

비트코인 사용 가이드

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



2판
2025. 9. 1. 기준

필레몬 지음
HYPE 감수
익스투스 출판

비트코인 사용 가이드

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

비트코인 사용 가이드: 개인 지갑, 결제, 폴 노트, 라이트닝 노트, 노스터, 홈 채굴 가이드, 제2판
저작권 없음 © ① 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: H9gTJU0T1JIYQ6VxsDd89A0TgiE1by7bdK4EDXf7arjFDg3gqP/wdqoRcL
SiwXwp/rNNSen3t/pxK2AFDDxmKjE=

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

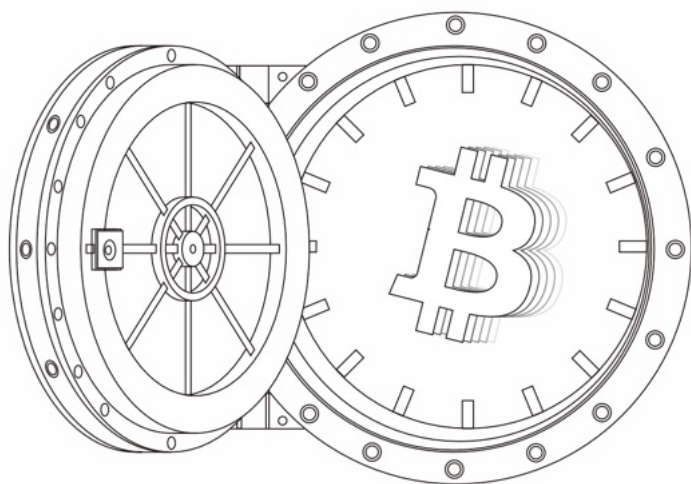
저자의 저작재산권 포기가 상표권, 저작권격권, 퍼블리시티권, 프라이버시권, 저자에게 귀속되지 않는 제3자의 권리 등의 포기를 의미하지 않습니다. 이를 무시하여 발생하는 문제에 대한 책임은 전적으로 사용자에게 있습니다.

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

익스투스 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 년척에 확장 공개키 내보내 워치-온리 지갑 만들기 · 94 코코넛 월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 · 101 블루월렛으로 서명 연습 · 105 년척으로 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 번조 여부 확인(윈도우OS) · 130 소프트웨어 번조 여부 확인(맥OS) · 141 부팅 마이크로SD카드 만들기 · 150 발레나에 처로 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 년척에 확장 공개키 내보내 워치-온리 지갑 만들기 · 204 코코넛 월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 · 212 블루월렛으로 서명 연습 · 218 년척으로 서명 연습 · 224 코코넛 월렛으로 서명 연습 · 231 시드사이너를 게임기로 만들기 · 236	

<ul style="list-style-type: none"> <ul style="list-style-type: none"> 스마트폰 공기계계를 콜드월렛으로 사용해 지갑 생성하기 · 247 블루월렛에 확장 공개키 내보내 워치-온리 지갑 만들기 · 256 년척에 확장 공개키 내보내 워치-온리 지갑 만들기 · 262 블루월렛으로 서명 연습 · 269 년척으로 서명 연습 · 274 공기계 블루월렛에서 간접 복구 테스트 · 279 	247
<ul style="list-style-type: none"> <ul style="list-style-type: none"> 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 	282
<ul style="list-style-type: none"> <ul style="list-style-type: none"> 전송 경로 · 322 개인 지갑에서 해외 거래소로 전송 · 323 해외 거래소에서 국내 거래소로 전송 · 324 국내 거래소에서 원화 환전 후 은행 계좌로 출금 · 330 	322
<ul style="list-style-type: none"> <ul style="list-style-type: none"> 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 년척에서 UTXO 정리하기 · 368 	334
<ul style="list-style-type: none"> <ul style="list-style-type: none"> 온-체인 수수료 · 376 멤풀 웹사이트 보는 방법 · 379 적정 수수료율 설정하기 · 382 RBF · 386 CFPF · 401 	376
<ul style="list-style-type: none"> <ul style="list-style-type: none"> 패스플레이즈와 주의 사항 · 418 키스톤에서 패스플레이즈 설정하기 · 420 시드사이너에서 패스플레이즈 설정하기 · 424 공기계 콜드월렛에서 패스플레이즈 설정하기 · 425 서명 기기에서 서명이 안 될 때 · 430 	418
<ul style="list-style-type: none"> <ul style="list-style-type: none"> 멀티시그(다중서명) · 431 블루월렛에서 멀티시그 지갑 생성 · 434 년척에서 멀티시그 지갑 생성 · 446 스패로우 지갑에서 멀티시그 지갑 생성 · 461 블루월렛 멀티시그 지갑에서 서명하기 · 478 년척 멀티시그 지갑에서 서명하기 · 487 스패로우 멀티시그 지갑에서 서명하기 · 495 멀티시그 워치-온리 지갑 삭제 후 복구하기 · 505 	431

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
- **엠프렐 홈 구매 및 세팅** 587
풀 노드 구축 방법 · 587 | 엠프렐 홈 구매 방법 · 588 | 엠프렐 홈 세팅 · 596
- **미니 PC 조립하고 엠프렐OS 설치하기** 598
미니 PC 준비물 · 598 | 미니 PC 조립하기 · 603 | 바이오스에서 램 설정하기 · 609 | OS 설치용 USB 만들기 · 611 | 엠프렐OS 설치하기 · 618
- **라즈베리파이5 조립하고 엠프렐OS 설치하기** 623
라즈베리파이5 준비물 · 623 | SSD에 엠프렐OS 설치하기 · 630 | 라즈베리파이5 조립 · 639 | 부팅이 안 될 경우 · 650 | 케이스 조립 · 660

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 위치타워 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 앱 보스에서 노드 정보 입력하기 · 984	
■ 라이트닝 노드로 온라인 비트코인 결제 매장 구축하기	990
워드프레스에 BTC Pay Server, 우커머스 플러그인 설치 · 990 우커머스 기본 설정 및 테마 선택 · 992 우커머스 상품 올리기 · 996 엠브렐에서 BTC Pay Server 다운로드하고 설정하기 · 1001 클라우드플레이어 회원가입 · 1009 클라우드플레이어 터널 연결 · 1016 도메인 연결 · 1020 SSL 적용 · 1025 워드프레스 우커머스와 자신의 BTC Pay 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 중단간 암호화 · 1046 잭(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 잭을 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 잭을 받기 위한 라이트닝 주소 연결 · 1068 다른 사람에게 잭 보내기 · 1070	
■ 피닉스 사용 방법	1073
피닉스에서 개인키-공개키 쌍 생성 · 1073 다른 사람들에게 npub 알려주기 · 1079 팔로우 추가 · 1081 잭을 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	
■ 엮브렐에서 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 잭 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 다팀과 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	
■ 다팀으로 풀 노드와 채굴기 연결하기	1200
비트코인 노츠 설치 · 1200 다팀 설치 · 1202 다팀에서 솔로 채굴 설정하기 · 1204 비트엑스를 다팀 에 연결하기 · 1208 아발론 나노 3를 다팀에 연결하기 · 1210 채굴이 잘 되는지 확인하기 · 1211 다 팀을 이용하여 채굴 풀(오션 풀) 참여하기 · 1213 블루월렛에서 생성된 지갑 주소 사용 · 1214 라이트 닝 노드에서 생성된 온-체인 주소 사용 · 1216 다팀 설정하기 · 1216 비트엑스를 다팀에 연결하기 · 1220 아발론 나노 3를 다팀에 연결하기 · 1222 채굴이 잘 되는지 확인하기 · 1223 라이트닝 지갑으 로 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 기 기의 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

2. 비트코인 스탠다드 가이드

2. 비트코인 스탠다드 가이드

| 비트코인은 돈이다

비트코인은 돈이다

비트코인은 종종 '디지털 금'이라고 불린다. 이는 비트코인의 희소성과 구매력 보존 기능을 강조하는 비유지만, 비트코인의 진짜 본질을 모두 설명하지는 못한다. 비트코인은 돈이고, 현금이다. 비트코인 백서의 제목이 「비트코인: 개인 대 개인 전자 화폐 시스템」이지 않은가? 지금 우리 사회는 특정 돈을 쓰라고 강제되는 명령 화폐(법정 화폐) 제도하에 살고 있지만, 원래 돈은 시장에서 자유롭게 경쟁해야 한다. 그러다가 더 우수한 특질을 가진 돈이 시장에서 자연스럽게 선택된다. 돈의 3대 기능은 교환 매개, 구매력 보존, 회계 단위다. 그러니 비트코인을 디지털 금이라고만 부르는 것은 비트코인의 진짜 본질 중 한 가지만 보는 것이다. 이런 잘못된 시각을 가지면 비트코인이 가져올 미래를 지나치게 축소해서 볼 수밖에 없다.

경제학자인 사이페딘 아모스 Saifedean Ammous는 자신의 저서 『비트코인 스탠다드』(한국어판: 『달리는 왜 비트코인을 싫어하는가』)에서 비트코인 때문에 정부 발행 지폐도 조개껍데기, 소금, 소, 귀금속과 같은 골

동품이 될 것이라고 했다. ‘비트코인 스탠다드’는 비트코인이 표준 화폐로 채택된 시대를 뜻한다.

기술이 발전하고 현실이 바뀔 때마다 사람들이 채택하는 화폐 기준이 바뀌고, 이에 따라 경제와 사회가 엄청나게 큰 영향을 받는다. 카이사르 시절 로마인이나 콘스탄티누스 시절 비잔티움인, 금본위제 시절 유럽인 같이 건전화폐를 선택한 사회와 개인은 엄청난 혜택을 누렸다. 한편 오키프가 도착할 당시 압섬 사람들이나 유리구슬을 쓰던 서아프리카인, 19세기 은본위제 시절 중국인처럼 불건전화폐나 기술이 열등한 화폐를 쓰던 사람은 비싼 값을 치렀다.

사이페딘 아모스 지움, 위대선 옮김, 『달리는 왜 비트코인을 싫어하는가』, 터닝포인트, 2018.

이게 사실이라면 비트코인을 채택한 사회와 비트코인을 채택하지 않은 다른 사회의 격차는 물론이고, 한 사회 내에서도 비트코인을 채택한 개인과 비트코인을 채택하지 않은 다른 개인의 격차도 벌어진다는 뜻이다. 대체 비트코인의 무슨 속성이 다른 돈보다 뛰어나길래 법정화폐를 대체한다는 것일까? 이를 알아야 비트코인이 금처럼 금고에 저장해두는 자산이 아니라, 자유롭고 세계적인 교환 수단으로 설계된 진짜 돈이라는 것을 알게 될 것이다. 돈은 단순히 구매력만 보존하는 것이 아니라, 교환되고, 가격을 계산하며, 경제 활동을 매끄럽게 연결하는 기능을 수행해야 한다. 따라서 비트코인을 단순히 모으기만 한 사람과, 비트코인으로 직접 결제를 해보거나 받아본 사람의 비트코인에 대한 이해 수준은 천지 차이이다. 비트코인을 디지털 금이라 생각하는 사람들은 비트코인의 가격 상승만 기대하며 비트코인을 사용하는 것을 망설인다.

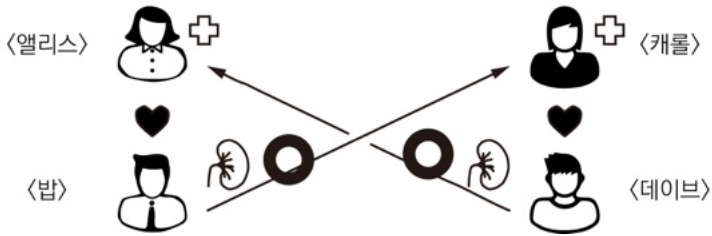
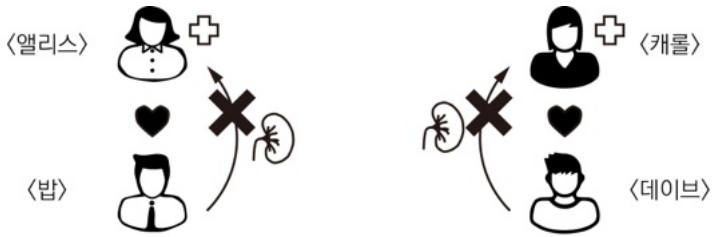
교환 매개

돈의 가장 중요한 기능은 교환 매개다. 돈이란 본질적으로 교환을 매끄럽게 해주는 수단이다. 물물교환을 통해 경제 활동을 하는 사회를 상상해 보자. 이런 사회에서는 물건을 교환하려는 두 당사자의 수요가 정확

히 일치해야만 교환이 가능하다. 사과를 먹고 싶은 목수에게 생선을 주며 집을 지어달라고 할 수는 없기 때문이다.

물물교환의 문제점은 장기 교환(신장 이식 매칭) 문제에 대한 앨빈 로스 Alvin Roth의 연구에서 단적으로 드러난다. 앨리스와 밥 부부가 있고, 캐롤과 데이브 부부가 있다고 해보자. 앨리스와 캐롤은 신장 문제가 있어서 신장 이식을 받아야 한다. 앨리스의 남편인 밥은 앨리스에게 신장을 기부하고 싶고, 캐롤의 남편인 데이브는 캐롤에게 신장을 기부하고 싶다. 그러나 신장은 신장 조직이 서로 맞아야만 이식이 가능하다. 안타깝게도 밥의 신장은 아내인 앨리스와 맞지 않고, 데이브의 신장은 캐롤에게 맞지 않다. 하지만 밥의 신장은 캐롤에게 맞고, 데이브의 신장은 앨리스에게 맞는다면 두 커플은 교차 기증을 통해 신장 이식 수술을 진행할 수 있다.

두 커플 사이에서 신장 교차 이식이 가능하게 하려면 신장이 서로 맞는 사람을 찾아야 한다. 다른 신장 기증자 중 적합한 사람을 찾지 못하면 이식 수술이 불가능하다. 이때 매칭된 두 커플의 수술은 반드시 동시에 같은 장소에서 진행되어야 하는데, 둘 중 하나의 수술이 먼저 진행된다면 나중에 진행될 수술의 기증자가 마음을 바꿀 수도 있기 때문이다. 따라서 수술팀은 총 네 팀이 필요하다. 앨리스, 밥, 캐롤, 데이브의 수술이 모두 동시에 이뤄져야 하기 때문이다. 실제로 미국 테네시주에서는 기증자 두 명, 환자 두 명, 총 네 건의 수술이 같은 병원에서 동시에 이뤄졌다.



이제 커플의 수를 확장해 보자. A 커플은 B 커플에게 신장을 기증할 수 있고, B 커플은 C 커플에게 신장을 기증할 수 있고, C 커플은 A 커플에게 신장을 기증할 수 있다고 해보자. 그러면 세 커플은 신장 이식 수술이 가능하다. 물론, 세 커플은 같은 장소에서 같은 시각에 수술을 진행해야 한다. 그렇지 않으면 배신의 문제에 직면하기 때문이다. 이때 수술팀은 총 여섯 팀이 필요하다. 실제로 존스 홉킨스 병원에서 6명의 수술이 동시에 진행됐다.

이런 문제가 3팀이 아니라 4팀, 5팀으로 확장될수록 문제는 매우 복잡해진다. 물물교환은 사기의 위험 때문에 ‘같은 장소’에서 ‘동시’에 이뤄져야 한다. 화폐는 이를 해결해 준다. 그리고 해결해 주어야 한다. 이것이 화폐의 효용이다. 화폐는 장소와 시간을 뛰어넘어 수요와 공급을 매칭해 주어야 한다. 화폐가 시간을 뛰어넘어 이를 매칭해 줄 때 필요한 핵심적인 기능이 구매력 보존의 기능이다. 구매력이 온전히 보존되

어야 과거의 내가 미래의 누군가와 거래할 수 있게 되기 때문이다. 이를 위해서는 화폐가 다른 무엇으로도 쉽게 교환될 수 있는 '시장성'을 갖고 있어야 한다.

비트코인은 공간을 뛰어넘어서도 교환이 가능하게 해준다. 비트코인은 어떤 화폐보다도 휴대성이 뛰어나다. 수 톤의 금을 다른 나라로 옮긴다고 해보자. 수많은 호위함, 전투기가 동원되어야 한다. 비트코인은 그걸 얼마든 빛의 속도로 지구 반대편으로 보낼 수 있다.

교환 매개 기능을 만족하려면 휴대성 외에도 분할성, 대체 가능성이 뛰어나야 한다. 비트코인은 지금까지 존재했던 돈 중에 분할성이 가장 높다. 비트코인은 1억 분의 1로 쪼개진다. 심지어 다중 레이어 위에서는 더 쪼개질 수도 있다.

대체가능성에 대해 살펴보자. 금 1kg과 다른 금 1kg이 같은지 검증하는 것은 굉장히 까다롭다. 일반인들은 이것 알아내기 어렵기 때문에 순도가 낮은 금이 유통되었고, 그래서 금 세공업자들이 금의 순도를 인증해 주었다. 현재도 그렇다. 민간 금 세공업자들이 몇 K인지 인증을 해준다. 이것이 금의 치명적인 약점이었는데, 금 세공업자나 국가만이 금의 순도를 검증할 수 있었기 때문에 사람들이 금을 금 세공업자나 국가에 맡기고 그들을 신뢰하며 거래할 수밖에 없었다. 금 세공업자들은 자신들이 가진 것보다 더 많은 금을 다른 사람들에게 빌려주었고(이것이 은행의 탄생 배경이다), 국가는 금화에 불순물을 섞어 화폐 주조 차익을 챙겼다. 하지만 비트코인은 이 코인이 이중지불된 건지 아닌지 누구나 풀 노드를 운영해 검증할 수 있다. 1 BTC와 다른 1 BTC가 같은 건 누구나 검증 가능하다.

비트코인은 공간을 초월해 교환을 가능하게 할 뿐 아니라, 중개자 없이도 송금이 가능하게 해준다. 기존의 금융 시스템에서는 국제 송금이나 대규모 거래를 할 때 여러 은행과 결제 시스템을 거쳐야 했지만, 비트코인을 통해 거래할 때는 이러한 과정 없이 분산된 네트워크 안에서 직접 검증할 수 있는 거래가 이루어진다. 이는 곧 비용 절감, 거래 시간 단축, 그리고 시스템 전반의 투명성 향상으로 이어진다.

이 덕분에 비트코인은 검열 저항성을 갖는다. 어느 누구도 비트코인으로 거래하려는 것을 막을 수 없다. 전통적인 금융 시스템에서는 정부, 은행, 결제 사업자가 특정 거래를 차단하거나 특정 사람을 금융망에서 배제할 수 있다. 이런 사례는 매우 많은데, 단순히 정부가 돈의 용처를 지정하는 것부터(특정 지역에서만 쓸 수 있거나, 주식/부동산에는 못 쓰고 특정 업종에만 돈을 쓸 수 있게 하는 사례는 너무 많다.) 아예 특정 사상을 가진 사람들의 돈을 동결하는 사례들도 있다. 예를 들어 2022년 캐나다에서는 트럭 시위가 일어났는데, 당시 캐나다 정부는 비상사태법을 발동하여 시위 참가자들의 은행 계좌를 동결했으며, 그들에게 모금된 자금을 차단했다.

비트코인은 시공간을 초월할 뿐 아니라, 정치적 경계와 권력의 압력조차 넘어설 수 있는 새로운 형태의 교환 수단이다. 비트코인은 단순한 디지털 금이 아니라, 교환 매개로서도 완벽하다.

구매력 보존

돈은 구매력을 보존할 수 있어야 한다. 구매력 보존이란 내가 현재 생산한 것에서 필수적으로 이용해야 하는 것을 제외하고 나머지를 남겨두었다가 그것을 대가로 ‘미래에’ 내가 원하는 것을 얻는 것이다. 이를 통해

인간은 미래를 대비할 수 있게 된다. 또한 사람들이 화폐로 저축함에 따라 화폐 보유의 한계 효용이 감소하고 투자나 후원 등이 생겨 문명화를 이루게 된다.

그런 점에서 보면 현대 법정 화폐 시스템은 고장 났다. 돈이 구매력 보존의 기능을 못 하기 때문이다. 각국의 정부는 케인스 경제학을 주류 경제학 이론으로 받아들이고 있다. 케인스 경제학은 개인이 저축을 통해 구매력을 보존하려는 행위를 경제에 해로운 것으로 간주하며, 소비를 유도하기 위해 의도적으로 화폐 구매력을 지속적으로 떨어뜨리는 정책을 추진한다. 이로 인해 물가는 끊임없이 상승하고, 법정 화폐를 사용하는 개인들은 미래를 준비하는 데 심각한 제약을 받게 된다. 결국 사람들은 점점 더 국가의 복지와 재정 정책에 의존하게 되며, 독립적인 개인이 아니라 정부에 의존하는 소비자로 전락하고 만다. 물가가 오르는 것은 당연한 것이 아니다. 물가가 오르는 것은 우리가 사용하는 화폐 구매력이 떨어졌다는 뜻이다. 1975년 자장면 한 그릇의 가격은 약 138원이었다. 2025년 자장면 한 그릇의 가격은 7,500원이다. 50년 동안 가격이 약 50배가 올랐다. 사람들이 생각하는 자장면의 가치가 50배 오른 것일까? 그럴 리가 없지 않은가. 우리가 사용하는 돈의 구매력이 50분의 1로 폭락했을 뿐이다. 이는 누군가가 돈을 계속 찍어내고 있기 때문에 발생하는 일이다.

돈이 구매력을 보존하지 못 하게 되면 사람들은 구매력을 보존할 다른 수단을 찾는다. 현금을 갖고 있어봤자 내 구매력은 지속적으로 약해지므로 어떻게든 주식이나 부동산, 채권에 투자하여 구매력을 지키려고 한다. 그러나 이런 자산들은 모두 다른 누군가가 소유권을 보장해 주는 자산이다. 이런 자산들은 소유권을 보장해 주는 주체가 얼마든지 당

신의 구매력을 강탈해 갈 수 있다. 세금이든, 동결이든, 거래 허가제를 시행하든, 압류든 여러 방법을 통해서 말이다.

비트코인은 어떻게 구매력을 보존할 수 있을까? 비트코인이 희소하다는 건 이제 대부분의 사람이 아는 것 같다. 하지만 비트코인의 희소성은 공급량이 2,100만 개로 한정되어 있다는 것보다는 난이도 조정 메커니즘에서 더 비롯된다. 그리고 한정된 공급량과 난이도 조정 메커니즘은 분산된 네트워크에서 풀 노드들에 의해 수호되고 있다. 이 때문에 비트코인은 불변성을 지니게 되는데, 어떤 개인도 한정된 공급량과 난이도 조정 메커니즘을 수정할 수 없기 때문이다.

일반적인 상품은 가격이 오르면 생산자들이 그 상품을 더 많이 생산할 유인이 생긴다. 상품 가격이 올라서 생산자가 더 많은 생산을 하고 상품이 시장에 풀리면 가격이 내려간다. 만약 어떤 사람이 이 상품을 통해 구매력을 유지하고자 했다면, 생산자가 더 많은 생산을 함으로써 그 사람의 구매력이 내려간 것이다. 내려간 구매력은 어디로 갔을까? 상품 생산자가 가져간 것이다.

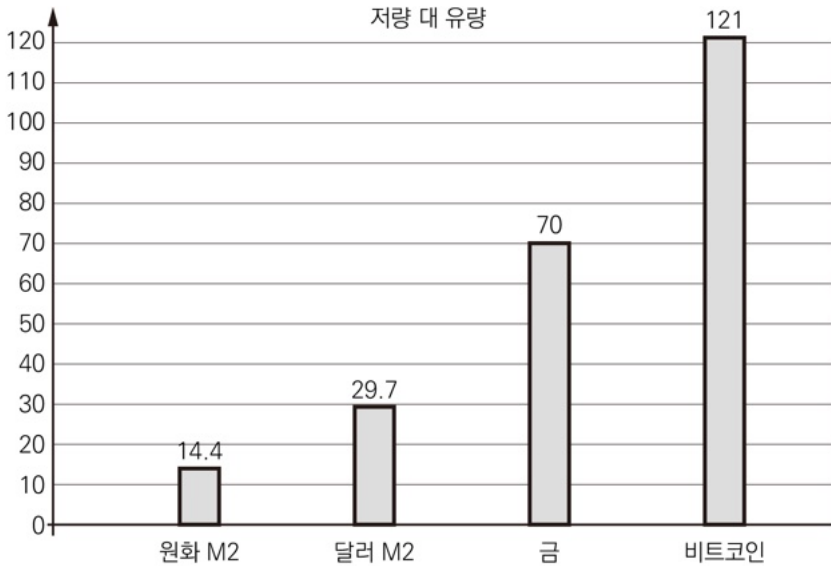
법정 화폐도 마찬가지다. 사람들이 지금 당장 소비하는 대신 구매력을 미래로 이전하고자 하면 화폐로 저축하려는 수요가 늘어난다. 그러면 중앙은행이나 정부는 화폐를 찍어낸다. 이로 인해 화폐를 갖고 있던 사람들은 구매력을 잃는다. 사람들이 잃어버린 구매력은 중앙은행과 정부가 가져간 것이다.

하지만 비트코인은 공급량이 한정되어 있으므로 내가 가진 비트코인 1개는 영원히 전체 2,100만 개 중 하나다. 또한, 난이도 조정 메커니즘으로 인해 비트코인 생산(채굴)에 더 많은 에너지를 쏟아부어도 정해진 양 이상을 생산할 수가 없다.



시장에 이미 존재하는 상품의 양을 저량이라고 하며, 새롭게 시장에 공급되는 상품의 양을 유량이라고 한다. 구매력 보존 기능이 제대로 작동하려면 저량 대 유량 비율이 높아야 한다. 새롭게 공급되는 양이 이미 존재하는 양에 비해 미미해야 한다는 뜻이다.

금조차도 에너지를 더 많이 쏟아부으면 더 많은 생산이 가능하다. 실제로 금의 '연간' 생산량은 인류가 에너지 혁명을 겪을 때마다 기하급수적으로 증가했다. 이렇게 유량이 높아짐에도 불구하고 금이 그동안 인류 역사에서 구매력 보존 기능을 할 수 있었던 이유는 유량에 비해 저량이 압도적으로 많기 때문이다. 금은 이온화경향이 가장 낮은 금속으로 일반적인 상태에서는 녹이 슬기가 매우 어렵다. 따라서 2천 년 전 채굴한 금도 지금까지 그대로 있다. 이런 특성 때문에 금은 저량이 매우 높아졌다.



비트코인은 어떤 상품보다 저량 대 유량 비율이 높으며, 반감기를 거쳐 언젠가는 저량 대 유량 비율이 무한대가 된다. 비트코인의 난이도 조정 메커니즘으로 인해 비트코인은 아무리 채굴에 에너지를 쏟아부어도 유량이 늘어나는 데 한계가 있다. 2024년 기준 한국은행 발표 자료를 바탕으로 계산한 원화의 저량 대 유량 비율(M2 기준)은 14.4고, 연방준비은행 발표 자료를 바탕으로 계산한 달러의 저량 대 유량 비율(M2 기준)은 29.7이다. 금의 저량 대 유량 비율은 70이고(2023년 기준), 현재 비트코인의 저량 대 유량 비율은 121이다. 저량 대 유량 비율에 역수를 취하면 생산자들이 매년 가져가는 구매력을 근사치로 알아낼 수 있다. 원화나 달러 같은 현금은 매년 전체 사람들이 저축한 구매력의 10-30분의 1을 중앙은행과 정부가 가져가며, 금은 금광 기업들이 70분의 1을 가져가고, 비트코인은 채굴자들이 121분의 1을 가져간다. 비트코인은 반감기마다 새롭게 채굴되는 비트코인이 반으로 줄어들어 유량이 점

점 0에 수렴한다. 시간이 지나 비트코인의 저장 대 유량이 무한대가 되면 이의 역수는 $\frac{1}{\infty}$, 즉 0이 된다. 인류는 역사상 처음으로 누군가에게 구매력을 도둑 맞지 않고 온전히 보존할 수 있는 돈을 얻게 된 것이다.

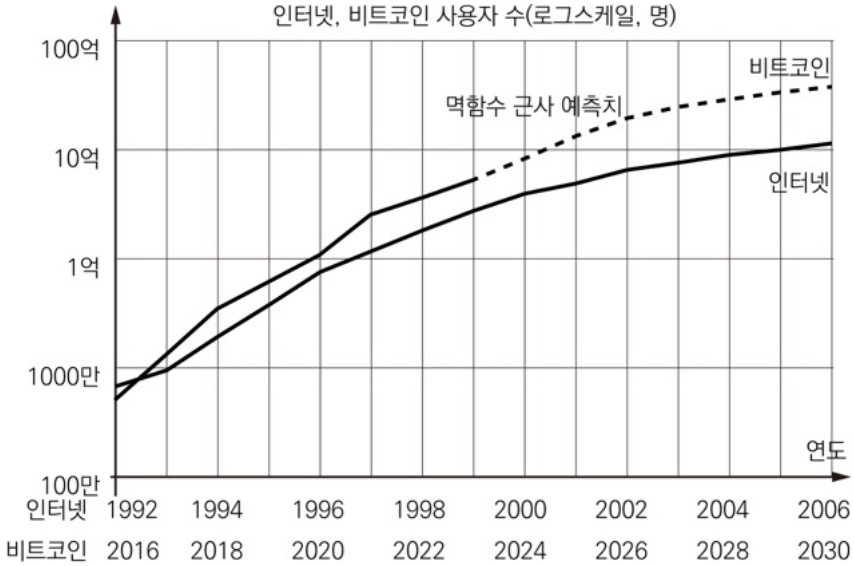
회계 단위

돈이 교환 매개와 구매력 보존 수단으로 기능한다면, 자연스럽게 회계 단위가 된다. 이렇게 되려면 그 돈을 쓰는 사람들이 많아져야 한다. 그래야 그 돈을 기반으로 상품 가격을 계산하는 사람들이 많아지고, 그러면 상품 간의 상대적인 가치를 추정할 수 있게 되기 때문이다.

사람들이 건전한 돈을 기준 단위로 쓰려면 네트워크 효과가 매우 중요하다. 점점 더 많은 사람들이 비트코인을 채택할수록 남은 사람들이 비트코인을 채택하는 속도가 가속화된다. 이를 '네트워크 효과'라 한다. 비트코인과 인터넷 채택률의 그래프를 보면 매우 비슷한 것을 알 수 있다. 심지어 비트코인의 채택 속도가 인터넷의 채택 속도보다 빠르다. 인터넷 창시자 중 한 명인 메트칼프가 이론화한 메트칼프의 법칙(Metcalfe's law)에 의하면 네트워크의 가치는 참여자 수의 제곱에 비례한다. 따라서 비트코인을 채택하는 사용자 수가 많아질수록 비트코인 네트워크의 가치는 급격히 증가하게 된다. 비트코인을 채택하는 사람이 늘어날수록 비트코인으로 가격을 책정하는 사례가 늘어나고, 비트코인으로 부를 계산하는 사고방식이 확산되며, 비트코인 기반 경제가 자연스럽게 형성된다.

만약 교환 매개 기능이나 구매력 보존 기능이 부족한 돈을 사람들에게 강제로 가격 단위로 쓰게 한다면 어떻게 될까? 원화로 측정한 자장면의 가격이 50년 전 138원에서 2025년 7,500원까지 올라온 사례를 다

시 생각해 보자. 이런 돈으로 상품 가격을 표시했다간 자장면의 가치가 50배가 올랐다는 착각을 하게 된다. 가격은 사람들이 어떤 행동을 할지 결정하게 하는 아주 중요한 정보인데, 화폐가 잘못되어 있으면 이러한 정보가 지속적으로 왜곡된다.



반면 개인이 비트코인을 채택하면 시간에 대한 사고방식이 근본적으로 바뀐다. 현재의 만족을 미래의 만족보다 얼마나 선호하는지를 나타내는 개념이 시간 선호(time preference)다. 현재의 행복과 만족을 더 중요시하면 시간 선호가 높은 것이고, 미래의 행복과 만족을 더 중요시하면 시간 선호가 낮은 것이다. 구매력이 지속적으로 하락하는 법정 화폐는 개인들이 저축을 통해 미래를 대비하기보다는 당장의 소비를 하도록 장려하며, 이 때문에 사람들은 점점 자신의 미래를 타인이나 국가에 맡기게 된다. 따라서 개인들의 시간 선호는 극단적으로 높아진다. 반면 비트코인을 채택하면 삶을 더 긴 관점에서 바라보고, 더 신중하게 소비하고 투

자할 수 있게 된다. 자신의 구매력을 온전히 보존할 수 있기 때문이다. 즉 시간 선호도가 낮아져 균형에 도달하고 미래 지향적 사고를 할 수 있게 한다.

비트코인은 많은 사람들이 사용할수록 강화되는 구조적 특성을 가지고 있다. 이 점이 법정 화폐와 가장 근본적으로 다른 부분이다. 달라나 원화는 정부의 강제력으로 사용되지만, 비트코인은 네트워크 효과로 가치를 확장해 간다. 그리고 그것이 옳다.

비트코인의 레이어 구조

비트코인은 하나의 레이어(층)로만 이뤄져 있지 않다. 비트코인은 기본적으로 제1레이어(온-체인)와 제2레이어(라이트닝 네트워크 등의 오프-체인)로 이루어져 있다.

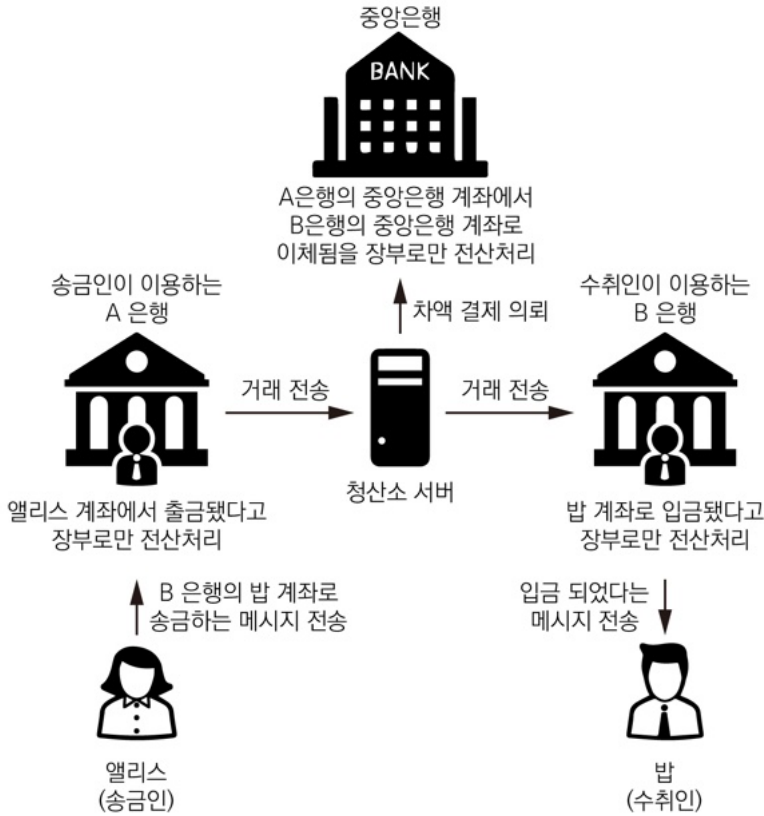
제1레이어는 모든 거래를 블록에 직접 기록하며, 전 세계 어디서나 검증 가능한 최종 정산 시스템이다. 온-체인 거래가 확정되려면 거래가 블록에 실려 채굴이 되어야 하는데, 적절한 수수료를 지불하는 거래라면 거래가 확정되는 데 평균적으로 10분이 걸린다. 이를 매우 느리다고 생각하면 안 된다.

일반적으로 우리가 사용하는 카드 결제 시스템을 생각해 보자. 상점에서 카드를 긁으면 결제는 '완료'된 것처럼 보인다. 그러나 정산 관점에서는 그렇지 않다. 먼저 상점의 포스기가 고객의 카드 정보를 읽는다. 그러면 결제대행사 PG가 카드사 네트워크에 승인을 요청한다. 카드사는 카드 상태(한도, 잔고, 체납, 거래 정지 여부 등)를 보고 승인 또는 거절 메시지를 PG사로 전달한다. PG사는 하루 동안 상점에서 발생한 이러한 여러 거래들을 모아 카드사에 정산 요청을 보낸다. 카드사는 일

반적으로 하루 단위로 가맹점 결제 내역을 모아서 정산 처리한다. 보통 밤 12시-새벽 1시 정도에 하루 매출을 마감하고 이러한 정산 과정이 일어난다. 카드사는 자체 정산 시스템을 통해 수수료를 제외하고, 대금을 조정한다. 상점은 2-3일 뒤에야 대금을 지급받는다.

은행 송금도 마찬가지다. 만약 앨리스가 A 은행 계좌에서 밥의 B 은행 계좌로 돈을 송금했다고 해보자. 그러면 A 은행은 앨리스에서 돈이 출금되었다고 장부로만 전산 처리한다. B 은행도 밥 계좌로 입금되었다고 장부로만 전산 처리한다. 그러면 A 은행이 B 은행에 돈을 줘야 한다. 이는 중앙은행의 청산소 서버에서 이뤄진다. 청산소 서버는 하루 동안 일어난 은행 간의 거래들을 모아 최종 정산을 한다. 예를 들면 A 은행의 중앙은행 계좌에서 B 은행의 중앙은행 계좌로 돈이 이체되었음을 장부로만 전산 처리하는 것이다. 당연히 이런 정산도 하루마다 밤 12시-새벽 1시 정도에 일어난다. 중앙은행의 청산소 서버가 제1레이어라면, 앨리스나 밥이 사용하는 A 은행, B 은행의 장부 서버들은 제2레이어와 같은 것이다.

기존 금융 시스템의 정산이 하루 단위로 일어나고 최종 정산이 2-3일 뒤에 일어나는 것과 대조해 보면, 비트코인의 온-체인에서 일어나는 정산은 매우 빠르다는 것을 알 수 있다. '정산'은 되돌릴 수 없어야 하는데, 비트코인은 보통 6컨펌이 되면 더 이상 되돌릴 수 없는 거래로 여겨진다(거래가 포함된 블록 위에 5개의 블록이 더 쌓이는 것을 말한다). 만약 블록 채굴이 너무 빠르게 이뤄지면 분기가 발생할 수 있어 '최종성'이 오히려 나빠지게 된다.



제2레이어인 라이트닝 네트워크에서 일어나는 결제를 보면 그 어떤 거래 수단보다 매우 빠르고 수수료가 저렴한 것을 알 수 있다. 라이트닝 네트워크는 비트코인 블록체인 위에 구축된 제2레이어로, 빠르고 수수료가 저렴한 거래를 가능하게 한다. 라이트닝 네트워크에서는 양 당사자가 결제 채널을 열어 서로 자유롭게 거래를 하고 이를 오프-체인에 서만 갖고 있다. 그러다가 필요할 때가 되면 그 최종 결과를 온-체인에 기록한다. 이 때문에 거래 수수료는 거의 0에 가까워진다. 비자VISA는 이론적으로 1초에 최대 약 65,000개의 거래를 처리할 수 있고, 마스

터카드 MasterCard는 1초에 최대 약 5,000개의 거래를 처리할 수 있다. 라이트닝 네트워크에서는 1초에 수백만~수십억 개의 거래를 처리할 수 있다. 채널이 많아지면 이론적으로 무한히 늘어나는 것도 가능하다. 비트코인은 일상적인 규모에서도 완전한 교환 매개체로 기능할 수 있다.

라이트닝 네트워크를 사용하는 방법

라이트닝 네트워크를 사용하는 데에는 크게 두 가지 방법이 있다. 첫째는 자신이 직접 라이트닝 노드를 운영하며 채널을 스스로 개설하고 관리하는 방법이다. 완전한 금융 주권을 지킬 수 있지만 기술에 대한 이해와 세심한 유동성 관리가 필요하다.

둘째는 라이트닝 수탁 서비스를 이용하는 방법이다. 라이트닝 지원 지갑 앱—월렛 오브 사토시, 블링크, 스피드 등—을 사용하면 채널 관리에 대한 지식 없이도 쉽게 라이트닝 네트워크를 사용할 수 있다. 그러나 이것은 거래소와 같은 수탁 서비스이므로 신뢰가 필요하며, 소액 이용에 적합하다.

라이트닝 지갑은 노드를 운영하든, 수탁 서비스를 이용하든 기본적으로 핫월렛이다. 애초에 라이트닝 네트워크는 소액 결제를 위한 기술이다. 따라서 일상적으로 결제에 사용할 소액만 라이트닝 지갑에 넣고 다니는 것이 좋다. 부동산 구매처럼 큰 금액을 결제할 때는 온-체인 결제를 이용하면 된다.

비트코인 결제 체험이 중요한 이유

비트코인은 단순한 투자 자산이 아니라, '돈'이다. 따라서 비트코인의 진정한 힘은 비트코인을 돈으로 체험할 때 느껴진다. 비트코인으로 직

접 커피를 사 마시는 것, 라이트닝 네트워크를 이용해 친구에게 즉시 송금하는 것, 해외에 검열 없이 돈을 보내는 것 등의 경험 말이다. 이런 경험들은 단순한 거래 이상의 의미를 갖는다. 자기 자산을 스스로 소유하고 검열 없이 자유롭게 교환하며 경제활동을 하는 경험은 비트코인이 자유의 돈이라는 사실을 몸으로 이해하게 해준다.

그리고 이것이 당연시되는 사회가 '비트코인 스탠다드'다. 비트코인 스탠다드를 먼저 경험해 본 사람은 비트코인에 대한 이해가 남다를 것이다. 비트코인은 실제로 사용함으로써 그 가치를 깨달을 수 있는 진짜 돈이다.

| 라이트닝 수탁 지갑 이용 방법

라이트닝 수탁 지갑 설치

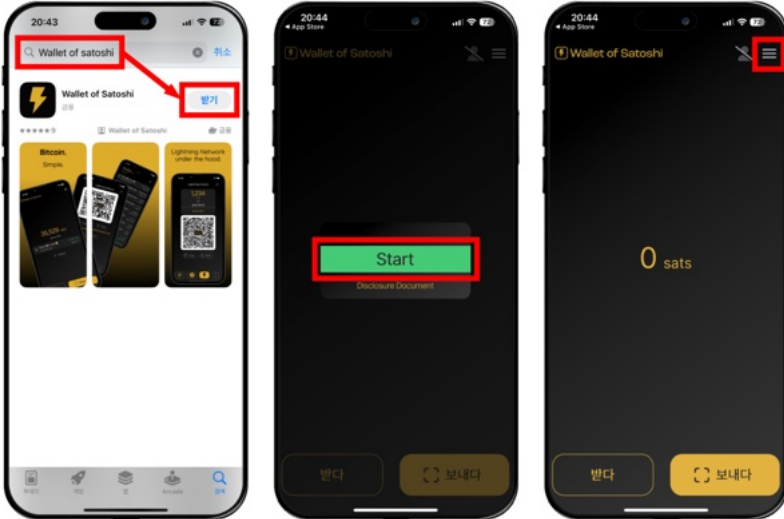
이번 장에서는 오프라인, 온라인에서 비트코인으로 결제하고 결제받기 위해 라이트닝 수탁 지갑을 설치하고 입금/출금/결제하는 방법을 알아볼 것이다. 수탁 지갑을 이용하지 않고 직접 라이트닝 노드를 운영하는 방법은 4부에서 알아볼 것이다.

라이트닝 수탁 서비스에는 월렛 오브 사토시, 블링크, 스피드 등이 있다. 이번에는 월렛 오브 사토시(이하 월오사) 앱을 통해 실습할 것이다. 월오사는 이메일 인증만 요구하지만 출금 시 금액의 0.3%를 월오사 앱에 남겨 놓아야 한다는 정책이 있고, 온-체인 입출금 수수료가 1.95%로 높은 편이라는 단점이 있다. 0.3%를 남겨 놓는 것은 여러 번 반복해서 출금하여 0-1 sat만 남기고 다 뺄 수 있고, 온-체인 입출금 수수료는 볼츠 등의 라이트닝-온-체인 스와프 서비스를 이용해 0.1-0.5%로 낮출 수 있다. 이번 장에서 이 방법도 알아볼 것이다.

월오사가 아닌 다른 수탁 라이트닝 앱들의 사용 방법도 크게 다르지 않다. 다만 과도한 신원 인증을 요구하는 앱들은 사용을 할지 다시 한번 고려해 보자.

이제 월오사 앱을 설치해 보자. 앱스토어 또는 구글 플레이스토어에서 'Wallet of Satoshi' 앱을 검색하고 다운로드한다.

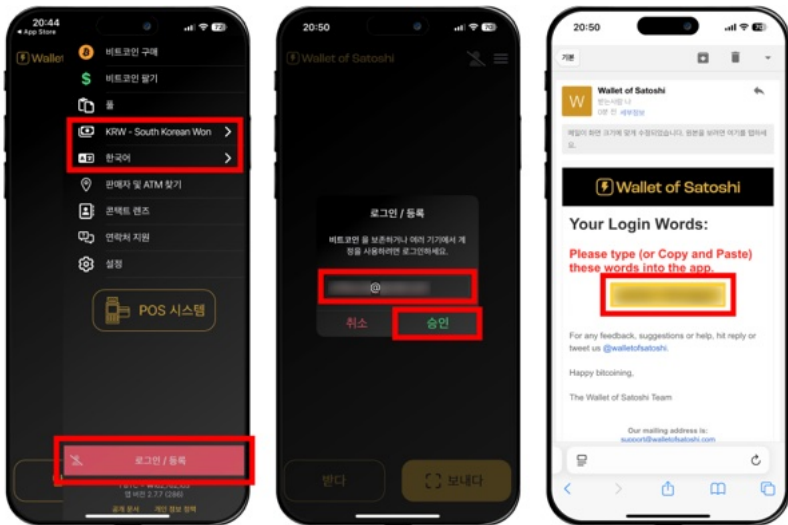
[Start]를 누르고 오른쪽 위 메뉴 버튼을 누른다.



통화를 한국 원화인 'KRW'로 바꾸고(KPW-북한 원과 헷갈리지 않도록 주의), 언어는 '한국어'로 바꿔 놓자.

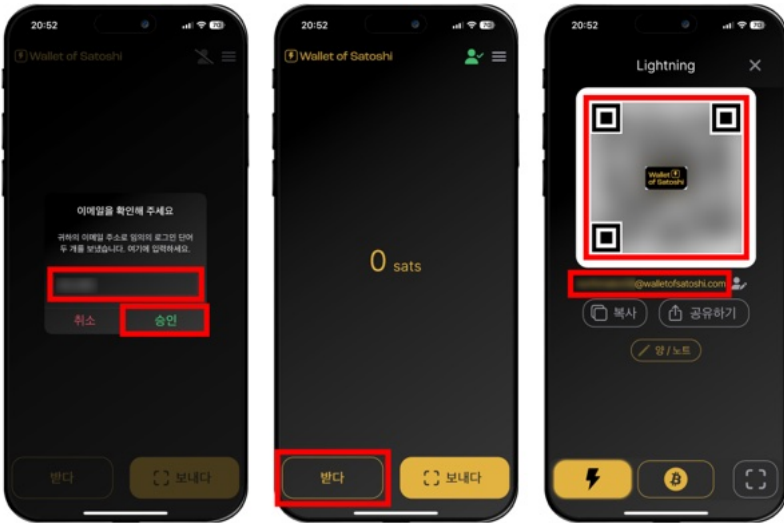
이제 이메일 인증을 할 것이다. 여러 기기에서 한 지갑을 이용하려고 할 때, 혹은 앱을 삭제하거나 스마트폰을 바꾸는 등의 이유로 지갑에 들어있는 금액 복구가 필요할 때에 대비하여 이메일 인증을 해둘 수 있다.

[로그인/등록]을 누르고 등록할 이메일을 입력한 후 [승인]을 누른다. 그러면 입력한 이메일로 두 영단어가 온다. 이 영단어를 복사하거나 잘 기억해 놓는다.



월오사 앱으로 돌아오면 방금 봤던 두 영단어를 입력하는 창이 나올 것이다. 두 단어를 입력하고 [승인]을 누른다.

이메일 연결이 되었다면 이제 메인 화면에서 [받다]를 눌러보자. 눌렀을 때 나오는 화면의 주소가 비트코인을 송금받을 라이트닝 주소다. 혹은 QR 코드로 송금받을 수도 있다. 주의할 점은 이 주소 혹은 이 QR 코드는 라이트닝 송금만을 지원한다는 것이다. 여기로 온-체인 송금은 되지 않는다.




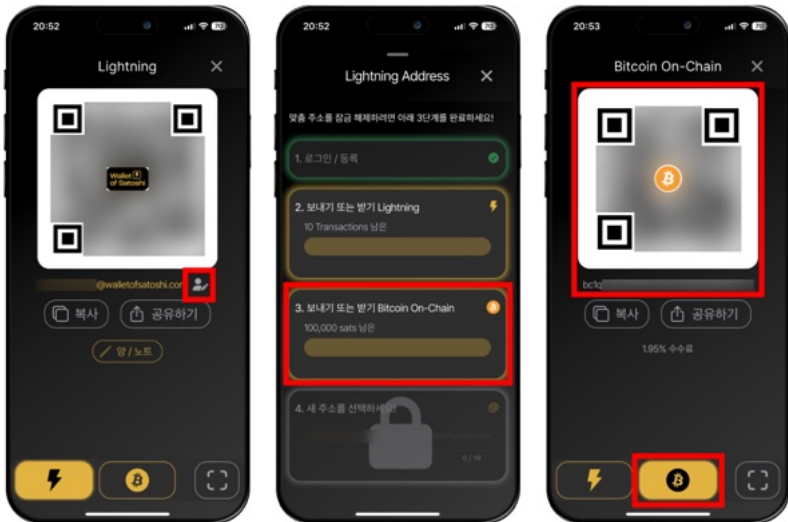
커스텀 라이트닝 주소 발급

월오사에서 [받기]를 눌렀을 때 나오는 라이트닝 주소는 랜덤으로 정해진 주소다. 이것을 내가 원하는 주소로 바꾸는 것을 ‘커스텀 라이트닝 주소’를 받는다고 한다. 월오사에서 커스텀 주소를 받기 위해서는 몇 가지 기준을 충족시켜야 한다.

이 절을 진행하려면 11만 sats가 필요하며, 약 3천 sats 정도가 소비될 수 있다. 이는 월오사에 입금 수수료로 내는 금액이다. 만약 커스텀 라이트닝 주소가 필요 없고, 이미 발급되어 있는 라이트닝 주소를 사용해도 괜찮다면 이 절을 건너뛰어도 좋다.

[받다]를 눌러서 나오는 화면에서 라이트닝 주소 옆에 있는 사람 모양의 체크 버튼을 누른다. 그러면 커스텀 주소를 발급받기 위한 조건이 나온다. 조건은 라이트닝으로 10번 보내거나 받기, 그리고 온-체인으로 10만 sats 이상 입출금을 하는 것이다. 먼저 온-체인으로 11만 sats를 입금해 보겠다.

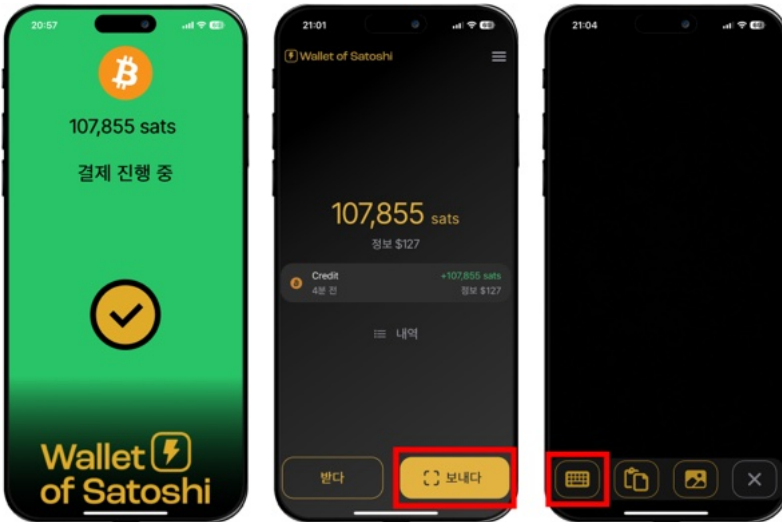
[3. 보내기 또는 받기 Bitcoin On-Chain]을 누른다. 아래에서 비트코인의  로고가 선택되어 있다면 온-체인으로 받을 주소가 뜨고 있는 것이다. QR 코드 혹은 그 아래에 보이는 'bc1q'로 시작하는 주소에 비트코인을 11만 sats를 보내보자.



거래가 블록에 담기고 아직 컨펌되기 전이라면(거래가 담긴 블록이 채굴되기 전이라면), '결제 진행 중'이라는 화면이 뜬다.

시간이 지나 거래가 담긴 블록이 채굴되어 입금이 잘 되었다면 다른 조건을 만족시키기 위해 라이트닝으로 10번 송금하면 된다. 여기서는 다른 곳으로 1 sat씩 10번 보낼 것이다.

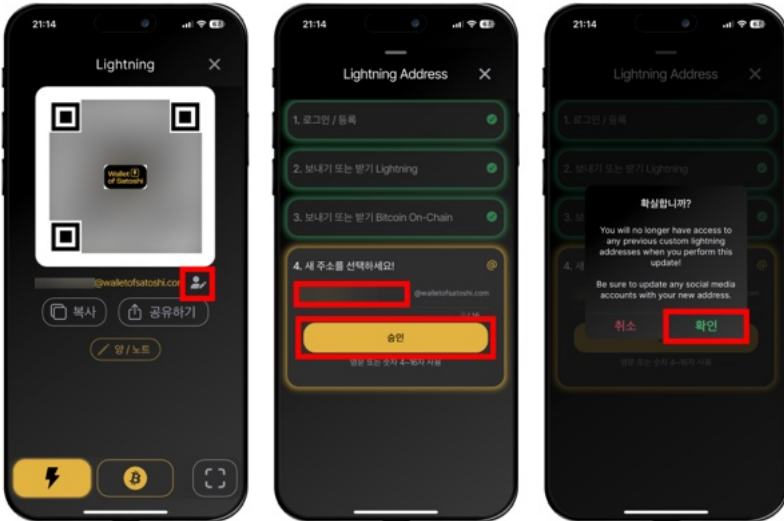
[보내다]를 누르고, 카메라 권한을 묻는다면 허용을 누른다. 카메라 화면이 나오면 아래에 있는 키보드 모양의 버튼을 누른다. 이 버튼은 카메라로 QR 코드를 인식하지 않고 직접 라이트닝 주소를 입력하겠다는 뜻이다.



1 sat를 보낼 라이트닝 주소를 입력하고, 화살표 버튼을 누른다. 1 sat를 입력하고, [보내다]를 누르면 완료된다.



1 sat를 어딘가로 보내는 과정을 10번 반복하면 커스텀 주소를 발급 받을 수 있게 된다. [받기]를 눌렀을 때 나오는 화면에서 '새 주소를 선택하세요!' 밑에 있는 주소 입력창에 자신이 사용할 주소를 입력하고, [승인]을 누른다. 이전에 랜덤으로 주어졌던 라이트닝 주소는 더 이상 사용할 수 없게 된다는 안내문이 나온다. [확인]을 누른다.



새 라이트닝 주소가 잘 발급된 것을 볼 수 있다. 이제 다른 사람에게 비트코인을 받을 때 이 라이트닝 주소를 알려주면 된다.



온-체인으로 라이트닝 수탁 지갑에 비트코인 입금하기

월오사에 입금을 할 때는 [받기] 버튼을 누르면 나오는 라이트닝 주소나 온-체인 주소로 입금을 하면 된다. 그러나 온-체인 입출금 시 채굴자에게 지불하는 온-체인 수수료 외에 월오사가 가져가는 수수료가 1.95%다. 이를 절약하는 방법이 수수료율이 상대적으로 저렴한 볼츠 등의 스와프 서비스를 이용하는 것이다. 볼츠는 온-체인 → 라이트닝 스와프 수수료가 0.1%이고, 라이트닝 → 온-체인 스와프 수수료가 0.5%이다.

볼츠를 이용해 개인 지갑에 있는 비트코인을 월오사로 옮겨 보자. 먼저 볼츠 웹사이트에 접속한다.

<https://boltz.exchange/>

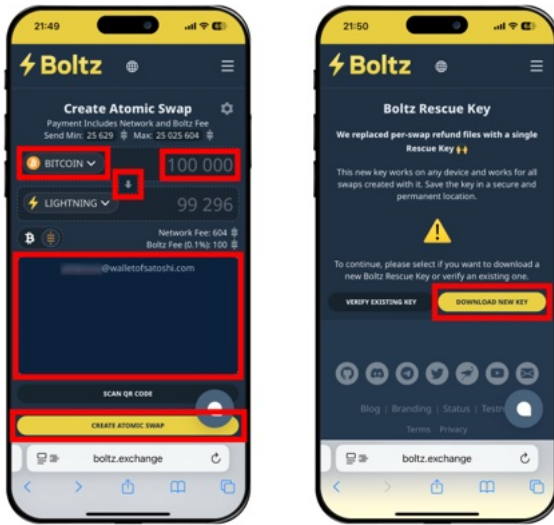


먼저 화살표를 눌러 'BITCOIN'이 위로 오게 만든다. 개인 지갑에서 보내는 비트코인은 기본적으로 온-체인 송금이다. 우리는 개인 지갑에서 비트코인을 보낼 것이므로 온-체인 비트코인을 라이트닝 비트코인으로 스와프하는 것이다.

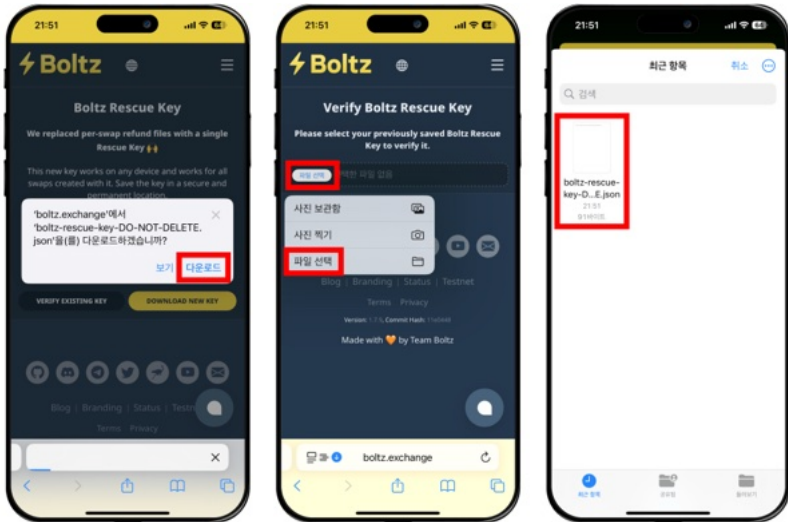
'BITCOIN'이 위로 왔으면 'BITCOIN' 옆에 입금할 금액을 입력한다. 필자는 10만 sats를 입금할 것이다. 바로 그 아래에 온-체인 수수료(비트코인 네트워크 상황에 따라 변동)와 볼츠가 가져가는 수수료 0.1%를 제외한 금액(사진에서는 99,296)이 표시된다. 아래 표시되는 이 금액을 정확히 봐야 한다.

그 아래에는 '~@walletofsatoshi.com' 등의 비트코인을 받을 라이트닝 주소나 라이트닝 인보이스를 입력해야 한다. 인보이스는 보통 받을 금액이 입력되어 있고, 유효 시간이 있으며, 일회용이다. 당연히 인보이스보다 라이트닝 주소를 입력하는 것이 편하다. (인보이스를 발급하는 방법은 월오사 앱에서 [받다] → [양/노트]를 누르고 금액을 입력하면 된다.) 지금은 라이트닝 주소를 입력하고 진행해 보겠다. 오타에 주의하여 입력하자.

그다음에는 키를 다운로드한다. 만약 채굴이 너무 늦게 되는 등의 이유로 인보이스가 만료되면 자금을 돌려받아야 하는데 그때 메뉴의 [Refund]를 눌러 키를 선택하면 비트코인을 돌려받을 수 있다. [DOWNLOAD NEW KEY]를 눌러 키를 다운로드한다.

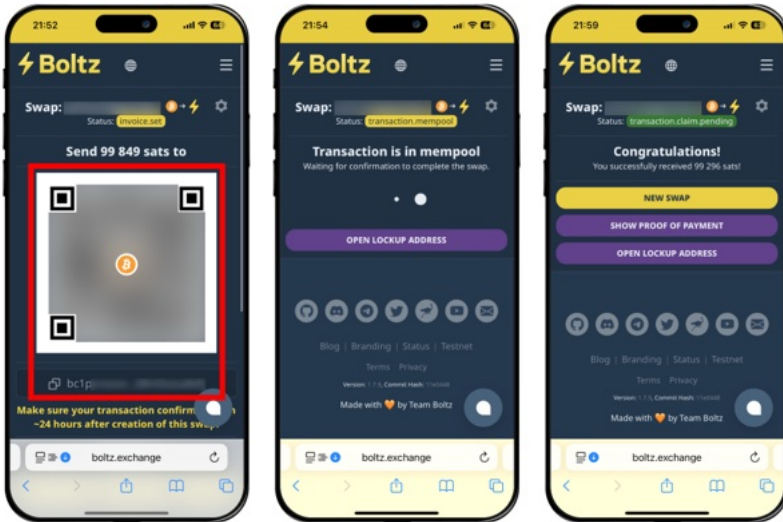


키를 다운로드했으면 [파일 선택]에서 방금 다운로드한 키 파일을 선택한다.



그러면 온-체인으로 입금할 주소가 나온다. QR 코드를 스캔하거나 아래에 나와 있는 주소로 개인 지갑에서 정확한 금액(사진상에서 99,849 sats)을 송금한다.

볼츠가 거래를 인식하면 거래가 뎀풀에 담겼다는 창이 나온다. 거래가 담긴 블록이 채굴될 때까지 기다리면 거래가 컨펌된다. 그러면 수수료를 제외한 비트코인이 라이트닝 주소로 잘 송금되었다고 축하한다는 안내 창('Congratulations!')이 나온다.



월오사 앱으로 들어가 보면 비트코인이 잘 입금된 것을 확인할 수 있다.



라이트닝 수탁 지갑에서 온-체인으로 비트코인 출금하기

월오사에서 온-체인으로 비트코인을 출금해 개인 지갑으로 옮기는 방법은 '1부. 셀프 커스터디 가이드'에서 보았던 방법과 비슷하다.

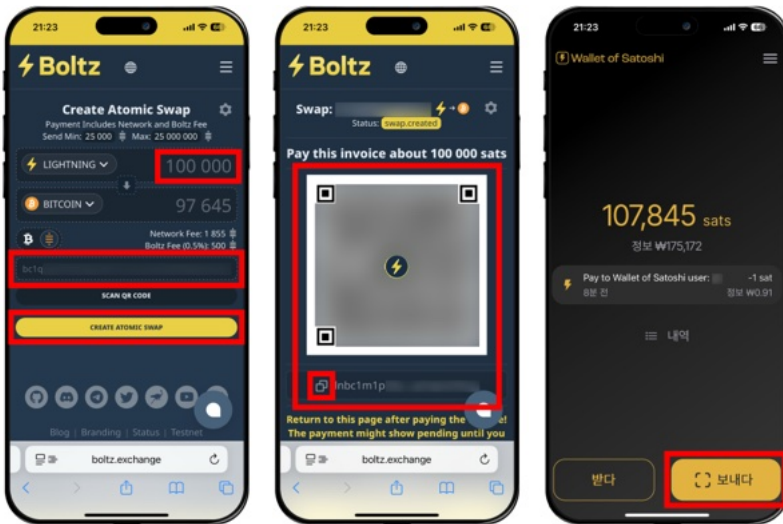
먼저 볼츠 웹사이트에 접속한다.

<https://boltz.exchange/>

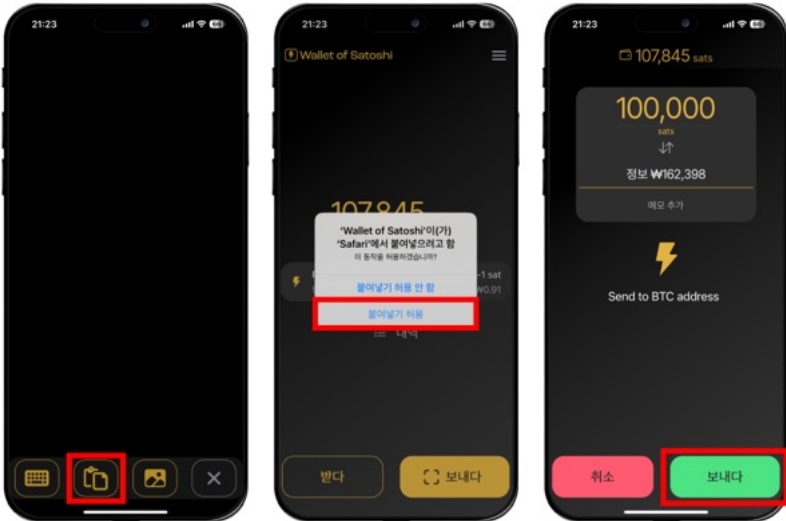


‘LIGHTNING’ 옆에 출금할 비트코인 금액을 적고 아래에 비트코인을 받을 주소(‘bc1q~’ 등)를 입력한다. 이때 반드시 오차가 없는지 주의하라. 잘못된 주소로 비트코인을 보내면 비트코인을 영영 못 찾을 수도 있다. 물론 이를 방지하기 위해 비트코인의 주소 체계에는 체크섬이 포함되어 있지만, 그래도 꼭 확인하자. 그다음에 [CREATE ATOMIC SWAP]을 누른다.

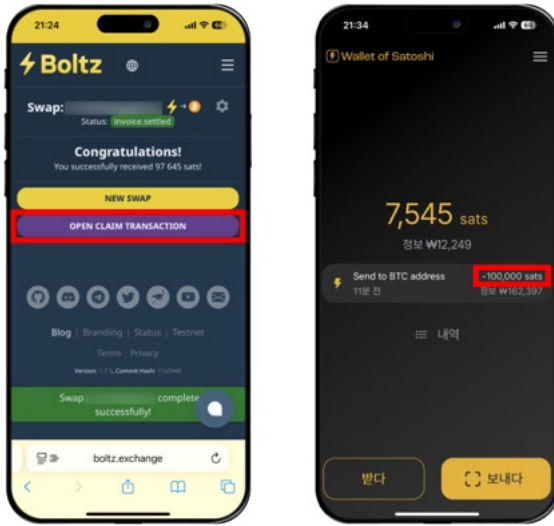
그러면 인보이스가 나온다. QR 코드 아래 인보이스 왼쪽에 있는 문서 모양의 복사 버튼을 누른다. 그다음 월오사 앱으로 들어가 [보내다]를 누른다.



카메라 화면이 나오면 아래 두 번째 문서 모양의 버튼을 누른다. 이 버튼은 클립보드에서 붙여넣는 버튼이다. [붙여넣기 허용]을 누르고 [보내다]를 누른다.

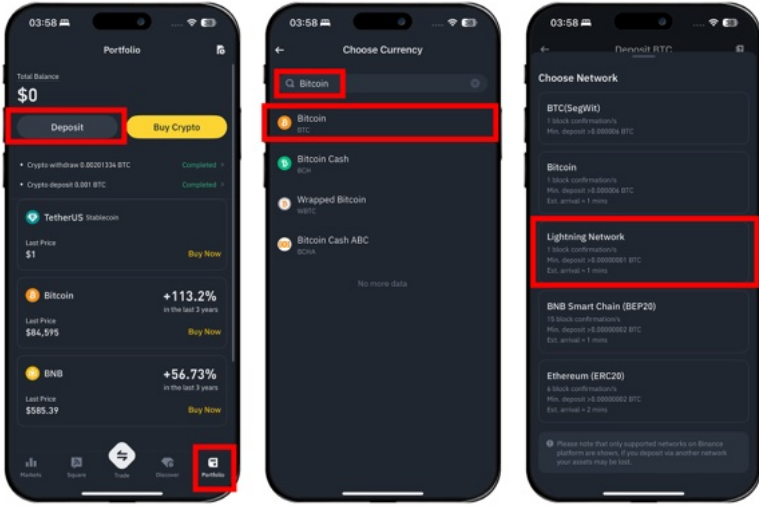


송금하면 개인 지갑으로 보내는 온-체인 거래가 송금되었다는 창이 나올 것이다. 거래가 컨펌될 때까지 기다려야 한다. [OPEN CLAIM TRANSACTION]을 누르면 멤폴 웹사이트에서 해당 거래의 상태를 확인할 수 있다. 월오사에서는 출금이 완료된 것을 확인할 수 있다.

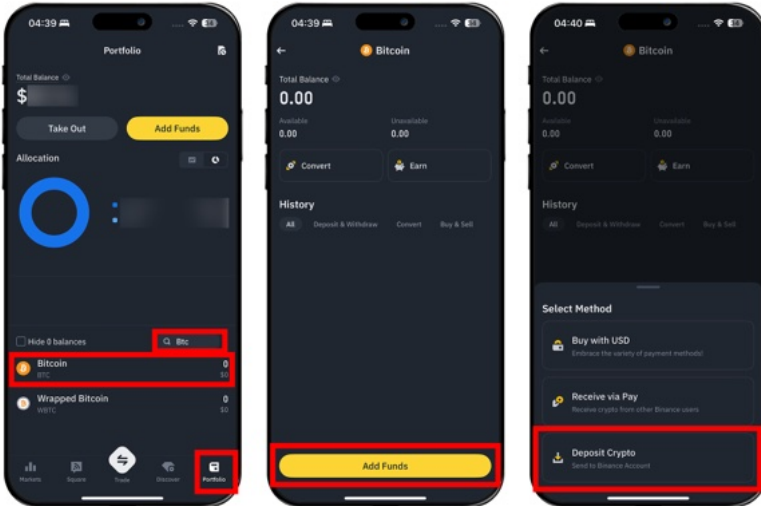


원화 환전을 위해 라이트닝 수탁 지갑에서 해외 거래소로 비트코인 송금하기 비트코인 결제 매장 등을 운영하면 월렛 오브 사토시와 같은 라이트닝 수탁 지갑에 있는 비트코인을 원화로 환전해야 할 일이 있을 것이다. '1부. 셀프 커스터디 가이드'에서 봤듯이 한국은 트래블룰 때문에 한국 거래소로 비트코인을 바로 입금할 수 없고, 해외 거래소를 거쳐야 한다. 라이트닝 수탁 지갑에서 바이낸스 등의 해외 거래소로 비트코인을 보내는 방법을 알아보자.

바이낸스 앱 [Portfolio] 탭에서 [Deposit]을 누르고, 네트워크에서 [라이트닝 네트워크(Lightning Network)]를 선택한다.

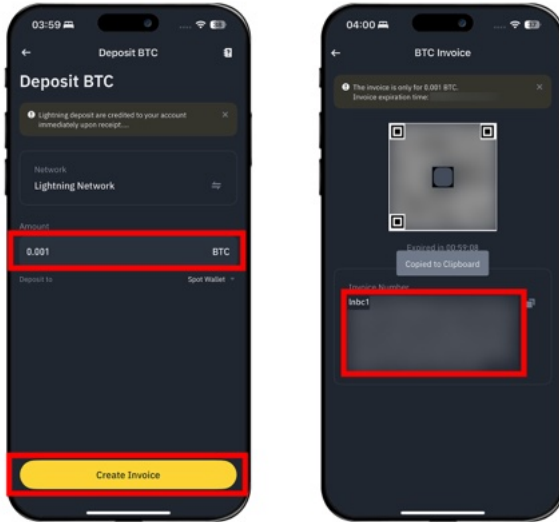


만약 이미 비트코인이나 테더 등이 있는 경우 [Deposit]이 바로 안 보일 수도 있다. 이때는 아래처럼 [Bitcoin]으로 들어간 다음 [Add Funds] → [Deposit Crypto]로 들어가면 된다. 네트워크를 선택하는 창이 나오면 [라이트닝 네트워크(Lightning Network)]를 선택한다.



여기에 원화로 환전하고 싶은 비트코인 양을 입력한다. 필자는 이번
에 10만 sats, 즉 0.001 BTC를 환전해 보도록 하겠다.

금액을 입력하고 [Create Invoice]를 누르면 인보이스가 생성된다.
인보이스는 라이트닝 네트워크에서 계좌번호와 비슷한 역할을 한다고
생각하면 된다. 대신에 한 번밖에 못 쓰고, 그때그때 새로 발급된다. 인
보이스 글자를 한 번 누르면 자동으로 복사가 된다.

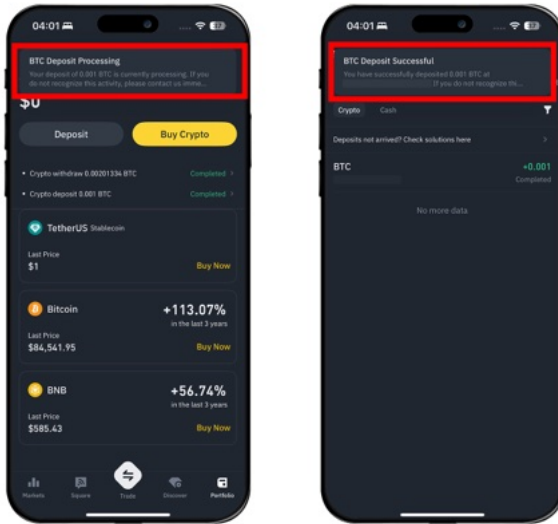


이제 월렛 오브 사토시 등의 라이트닝 수탁 지갑에서 보내기를 누르고 인보이스를 붙여넣어야 한다.

월렛 오브 사토시 앱에서 [보내다] → 아래 키보드 모양 버튼 → 인보이스 붙여넣기 → 화살표 버튼 → [보내다]를 누른다.



이렇게 하고 잠시 기다리면 해외 거래소로 송금이 될 것이다. 필자는 1분 정도 기다리니 입금이 되었다는 알림이 상단에 나타났다.



이후 해외 거래소에서 국내 거래소로 옮겨 원화로 출금하는 방법은 '1부. 셀프 커스터디 가이드'의 '해외 거래소에서 국내 거래소로 전송' 절을 참고하라.

| 오프라인 매장에서 라이트닝 결제하기

비트코인으로 커피 사 마시기

오프라인에서 비트코인 결제 매장을 찾아가 보자. 먼저 비트코인 결제 매장이 주변에 있는지 찾아보자. btcmap.kr이나 btcmap.org에 들어가면 주변에 비트코인 결제 매장이 있는지 찾아볼 수 있다.



<http://btcmap.kr>



<https://btcmap.org/>

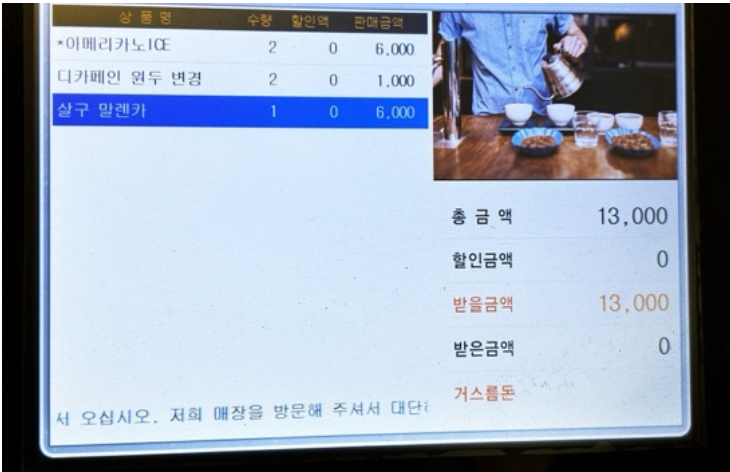


어디를 갈지 정했다면, 먼저 그 매장에 전화해서 비트코인 결제가 되는지 물어보자. 해당 시점에도 비트코인 결제를 받는지 확인하기 위해서다.

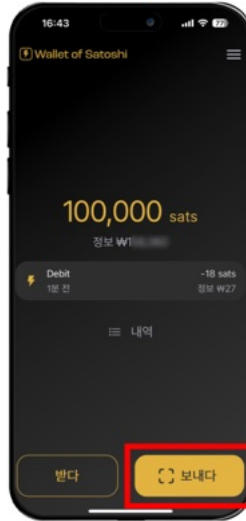
필자는 비트코인으로 커피를 마시기 위해 비트코인 결제가 되는 카페를 방문해 보았다. 카페 문 앞에 'bitcoin Accepted Here'라고 쓰인 스티커가 붙어있는 것을 볼 수 있다.



커피 두 잔과 케이크 하나를 시켰다. 금액을 확인한다.



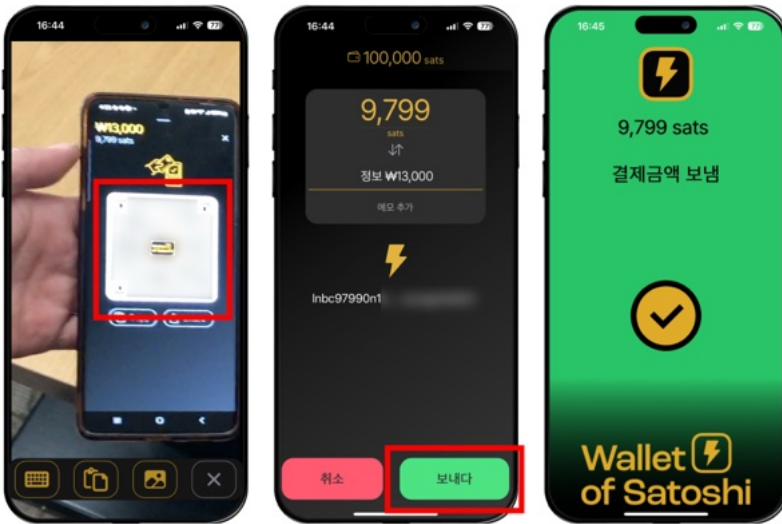
월오사에서 [보내다]를 누른다.



사장님이 QR 코드를 보여줄 것이다. 그 QR 코드를 스캔한다.



QR 코드를 스캔하고 [보내다]를 누르면 번개처럼 빠르게 결제가 완료된다.



이제 시원한 커피를 마시고 맛있는 케이크를 먹으면 된다.



| 온라인 매장에서 라이트닝 결제하기

비트코인으로 물건 구매하고 택배 받기

이번에는 온라인 스토어에서 비트코인으로 결제하는 방법을 알아보자. 해외 웹사이트에서 비트코인 관련 물품을 구매할 때 특히 유용하다. 비트코인은 국경이 없기 때문이다. 대한민국의 온라인 비트코인 결제 매장은 대표적으로 ‘사토시마켓’이나 ‘사토샵’이 있다.

필자가 집필했던 책을 ‘필레우시스 스토어’에서 구매해 보도록 하겠다. 먼저 웹사이트에 접속한다.

<https://store.phileucis.com/product/bk-btc-01-01/>



출 / 도서 / 비트코인 백서 해설



비트코인 백서 해설
★★★★☆ (6개의 고객 상품평)
21,000 Sats

상품 종류: 도서
책 제목: 비트코인 백서 해설
저자: 사토시 나카모토
번역, 해설: 필레온, 바우키스
출판사: 필레우시스
발행 정보: 1권(인쇄일 2025. 01. 09. / 발행일 2025. 02. 01.)
ISBN: 979-11-990974-0-7
도서 형태: 양장본 하드커버, 금장
페이지: 972p
크기: 신국판(내지: 152mm x 225mm, 표지: 164mm x 233mm, 두께: 56mm, 무게: 1450g)
문의: phileucis@gmail.com

1 장바구니 **지금 구매**

배송 받을 정보를 입력하고 [Proceed to BTCPay]를 누른다.

결제

청구 상세 내용

이름

가맹 입력도 가능합니다. 그러나 다른 가족 구성원이 오배송인줄 착각하는 경우가 있으니 주의하십시오. *

필라몬

이메일 주소

이 주소로 주문 정보 메일이 갑니다. 정확하게 입력해주세요. *

전화번호(선택 사항)

실물 배송인 경우 연락 가능한 번호를 정확하게 입력해주세요.

우편 번호 *

도로명 주소 *


상세 주소(선택 사항)

커피트나 공동주택인 경우 동, 호수를 제대로 입력해주세요.

주소를 제대로 입력하지 않아 발생하는 배송 사고에 대한 책임은 본인에게 있습니다.

고객님의 주문

상품	소계
비트코인 백서 해설 × 1	21,000 Sats
소계	21,000 Sats
배송	배송비 포함
총계	21,000 Sats

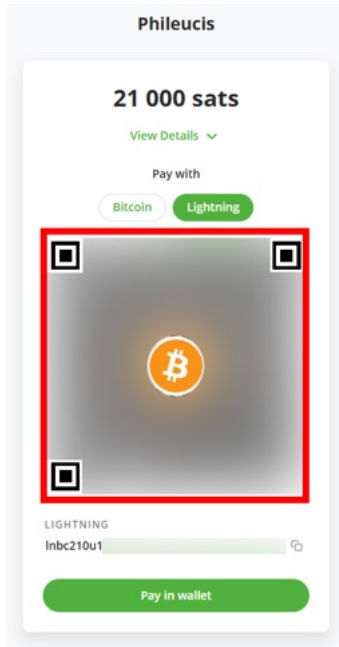
비트코인 라이트닝 또는 온체인 결제  BTCPAY

BTCPay 결제 페이지로 넘어갑니다.

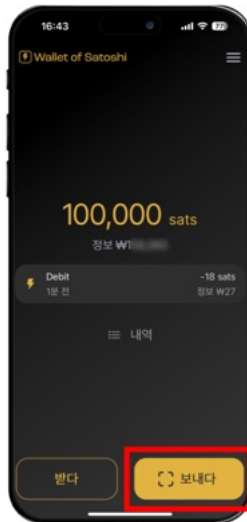
개인 데이터는 주문을 처리하고, 이 웹사이트 전체에서 사용자 환경을 지원하며, [개인정보 보호정책](#)에 설명한 기타 목적을 이행하는 데 사용됩니다.

[Proceed to BTCPay](#)

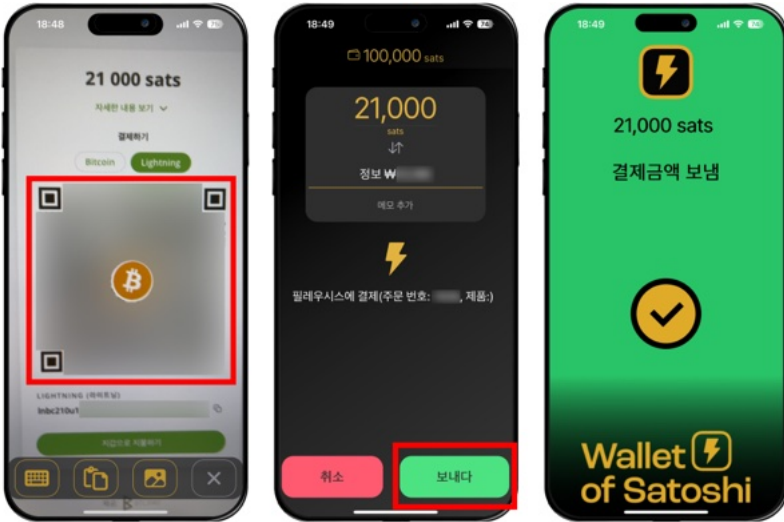
그러면 라이트닝 결제를 위한 QR 코드가 나오는 것을 볼 수 있다. 라이트닝 결제가 기본으로 설정되어 있지만, QR 코드 위에 있는 [Bitcoin]을 선택하면 라이트닝이 아니라 온-체인 송금으로 결제할 수도 있다. 하지만 온-체인 결제는 채굴자에게 지불하는 수수료가 있고 블록 컨펌을 기다려야 하므로 라이트닝으로 결제하는 것을 추천한다.



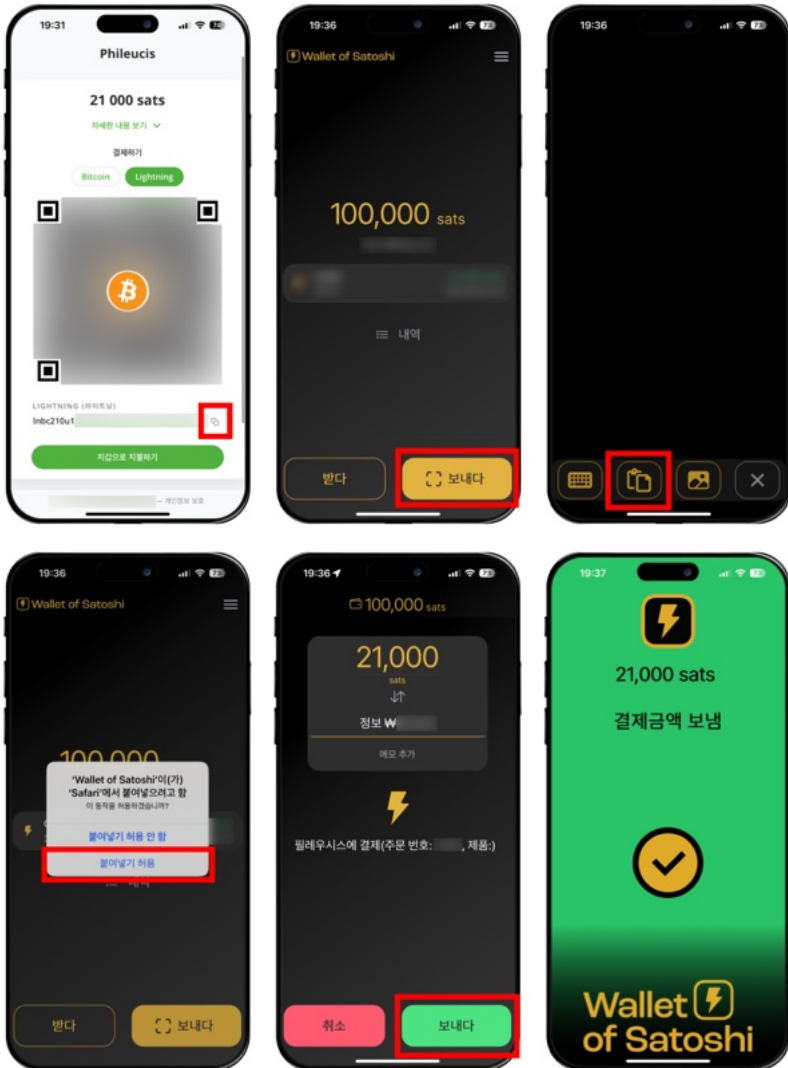
이제 월오사 앱에서 [보내다]를 누른다.



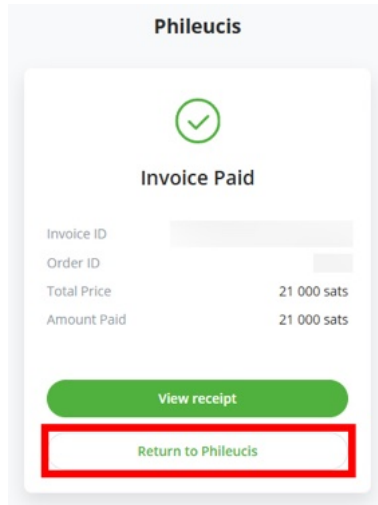
카메라 화면이 나오면 웹사이트에 나와 있는 QR 코드를 스캔한다.
[보내다]를 누르면 즉시 결제가 된다.



모바일에서 주문서를 작성하고 모바일에서 라이트닝으로 결제하는 경우, QR 코드 아래에 'lnbc'로 시작하는 라이트닝 인보이스를 복사한다. 그리고 월오사 앱에서 [보내다] → 하단 두 번째 문서 모양의 붙여넣기 버튼 → [붙여넣기 허용] → [보내다]를 누르면 즉시 결제가 된다.



웹사이트에서도 바로 반영이 되는 것을 볼 수 있다. [Return to Phileucis]를 눌러보자.



결제 정보가 나온다. 이로써 온라인 비트코인 결제 매장에서 비트코인으로 결제하는 방법을 알아보았다.

접수된 주문

감사합니다. 고객님의 주문이 접수되었습니다.

주문 번호: 날짜: **총계 21,000 Sats** 결제 방법: 비트코인 라이트닝 또는 온체인 결제

Payment Status

Payment processing

주문 상세 정보

상품	총계
비트코인 백서 해설 × 1	21,000 Sats
소계:	Sats21,000
배송:	배송비 포함
결제 방법:	비트코인 라이트닝 또는 온체인 결제
총계:	Sats21,000

| 1분 만에 비트코인 결제 매장 되기

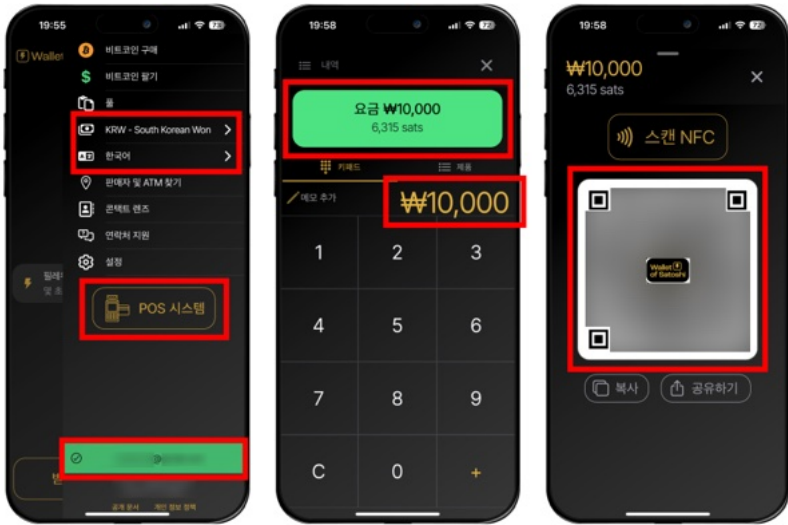
매장에서 라이트닝 결제받는 방법

‘월렛 오브 사토시’ 앱을 이용하여 비트코인으로 결제받는 방법을 알아보자. 매우 간단하다.

Wallet of Satoshi 앱(이하 월오사 앱)을 다운로드한다.

월오사 앱을 실행한다. 오른쪽 위 메뉴를 누르고 통화는 KRW로, 언어는 한국어로 설정되어 있는지, 이메일은 잘 연결되었는지 다시 한번 확인한다. 그다음 [POS 시스템] 버튼을 누른다.

금액을 입력하고 초록색 ‘요금’ 버튼을 누른다. 자동으로 원화 금액에 해당하는 비트코인 금액으로 표시된다. 그다음에 나오는 QR 코드를 고객에게 보여주면 끝이다.



고객이 사토시를 송금하면 다음과 같은 화면이 뜬다. 결제가 잘 되는 것을 확인할 수 있다.

