르게, 노스터에서 검열하려면 사용자가 연결한 모든 릴레이가 사용자의 글을 제공하는 것을 막아야 하기 때문이다. 그래봤자 사용자는 다른 릴레이에 연결하거나 직접 릴레이를 운영하면 끝이기 때문에 노스터에서 특정 글을 검열하는 것은 불가능에 가깝다.

다음 그림을 보자. 기존 소셜 미디어의 네트워크 구조처럼 중앙화되어 있는 경우에는 한 사람의 글이나 계정을 검열하기가 쉽다. 그림에서는 앨리스가 검열당하고 있다. 그러나 그 아래에 있는 그림처럼 사용자



들이 여러 릴레이들에 연결되어 있는 경우에는 누구 한 명을 검열하기가 쉽지 않다.

숙지해야 할 점이 있다. 다른 사람의 글을 보려면 그 사람과 1개 이상의 공통된 릴레이가 연결되어 있어야 한다. 다음과 같은 상황에서 캐롤은 데이브가 올린 글을 볼 수 있지만, 앨리스나 밥은 데이브가 올린 글을 볼 수 없다. 공통으로 연결된 릴레이가 없기 때문이다.



노스터에서 오가는 모든 글, 댓글, 다이렉트 메시지(이하 DM), 반응, 팔로우 정보, 프로필 변경, 잽 결제 요청 등은 전부 '이벤트'라는 형태로 표현된다. 이벤트는 JSON이라는 구조화된 표현 방식을 따른다.

사용자가 노스터 클라이언트 앱을 이용해 글을 작성했다고 해보자. 그러면 클라이언트 앱은 해당 내용을 JSON 이벤트 형식으로 만들고 개인키(비밀키)로 서명한다. 서명에 대해서는 잠시 후에 알아보자. 릴레이는 이렇게 서명된 이벤트를 저장하고 다른 클라이언트에 전달만 한다. 메시지를 해석하거나 수정하지 않고 오직 전달만 할 뿐이다. 서명을 하려면 노스터의 개인키가 있어야 하므로 릴레이는 메시지를 수정하거나 위조할 수가 없다. 릴레이를 신뢰할 필요가 없는 것이다. 또한 노스터는 텍스트 기반 프로토콜이므로 일반 소셜 미디어 서버를 운영하는 것보다 훨씬 낮은 사양으로도 릴레이 서버를 돌릴 수 있다.

노스터 구현 제안(NIP)

노스터는 프로토콜이므로 표준화된 기능이 필요하다. 이러한 기능들은 노스터 구현 제안NIP, Nostr Implementation Possibilities을 통해 제안된다. 각 노스터 앱들이 호환성을 유지해야 하는데, 클라이언트 앱들마다 다른 방식으로 기능을 확장한다면 호환이 안 될 것이기 때문이다. 따라서 노스터 생태계를 확장하면서도 호환성을 유지하기 위해 NIP가 있는 것이다. '비트코인 개선 제안'인 BIP와 비슷하게 의무 규격은 아니다.

몇 가지 주요 NIP를 살펴보자. NIP-04는 공개키 기반 종단간 암호화 방식을 쓰는 DM을 정의한다. NIP-05는 노스터 주소로, 사람이 읽기 힘든 노스터 공개키를 읽기 쉬운 이메일 형태의 노스터 주소와 연결하는 것을 정의한다. 덕분에 사칭 등의 피싱도 방지할 수 있다. NIP-09는 이벤트 삭제 요청 형식을 정의한다. 사실 NIP-09는 이벤트를 삭제하는 것은 아니고 숨김 처리하는 것이다. NIP-19에서는 노스터 개인키와 공개키의 형태인 nsec, npub 등의 Bech32 인코딩 식별자를 정의한다. note나 nevent 등의 인코딩 식별자도 정의한다. NIP-23은 블로그나 칼럼 스타일의 긴 콘텐츠 형식을 정의한다. NIP-57은 라이트닝 네트워크를 이용해 포스트나 계정에 비트코인을 보내는 잽 방식을 정의한다.

클라이언트나 릴레이가 모든 NIP를 따를 의무는 없다. 그러므로 클라이언트가 어떤 NIP 기능을 구현했는지, 내가 연결하는 릴레이가 어떤 NIP를 지원하는지 확인해야 한다. 예를 들어보자. 내가 이전 글을 삭제하는(숨김 처리하는) NIP-09 기능을 사용하고 싶다면 글 삭제 기능이 있는 클라이언트 앱을 사용해야 하고, 무엇보다 NIP-09를 지원하는 릴레이와 연결해야 한다. 이것은 매우 중요하다. 만약 NIP-09를 지원하

지 않는 릴레이가 하나라도 연결되어 있고 그 상태에서 글을 작성해서 올렸다면, 미지원 릴레이에 게시된 해당 글은 숨김 처리되지 않는다. 지원 릴레이라도 정책에 따라 요청을 받지 않거나, 다른 릴레이를 통해 재유통될 수 있어 영구 삭제는 보장되지 않는다. 릴레이들은 보통 어떤 NIP를 지원하는지에 대한 정보를 NIP-11에 따라 공개한다. 따라서 릴레이가 어떤 NIP들을 지원하는지 꼼꼼하게 보는 것이 좋다.

개인키(nsec)와 공개키(npub), 노스터 주소

노스터 이용을 위해서는 처음에 개인키-공개키 쌍을 생성해야 한다. 일반 소셜 미디어는 이름, 나이, 주소, 휴대폰 번호 등을 통해 신원 인증을 하고 계정을 생성해야 하지만 노스터에는 그런 것이 없다. 엄밀히 말하자면 개인키는 단지 숫자일 뿐이므로 계정을 생성하는 데 무언가 허락이 필요한 것이 아니라 그저 랜덤한 숫자를 고를 뿐이다. 비트코인의 개인키-공개키와 비슷하다.

노스터에서 개인키는 nsec이라는 형태로 표현된다. 물론 니모닉으로 표현할 수도 있다. 클라이언트는 랜덤한 숫자를 골라 그것을 nsec의 형태로 바꿔서 사용자에게 보여준다. nsec이 노출되면 누구나 내 노스터 계정에 접근할 수 있게 된다. 따라서 안전한 곳에 백업하는 것이 중요하다. 웹 브라우저에서는 로그인할 때마다 개인키를 이용하지 않고, 주로 알비 등의 확장 프로그램을 이용한다. 개인키를 웹 브라우저에 직접 입력할 때마다 보안이 감소하기 때문이다.

공개키는 npub이라는 형태로 표현된다. 다른 사용자에게 자신의 계정을 팔로우하라고 알릴 때 이 npub을 알려주거나, npub 정보가 담겨 있는 QR 코드를 전달하면 된다. 그런데 npub은 외우기가 너무 어

렵다. 그래서 NIP-05에 따라 이메일 형식과 같은 노스터 주소를 npub과 연결할 수 있다. 라이트닝 주소와 비슷하다고 생각하면 된다. 자신의 npub과 노스터 주소를 연결해 놓으면, 상대방에게 노스터 주소만 알려줘도 상대방이 내 계정을 팔로우할 수 있다.

앞에서 잠깐 봤듯이 각 이벤트는 사용자의 노스터 개인키인 nsec으로 서명된다. 그렇게 하여 이 이벤트가 정말로 이 사용자가 발생시킨 게 맞는지 확인하는 것이다. 공통된 릴레이를 사용하고 있는 다른 사용자들은 해당 사용자의 공개키를 통해 이벤트의 서명을 검증할 수 있다. 이러한 과정은 클라이언트에서 구현되기 때문에 릴레이를 신뢰할 필요가 전혀 없다.

노스터의 DM과 종단간 암호화

노스터의 이벤트 대부분은 공개 릴레이를 통해 누구나 열람할 수 있다. 그러나 상대방에게 보내는 메시지인 DM은 누구나 열람할 수 있으면 안 된다. 이 메시지는 메시지 송신자와 수신자만 열람할 수 있어야 한다. 그래서 여기에는 종단간 암호화E2EE, End-to-End Encryption 기술이 쓰인다.

중앙 서버를 통하는 소셜 미디어, 혹은 메신저 앱의 경우 메시지는 대부분 해당 서버의 키로 암호화되어 전송된다. 이런 경우 서버는 사용자들이 무슨 대화를 하는지 엿볼 수가 있다.

이를 막기 위해 종단간 암호화라는 기술이 있다. 잠시 비트코인의 서명 검증 과정에 대해 생각해 보자. 서명을 할 때는 개인키로 하고, 검증은 공개키로 한다. (서명이 브로드캐스트 된 이후에) 공개키는 말 그대로 공개되어 있으므로 누구나 서명을 검증할 수 있다. 종단간 암호화는

반대로 생각하면 된다. 상대방의 공개키로 메시지를 암호화해 전송하고, 이를 풀기 위해서는 그 공개키에 대응하는 개인키가 필요하다. 개인키가 있는 사람만 실제 메시지가 무엇인지 알 수 있는 것이다.

노스터의 종단간 암호화는 타원곡선 디피-헬만Elliptic-curve Diffie-Hellman, ECDH 키 교환 방식을 사용한다. 원리를 간략하게 설명하자면 메시지 발신자는 자신의 개인키와 수신자의 공개키를 조합해 암호키를 생성한다. 수신자도 자신의 개인키와 발신자의 공개키를 조합해 발신자가 만든 암호키와 똑같은 암호키를 만들 수 있다. 이 암호키로 메시지를 암호화하기 때문에 발신자와 수신자만 메시지를 해독할 수 있다.

발신자와 수신자를 제외한 제3자는 메시지 내용이 무엇인지 알 수가 없다. 릴레이도 암호화된 메시지만 전달하기 때문에 전송되는 메시지 내용이 무엇인지 알 수 없다. 그러나 메시지를 누구와 주고받는지는 제3자가 알 수 있다. 그래서 현재는 NIP-44의 암호화 방식과 NIP-59의 발신자 메타데이터 숨기기 방식이 통합된 NIP-17 DM 규격이 정의되어 있다.

잽(Zaps)과 NWC (노스터 지갑 연결)

노스터는 텍스트 기반의 탈중앙화 프로토콜이지만, 여기에 라이트닝 네트워크를 이용해 비트코인을 전송하는 기능이 더해졌다. 이는 NIP-57에서 명시되었고, 이 기능을 잽Zaps이라고 한다.

기존 소셜 미디어의 수익 모델을 생각해 보자. 중앙화된 소셜 미디어 서비스들은 사용자들의 시간을 광고주에게 판매한다. 즉, 광고주가 비용을 지불하면 플랫폼이 그 수익을 전부 가져가거나, 플랫폼이 콘텐츠 생산자에게 수익을 일부 나눠 준다.

비트코인과 라이트닝 네트워크를 통해 개인 대 개인으로 가치를 빠르게 보낼 수 있게 되면서, 이런 중앙화된 수익 구조를 탈피할 수 있게 되었다. 좋은 콘텐츠를 생산한 사람에게 사용자가 직접 잽을 통해 비트코인을 보낼 수 있는 것이다. 잽은 단순히 마음에 든다는 '좋아요' 반응을 넘어 실제 금전적 가치를 창작자에게 전송하는 것이다.

사용자가 자신의 프로필에 라이트닝 주소(혹은 LNURL)를 등록하면 잽을 받을 수 있게 된다. 잽도 이벤트 형식으로 만들어진다. 이 잽 요청zap request 이벤트에는 NIP-57 표준에 따라 결제 금액, 메모, 대상 이벤트(어떤 글에 잽을 보내는지 등), 발신자의 서명이 포함되어 있다. 잽을 받을 사람이 등록한 LNURL을 통해 인보이스가 생성되어 잽을 보내는 사람에게 전달되면, 잽을 보내는 사람은 라이트닝 지갑을 이용해 이 금액을 결제한다. 그러면 잽 영수증zap receipt 이벤트가 생성되어 릴레이에 게시된다. 이를 통해 다른 사람들도 어떤 글에 누가 얼마의 잽을 보냈는지 등을 확인할 수 있다. 비공개 잽도 가능하다. 이렇듯 잽은 긍정적 반응과 경제적 보상을 동시에 전달한다.

잽 기능을 사용하려면 사용자가 라이트닝 지갑을 사용해야 한다. 그런데 노스터 클라이언트와 라이트닝 지갑이 항상 같은 앱일 필요는 없다. 여러 라이트닝 지갑을 각각의 노스터 클라이언트와 연동할 수 있도록 해주는 것이 노스터 지갑 연결NWC, Nostr Wallet Connect 표준이며, 이는 NIP-47에서 명시되어 있다. NWC를 사용하면 클라이언트가 NIP-47 이벤트 형식으로 결제 요청을 라이트닝 지갑에 전달하고, 라이트닝 지갑이 이를 개인키로 서명하여 승인하거나 거부한다. 승인된 경우, 결제 결과가 다시 클라이언트로 전달된다. 각 이벤트는 모두 서명되어 있으므로 릴레이나 제3자가 결제 내용을 변조할 수 없다.

노스터의 단점과 광고 필터, 리스트 구독

노스터에는 치명적인 단점이 하나 있다. 스팸이 쉽게 퍼진다는 것이다. 기존 중앙화된 소셜 미디어 구조에서는 플랫폼 운영자가 자신들과 계약하지 않은 광고나 스팸 글들을 삭제하거나, 숨기거나, 알고리즘을 이용해 노출되지 않게 한다. 노스터는 중앙 관리자가 없기 때문에 아무 대처를 하지 않으면 스팸성 봇들이 댓글을 무차별적으로 달 수 있다.

그래서 각 클라이언트들은 스팸성 글을 걸러낼 수 있는 더 좋은 필터를 만들기 위해 서로 경쟁한다. 릴레이들도 자체적인 필터 정책을 도입할 수 있다. 예를 들어 릴레이에는 일정 시간마다 최대 몇 개의 이벤트 게시를 할 수 있는지 제한을 둘 수 있다. 유료로 연결할 수 있는 릴레이도 있는데, 양산되는 광고 봇들은 이런 유료 릴레이에서 활동하기 어렵다.

다만, 필터링이 클라이언트나 릴레이에 의해 일방적으로 적용될 경우 자칫하면 검열 논란이 생길 수 있다. 또한, 이러한 기능은 보통 클라이언트 측에서 유료 기능으로 제공하는 경우가 많다. 따라서 이보다는 사용자가 직접 선택, 설정하는 편이 나을 것이다. 노스터에서는 NIP-51에 의해 팔로우 리스트, 뮤트 리스트, 화이트 리스트 등을 만들 수 있다. 뮤트는 해당 사용자의 글을 자신의 피드에서 노출시키지 않는 것을 의미한다. 어떤 클라이언트들은 뮤트 리스트 가져오기/내보내기 기능을 제공한다. 이를 통해 사용자들이 관리하는 여러 뮤트 리스트를 가져올 수 있다.

노스터는 스팸성 광고를 잡기 위해 발전하고 있는 중이다. 더 나은 방법들이 점점 등장할 것으로 기대한다.

정리해 보자. 기존 중앙화된 소셜 미디어에서는 플랫폼 운영자나 정부, 기업의 압력에 따라 특정 발언이나 계정이 손쉽게 차단될 수 있었다. 그러나 노스터는 누구나 릴레이를 운영할 수 있고, 사용자가 여러 릴레이를 동시에 연결할 수 있기 때문에 어느 한 곳이 차단되더라도 다른 경로를 통해 소통이 가능하다. 이 구조는 표현의 자유를 지키는 방패가 된다. 따라서 노스터는 강력한 검열 저항성을 갖는다.

노스터는 잽이라는 라이트닝 네트워크 기반의 소액 결제 기능을 통해 창작자와 이용자가 개인 대 개인으로 직접 연결되는 새로운 후원 문화를 만들어 가고 있다. 기존 플랫폼에서는 광고 수익, 유료 구독, 중개 수수료에 의존했지만, 노스터에서는 중간자 없이 창작자가 곧바로 보상을 받을 수 있다. 이는 광고에 종속된 알고리즘 구조에서 벗어나, 실제로 가치 있는 콘텐츠가 사용자들에 의해 직접 평가받고 보상받는 구조를 만든다.

노스터는 단순한 소셜 미디어 프로토콜을 넘어, 표현의 자유를 보장하고 창작자 중심의 수익 구조를 지원하는 새로운 인터넷 문화의 기반으로 급격히 성장하고 있다.

| 프라이멀 사용 방법

노스터를 처음 시작하는 사용자라면 자신의 상황에 따라 어떤 앱을 사용할지 선택할 수 있다. 만약 라이트닝 노드를 직접 운영하고 있다면 아이폰 사용자는 다무스Damus, 안드로이드 사용자는 애머시스트Amethyst, 데스크탑 웹 브라우저에서는 피닉스Phoenix 등을 추천한다. NWC를 통한 연결로 자신의 라이트닝 노드에서 잽을 보낼 수 있기 때문이다.

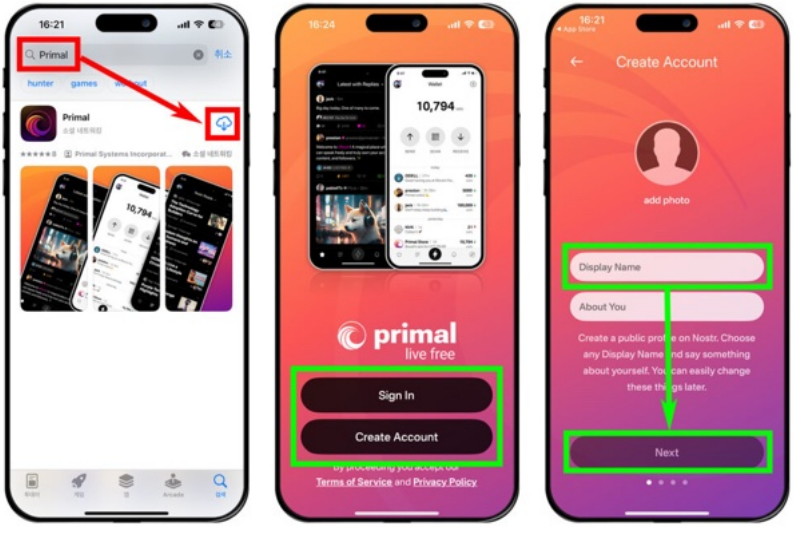
만약 라이트닝 노드를 운영하지 않고, 노스터를 처음 이용한다면 프라이멀Primal 앱 사용을 추천한다. 프라이멀은 앱 내에서 자체적으로 라이트닝 지갑을 이용할 수 있기 때문에 잽을 주고받기가 더욱 쉽다. 그러나 분명히 인지해야 할 사실은 프라이멀에서 사용하는 지갑은 라이트닝 수탁 서비스이므로 거래소와 같은 위험이 있다는 것이다. 월렛 오브 사토시나 블링크와 비슷하다고 생각하면 된다. 이제 프라이멀 앱 사용 방법에 대해 알아보자.

프라이멀 앱 설치 및 개인키-공개키 쌍 생성

앱스토어 또는 구글 플레이스토어에서 'Primal'을 검색하고 앱을 다운로드한다.

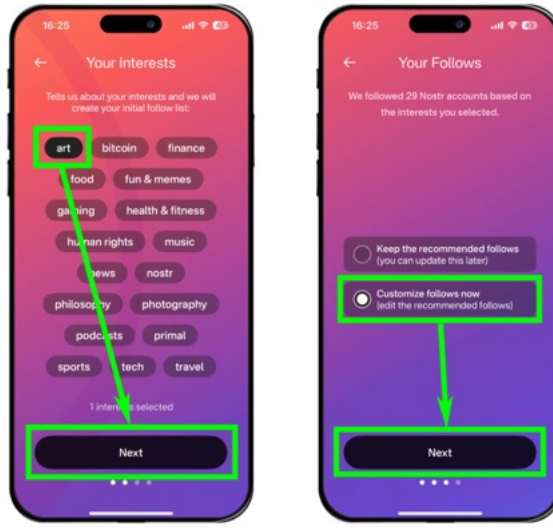
이전에 노스터를 사용한 적 없다면 [Create Account]를 누른다. 만약 이전에 노스터를 사용한 적이 있어서 노스터 개인키인 nsec이 있다면 [Sign In]을 눌러 nsec을 입력하고 로그인할 수도 있다.

[Display Name]에 유저네임을 입력하고 [Next]를 누른다.

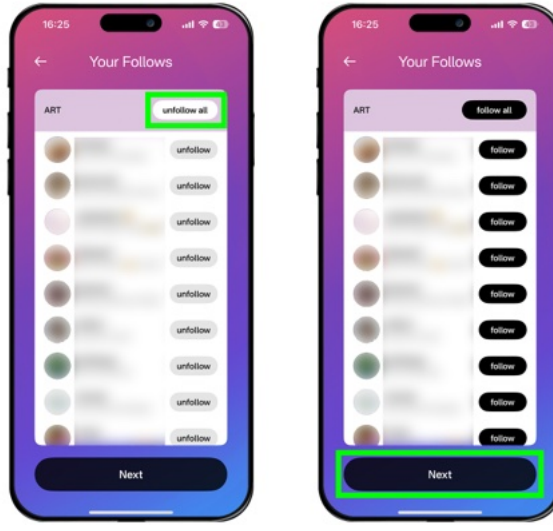


관심사를 선택하라는 창이 나온다. 그런데 여기서 관심사를 선택하면 자신이 팔로우를 원치 않는 계정들까지 전부 팔로우하게 된다. 따라서 일단 [art]만 선택한 뒤 [Next]를 누른다. 뒤에서 해제할 것이다.

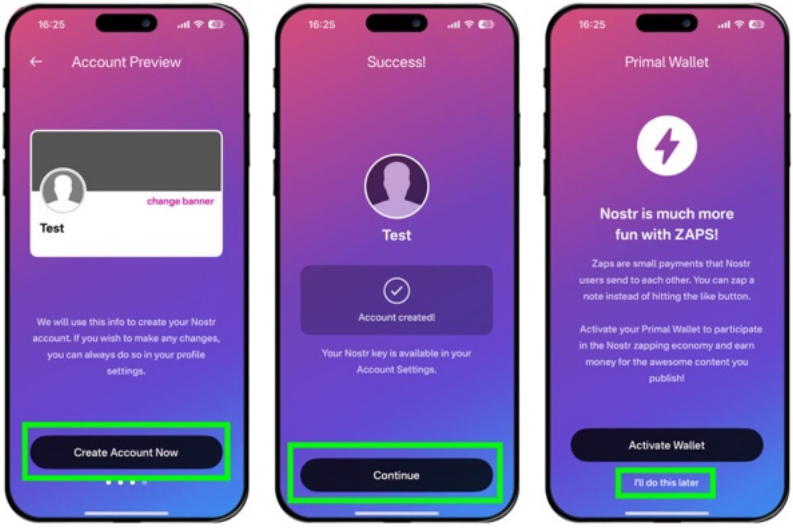
다음 화면으로 넘어가면 [Customize follows now]를 선택하고, [Next]를 누른다.



앞에서 말한 것처럼 모든 관심사를 끌 것이다. 'ART' 옆에 있는 [unfollow all]을 누르고, 아래에 있는 [Next]를 누른다.

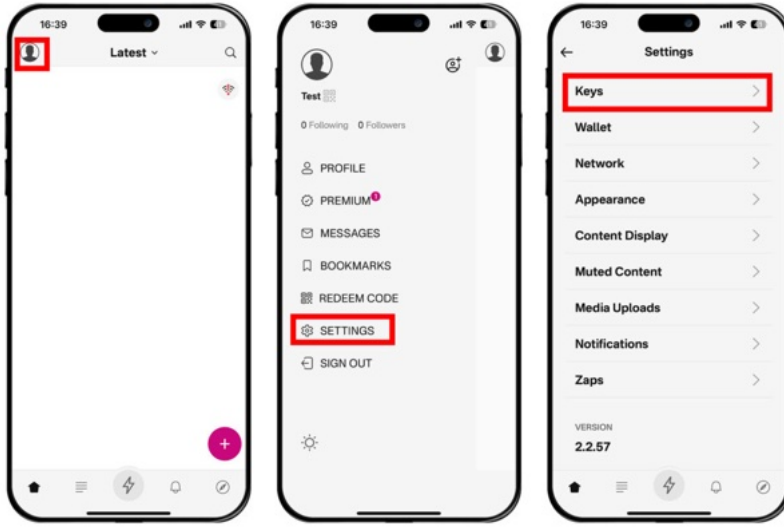


[Create Account Now] → [Continue] → [I'll do this later]를 누른다.

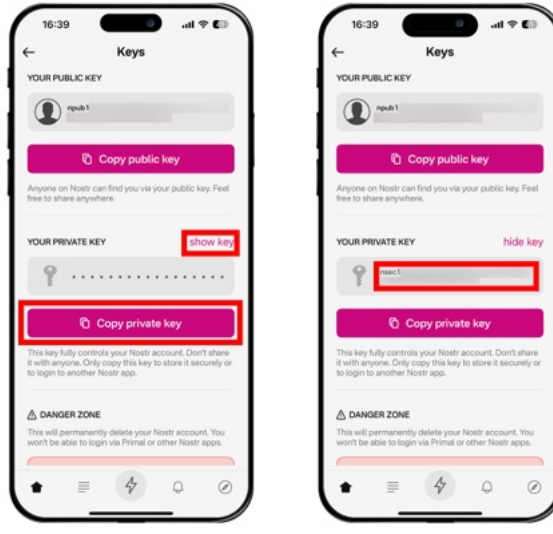


그러면 개인키-공개키 쌍이 생성된 것이다. 노스터는 다른 중앙 집중화된 소셜 미디어 플랫폼들과 달리 비트코인처럼 개인키-공개키 쌍을 만들면 그게 자신의 계정이 된다. 개인키는 nsec이라 하며, 공개키는 npub이라 한다. 따라서 개인키인 nsec을 백업해 놓는 것은 매우 중요하다.

왼쪽 상단의 프로필 사진을 누른다. 그다음 [SETTINGS] → [Keys]에 들어간다.

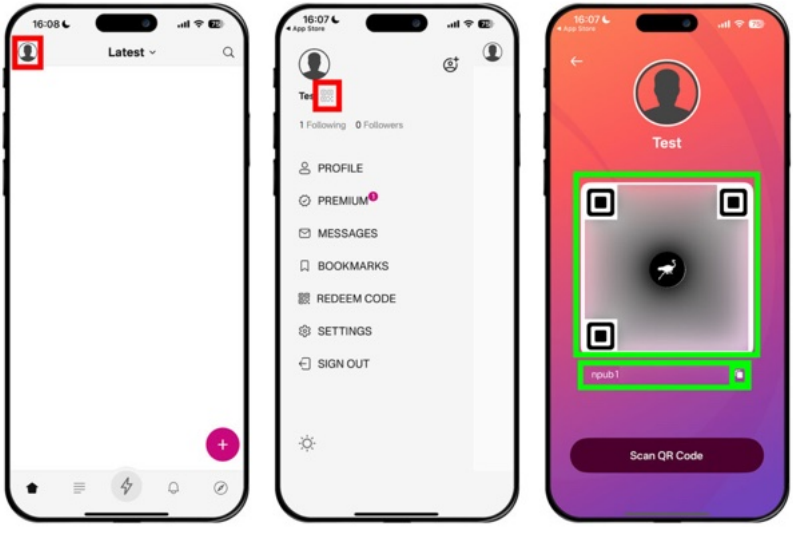


'PRIVATE KEY' 옆에 나오는 [show key]를 누르면 개인키가 보인다. 종이에 적는 등 물리적으로 백업하거나, [Copy private key]를 눌러 개인키를 저장할 수 있다(암호화된 상태로 저장하는 것을 추천한다).



다른 사람들에게 npub 알려주기

누군가에게 자신의 노스터 계정을 알려줄 때는 노스터 공개키인 npub을 알려주면 된다. 먼저 프라이멀에서 왼쪽 상단 프로필 모양을 누른다. 유저네임 옆에 있는 QR 코드 모양을 누른다. 그러면 QR 코드가 나오는데 이 QR 코드를 상대방에게 보여주거나, 그 밑에 있는 npub 오른쪽의 복사 버튼을 눌러 상대방에게 보내주면 된다.



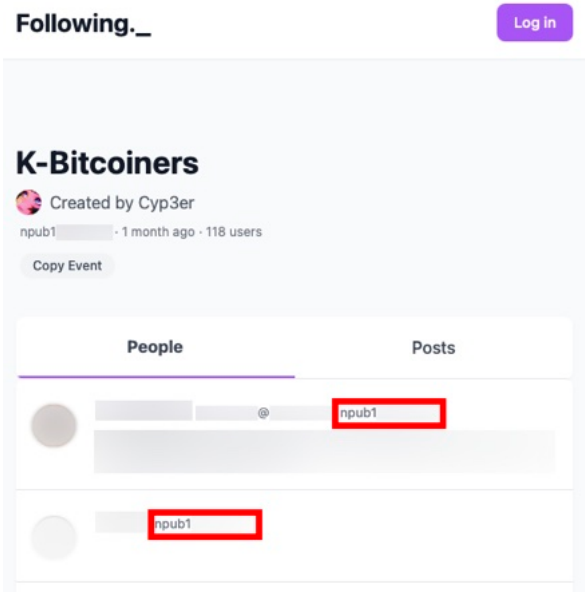
팔로우 추가

처음에는 아무런 글도 안 나타날 것이다. 팔로우하고 있는 계정이 없기 때문이다.

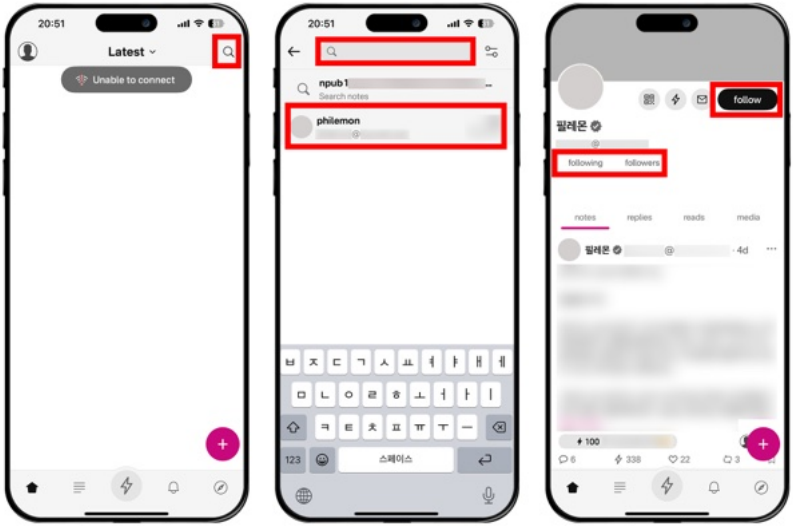
아직 노스터에는 한국인 유저보다 외국인 유저가 압도적으로 많으므로 처음 노스터를 시작할 때 한국인 유저를 찾기 어려울 수 있다. 다음 웹사이트는 노스터 팔로우 리스트를 보여주는 곳인데, 여기서 한국인 비트코이너 노스터 계정 리스트도 볼 수 있다.

https://following.space/d/F2452BFA-8F91-4EAD-8BF4- 63A16A0C6089

이 웹사이트에서 특정 계정으로 들어가 그 사람의 팔로워, 팔로잉 목록을 보고 다른 사람을 찾아나갈 수도 있다. 유저네임 옆에 있는 npub을 누르면 npub이 복사된다.



계정을 팔로우하는 과정을 알아보자. 오른쪽 상단에 있는 검색 버튼을 누른다. 검색창에 npub을 붙여넣고 프로필이 나오면 프로필을 누른다. 다음에 나오는 화면에서 오른쪽의 [follow] 버튼을 누르면 계정을 팔로우할 수 있다. 혹은 그 아래에 있는 팔로잉(following), 팔로워(followers) 목록을 보고 마음에 드는 프로필을 찾아 들어가 팔로우를 할 수 있다. 이런 방식으로 관심이 있는 계정을 팔로우하면 피드에 글이 뜨기 시작한다.



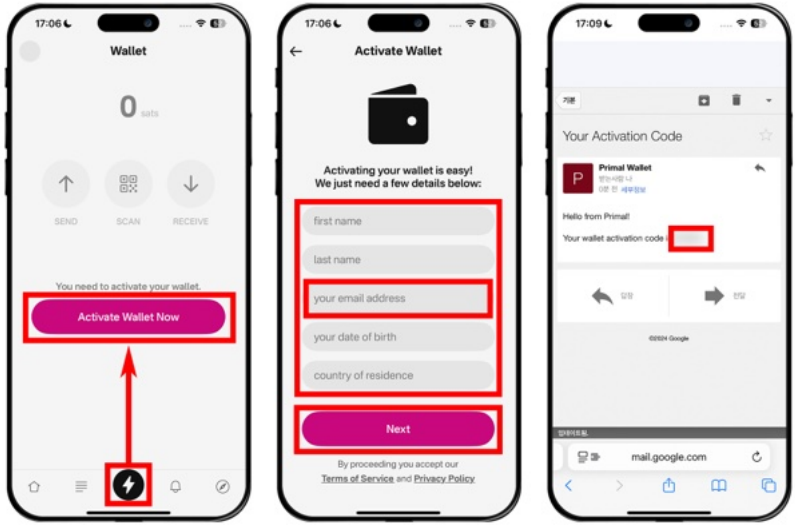
잽을 위한 지갑 추가

프라이멀에서는 자체적인 라이트닝 지갑을 추가하고, 거기에 비트코인을 보낸 뒤 잽을 보낼 수 있다.

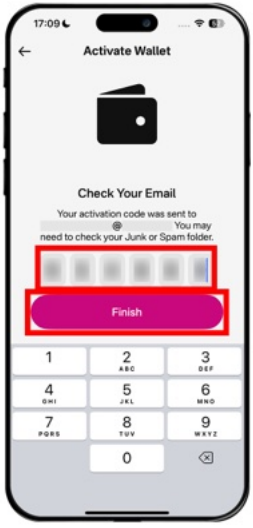
먼저 하단 탭 가운데에 있는 번개 모양의 버튼을 누른다. 그다음 [Activate Wallet Now]를 누른다.

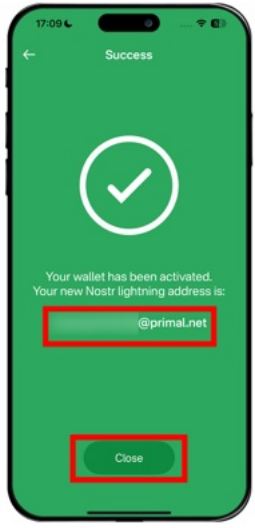
프라이멀 지갑을 이용할 때는 다른 라이트닝 수탁 서비스들처럼 기본 정보를 작성해야 한다. ‘first name’에는 성을 제외한 이름, ‘last name’에는 성, ‘your email address’에는 이메일 주소, ‘your date of birth’에는 생년월일, ‘country of residence’에는 거주 지역을 적는다. 이때 다른 것들은 실제 정보와 상이하게 적더라도 이메일만큼은 제대로 적어야 한다. 바로 뒤에 이메일 인증을 해야 하기 때문이다. 여타 라이트닝 수탁 서비스들과 마찬가지로, 이러한 수탁 서비스들은 언제나 자금 동결 위험이 있다. 이러한 상황들에 대비해 정보를 제대로 적을지, 상이하게 적을지는 당신의 자유이며, 당신이 스스로 책임져야 한다.

잘 입력하고 [Next]를 누르면 입력했던 이메일로 확인 코드가 온다. 이메일에서 코드를 확인한다. 만약 이메일이 보이지 않는다면 스팸 메일함에 이메일이 있는 것은 아닌지 확인하자.

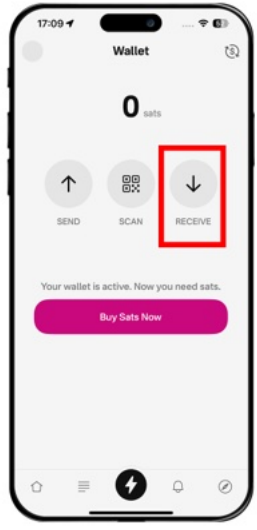


이메일에서 확인했던 코드를 프라이멀 앱 화면에 입력하고 [Finish]를 누른다. 그러면 이메일 주소처럼 생긴 어떤 주소가 나온다. 이것이 프라이멀에서 생성한 라이트닝 지갑의 라이트닝 주소이다. 아래 [Close]를 누른다.





성공적으로 지갑이 생성되었다. [RECEIVE]를 누르면 라이트닝 주소와 그에 해당하는 QR 코드가 보인다. [COPY]를 눌러 이 라이트닝 주소로 비트코인을 보내거나, [ADD DETAILS]를 통해 인보이스를 발행하여 비트코인을 보낼 수 있다. 프라이멀 지갑에 비트코인을 보내 잔액이 생기면 잽을 보낼 수 있다.



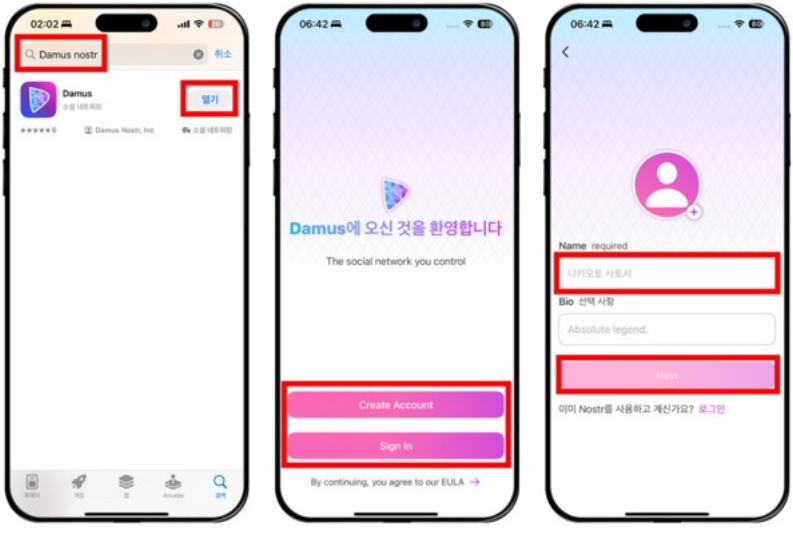
| 다무스 사용 방법

다무스 앱 설치 및 개인키-공개키 쌍 생성

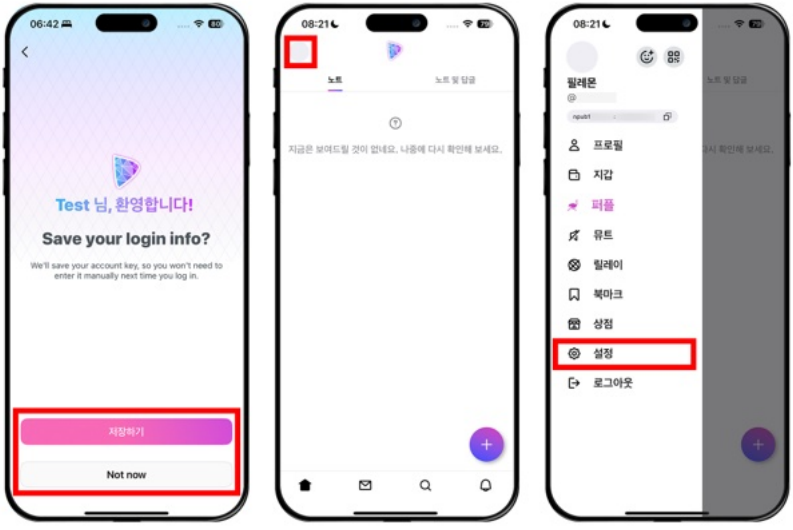
아이폰과 같은 iOS 기기나 맥OS에서는 다무스를 사용하는 것도 좋다. 다무스에서는 자신이 사용하는 라이트닝 지갑을 이용해 잽을 날리는 것이 가능하다.

먼저 앱을 설치해 보자. 앱스토어에 'Damus' 또는 'Damus nostr'를 검색하고 앱을 다운로드한다. 이미 노스터 개인키인 nsec이 있다면 [Sign In]을 누르고, 새 계정을 만들 거라면 [Create Account]를 누른다. 필자는 [Create Account]를 눌러 새 키 쌍을 생성해 보겠다.

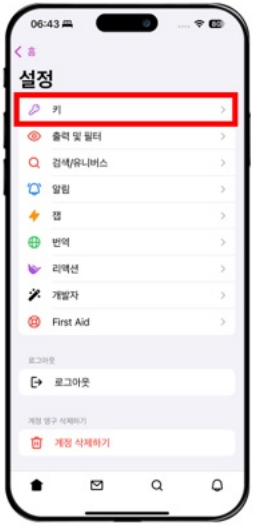
'Name'에 유저네임을 적고 [Next]를 누른다.

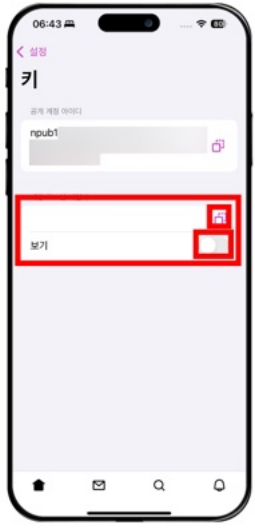


[저장하기]를 누르면 키 쌍이 아이폰 암호 앱에 저장된다. 원하지 않는다면 [Not now]를 눌러 넘어가면 된다. 메인 화면에 들어오면 왼쪽 상단 원 모양의 프로필을 누른다. 그다음 [설정]을 누른다.



[키]를 눌러 들어가면 개인키 nsec을 볼 수 있다. [보기]를 누르고 개인키를 종이에 적는 등 물리적으로 백업하거나, 복사 버튼을 눌러 저장할 수 있다(암호화된 상태로 저장하는 것을 추천한다).

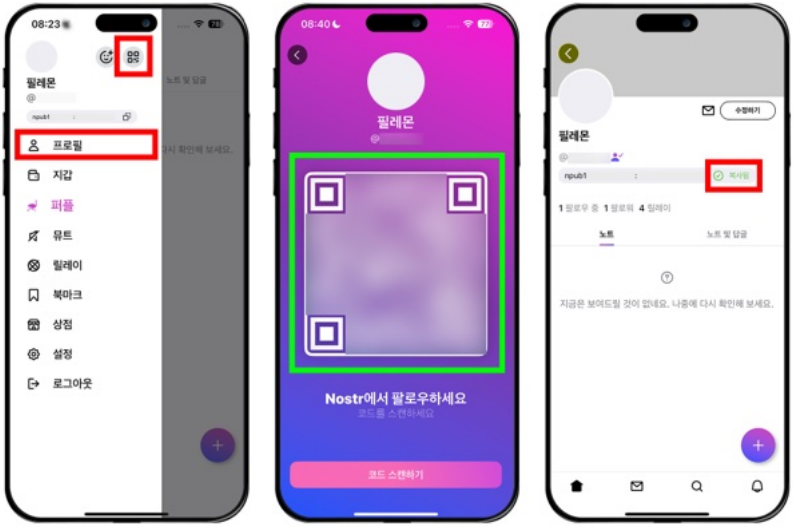




다른 사람들에게 npub 알려주기

누군가에게 자신의 노스터 계정을 알려줄 때는 노스터 공개키인 npub을 알려주면 된다. 다무스 메인 화면에서 왼쪽 상단 원 모양의 프로필을 누른 뒤, 프로필 오른쪽에 있는 QR 코드 모양의 버튼을 누른다. 그러면 QR 코드가 나오는데 이 화면을 보여주거나, 캡처해서 상대방에게 공유하면 된다.

혹은 [프로필]을 눌러 자신의 프로필 화면으로 들어가고, 아이디 밑에 있는 npub을 복사해 상대방에게 보내주면 된다.



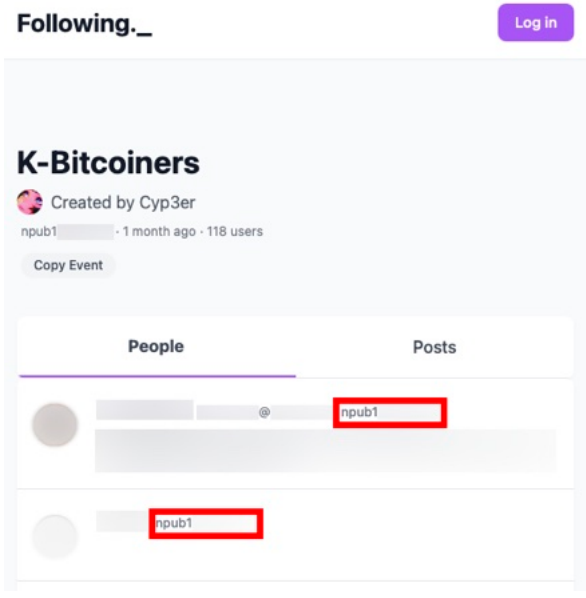
팔로우 추가

처음에는 다무스 운영자의 계정만 팔로우가 되어있을 것이다. 다른 계정들을 팔로우하는 방법을 알아보자.

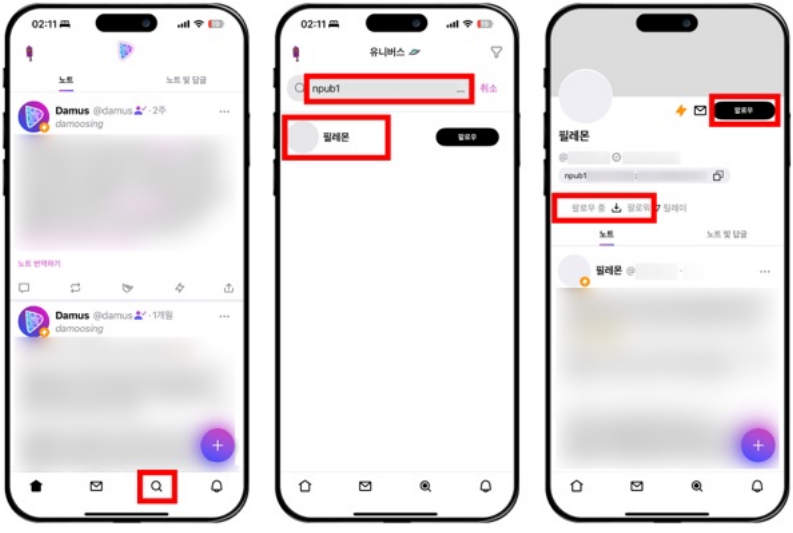
아직 노스터에는 한국인 유저보다 외국인 유저가 압도적으로 많으므로 처음 노스터를 시작할 때 한국인 유저를 찾기 어려울 수 있다. 다음 웹사이트는 노스터 팔로우 리스트를 보여주는 곳인데, 여기서 한국인 비트코이너 노스터 계정 리스트도 볼 수 있다.

https://following.space/d/F2452BFA-8F91-4EAD-8BF4- 63A16A0C6089

이 웹사이트에서 특정 계정으로 들어가 그 사람의 팔로워, 팔로잉 목록을 보고 다른 사람을 찾아나갈 수도 있다. 유저 네임 옆에 있는 npub을 누르면 npub이 복사된다.

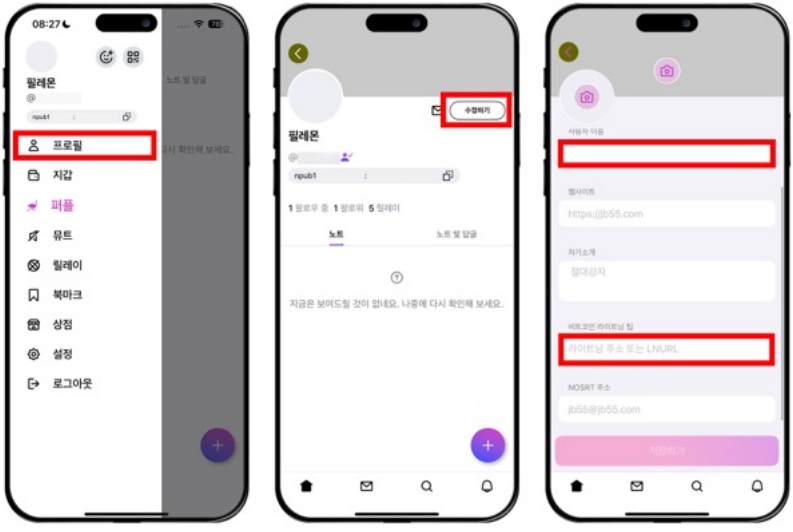


계정을 팔로우하는 과정을 알아보자. 하단 탭에서 돋보기 모양의 버튼을 눌러 검색 창으로 진입한다. 검색창에 npub을 붙여넣고 프로필이 나오면 프로필을 누른다. 다음에 나오는 화면에서 오른쪽의 [팔로우] 버튼을 누르면 계정을 팔로우할 수 있다. 혹은 그 아래에 있는 [팔로우] 또는 [팔로워] 목록을 보고 마음에 드는 프로필을 찾아 들어가 팔로우를 할 수 있다. 이런 방식으로 관심이 있는 계정을 팔로우하면 피드에 글이 뜨기 시작한다.

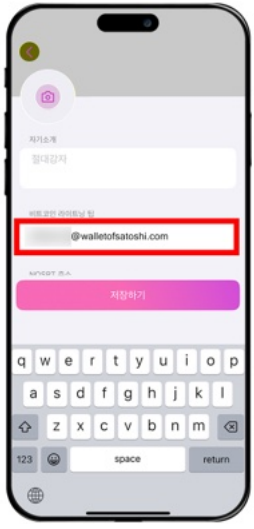


잽을 받기 위한 라이트닝 주소 연결

잽을 받으려면 프로필에 라이트닝 주소를 연결해 놓아야 한다. 왼쪽 상단 원 모양의 프로필을 누르고 [프로필]에 들어간다. 그다음 [수정하기]를 누른다. 여기서 유저네임을 설정할 수 있다. 스크롤을 아래로 내려서 '비트코인 라이트닝 팁' 필드로 내려간다.



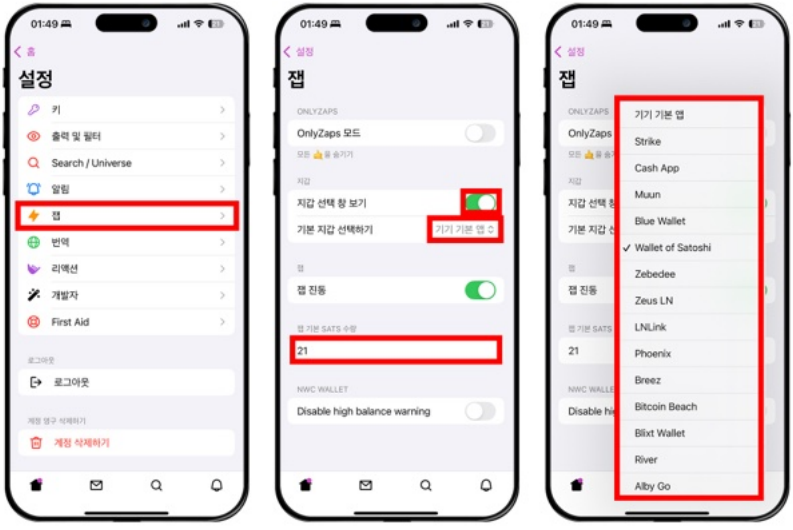
여기에 라이트닝 주소를 입력하고, [저장하기]를 누른다. 프로필 옆에 번개 표시가 뜬 것을 볼 수 있다. 번개 표시가 뜨면 다른 사람들이 나에게 잽을 보낼 수 있다.



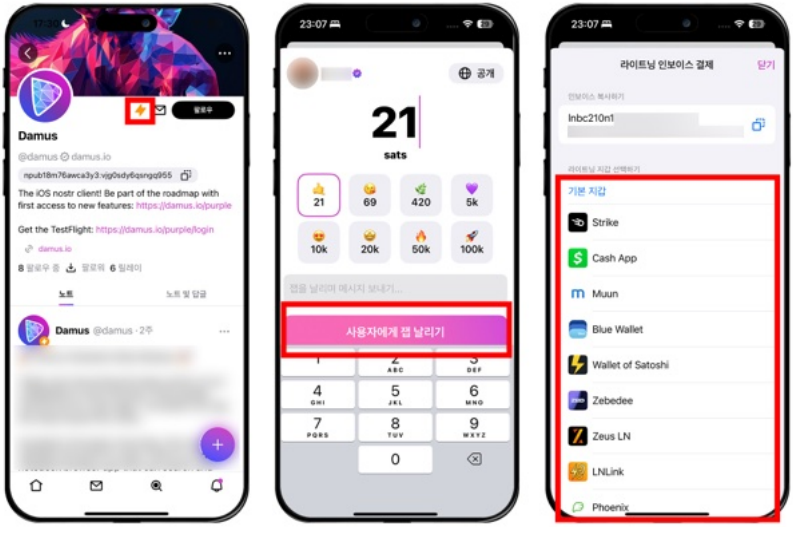
다른 사람에게 잽 보내기

받기만 하는 사람이 되는 것은 유쾌하지 않다. 이번에는 다무스에서 잽을 보내는 방법에 대해 알아보자.

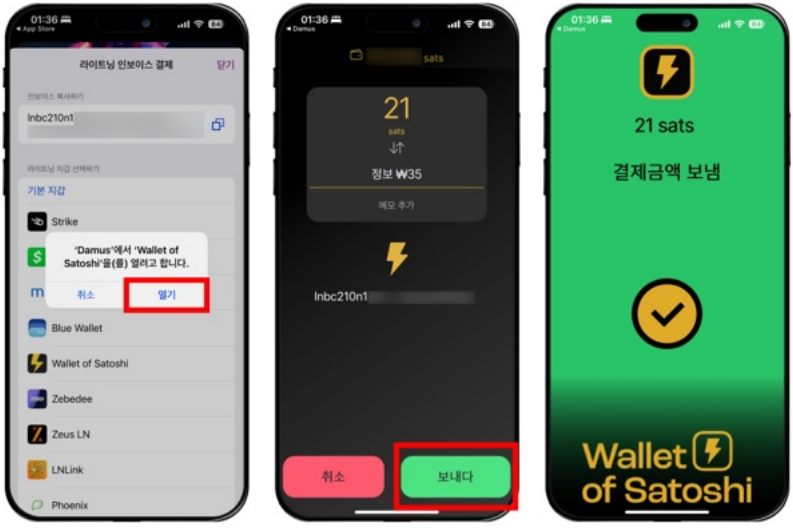
왼쪽 상단 원 모양의 프로필을 누르고 [설정]에 들어간다. 그다음 [잽]을 누른다. 여기서 [지갑 선택 창 보기] 토글 스위치를 켜면 잽을 보낼 때마다 어떤 지갑에서 보낼지 선택할 수 있다. 그 아래 '기본 지갑 선택하기' 옆의 [기기 기본 앱]을 눌러 자신이 사용하고 있는 지갑 앱을 선택할 수 있다. 아래에서 '잽 기본 sats 수량'을 설정할 수도 있다.



이렇게 설정했으면 이제 설정 창에서 빠져나오자. 잽을 날리고 싶은 프로필이나 포스트에 간다. 거기서 번개 모양의 버튼을 누른다. 그러면 잽을 보내는 창이 뜰 것이다. 금액을 설정하고 [사용자에게 잽 날리기]를 누른다. 그러면 설정한 대로 어떤 지갑을 통해 보낼지 선택하는 창이 나온다. 필자는 월렛 오브 사토시(이하 월오사) 앱을 통해 진행해 보겠다.



월오사 앱을 열지 물어보는 창이 나오면 [열기]를 누르고, 월오사에서는 [보내다]를 누른다. 그러면 상대방에게 잽이 간다.



| 피닉스 사용 방법

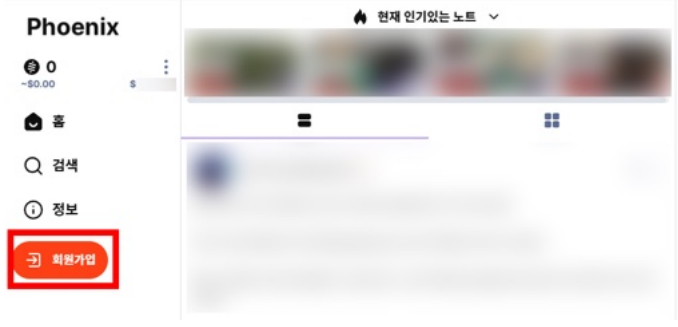
맥OS에서는 다무스 앱을 사용할 수 있지만, 윈도우OS와 같은 환경에서는 크롬 등의 웹 브라우저에서 노스터를 사용하고 싶을 수도 있다. 이럴 때는 여러 클라이언트가 있지만, 프라이멀이나 피닉스를 추천한다.

피닉스에서 개인키-공개키 쌍 생성

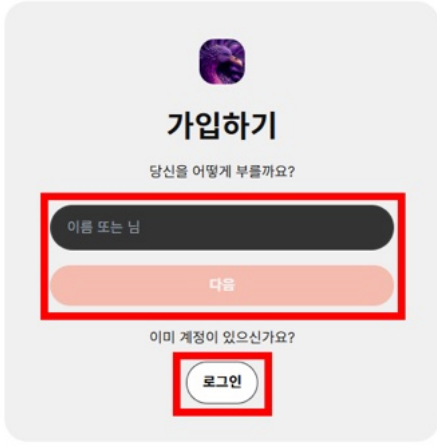
피닉스(구 스노트) 사용 방법을 알아보자. 다음 링크에 접속한다.

https://phoenix.social

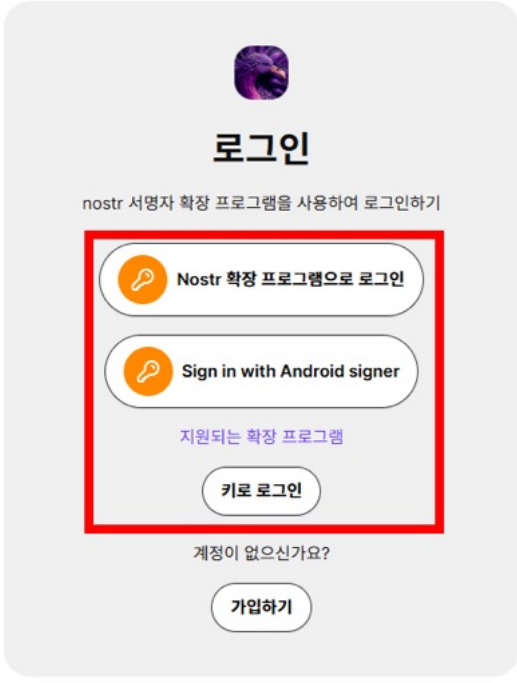
왼쪽에 있는 [회원가입]을 누른다.



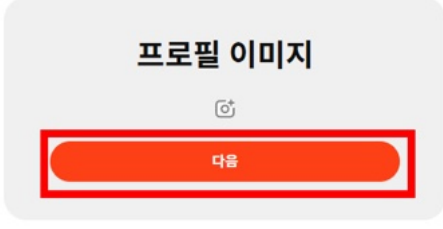
이미 nsec-npub 쌍이 있다면 로그인을 누른다. 새로 계정을 생성할 것이라면 유저네임을 입력하고 [다음]을 누른다.



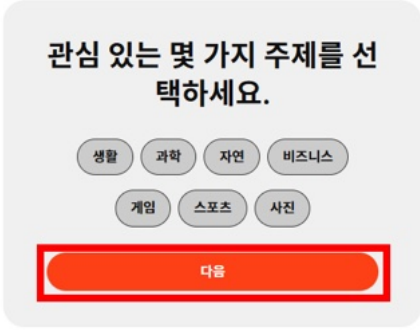
[로그인]을 눌렀을 때는 몇 가지 방법으로 로그인할 수 있지만 [키로 로그인]을 추천하지는 않는다. 이 방식은 직접 nsec을 입력하여 로그인하는 방식인데, 웹 브라우저에 직접 노스터 개인키를 입력하는 것은 권장되지 않는다. 그보다는 알비 익스텐션 등의 노스터 서명 확장 프로그램 등을 통해 로그인하는 것이 좋다. [Nostr 확장 프로그램으로 로그인]을 누르면 이러한 방식으로 로그인할 수 있다. 자세한 내용은 '노스터 서명 확장 프로그램' 장에서 설명하도록 하겠다.



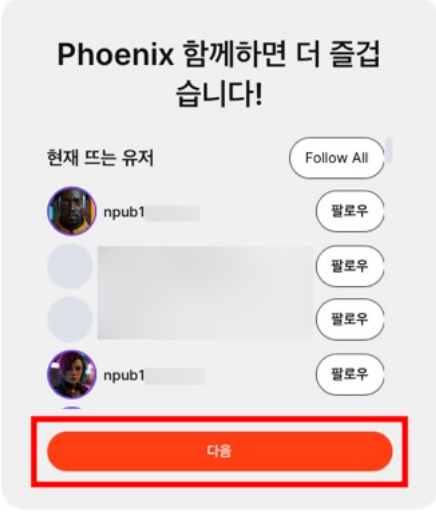
계정을 새로 생성했을 때는 다음과 같이 프로필 이미지를 설정하는 창이 나온다. 나중에 해도 되므로 [다음]을 누른다.



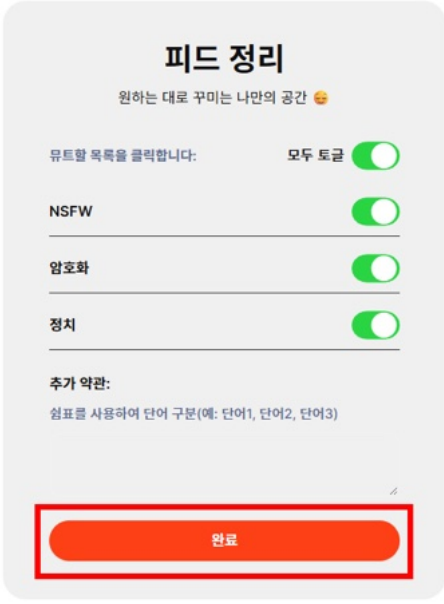
관심 있는 주제를 선택하라는 창이 나오면 [다음]을 누른다.



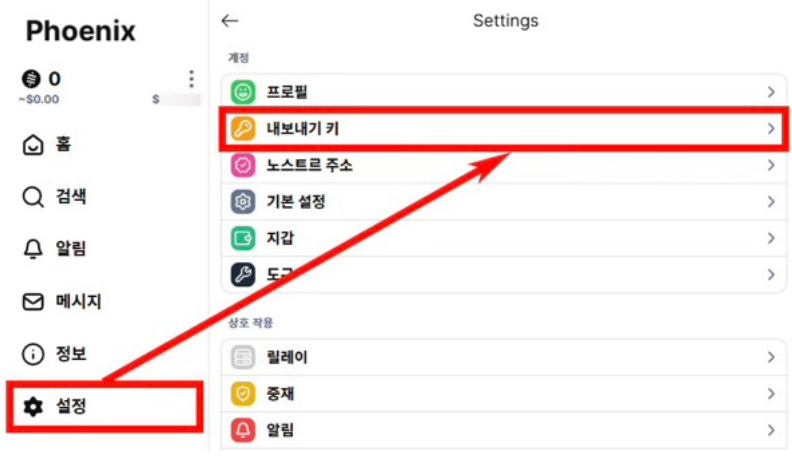
계속 [다음]을 누른다.



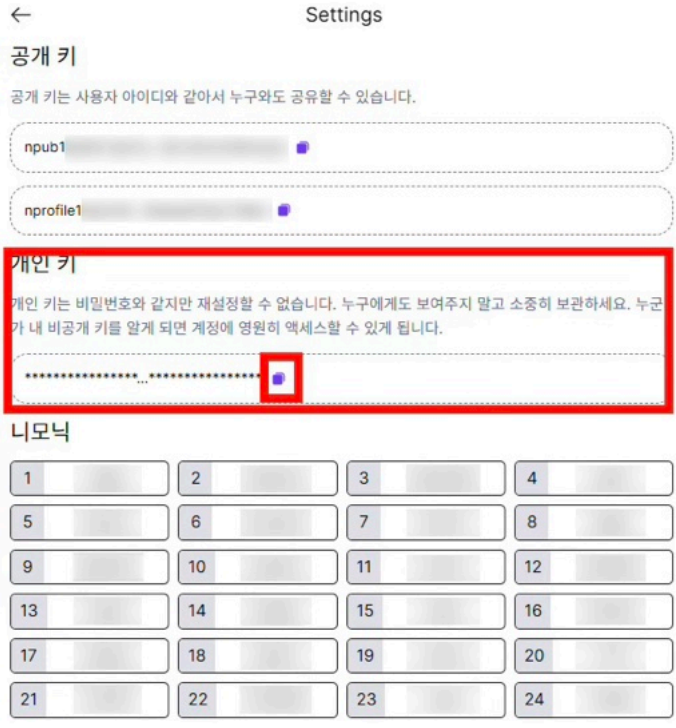
피드 필터 설정 창이 나오면 계속 [다음]을 누른다.



키 쌍을 새로 생성한 것이라면 키를 백업해야 한다. [설정] → [내보내기 키]를 누른다.



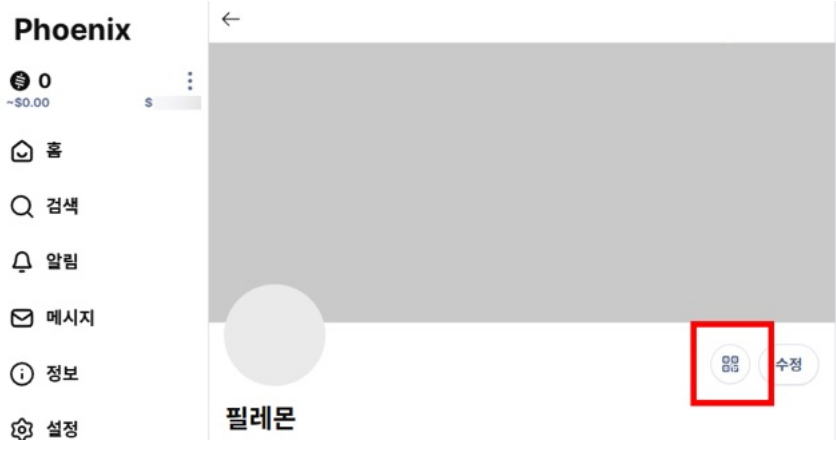
개인키 부분의 문서 모양 버튼을 눌러 개인키를 복사하고, 잘 백업한다.



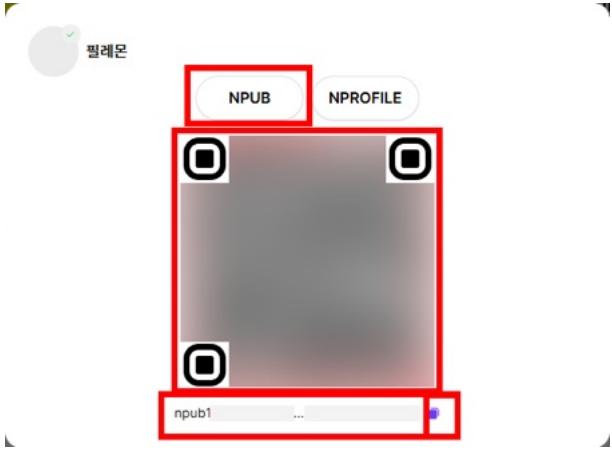
다른 사람들에게 npub 알려주기

누군가에게 자신의 노스터 계정을 알려줄 때는 노스터 공개키인 npub을 알려주면 된다. 피닉스 메인 화면에서 왼쪽 하단에 있는 자신의 프로필을 누르고, [프로필]을 클릭한다.

자신의 프로필 창에 들어가서 QR 코드 모양의 버튼을 누른다.



[NPUB]을 누르고 QR 코드를 다른 사람에게 보여주거나, npub 옆에 있는 문서 모양의 버튼을 눌러 npub을 복사하고 상대방에게 보내주면 된다.



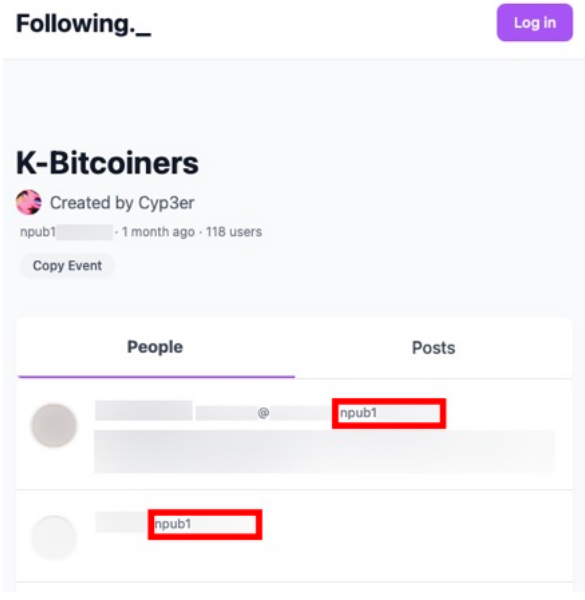
팔로우 추가

처음에는 아무도 팔로우가 안 되어 있어서 피드에 아무것도 뜨지 않을 것이다.

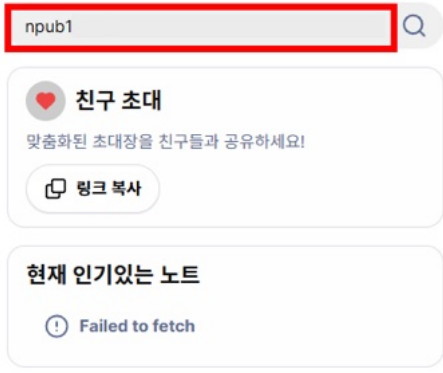
아직 노스터에는 한국인 유저보다 외국인 유저가 압도적으로 많으므로 처음 노스터를 시작할 때 한국인 유저를 찾기 어려울 수 있다. 다음 웹사이트는 노스터 팔로우 리스트를 보여주는 곳인데, 여기서 한국인 비트코이너 노스터 계정 리스트도 볼 수 있다.

https://following.space/d/F2452BFA-8F91-4EAD-8BF4- 63A16A0C6089

이 웹사이트에서 특정 계정으로 들어가 그 사람의 팔로워, 팔로잉 목록을 보고 다른 사람을 찾아나갈 수도 있다. 유저 네임 옆에 있는 npub을 누르면 npub이 복사된다.



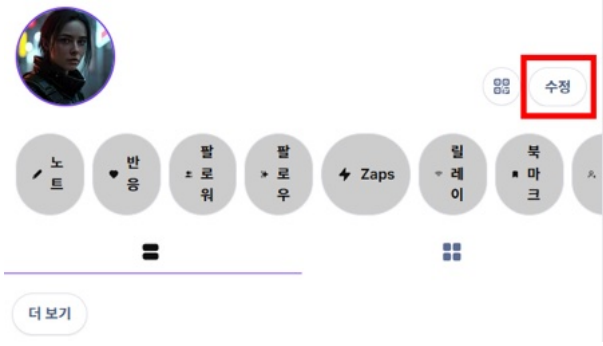
피닉스에서 다른 계정들을 팔로우하는 방법을 알아보자. 피닉스 창 오른쪽 상단의 검색창에 상대방이 보내준 npub을 붙여넣기 한다. 그러면 그 사람의 프로필이 바로 뜰 것이다.



오른쪽의 [팔로우] 버튼을 누르면 계정을 팔로우할 수 있다. 혹은 그 아래에 있는 [팔로워] 또는 [팔로우] 목록을 보고 마음에 드는 프로필을 찾아 들어가 팔로우를 할 수 있다. 이런 방식으로 관심이 있는 계정을 팔로우하면 피드에 글이 뜨기 시작한다.

잽을 받기 위한 라이트닝 주소 연결

잽을 받으려면 프로필에 라이트닝 주소를 연결해 놓아야 한다. 자신의 프로필에 들어가 오른쪽에 있는 [수정]을 누른다.



라이트닝 주소를 입력하고 [저장]을 누른다. 그러면 다른 사람들이 나에게 잽을 보낼 수 있다.

참고로 피닉스에서 다른 사람에게 잽을 보내려면 NWC를 통해 지갑을 연결해야 한다. 이 방법은 뒤에서 다룰 것이다.

| 노스터 서명 확장 프로그램

서명 확장 프로그램을 쓰는 이유

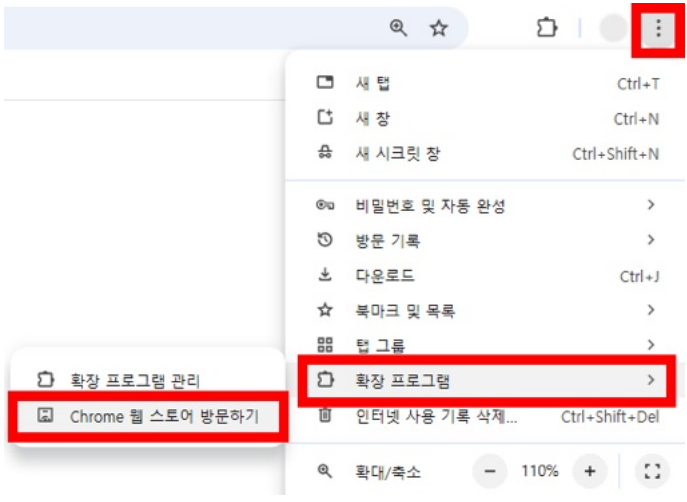
피닉스 같은 노스터 웹 브라우저 클라이언트에서는 주의할 점이 있다. 노스터 개인키를 웹사이트에서 직접 입력하는 것을 삼가야 한다는 것이다. 웹 브라우저에서는 보통 자바스크립트라는 언어를 통해 개인키를 메모리에 올려 서명 연산을 한다. 이러면 페이지 단에서 이를 가로채기가 쉽다. 심지어 광고나 추적 스크립트도 이러한 방식으로 개인키를 가로챌 수 있다. 반면 정상적인 앱 클라이언트들은 개인키를 앱 내부에서만 접근할 수 있도록 제한하므로, 같은 조건이라면 웹보다 앱이 안전하다. 그래서 웹 브라우저에서 노스터 클라이언트를 쓸 때는 '알비 익스텐션' 같은 서명 확장 프로그램을 사용하고, 개인키를 웹페이지에 직접 입력하지 않는 것이 권장된다.

노스터 서명 확장 프로그램은 노스터 개인키를 웹페이지에 직접 주지 않고도 서명을 할 수 있게 해주는 확장 도구다. 비트코인에서 하드웨어 월렛이 하는 역할과 비슷하다고 생각하면 된다. 개인키는 확장 프로그램이 보관하고, 웹페이지는 이 데이터에 서명해달라고 확장 프로그램에 요청한다. 확장 프로그램은 서명 결과만 웹페이지에 돌려준다. 그러면 웹페이지는 노스터 개인키를 알 수 없다.

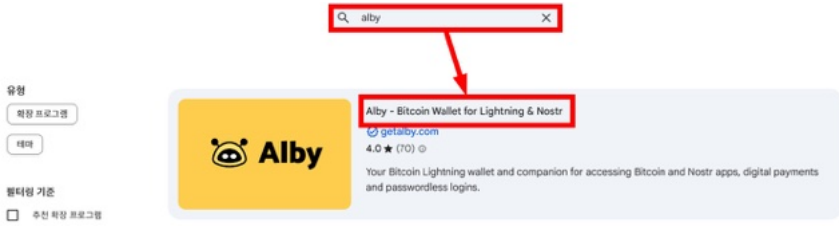
참고로 2025년 8월 기준, 맥OS의 기본 웹 브라우저인 사파리에는 노스터 서명 확장 프로그램이 없다. 따라서 맥OS에서는 앱스토어에서 아이패드용 다무스나 프라이멀 앱 등을 다운로드해서 사용하거나 크롬 웹사이트에서 크롬 브라우저를 다운로드해 사용하는 것을 권장한다.

크롬에서 알비 익스텐션 사용 방법

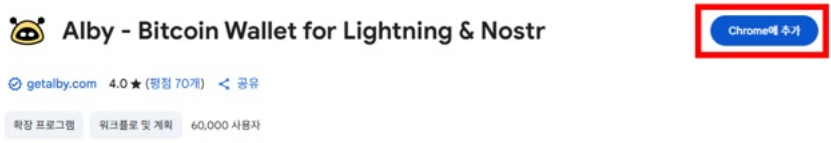
이제 크롬에서 서명 확장 프로그램인 알비 익스텐션을 이용하는 방법을 알아보자. 먼저 크롬에서 크롬 웹 스토어에 들어가야 한다. 우측 상단 점 세 개 → [확장 프로그램] → [Chrome 웹 스토어 방문하기]를 누른다.



검색창에 'Alby'를 검색하고 [Alby - Bitcoin Wallet for Lightning & Nostr]를 누른다.

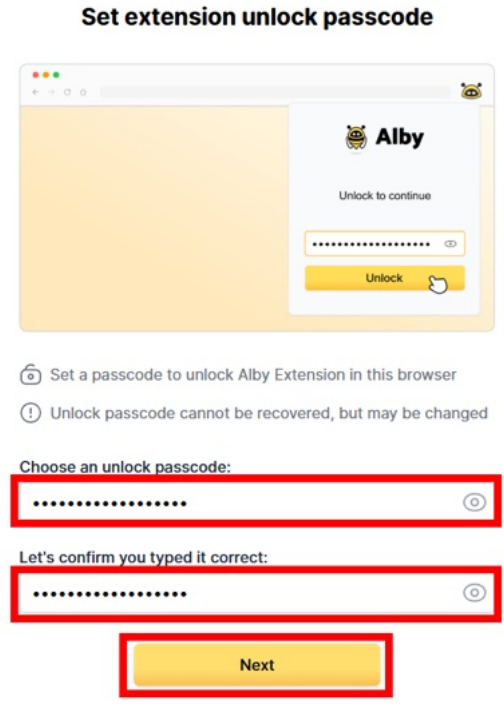


[Chrome에 추가]를 누른다.

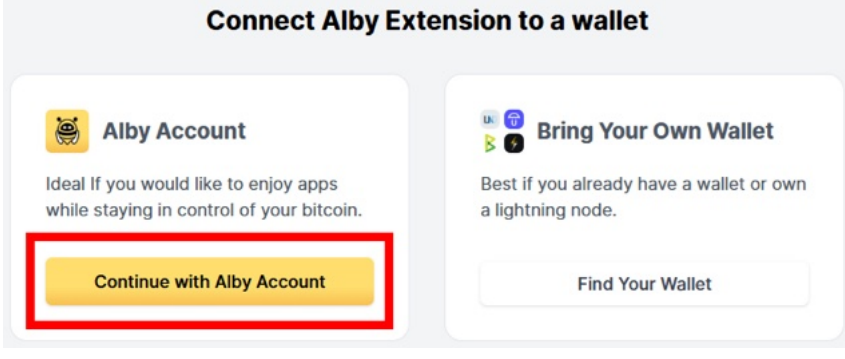


알비 익스텐션을 확장 프로그램에 추가할 건지 묻는 창이 나오면 [확장 프로그램 추가]를 누른다.

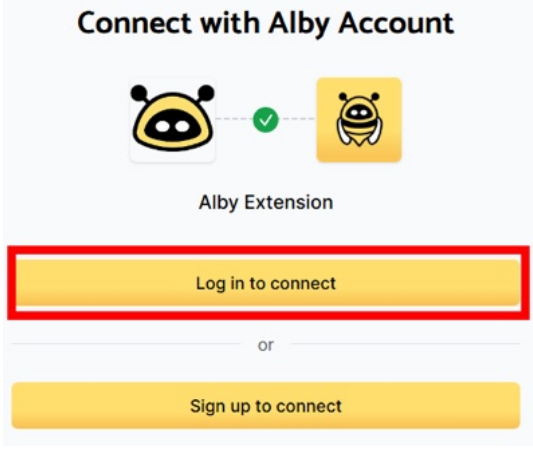
알비 익스텐션의 비밀번호를 설정한다. 아래 입력창은 '비밀번호 확인'으로, 위와 똑같은 비밀번호를 입력해야 한다. 그다음 [Next]를 누른다.



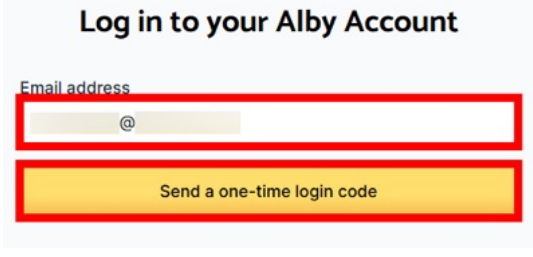
왼쪽에 있는 [Continue with Alby Account]를 누른다.



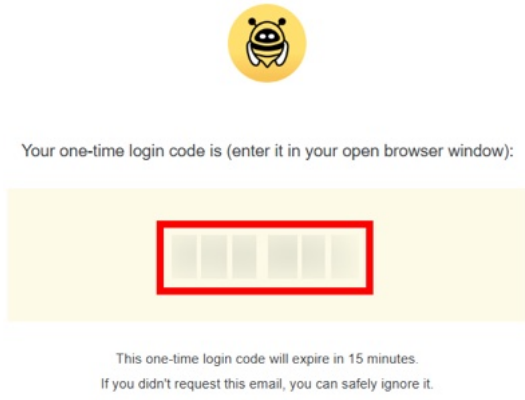
지금부터는 라이트닝 노드 설정 중 알비 허브를 사용하는 과정에서 알비에 가입했다는 것을 전제로 설명하겠다. [Log in to connect]를 누른다. 만약 알비에 가입한 적이 없다면 [Sign up to connect]를 눌러 알비에 가입한 뒤 진행하면 된다. 자세한 가입 방법은 '4부. 라이트닝 노드 운영 가이드'의 '라이트닝 주소 설정, 자신의 노드 알리기' 장에 나와 있다.



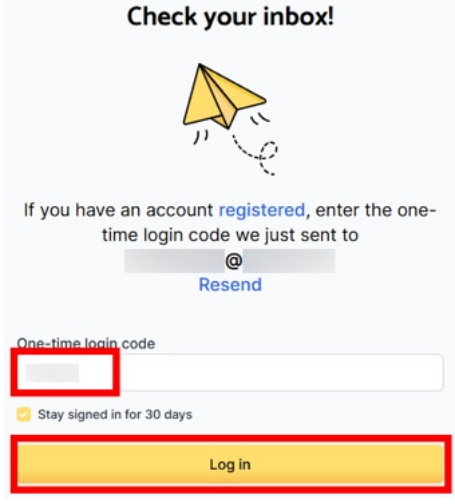
알비에 가입할 때 적었던 이메일 주소를 입력한 뒤, [Send a one-time login code]를 누른다.



그러면 6자리 문자열이 적혀 있는 이메일이 올 것이다. 이 문자열을 복사하거나 잘 기억한다.

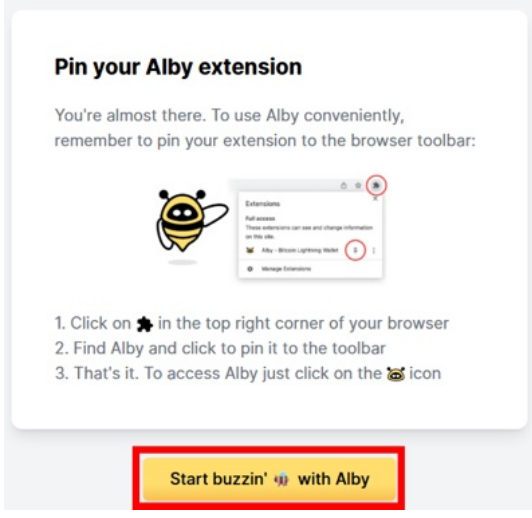


알비 로그인 페이지로 돌아가 6자리 문자열을 입력하고, [Log in]을 누른다.

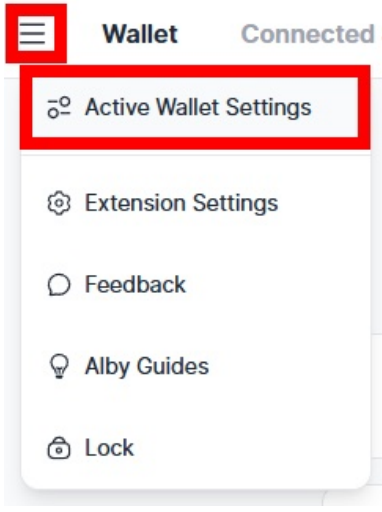


잠시 기다리면 다음 화면으로 넘어간다.

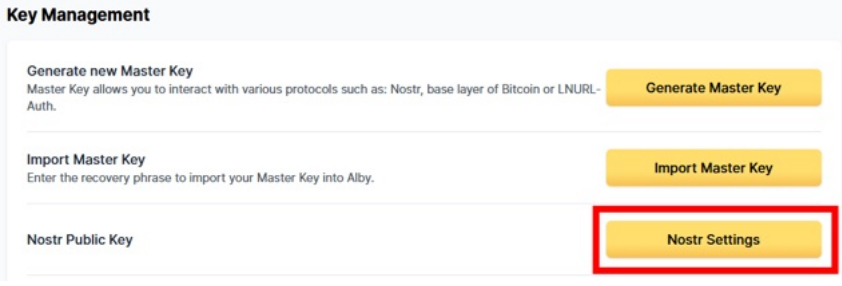
다음 화면으로 넘어갔다면 [Start buzzin' with Alby]를 누른다.



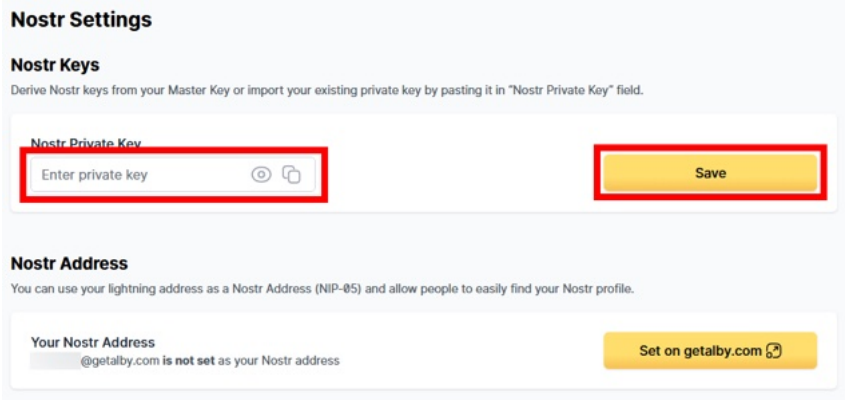
이제 알비 익스텐션과 알비 계정이 잘 연결되었을 것이다. 왼쪽 상단 메뉴 버튼을 누르고, [Active Wallet Settings]를 누른다.



'Key Management' 탭에 있는 [Nostr Settings]를 누른다.



'Nostr Private Key' 아래에 있는 입력창에 nsec으로 시작하는 노스터 개인키를 입력한다. 참고로 맨 앞 'nsec1'에 나오는 숫자 1 이후에는 숫자 1이 안 나온다. 숫자 1은 구분자로만 쓰이는데 그 뒤에 나오는 1과 비슷한 문자는 전부 영어 알파벳 l (엘)이다.

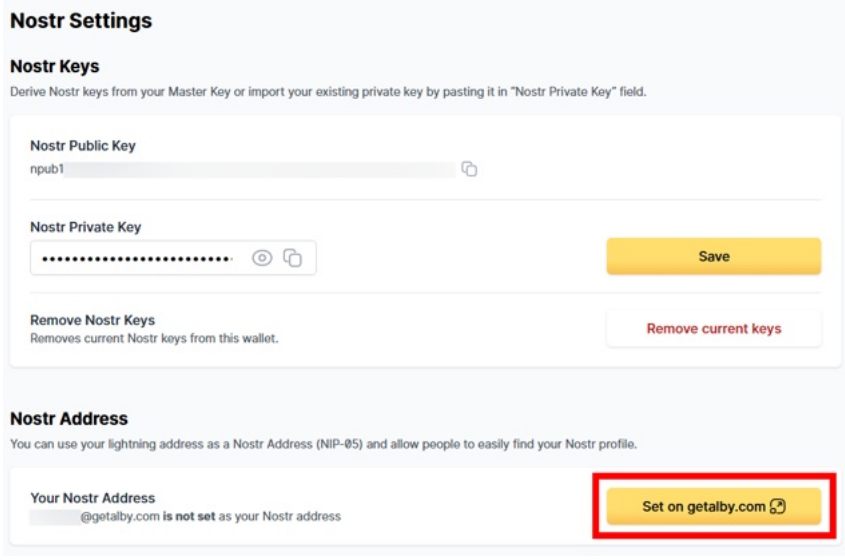


그러면 하단에 알비 익스텐션에 노스터 개인키가 잘 저장되었다는 알림이 나온다.

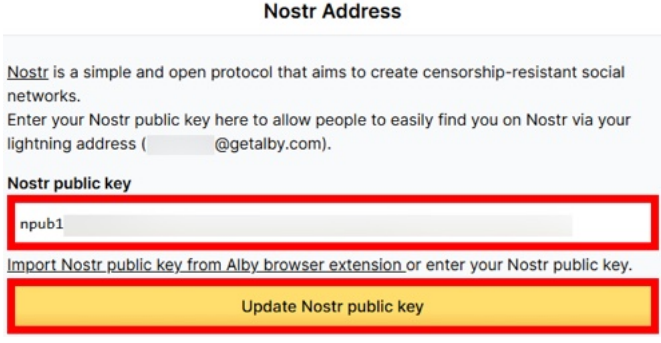
알비에서 노스터 주소 사용하기

알비에서 라이트닝 주소(~@getalby.com 형태)를 사용 중이라면 같은 주소를 노스터 주소로도 사용할 수 있다. 노스터 주소를 사용하면 상대방에게 알려주기도 쉽고, 노스터 주소로 인증된 사용자라는 배지를 받을 수도 있다. 이를 통해 사칭을 예방할 수 있다.

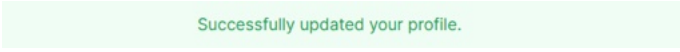
'Key Management' 탭에 있는 [Nostr Settings]에서 'Nostr Address' 아래에 있는 [Set on getalby.com ↗]을 누른다.



연결된 웹사이트에서 Nostr public key 아래 입력창에 npub으로 시작하는 노스터 공개키를 입력한 뒤, [Update Nostr public key]를 누르면 노스터 주소와 노스터 공개키 연결이 완료된다.

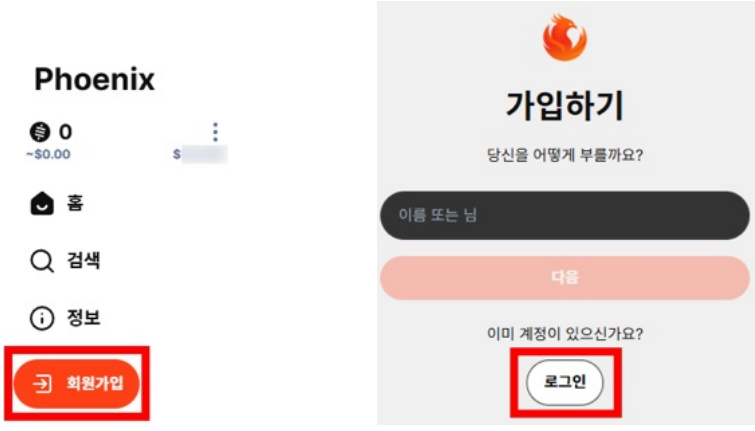


노스터 주소 연결이 성공적으로 되면 프로필이 잘 업데이트 되었다는 알림창이 상단에 나온다.

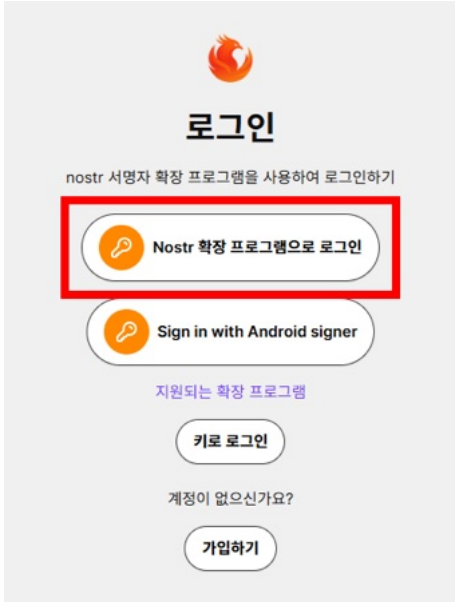


웹 클라이언트에서 알비 익스텐션으로 로그인하기

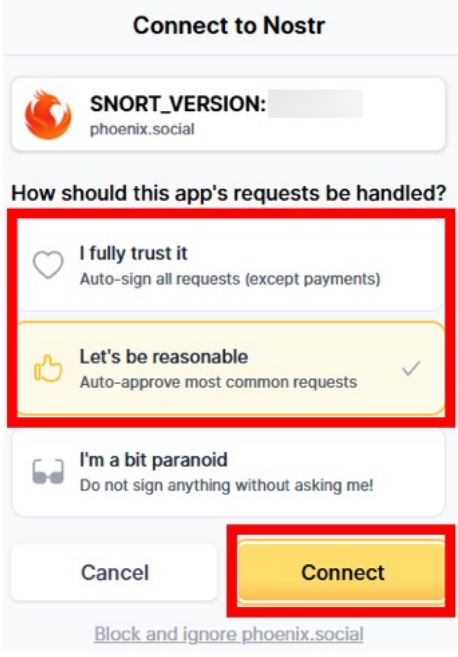
이제 알비 익스텐션을 이용해 로그인이 잘 되는지 확인해 보자. 먼저 피닉스 웹사이트에서 확인해 보겠다. [회원가입] → [로그인]을 누른다.



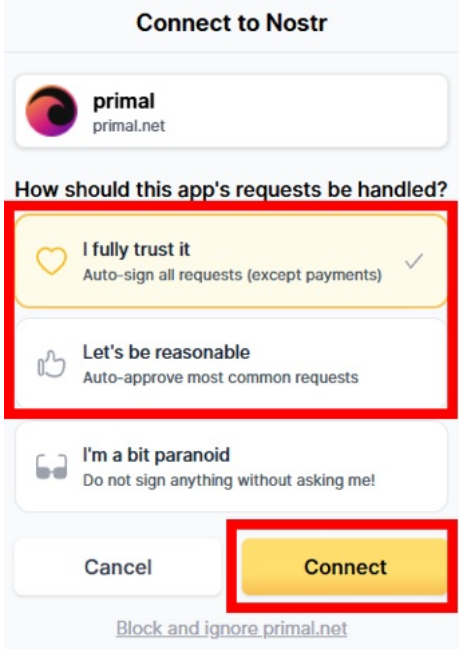
[Nostr 확장 프로그램으로 로그인]을 누른다.



그러면 [I fully trust it]과 [Let's be reasonable] 중 하나를 선택하고 [Connect]를 누르면 로그인이 된다. [I fully trust it]은 이 웹에서 일어나는 서명 요청 중 결제 요청만 빼고 전부 승인한다는 뜻이고, [Let's be reasonable]은 주요 서명 요청만 승인한다는 뜻이다.



이번에는 프라이멀 웹사이트(primal.net)에서 로그인이 잘 되는지 확인해 보자. 프라이멀 웹사이트에 접속하면 피닉스에 접속할 때와 똑같은 로그인 창이 바로 나온다. 그러면 [I fully trust it]과 [Let's be reasonable] 중 하나를 선택하고 [Connect]를 누르면 로그인이 된다.



| 노스터에서 기사, 칼럼 등의 긴 글 쓰기

하블라에서 긴 글 쓰기

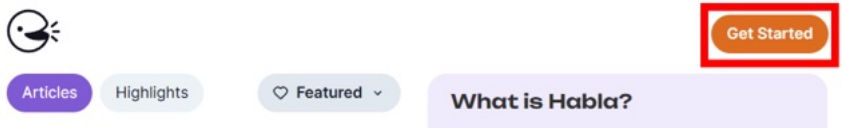
소셜 미디어에 특화된 노스터 클라이언트에서 올리는 글은 일반적으로 NIP-01에서 정의된 '노트'라는 기본 이벤트다. 이러한 노트 형태도 글자 수 제한은 없다. 하지만 노스터에서는 기사나 칼럼 등에 특화된 긴 글을 쓸 수도 있는데 NIP-23에서 '롱 폼 콘텐츠'를 정의하고 있다.

이번에는 하블라Habla에서 이러한 긴 글을 쓰는 방법을 알아보자. 하블라에 로그인하기 위해서는 기본적으로 알비 익스텐션 같은 노스터 서명 확장 프로그램이 필요하다. 맥OS의 경우 크롬 다운로드 웹사이트에서 크롬 브라우저를 설치해야 한다. 자세한 내용은 앞의 '노스터 서명 확장 프로그램' 장을 참고하라.

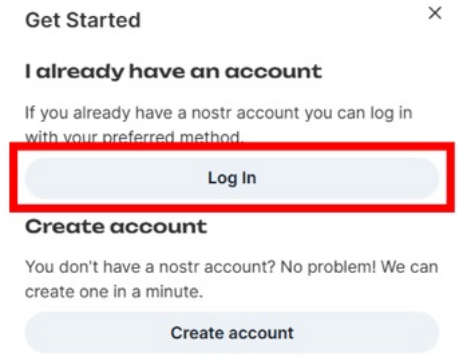
먼저 다음 웹사이트에 접속한다.

https://habla.news

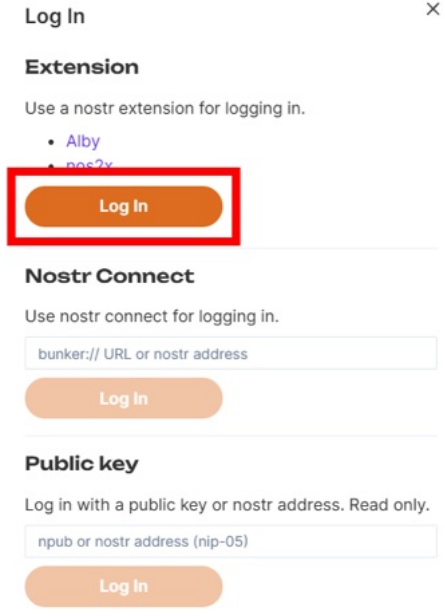
웹사이트 우측 상단에 있는 [Get Started]를 누른다.



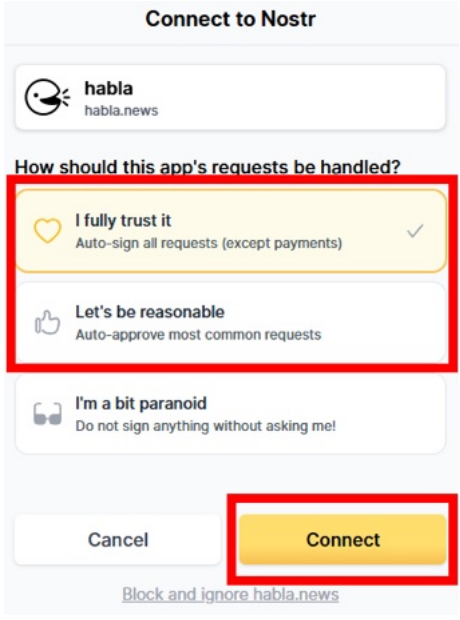
[Log In]을 누른다.



우리는 알비 익스텐션을 통해 로그인할 것이므로 'Extension' 아래에 있는 [Log In]을 누른다.



[I fully trust it]과 [Let's be reasonable] 중 하나를 선택하고 [Connect]를 누르면 로그인이 된다.

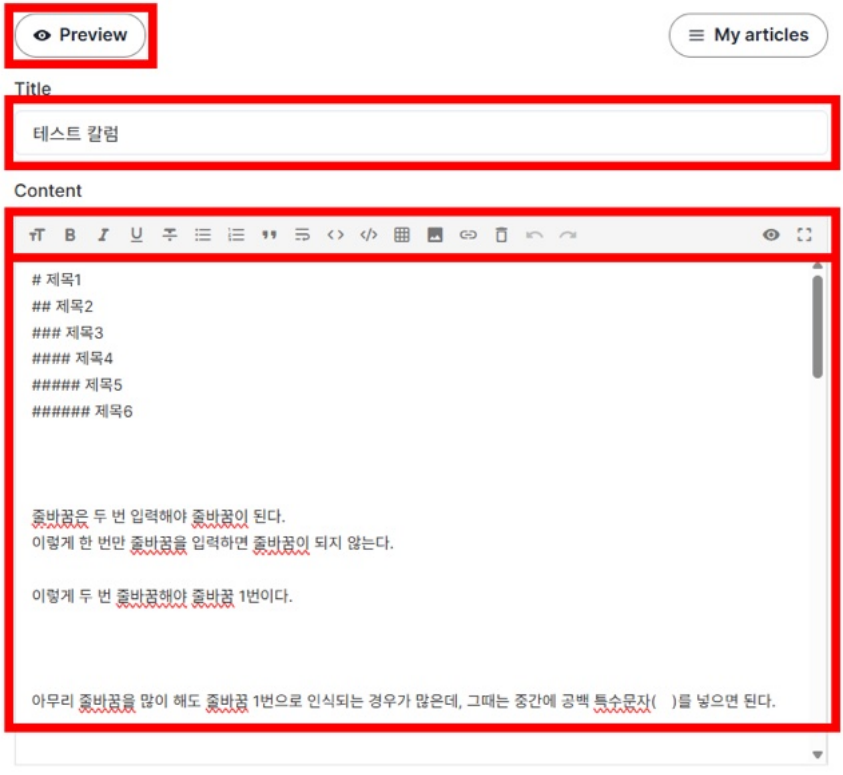


로그인이 되면 [Write]를 누른다.

그러면 긴 글 입력창이 나온다. 'Title' 아래에는 제목을 쓰면 된다.

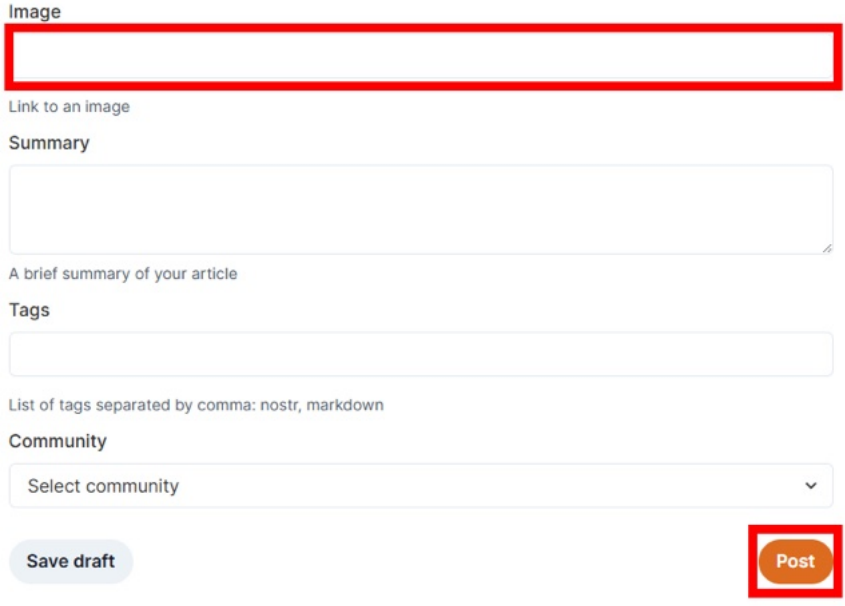
'Content' 아래에 있는 입력기에 본문 내용을 입력하면 된다. 노스터에서 긴 글을 쓸 때는 보통 '마크다운 문법'이라는 문법을 쓰는데 이는 뒤에서 조금 더 자세히 설명하겠다.

[Preview]를 누르면 글 미리보기를 할 수 있다. 노스터는 글 수정이 매우 까다로우니 글 발행 전 미리보기를 꼭 확인하는 것이 좋다.



그 아래로 내려가면 'Image' 아래에 입력창이 있다. 여기에는 이미지의 URL 주소를 입력한다. 여기에 입력한 주소의 이미지는 글의 섬네일, 혹은 배경 이미지 역할을 한다.

[Post]를 누르면 글 발행이 완료된다.



마크다운 문법 간략히 알아보기

마크다운 문법은 간단한 기호로 글의 구조와 서식을 표현하는 방법이다. 노스터 긴 글에서는 마크다운 문법을 사용하기 때문에 자주 쓰는 마크다운 문법을 기억해 놓으면 편하다. 특히 이미지 삽입 마크다운은 자주 사용하므로 알아두면 편하다.

먼저 제목은 맨 앞에 #을 적어 표현한다. #을 여러 개 쓰면 제목 크기를 결정할 수 있다.

```
# 제목 1
## 제목 2
### 제목 3
#### 제목 4
##### 제목 5
###### 제목 6
```

이렇게 입력했을 경우 다음과 같이 표시된다.

제목1

제목2

제목3

제목4

제목5

제목6

줄 바꿈은 엔터를 두 번 입력해야 한다. 줄 바꿈을 여러 번 해야 할 경우 공백을 섞어 쓰면 편하다. 공백은 윈도우에서 ㄱ + '한자 키'를 입력했을 때 나오는 첫 번째 특수문자다. 혹은 인터넷에 '공백 특수문자'를 검색하고 복사, 붙여넣기를 해서 사용할 수도 있다. 아래 예시는 공백 문자가 잘 보이도록 표시하기 위해 배경을 검은색으로 칠했다.

```
줄바꿈은 두 번 입력해야 줄바꿈이 된다.
이렇게 한 번만 줄바꿈을 입력하면 줄바꿈이 되지 않는다.

이렇게 두 번 줄바꿈해야 줄바꿈 한 번이다.


아무리 줄바꿈을 많이 해도 줄바꿈 한 번으로 인식되는 경우가 많은데, 그때는 중간에 공백 특수문자(  )를 넣으면 된다.
```

이렇게 입력했을 경우 다음과 같이 표시된다.

줄바꿈은 두 번 입력해야 줄바꿈이 된다. 이렇게 한 번만 줄바꿈을 입력하면 줄바꿈이 되지 않는다.

이렇게 두 번 줄바꿈해야 줄바꿈 한 번이다.

아무리 줄바꿈을 많이 해도 줄바꿈 한 번으로 인식되는 경우가 많은데, 그때는 중간에 공백 특수문자( )를 넣으면 된다.

다른 입력 방법은 예시를 통해 보겠다. \ 문자는 일반 키보드에서 '₩' 키를 누르면 된다.

```
기울임 표시는 *이렇게* 별표로 감싸주면 된다.

굵음 표시는 **이렇게** 별표 두 개로 감싸주면 된다.

취소선 표시는 ~~이렇게~~ 물결 표시 두 개로 감싸주면 된다.

일반 별표를 쓰고 싶을 때는 \* 이렇게 작성하면 된다.
```

이렇게 입력했을 경우 다음과 같이 표시된다.

기울임 표시는 *이렇게* 별표로 감싸주면 된다.

굵음 표시는 **이렇게** 별표 두 개로 감싸주면 된다.

취소선 표시는 ~~이렇게~~ 물결 표시 두 개로 감싸주면 된다.

일반 별표를 쓰고 싶을 때는 * 이렇게 작성하면 된다.

```
> 맨 앞에 화살괄호(>)를 넣으면 인용문이 된다.
```

이렇게 입력했을 경우 다음과 같이 표시된다.

> ***맨 앞에 화살괄호(>)를 넣으면 인용문이 된다.***

1. 순서 있는 목록은 앞에 번호와 마침표를 쓰면 된다.
2. 자동으로 번호가 매겨진다.
1. 숫자를 다시 1로 해도 줄바꿈 두 번이 아니면 계속 번호가 이어져서 '3.'으로 표시된다.

- 순서 없는 목록은 맨 앞에 하이픈(-)을 붙이면 된다.
- 순서 없는 목록 예시

이렇게 입력했을 경우 다음과 같이 표시된다.

1. 순서 있는 목록은 앞에 번호와 마침표를 쓰면 된다.
2. 자동으로 번호가 매겨진다.
3. 숫자를 다시 1로 해도 줄바꿈 두 번이 아니면 계속 번호가 이어져서 '3.'으로 표시된다.

- 순서 없는 목록은 맨 앞에 하이픈(-)을 붙이면 된다.
- 순서 없는 목록 예시

링크 삽입은 다음과 같은 형태를 따른다.

[링크 텍스트](링크 URL)

예시:

[비트코인 사이트](https://bitcoin.org)

이렇게 입력했을 경우 다음과 같이 표시된다.

링크 삽입은 다음과 같은 형태를 따른다.

[링크 텍스트](링크 URL)

예시:

비트코인 사이트

이미지를 삽입할 때는 이미지 대체 텍스트를 입력해야 하는데, 이는 이미지가 로드되지 않았을 때 대신 표시되는 글자를 의미한다. 혹은 시각장애인을 위한 스크린 보조 기능이 이미지를 설명할 때 읽어주는 내용이기도 하다. 이미지가 정상적으로 로딩되면 화면에서는 보이지 않는 부분이다.

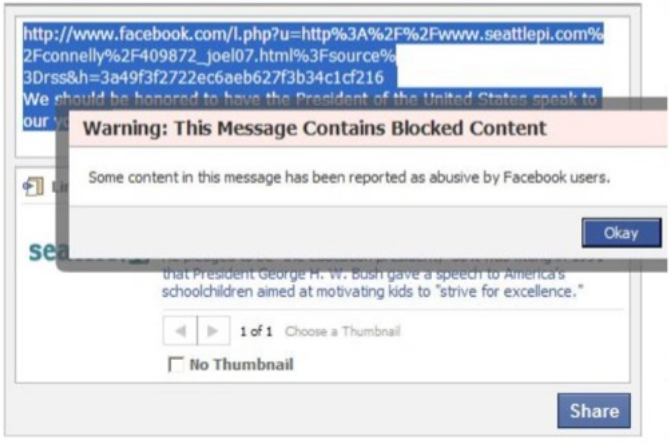
```
이미지 삽입은 다음과 같은 형태를 따른다.

![이미지 대체 텍스트](이미지 URL)

예시:

![페이스북에서 콘텐츠가 검열되었을 때 뜨는 알림창](https://upload.wikimedia.org/wikipedia/commons/b/be/Facebook_Censorship_Cropped.jpg)
```

이렇게 입력했을 경우 다음과 같이 표시된다.

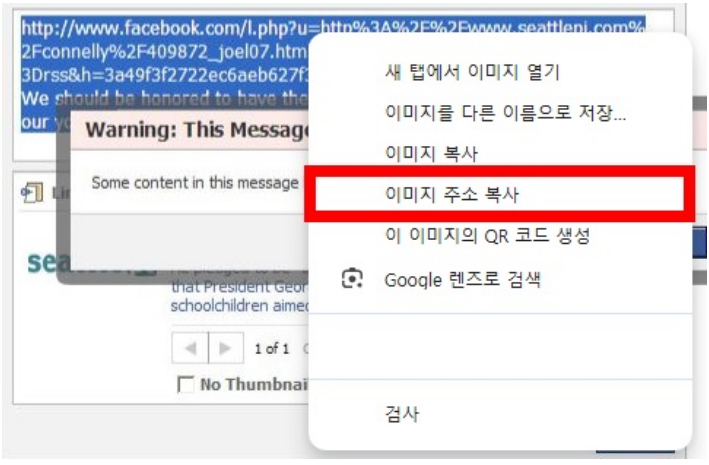
이미지 삽입은 다음과 같은 형태를 따른다.

![이미지 대체 텍스트](이미지 URL)

예시:



노스터는 텍스트 기반 프로토콜이기 때문에 이미지는 다른 곳에 업로드를 한 뒤 이미지 주소를 복사해 링크를 삽입하는 방식을 이용한다. 만약 이미 사용하는 블로그나 자신의 웹사이트가 있다면 블로그나 웹사이트에 사진을 업로드한 뒤 이미지 주소를 복사해 오는 게 편하다. 노스터 이미지 전용 업로드 웹사이트가 있는데 이는 유료이므로 따로 작성하지 않았다.




```
수평선은 하이픈(-)을 세 번 입력하면 된다.

---
```

이렇게 입력했을 경우 다음과 같이 표시된다.

수평선은 하이픈(-)을 세 번 입력하면 된다.

표는 파이프(|)와 하이픈(-)을 조합해 작성한다. 이때 파이프(|)는 일반 키보드에서 'Shift' + '₩' 키를 누르면 된다. 파이프 사이에 아무것도 입력하지 않으면 빈 셀이 되는데 간혹 이게 제대로 반영이 안 될 때가 있다. 그럴 때는 파이프 사이에 공백 특수문자를 넣으면 된다.

```
표는 다음과 같이 파이프(|)와 하이픈(-)을 조합해 작성한다. 첫 행은 반드시 제목 행이 된다.

| 제목 1 | 제목 2 |
| --- | --- |
| 내용 11 | 내용 12 |
| 내용 21 | 내용 22 |
|  | 왼쪽은 빈 셀 |
```

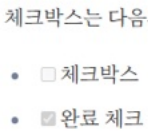
이렇게 입력했을 경우 다음과 같이 표시된다.

표는 다음과 같이 파이프(|)와 하이픈(-)을 조합해 작성한다. 첫 행은 반드시 제목 행이 된다.

제목 1	제목 2
내용 11	내용 12
내용 21	내용 22
	왼쪽은 빈 셀

```
체크박스는 다음과 같이 작성한다.

- [ ] 체크박스

- [x] 완료 체크
```

이렇게 입력했을 경우 다음과 같이 표시된다.



이렇게 기본적인 마크다운 문법 사용 방법을 살펴보았다. 좀 더 자세한 마크다운 문법은 인터넷에 검색하여 사용하길 바란다. css 문법을 숙지하고 있는 경우 〈span style="css 스타일 지정"〉〈/span〉으로 감싸 적용할 수 있는데, 필자의 경험상 노스터 클라이언트에서 css 지정 스타일은 제대로 지원하지 않는 경우가 많았다.

이로써 하블라에서 긴 글을 쓰는 방법과, 긴 글을 쓰는 데 필요한 마크다운 문법까지 살펴보았다.

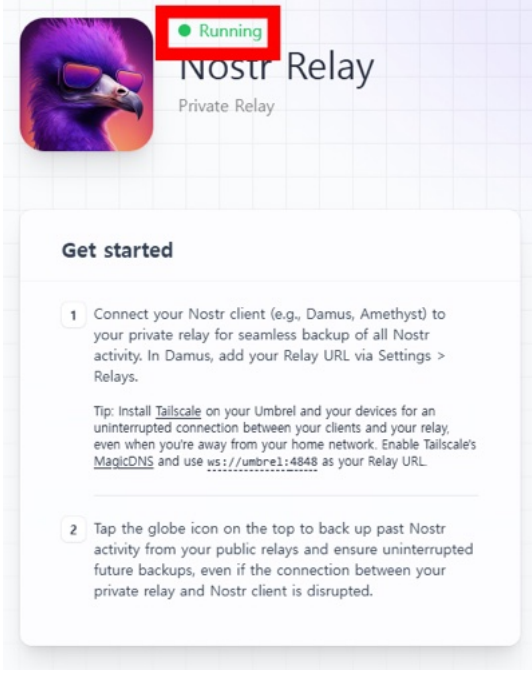
| 엄브렐에서 노스터 릴레이 서버 운영하고 연결하기

이제 엄브렐OS에서 자신만의 릴레이 서버를 운영하고, 클라이언트에서 자신의 릴레이 서버에 연결하는 방법을 알아보자. 이렇게 하면 그 누구도 자신의 글을 검열할 수 없고, 포스트와 활동(이벤트)이 온전히 자신의 릴레이 서버에 보관된다.

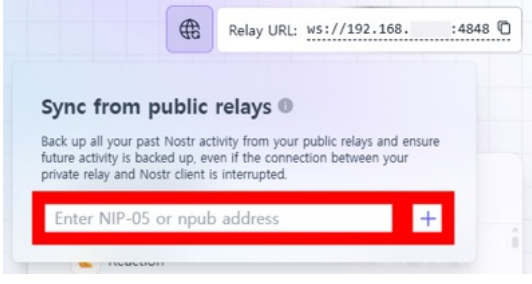
프라이빗 릴레이 서버 운영하기

먼저 엄브렐의 앱스토어에 들어가 'Nostr Relay'를 설치한다. 설치가 다 되면 [열기]를 누른다.

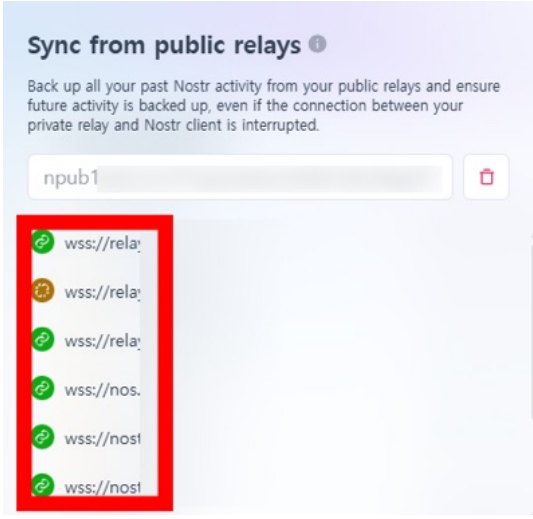
처음 들어갔을 때 초록색 점과 함께 'Running' 표시가 나오면 잘 실행되고 있다는 뜻이다.



이제 과거에 있었던 자신의 활동들을 전부 자신의 릴레이 서버에 백업하는 과정을 알아보자. 'Sync from public relays' 아래에 자신의 npub을 붙여넣고 옆에 있는 [+]를 누른다.



그러면 자신이 연결해 놓은 퍼블릭 릴레이들에서 자신과 관련된 이벤트들을 동기화하고 백업한다.

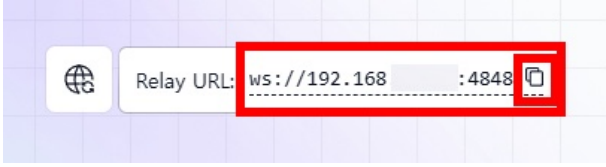


로컬 네트워크에서 자신의 릴레이 서버에 연결하기

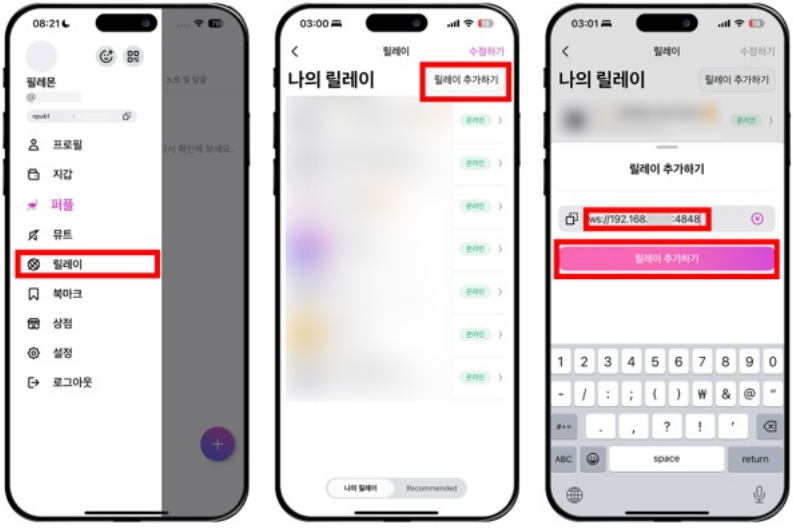
이제 클라이언트에서 자신의 릴레이 서버와 연결하는 방법을 알아보자. 먼저 로컬 네트워크에서 연결하는 방법을 알아볼 것이다. 로컬 네트워크에서의 연결이므로 릴레이 서버와 클라이언트가 실행되는 기기가 같은 네트워크에 있어야만 연결이 된다. 스마트폰이 엄브렐 기기와 연결된 공유기의 와이파이를 사용할 때만 릴레이 서버에 연결될 것이다.

따라서 외부에서 했던 노스터 활동들은 자신의 릴레이 서버에 기록되지 않다가, 집에 와서 같은 와이파이를 사용하면 그때부터 자신의 릴레이 서버에 저장될 것이다.

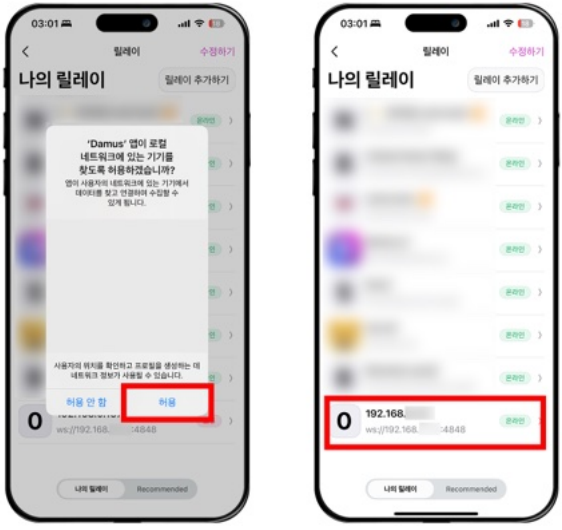
노스터 릴레이 오른쪽 상단에 로컬 네트워크 주소(192.168.???.???)와 포트 번호(:4848)가 나온다.



클라이언트는 다무스를 기준으로 설명하겠다. 다른 클라이언트도 크게 다르지 않다. 다무스 메뉴에서 [릴레이] → [릴레이 추가하기]를 누른 뒤, 앞에서 본 노스터 릴레이 주소를 붙여넣기 한다. 이때 맨 앞의 'ws://'도 포함해서 붙여넣어야 한다.



로컬 네트워크에 있는 기기를 연결할지 물어보면 [허용]을 누른다. 그러면 자신의 릴레이 서버가 잘 연결된 것을 확인할 수 있다.

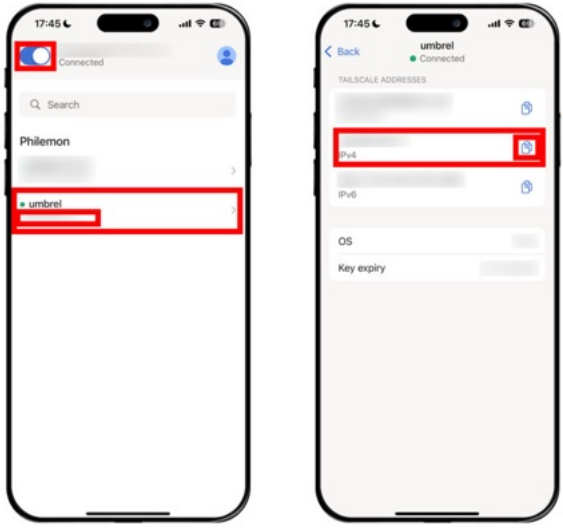


테일스케일을 이용해 원격으로 자신의 릴레이 서버에 연결하기

로컬 IP 주소를 이용해 릴레이를 연결하면 엄브렐 기기와 같은 네트워크에 연결되어야 릴레이 서버가 그동안의 이벤트들을 백업한다. 같은 네트워크가 아닐 때도 원격으로 계속 연결을 하고 싶다면 테일스케일을 사용하면 된다.

먼저 테일스케일 앱을 켠다. 엄브렐 기기와 노스터 클라이언트(다무스 등)를 사용할 기기에 초록색 불이 들어와 있어야 한다.

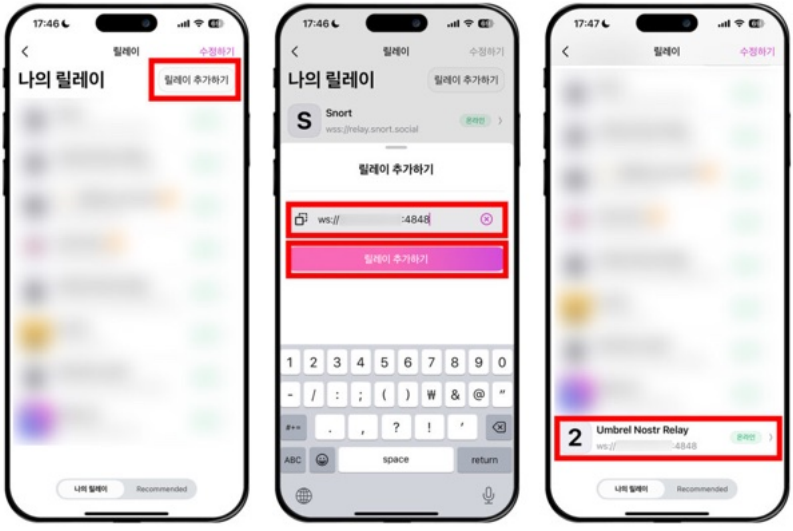
엄브렐 기기 밑에 IP 주소가 보일 것이다. 엄브렐 기기를 누르면 상세 페이지가 나오는데, 거기서 IPv4 옆에 있는 문서 모양의 버튼을 누르면 이 IP 주소를 복사할 수 있다.



다무스에서 [릴레이 추가하기]를 누른 뒤 다음과 같이 입력한다.

ws://테일스케일에 있던 IP 주소:4848

반드시 앞에 스킴인 ws://와 뒤에 포트 번호인 :4848을 붙여서 입력해야 한다. 그러고 [릴레이 추가하기]를 누르면 성공적으로 연결된 것을 볼 수 있다. 이제 테일스케일만 켜져 있다면 엄브렐 기기와 같은 네트워크 와이파이를 사용하지 않더라도 계속 릴레이 서버에 자신의 이벤트를 기록하게 될 것이다.



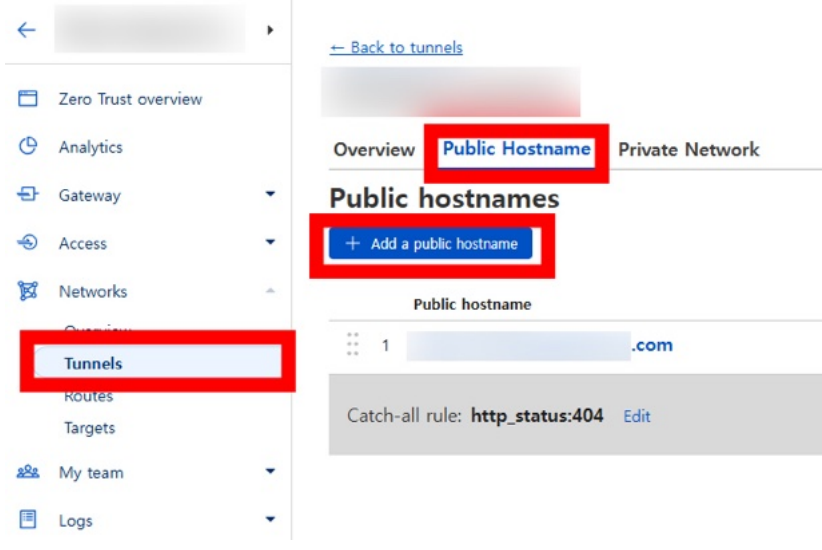
도메인을 연결해 퍼블릭 릴레이 서버로 만들기

엄브렐 기기에서 돌아가는 노스터 릴레이 서버에 도메인을 연결하고 퍼블릭 릴레이 서버로 만들 수도 있다. 이렇게 연결한 도메인 주소는 지인들에게 알려주고, 지인들이 자신의 릴레이 서버를 사용하게 할 수 있다.

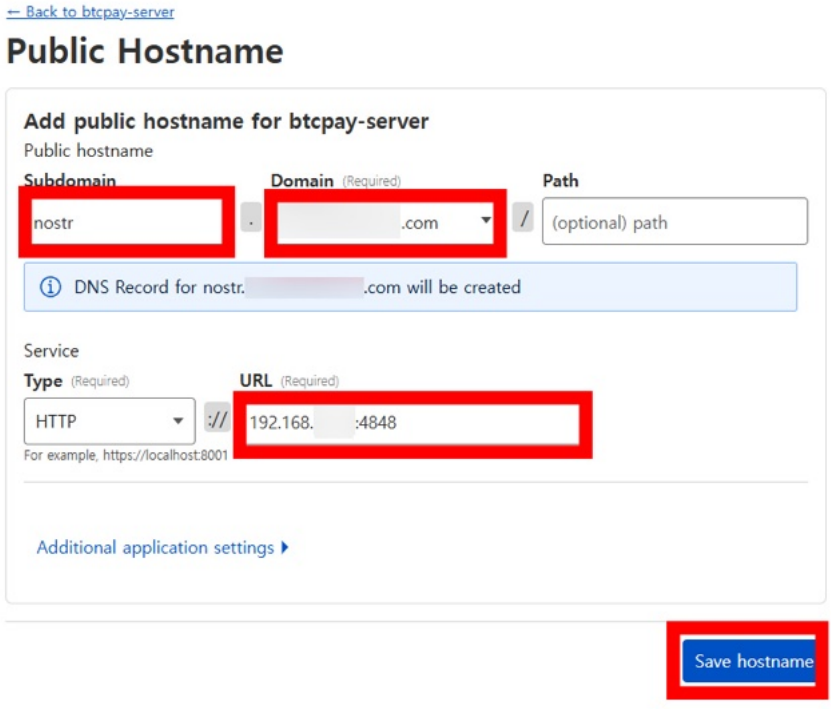
지금은 도메인을 연결하는 방법을 알아보겠다. 클라우드플레어를 이용할 것인데, 앞에서 BTCPay Server 도메인이 클라우드플레어 터널링으로 이미 연결되어 있다면, 서브도메인을 하나 추가하여 릴레이 서버와 연결하는 것은 매우 간단하다. 클라우드플레어에 가입하고, 도메인을 구매하는 방법은 '4부. 라이트닝 노드 운영 가이드'의 '라이트닝 노드로 온라인 비트코인 결제 매장 구축하기' 장을 참고하라.

클라우드플레어 웹사이트에서 로그인을 하고 대시보드에서 [Zero Trust]를 누른다.

왼쪽 탭에서 [Networks] → [Tunnels] → [Public Hostname] → [+ Add a public hostname]을 누른다.

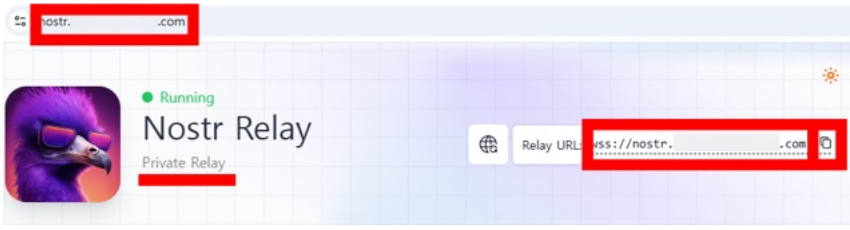


여기서 도메인을 선택하고, 'Subdomain'에 BTCPay Server를 연결했던 서브도메인과는 다른 서브도메인을 입력하면 된다. 예를 들어 서브도메인에 'nostr'를 입력하면 nostr.내 도메인.com으로 연결될 것이다. 그 아래에 있는 'URL'에는 엄브렐 기기의 로컬 네트워크 IP 주소를 입력하고 뒤에 포트 번호 :4848을 붙인다. 그다음 [Save hostname]을 눌러 저장한다.

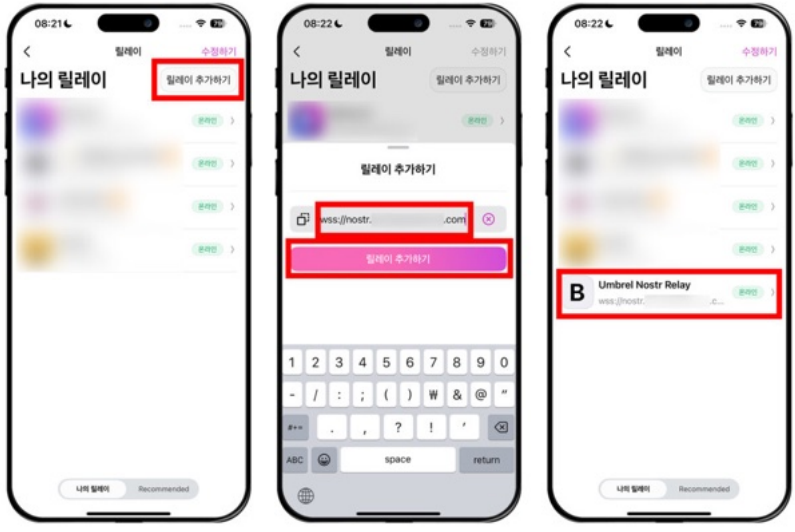


이제 웹 브라우저 주소창에 nostr.내 도메인.com을 입력해 보면 나의 노스터 릴레이 서버로 접속이 되는 것을 알 수 있다. 오른쪽 상단에 연결할 수 있는 주소가 나온다. SSL 인증도 되었으므로 스킴이 ws://가

아니라 wss://가 되는 것을 알 수 있다. 아래에 'Private Relay'라고 나오는 것은 UI상에서만 그렇게 나오는 것이지, 이렇게 도메인을 연결하면 퍼블릭 릴레이 서버로 운영할 준비가 된 것이다.



노스터 클라이언트에서 [릴레이 추가하기]를 누르고 해당 주소를 입력한다. 이때 맨 앞에 프로토콜 스킴으로 wss://를 붙이고, 그 뒤에 서브도메인을 포함한 도메인 주소(nostr.내 도메인.com 등)를 적는다. 그 다음에 [릴레이 추가하기]를 누르면 도메인을 이용해 자신의 릴레이 서버에 잘 연결된 것을 알 수 있다.



엄브렐 앱스토어에서 설치한 노스터 릴레이 서버 앱으로 퍼블릭 릴레이 서버를 제대로 운영할 것이라면, config 파일에서 몇 가지 설정을 해야 한다. 엄브렐에서 [파일] 앱 → [앱] → [nostr-relay] → [data] → [relay] 폴더에 들어있는 config.toml에서 변경할 수 있다. 도메인 주소를 알고 있는 모두가 릴레이 서버에 연결할 수 있도록 허용할 것이 아니라면, [authorization] 섹션에서는 'pubkey_whitelist'에 연결을 허용할 계정들의 공개키를 배열로 입력해야 한다.

[info] 섹션에서는 'relay_url'을 제대로 명시하고, 'name'(릴레이 서버 이름)과 'description'(릴레이 서버 설명), 'pubkey'(관리자 노스터 공개키), 'contact'(연락할 관리자 이메일) 등을 입력한다.

[limits] 섹션에는 스팸 계정이나 과도한 이벤트 요청, 과도한 트래픽으로 인한 서비스 거부 공격을 막기 위해 설정하는 옵션들이 있다. 'messages_per_sec'는 1초에 몇 번의 이벤트를 생성할 수 있는지 제한하는 용도다. 2-5 정도면 적당하다. 'subscriptions_per_min' 옵션은 1분에 이벤트 검색을 몇 번 요청할 수 있는지 제한하는 용도다. 20 정도면 적당하다.

노스터에서 NIP-05 노스터 주소를 이용해 인증된 npub을 식별할 수 있게 하려면 [verified_users] 섹션에서 'mode'를 'passive'로 변경해 놓으면 된다.

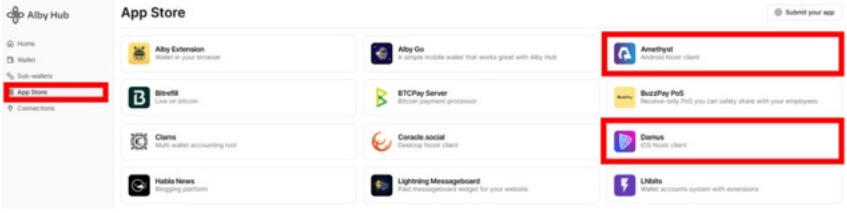
[network] 섹션에서 'remote_ip_header' 옵션은 'cf-connecting-ip'로 설정해 놓으면 된다. 우리는 클라우드플레어 터널로 연결을 했기 때문에 기존 방법으로는 릴레이 서버에 연결하는 사용자들의 IP 주소를 볼 수 없기 때문이다.

다른 옵션들도 config 파일에 주석을 보면 영어로 설명되어 있으니, 찬찬히 보고 설정할 수 있을 것이다. config 파일을 특별히 만지고 싶지 않다면 자신의 지인들에게만 도메인을 알려줄 수도 있다. 그러나 일단 자신이나 지인이 도메인을 통해 릴레이 서버에 연결하면 누구나 해당 도메인을 볼 수 있으므로, config 파일에서 신중하게 옵션들을 설정한 뒤 퍼블릭 릴레이 서버를 운영할 것을 권장한다.

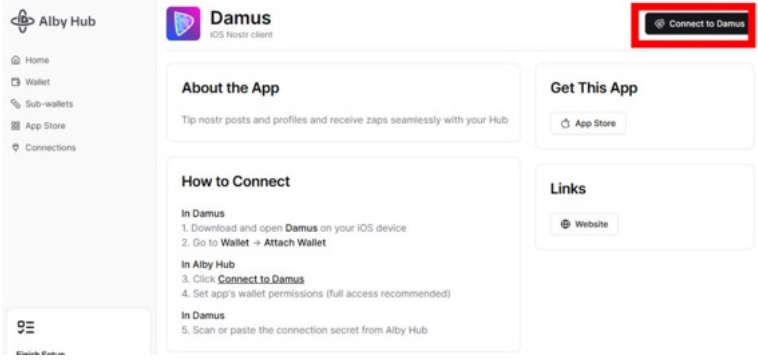
| NWC를 이용해 자신의 라이트닝 노드에서 잽 보내기

알비 허브를 통해 NWC 지갑 생성하기

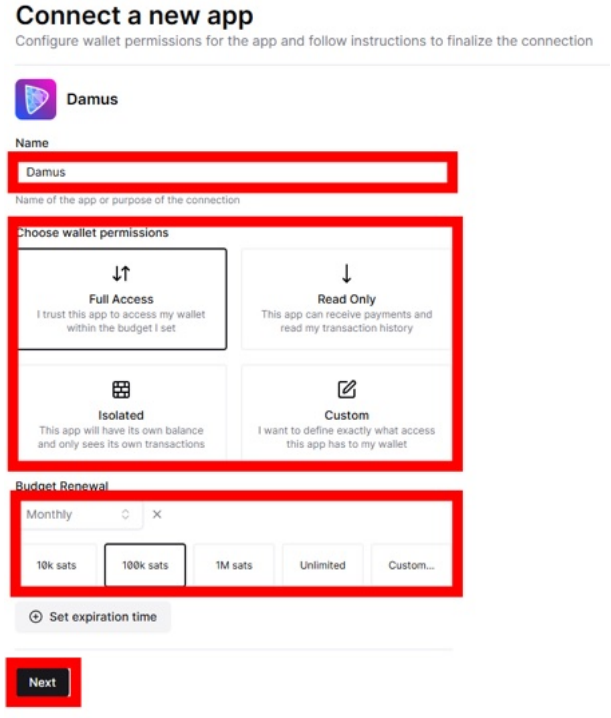
알비 허브에서 NWC 지갑을 설정하고 연결할 수 있다. 알비 허브를 실행하고, 왼쪽 탭에서 [App Store]를 누른다. 그다음에 연결할 클라이언트 앱(다무스, 애머시스트, 피닉스 등)을 선택한다.



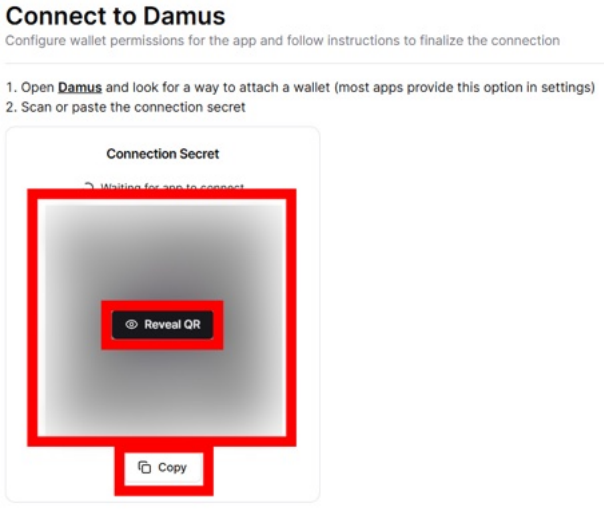
이번에는 다무스를 연결해 보겠다. [Damus]를 누르고, 우측 상단의 [Connect to Damus]를 누른다.



'Name'에서 지갑 이름을 설정한다. 그다음 'Budget Renewal'에서 일정 기간 동안 최대 얼마나 사용할 수 있게 할지 설정한다. 만약 Monthly를 선택하고, 100k sats를 선택하면 한 달에 최대 10만 sats까지만 보낼 수 있다. 'Budget Renewal'에서 [Monthly] → [100k sats]를 선택해 보겠다. 그다음 [Next]를 누른다.

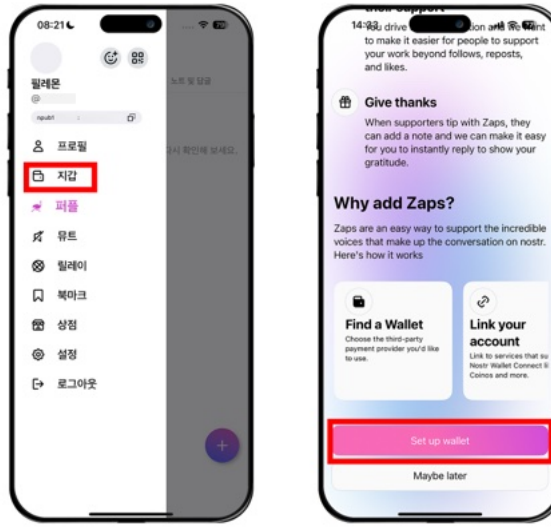


[Copy]를 눌러 NWC 지갑 연결 주소를 복사할 수도 있고, [Reveal QR]을 눌러 연결 QR 코드를 볼 수도 있다. 여러 앱에서 NWC를 통해 지갑을 연결하고 싶은 경우 이 주소를 잘 보관해야 한다. 다만, 연결 주소가 유출되지 않게 조심하자.

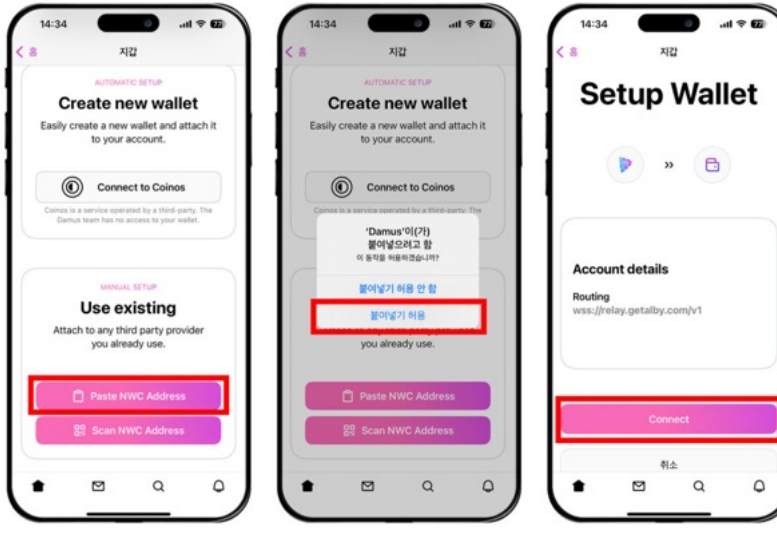


다무스에서 NWC 지갑 연결하기

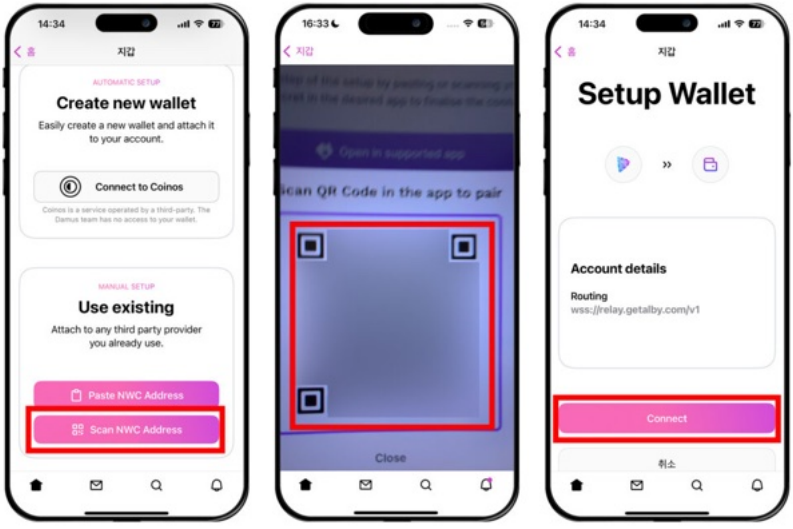
이제 다무스에서 NWC 지갑을 연결하는 과정을 알아보자. 메뉴에서 [지갑]을 누르고 스크롤을 내려 [Set up wallet]을 선택한다.



[Paste NWC Address]를 눌러 앞에서 알비 허브에서 복사했던 NWC 지갑 연결 주소를 붙여넣는다. 그다음 [Connect]를 누르면 된다.

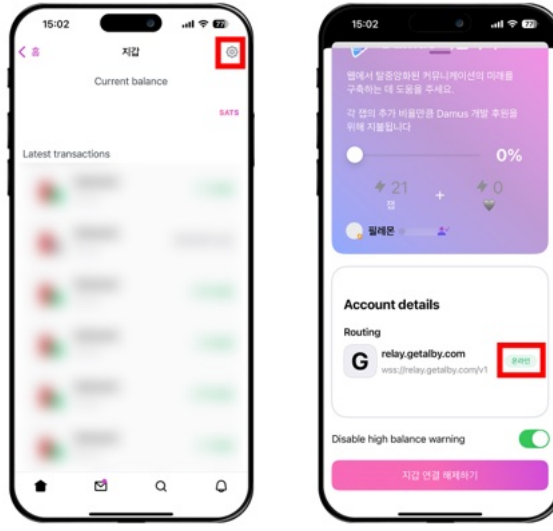


혹은 [Scan NWC Address]를 누르고, 알비 허브에서 볼 수 있는 QR 코드를 스캔하면 된다. 그다음 [Connect]를 누른다.



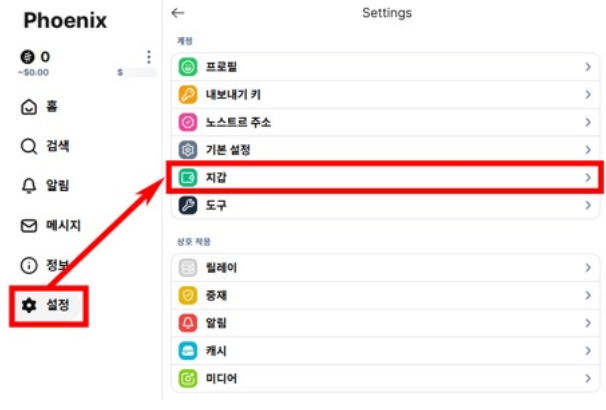
그러면 지갑이 연결될 것이다. 참고로 NWC 지갑을 생성한 지 얼마 되지 않은 경우 지갑 연결이 원활하지 않을 수 있다. 하루 정도 기다리면 잘 연결될 것이다.

지갑 창에서 오른쪽 상단 톱니바퀴 모양의 버튼을 눌러 설정 창으로 진입한다. '온라인'으로 표시된다면 연결이 잘 된 것이다. 다른 사람에게 잽을 날리고, 잘 보내지는지 확인해 보자.

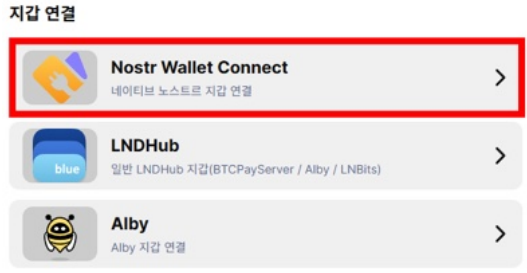


피닉스에서 NWC 지갑 연결하기

이번에는 피닉스에서 NWC 지갑을 연결하는 방법을 알아보자. 왼쪽 탭에서 [설정] → [지갑]을 누른다.



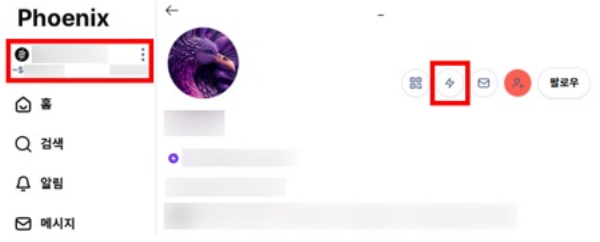
지갑 연결에서 [Nostr Wallet Connect]를 선택한다.



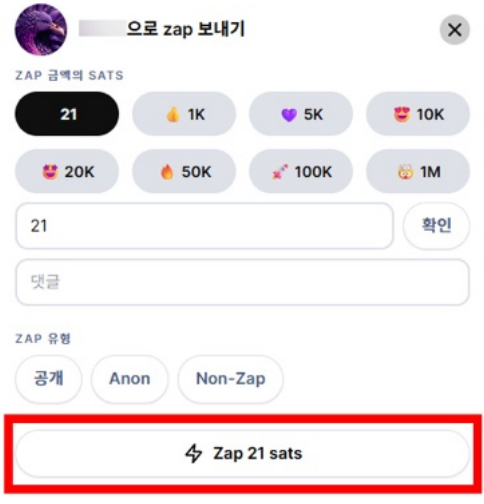
여기에 알비 허브에서 복사했던 지갑 연결 주소를 입력하고, [연결]을 누른다.

연결이 잘 되면 왼쪽에 지갑 잔액이 나온다. 피닉스도 마찬가지로 NWC 지갑을 생성한 지 얼마 되지 않았다면 제대로 연결될 때까지 시간이 좀 필요할 수도 있다. 연결이 잘 안된다면 최대 하루 정도 기다려보자.

다른 사람의 프로필이나 포스팅에서 잽을 날려보자. 번개 모양의 버튼을 누르면 된다.



잽 금액과 함께 보낼 댓글을 입력한 후 [Zap ?? sats]를 누르면 잽이 전송된다.

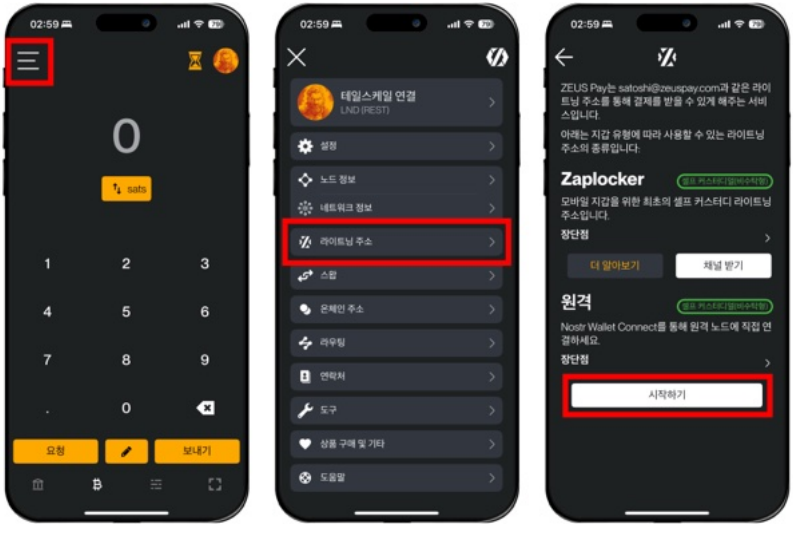


| NWC를 이용해 제우스에서 라이트닝 주소 발급하기

제우스에서 라이트닝 주소 발급하기

제우스에서는 NWC를 이용해 '~@zeuspay.com' 형태의 라이트닝 주소를 간단하게 발급할 수 있다. 이 방법에 대해 알아보자. 참고로 커스텀 주소를 발급받기 위해서는 유료 플랜을 구독해야 한다.

먼저 제우스 홈 화면에서 좌측 상단의 메뉴 버튼을 누른 후, [라이트닝 주소]를 누른다. 그다음 '원격' 밑에 있는 [시작하기]를 누른다.



입력창에 NWC 주소를 붙여넣고, [연결 문자열 테스트]를 누른다. NWC 지갑 연결에 성공하면 '연결 테스트 완료'라는 문구가 나온다. 그러고 [라이트닝 주소 만들기]를 누르면 라이트닝 주소가 발급된다. 그 아래에 있는 QR 코드 모양의 버튼을 누르면 QR 코드도 볼 수 있다. 커스텀 주소를 발급받기 위해서는 'ZEUS Pay+'라는 플랜을 구독해야 한다.

이로써 노스터 클라이언트 이용 방법뿐만 아니라 릴레이 운영 방법, NWC를 이용해 자신의 라이트닝 노드에서 잽을 보내는 방법까지 모두 알아보았다. 검열 불가능한 진정한 자유의 공간 노스터에 양질의 글을 올려보고, 잽을 통해 보상도 노려보자.