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

| 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.

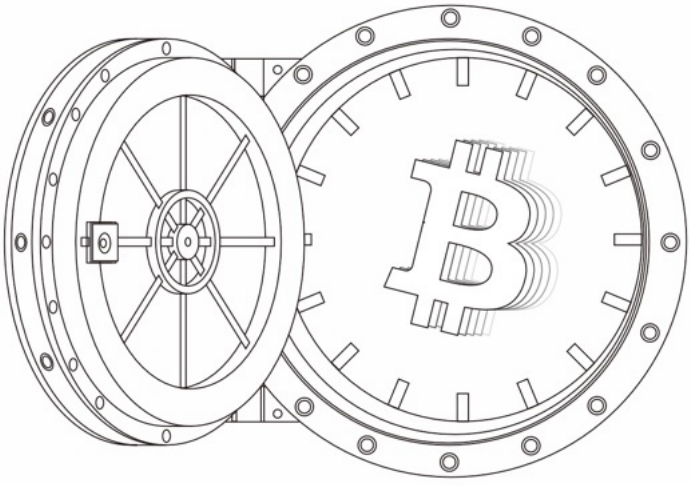
선언문 해시값: `45046C4A0858AD664122B30974353D46580D7F107A68CF761724A4E30170BA0D`
비트코인 메시지 서명: `H9gTJUOT1JIYQGVxsDd89AOTgiE1by7bdk4EDXf7arjFDg3gqP/wdqoRclSiwXwp/rNNSen3t/pxK2AFDDxmkjE=`

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

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

서문. 당신의 돈을 스스로 통제하라

내용 없는 사상은 공허하며, 개념 없는 직관은 맹목이다. (…)
지성은 아무것도 직관할 수 없으며, 감각기관은 아무것도 사유할 수 없다.
직관과 지성이 결합할 때만 인식이 성립된다.
—임마누엘 칸트, 『순수이성비판』

비트코인을 진정으로 이해하기 위해서는 단지 이론서 몇 권을 읽는 것만으로는 부족하다. 분산화, 검열 저항성, 고정된 공급량, 자발적 합의와 같은 비트코인의 철학들은 책 속에서 찾아볼 수도 있다. 그러나 그 진짜 의미는 지갑을 생성하고, 첫 사토시를 송금해 보고, 블록 컨펌을 기다려보고, 풀 노드를 운영해 블록과 거래를 독립적으로 검증하고, 단일한 장부를 보유하고 열람하며, 라이트닝 네트워크에서 비트코인으로 실물을 결제해 보는 과정에서 비로소 피부에 와닿는다.

임마누엘 칸트는 『순수이성비판』에서 내용 없는 사상은 공허하고, 개념 없는 직관은 맹목이라고 했다. 내용이란 직관들이 제공하는 감각적 요소로, 머리로만 생각하는 것이 아니라 실제로 우리가 경험하며 얻는 느낌들을 말한다. 사상은 생각의 산물이다. 따라서 이 말은 직관적 경험 없이 생각만 하는 것은 공허하다는 말이다.

비트코인도 마찬가지다. 아무리 분산화, 검열 저항 같은 개념의 원리와 철학을 공부해 봐도 직접 비트코인을 송금하거나 풀 노드를 운영해 비트코인 네트워크에 참여해 본 적이 없으면 그런 개념들은 공허하다.

경험 없이 혼자만의 상상에 갇혀 비트코인이 이렇게 되면 어떻고, 저렇게 되면 어떨지 생각하는 것들은 의미가 없다. 검증은 사유만으로 성립하지 않는다. 적어도 비트코인에서는 더욱 그렇다.

거꾸로 지식 없이 경험만 있는 것도 위험하다. 칸트가 개념 없는 직관이 맹목적이라고 말한 것처럼 말이다. 어떤 개인이 비트코인의 작동 원리나 정신에 대한 이해가 전혀 없이 비트코인을 모으기만 한다고 해보자. 이들의 경험의 폭은 매우 제한되고 비트코인에 대한 이해는 왜곡되기 쉽다. 비트코인은 사용자가 자신의 삶을 스스로 책임지고, 사용자에게 자유를 가져다줄 시작점이 될 수 있는 돈이다. 하지만 지식 없이 맹목적으로 비트코인을 경험하는 사람은 오히려 외부에 의존할 수밖에 없다. "국가나 은행, 기업, 정치인들이 비트코인을 채택해 줬으면 좋겠어.", "어서 제도권으로 들어가서 내가 가진 비트코인의 가격이 상승해 줬으면 좋겠어.", "비트코인 가격이 올라서 내가 일을 그만둘 수 있으면 좋겠어." 등등. 안타깝게도 비트코인은 "…해줬으면 좋겠어."라고 생각하는 사람들에게 적합한 돈이 아니다. 그보다는 자신이 스스로 "…하겠어."라고 생각하는 사람들에게 더 적합한 돈이다. 전자의 사람들은 외부 요인에 대한 맹목적 기대가 좌절될 경우 자신에게 가야 할 비난의 화살을 비트코인으로 쉽게 돌린다. 그게 그 사람의 마음을 조금 편해지게 해줄지언정, 그가 미래에 놓칠 기회들에 대한 책임은 그 스스로 책임져야 한다. 지식 없이 비트코인에 대한 경험만 하는 것은 사람을 맹목적으로 만들면서도, 그의 자유에 대한 의지는 매우 취약한 상태에 있게 되므로 자신의 비트코인을 지키기 어렵게 만든다.

따라서 자유와 비트코인에 대한 끊임없는 공부가 비트코인에 대한 경험과 병행되어야 한다. 직관과 지성이 결합할 때만 지식이 생긴다. 자유

는 쉽게 얻어지는 것이 아니다. 끊임없이 공부하고 사유하고, 경험하고 실천해야 도달할 수 있는 이상인 것이다.

필자가 『비트코인 백서 해설』의 일부를 집필했을 때 이메일로, 혹은 주변 사람에게 많이 받았던 문의는 다음과 같은 것이었다. "그래서 어떻게 해야 하는가?" 이 책은 그에 대한 답을 스스로 찾을 수 있게 하기 위한 실용서다. 그러나 전문적인 수준의 실용서가 아니라 일단 비트코인을 경험하기 위한 실용서다. 이 책은 실용서이므로 여러 가지 기기와 소프트웨어들을 다루고 있다. 따라서 각 기기의 펌웨어가 업데이트되는 등의 사건이 발생하면 책에 나와 있는 방법과 현재 수행해야 하는 방법이 약간씩 달라질 수 있다. 그러므로 독자들은 이 점을 인지해야 한다. 책을 보며 따라 할 계획이었다면 미루지 말고 최대한 빠르게 시간을 들여 따라 해보길 권장한다. 또한 모든 부분을 다 읽으려 하기보다는 사전처럼 필요한 부분을 찾아 읽되 각 부의 첫 장에 서술한 기본 지식 글은 읽을 것을 권장한다.

이 책은 어떤 제품이나 소프트웨어를 광고하려는 목적으로 저술한 것이 절대 아님을 밝힌다. 모두 필자가 직접 돈을 들여 구매한 것들이며, 업체로부터 그에 상응하는 대가를 받은 적이 없다. 개인 지갑의 경우 에어-갭 상태를 유지할 수 있고 전용 프로그램을 강제하지 않는 것을 기준으로 선정했으며, 해당 지갑이 대한민국에서 판매 중인지도 중요한 요인이었다(더 다양한 비트코인 콜드월렛이 한국에서 판매되기를 바란다). 접근성 때문에 지갑의 경우 스마트폰 공기계를 콜드월렛으로 사용하는 방법도 (개인적으로 추천하지 않음에도 불구하고) 서술했고, 풀 노드의 경우에는 직접 미니 PC를 조립하거나 남는 노트북을 이용해 운영하는 방법도 서술했다.

이 책은 총 6개의 부로 이루어져 있다. 1부에서는 개인 지갑(콜드월렛) 사용 방법, 그중에서도 특히 에어-갭 지갑의 사용 방법을 알아볼 것이다. 비트코인을 개인 지갑에 보관하는 것을 '셀프 커스터디'라고 부른다. 셀프 커스터디를 하고 나면 비트코인이 어느 누구도 빼앗을 수 없고 자신의 구매력을 지켜줄 돈이라는 것을 경험할 수 있다. 2부에서는 비트코인으로 실물 상품을 결제하거나, 결제받는 방법을 알아볼 것이다. 이를 통해 비트코인이 '돈'이라는 것을 경험할 것이다. 3부는 풀 노드 운영 방법에 관한 것으로, 비트코인 네트워크에 직접 참여하고, 자기 지갑의 잔액 조회나 거래 전파 등을 자신의 풀 노드를 통해 직접 하는 단계까지 알아볼 것이다. 이를 통해 비트코인의 분산화 속성이 개인 사용자들로부터 나오고, 자신이 네트워크의 일부가 됨으로써 비트코인의 분산화 속성을 강화할 수 있다는 것을 경험할 것이다. 4부에서는 라이트닝 노드 운영 방법에 대해 알아볼 것이다. 누군가에게 수탁하는 라이트닝 지갑을 사용하지 않고, 스스로 라이트닝 노드를 운영하고 채널을 개설해 볼 것이다. 이로써 비트코인 제2레이어에 대해 이해하고, 비트코인의 확장성에 기여하는 것을 경험할 것이다. 5부에서는 분산 소셜 미디어 프로토콜인 노스터 사용 방법에 대해 알아볼 것이다. 기존 소셜 미디어의 문제점들을 훑어본 뒤, 콘텐츠 생산자에게 비트코인을 직접 전송하고 본인도 비트코인을 받을 수 있는 분산 소셜 미디어 프로토콜을 직접 경험할 것이다. 6부는 비트코인의 홈 채굴 방법에 관한 것으로, 비트코인 네트워크를 스스로 보호하는 것을 경험할 것이다.

필자는 『비트코인 백서 해설』의 일부를 집필할 때 어떤 당위를 주장하지 않으려고 애를 썼다. 생각은 본인 스스로 하는 것이기 때문이다. 물론 개념에 주관은 반영되어 있을 수 있지만, 그에 대한 판단은 독자의

몫이라는 것을 인지하고 있었다. 그러나 이 책에서는 적극적으로 당위를 주장하겠다. 비트코인을 적극적으로 경험할 것을 권고한다. 이렇게 당당히 주장할 수 있는 이유는 어차피 경험 이후에 오는 느낌은 당신의 몫이기 때문이다.

거래를 직접 전파하라. 돈을 사용해 보기도, 저축해 보기도 하라. 네트워크에 직접 참여하라. 전 세계에서 일어나는 모든 비트코인의 거래 장부를 직접 보유하고 업데이트하라. 거래와 블록을 독립적으로 검증하라. 남을 신뢰하지 말고 스스로 잔액을 조회하고, 거래와 블록을 전파하라. 스스로 네트워크를 확장하라. 네트워크를 직접 보호하라. 금융 주권을 가져라. 신뢰하지 말고 검증하라. 당신의 돈을 스스로 통제하라.

이 과정에서 얻는 경험과 느낌이 당신을 진정한 자유로 이끄는 데 도움이 되길 바란다.

필레몬

감수의 글

2024년 초, POW라는 이름의 비트코인 커뮤니티를 처음 알게 되었다. 그때 나는 한창 셀프 커스터디에 관심을 가지기 시작한 입문자들을 도우면서 스스로도 많이 배우고 있었다. 그해 여름, 커뮤니티에 올라온 글 하나가 시선을 붙잡았다. 그 글은 비트코인 백서의 한 부분을 해설한 글이었다. 글을 읽으며 생각했다. "이건 좀, 다른데?" 단순한 요약이 아니라 기술적 정확성과 철학적 통찰이 뛰어났고, 말 한마디 한마디에서 진심이 느껴졌다. 이런 글을 쓰는 사람이라면, 뭔가 보여줄 게 많겠구나 싶은 생각이 들었고, 지금 돌이켜보면 그 직감은 틀리지 않았다. 이 책은 그 느낌이 어떤 결과로 이어졌는지를 잘 보여준다.

그렇게 시작된 인연은 시간이 흐른 뒤, 나에게 한 통의 메시지로 이어졌다. 저자는 『비트코인 사용 가이드』라는 제목으로 새 책을 준비하고 있었고, 그 감수를 맡아줄 수 없겠느냐고 조심스럽게 부탁해 왔다. 나는 망설일 이유가 없었다. 그가 초보 비트코이너들을 위해 어떤 노력을 해왔는지, 그리고 그 노력이 단지 기술적인 안내가 아니라 '비트코인 스탠다드'를 위한 실천이자 헌신이었다는 것을 누구보다 잘 알고 있었기 때문이다. 그 요청은 내게 부담이 아닌, 영광스러운 제안이었다.

원고를 처음 읽었을 때, 저자가 자신의 경험을 얼마나 성실하게 담아냈는지가 가장 먼저 눈에 들어왔다. 이 책은 단순한 매뉴얼이 아니다.

저자는 책이라는 매체가 인터넷 정보보다 더 무게감 있고, 쉽게 사라지지 않는다고 보았다. 그래서 더 많은 일반인들이 직접 해볼 수 있도록, 셀프 커스터디부터 결제, 풀 노드, 라이트닝, 채굴에 이르기까지 하나하나 안내하고자 했다. 나는 감수자로서 책의 구성이나 흐름을 바꾸기보다는, 저자의 의도가 왜곡되지 않도록 표현의 정확성을 다듬고 실용적 맥락에서 혼동을 줄이는 데 집중했다. 그로 인해 독자의 입장에서 이 책을 처음부터 끝까지 따라가 볼 수 있었고, 『비트코인 사용 가이드』의 가장 큰 강점이 정보와 실천, 철학과 실제가 유기적으로 연결되어 있다는 점임을 자연스럽게 느낄 수 있었다.

지갑을 만들고 노드를 설치하며 라이트닝 채널을 개설하는 설명이 이어질 때조차, 그 모든 절차에는 '왜 이걸 해야 하는가?'라는 질문이 깔려 있다. 독자가 단순히 따라 하기만 하도록 놔두지 않고, 행동의 배경에 있는 동기를 함께 전달하려는 책이다. 설명은 실천을 위한 것이지만, 그 방향은 언제나 자유와 주권이라는 본질을 향한다. 바로 그 지점에서, 서문에 인용된 칸트의 말이 의미를 선명히 드러낸다. "내용 없는 사상은 공허하며, 개념 없는 직관은 맹목이다." 이 문장을 서문에서 처음 읽었을 때, 나는 그 의미를 곱씹지 않을 수 없었다. 비트코인을 단지 이론으로만 이해하는 것은 공허할 수 있으며, 실천 없이 접근한다면 그 가치를 온전히 체감하긴 어려울 것이다. 결국 우리는 직접 해보는 과정을 통해서 비트코인을 더 잘 배울 수 있고, 그것이 비트코인의 방식이라고 생각한다. 지갑을 설치하고 사토시를 보내며 블록 컨펌을 기다리는 일은, 자유에 대한 실천이자 철학을 몸으로 이해하는 방식이다. 은행이 아닌 나의 키를 갖고, 제3자의 서버가 아닌 내가 직접 운영하는 노드를 선

택하는 모든 행위가 곧 '나는 누구에게도 의존하지 않겠다'는 선언이자 실천이 된다.

요즘 우리는 너무 쉽게 소유하고, 너무 가볍게 내려놓는다. 무언가를 '갖는다'는 말은 이제 클릭 한 번이면 가능하지만, 비트코인은 그렇게 되지 않는다. 갖는다는 것은 지킨다는 것이고, 지킨다는 것은 알아야 가능한 일이다. 그 앎은 책 속 이론이 아니라, 손끝의 경험에서 비롯된다. 이 책은 특정한 독자만을 위한 책이 아니다. 비트코인을 처음 접하는 사람에게는 좋은 입문서가 될 것이며, 이미 경험을 쌓은 사람에게는 다시 초심으로 돌아가는 계기를 제공할 것이다. 무엇보다, 비트코인의 가치를 실천하고 책임지려는 이들에게 꼭 필요한 책이다.

비트코인을 이해하는 데 가장 중요한 자산은 '시간'이다. 『비트코인 사용 가이드』는 독자의 시간을 아끼지 않는다. 대신, 들인 시간만큼 확실한 경험과 깨달음을 되돌려준다. 그러니 이 책을 단순히 읽는 데 그치지 말고, 각 챕터를 실행해 보며 따라가기를 권한다. 노드를 직접 설치하고, 키를 지키며, 자신의 거래를 전파하는 사람들이야말로 비트코인을 진정으로 이해한 사람들이다. 당신도 그중 한 사람이 되기를. 그리고 이 책이 그 출발점이 되기를 진심으로 바란다.

HYPE

| 목차 |

1부. 셀프 커스터디 가이드

2부. 비트코인 스탠다드 가이드

3부. 풀 노드 운영 가이드

4부. 라이트닝 노드 운영 가이드

5부. 노스터 가이드

6부. 홈 채굴 가이드

부록

비트코인 사용 가이드

1. 셀프 커스터디 가이드

| 비트코인 지갑 사용을 위한 지식

셀프 커스터디

비트코인 개인 지갑을 사용하기 위한 지식들을 알아보자. 처음 보는 내용이 많을 수도 있지만 겁먹을 필요 없다. 차근차근 연습하다 보면 체득하게 될 것이다. 먼저 셀프 커스터디self-custody가 무슨 뜻인지부터 알아보자. '커스터디'는 한국어로 '수탁'이다. 수탁은 누군가에게 맡기는 것을 뜻한다. 셀프는 '자신'을 뜻하니까 셀프 커스터디는 '자신에게 맡긴다', 즉 비트코인을 내가 직접 보관한다는 뜻이다. 그래서 셀프 커스터디를 다른 말로 '비수탁'이라고도 한다.

셀프 커스터디의 반대를 생각해 보면 더 이해가 쉬울 것이다. 셀프 커스터디의 반대는 커스터디, 즉 수탁이다. 내 비트코인을 거래소 등에 맡기는 것이 수탁이다. 정리하면 비트코인을 업비트나 빗썸, 바이낸스 같은 거래소에 보관하면 커스터디, 비트코인을 내가 직접 개인 지갑에 보관하면 셀프 커스터디다.

비트코인의 소유권과 셀프 커스터디의 필요성, 책임

비트코인 사용자들 사이에서 아주 중요하게 다뤄지는 말이 있다. '당신의 키가 아니면, 당신의 비트코인이 아니다. (Not Your Keys, Not Your Bitcoin.)'라는 말이다. 잠시 뒤에 개인키가 무엇인지 좀 더 자세히 알아볼 텐데, 개인키가 있어야 비트코인을 사용할 수 있다. 그래서 비트코인 세계에서는 비트코인을 사용할 수 있는 개인키를 가진 사람이 그 비트코인을 가진 것으로 여겨진다.

어떤 사람이 비트코인을 잃어버렸다면, 그건 비트코인을 잃어버린 게 아니라 사실 비트코인을 쓸 수 있는 개인키에 대한 통제권이 없어진 것이다. 그러므로 셀프 커스터디란, 개인키를 자기가 직접 보관하는 것을 의미한다.

거래소를 이용해 본 적이 있는가? 거래소를 이용할 때 거래소가 개인키를 알려주던가? 그렇지 않다. 개인키는 거래소만 알고 있다. 따라서 거래소에 비트코인을 두는 것은 내가 그 비트코인을 소유한 것이 아니다. 거래소에 둔 비트코인은 거래소의 것이다. 이런 방식은 내가 출금을 요청했을 때 거래소가 나에게 순순히 출금 처리를 해줄 것이라는 믿음에 기대야 한다. 이런 상황에서는 거래소가 갑이고, 내가 을이다. 출금해 줄지 말지는 거래소 마음이다. 거래소는 출금을 빌미로 온갖 개인정보를 요구할 수 있고, 갑자기 출금을 정지할 수도 있다.

비트코인은 소유권을 포함한 금융 주권을 개인이 온전히 누릴 수 있게 하는 돈이다. 그런데 거래소에 비트코인을 보관한다면 그 비트코인은 나의 것이 아니게 된다. 따라서 비트코인을 내가 갖고자 한다면 셀프 커스터디는 선택이 아닌 필수다.

비트코인은 모든 권한이 분산화되어 있다. 중앙 관리 주체가 없기 때문에 운영자나 고객센터가 없다. 따라서 셀프 커스터디를 할 때는 모든 것을 자신이 책임지는 태도도 필요하다. 공부하기 싫어하고, 남에게 맡기기 좋아하는 사람은 진정한 소유권을 누릴 수가 없다. 자유에는 책임이 따르기 때문이다.

BTC와 sats 단위

본격적으로 비트코인을 알아보기 전에 꼭 알고 가야 할 사실이 있다. 1비트코인은 1억 분의 1로 쪼갤 수 있다. 그러니까 비트코인이 너무 비싸서 못 산다는 말은 잘못된 말이다. 비트코인은 꼭 1개, 2개만 살 수 있는 게 아니라 0.5개를 살 수도 있고, 0.00000001개를 살 수도 있다. 비트코인은 BTC라는 단위로 표현한다. 1억 분의 1 BTC는 1 sat (사토시)라고 한다.

0.00000001 BTC = 1 sat

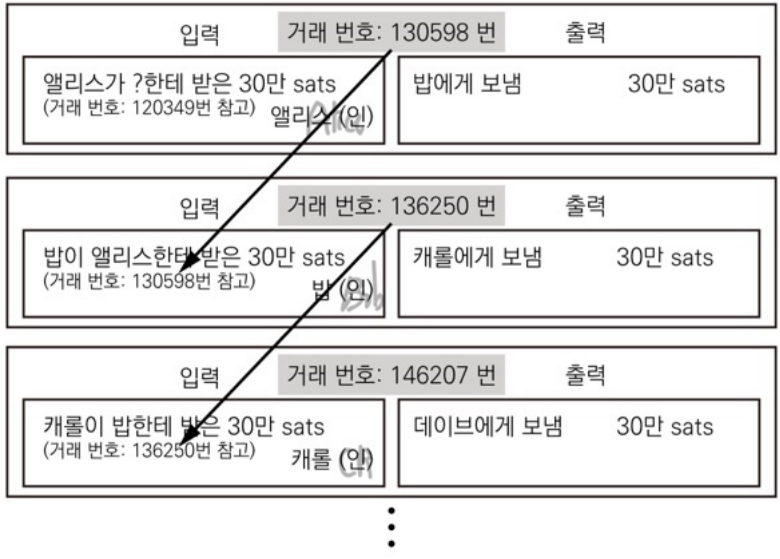
1 BTC = 100,000,000 sats (1억 sats)

잔고 모델과 UTXO 모델

이제 비트코인에 대해 본격적으로 알아보자. 비트코인은 우리가 일반적으로 사용하는 은행 시스템과 근본적으로 다르다. 내 은행 계좌에 100만 원이 들어있으면 은행은 '앨리스의 계좌번호 XXXX에 100만 원이 들어 있음.'이라는 데이터를 저장해놓는다. 이런 시스템을 '잔고 모델'이라고 한다. 잔고 모델의 문제점은 돈을 마음대로 생성해 내는 것에 취약하다는 것이다. 해커가 이 시스템을 해킹해서 자기 계좌 잔액을 100

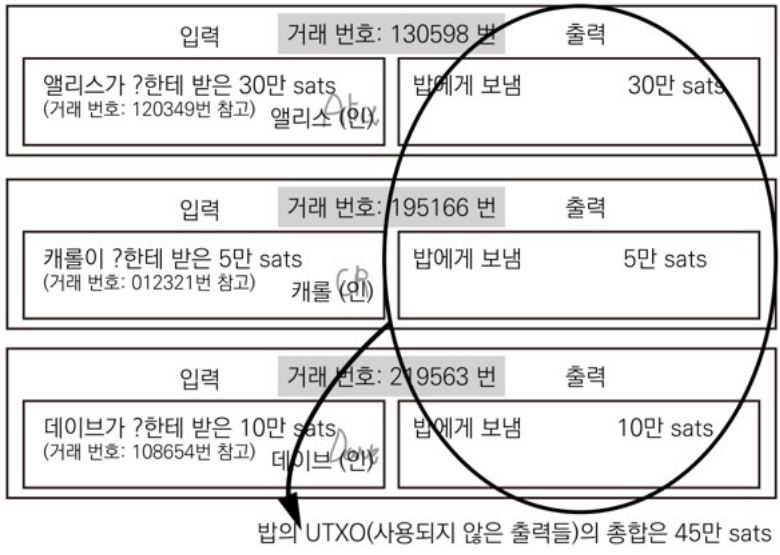
만 원에서 100억 원으로 바꾼다고 생각해 보자. 물론 은행은 이를 막기 위해 잔고 데이터에 오류가 없는지 매일 밤 정산을 한다. 밤 12시쯤에 이체가 안 되는 것을 경험해 본 적이 있다면, 이 정산 때문이다.

비트코인은 잔고 모델이 아니라 UTXO 모델이다. 비트코인에는 '어떤 주소에 100만 sats가 들어 있음.'이라는 데이터가 없다. 다만 '100만 sats가 앨리스 주소에서 밥의 주소로 이동했음.', '그렇게 이동한 100만 sats가 밥의 주소에서 캐롤의 주소로 이동했음.' 이러한 꼬리에 꼬리를 무는 데이터만 저장된다. 즉, 잔액이라는 데이터는 없고 비트코인의 소유권을 계속 바꿔주는 것이다. 이것이 비트코인의 장부에 저장되어 있는 데이터다.



그러니까 비트코인은 어디에도 저장되지 않는다. 내가 비트코인을 100만 sats 갖고 있다면, 비트코인 100만 sats는 어디에도 없다. 그저 '캐롤이 갖고 있던 100만 sats가 내 주소로 이동했다.' 이 데이터만 있는

것이다. 그리고 이 데이터는 전 세계 2만 개가 넘는 풀 노드full node(컴퓨터)에 전부 저장되어 있다. UTXO 모델의 장점은 금액을 누군가의 마음대로 생성해 낼 수 없다는 것이다. 그래서 투명성과 보안성이 높다.



앨리스가 밥에게 30만 sats를 보내고, 캐롤도 밥에게 5만 sats, 데이브도 밥에게 10만 sats를 보냈다고 해보자. 밥은 총 45만 sats를 받았다. 만약 밥이 이 45만 sats를 아직 다른 누군가에게 보내지 않았다면, 이를 '사용하지 않은 거래 출력UTXO, Unspent Transaction Output'(이하 UTXO)이라고 한다.

비트코인 지갑 앱을 사용해 보면 잔액을 보여주는 것을 알 수 있다. 비트코인 장부에는 잔액이 저장되지 않는다고 했는데, 지갑 앱들은 어떻게 잔액을 보여주는 것일까? UTXO들의 금액을 합해서 화면에 표시해 주는 것이다. 30만 sats의 UTXO, 5만 sats의 UTXO, 10만 sats의

UTXO가 있다면 지갑 앱은 이 금액들을 더해 총잔액이 45만 sats라고 화면에 표시해 준다. UTXO는 조금 뒤에 더 자세히 알아보도록 하자.

에어-갭 지갑과 워치-온리 지갑

셀프 커스터디를 하려면 지갑을 골라야 한다. 지갑은 크게 핫월렛과 콜드월렛으로 나눠진다. 핫월렛은 지갑 기기가 인터넷에 연결된 것을 말한다. 콜드월렛은 지갑 기기가 인터넷에 연결되지 않은 것을 말한다. 무엇이 안전할까? 당연히 콜드월렛이 더 안전하다. 기기가 인터넷에 연결되어 있으면 해커가 인터넷을 타고 내 기기에 있는 개인키를 해킹할 수도 있기 때문이다.

어떤 콜드월렛은 비트코인을 전송하려고 할 때 USB나 블루투스를 통해 잠깐 인터넷에 간접적으로 연결되어야 하는 경우가 있다. 잠깐 인터넷에 연결된 순간에는 핫월렛과 다를 바가 없게 되니 개인키가 노출될 위험이 생긴다. 따라서 최고의 보안을 위해서는 콜드월렛 중에서도 에어-갭 지갑air-gapped wallet을 사용하는 것이 좋다. 에어-갭 지갑은 와이파이 같은 인터넷은 물론이고, 블루투스, NFC, USB 연결 같은 모든 연결이 막힌 지갑을 뜻한다.

또한, 지갑을 고를 때 전용 프로그램을 강제하는 지갑은 사지 않을 것을 권장한다.

중요한 사실이 있다. 에어-갭 지갑은 인터넷을 포함한 어떠한 통신도 안 되기 때문에 비트코인 잔액을 확인하거나 거래 전송 등을 할 수가 없다. 에어-갭 지갑이 데이터를 내보낼 때는 주로 QR 코드만을 사용한다.

핫 월렛은
도로(인터넷)가 연결된 섬과 같다.
해커가 이 도로를 이용해
섬에 들어갔다 나올 수도 있다.

에어-갭 지갑은 고립된 섬과 같다.

이 때문에 에어-갭 지갑은 잔액 확인이 가능한 워치-온리 지갑watch-only wallet과 함께 사용한다. 보통 워치-온리 지갑은 스마트폰에 설치하는 앱이다. 대표적으로 블루월렛BlueWallet이나 넌척Nunchuk, 코코넛 월렛이 있고, PC에 설치하는 앱으로는 스패로우 월렛Sparrow Wallet이 있다. 워치-온리 지갑은 잔액을 보는 것만 가능하다. 왜냐하면 워치-온리 지갑에는 개인키가 없기 때문이다. 따라서 어딘가로 비트코인을 보내려고 할 때는 워치-온리 지갑과 에어-갭 지갑이 협력해야 한다. 에어-갭 지갑이 개인키를 이용해 서명을 하면, 그 서명 데이터를 워치-온리 지갑이 QR 코드로 읽어와서 인터넷에 퍼뜨린다.

다시 말하지만 비트코인은 에어-갭 지갑에 저장된 것도 아니고, 워치-온리 지갑에 저장된 것도 아니다. 전 세계 모든 풀 노드에 비트코인이 어디로 이동했는지가 다 저장되어 있다. 단지 에어-갭 지갑은 개인키를 저장하고 필요할 때마다 비트코인을 옮길 수 있게 디지털 서명을 계산하는 역할을 한다.

PSBT

PSBT는 '부분적으로 서명된 비트코인 거래Partially Signed Bitcoin Transactions'(이하 PSBT)다. 워치-온리 지갑과 에어-갭 지갑이 QR 코드로 데이터를 주고받을 때 이 PSBT라는 정보를 공유한다.

트랜잭션(거래)을 만들 때 먼저 워치-온리 지갑이 거래를 구성한다. 워치-온리 지갑에는 개인키가 없으므로 서명을 할 수가 없다. 따라서 워치-온리 지갑이 만드는 정보를 '서명되지 않은 PSBT'라고 한다.

이 QR 코드를 에어-갭 지갑이 인식하면 에어-갭 지갑은 서명을 해서 그 데이터를 QR 코드로 내보낸다. 이때 에어-갭 지갑이 만든 정보를 '서명된 PSBT'라고 한다. 워치-온리 지갑이 에어-갭 지갑으로부터 서명된 PSBT를 읽어오면 이 정보를 직렬화된 정보로 바꿔 네트워크에 전파한다(정확히는 워치-온리 지갑과 연결된 일렉트럼 서버에서 풀 노드의 RPC 명령을 이용해 전파한다). 쉽게 이해하자면 거래/서명을 위해 워치-온리 지갑과 에어-갭 지갑이 주고받는 QR 코드를 PSBT라고 생각하면 된다.

개인키와 주소

비트코인 공부를 하다 보면 개인키와 공개키, 주소에 관한 내용이 많이 나온다. 개인키에서 타원곡선 암호화ECC, Elliptic Curve Cryptography 함수라는 암호 함수를 통해 공개키를 만들고, 공개키에서 해시 함수라는 암호 함수를 통해 주소를 만든다.

그런데 비트코인을 사용하면서 우리가 가장 많이 보게 되는 데이터는 주소뿐이다. 개인키나 공개키는 보통 콜드월렛들이 알아서 저장하고 계산하기 때문에 우리가 볼 일이 거의 없다. 따라서 비트코인을 사용할 때는 개인키, 주소 이 두 가지만 우선적으로 알아도 된다.

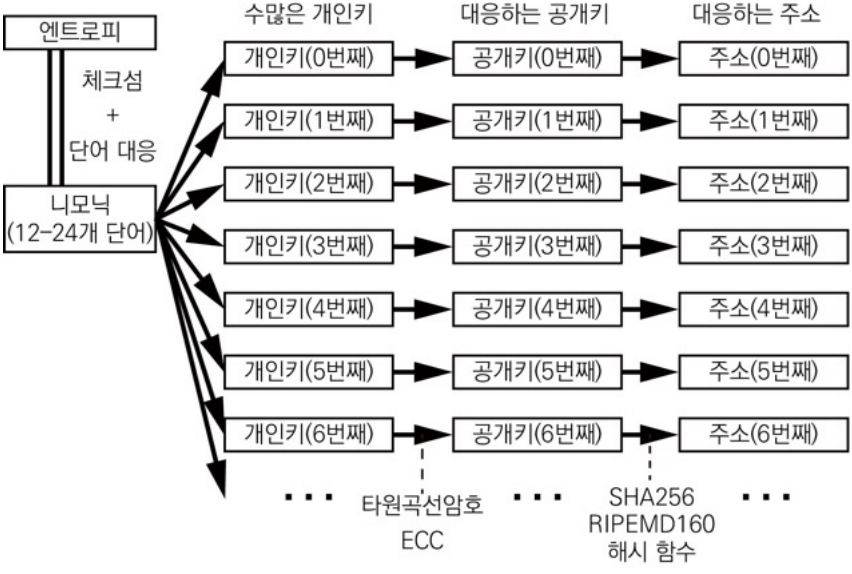
주소는 계좌번호에 비유할 수 있다. 내가 비트코인을 받으려면 나의 주소를 상대방에게 알려줘야 한다. 앞에서 비트코인 장부에는 '비트코인이 앨리스의 주소에서 밥의 주소로 이동', '밥의 주소에서 나의 주소로 이동' 이런 데이터들만 저장된다고 했다. 사실 '앨리스', '밥', '나' 이런 데이터도 없다. '주소 bc1q222…에서 주소 bc1q333…으로 이동', '주소 bc1q333…에서 주소 bc1q444…으로 이동' 이런 데이터만 있다. 이 주소들은 실제 신원과 연결되지 않으므로 어느 것이 누구의 것인지 알 수가 없다.

내가 가진 비트코인을 다른 주소로 전송하려면 개인키가 필요하다. 개인키는 비밀번호라고 생각하면 편하다. 정확히는 개인키로 서명해야 비트코인을 이동할 수 있는 건데, 이 서명이라는 것도 우리가 종이에 사인하는 그런 서명이 아니라 디지털 서명이다. 디지털 서명은 개인키를

갖고 있다는 것을 증명할 수 있는 특정 숫자를 계산하는 것이다. 이체를 할 때 계좌 비밀번호를 입력해야 하는 것처럼 개인키를 알아야 어떤 주소에 들어있는 비트코인을 전송할 수 있다.

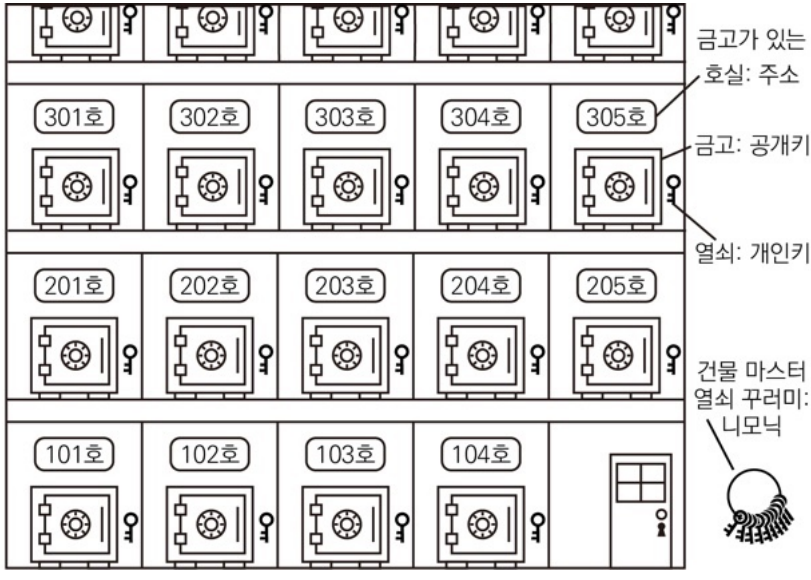
니모닉과 개인키, 주소

처음 지갑을 사용할 때 주사위를 굴리고 나면 기기가 어떤 영어 단어를 보여줄 것이다. 이것이 니모닉mnemonic이다. 니모닉 하나를 통해 수많은 개인키와 주소를 만들 수 있다. 워치-온리 지갑에서는 보통 처음에 10-20개 주소만 보여줄 것이다. 사실 우리가 사용할 수 있는 주소는 니모닉 하나에 42억 개가 있는데, (일반 주소 21억 개, 잔돈 주소 21억 개이지만 이론적으로는 이것보다 훨씬 많다.) 그중에 10-20개만 보여주는 것이다. 주소를 사용하면 그다음 주소를 계속 보여줄 것이다.



니모닉으로 개인키를 계산하는 것이기 때문에 니모닉만 잘 보관하면 언제든지 42억 개 주소에 들어있는 비트코인에 접근할 수 있다.

그리고 니모닉은 어딘가에서 생성해 주는 게 아니라 그냥 자기가 고르는 것이다. 은행 계좌를 개설할 때는 은행이 계좌를 개설해 준다. 이때 은행은 중복되지 않는 계좌번호를 골라 계좌를 개설해 준다. 그런데 비트코인은 운영자도 없고, 고객센터 같은 건 더더욱 없다고 했다. 따라서 니모닉 개설 같은 건 있을 수가 없다. 그냥 여러 숫자 중 랜덤한 숫자 하나를 자기가 고르는 것이다. 그 랜덤한 숫자를 고르기 위해 주사위를 굴리는 것이다. 그러면 혹시나 다른 사람과 니모닉이 겹치진 않을까 하는 걱정이 생길 수도 있다. 지구상에서 모래 한 톨을 고를 수 있다고 해보자. 내가 고른 모래 한 톨과 똑같은 모래를 다른 사람이 고를 수 있을까? 랜덤하게 고른 니모닉이 겹칠 확률은 이것보다 훨씬 어마어마하게 희박하다. 경우의 수가 너무 커서 우주에서 일어날 수가 없는 일이다.

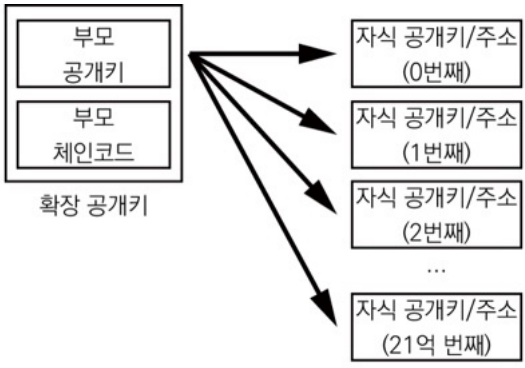


니모닉에 관해 마지막으로 정리하고 가자. 니모닉은 12개 혹은 24개의 단어 목록이다. 니모닉 하나로 수많은 개인키와 주소를 만들어낼 수 있다. 주소가 금고이고 개인키가 열쇠라면, 니모닉은 열쇠 꾸러미 같은 것이다. 따라서 니모닉은 절대 노출되지 않게 조심해야 한다.

확장 공개키

워치-온리 지갑은 개인키를 모르고 주소만 알고 있다. 워치-온리 지갑이 처음에 이 주소들을 계산하기 위해서는 확장 공개키ex-pub라는 것이 필요하다. 그래서 에어-갭 지갑과 워치-온리 지갑을 연동할 때, 에어-갭 지갑이 보여주는 QR 코드를 워치-온리 지갑이 스캔한다. 이 스캔하는 과정이 에어-갭 지갑이 워치-온리 지갑한테 확장 공개키를 넘겨주는 과정이다. 이 과정을 진행하고 나면 워치-온리 지갑에서 잔액을 조회하는 것이 가능하다.

정확히 알고 가야 할 것이 있다. 공개키와 확장 공개키는 완전히 다르다. 확장 공개키는 개인키 없이 수많은 공개키와 주소를 계산할 수 있게 하는 값이다. 공개키는 개인키로부터 만들어지는 값이고, 공개키를 통해 주소를 만들 수 있다. 쉽게 말하자면 공개키 하나는 개인키 하나로부터 하나의 주소를 계산할 때 중간에 거치는 계산값이고, 확장 공개키는 개인키들 없이 수많은 공개키와 주소를 계산할 수 있게 해주는 값이다. 둘은 의미가 완전히 다르다.



주사위를 굴릴 때 주의할 점

필자는 비트코인에 입문하는 사람이라면, 반드시 주사위를 굴려서 니모닉을 만들라고 이야기한다. 기계가 만들어주는 니모닉을 사용하면 그 기계를 신뢰해야 하는 문제가 생기기 때문이다. 주사위를 굴리면 완전히 랜덤하게 생성된 니모닉을 고를 수 있게 된다.

주사위를 굴려 니모닉을 만들 때는 주변에 카메라가 없는지 꼭 확인하고, 카메라가 없는 장소에서 해야 한다. 또한 전자기기 옆에서 니모닉을 소리 내어 읽어서도 안 된다. 해커들은 인터넷만 연결되어 있다면 무엇이든 할 수 있다는 걸 항상 생각하자. 처음에 부주의한 상태로 니모닉을 만들면, 문제가 없더라도 나중에 찜찜해서 바꾸게 된다.

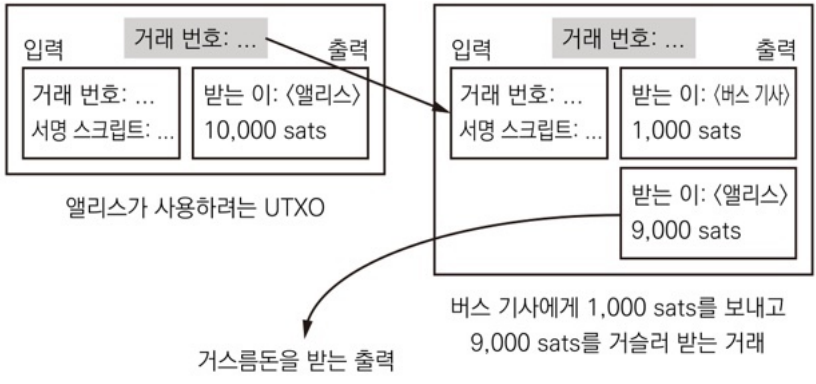
니모닉은 절대로 온라인 기기에 입력해서는 안 된다. 예를 들어 니모닉을 적은 종이를 스마트폰 카메라로 찍어놓는다거나, 스마트폰 메모장 앱 등에 기록하면 안 된다. 인터넷이 연결되어 있으면 해커가 해당 파일들을 해킹할 수 있는 여지가 생기기 때문이다. 종이나 철판 등에 잘 기록하거나 아예 외우는 것이 좋다.

거래 데이터(트랜잭션)

비트코인을 사용하다 보면 '트랜잭션'이라는 단어를 많이 듣게 될 것이다. 트랜잭션은 간단하게 그냥 거래 데이터다.

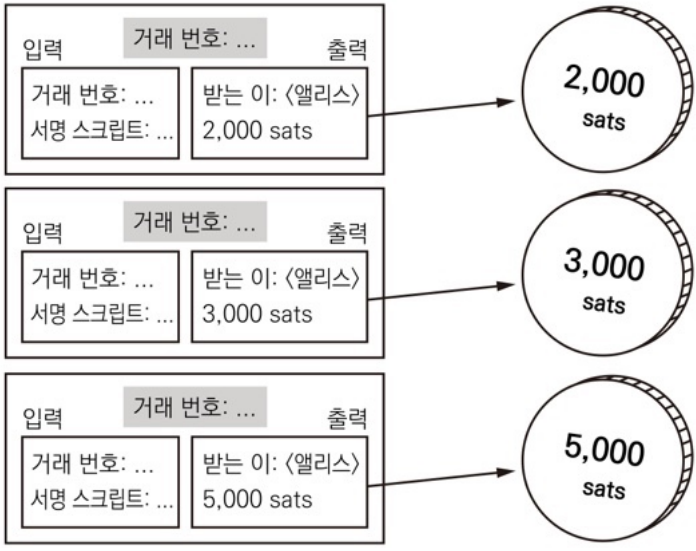
거래 데이터에는 입력 부분과 출력 부분이 있다. 입력 부분에는 내가 사용할 UTXO가 들어간다. 출력 부분에는 어느 주소로 얼마만큼의 금액을 보낼 건지에 대한 데이터가 들어간다.

거래 데이터에는 여러 개의 입력과 여러 개의 출력이 들어갈 수 있다. 만약 1만 sats 짜리 UTXO를 사용해 1천 sats짜리 버스 요금을 내면 거래 데이터는 어떤 형식이 될까? 입력에는 나의 1만 sats 짜리 UTXO가 들어갈 것이다. 출력에는 버스 회사의 주소로 보내는 1천 sats의 출력과 나머지 거스름돈 9천 sats를 나의 잔돈 주소로 보내는 데이터가 들어갈 것이다.

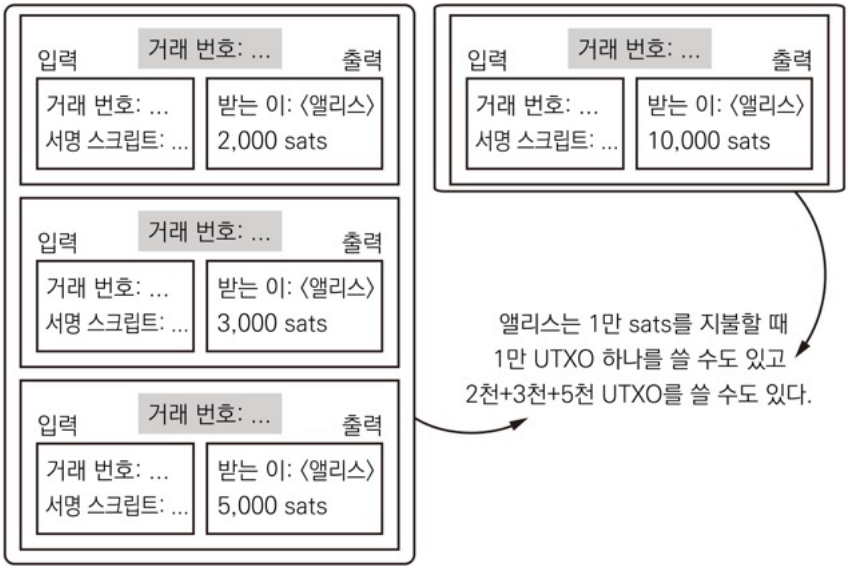


UTXO에 대한 비유

자신에게 왔지만 아직 소비하지 않은 거래들(정확히는 거래 출력들)을 UTXO라고 한다고 했다. UTXO 하나하나는 모두 동전 하나 또는 지폐와 같다. 금액이 모두 다르게 적힌 지폐나 수표를 생각하면 된다.



만 원짜리 물건을 사는 상황을 생각해 보자. 이때, 만 원짜리 지폐 1장을 내도 되고, 천 원짜리 지폐 10장을 지불해도 되고, 10원짜리 동전 1,000개를 내도 된다. UTXO도 똑같다. 앨리스가 1만 sats를 내야 하는 상황이면 1만 sats 짜리 UTXO 하나를 써서 지불할 수도 있고, 2천, 3천, 5천 sats 짜리 UTXO를 한 번에 써서 지불할 수도 있다. 지갑 앱들은 보통 비트코인을 전송할 때 자기들이 알아서 UTXO를 선택해 주지만, 스패로우나 넌척, 코코넛 월렛 같은 지갑의 경우 어떤 UTXO를 써서 지불할지 직접 선택할 수도 있다.



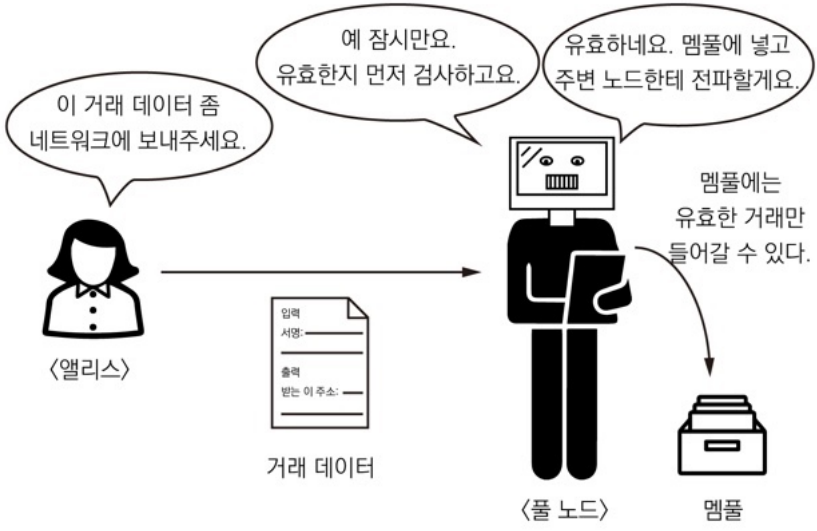
거래 데이터와 블록

내가 비트코인을 다른 누군가에게 전송하는 거래를 생성했다고 해보자. 만약 지갑 앱을 통해 이 거래를 네트워크에 전송하면 거래가 네트워크에 퍼지기 시작한다.

비트코인을 공부하다 보면 '채굴'이라는 용어를 듣게 될 것이다. 채굴자들은 이렇게 사람들이 제출하는 거래 데이터들을 모아 블록을 만들려는 사람들이다.

거래 데이터가 블록에 담기기 전에는 먼저 풀 노드들의 멤풀Mempool이라는 공간에 담긴다. 채굴자들은 멤풀에 담겨있는 거래 데이터를 블록에 넣고, 규칙에 맞는 블록을 생성하기 위해 열심히 해시 함수를 돌린다. 이렇게 조건에 맞는 블록을 생성하는 것을 작업증명PoW, proof-of-work이라고 한다. 블록을 생성하기 위해서는 에너지와 시간이 비용으로

들어간다. 만약 작업증명에 성공하여 블록을 생성하면 채굴자들은 보상을 받는데, 이 보상은 '코인베이스' 보조금과 수수료 인센티브가 합쳐져 있다. 작업증명과 인센티브 시스템을 합쳐 채굴이라고 한다.



거래를 전송하는 우리 입장에서 생각해 보자. 거래 데이터를 전송하면 거래 데이터가 우선 풀 노드들의 멤풀에 들어간다. 채굴자들은 멤풀에 있는 거래들을 꺼내서 블록을 만든다. 아직 내 거래가 블록에 실리기 전이면 지갑 앱에서는 미확정unconfirmed 거래라고 뜬다. 만약 내 거래가 실린 블록이 채굴되면 거래가 확정confirmed(컨펌)되었다고 뜬다. 종종 2컨펌, 6컨펌 이런 말을 들을 텐데, 2컨펌은 거래가 실린 블록을 포함하여 총 2개 블록이 채굴된 것을 말한다. 6컨펌은 거래가 실린 블록을 포함하여 총 6개 블록이 채굴된 것을 말한다. 거래가 실린 블록 위에 블록이 쌓일수록 거래를 바꾸는 것이 불가능에 가까워진다.

수수료

비트코인 온-체인에는 수수료 시스템이 있다. 이 수수료는 채굴자들에게 지불하는 것이다. 블록의 크기에는 제한이 있어서 모든 거래가 들어갈 수 없을 때가 많다. 그러면 채굴자들은 당연히 수수료를 많이 지불하는 거래 데이터를 먼저 블록에 싣는다. 그래야 자기가 비트코인을 많이 벌 수 있으니 말이다.

수수료는 데이터당 수수료(sat/vB)로 측정한다. 만약 수수료를 너무 낮게 설정하면 어떤 일이 일어날까? 거래가 네트워크에 퍼져 있는데 채굴자들이 아무도 거래를 블록에 실어주지 않아 거래가 계속 컨펌되지 못하는 사태가 일어난다. 이런 상황을 해결하기 위해 'RBF'나 'CPFP'를 사용할 수도 있지만, 초보일 때부터 이것저것 다 해보며 힘들게 훈련할 생각이 아니라면 적당한 수수료를 설정하는 것이 좋다.

멤풀 웹사이트

그렇다면 적당한 수수료율은 어디서 확인할 수 있을까? 대표적으로 멤풀 웹사이트가 있다. 멤풀 웹사이트는 멤풀과 다르다. 멤풀은 앞에서 봤듯이 풀 노드들이 거래가 블록에 실리기 전 임시로 저장해놓는 공간을 뜻하는 것이다. 멤풀 웹사이트는 이 멤풀에서 이름을 따온 웹사이트다.

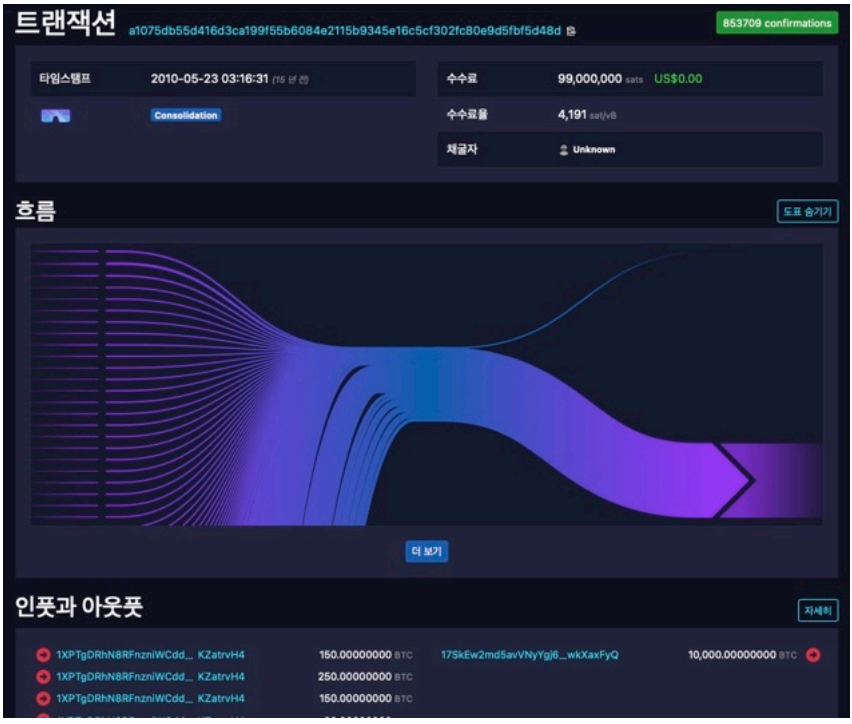
멤풀 웹사이트는 현재 비트코인 네트워크 상황을 보여준다. 사실 멤풀 웹사이트는 웹사이트 운영자의 풀 노드와 연결되어 있는 것이므로 이 웹사이트 운영자의 풀 노드 상황을 보여주는 것이다. 만약 멤풀 웹사이트 운영자의 풀 노드를 신뢰하기 싫다면 자신이 직접 풀 노드를 운영하면 된다.

멤풀 웹사이트에서는 현재 적정 수수료율을 확인할 수 있다. 이 웹사이트를 보고 수수료율을 설정할 때 중간 우선순위 이상으로 설정하는 것을 추천한다. 낮은 우선순위로 수수료율을 설정하면 거래가 언제 컨펌될지 모르는 채로 한참 기다려야 하는 사태가 일어날 수도 있다. 보통 지갑 앱들은 현재 네트워크 상황에 따라 적정 수수료율을 자동으로 설정해 준다. 하지만 자기가 직접 수수료율을 설정할 수도 있다.

이 외에도 멤풀 웹사이트에서는 거래 데이터도 확인할 수 있다. 각 거래에는 'txid'라는 고유의 이름이 붙어 있다. 이 txid를 멤풀 웹사이트에서 검색하면 거래도 더 자세히 확인할 수 있다.

멤풀 웹사이트 링크는 아래와 같다.

https://mempool.space/ko/



UTXO 정리

UTXO는 너무 큰 금액으로 보관해도, 너무 작은 금액으로 보관해도 단점이 있다. 그래서 적당한 금액으로 쪼개놓는 것이 좋다.

UTXO의 금액이 너무 크면 다음에 거래할 때 자신이 대략 얼마의 비트코인을 가졌는지 노출되기 때문에 좋지 않다. 당신이 요금이 천 원인 버스에 탔는데 1,000만 원짜리 수표를 냈다고 해보자. 버스 기사가 999만 9천 원을 거슬러 주면 될 일이다. 하지만 당신이 그 수표를 사용함으로써 당신은 1,000만 원을 가졌다는 사실이 드러났다. 따라서 UTXO는 일상에서 사용할 수 있는 적절한 금액으로 쪼개 놓는 것이 좋다.

하지만 너무 잘게 쪼갠다면 한 번의 거래에서 많은 입력을 사용해야 한다. 앞에서 말했듯이 데이터 크기가 커지면 내야 하는 수수료도 많아진다. 입력이 많아지면 거래 데이터의 크기가 커지니 당연히 내야 하는 수수료도 커질 것이다.

따라서 권장하는 UTXO 관리 방법은 하나의 UTXO 당 2주-세 달 정도마다 사용할 양으로 분할하는 것이다. 약 100만-200만 sats 정도로 말이다. 큰 지불에 대비해 좀 더 크게 쪼갠 UTXO를 만들어도 좋다.

주소 재사용 주의

앞에서 우리는 니모닉 하나에 엄청나게 많은 개인키와 그에 대응하는 주소가 있다는 것을 알아보았다. 한 번 사용한 주소는 다시 사용하지 않는 것이 좋다. 프라이버시의 이유가 크다.

같은 주소를 반복해서 사용할 경우, 해당 주소로 입금된 과거 내역이 모두 공개된다. 그러면 새로운 거래 역시 해당 기록과 연결되어 추적이 쉬워진다. 이는 사용자의 전체 잔고나 거래 패턴을 타인이 파악할 수 있게 만들어 프라이버시를 심각하게 침해할 수 있다.

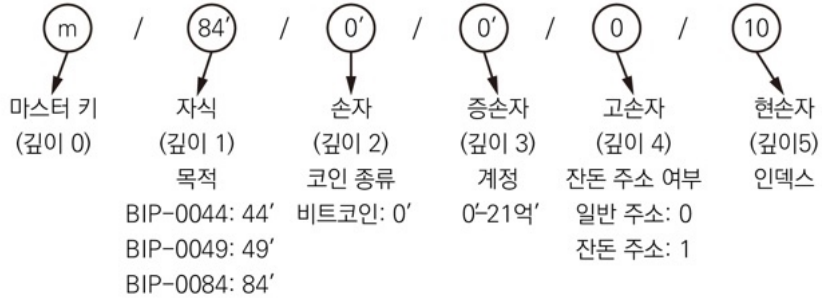
파생 경로

주소에는 여러 형식이 있다. '1'로 시작하는 주소도 있고, '3'으로 시작하는 주소, 'bc1q'로 시작하는 주소, 'bc1p'로 시작하는 주소가 있다. 하지만 비트코인에 처음 입문하면 대부분 'bc1q'를 사용하게 될 것이다.

주소 형식이 다르면 당연히 워치-온리 지갑이 스캔하는 주소들도 달라진다. 따라서 자신이 어떤 주소로 파생했는지 기억하는 것도 중요하다. 많이 사용하는 주소 형식을 표로 정리하면 다음과 같다.

주소 접두사	목적 구분(BIP 번호)	종류
1	44	레거시 주소
3	49	네스티드 세그윗 주소
bc1q	84	네이티브 세그윗 주소
bc1p	86	탭루트 주소

이 주소가 어떤 주소인지 파악하기 쉽게 하기 위해 파생 경로라는 것이 있다. m/84'/0'/0'/0/10 이런 방식으로 표현되는 것이 파생 경로다. 간단히만 훑으면 두 번째 구분인 84'는 네이티브 세그윗 주소로 파생한다는 뜻이다. 마지막 구분인 10은 이 지갑의 10번 주소(11번째 주소)라는 것이다. 10번 주소가 10번째가 아니라 11번째인 이유는 숫자를 0부터 세기 때문이다.



갭 리밋과 주소 순차 사용

니모닉 하나에는 매우 많은 주소가 있다고 했다. 이 주소들에는 '인덱스'라는 각각의 번호가 붙는다. 파생 경로에서 맨 마지막에 오는 숫자가 인덱스다. 예를 들어 파생 경로 m/84'/0'/0'/0/0은 0번 주소, m/84'/0'/0'/0/10은 10번 주소라는 식으로 이야기한다.

주소는 앞에서부터 순차적으로 사용하는 것이 좋다. 특정한 목적을 위해 후순위 주소를 사용할 수도 있겠으나 다른 목적이 없다면 앞번호 주소부터 순차적으로 사용하는 것이 좋다. 앞번호 주소보다 후순위 주소를 계산하는 데 특별히 시간이 더 걸리는 것도 아니다.

워치-온리 지갑들이 한 번에 수억 개 주소를 스캔하는 것은 불가능하다. 시간이 매우 많이 걸릴 테니 말이다. 그래서 보통 워치-온리 지갑들은 한 번에 마지막 사용 주소로부터 20개 정도의 주소만 더 스캔한다. 워치-온리 지갑들이 한 번에 스캔하는 주소의 개수를 갭 리밋gap limit이라고 한다.

갭 리밋이 20인 워치-온리 지갑이 있다고 해보자. 이 지갑의 주소를 사용한 적이 없다면 20개 주소만 스캔할 것이다. 만약 10번 주소까지 사용했다면 20개 주소를 더 스캔해 30번 주소까지 스캔할 것이다. 그러면 50번 주소에 비트코인이 있더라도 워치-온리 지갑이 스캔하지 못한다. 워치-온리 지갑이 스캔을 못 하면 당연히 PSBT도 생성할 수 없으므로 그 주소에 있는 비트코인은 다른 곳으로 보낼 수 없는 상태가 된다. 이럴 때는 다른 특수한 방법을 통해 비트코인을 앞번호 주소로 보내야 한다. 이렇듯 워치-온리 지갑들에는 보통 갭 리밋이 있으므로 주소는 순차적으로 사용하는 것이 좋다.

패스프레이즈

간혹 패스프레이즈passphrase라는 것을 들어볼 수도 있다. 입문자라면 패스프레이즈를 설정하지 않기를 권장한다. 패스프레이즈를 적용하면 같은 니모닉이어도 완전히 다른 지갑이 생성되기 때문이다. 이에 대한 제대로 된 이해 없이 패스프레이즈를 설정했다가 비트코인을 완전히 잃어

버린 입문자들이 많다. 패스프레이즈는 먼저 그 원리와 필요성을 제대로 알고 난 후에 설정해도 늦지 않다.

패스프레이즈를 설정하면 완전히 다른 지갑이 생성된다고 했다. 패스프레이즈를 설정해 놓고 패스프레이즈를 설정한 지갑에 대부분의 비트코인을 보낸 뒤, 패스프레이즈가 없는 지갑에는 소량의 비트코인만 보냈다고 해보자. 강도가 들어서 비트코인을 내놓으라고 하면 그냥 니모닉만 알려주고 그것을 가져가게 할 수 있다.

같은 니모닉에 서로 다른 패스프레이즈를 이용해 여러 지갑을 생성할 수도 있다. 하지만 이러한 목적이라면 패스프레이즈보다는 파생 경로의 계정 구분을 이용할 수 있고, BIP-0085에서 정의된 자손 니모닉을 이용할 수도 있다. 너무 깊게 들어가지는 않겠다. 어쨌든 이와 같은 용도로 패스프레이즈를 쓸 수 있다. 이 부분에 대한 이해가 제대로 되어 있지 않은 입문자는 패스프레이즈를 쓰지 말 것을 권고한다.

니모닉 체크섬과 MFP

주사위를 굴려 만든 숫자(엔트로피)는 외우기가 너무 어렵기 때문에 이를 니모닉 단어로 변환하는데, 이때 체크섬checksum 정보가 추가된다. 니모닉에는 오기입을 방지하기 위한 몇 가지 장치가 있다.

먼저 니모닉 단어는 2,048개 영단어인데 이들 중 맨 앞 4글자가 겹치는 단어는 없다. 예를 들어 니모닉 단어에는 base (기초)라는 단어가 이미 있는데 맨 앞의 4글자가 똑같은 basement (지하실)가 포함될 수 없는 것이다. 따라서 니모닉 단어를 적을 때는 사실 앞 4글자만 적어도 무방하다. 5번째 자리부터 나는 오타는 보정이 가능하다. abandon (포기

하다)이라는 단어를 실수로 abandoned (포기된)라고 적어도 니모닉 단어 목록을 보고 보정이 가능하다는 뜻이다.

니모닉에는 체크섬 정보가 추가된다. 니모닉에서 체크섬은 실수로 다른 니모닉 단어를 입력하진 않았는지 확인할 수 있게 하는 정보다. 체크섬이 무엇인지 이해를 돕기 위해 예시를 들어보겠다. 0 또는 1로만 이루어진 네 자리 수열이 있다고 해보자. 1 1 0 1과 같이 말이다. 여기에 혹시 오타가 나지는 않는지 확인하기 위해 마지막에 각 자리를 전부 더한 값을 쓰면 3이 추가될 것이다. 1 + 1 + 0 + 1 = 3이기 때문이다. 그러면 전체 수열은 1 1 0 1 3이 된다. 만약 실수로 오타가 나서 두 번째 숫자를 1이 아닌 0으로 썼다고 해보자. 그러면 수열은 1 '0' 0 1 3 이 된다. 우리는 마지막에 각 자리를 전부 더한 값을 뒤에 추가한다는 규칙 덕분에 무언가 잘못되었다는 것을 알 수 있다. 1 + '0' + 0 + 1은 3이 아니기 때문이다. 이렇듯 마지막에 추가되는 3과 같이 수열에 잘못된 것이 있는지 알려주는 정보가 체크섬이다. 이 상황에서 정말 우연히 세 번째 자리도 오타가 나서 0을 1이라고 썼다고 해보자. 그러면 수열은 1 '0' '1' 1 3이 될 것이다. 이때는 체크섬이 제 기능을 못 하게 된다. 그러므로 체크섬은 대체로 잘못된 정보가 있는지 알려주지만, 완벽하게 알려주는 것은 아니다. 니모닉 생성 시 들어가는 체크섬은 이 예시처럼 정보를 다 더한 값은 아니고 해시 함수라는 규칙을 통해 만들어진다.

니모닉에는 체크섬 정보가 12단어는 12번째 단어에, 24단어는 24번째 단어에 포함되어 있다. 그래서 니모닉은 마지막 단어까지 자기 마음대로 고를 수는 없다. 당연히 자기 마음에 드는 니모닉 단어를 고르는 것은 추천하지 않는다. 알게 모르게 인간의 어떤 편향이 들어갈 수 있으므로 주사위를 던져 니모닉 시드를 만드는 것을 추천한다. 아무튼 체크

섬 때문에 중간에 단어 하나를 잘못 써도 이 니모닉이 잘못되었다는 것을 알 수 있다. 다음 니모닉을 보자.

abandon abandon abandon abandon abandon abandon abandon abandon abandon abandon abandon about

이런 니모닉이 있는데 실수로 첫 번째 단어를 다음처럼 바꿔서 입력했다.

"abuse" abandon abandon abandon abandon abandon abandon abandon abandon abandon abandon about

그러면 체크섬 계산 결과가 맞지 않으므로 기계는 잘못된 니모닉이라고 판별해 우리에게 잘못된 니모닉이라는 것을 알려준다.

이러한 장치들은 매우 중요한데, 비트코인은 중앙 주체가 전혀 없으므로 자신이 모든 걸 책임져야 하기 때문이다. 일반적으로 우리가 사용하는 중앙 집중형 웹사이트에서 ID와 비밀번호를 입력했을 때를 생각해 보자. 비밀번호에 오타가 나면 웹사이트 서버는 비밀번호가 잘못되었다는 정보를 우리에게 보낸다. 하지만 비트코인에는 그런 게 없다. 그래서 지갑 같은 기계가 스스로 계산할 수 있도록 이러한 체크섬과 같은 기능이 들어 있는 것이다.

하지만 체크섬 기능도 완벽하지 않다. 12단어의 경우에는 다른 니모닉을 입력해도 16분의 1 확률로 니모닉이 잘못되었다는 것을 감지하지 못할 수도 있다. 사실 이런 경우에는 '잘못된' 니모닉이 아니라 그냥 다른 지갑이 만들어진 것이다. 지갑은 생성하는 것보다는 그냥 무작위적

인 숫자를 고르는 것에 가깝기 때문이다(체크섬을 제외하면). 24단어의 경우에는 256분의 1 확률로 감지하지 못할 수도 있다.

따라서 지갑을 사용할 때 MFP도 꼭 함께 기억하거나 백업할 것을 권장한다. MFPMaster Fingerprint혹은 XFP는 지갑의 고유 식별자라고 생각하면 된다. MFP가 무엇인지 정확히 이해하려면 니모닉과 엔트로피, 마스터 공개키 등에 대해 알아야 한다. 니모닉을 통해 시드를 만들고, 시드로 마스터 개인키를, 마스터 개인키로 마스터 공개키를 만든다. 마스터 공개키를 SHA256과 RIPEMD160 함수로 순차적으로 해싱하여 HEX 값 8자리를 취하면 MFP가 나온다.

쉽게 생각하자. 무슨 뜻이냐면 지갑마다 고유의 이름 같은 게 있다고 생각하면 된다. MFP는 서로 다른 지갑에서 겹칠 확률이 약 42억 분의 1이다. 따라서 내가 지갑을 복구했는데 다른 MFP가 보인다면 예전에 쓰던 지갑과 다른 지갑이 생성되었다는 것을 알 수 있다.

MFP는 특히 패스프레이즈를 사용할 때 중요해진다. 패스프레이즈는 '틀린다'는 개념이 아예 없다. 무엇을 입력하든 그대로 지갑을 생성해 준다. 따라서 패스프레이즈에 대소문자, 점 하나, 공백 하나를 잘못 입력하면 완전히 다른 지갑이 생성되어 버린다. 이를 알기 위해서는 기존에 사용하던 지갑의 MFP를 알아놓는 것이 좋다. 패스프레이즈를 사용하지 않아도 MFP는 적거나 백업하는 것을 추천하며, 패스프레이즈를 사용한다면 필수적으로 MFP를 적거나 백업해야 한다.

5달러 렌치 공격과 수량 발설 주의

비트코인을 얼마나 모았는지 자랑하고 싶은 사람들도 있는 것 같다. 이는 비트코인이 얼마나 중요해질지 잘 모르기 때문인 것도 있다. 자산을

자랑하는 것은 아직 부를 지키는 방법에 대해서는 배우지 않은 졸부들의 특징이라 저급 아비투스로 여겨진다는 것은 둘째 치고 말이다. 당신이 비트코인을 에어-갭 지갑에 모으고 있다면 누군가가 이 소중한 비트코인을 해킹하는 가장 쉬운 방법이 있다. 바로 당신을 해킹하는 것이다. 당신을 납치하고 협박하여 니모닉을 말하게 하고, 패스프레이즈를 말하게 하면 된다.

잘 보관된 비트코인을 컴퓨터로 해킹하는 것은 불가능에 가깝다. 왜냐하면 천문학적인 비용과 시간이 들어가기 때문이다. 무차별 대입 공격brute-force attack에 들어가는 비용을 따져보자면, 전 세계 에너지 사용량을 다 합쳐도 안 되는 수준임은 물론이고 우리 태양계를 전부 에너지 발전소로 바꿔도 어려운 일이다. 시간으로 따져보자면 빅뱅부터 지금까지의 시간(약 138억 년)이 여러 번 반복되어도 어려운 일이다. 따라서 가장 저렴한 해킹 방법은 그냥 5천 원짜리 둔기를 산 뒤 비트코인이 많이 있는 것이 확실한 사람을 공격하는 것이다. 이를 '5달러 렌치 공격'이라고 한다.

비트코인이 매우 중요해진 사회를 생각해 보자. 약탈 이익이 극대화될 때는 이런 공격에 대한 동기가 커진다. 단순히 생각해 봐도 리스크가 동일하다면 5천만 사토시가 있는 사람보다는 50억 사토시가 있는 사람을 공격하는 편이 좋지 않겠는가.

따라서 비트코인 세계에서는 수량을 말하는 것을 피해야 하는 것이 암묵적인 규칙처럼 여겨진다. 물론 말하는 것은 자신의 자유지만 그에 따르는 결과도 얼마든지 책임질 각오가 되어 있어야 한다.

가끔 평단가를 묻는 사람들이 있는데, 개인 지갑을 사용하면 평단가를 알 수가 없다. 따라서 평단가를 묻는 행위는 개인 지갑을 사용하지

않는다는 방증이며, 아직 비트코인에 대해 제대로 경험해본 적이 없다는 뜻이다. 평단가보다 수량이 중요하다. 만약 평단가나 수량에 대한 곤란한 질문을 받는다면 비트코인이 하나도 없다고 유쾌하게 답하거나 비밀이라고 답해도 된다.

KYC (고객 확인) 제도와 트래블 룰

비트코인의 프라이버시는 주소와 개인의 신원이 연결되지 않는 데서 온다. 그렇다면 국가가 계속 개인의 소비 내역을 감시할 수 있으려면 어떻게 해야 할까? 주소와 개인의 신원을 연결하면 된다. 백서에도 적혀 있다. "어떤 키의 소유자가 드러나면, 이 연결 고리가 동일 소유자의 다른 거래들도 드러낼 수 있는 위험이 있다." 그래서 대한민국을 비롯한 몇몇 국가들에서는 거래소가 고객 신원 확인KYC, Know Your Customer(이하 KYC)을 의무적으로 실시한다. 각 국가들은 지갑 주소와 개인 신원을 연결하기 위해 온 힘을 다하고 있다. 자금 세탁이나 범죄를 막기 위함이라는 명분으로 말이다. 감시할 수 있는 수단을 확보하기 위해 국가는 계속 KYC 제도를 강제할 것이다.

트래블 룰은 대한민국에서 가장 빠르게 비트코인 거래에 제도화되었다. 이는 자금 세탁을 방지하기 위한 것이라고 명시하고 있다. 트래블 룰은 거래소에서 다른 주소로 비트코인이 이동할 때 송/수신자의 정보를 반드시 함께 전송하도록 요구하는 규제다. 트래불 룰 때문에 본인의 신원과 일치하는, 고객 인증이 완료된 지갑 주소로만 비트코인을 전송할 수 있다. 한국 거래소들은 여기에 더해 신원이 일치하더라도 입출금을 처리해 주지 않고 자금 출처를 묻거나 머그샷을 찍게 하는 등의 만행을 저지르고 있다.

따라서 한국에서는 자금 세탁을 방지한다는 이유로 등장한 각종 규제 때문에 거래소에서 등록되지 않은 개인 지갑으로 비트코인을 바로 전송할 수가 없다. 반대 방향도 마찬가지다. 개인 지갑에서 국내 거래소로 비트코인을 바로 전송할 수가 없다. 한국 거래소의 신원과 동일한 신원이 인증된 해외 거래소로 먼저 비트코인을 보내고, 그 해외 거래소에서 개인 지갑으로 비트코인을 보내야 한다.

한국 거래소에서 해외 거래소로 보낼 때는 보통 비트코인보다는 '테더'를 이용한다. 이유는 한국 거래소들이 라이트닝 네트워크 전송을 지원하지 않고, 비트코인 출금 수수료는 비싼 반면 테더 출금 수수료는 저렴하기 때문이다.

라이트닝 네트워크와 인보이스, 라이트닝 주소

비트코인은 거래가 컨펌되기까지, 즉 블록이 채굴되기까지 평균적으로 10분을 기다려야 한다. 평균적으로 10분이기 때문에 컨펌되기까지 40분이 걸릴 수도 있고, 운이 좋아 2분 만에 컨펌될 수도 있다. 이는 정산의 측면에서 보면 매우 빠르다. 하지만 결제의 관점에서는 느리게 느껴질 수 있다.

속도와 수수료 문제를 해결하기 위해 라이트닝 네트워크Lightning Network, LN가 나왔다. 라이트닝 네트워크는 비트코인을 훨씬 빠르게 전송할 수 있는 기술이다. 라이트닝 네트워크를 이용하는 방법은 라이트닝 지갑 수탁 서비스를 이용하거나 자신이 직접 라이트닝 노드를 운영하는 것이다. 라이트닝 지갑 수탁 서비스에는 대표적으로 월렛 오브 사토시, 블링크, 스피드 등이 있다.

온-체인 거래와 라이트닝 네트워크 거래는 다르다. 온-체인은 비트코인을 주고받을 때 '주소'를 이용해 거래한다. 하지만 라이트닝 네트워크를 이용한 전송에서는 주소가 아니라 '인보이스'를 사용한다. 인보이스는 메모나 금액과 같은 정보도 포함할 수 있다. 그리고 인보이스는 일회용이다.

인보이스는 재활용이 불가능하기 때문에 상시 사용하는 라이트닝 주소도 있다. 라이트닝 주소는 ~@walletofsatoshi.com과 같은 주소를 말한다.

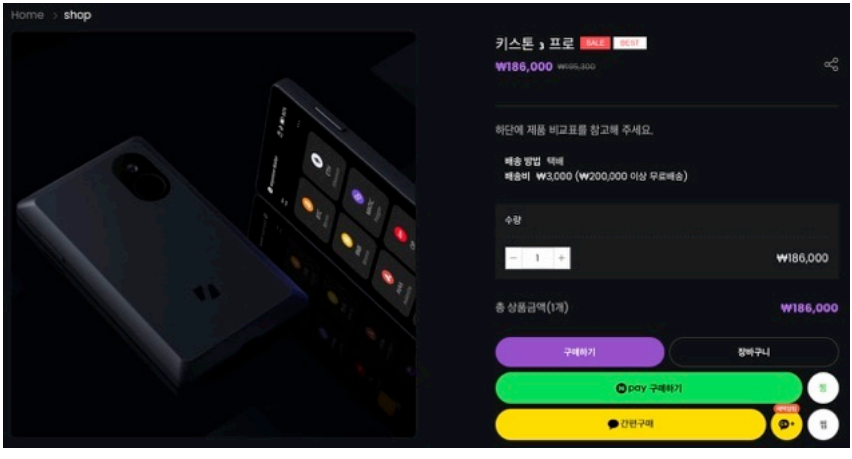
여기까지가 셀프 커스터디를 위해 알아야 할 지식이다. 처음 보는 내용이 많았을 수도 있지만 괜찮다. 앞에서 이야기했듯이 차근차근 연습하다 보면 체득하게 될 것이다. 이제 본격적으로 지갑 사용법을 알아보자.

| 키스톤 지갑

키스톤은 대한민국에서 입문자들이 가장 많이 선택하는 지갑이다. 터치 스크린 방식이 편리하고 QR 인식률이 높기 때문이다. 키스톤 사용 방법에 대해 알아보자.

필수 준비물

1. 키스톤 3 프로



2. 마이크로SD카드와 리더기

마이크로SD카드는 8GB를 추천한다. 앞으로 비트코인에 점점 깊게 빠질수록 마이크로SD카드는 쓸 일이 많다. 집에 없다면 '마이크로SD카드 8GB'랑 'SD카드 리더기'를 검색해서 구매하면 된다. 노트북 같은 경우 마이크로SD카드를 꽂는 칸이 있기도 한데, 그러면 리더기는 안 사도 된다. (다음 사진 참고)

권장 준비물

1. 주사위

주사위는 1개여도 상관없다. 하지만 많을수록 편하다. 니모닉을 만들면서 주사위를 총 50-100번 던져야 하는데 주사위가 많으면 한 번에 던질 수 있기 때문이다.

2. 5V 1.2A C타입 충전기

키스톤 충전 규격은 5V 1A다. 원래 전류 단위인 A는 좀 높아도 된다. 키스톤 측에서는 5V 2A까지 괜찮다는데 필자의 경험상 5V 1A가 제일 충전이 잘 됐다.

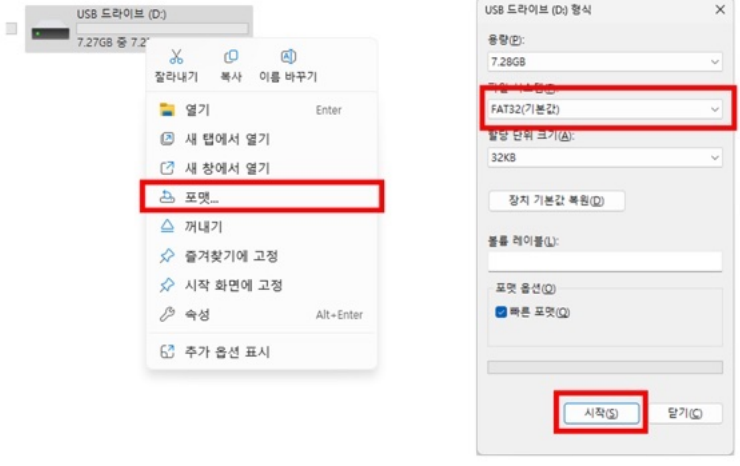
또한, 필자의 주관적 의견으로는 중간에서 이상한 짓 하기 힘든 일체형이 좋다고 생각한다. '5V 1.2A C타입 충전기'라고 검색해서 하나 구매하면 된다. (다음 사진 참고)

준비물을 마련했다면 본격적으로 지갑을 만들어보자. 먼저 배송 과정에서 변조가 없었는지 확인하고, 펌웨어 업데이트를 할 것이다.

업데이트를 위한 마이크로SD카드 준비

마이크로SD카드를 리더기에 연결하고 컴퓨터에 꽂는다.

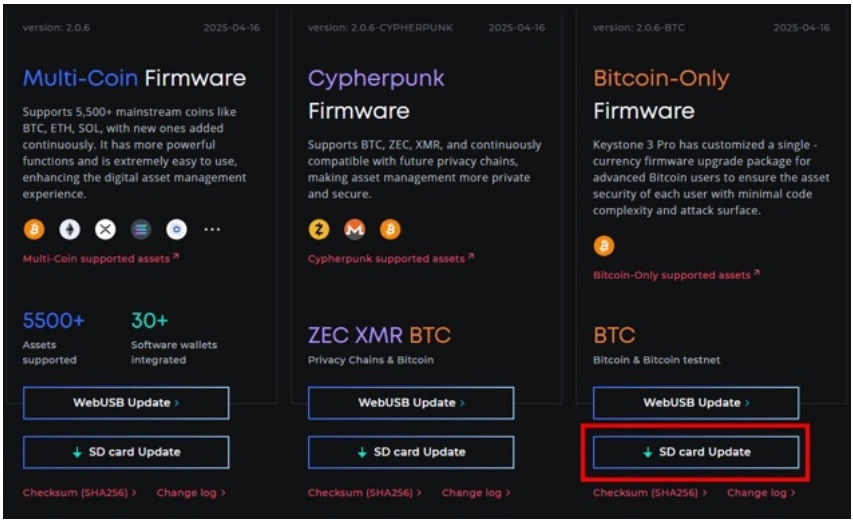
먼저 SD카드를 FAT32 형식으로 포맷해야 한다. 내 컴퓨터(혹은 내 PC) → SD카드 우클릭 → [포맷]을 누른다. 그다음 파일 시스템에서 [FAT32]를 선택하고 [시작]을 누른다. 경고가 뜨면 확인을 누르면 된다.



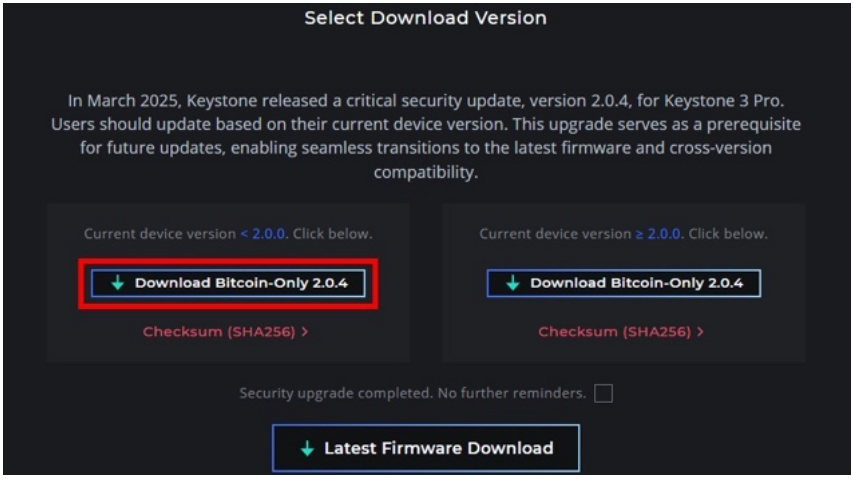
컴퓨터에서 다음 웹사이트에 접속한다.

https://keyst.one/firmware

스크롤을 아래로 내려 'Bitcoin Only Firmware' 아래에 있는 [SD Card Update]를 누른다.



키스톤을 처음 구매했을 경우 보통 펌웨어 버전이 2.0.0 이전일 것이다. 따라서 'Current device version 〈 2.0.0.' 아래에 있는 [Download Bitcoin-Only 2.0.4]를 누른다.



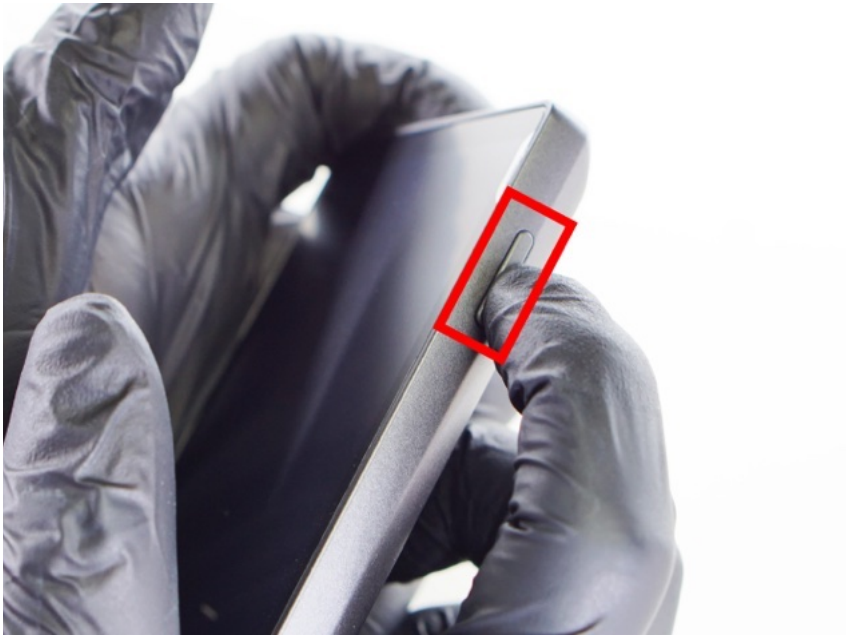
keystone3.bin이라는 파일이 다운로드 되었다. 다운로드한 파일을 SD카드에 복사한다. 주의할 점이 있다. 파일을 여러 번 다운로드할 경우 keystone3(1).bin 이런 식으로 뒤에 숫자가 붙는데, 숫자가 붙은 파일을 SD카드에 복사하면 안 된다.

이제 업데이트를 위한 마이크로SD카드가 준비되었다. 마이크로SD카드를 컴퓨터에서 분리하고, 키스톤 좌측에 꽂는다.

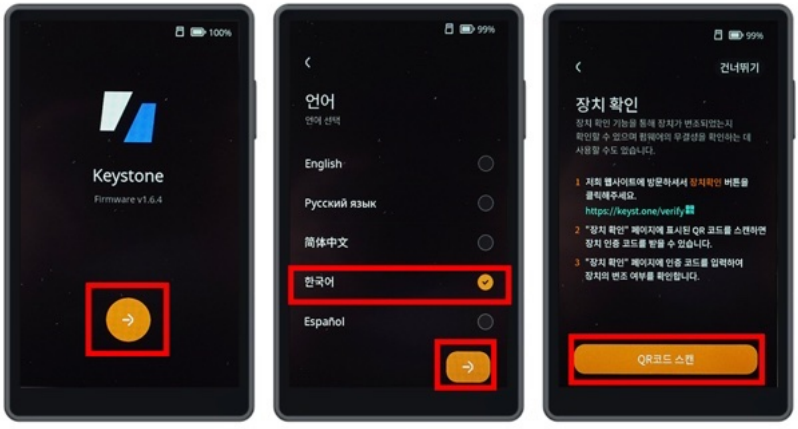
기기 검증

우리는 앞으로 니모닉을 만들고 니모닉으로부터 파생된 주소에 비트코인을 보낼 것이다. 그런데 불안함이 들지 않는가? 혹여나 배송 과정에서 어떤 해커가 몰래 키스톤 기기에 악성 코드를 심거나, SD카드에 다운로드한 업데이트 파일에 악성 코드가 심겨 있으면 어떡할까? 이를 확인하기 위해 기기 변조가 일어난 적은 없는지, 펌웨어 변조는 일어나지 않았는지 확인할 것이다.

이제 키스톤 우측 버튼을 꾹 눌러서 키스톤의 전원을 켜자.



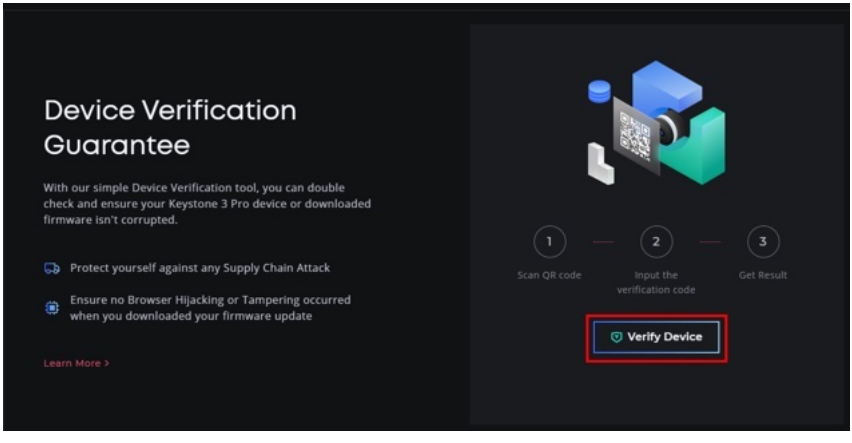
언어는 한국어로 설정한다. 장치 확인 창이 나오면 [QR 코드 스캔]을 누른다.



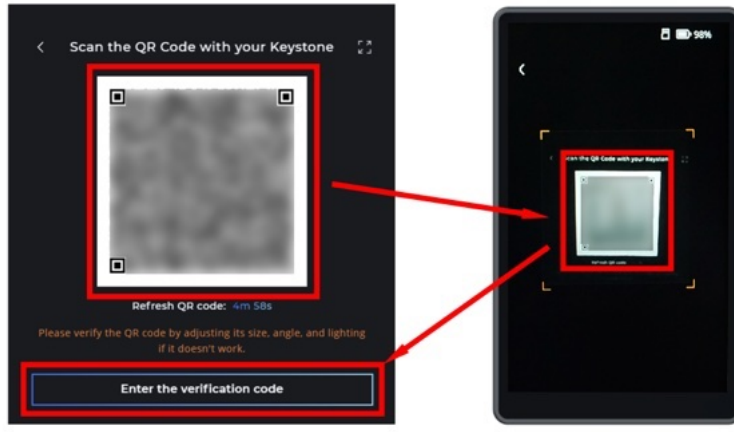
PC에서 다음 웹사이트에 접속한다.

https://keyst.one/authentication

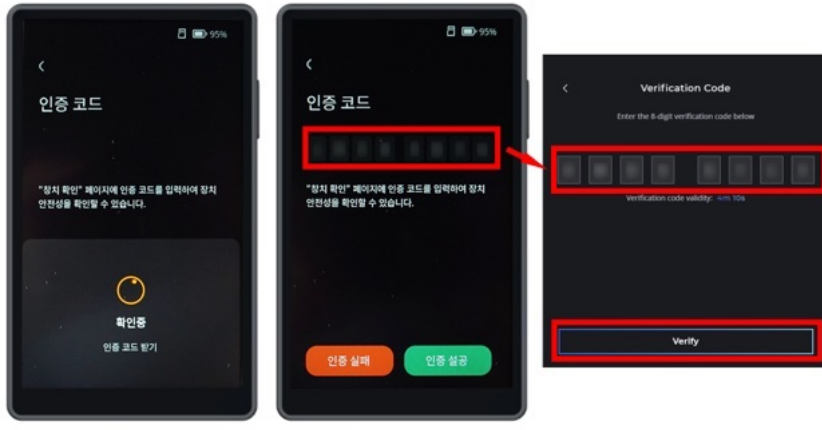
[Verify Device]를 누른다.



화면에 뜨는 QR 코드를 키스톤으로 스캔한다.



잠시 기다리면 키스톤 화면에서 8자리 코드가 나온다. 이 코드를 PC에 나오는 화면에 입력하고, [Verify]를 누른다.

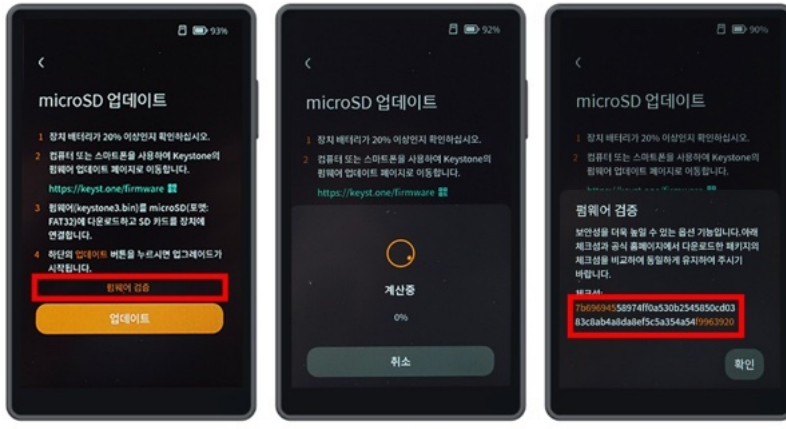


아래와 같은 화면이 뜬다면 기기 변조가 발생하지 않았다는 뜻이다. 이제 키스톤에서 [인증 성공]을 누르고 펌웨어 업데이트를 해보자.

펌웨어 2.0.4 검증 및 업그레이드

이제 펌웨어 업그레이드를 하기 전에 펌웨어 검증을 할 것이다. 컴퓨터에 SD카드가 잠깐 연결되어 있는 사이에 업그레이드 파일에 변조가 일어났을지 모르는 일이다. 이런 일이 없었는지 검증을 해보자. 이 과정을 건너뛰고 싶다면 바로 [업데이트]를 누르면 된다.

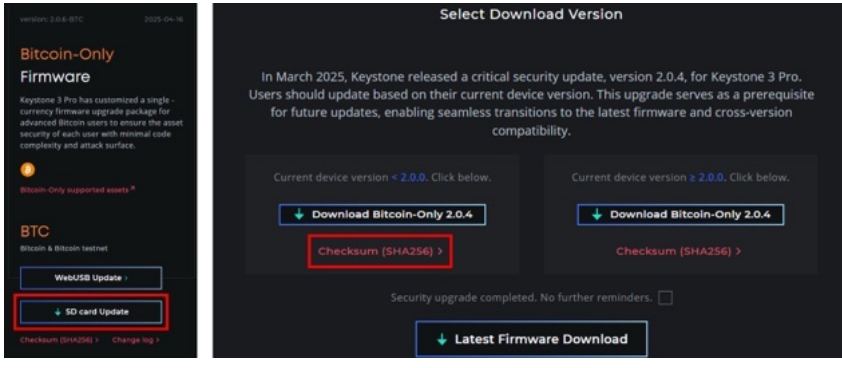
[펌웨어 검증]을 눌러보자. '계산 중' 화면이 뜨고 나서 체크섬 밑에 어떤 코드가 보인다.



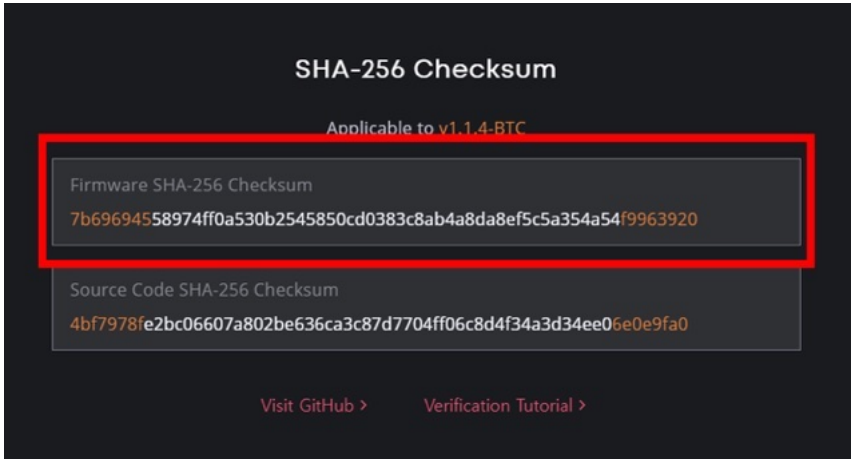
업그레이드 파일을 다운로드했던 링크로 다시 들어간다.

https://keyst.one/firmware

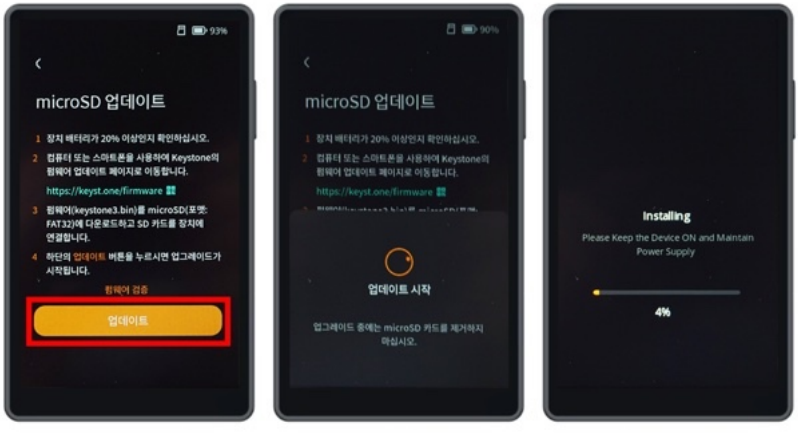
'Bitcoin-only Firmware' 아래에 있는 [SD card Update]를 누르고, 아래에 있는 [Checksum (SHA-256)]을 누른다.



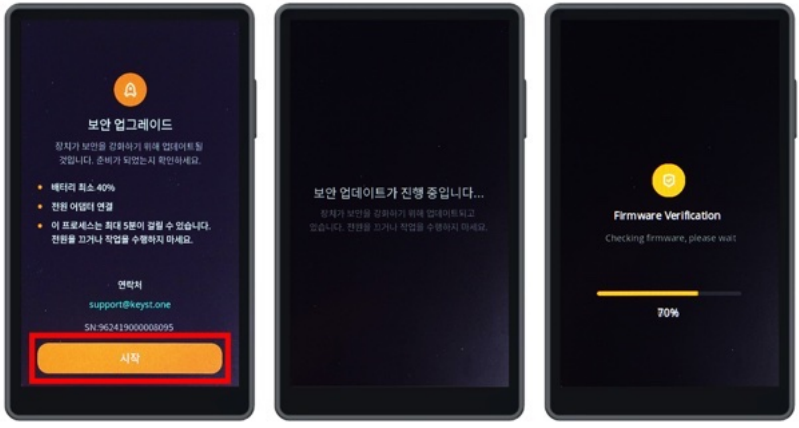
그러면 어떤 코드가 적혀 있는 창이 나온다. 이 코드가 키스톤에 표시된 코드와 일치한다면 변조가 일어나지 않은 것이다.



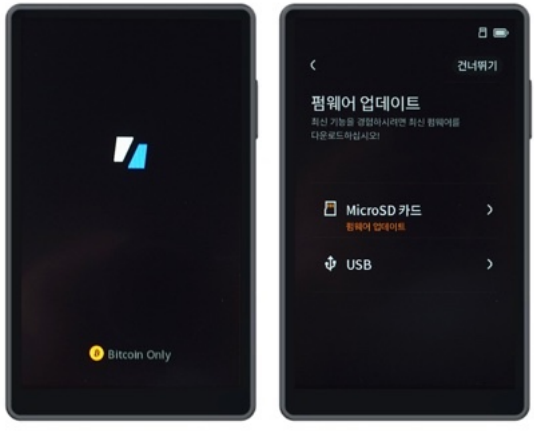
이제 펌웨어 검증까지 완료했으니 펌웨어 업그레이드를 하자. [업데이트]를 누른다.



펌웨어 버전 2.0.0 이후부터는 보안 업그레이드 화면이 나타날 수도 있다. 이때 충전 전원선이 연결되어 있어야 한다. 장치에 연결할 건지 안내 창이 나오면 [지금 안 함] 버튼을 누른다. 이 안내창은 설정에서 에어갭 모드를 켜고 나면 안 뜰 것이다. [시작]을 누르면 알아서 펌웨어 검증을 한다.



잠시 후에 화면이 꺼졌다가 켜진다.

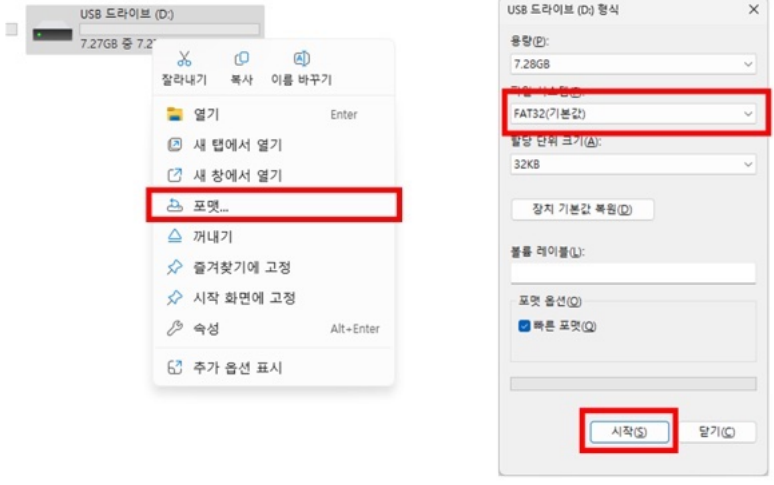


최신 펌웨어 업데이트

지금은 2.0.4 이후의 버전이 나왔다. 따라서 최신 펌웨어로 업데이트를 다시 해줘야 한다. 2.0.4로 업그레이드하는 건 앞으로의 펌웨어 업데이트를 위해 필수적인 과정이었다. 2.0.4로 업그레이드를 했으면 새로운 펌웨어가 나올 때마다 다음과 같은 방법으로 업데이트하면 된다. 최신 버전으로 업데이트하는 방법은 앞의 내용과 거의 똑같다.

마이크로SD카드를 빼서 컴퓨터에 다시 꽂는다.

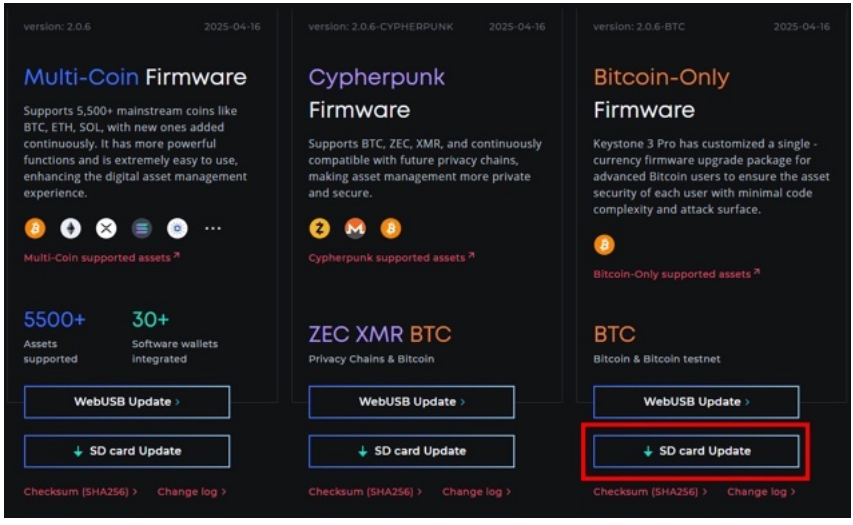
먼저 마이크로SD카드를 포맷할 것이다. 내 컴퓨터(혹은 내 PC) → SD 카드 우클릭 → [포맷]을 누른다. 그다음 파일 시스템에서 [FAT32]를 선택하고 [시작]을 누른다. 경고가 뜨면 확인을 누르면 된다.



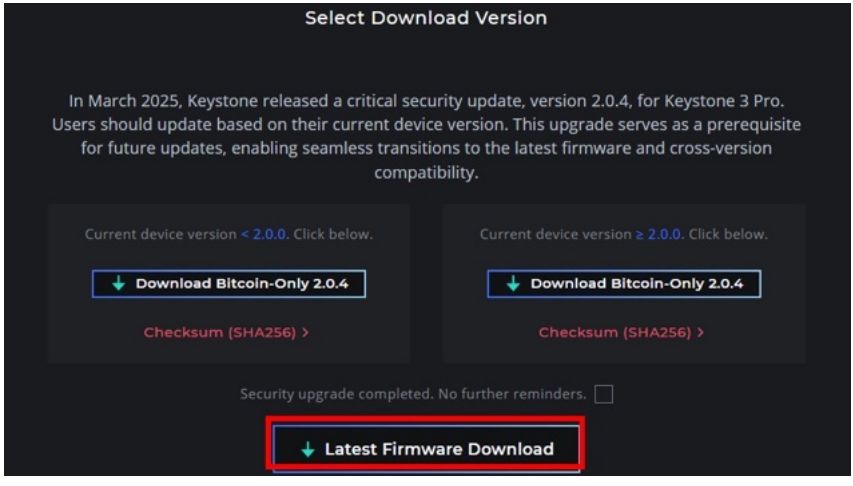
컴퓨터에서 다음 웹사이트에 접속한다.

https://keyst.one/firmware

스크롤을 아래로 내려 'Bitcoin Only Firmware' 아래에 있는 [SD Card Update]를 누른다.



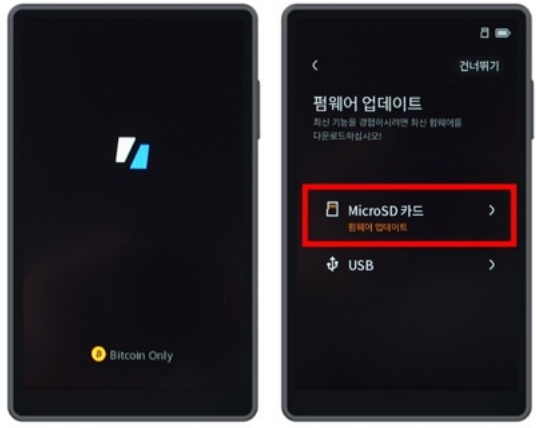
이제는 버전 2.0.4가 아니라 더 최신 버전으로 업데이트를 해야 한다. [Latest Firmware Download]를 누른다.



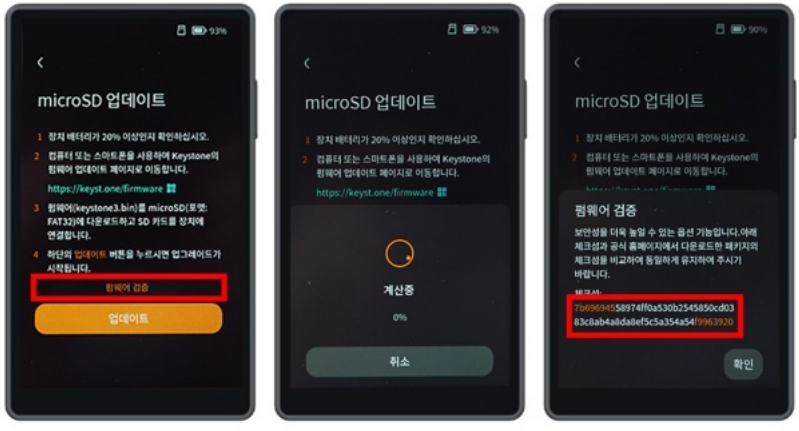
keystone3.bin이라는 파일이 다운로드 되었다. 다운로드한 파일을 SD카드에 복사한다. 앞서 언급했듯이 파일을 여러 번 다운로드할 경우 keystone3(1).bin 이런 식으로 뒤에 숫자가 붙는데, 숫자가 붙은 파일을 SD카드에 복사하면 안 된다. 이런 경우에는 먼저 다운로드 폴더에 있던 keystone3.bin 파일을 전부 지우고, 다시 keystone3.bin 파일을 다운로드하자.

이제 업데이트를 위한 마이크로SD카드가 준비되었다. 마이크로SD카드를 컴퓨터에서 분리하고, 키스톤 좌측에 꽂는다.

펌웨어 업데이트 화면에서 [MicroSD 카드 펌웨어 업데이트]를 누른다.



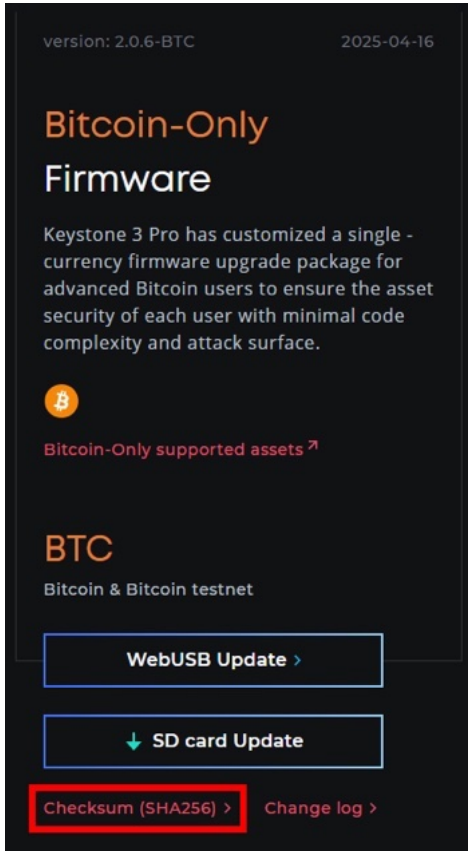
[펌웨어 검증]을 누른다.



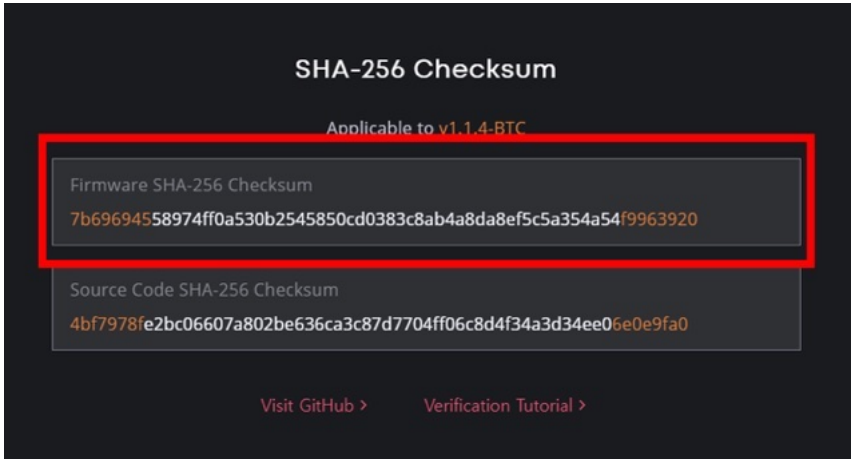
업데이트 파일을 다운로드했던 링크로 다시 들어간다.

https://keyst.one/firmware

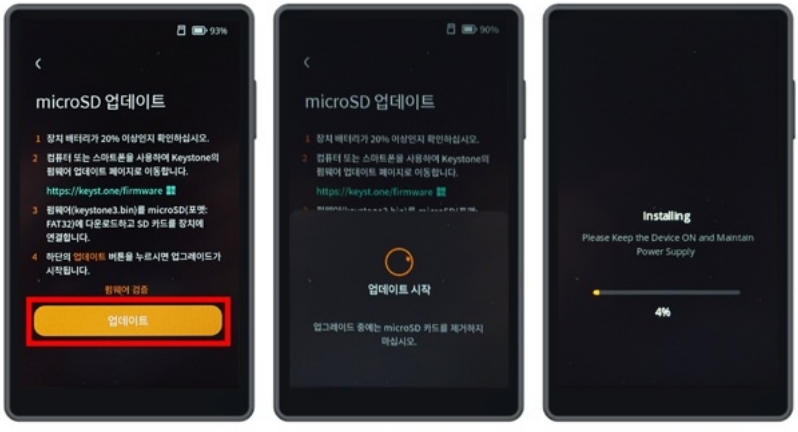
Bitcoin-only Firmware 아래에 있는 [Checksum (SHA-256)]을 누른다.



어떤 코드가 적혀 있는 창이 나온다. 이 코드가 키스톤에 표시된 코드와 일치한다면 변조가 일어나지 않은 것이다.



이제 펌웨어 검증까지 완료했으니 펌웨어 업데이트를 하자. [업데이트]를 누른다.



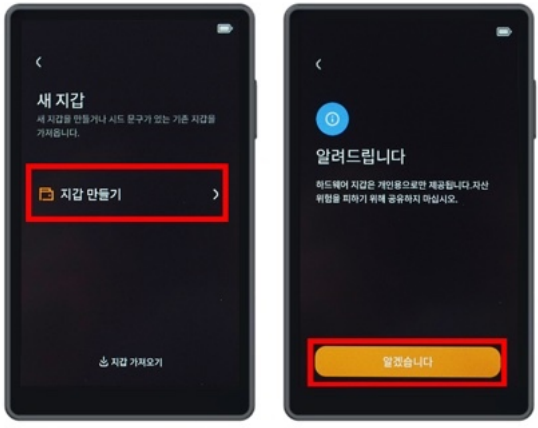
업데이트가 완료되면 마이크로SD카드를 제거한다.

펌웨어 업데이트도 완료되었으니 이제 본격적으로 니모닉과 지갑을 만들어보자.

지갑 생성

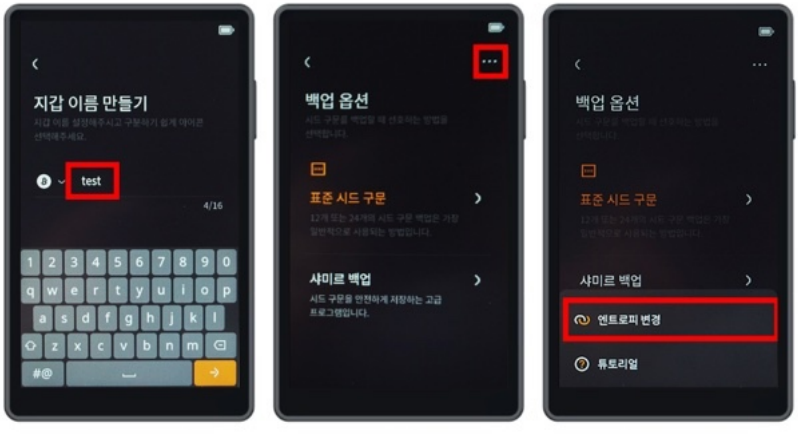
이제 지갑을 만들어보자. 주의할 점이 있다. 지갑을 만들 때는 어떠한 카메라, 녹음 장치 등이 없는 곳에서 하자. 필자는 주사위를 굴릴 때 전자기기가 아무것도 없는 방에 들어가 가족과 수신호로만 대화하며, 주사위 굴리는 소리가 나지 않도록 담요를 깔거나 침대 위에서만 진행한다.

키스톤에서 [지갑 만들기]를 누른다.

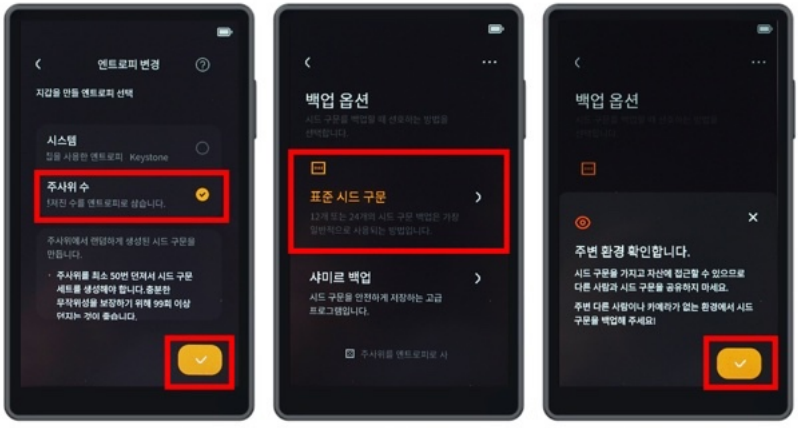


6자리 PIN 코드를 설정한다. 도둑이 키스톤 프로 3가 어디 있는지 알아서 기기를 훔쳐 가고 PIN 코드도 안다면 비트코인을 탈취할 수 있다. 그러니 보안을 생각해서 000000이나 123456 같은 PIN 코드는 설정하지 않도록 하자. 참고로 키스톤 프로 3는 최대 3개의 지갑을 만들 수 있다. 이때 각 지갑의 PIN 코드는 달라야 한다. (PIN 코드는 6번 틀리면 1분간 잠기고, 7번째에는 5분, 8번째에는 15분, 9번째에는 60분간 잠기며, 10번째에도 틀리면 기기가 초기화된다.)

지갑 이름을 설정하자. 자기 마음대로 설정하면 된다. 백업 옵션에서 넘어가기 전에 엔트로피 생성 방법을 변경할 것이다. 우리는 직접 주사위를 던져서 지갑을 만들 것이므로 이 화면에서 그냥 넘어가면 안 된다. 오른쪽 위 점 세 개 → [엔트로피 변경]을 누른다.



[엔트로피 변경]에서 [주사위 수]를 선택한다. 그다음 백업 옵션에서 [표준 시드 구문]을 선택한다.

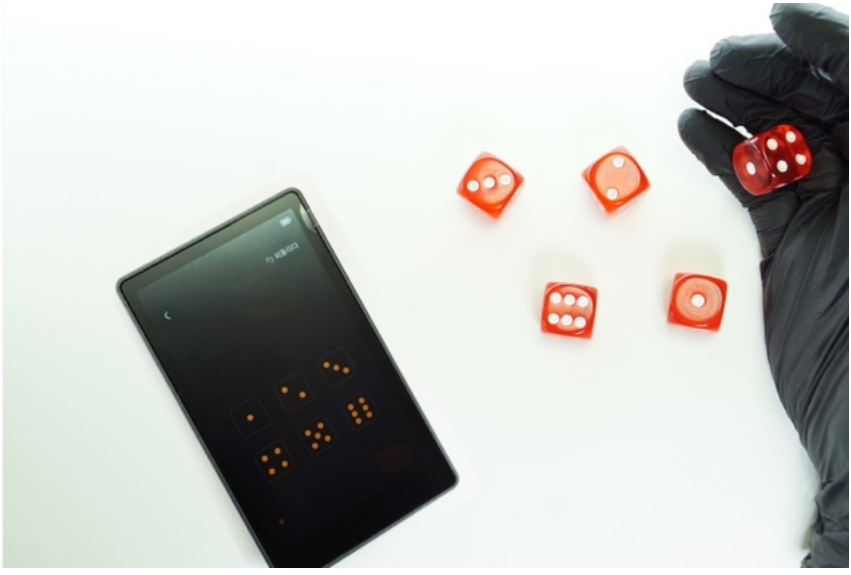


이제 주사위를 던져보자. 12단어 니모닉을 만들 것이라면 50번 이상, 24단어 니모닉을 만들 것이라면 100번 이상 주사위를 던지면 된다. 그 이상 던져도 보안이 더 높아지진 않는다.

어떤 다른 사람이 주사위를 50번 연속으로 당신과 똑같이 던질 확률은 로또 1등에 당첨될 확률보다 9,000만×1조×1조 배 더 희박하다. 우주에서 이런 일이 일어나는 것은 불가능하다.

니모닉 단어 수에 대해 이야기해보겠다. 12단어로 할지 24단어로 할지 고민이 될 것이다. 필자는 주변인에게 셀프 커스터디를 알려줄 때, 12단어는 충분한 것이고, 24단어는 과도한 것이라고 말한다. 앞에서 본 확률처럼 12단어(주사위 50번)도 똑같이 재현하는 것은 불가능하다. 그러나 보안에 있어서는 과도한 것도 나쁘지 않다. 12단어는 외우기 쉽다는 장점이 있으므로 자신이 선택하면 된다. 비트코인은 자신이 온전히

통제권을 갖는 것이므로, 누군가 정해줄 수 없고 자신이 직접 선택해야 할 일이 많다. 다만 12단어로 할 때는 꼭 주사위를 50번 이상 던지고, 24단어로 할 때는 꼭 주사위를 100번 이상 던지자.



주사위를 다 굴리고 다음으로 넘어가면 '시드 구문 백업'이 나올 것이다. 여기 나와 있는 단어들이 '니모닉'이라고 하는 것이다. 먼저 오른쪽 위에서 24단어로 할지, 12단어로 할지 선택하자. 필자는 이번에 12단어를 선택했다.

이제 니모닉을 어딘가에 적어놓자. 이 니모닉은 절대 누군가에게 노출되어서는 안 된다. 다시 말하겠다. 니모닉은 절대 누군가에게 노출되어서는 안 된다. 누군가 도움을 준다고 하며 니모닉을 요구해도 절대로 주면 안 된다.

니모닉이 노출되면 나중에 여기에 비트코인을 보냈을 때 해커가 당신의 소중한 비트코인을 탈취할 수 있다. 앞에서 말한 것처럼 카메라나 녹음 장치 등을 조심해야 한다. 카메라 렌즈가 니모닉 단어들을 향하지 않도록 하고, 니모닉 단어를 입으로 소리 내어 말하지 않도록 한다.

지금은 종이로 적어놓지만, 언젠가는 외우는 것이 좋다. 집에 불이 나서 니모닉을 적어놓은 종이가 타버릴 것에 대비해 철판에 새기기도 한다. 그만큼 니모닉은 중요하다.

니모닉은 순서도 중요하다. 순서를 헷갈리면 나중에 복구가 어려워질 수도 있다.

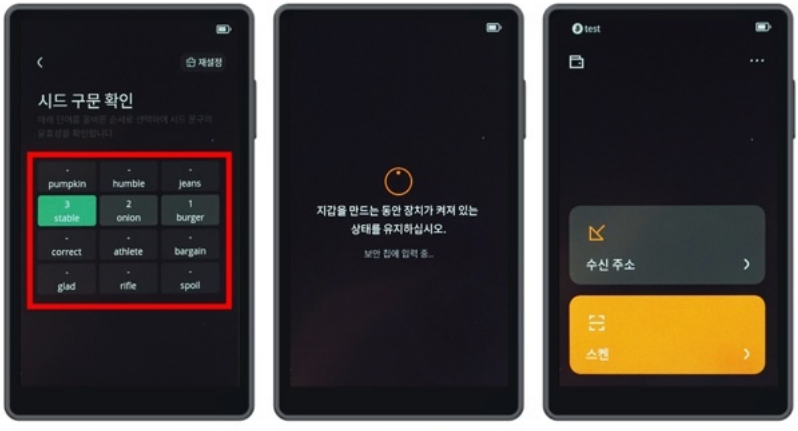
아래 주의 사항을 꼭 읽어보자.

1. 절대로 니모닉을 사진 찍지 않는다.
2. 절대로 니모닉을 소리 내어 읽지 않는다.
3. 절대로 니모닉을 전자기기(메모장 앱) 등에 기록하지 않는다.
4. 니모닉을 적은 종이는 자신의 통제하에 있는 곳에 안전하게 보관한다. 다른 누군가에게 종이의 위치를 발설하지 않는다.
5. 니모닉을 외우지 못했다면 철판 등에 니모닉을 백업하는 것도 고려하자.
6. 누군가 니모닉을 알려달라고 요구한다면 어떠한 경우에도 절대 응하지 말자.

니모닉만 있다면 키스톤 기기가 고장 나도 얼마든지 다른 기기로 자신의 비트코인을 복구할 수 있다.

이 사진에 나와 있는 니모닉을 절대 사용하지 말 것. 이 니모닉은 테스트용으로 쓰였으며 온라인에 노출되었다. 이 니모닉에서 파생되는 주소에 비트코인을 보내면 영영 되찾지 못할 수도 있다.

'시드 구문 확인'에서 니모닉 단어를 순서대로 누른다. 이는 사용자가 니모닉을 잘 적었는지 확인하기 위한 과정이다. 다 누르고 나면 지갑이 만들어진다.

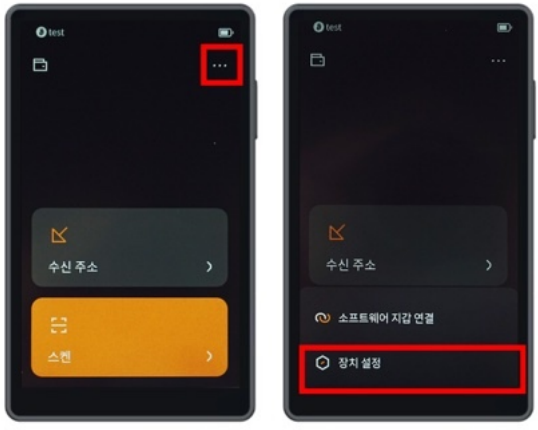


축하한다. 이제 당신만의 지갑이 완성되었다. 이제 주소도 확인하고 비트코인을 빨리 보내보고 싶은 마음이 크겠지만, 아직 할 일이 남았다. 꼭 복구 연습을 먼저 해보고 나서 비트코인을 본격적으로 보내봐야 한다. 나중에 갑작스럽게 기기가 망가졌을 때 처음 복구하게 되면 큰 혼란에 빠질 수 있기 때문이다.

따라서 워치-온리 지갑에 확장 공개키를 내보내고, 소액의 비트코인을 보내본 뒤 일부러 지갑을 초기화하고 복구해 볼 것이다.

키스톤 사전 설정

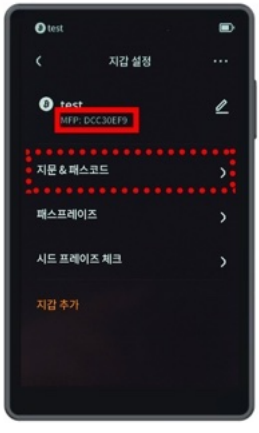
지갑을 본격적으로 사용하기 전에 몇 가지 설정을 하고 가자. 홈 화면에서 오른쪽 위 점 세 개를 누르고, [장치 설정]을 누른다.



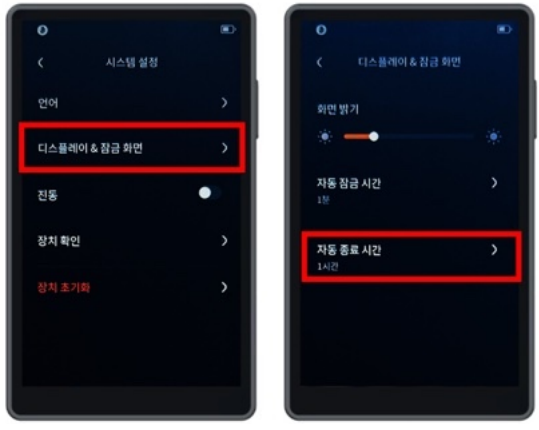
[연결]에 들어가 [에어갭 모드]를 활성화한다. 이 모드를 켜면 USB 연결을 통해 데이터에 접근할 수 없고 충전만 가능하다.

뒤로 가기를 누른 후 [지갑 설정]에 들어간다. 여기서 지문 설정을 할 수 있다.

이제 여기 보이는 MFP를 기록할 것이다. MFP는 자기 지갑이 맞는지 쉽게 검증할 수 있도록 하는 역할을 한다. 필자는 니모닉과 함께 적었다.



마지막으로 '시스템 설정' → [디스플레이 & 잠금 화면] 설정에 들어가서 [자동 종료 시간]을 1시간으로 설정한다. 키스톤은 전원이 켜져 있기만 해도 배터리가 금방 닳아서 방전된다. 따라서 사용할 때마다 기기를 켜고, 사용하지 않을 때는 알아서 기기가 꺼지도록 이렇게 설정하는 것이다.



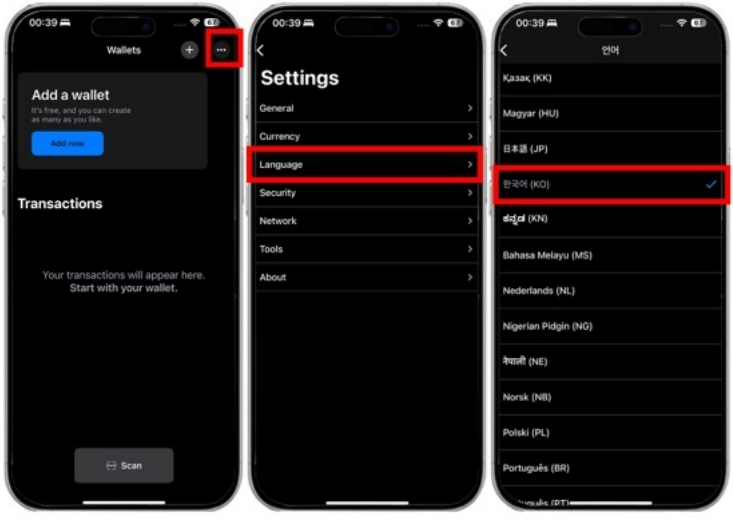
사전 설정은 끝났다. 이제 워치-온리 지갑에 확장 공개키를 내보낼 것이다.

블루월렛에 확장 공개키 내보내 워치-온리 지갑 만들기

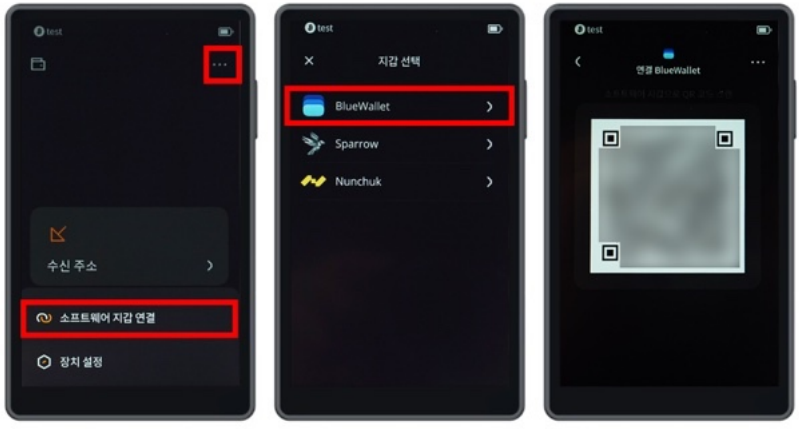
스마트폰에서 사용하는 워치-온리 지갑에는 블루월렛과 넌척, 코코넛 월렛 등이 있다. 블루월렛은 잔오류가 많다는 단점이 있지만, 현재 한국어를 지원하기 때문에 영어가 불편한 사람들은 편하게 사용할 수 있다. 넌척은 블루월렛보다 훨씬 안정성이 있지만 한국어 지원이 안 돼서 영어를 못하는 경우 불편하다. 코코넛 월렛은 한국의 포우팀에서 개발한 지갑으로, 당연히 한국어가 지원되고 기능도 많다(심지어 고객센터도 있다). 워치-온리 지갑은 어느 하나만 사용하는 것보다는 두 가지 이상을 사용하며 교차 검증하는 것이 좋다.

블루월렛과 넌척, 코코넛 월렛을 먼저 설치하자. 구글 플레이스토어나 애플 앱스토어에서 BlueWallet, Nunchuk, 코코넛 월렛을 검색하고 다운로드한다. iOS 기준으로 설명하지만, 안드로이드도 크게 다르지 않다.

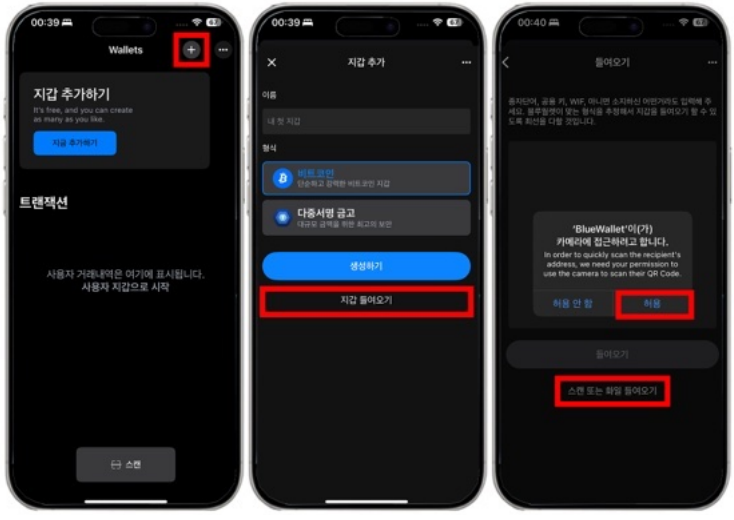
블루월렛 앱을 실행한다. 한국어가 편하다면 언어 설정부터 바꾸자. 오른쪽 위 점 세 개 → [Language] → [한국어]를 선택하고 뒤로 가기를 누른다.



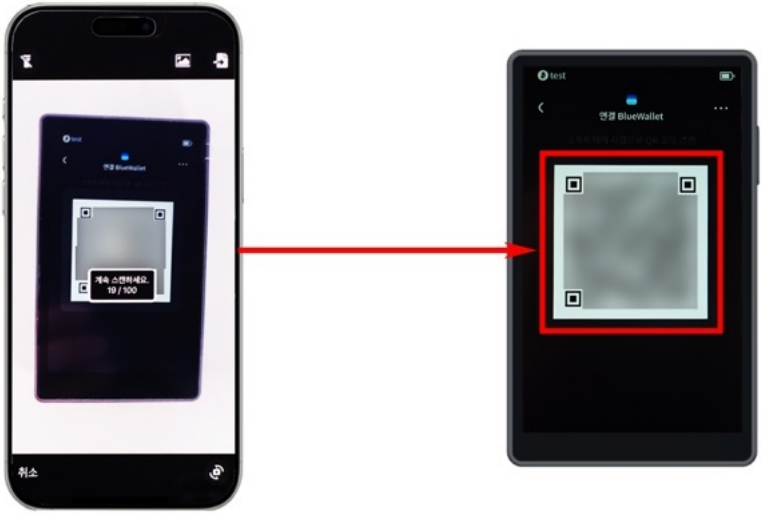
키스톤 기기 홈 화면에서 오른쪽 위 점 세 개 → [소프트웨어 지갑 연결] → [BlueWallet]을 선택한다. 그러면 QR 코드가 계속 바뀔 것이다.



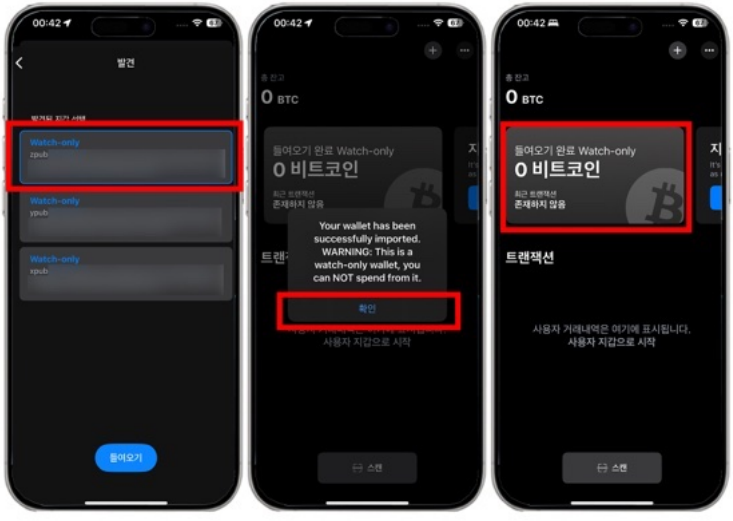
스마트폰의 블루월렛에서 우측 상단 [+] → [지갑 들여오기] → [스캔 또는 화일 들여오기] → 카메라 [허용]을 누른다.



블루월렛에서 카메라 화면이 뜨면 키스톤에 나오는 QR 코드를 찍는다. 이것이 확장 공개키를 내보내는 과정이다.



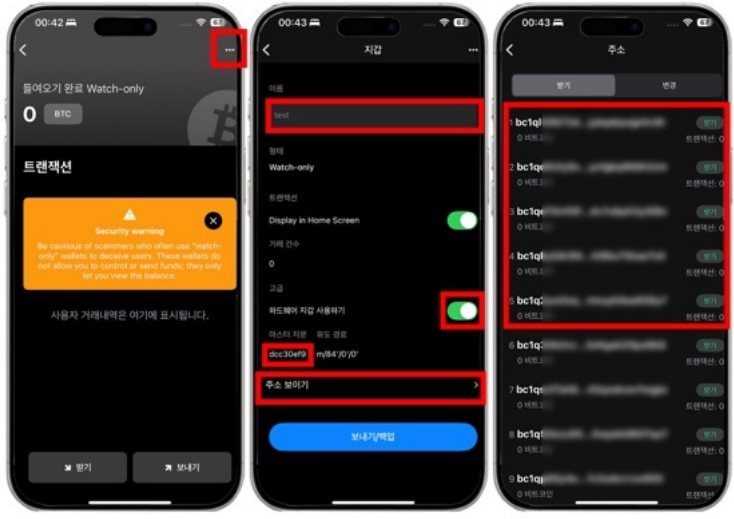
우리는 네이티브 세그윗 주소로 만들었으므로(키스톤에서 기본 설정이 네이티브 세그윗 주소: 84로 되어 있다) 맨 위의 [zpub]을 선택한다. 경고창이 나오면 [확인]을 누른다. 경고창은 현재 서명 기능이 꺼져있다는 뜻이다. 잘 들여와졌으면 지갑을 누른다.



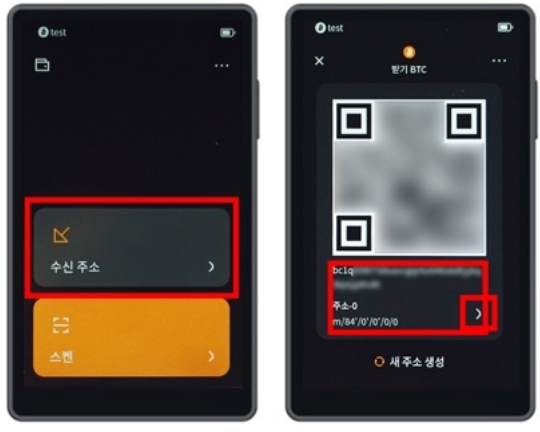
지갑에 들어와서 오른쪽 위 점 세 개를 누른다. 지갑의 이름을 설정한다.

[하드웨어 지갑 사용하기]를 켠다. 앞에서 나온 경고창이 이 옵션 때문에 떴던 것이다. 이 옵션을 켜야 키스톤에서 서명을 받아올 수 있다. 마스터 지문 아래에 있는 [보기]를 눌러 MFP를 확인한다. 키스톤에서 확인했던 MFP와 동일한지 확인한다. 대소문자는 상관없다.

[주소 보이기를 누르면] 주소 목록이 나온다.



블루월렛에서 보이는 주소들과 키스톤에서 보이는 주소들이 같은지 한번 확인해 보자.

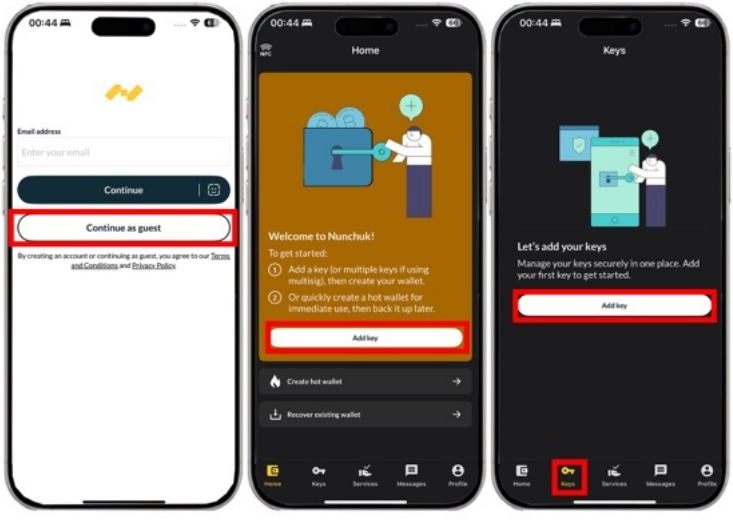


이제 워치-온리 지갑인 블루월렛과 키스톤 연동이 끝났다. 앞으로 블루월렛에서 '받기'를 누르고 비트코인을 받으면 된다. 하지만, 일단 소액만 보내보고 복구 연습을 한 뒤에 본격적으로 사용하길 바란다.

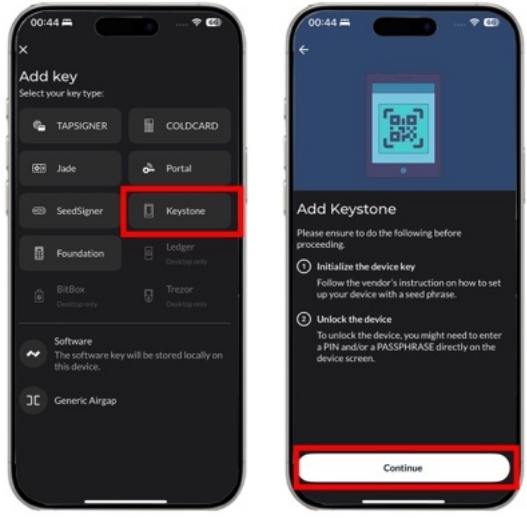
넌척에 확장 공개키 내보내 워치-온리 지갑 만들기

이제 워치-온리 지갑인 넌척과 키스톤을 연동해 보자. 앞에서 설치했던 넌척을 켠다. 우리는 게스트 모드로 넌척을 사용할 것이다. 어차피 얼마든지 키스톤과 넌척을 연동할 수 있으므로 로그인이 필요 없기 때문이다. [Continue as guest]를 누른다.

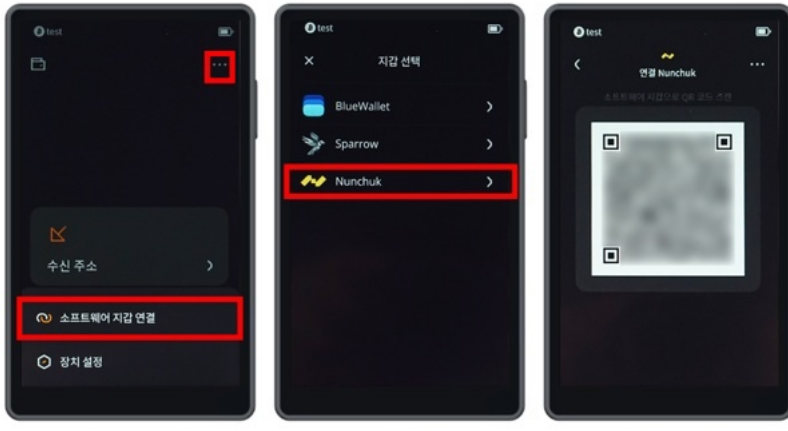
이후 화면에서 [Add key] 버튼이 보인다면 바로 누르고, 안 보인다면 아래 탭에서 [Keys]를 누른 뒤 [Add key]를 누른다.



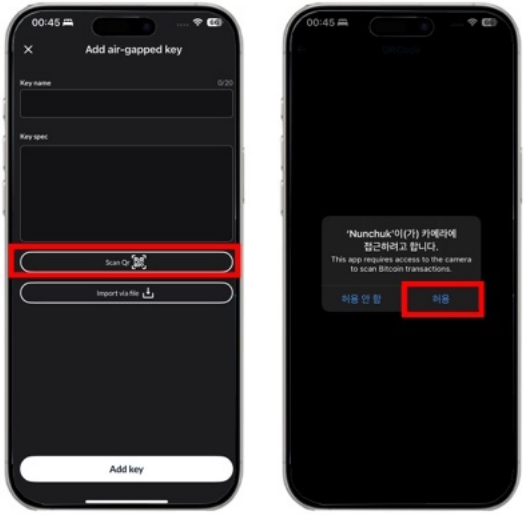
기기를 선택하는 창이 나오면 [Keystone]을 선택한다. 이후에 [Continue]를 누른다.



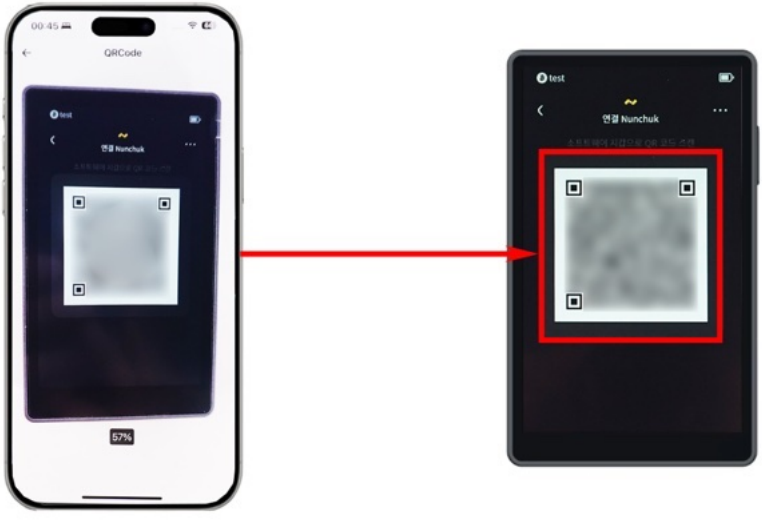
이제 키스톤 홈 화면에서 오른쪽 위 점 세 개 → [소프트웨어 지갑 연결] → [Nunchuk]을 누른다. 앞에서와 마찬가지로 움직이는 QR 코드가 나올 것이다.



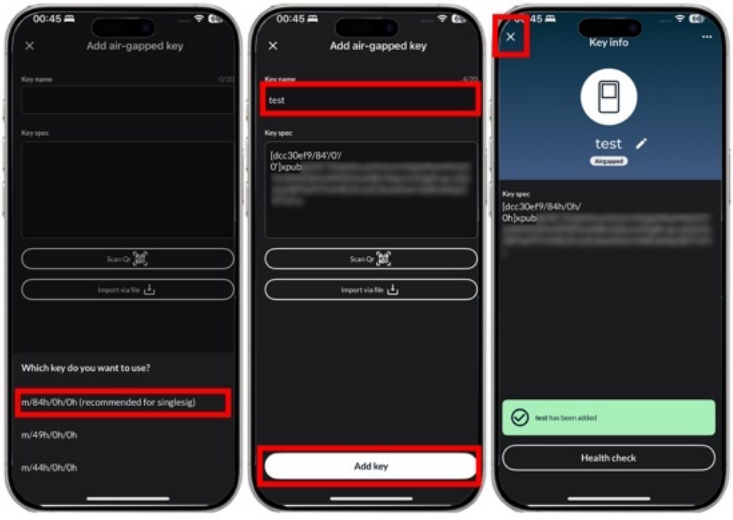
넌척에서 [Scan Qr]을 누른다. 카메라 접근 권한을 요구하면 [허용]을 누른다.



넌척에서 카메라 화면이 뜨면 키스톤의 QR 코드를 스캔한다.

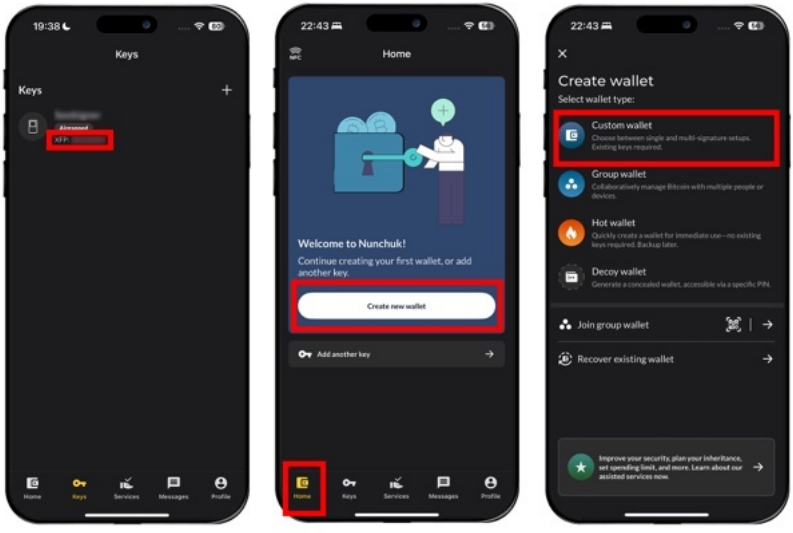


파생 경로는 [m/84h/0h/0h]를 선택한다. 그다음 나오는 창에서 지갑 이름을 설정하고, 아래에 있는 [Add key]를 누른다. 그다음 왼쪽 위 [x] 버튼을 누른다.

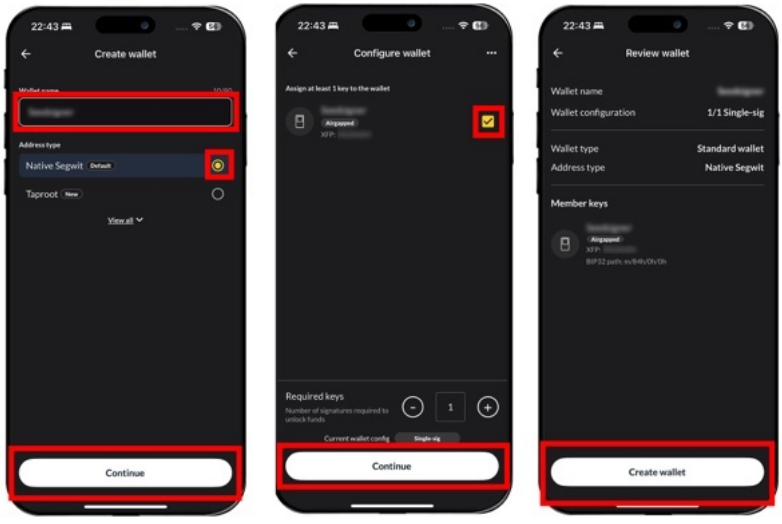


XFP 옆에 있는 문자가 MFP다. 앞에서 적었던 MFP와 일치하는지 확인해 보자.

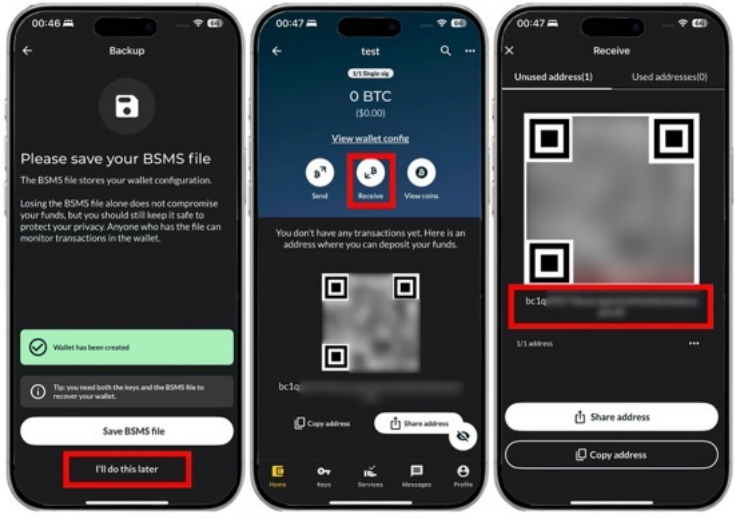
아래 탭에서 [Home]을 누르고 [Create new wallet]을 누른다. 다음에 뜨는 화면에서 [Custom wallet]을 누른다.



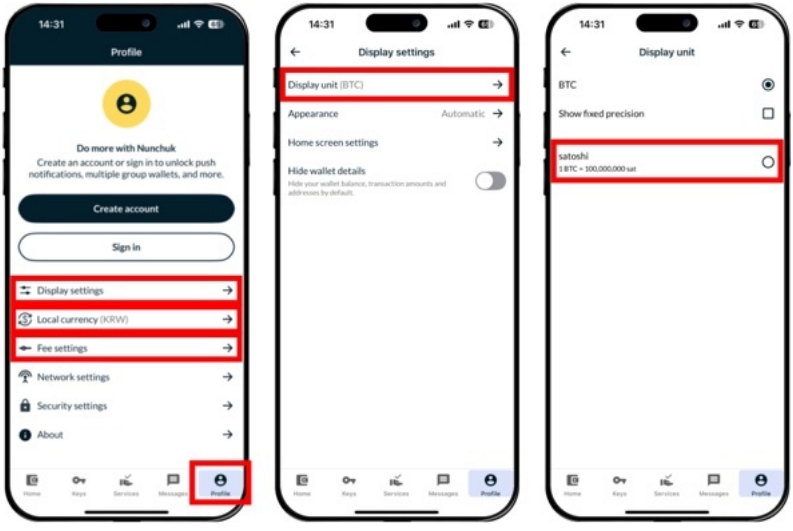
지갑 이름을 설정하고, [Continue]를 누른다. 앞에서 추가했던 Key를 선택하고 [Continue] → [Create wallet]을 누른다.



이제 [I'll do this later]를 누른다. 그러면 넌척에 확장 공개키를 내보내는 것도 완료되었다. [Receive]를 누르고 주소가 키스톤 기기에서 나오는 주소와 같은지 확인하자.



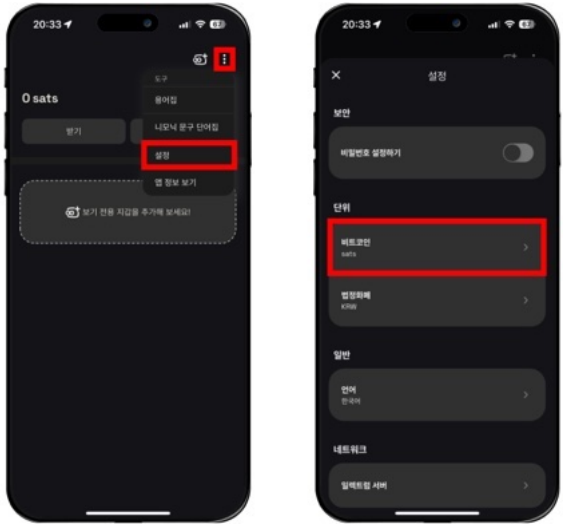
참고로 넌척 하단 탭의 [Profile]을 선택하면 몇 가지 설정을 할 수 있다. [Display settings]에서 일상적인 단위인 sat로 변경할 수 있다. [Display unit]을 누르고 [satoshi]를 선택하면 된다. 이 외에도 [Local currency]에서 [South Korean Won (KRW)]를 선택해 통화 단위를 바꿀 수 있고, [Fee settings] → [Default fee rate] → [Priority]를 선택해 온-체인 수수료를 좀 더 많이 지불하는 대신 거래가 빠르게 컨펌되도록 할 수도 있다.



코코넛 월렛에 확장 공개키 내보내 워치-온리 지갑 만들기

이제 워치-온리 지갑인 코코넛 월렛과 키스톤을 연동해 보자. 앞에서 설치했던 코코넛 월렛을 켠다.

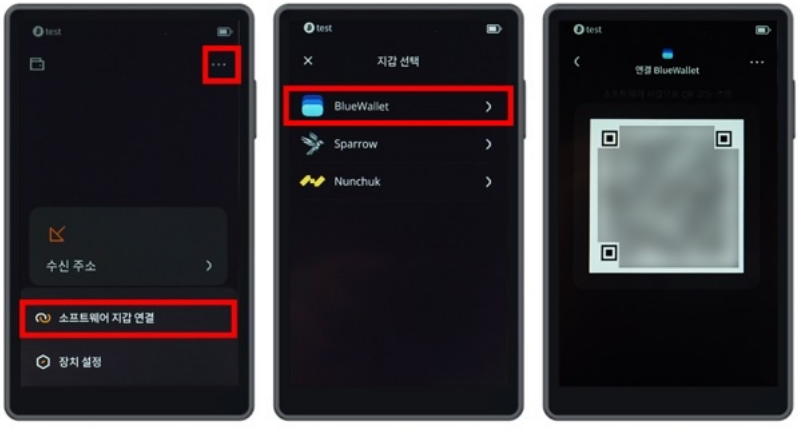
일상적으로는 BTC 단위보다 sats 단위를 더 많이 쓰므로 단위를 바꿔보자. 코코넛 월렛 홈 화면에서 우측 상단 점 세 개 → [설정]을 누르고, 단위: 비트코인을 'sats'로 바꾼다.



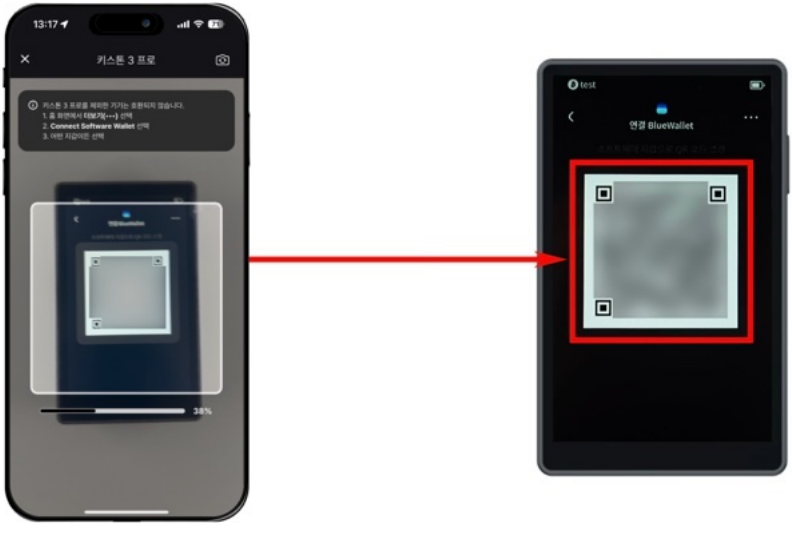
이제 오른쪽 위의 지갑 추가 버튼을 누르거나 아래의 [보기 전용 지갑을 추가해 보세요!]를 누른다.

지갑을 고르는 창이 나오면 [키스톤 3 프로]를 누른다. 카메라 접근 권한을 요구하면 [허용]을 누른다.

키스톤 기기 홈 화면에서 오른쪽 위 점 세 개 → [소프트웨어 지갑 연결] → [BlueWallet]을 선택한다. 그러면 QR 코드가 계속 바뀔 것이다.

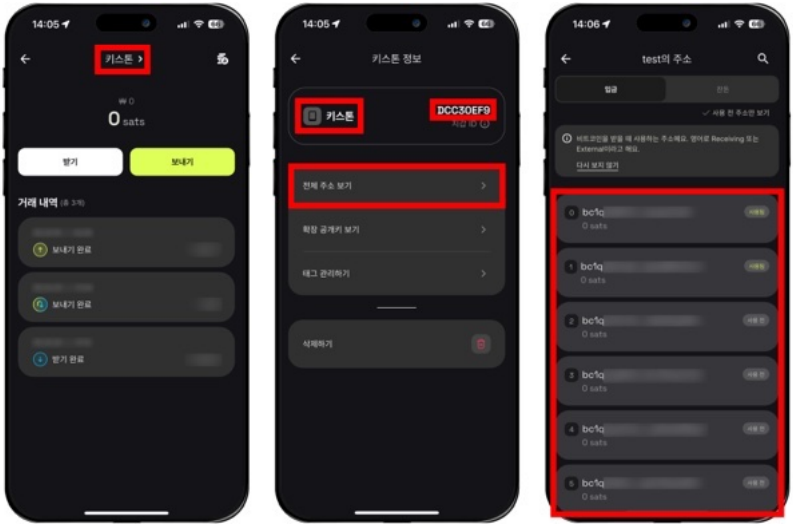


스마트폰의 코코넛 월렛에서 카메라 화면이 나오면 키스톤에 나오는 QR 코드를 스캔한다.

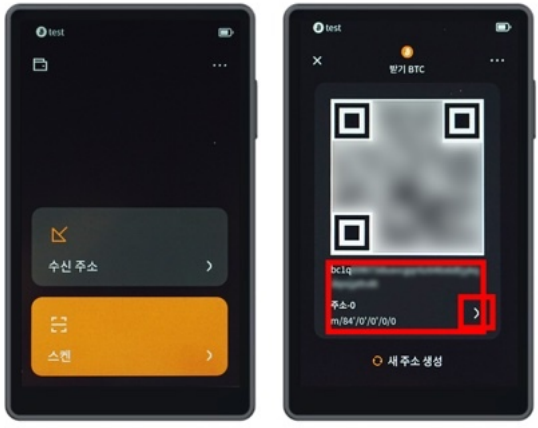


바로 워치-온리 지갑이 불러와진다. 상단의 [키스톤 〉]을 누른다. 먼저 오른쪽에 보이는 MFP가 키스톤에서 확인했던 MFP와 일치하는지 확인한다. [키스톤]을 누르면 지갑 이름을 설정할 수도 있다.

[전체 주소 보기]를 누르면 주소 목록이 나온다.



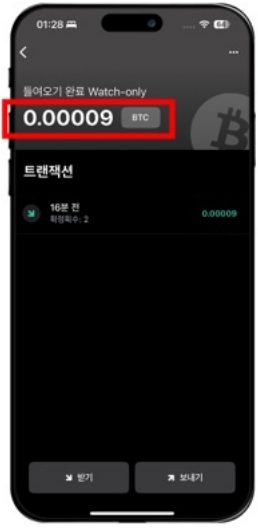
코코넛 월렛에서 보이는 주소들과 키스톤에서 보이는 주소들이 같은지 한번 확인해 보자.

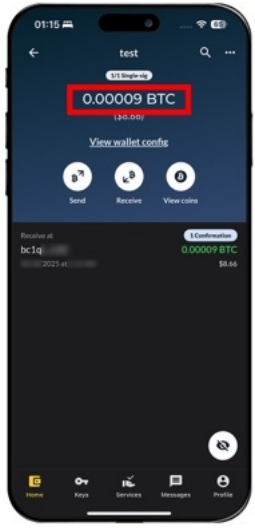


블루월렛으로 서명 연습

본격적으로 비트코인을 지갑에 보관하기 전 꼭 해야 하는 것이 있다. 서명이 잘 되는지 확인과 복구 연습을 미리 해봐야 한다. 비트코인을 다른 곳으로 보내려면 서명을 해야 한다. 만약 서명이 안 되면 다른 곳으로 보낼 수가 없으니 해당 주소에 모은 비트코인은 그림의 떡이 된다. 이것을 안 하고 덜컥 비트코인 모으기부터 시작하는 경우가 있는데, 이러면 나중에 거액이 들어간 상태에서 서명이나 복구를 처음 해보다가 안 되는 경우 난감해질 수 있다.

서명 연습을 해보자. 서명을 연습하기 위해 9천 sats 정도를 지갑에 일단 보내보았다. 비트코인을 지갑에 보내는 방법은 뒤에 나오는 '거래소에서 지갑으로 비트코인 옮기기' 장을 참고하라. 블루월렛과 넌척 둘 다 금액이 잘 확인된다.



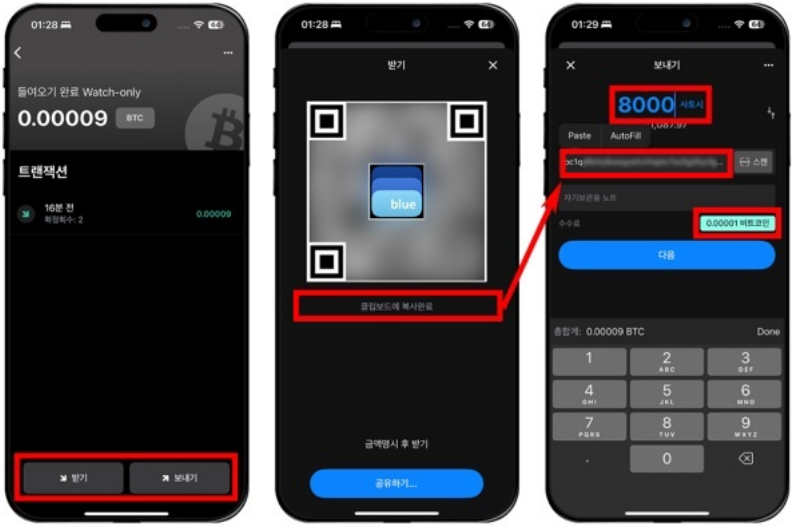


블루월렛에서 서명 연습을 해보자. 먼저 [받기] 버튼을 누르고 뜨는 주소를 복사한다. 프라이버시와 보안을 위해 주소는 재사용하지 않는 것이 좋은데, 블루월렛과 넌척, 코코넛 월렛은 안 쓴 주소를 자동으로 보여준다. 주소를 한 번 누르면 자동으로 주소가 복사된다.

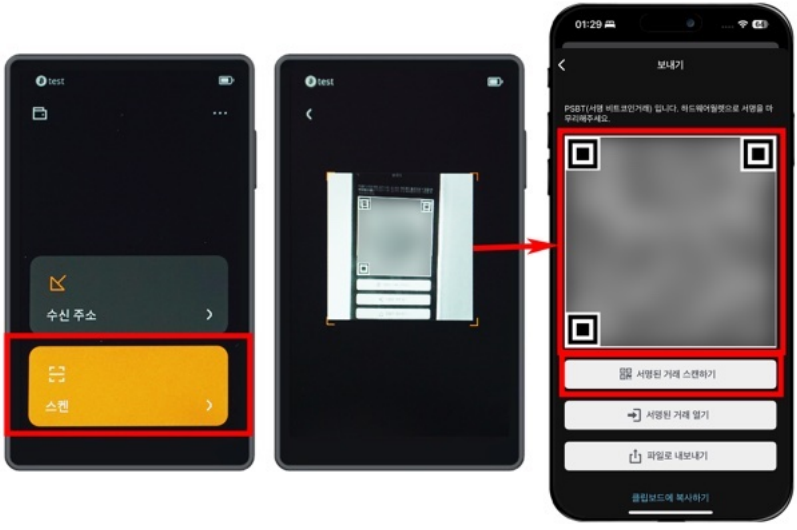
이제 [x] 버튼을 누른 뒤 [보내기] 버튼을 누른다. 주소창에 아까 복사했던 주소를 붙여넣는다. 서명 연습을 하기 위해 내 비트코인을 다시 나에게 보내는 거래(트랜잭션)를 일으키는 것이다.

그 위에 있는 금액에는 수수료를 제외하고 보낼 금액을 입력한다. 비트코인 온-체인에는 수수료가 있기 때문에 2,000-3,000 sats 이상 제외하고 송금 연습을 해야 한다.

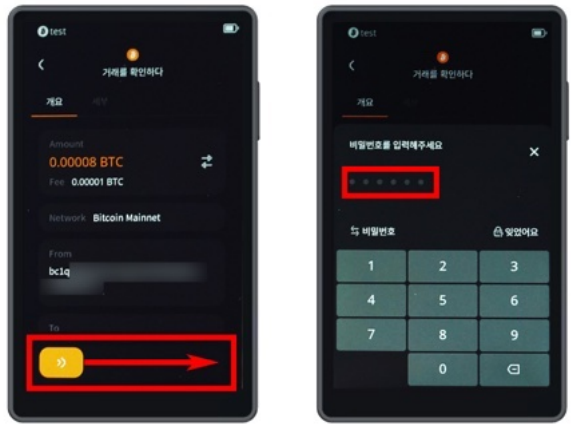
참고로 수수료 옆에 있는 민트색 박스를 누르면 수수료율을 자신이 직접 설정할 수도 있다. 멤풀을 보고 적정 수수료율을 설정하는 연습도 해보면 좋다.



키스톤에서 [스캔]을 누르고, 블루월렛 화면에 나오는 움직이는 QR 코드를 스캔한다.



키스톤에 나오는 화면에서 스크롤을 내려 'To'에 있는 주소를 확인한다. 주소가 맞다면 화살표 버튼을 오른쪽으로 민다. 비밀번호를 입력하라는 창이 나오면 비밀번호를 입력한다.

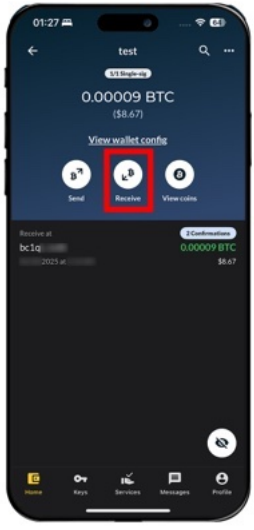


키스톤에서 QR 코드가 나올 것이다. 블루월렛에서 [서명된 거래 스캔하기]를 누르고 키스톤 화면을 스캔한다.

서명이 올바르다면 직렬화된 서명 데이터(나열된 숫자들)가 나타날 것이고, 여기서 [바로 보내기]를 누르면 네트워크에 전송된다.

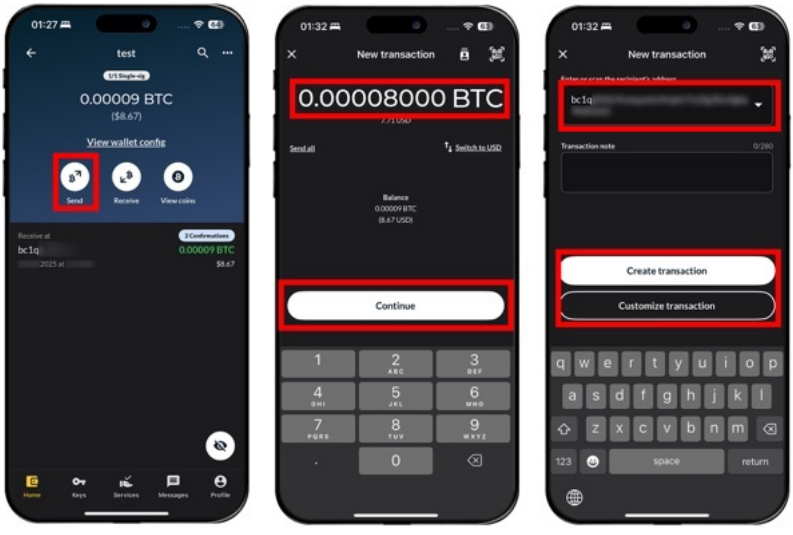
넌척으로 서명 연습

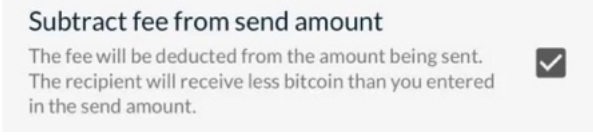
넌척에서 서명할 때도 블루월렛과 비슷하게 진행한다. 먼저 [Receive(받기)]를 누르고 [Copy address]를 눌러 주소를 복사한다.



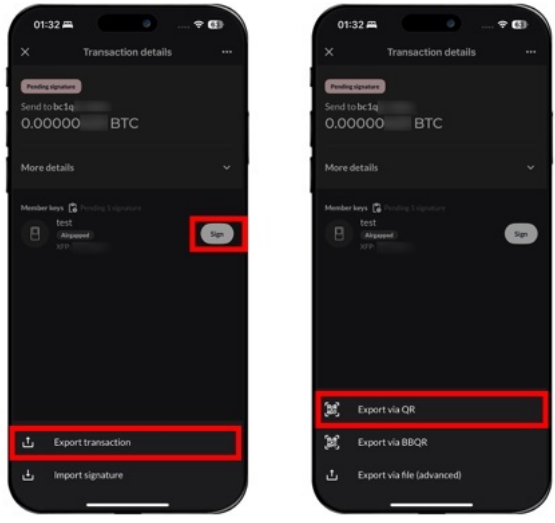
이제 [Send]를 누르고 보낼 금액을 입력한다. 이때 수수료는 제외하고 보내야 한다. [Continue]를 누른다. 아까 복사했던 주소를 붙여넣기 하고 [Create transaction]을 누른다. 참고로 [Customize transaction]을 누르면 수수료율을 직접 설정하거나, 어떤 UTXO를 선택해서 보낼지 설정할 수 있다.

[Customize transaction]에서 [Subtract fee from send amout] 옵션을 체크하면 넌척이 보낼 금액에서 알아서 수수료만 차감하고 보낸다. 이렇게 하면 예상 수수료를 계산할 필요 없이 전액을 보내면 되기 때문에 편리하다.

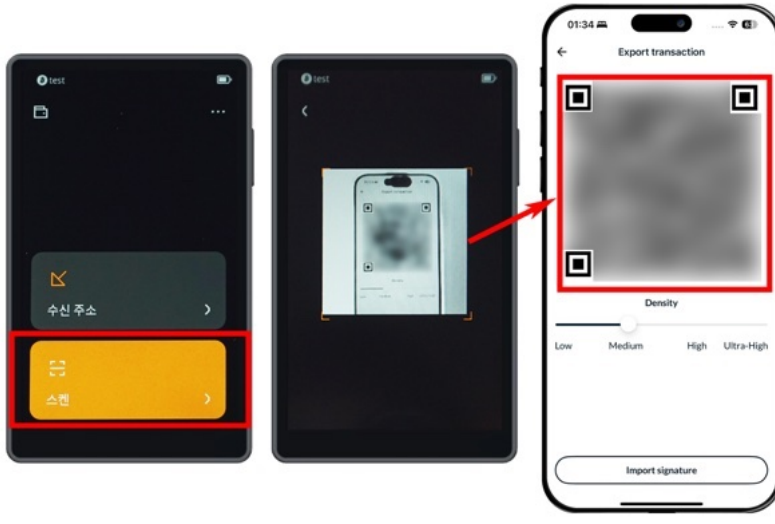




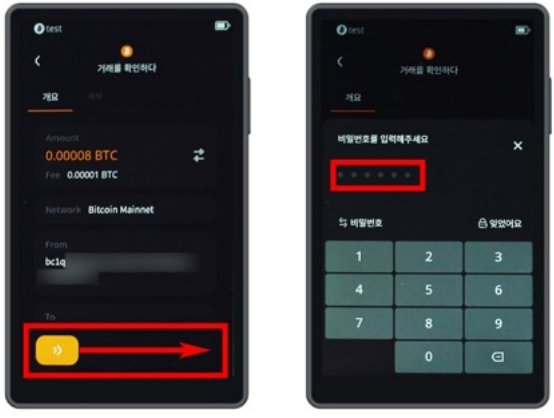
[Sign]을 누르고, [Export transaction]을 누른다. 그다음에 맨 위에 있는 [Export via QR]을 누르면 QR 코드가 나올 것이다.



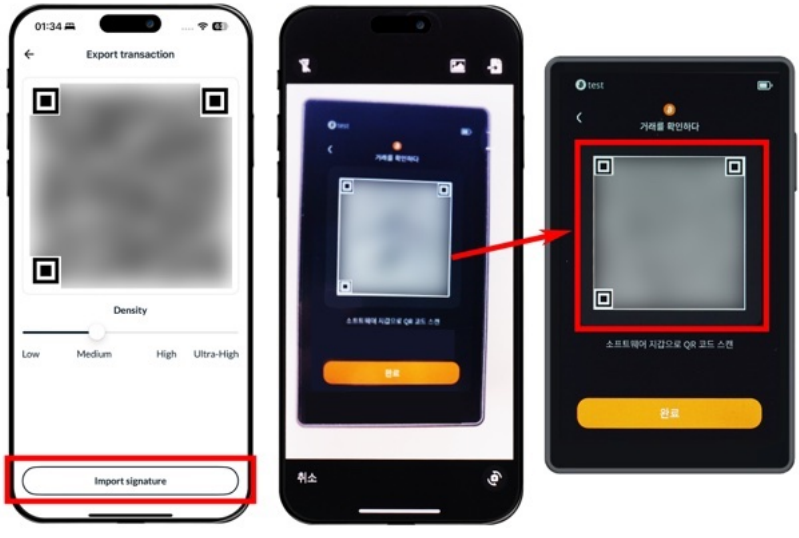
키스톤에서 [스캔]을 누르고 넌척이 보여주는 QR 코드를 스캔한다.



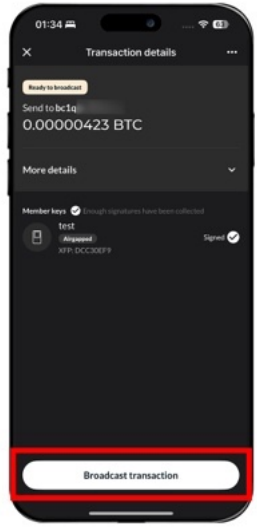
키스톤에 나오는 화면에서 스크롤을 내려 'To'에 있는 주소를 확인한다. 주소가 맞다면 화살표 버튼을 오른쪽으로 민다. 비밀번호를 입력하라는 창이 나오면 비밀번호를 입력한다.

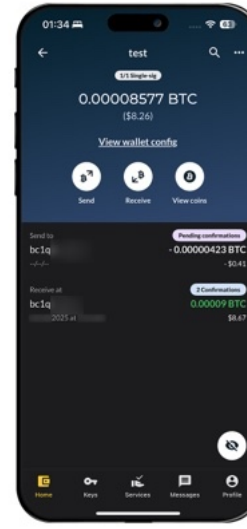


키스톤에서 QR 코드가 나올 것이다. 넌척에서 [Import signature]를 누르고 키스톤 화면을 스캔한다.



[Broadcast transaction]을 누르면 네트워크에 전파된다.

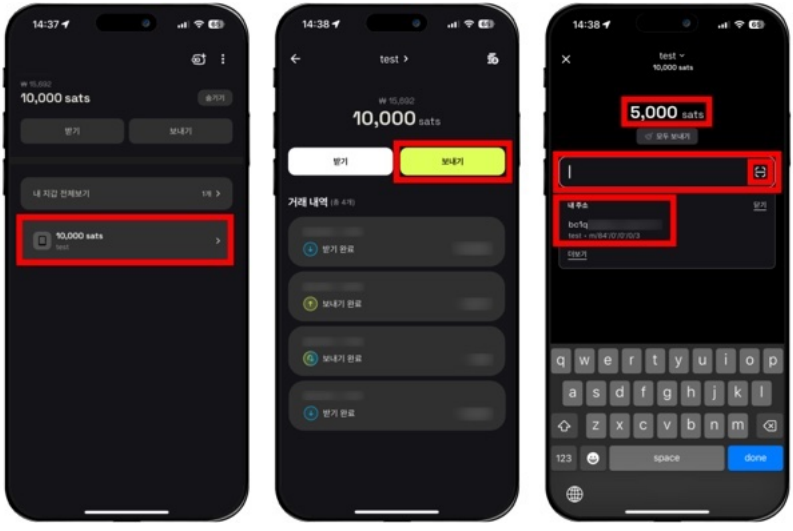




코코넛 월렛으로 서명 연습

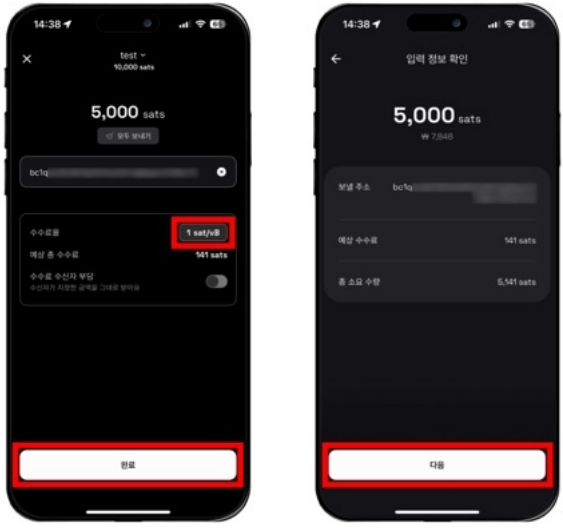
코코넛 월렛에서 서명하는 과정도 비슷하다. 코코넛 월렛 홈 화면에서 지갑을 선택하고 [보내기]를 누른다.

금액을 입력하고 아래 보낼 주소 입력창을 누른다. 코코넛은 다른 워치-온리 지갑들보다 서명 연습하는 것이 훨씬 편하다. 보낼 주소 입력창을 누르면 아래에 자신의 지갑 주소 목록이 나오기 때문이다. '내 주소' 아래에 있는 주소를 누른다.

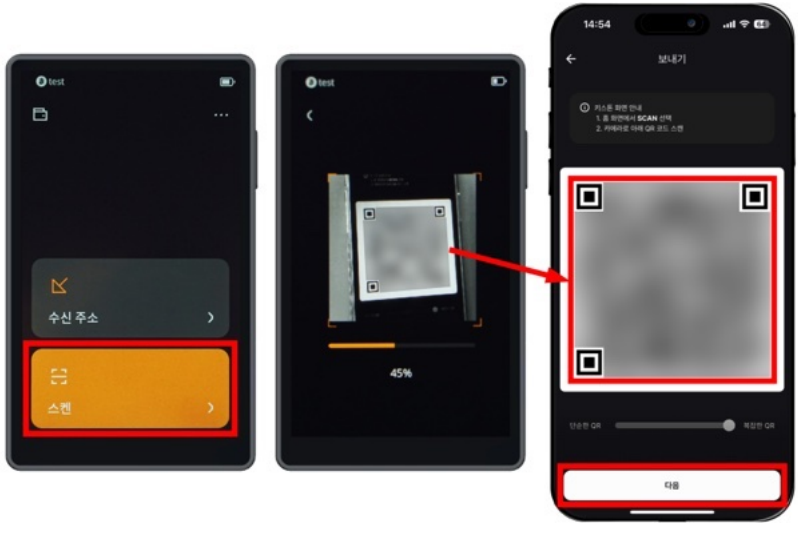


코코넛 월렛에서는 바로 수수료율을 조정할 수 있다. 현재 적절한 수수료가 자동으로 입력되어 있지만 더 안정적으로 바로 다음 블록에 거래가 컨펌되게 하고 싶다면 수수료율을 높여도 좋다. 수수료율까지 설정했으면 [완료]를 누른다.

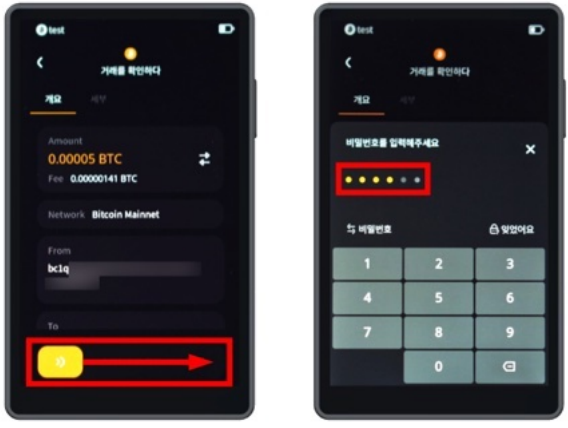
보낼 주소와 예상 수수료 등을 확인한 뒤 정보가 맞으면 [다음]을 누른다.



키스톤에서 [스캔]을 누르고, 코코넛 월렛 화면에 나오는 QR 코드를 스캔한다.

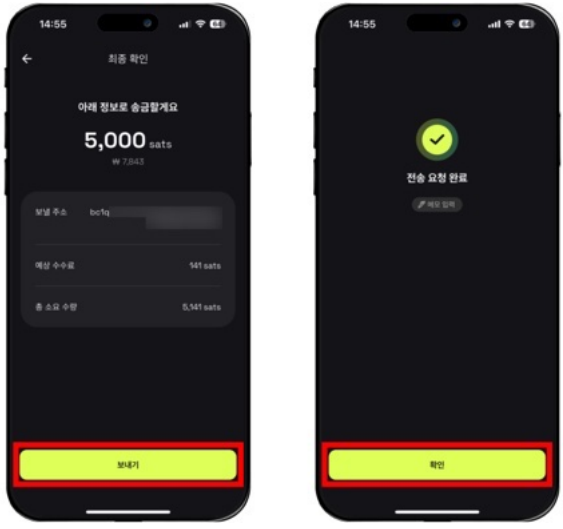


키스톤에 나오는 화면에서 스크롤을 내려 'To'에 있는 주소를 확인한다. 주소가 맞다면 화살표 버튼을 오른쪽으로 민다. 비밀번호를 입력하라는 창이 나오면 비밀번호를 입력한다.



키스톤에서 QR 코드가 나올 것이다. 코코넛 월렛에서 [다음]을 누르고 키스톤 화면을 스캔한다.

거래 정보를 한 번 더 확인하고 [보내기]를 누르면 네트워크에 전파된다.



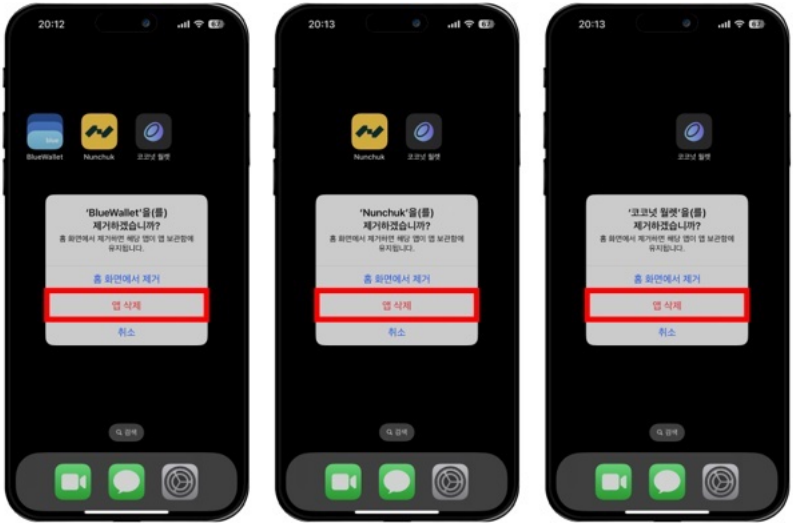
이로써 서명까지 잘 되는 것을 모두 확인해 보았다.

복구 연습

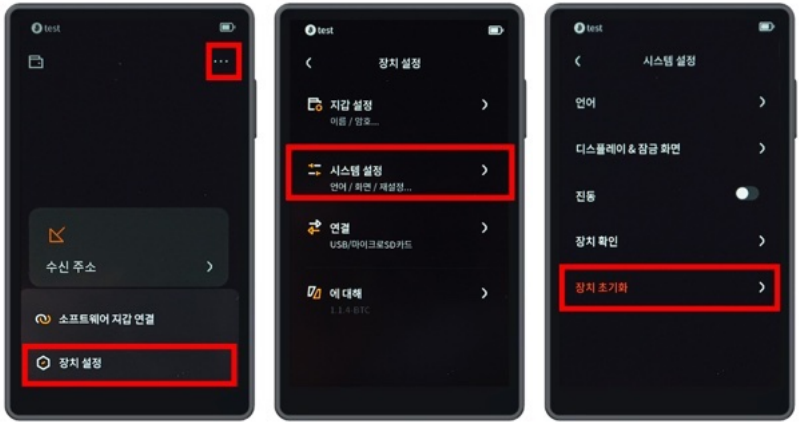
어떤 기기든지 수명이 있기 마련이다. 지갑을 쓰다가 지갑이 망가질 수도 있고, 지갑이나 워치-온리 앱이 깔린 스마트폰을 바꿔야 할 수도 있다. 따라서 복구 연습은 미리 해보는 것이 좋다.

니모닉만 있다면 어떤 지갑이든 상관없이 내가 가진 비트코인을 복구할 수 있다. 지금부터 지갑을 복구하는 방법을 알아보자.

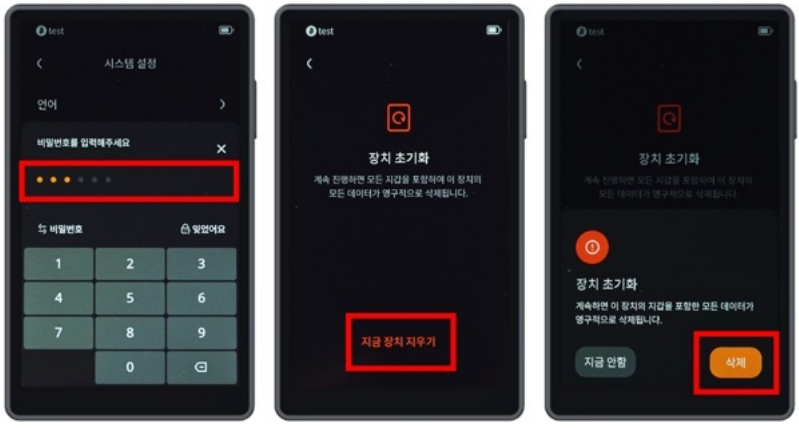
먼저 스마트폰에서 워치-온리 지갑인 블루월렛과 넌척, 코코넛 월렛을 모두 지운다.



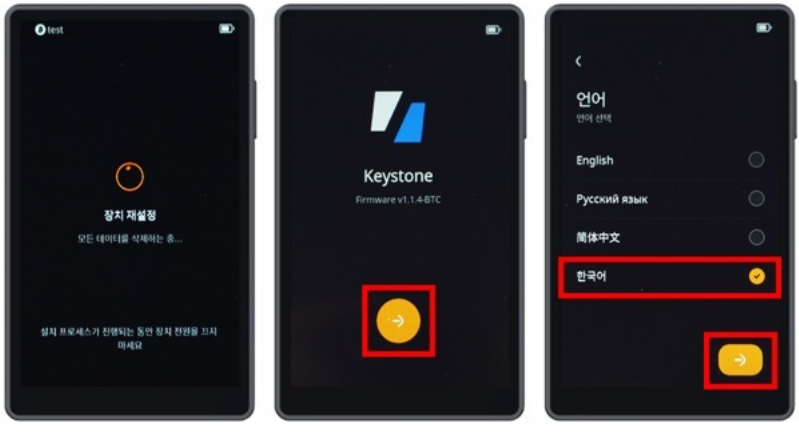
지갑을 초기화하기 위해 키스톤 홈 화면에서 오른쪽 위 점 세 개 → [장치 설정] → [시스템 설정] → [장치 초기화]를 누른다.



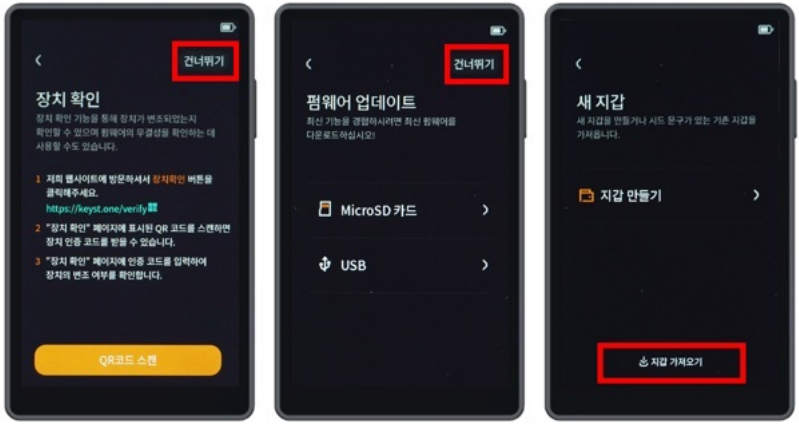
비밀번호를 누르고, [지금 장치 지우기]를 누른다. 알림창이 뜨면 [삭제]를 누른다.



잠시 기다리면 장치가 초기화될 것이다. 화살표 버튼을 누른 뒤 언어는 [한국어]를 선택한다.

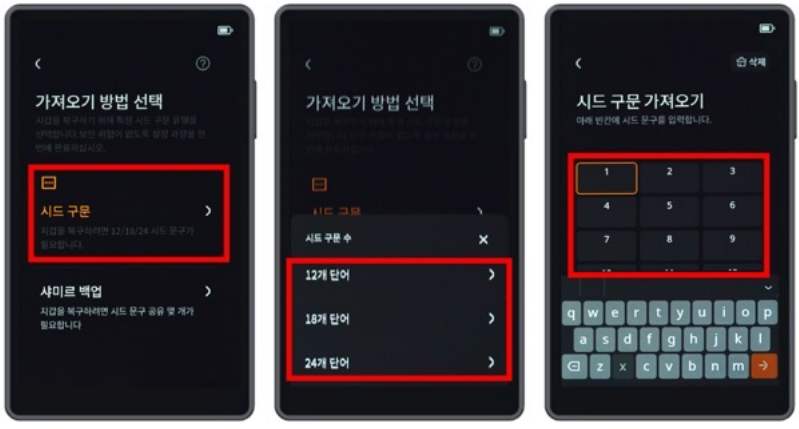


장치 확인은 처음에 했으므로 건너뛰겠다. 펌웨어 업데이트도 했으므로 건너뛰자. 복구할 때는 '새 지갑'에서 [지갑 가져오기]를 눌러야 한다.



PIN 코드를 설정한다. PIN 코드 확인까지 끝나면 지갑 이름을 입력한다.

가져오기 방법에서 [시드 구문]을 선택한다. 그러면 시드 구문 수를 선택하는 창이 나온다. 필자는 니모닉 12단어로 지갑을 만들었으므로 12단어를 선택했다. 그다음 '시드 구문 가져오기'에서 니모닉을 틀리지 않게 순서대로 입력한다.



잠시 기다리면 지갑이 만들어진다.

이제 앞에서 했던 워치-온리 연동과 서명 연습을 다시 해보면 모든 복구 연습이 끝난다. 참고로 블루월렛은 앱을 삭제해도 잔여 캐시가 남아 지갑이 제대로 삭제되지 않기도 한다. 이런 경우에는 넌척과 코코넛 월렛에서 제대로 복구가 되는지를 중점적으로 확인해 보자.

여기까지 완료됐다면 이제 비트코인을 모으면 된다.

| 시드사이너 지갑

편리함 때문에 키스톤으로 입문을 많이 하긴 하지만, 시드사이너는 자신이 직접 부품들을 구해 기기를 조립할 수 있다는 점에서 키스톤보다 더 신뢰 지점이 없어 안심이 된다.

또한, 저장 장치가 없어서 매번 니모닉을 입력해야 한다는 점은 단점이기도 하지만, 정말 큰 장점이기도 하다. 누가 훔쳐 가도 상관없기 때문이다(콜드부트 공격 가능성이 있긴 하지만 거의 불가능에 가깝다).

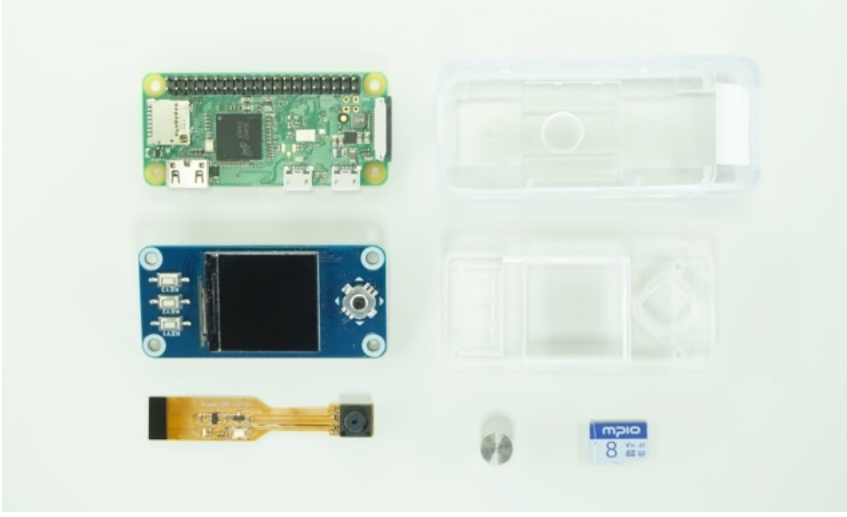
편리하게 시드 QR을 만들고 스캔하는 방법도 있지만, 아예 니모닉을 외워서 그때그때 입력하는 게 조금 불편하더라도 마음이 훨씬 편하다. 편리함과 보안은 반비례한다.

그럼 이제 시드사이너 사용 방법을 알아보자. 필자는 '비트키트'에서 구매한 시드사이너를 기준으로 글을 썼다.

필수 준비물

시드사이너를 만들 때 제일 좋은 건 자기가 직접 부품들을 따로 구하는 것이겠지만 비트키트처럼 필요한 부품들을 모아서 파는 곳도 있으니 참고하기 바란다.

https://smartstore.naver.com/bitkit/



1. 라즈베리파이 제로 보드(핀 납땜 버전)

라즈베리파이 제로 보드가 제일 좋다. 라즈베리파이 제로 보드는 처음부터 무선 통신 모듈이 없는 채로 나온다.

하지만 국내에서는 라즈베리파이 제로 보드를 구하기가 어렵다. 그래서 보통 라즈베리파이 제로 W 보드를 사고, 와이파이/블루투스 모듈을 단선시켜 사용한다. 비트키트에서 시드사이너 조립 세트를 구매한 경우 라즈베리파이 제로 W 보드가 온다.

필자는 알리에서 라즈베리파이 제로 보드(핀 납땜 되어있는 버전)도 구매해서 사용 중이다. 부품을 각각 구할 용기가 없다면 비트키트 같은 쇼핑몰을 이용하고, 용기가 생기면 부품을 각각 구해보는 것도 방법이다.

다음 사진에서 위에 있는 보드가 라즈베리파이 제로 오리지널, 아래 있는 보드가 라즈베리파이 제로 W 보드다. 라즈베리파이 제로 오리지

널 보드는 앞면에 와이파이/블루투스 칩이 없고 대신 라즈베리파이 로고가 있는 것을 알 수 있다.

(상) 라즈베리파이 제로 오리지널, (하) 라즈베리파이 제로 W

2. 라즈베리파이 제로용 LCD 1.3인치 240 x 240 px

따로 구하는 경우 인치 수와 픽셀 수를 꼭 맞춰서 사야 한다.

3. 라즈베리파이 제로용 카메라 모듈

4. 마이크로SD카드 8GB (4GB 이상)

5. 케이스

(필자는 투명 케이스를 사용하므로 사진상에서 잘 안 보인다.)

권장 준비물

1. 핀셋 또는 얇은 일자 드라이버

라즈베리파이 제로 W 보드의 경우 무선 통신 모듈을 단선시켜야 한다. 이때 핀셋이 있으면 편하다. 핀셋이 없는 경우 얇은 일자 드라이버로 밀어서 뗄 수도 있다. 다만 이때 다른 부품들이 상하지 않도록 힘 조절을 잘 하면서 밀어야 할 것이다.

2. SD카드 리더기

마이크로SD카드를 부팅용 카드로 만들기 위해 컴퓨터에 연결해야 한다. 이때 SD카드 리더기가 필요하다.

3. 마이크로 5핀 충전 케이블

4. 5V 1↑A 어댑터 또는 보조배터리

시드사이너는 배터리가 없으므로 전원 공급이 되어야 사용할 수 있다. 어댑터와 5핀 케이블을 이용할 수도 있고, 보조배터리를 이용할 수도 있다. 보조배터리를 이용하면 돌아다니면서 사용할 수 있다.

이미지 파일 다운로드

먼저 깃허브에서 시드사이너 소프트웨어 이미지 파일을 다운로드할 것이다. 아래 링크에 접속한다.

https://github.com/seedsigner/seedsigner?tab=readme-ov-file#downloading-the-software

스크롤을 내리고 보드가 라즈베리파이 제로인지, 라즈베리파이 제로 W인지에 따라 알맞은 img 파일을 다운로드한다.

README MIT license

Downloading the Software

Download the current Version (0.8.5) software image that is compatible with
1.3 is the most common and recommended board.

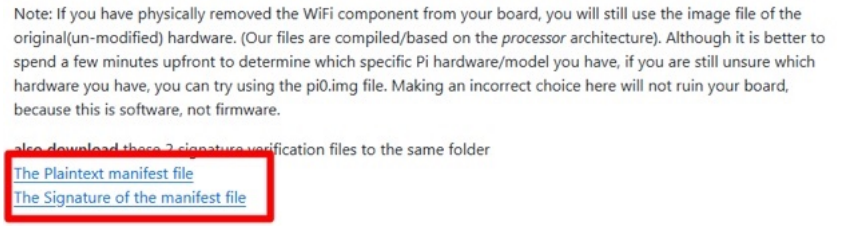
Board	Download Image Link/Name
Raspberry Pi Zero 1.3	seedsigner_os.0.8.5.pi0.img
Raspberry Pi Zero W	seedsigner_os.0.8.5.pi0.img
Raspberry Pi Zero 2 W	seedsigner_os.0.8.5.pi02w.img
Raspberry Pi 1 Model B/B+	seedsigner_os.0.8.5.pi0.img
Raspberry Pi 2 Model B	seedsigner_os.0.8.5.pi2.img
Raspberry Pi 3 Model B	seedsigner_os.0.8.5.pi02w.img
Raspberry Pi 4 Model B	seedsigner_os.0.8.5.pi4.img
Raspberry Pi 400	seedsigner_os.0.8.5.pi4.img

비트코인을 관리할 때는 누구도 믿지 않고 스스로 검증하는 태도가 중요하다. 우리가 다운로드한 파일이 시드사이너 측이 배포한 파일이 아니라 우리의 소중한 비트코인을 노리는 해커가 만든 변조된 파일일 수도 있지 않겠는가? 이런 의심이 드는 경우 다음 절에서 말하는 소프트웨어 검증 절차를 따라 해보면 된다(다소 어려울 수 있다).

소프트웨어 변조 여부 확인(윈도우OS)

이제 윈도우OS와 맥OS에서 이미지 파일 무결성 검증을 하는 방법을 알아볼 것이다. 먼저 윈도우OS에서 하는 방법을 알아보자. 맥OS에서 검증하려면 다음 절로 넘어가면 된다.

스크롤을 조금 더 내려보면 다음 사진과 같은 파일 링크가 있다. 이 링크를 누르면 seedsigner.?.?.?.sha256.txt 파일과 seedsigner.?.?.?.sha256.txt.sig 파일이 다운로드 될 것이다. ?로 표기한 부분에는 버전 숫자가 들어간다.


Note: If you have physically removed the WiFi component from your board, you will still use the image file of the original(un-modified) hardware. (Our files are compiled/based on the *processor* architecture). Although it is better to spend a few minutes upfront to determine which specific Pi hardware/model you have, if you are still unsure which hardware you have, you can try using the pi0.img file. Making an incorrect choice here will not ruin your board, because this is software, not firmware.

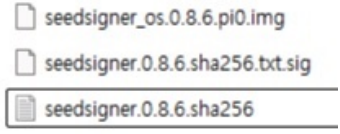
also download these 2 signature verification files to the same folder

The Plaintext manifest file

The Signature of the manifest file

seedsigner.?.?.?.sha256.txt 파일은 우리가 다운로드한 이미지 파일의 해시값이 적혀 있는 텍스트 파일이다. seedsigner.?.?.?.sha256.txt.sig 파일은 그 해시값이 적힌 텍스트 파일을 시드사이너 개발자의 개인키로 서명한 것이다.

※ 주의: 3개 파일을 모두 같은 경로에 다운로드해야 한다. '다운로드' 폴더에 모두 다운로드하는 것을 권장한다.



서명 파일은 PGP 암호화 방식을 통해 서명된 것이다. 따라서 서명 검증은 PGP의 오픈소스 버전인 GPG 프로그램을 통해 할 수 있다. PGP는 개인키를 이용해 메시지를 암호화하고 공개키를 이용해 암호화된 메시지를 복호화할 수 있는 기술이다. 또한 자신의 공개키가 공개된 상태에서 자신의 개인키로 메시지나 파일에 서명을 할 수가 있다. 그러면 사람들은 공개키를 이용해 그 서명을 검증할 수가 있는데, 오직 개인키를 가진 사람만이 서명을 할 수 있으므로 이는 그 메시지를 자신이 썼다는, 위조할 수 없는 강력한 증거가 된다. 비트코인과 굉장히 비슷하다고 느꼈다면 잘 이해한 것이다. PGP 암호화 방식은 일반인이 쉽게 사용할 수 있던 최초의 암호학 기술이다. 비트코인은 그 계보에서 내려왔다. PGP의 의미가 무엇인지 궁금하다면 필자가 공동 집필자로 참여한 『비트코인 백서 해설』 10장의 심층적 이해에서 '필 짐머만, PGP 배포' 절을 읽어보면 좋다.

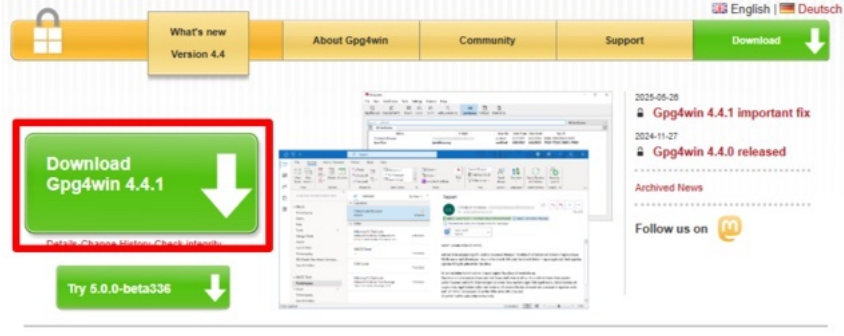
변조 여부 검증은 다음과 같이 한다. 시드사이너 개발자는 시드사이너 프로그램의 해시값을 공개해 놨다. 우리는 시드사이너 이미지 파일을 SHA256 함수로 해싱해 보고 그 해시값을 공개된 해시값과 비교하면 된다. 만약 파일의 코드에 한 글자라도 변조가 있었다면 완전히 다른 해시값이 나올 것이기 때문이다.

하지만 문제가 있다. 해시값이 적힌 텍스트 파일이 정말 시드사이너 개발자가 공개한 것인지 어떻게 알까? 해커가 파일을 변조해 놓고 변조한 파일의 해시값을 텍스트 파일로 공개한 것인데 그걸 철석같이 시드사이너 개발자가 공개한 것이라고 믿을 수도 있는 것이 아닌가? 그래서 서명 파일이 있는 것이다. 우리는 해시값 파일의 서명이 시드사이너 개발자가 한 서명이 맞는지를 시드사이너 개발자의 공개키로 검증할 것이다. 맞다면 우리가 다운로드한 시드사이너 해시값 텍스트 파일이 해커가 아닌 시드사이너 개발자가 만든 것이라고 확신할 수 있다.

이제 GPG의 윈도우 버전인 Gpg4win을 다운로드할 것이다. 다음 링크에 접속한다.

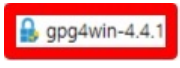
https://www.gpg4win.org/

[Download Gpg4win]을 누른다.

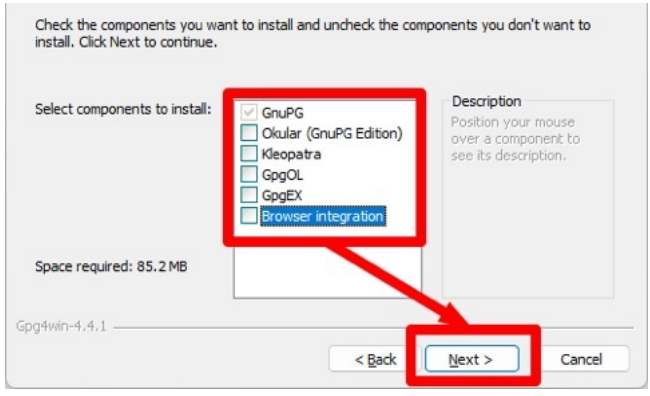


그러면 기부를 바라는 안내창이 나올 것이다. 'PayPal'에서 $0를 선택하고 [Donate & Download]를 누르거나, 왼쪽의 비트코인을 누르고 [Download Gpg4win ?.?.?]을 누른다.

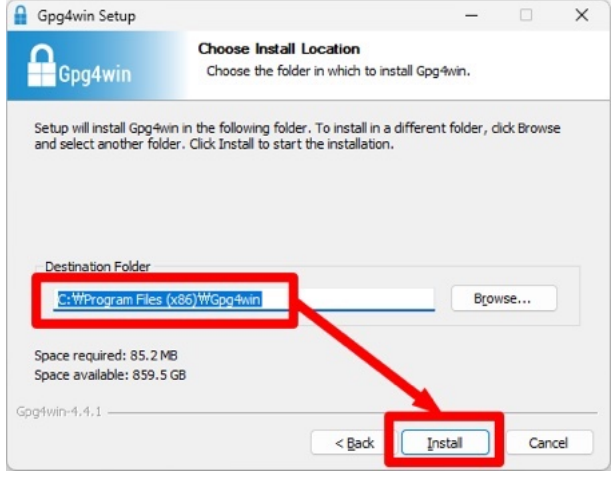
'gpg4win' 설치 프로그램이 다운로드되면, 프로그램을 실행한다.



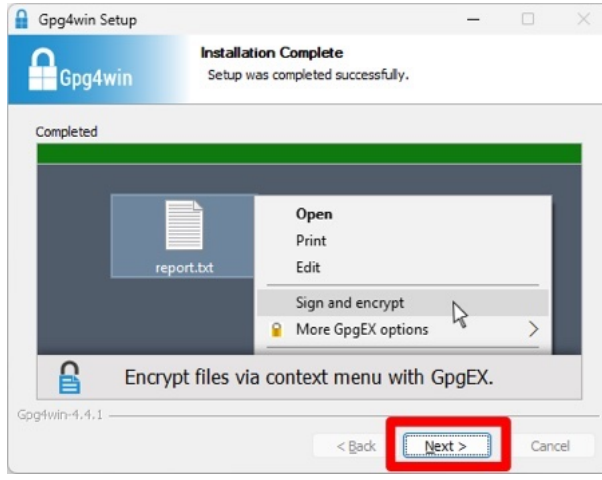
설치를 원하는 프로그램을 모두 선택하고, [Next]를 누른다. 참고로 'Kleopatra'는 이메일이나 파일 등의 메시지를 쉽게 암호화/복호화하고, 서명/검증을 하기에 용이한 프로그램이다. 프로톤 메일에서는 기본적으로 PGP 암호화/복호화/서명/검증을 지원하지만, 지메일이나 네이버 메일은 그렇지 않으므로 'Kleopatra'를 사용할 수 있다. 지금은 PGP 서명 검증이 목적이므로 'GnuPG'만 설치하겠다.

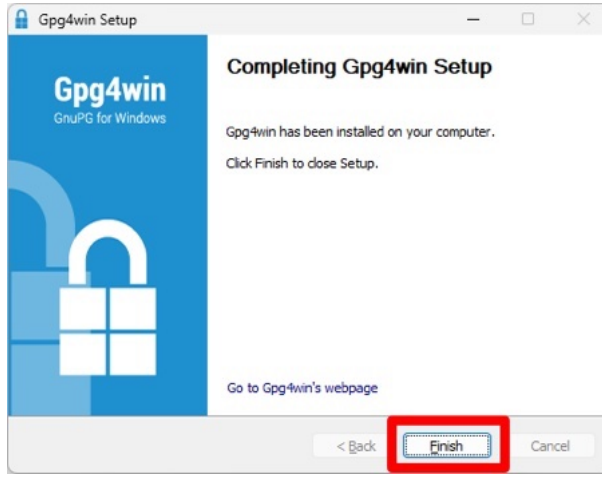


설치 위치를 정하고 [Install]을 누른다.

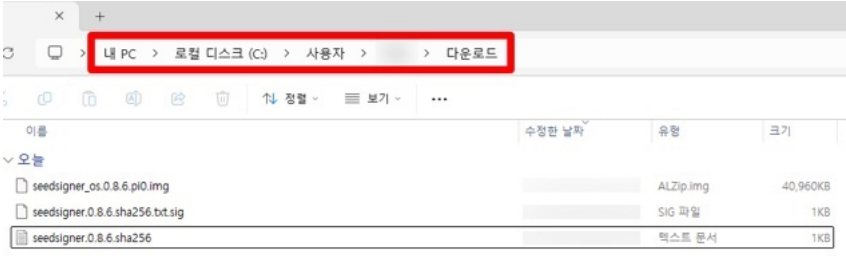


설치가 완료되면 [Next] → [Finish]를 누른다.

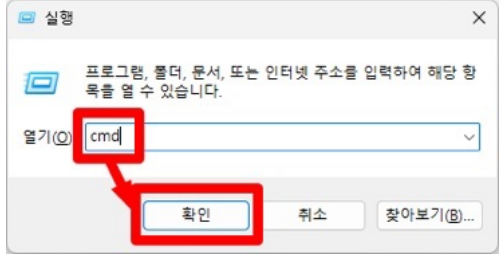




파일 탐색기에서 3개 파일이 다운로드 된 곳에 들어가 주소창을 클릭하면 나오는 경로를 복사한다.

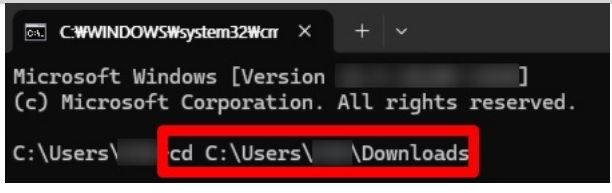


키보드에서 '윈도우 키 + R'을 누르거나 시작 버튼을 누르고 '실행'을 검색하여 실행하고, 'cmd'를 실행한다.



그러면 터미널 창이 나온다. 여기에 다음과 같이 입력한다. 이는 해당 폴더로 이동하라는 명령어다.

```
cd [방금 복사한 경로]
```



이제 다음과 같이 입력한다. 이는 시드사이너 개발자의 공개키를 가져오는 명령어다. 보통 PGP 공개키는 keybase 웹사이트에 등록하여 사용하는데 여기 등록된 시드사이너 개발자의 공개키를 가져오는 것이다.

```
gpg --fetch-keys https://keybase.io/seedsigner/
   pgp_keys.asc
```

```
C:\Users\      \Downloads>gpg --fetch-keys https://keybase.io/seedsigner/pgp_keys.asc
```

그러면 다음 사진과 같이 결과가 표시되어야 한다.

```
gpg: requesting key from 'https://keybase.io/seedsigner/pgp_keys.asc'
gpg: key C7EF709007260119: public key "seedsigner <btc.hardware.solutions@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

이제 다음과 같이 입력한다. 이는 시드사이너 개발자의 공개키와 해시값 파일을 통해 서명을 검증하는 명령어다.

```
gpg --verify [서명 파일 이름] [해시값 텍스트 파일 이름]
```

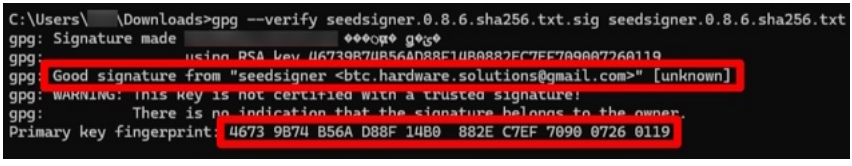
아마 다음과 같은 형태일 것이다.

```
gpg --verify seedsigner.?.?.?.sha256.txt.sig
   seedsigner.?.?.?.sha256.txt
```

```
C:\Users\      \Downloads>gpg --verify seedsigner.0.8.6.sha256.txt.sig seedsigner.0.8.6.sha256.txt
```

그러면 다음 사진과 같은 결과가 나올 것이다. 여기서 **Good signature** ~가 꼭 있어야 한다. 마지막에 나오는 공개키 지문도 확인해 놓자.

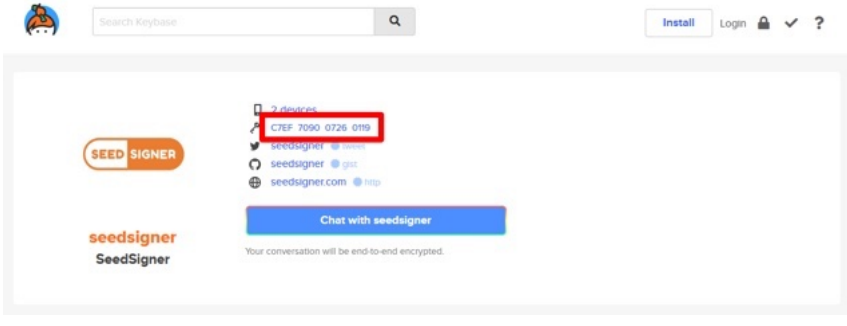
만약 이 결과가 나오지 않는다면 다시 시도해 보자. 그래도 나오지 않는다면 즉시 과정을 중단하고, 이미지 파일과 해시값, 서명 파일을 깃허브 공식 시드사이너 페이지에서 받은 것이 맞는지 확인해 보자.



터미널에 나온 공개키 지문을 대조하여 우리가 검증에 사용한 공개키가 정말 시드사이너 개발자의 것이 맞는지 확인할 것이다. 다음 웹사이트에 들어간다.

https://keybase.io/seedsigner

열쇠 옆에 있는 16자리 지문 코드를 눌러 지문 코드 전체를 확인한다.



지문 코드 전체가 터미널에 나온 지문 코드와 일치하는지 확인한다.

여기까지 되었다면 이제 시드사이너 프로그램을 해싱하여 해시값을 비교해 볼 차례다. 다음과 같이 입력한다. 이는 시드사이너 이미지 파일을 SHA256 함수로 해싱하는 명령어다.

```
CertUtil -hashfile [이미지 파일 이름] SHA256
```

아마 다음과 같은 형태일 것이다.

```
CertUtil -hashfile seedsigner_os.?.?.?.pi0.img
  SHA256
```

파일의 해시값을 계산하고 출력할 것이다.

```
C:\Users\     \Downloads>CertUtil -hashfile seedsigner_os.0.8.6.pi0.img SHA256
SHA256 hash of seedsigner_os.0.8.6.pi0.img:
da32ce21f185404ccefd58e76e55ae7f1ac9fe2df2100bc7bbab3e03c5d71b6d
CertUtil: -hashfile command completed successfully.
```

해시값 텍스트 파일(seedsigner.?.?.?.sha256.txt)을 열어본다.

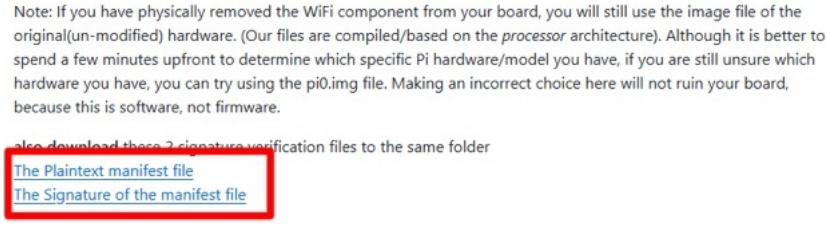
그러면 seedsigner_os.?.?.?.pi0.img 왼쪽에 해시값이 있을 것이다.

이 값이 터미널에 나와 있는 해시값과 같다면 이미지 파일에 변조가 일어나지 않은 것이다. 이제 이 이미지 파일을 이용해 시드사이너 부팅용 마이크로SD카드를 만들 것이다. '부팅 마이크로SD카드 만들기' 절로 넘어가면 된다.

소프트웨어 변조 여부 확인(맥OS)

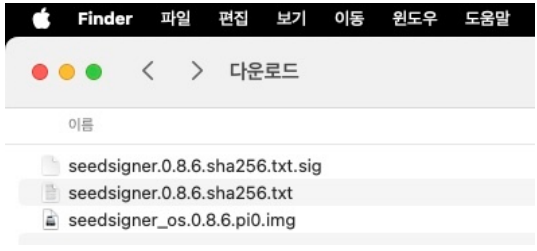
이제 맥OS에서 이미지 파일 무결성 검증을 하는 방법을 알아보자. 윈도우OS에서 하는 방법과 비슷하다.

스크롤을 조금 더 내려보면 다음 사진과 같은 파일 링크가 있다. 이 링크를 누르면 seedsigner.?.?.?.sha256.txt 파일과 seedsigner.?.?.?.sha256.txt.sig 파일이 다운로드 될 것이다. ?로 표기한 부분에는 버전 숫자가 들어간다.



seedsigner.?.?.?.sha256.txt 파일은 우리가 다운로드한 이미지 파일의 해시값이 적혀 있는 텍스트 파일이다. seedsigner.?.?.?.sha256.txt.sig 파일은 그 해시값이 적힌 텍스트 파일을 시드사이너 개발자의 개인키로 서명한 것이다.

※ 주의: 3개 파일을 모두 같은 경로에 다운로드해야 한다. '다운로드' 폴더에 모두 다운로드한다.



서명 파일은 PGP 암호화 방식을 통해 서명된 것이다. 따라서 서명 검증은 PGP의 오픈소스 버전인 GPG 프로그램을 통해 할 수 있다. PGP는 개인키를 이용해 메시지를 암호화하고 공개키를 이용해 암호화된 메시지를 복호화할 수 있는 기술이다. 또한 자신의 공개키가 공개된 상태에서 자신의 개인키로 메시지나 파일에 서명을 할 수가 있다. 그러면 사람들은 공개키를 이용해 그 서명을 검증할 수가 있는데, 오직 개인키를 가진 사람만이 서명을 할 수 있으므로 이는 그 메시지를 자신이 썼다는, 위조할 수 없는 강력한 증거가 된다. 비트코인과 굉장히 비슷하다고 느꼈다면 잘 이해한 것이다. PGP 암호화 방식은 일반인이 쉽게 사용할 수 있던 최초의 암호학 기술이다. 비트코인은 그 계보에서 내려왔다. PGP의 의미가 무엇인지 궁금하다면 필자가 공동 집필자로 참여한 『비트코인 백서 해설』 10장의 심층적 이해에서 '필 짐머만, PGP 배포' 절을 읽어보면 좋다.

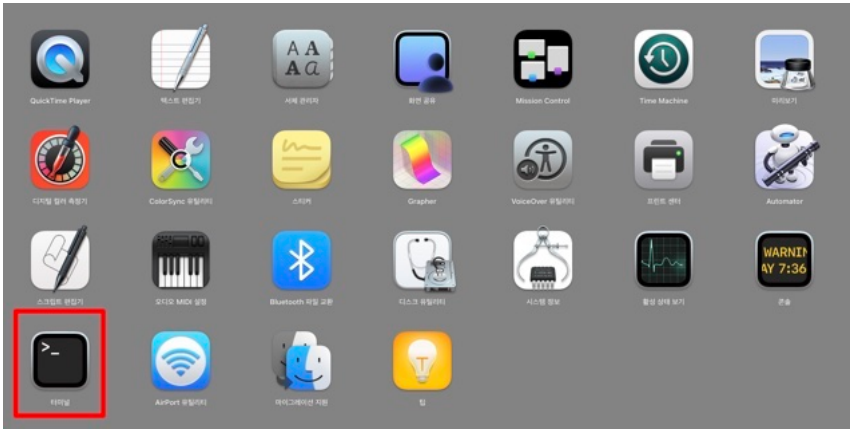
변조 여부 검증은 다음과 같이 한다. 시드사이너 개발자는 시드사이너 프로그램의 해시값을 공개해 놨다. 우리는 시드사이너 이미지 파일을 SHA256 함수로 해싱해 보고 그 해시값을 공개된 해시값과 비교하면 된다. 만약 파일의 코드에 한 글자라도 변조가 있었다면 완전히 다른 해시값이 나올 것이기 때문이다.

하지만 문제가 있다. 해시값이 적힌 텍스트 파일이 정말 시드사이너 개발자가 공개한 것인지 어떻게 알까? 해커가 파일을 변조해 놓고 변조한 파일의 해시값을 텍스트 파일로 공개한 것인데 그걸 철석같이 시드사이너 개발자가 공개한 것이라고 믿을 수도 있는 것이 아닌가? 그래서 서명 파일이 있는 것이다. 우리는 해시값 파일의 서명이 시드사이너 개발자가 한 서명이 맞는지를 시드사이너 개발자의 공개키로 검증할 것이

다. 맞다면 우리가 다운로드한 시드사이너 해시값 텍스트 파일이 해커가 아닌 시드사이너 개발자가 만든 것이라고 확신할 수 있다.

이제 GPG (GnuPG)를 다운로드할 것이다. 이를 설치하기 위해서는 'Homebrew'와 'Xcode CLI Tools'를 먼저 설치해야 한다. 우리가 일반적으로 사용하는 컴퓨터 화면을 GUIgraphical user interface (그래픽 사용자 인터페이스)라고 하고, 해커나 개발자들이 사용할 것 같은, 터미널에서 명령어를 입력해 조작하는 컴퓨터 화면을 CLIcommand-line interface (명령줄 인터페이스)라고 한다. 명령줄 인터페이스인 터미널에서 설치 등의 명령어를 쉽게 입력할 수 있게 하기 위해 'Homebrew'와 'Xcode CLI Tools'를 설치하는 것이다.

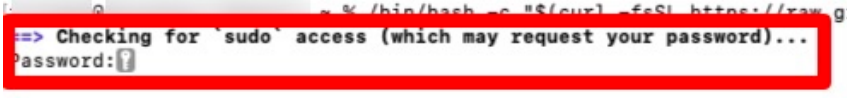
먼저 맥에서 터미널에 들어간다.



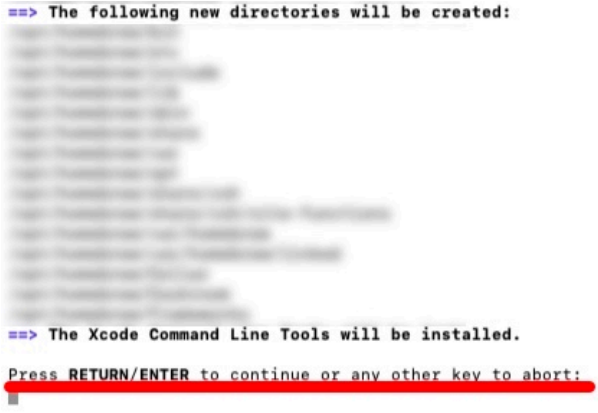
터미널에서 다음 명령어를 입력한다. 이는 'Homebrew'와 'Xcode CLI Tools'를 설치하는 명령어다.

```
/bin/bash -c "$(curl -fsSL https://raw.
  githubusercontent.com/Homebrew/install/
  HEAD/install.sh)"
```

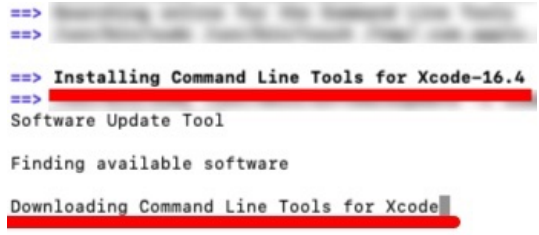
맥에 설정된 비밀번호를 입력한다. 입력이 안 되는 것처럼 보여도 입력이 되고 있는 것이니 정확한 비밀번호를 입력한다.



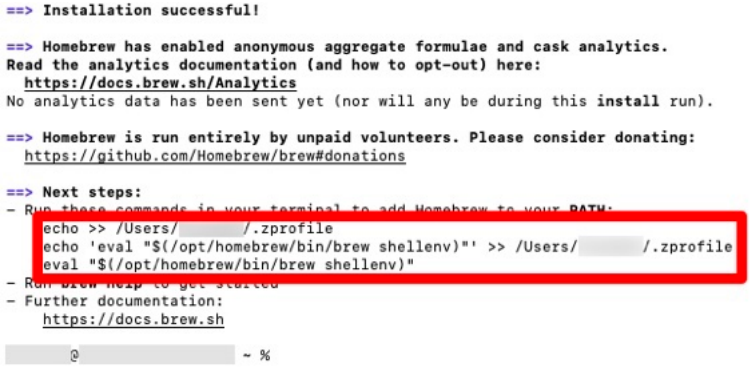
그러면 결과가 여러 줄 출력되다가, 'Xcode CLI Tools'를 설치할 것인지 묻는다. 엔터 키를 누른다.



이제 조금 기다려야 한다. 특히 **Downloading Command Line Tools for Xcode**와 **Installing Command Line Tools for Xcode**에서 한참 멈춘 것처럼 보일 수 있는데, 다운로드와 설치가 진행 중인 것이니 더 기다려야 한다.



설치가 다 되면 **echo**로 시작하는 명령어를 입력하라는 안내문이 나온다. 두세 줄 되는 이 명령어를 복사한다.



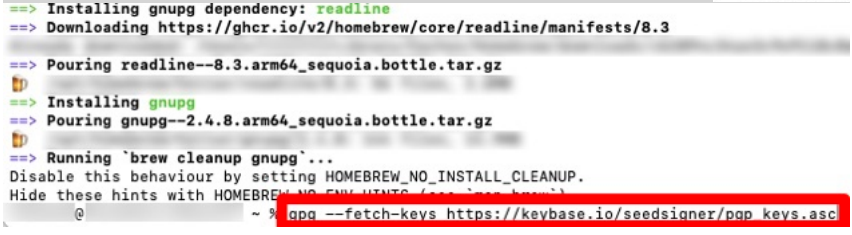
복사한 명령어를 붙여넣고 엔터 키를 누른다.

이제 GPG 설치를 위한 준비가 끝났다. 다음 명령어를 입력한다. GPG를 설치하는 명령어다.

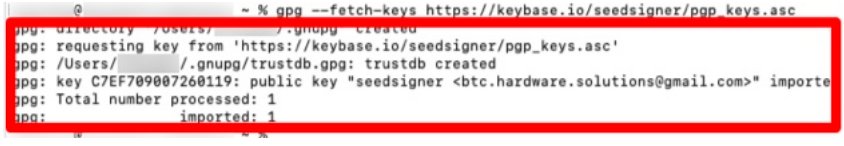
```
brew install gnupg
```

이제 시드사이너 개발자의 공개키를 가져올 것이다. 다음과 같이 입력한다. 보통 PGP 공개키는 keybase 웹사이트에 등록하여 사용하는데 여기 등록된 시드사이너 개발자의 공개키를 가져오는 것이다.

```
gpg --fetch-keys https://keybase.io/seedsigner/
   pgp_keys.asc
```

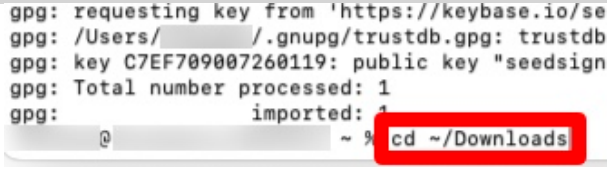


그러면 다음 사진처럼 결과가 표시되어야 한다.



이제 이미지 파일과 해시값 텍스트 파일, 서명 파일이 있는 '다운로드' 폴더로 들어갈 것이다. 다음 명령어를 입력한다.

```
cd ~/Downloads
```



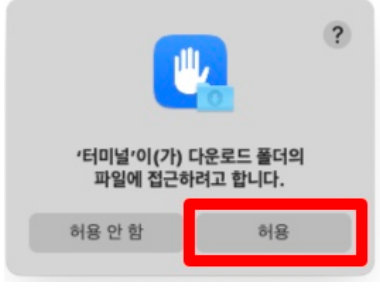
이제 다음과 같이 입력한다. 이는 시드사이너 개발자의 공개키와 해시값 파일을 통해 서명을 검증하는 명령어다.

```
gpg --verify [서명 파일 이름] [해시값 텍스트 파일 이름]
```

아마 다음과 같은 형태일 것이다. ?에는 버전 정보가 들어간다.

```
gpg --verify seedsigner.?.?.?.sha256.txt.sig
   seedsigner.?.?.?.sha256.txt
```

파일 접근 권한을 요구하면 [허용]을 누른다.



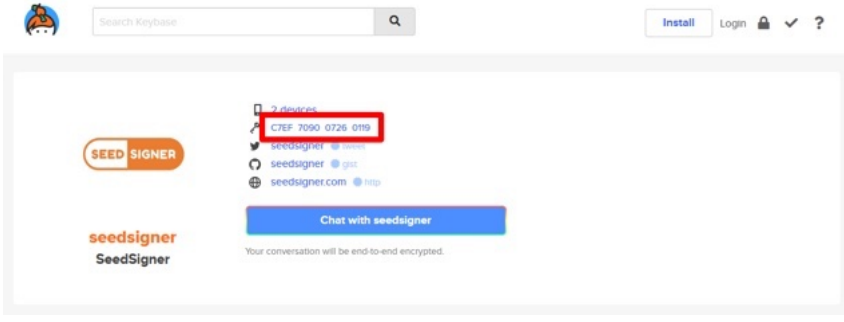
그러면 다음 사진과 같은 결과가 나올 것이다. 여기서 **Good signature** ~가 꼭 있어야 한다. 마지막에 나도는 공개키 지문도 확인해 놓자.

만약 이 결과가 나오지 않는다면 다시 시도해 보자. 그래도 나오지 않는다면 즉시 과정을 중단하고, 이미지 파일과 해시값, 서명 파일을 깃허브 공식 시드사이너 페이지에서 받은 것이 맞는지 확인해 보자.

터미널에 나온 공개키 지문을 대조하여 우리가 검증에 사용한 공개키가 정말 시드사이너 개발자의 것이 맞는지 확인할 것이다. 다음 웹사이트에 들어간다.

https://keybase.io/seedsigner

열쇠 옆에 있는 16자리 지문 코드를 눌러 지문 코드 전체를 확인한다.

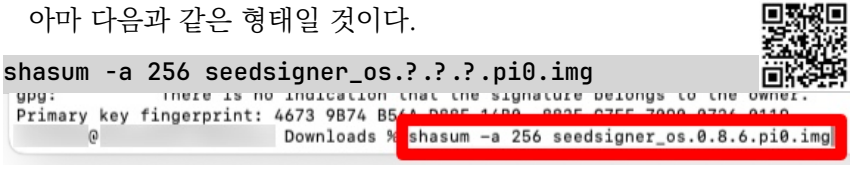


지문 코드 전체가 터미널에 나온 지문 코드와 일치하는지 확인한다.

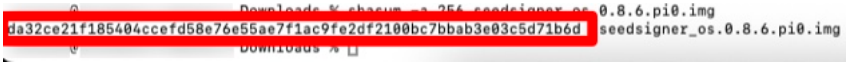
여기까지 되었다면 이제 시드사이너 프로그램을 해싱하여 해시값을 비교해 볼 차례다. 다음과 같이 입력한다. 이는 시드사이너 이미지 파일을 SHA256 함수로 해싱하는 명령어다.

```
shasum -a 256 [이미지 파일 이름]
```

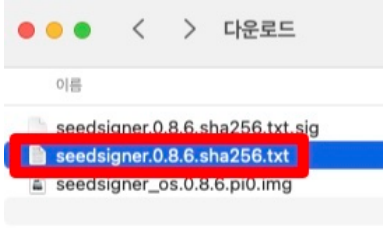
아마 다음과 같은 형태일 것이다.



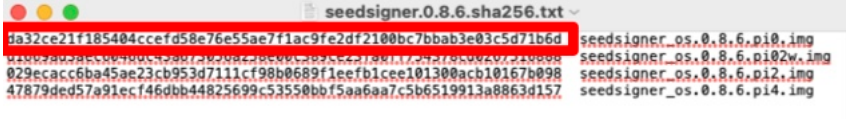
파일의 해시값을 계산하고 출력할 것이다.



이제 해시값 텍스트 파일(seedsigner.?.?.?.sha256.txt)을 열어본다.



그러면 seedsigner_os.?.?.?.pi0.img 왼쪽에 해시값이 있을 것이다.



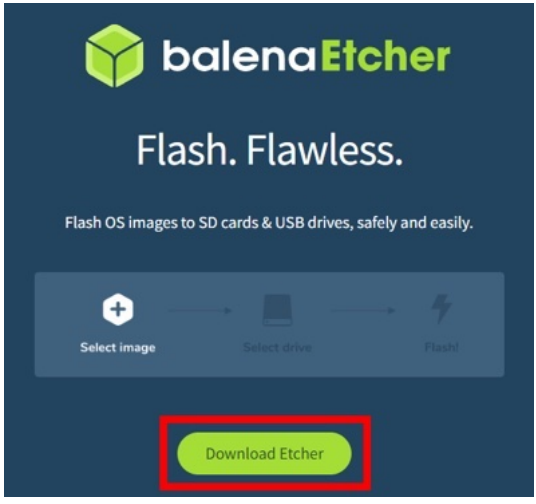
이 값이 터미널에 나와 있는 해시값과 같다면 이미지 파일에 변조가 일어나지 않은 것이다. 이제 이 이미지 파일을 이용해 시드사이너 부팅용 마이크로SD카드를 만들 것이다.

부팅 마이크로SD카드 만들기

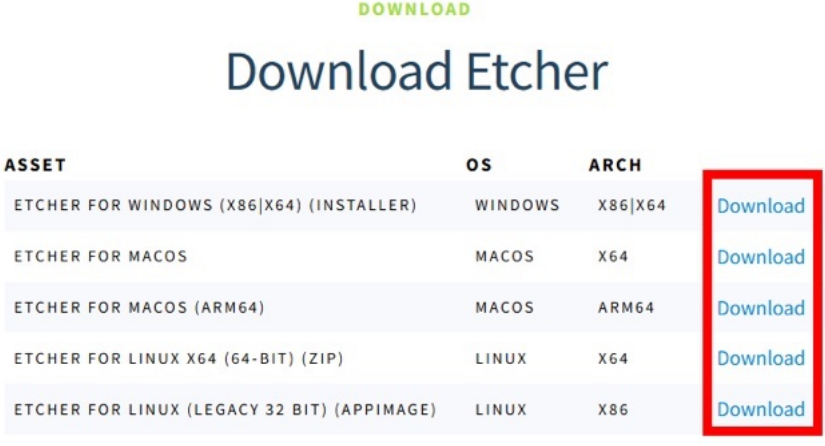
이제 마이크로SD카드를 부팅용으로 만들기 위해 발레나에처 프로그램으로 구워야 한다. 아래 링크에서 발레나에처 프로그램을 다운로드한다.

https://etcher.balena.io/

[Download Etcher]를 누른다.

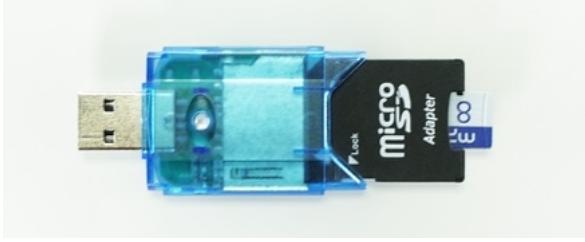


자신의 컴퓨터 운영체제에 맞는 버전을 다운로드한다.

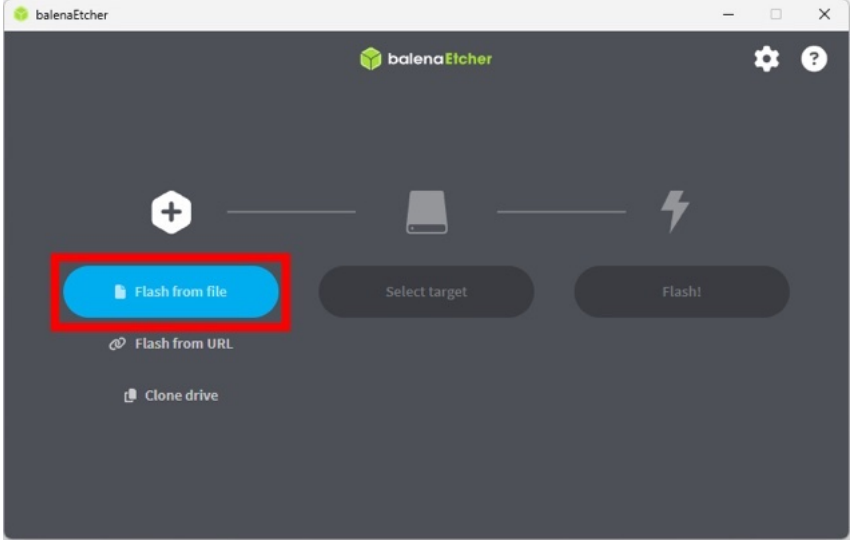


설치가 완료되었으면 발레나에처를 실행한다.

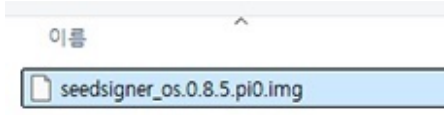
컴퓨터에 마이크로SD카드를 꽂는다.



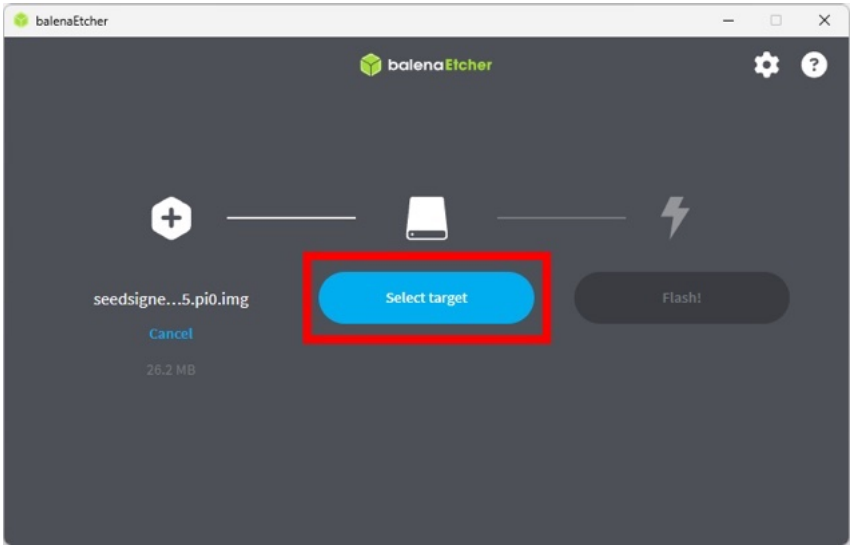
발레나에처를 실행하면 다음과 같은 화면이 나온다. [Flash from file]을 누른다.



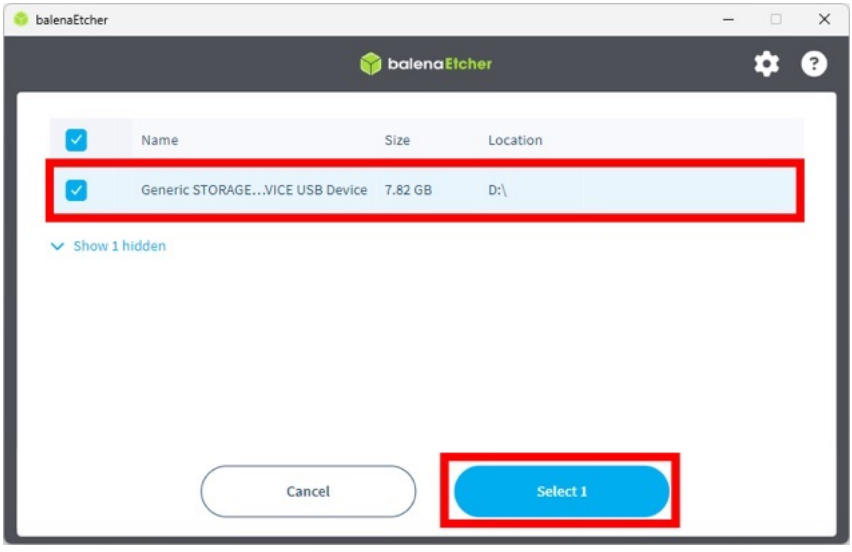
이미지 파일을 선택하는 창이 뜰 것이다. 아까 다운로드했던 시드사이너의 이미지 파일을 찾아서 더블 클릭하자.



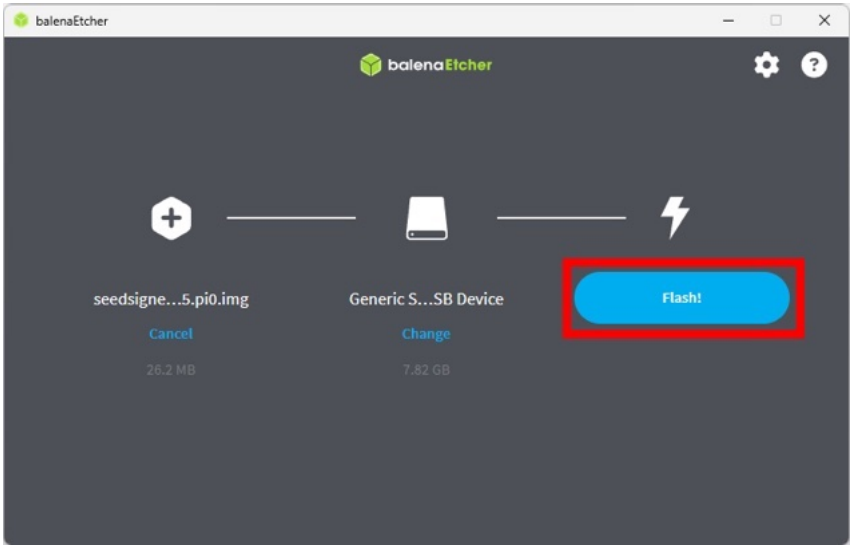
[Select target]을 누른다.



우리가 꽂은 마이크로SD카드 리더기 USB를 선택한다.



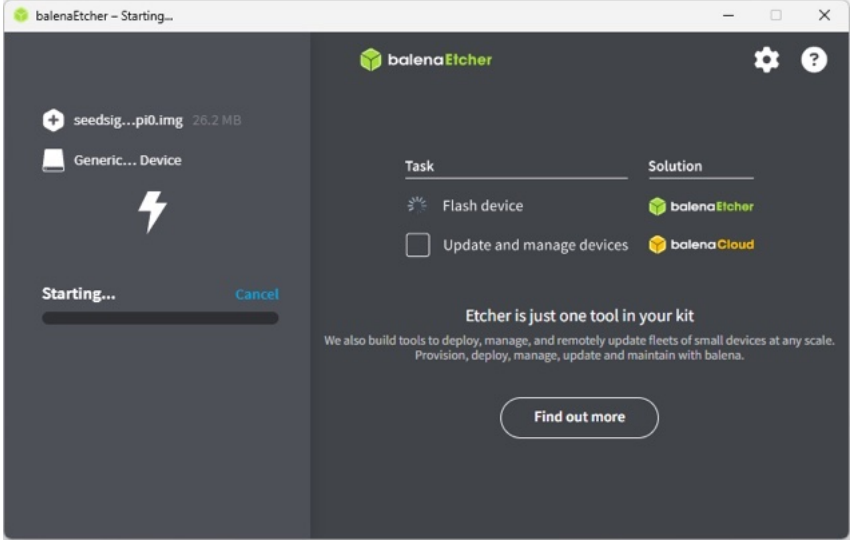
이제 [Flash]를 누른다.

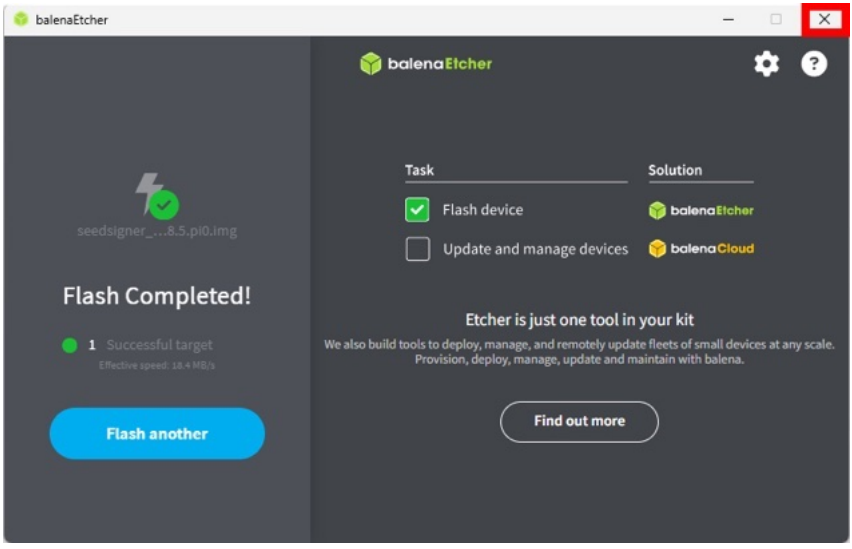


다음과 같은 화면이 뜨다가 'Flash Completed!'가 뜰 것이다. 뜨면 오른쪽 위 [x] 버튼을 누르고 마이크로SD카드를 빼면 된다.

만약 Flash에 실패하면 마이크로SD카드를 초기화하고 다시 플래싱해야 한다. 이때 일반적인 포맷 방법으로는 안 되는데, '부팅 USB 초기화 방법'이라고 검색하면 결과가 많이 나온다.

윈도우의 경우 윈도우 키 + R → cmd 입력 후 실행 → 터미널이 나오면 **`diskpart`** 입력 → **`list disk`** → 마이크로SD카드 디스크 번호 확인 → **`select disk [디스크 번호]`** → **`clean`**을 입력하면 된다. 그러고 다시 포맷하고 처음부터 진행하면 된다.

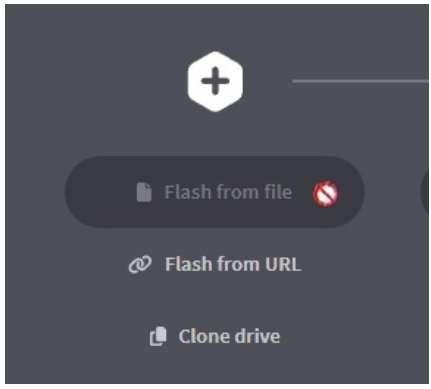




플래싱이 완료되었다면 이제 '무선 통신 모듈 제거(라즈베리파이 제로 W 보드만 해당)' 절로 넘어가면 된다. 혹시라도 발레나에처로 시드사이너 이미지 파일 플래싱이 안 될 경우에는 다음 절을 따라 하면 된다.

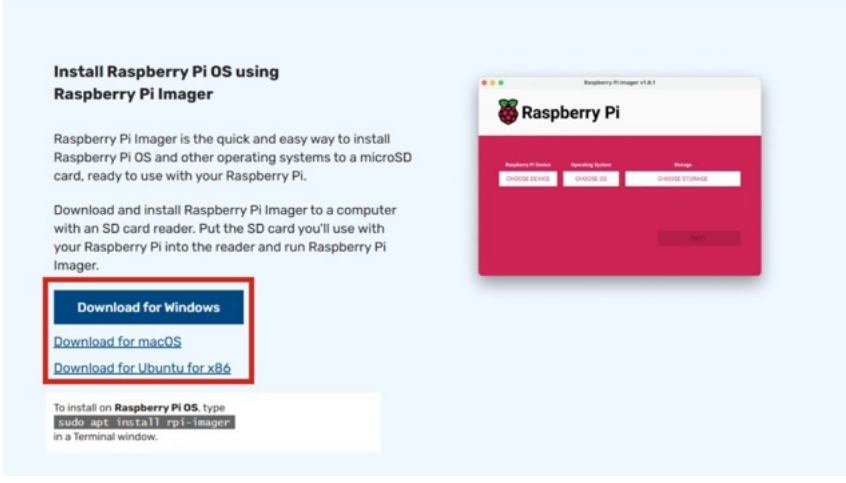
발레나에처로 시드사이너 이미지 파일 플래싱이 안 될 경우 해결 방법

발레나에처에서 종종 시드사이너 이미지 파일 플래싱이 안 되는 경우가 있다.

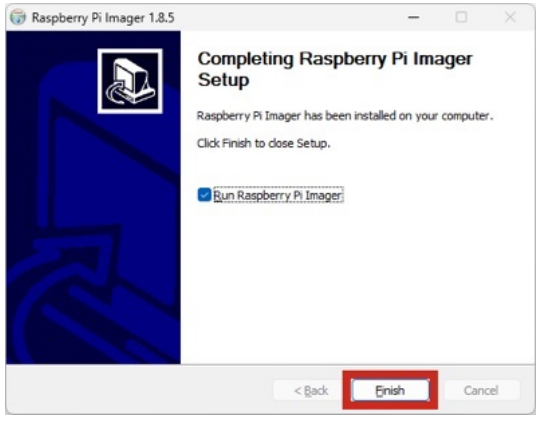


이때는 '라즈베리파이 이미저'를 사용하여 해결할 수 있다. 먼저 아래 웹사이트에 접속하여 스크롤을 내리고, 자신의 운영체제에 맞는 라즈베리파이 이미저를 다운로드한다.

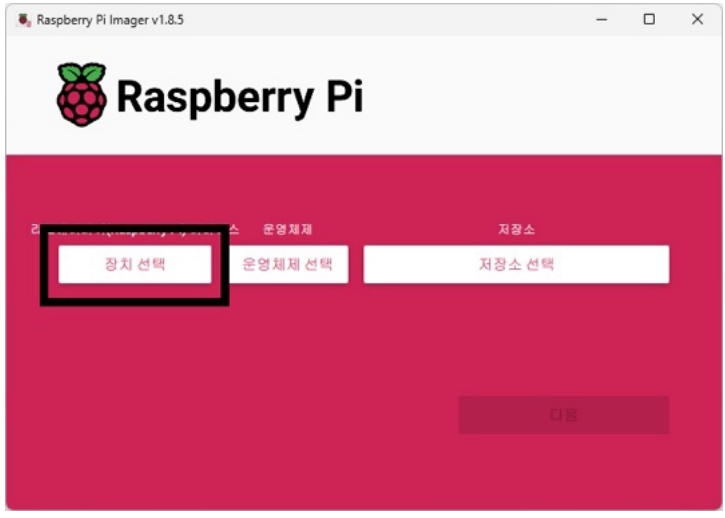
https://www.raspberrypi.com/software



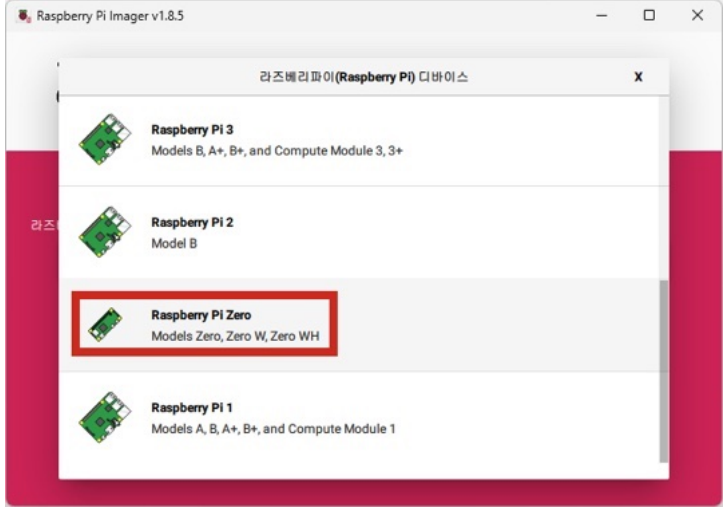
다운로드가 완료되면 파일을 실행하여 라즈베리파이 이미저를 설치한다.



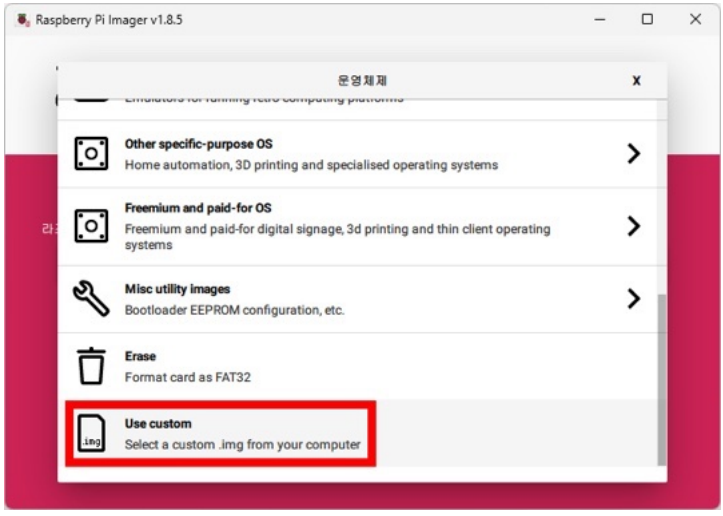
라즈베리파이 이미저를 실행한다. 먼저 [장치 선택]을 누른다.



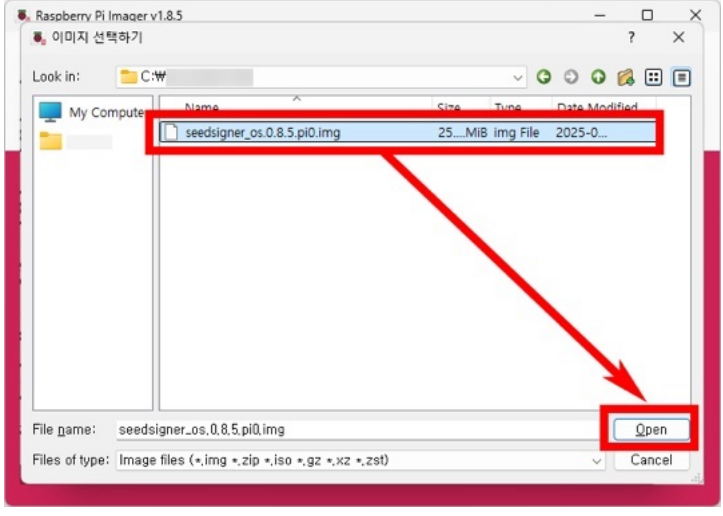
장치에서 [Raspberry Pi Zero]를 선택한다.



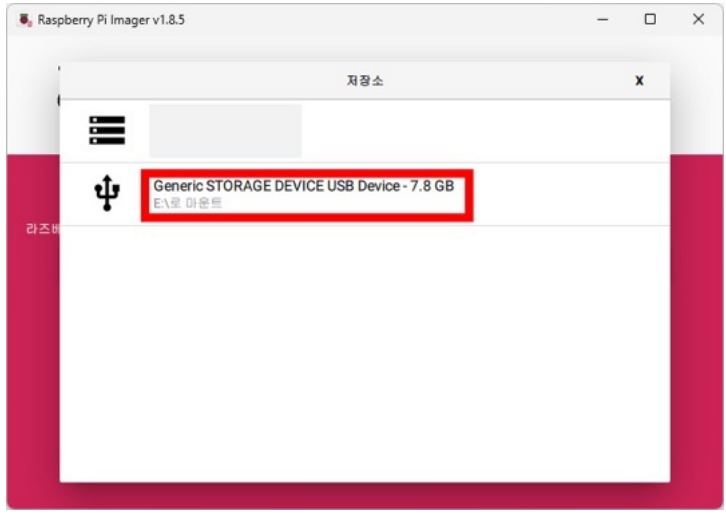
운영체제 선택 창에서는 스크롤을 아래로 내려 [Use custom]을 누른다.



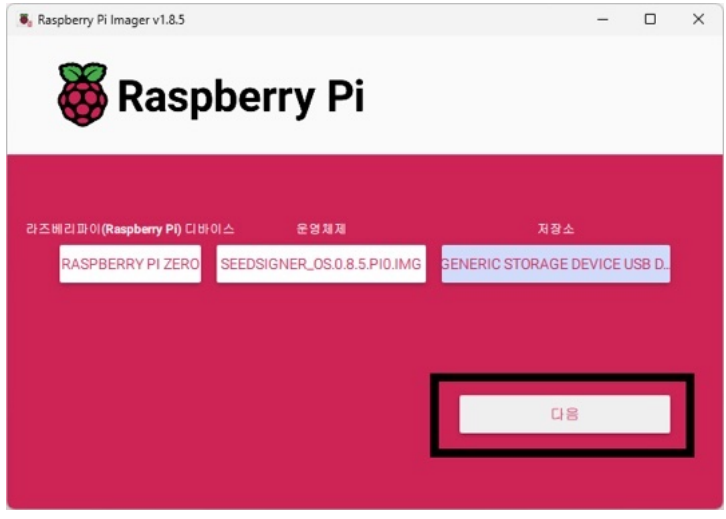
미리 다운로드했던 시드사이너 이미지 파일을 선택하고, [Open]을 누른다.



저장소에서는 시드사이너 부팅용으로 사용할 마이크로SD카드를 선택한다.



[다음]을 누른다.



OS 커스터마이징 설정을 할 건지 물어보면 [아니요]를 눌러 넘어간다.

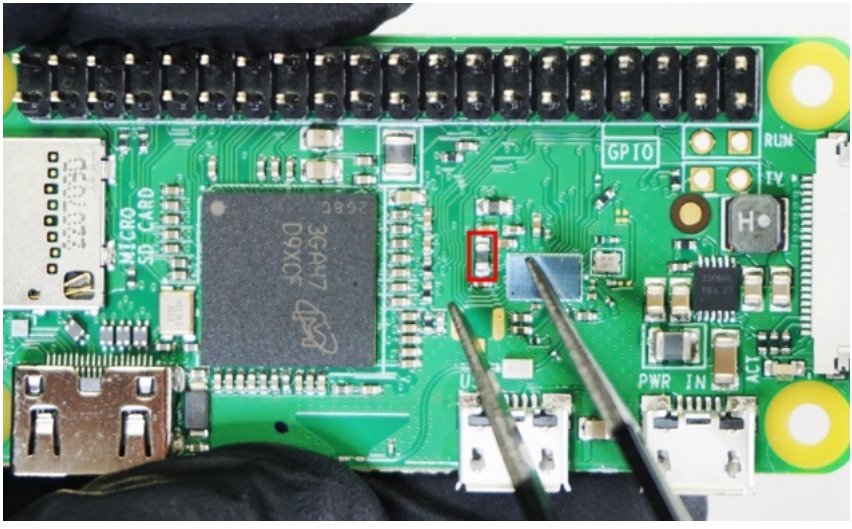
데이터가 지워질 거라는 안내문이 나오면 [예]를 누른다.

이제 시드사이너 부팅용 마이크로SD카드가 만들어졌다.

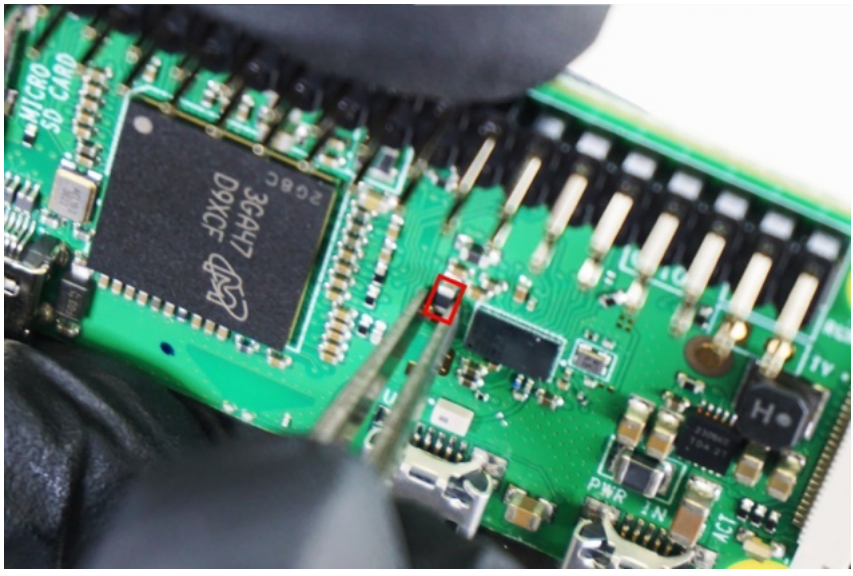
무선 통신 모듈 제거(라즈베리파이 제로 W 보드만 해당)

라즈베리파이 제로 W 보드의 경우 완전한 에어-갭 상태를 만들기 위해서는 무선통신 모듈을 아예 단선시켜야 한다(라즈베리파이 제로 보드를 구매했다면 다음 절로 넘어가면 된다). 한 가지 부품만 제거하면 모든 통신 모듈이 작동되지 않는다. 아래 그림에 빨간색 네모로 표시된 부품을 제거하면 된다.

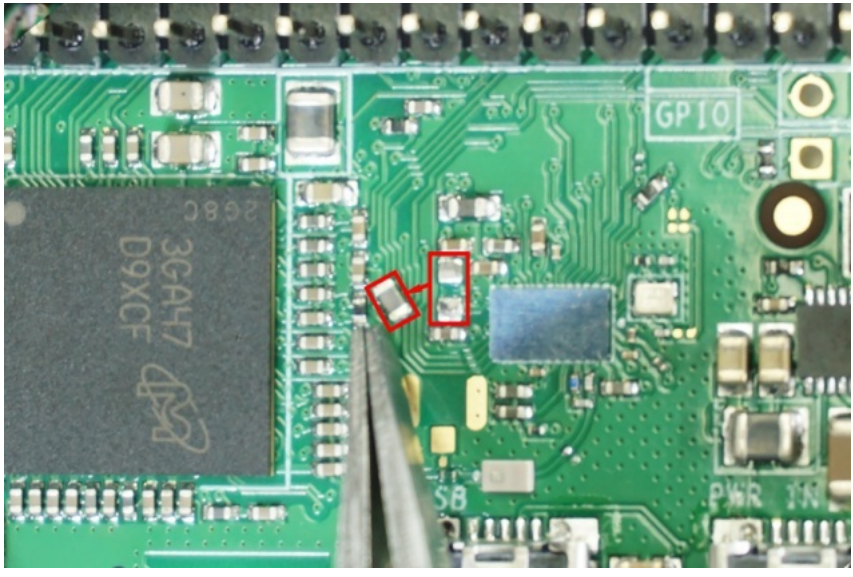
이 부품은 전기가 CYW43438 칩으로 가는 전압을 변경해 주는 인덕터이다. 이 부품을 부수면 무선 통신 모듈로 가는 전원이 차단된다. 따라서 이 부품이 제거되면 와이파이 랜/블루투스 통신 전부 불가능해진다. 우리는 일부러 와이파이와 블루투스가 안 되도록 만드는 것이다.



부품을 제거할 때는 핀셋으로 잡고 떼면 된다. 핀셋이 없는 경우 얇은 일자 드라이버로 세게 밀면 된다. 이때 다른 부품이 상하지 않도록 주의하라.

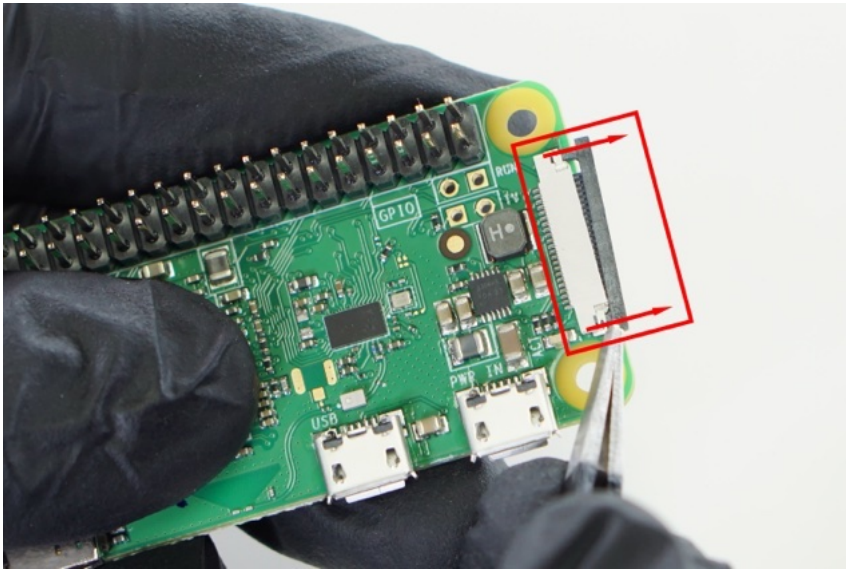


다음 사진은 부품을 떼어낸 모습이다.

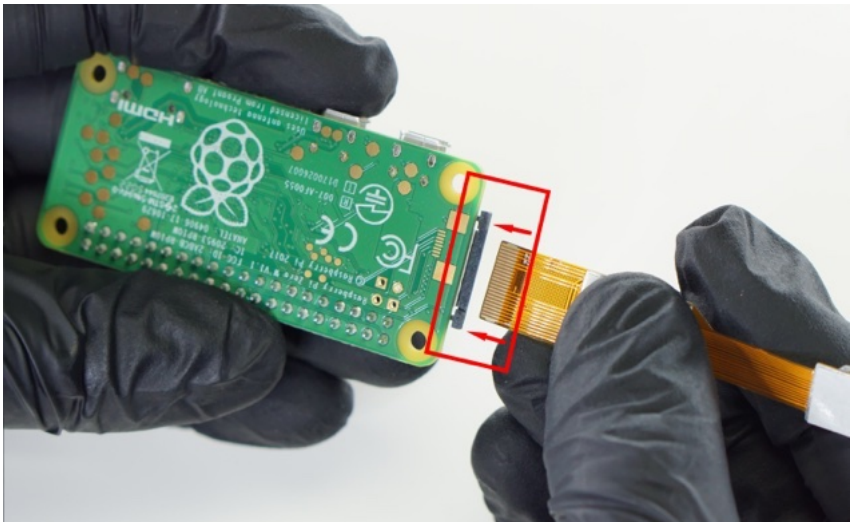


시드사이너 조립

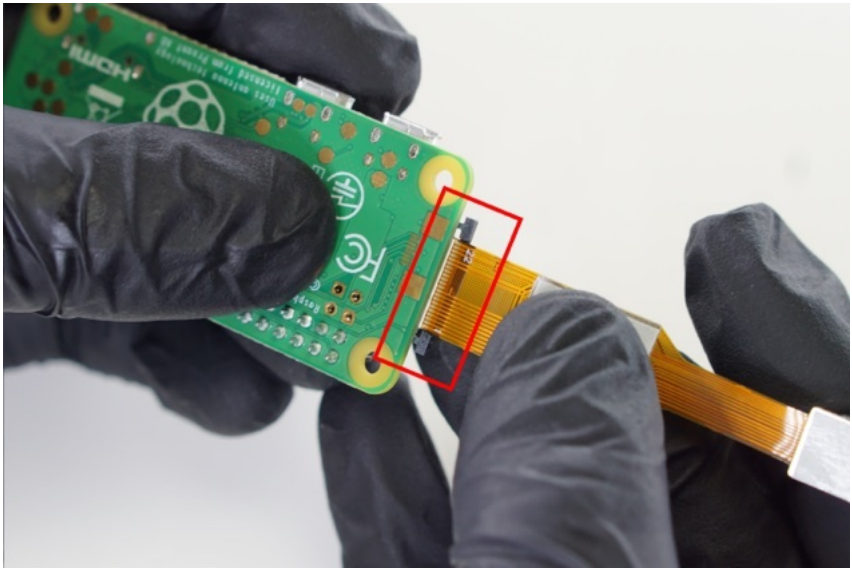
이제 시드사이너를 조립하자. 먼저 카메라부터 연결하겠다. 라즈베리파이 보드 앞면을 보면 다음 사진과 같이 카메라 모듈을 연결할 부분에 검은색 캡이 있다. 이걸 살짝 밀면 열리는데 양쪽 모두 열어준다.



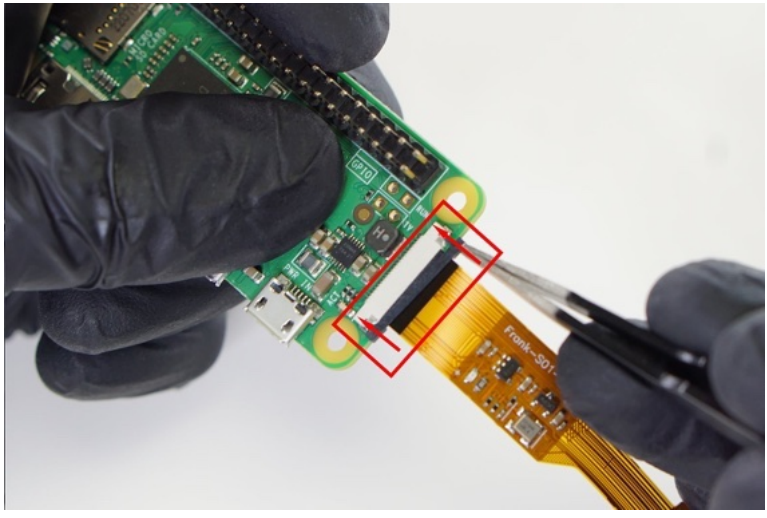
이제 카메라 모듈을 끼운다. 방향에 주의해야 한다. 금색 전선이 있는 부분이 뒷면에 오도록 해야 한다. 사진을 참고하라. 금색 부분이 라즈베리파이 보드 뒷면을 향해야 한다.



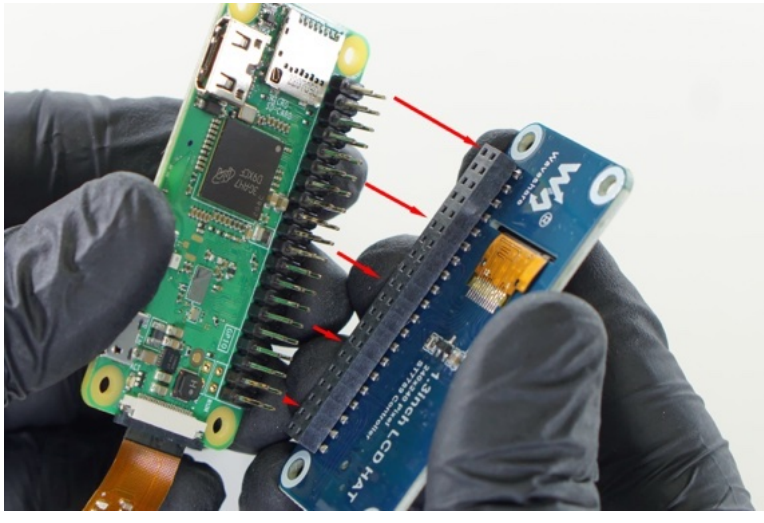
끼우면 다음과 같은 모습이 된다.

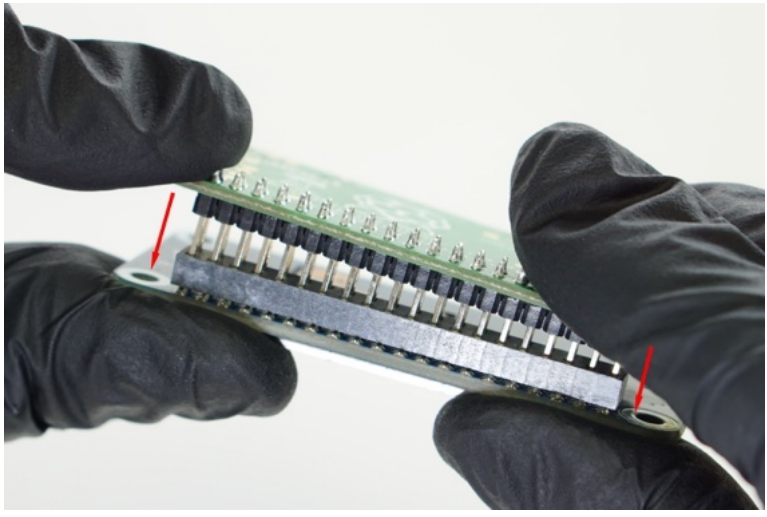


라즈베리파이 보드를 다시 앞면으로 돌려 카메라 모듈이 끼워진 부분의 검은색 캡을 다시 끼워준다.

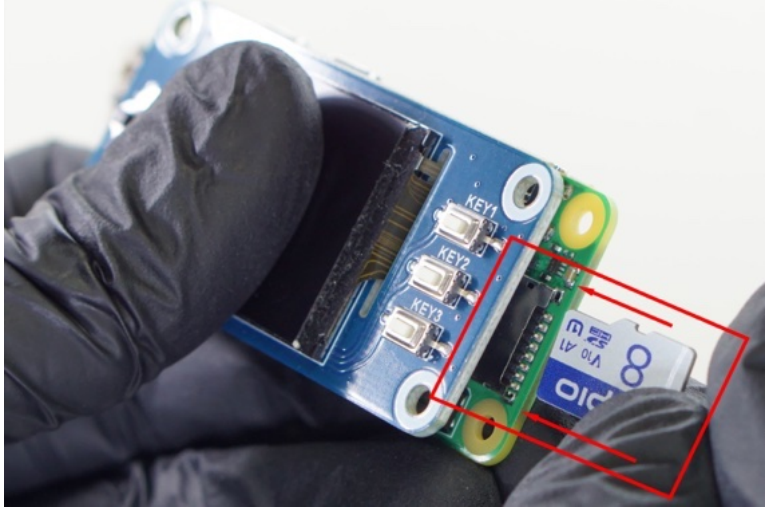


이제 LCD를 연결한다. 사진과 같이 연결하면 된다. 핀이 휘어지지 않도록 주의하여 꽂는다.

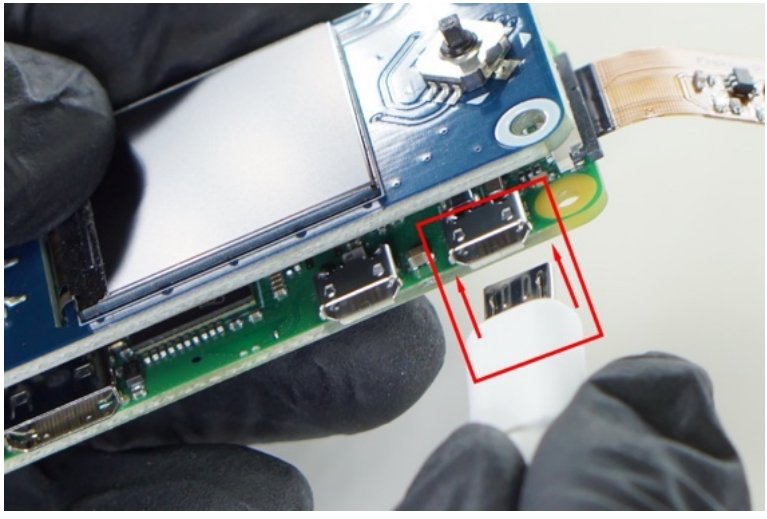




앞에서 시드사이너 부팅용으로 만들었던 마이크로SD카드를 라즈베리파이 보드 오른쪽에 꽂는다.



이제 전원선을 연결하자. 전원선은 오른쪽에 꽂아야 한다. 마이크로 5핀을 꽂는 부분이 2개가 있어서 헷갈릴 텐데 오른쪽에 꽂아야 한다. 왼쪽은 충전도 되고 저장장치에도 접근할 수 있는 5핀 포트다. 오른쪽은 충전만 되는 포트다.



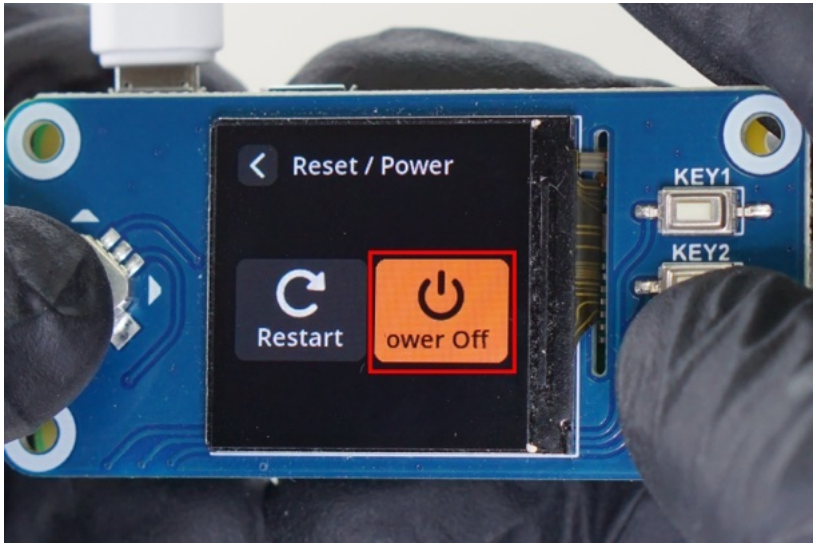
잠시 기다리거나, 조이스틱을 수직으로 누르면 시드사이너 화면이 나올 것이다.

홈 화면이 나오면 다시 조이스틱을 눌러 [Scan]을 누른다.

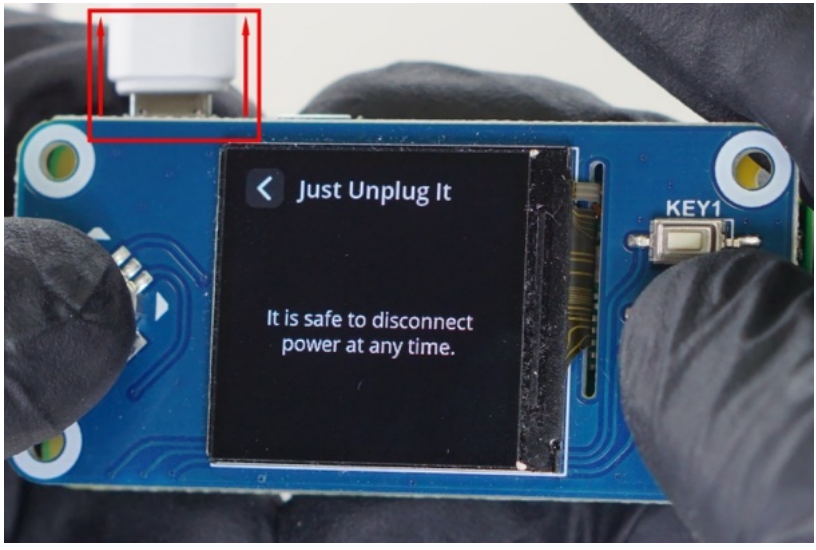
카메라 화면이 잘 나오는지 확인한다.

조이스틱을 ↑ 방향으로 밀고 전원 버튼을 누른다.

조이스틱을 → 방향으로 민 후 [Power off]를 누른다.



다음 사진과 같은 화면이 뜨면 전원선을 분리한다.

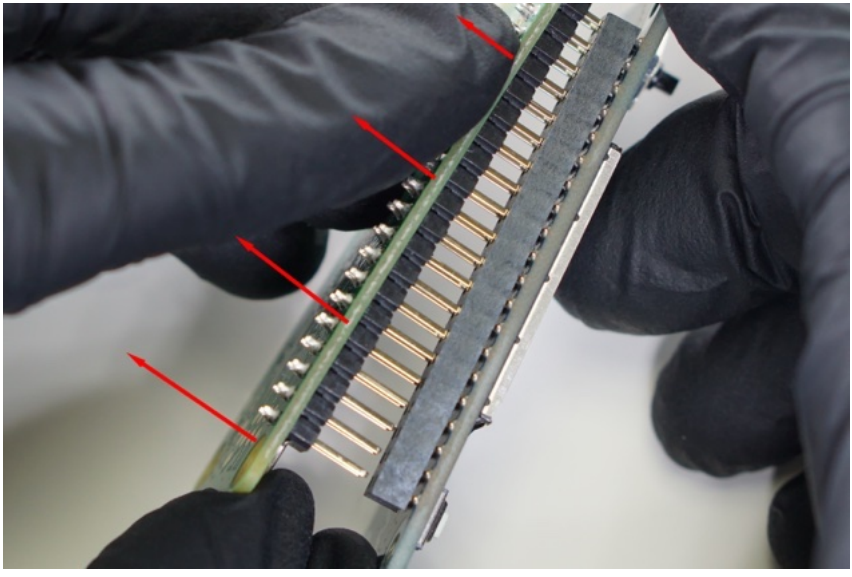


시드사이너 케이스까지 조립

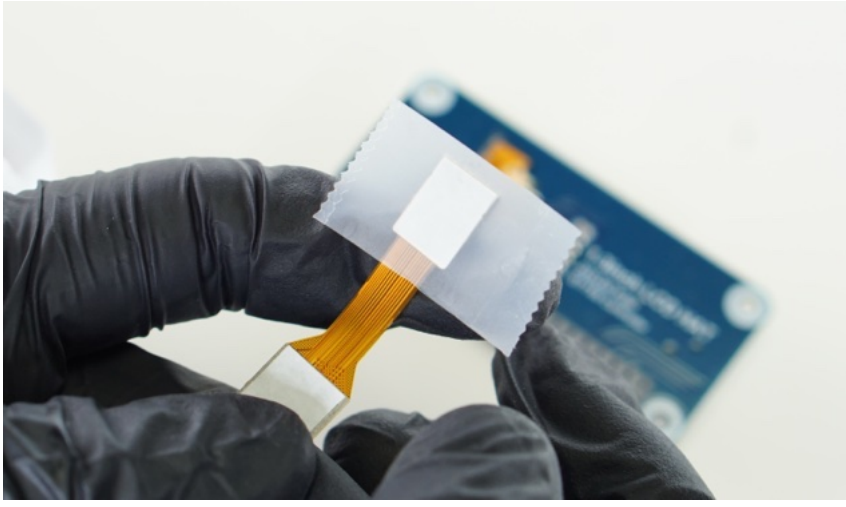
이제 시드사이너가 잘 작동하는 것을 확인했으니 케이스까지 조립하자. 케이스는 어디서 샀는지에 따라 조립 방법이 달라진다. 필자는 '비트키트' 케이스를 기준으로 글을 쓰겠다.

먼저 시드사이너를 다시 분해해야 한다. 전원선을 뽑았으면 마이크로SD카드를 제거한다.

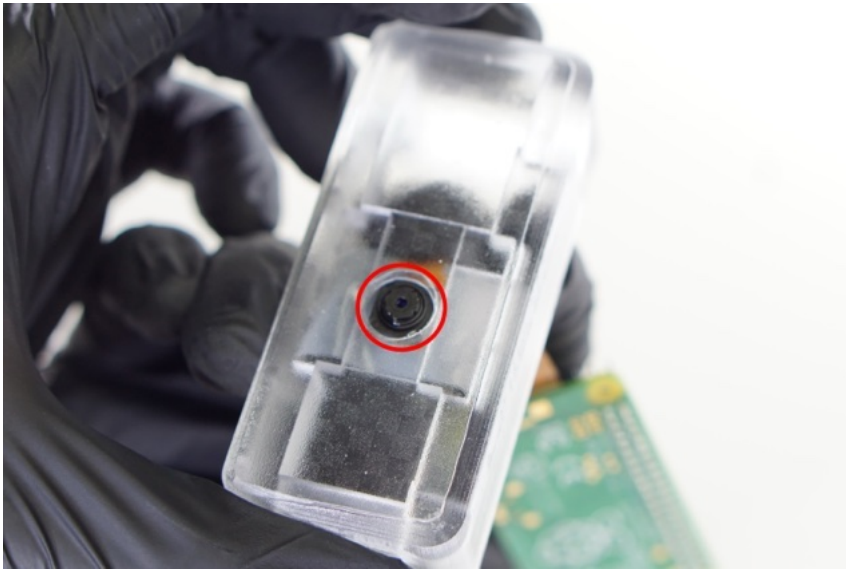
LCD도 제거해야 하는데, 핀이 휘어지거나 부러지지 않도록 조심해서 뽑는다. 힘을 좀 주어야 한다.

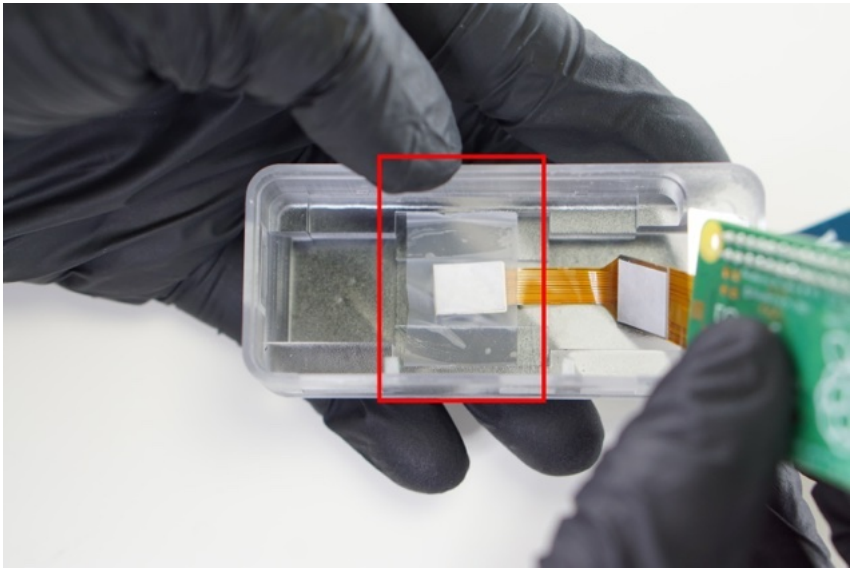


분리가 되었으면 이제 카메라 뒷면에 테이프를 붙인다.

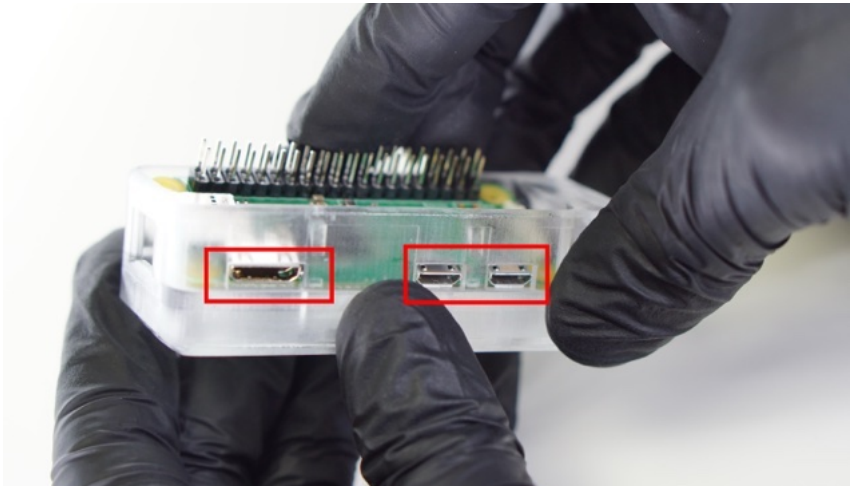


시드사이너 케이스 뒷면에서 카메라의 위치를 보고, 테이프를 붙여 카메라를 고정한다.

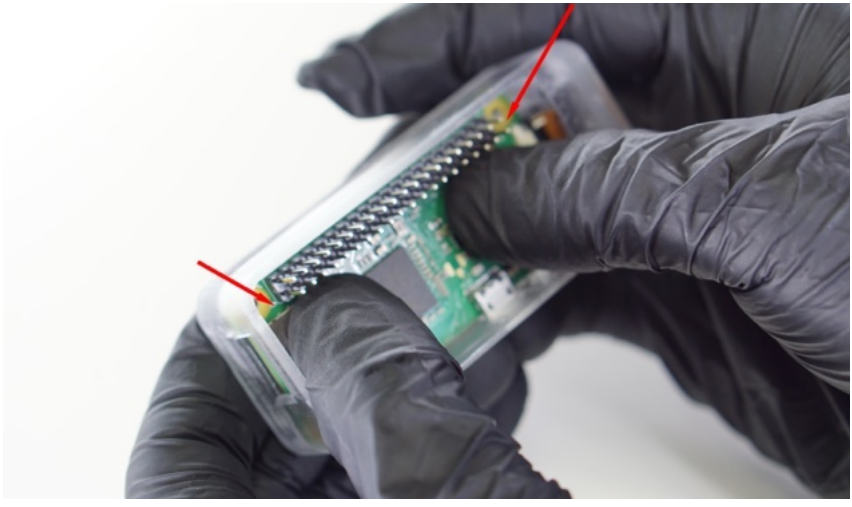




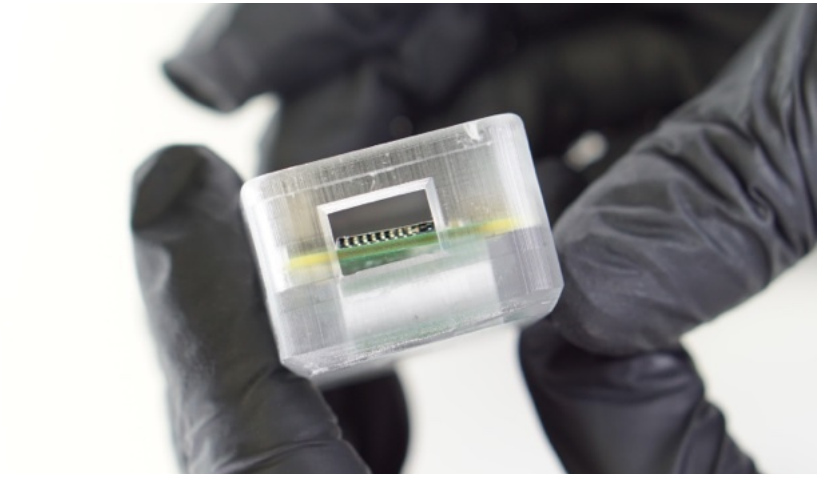
이제 라즈베리파이 보드를 시드사이너 케이스에 결합할 것이다. 꼭 포트를 먼저 맞춰야 한다. 라즈베리파이 보드를 기울여 각 포트가 케이스 구멍에 맞도록 위치시킨다.



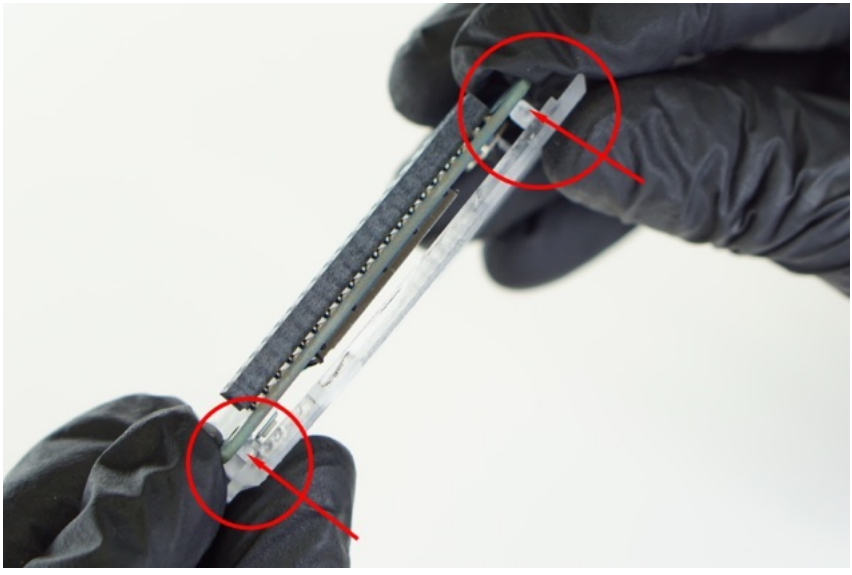
라즈베리파이 보드의 반대편을 눌러 보드를 케이스에 밀착시킨다.

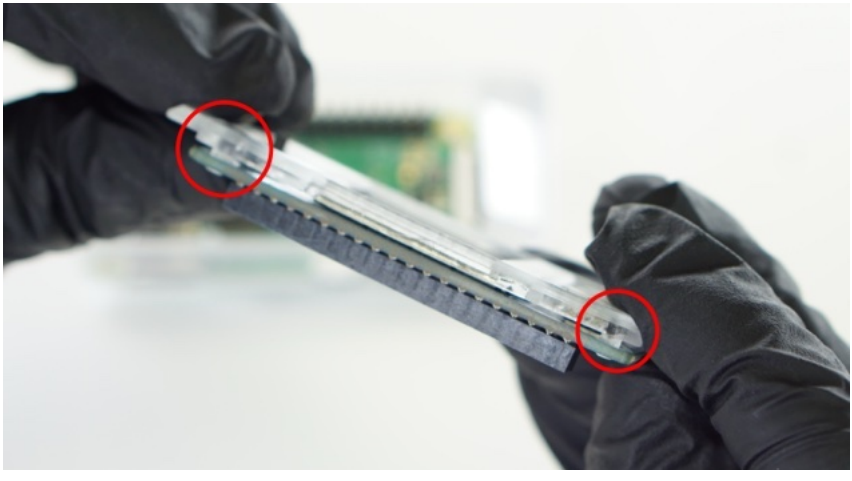


밀착시킨 뒤 케이스 옆면의 모습은 다음과 같다.



LCD에 케이스 덮개를 조립할 것이다. LCD 보드의 네 귀퉁이에 구멍이 있다. 그 구멍에 케이스 덮개를 끼우면 된다. 너무 꽉 끼우다가 LCD 보드나 케이스 덮개가 상하지 않도록 주의하자.

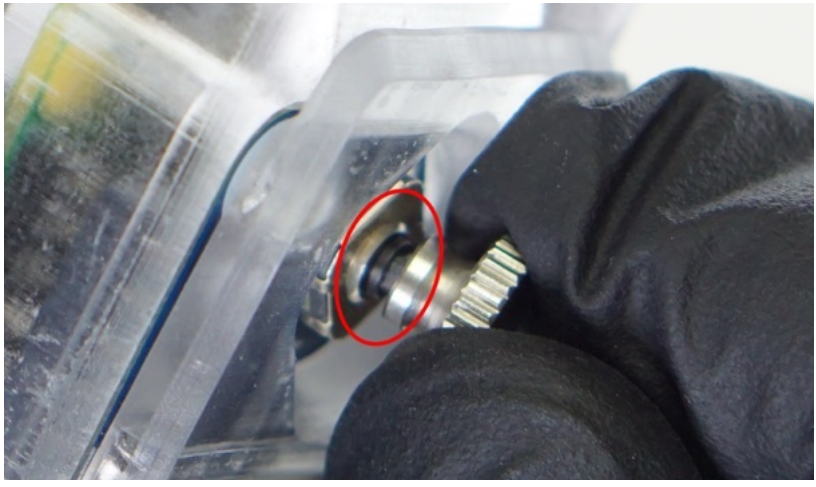




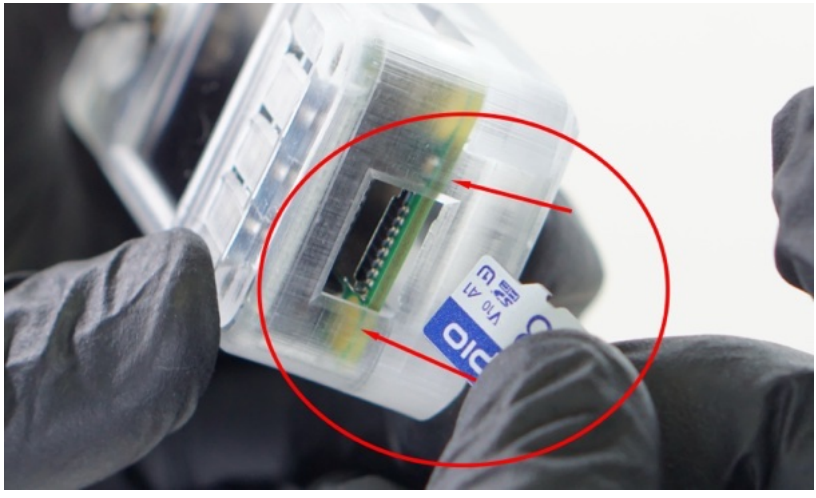
이제 라즈베리파이 보드와 LCD를 연결한다. 이번에도 핀이 상하지 않도록 주의하여 끼운다.

마지막으로 조이스틱 캡을 돌려서 끼우면 된다. 주의할 점이 있다. 조이스틱 캡을 너무 끝까지 꽉 끼우면 안 된다.

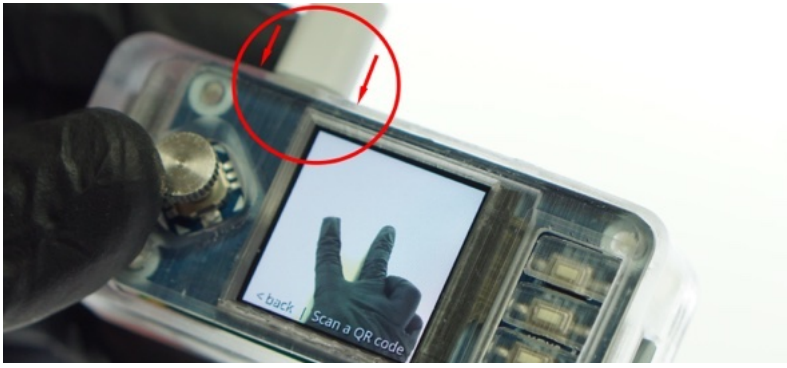
다음 사진을 보면 끝까지 꽉 돌리지 않고 약간 틈을 남겨둔 것을 알 수 있다. 끝까지 꽉 돌리면 조이스틱이 잘 안 눌리기 때문에 약간 틈을 남기는 것이다.



이제 마이크로SD카드를 꽂는다.



전원선을 꽂고, 다시 카메라가 잘 되는지 등을 확인한다.



이렇게 해서 시드사이너 조립이 끝났다.

지갑 생성

이제 시드사이너에서 주사위를 굴려 지갑을 생성하는 방법을 알아보자. 시드사이너 조작 방법은 조이스틱으로 상하좌우를 움직이면 된다. 무언가를 선택할 때는 왼쪽에 있는 조이스틱을 수직으로 누르거나, 오른쪽의 세 개 버튼 중 아무거나 누르면 된다.

홈 화면 → [Seeds] → [Create a seed]를 선택한다.

맨 위 카메라 모양의 [📷 New seed]는 사진을 엔트로피로 삼아 지갑을 만드는 방식이다. 두 번째에 있는 주사위 모양의 [🎲 New seed]는 주사위를 던져 엔트로피를 만들고 지갑을 만드는 방식이다. 세 번째에 있는 [Calc 12th/24th word]는 동전을 직접 던져 니모닉에 대응시키는 등의 방식을 쓸 때 마지막 니모닉 단어를 계산해 주는 기능이다. 우리는 주사위를 직접 던져 지갑을 만들 것이므로 두 번째에 있는 주사위 모양의 [🎲 New seed]를 선택한다.

단어 수는 12단어와 24단어를 선택할 수 있다. 12단어로 할지 24단어로 할지 고민이 될 것이다. 필자는 주변인에게 셀프 커스터디를 알려줄 때, 12단어는 충분한 것이고, 24단어는 과도한 것이라고 말한다. 12단어도 똑같이 재현하는 것은 불가능하다. 그러나 보안에 있어서는 과도한 것도 나쁘지 않다. 12단어는 외우기 쉽다는 장점이 있으므로 자신이 선택하면 된다. 비트코인은 자신이 온전히 통제권을 갖는 것이므로 누군가 정해줄 수 없고 자신이 직접 선택해야 할 일이 많다.

이제 주사위를 던져보자. 12단어 니모닉을 만들 것이라면 주사위를 50번, 24단어 니모닉을 만들 것이라면 주사위를 100번 던지면 된다.

어떤 다른 사람이 주사위를 50번 연속으로 당신과 똑같이 던질 확률은 로또 1등에 당첨될 확률보다 9,000만×1조×1조 배 더 희박하다. 우주에서 이런 일이 일어나는 것은 불가능하다. 필자는 12단어를 선택해 진행해 보겠다.

주의할 점이 있다. 주사위를 던지거나 니모닉을 기록할 때는 반드시 주변에 카메라가 없는지 확인해 보고 하라. 또한 전자기기가 있는 곳에서 주사위의 눈이나 니모닉을 소리 내 읽으면 안 된다. 필자는 니모닉을 만들 때 아무 전자기기도 없는 방에서 만든다.

주사위를 다 던져서 입력했다면 [I Understand]를 누른다. 그러면 니모닉 목록을 보여줄 것이다.

니모닉 목록을 종이에 잘 기록한다. 종이가 불에 탈 것을 염려해 철판 등을 사용할 수도 있다.

이 사진에 나와 있는 니모닉을 절대 사용하지 말 것. 이 니모닉은 테스트용으로 쓰였으며 온라인에 노출되었다. 이 니모닉에서 만들어지는 주소에 비트코인을 보내면 영영 되찾지 못할 수도 있다.

[Next]를 누르면 [Verify(검증)] 버튼이 나온다. 이걸 선택한다.

번호에 맞는 니모닉을 고른다.

다 고르면 성공했다는 알림이 나온다. [OK]를 누른다.

MFP도 꼭 기록한다. 비트코인은 당연히 고객센터가 없는데, 자신이 생성한 지갑이 맞는지 확인하기 위해 MFP를 적는 것이다. 다른 지갑이면 MFP도 달라진다. 참고로 MFP가 겹칠 확률은 42억분의 1이다.

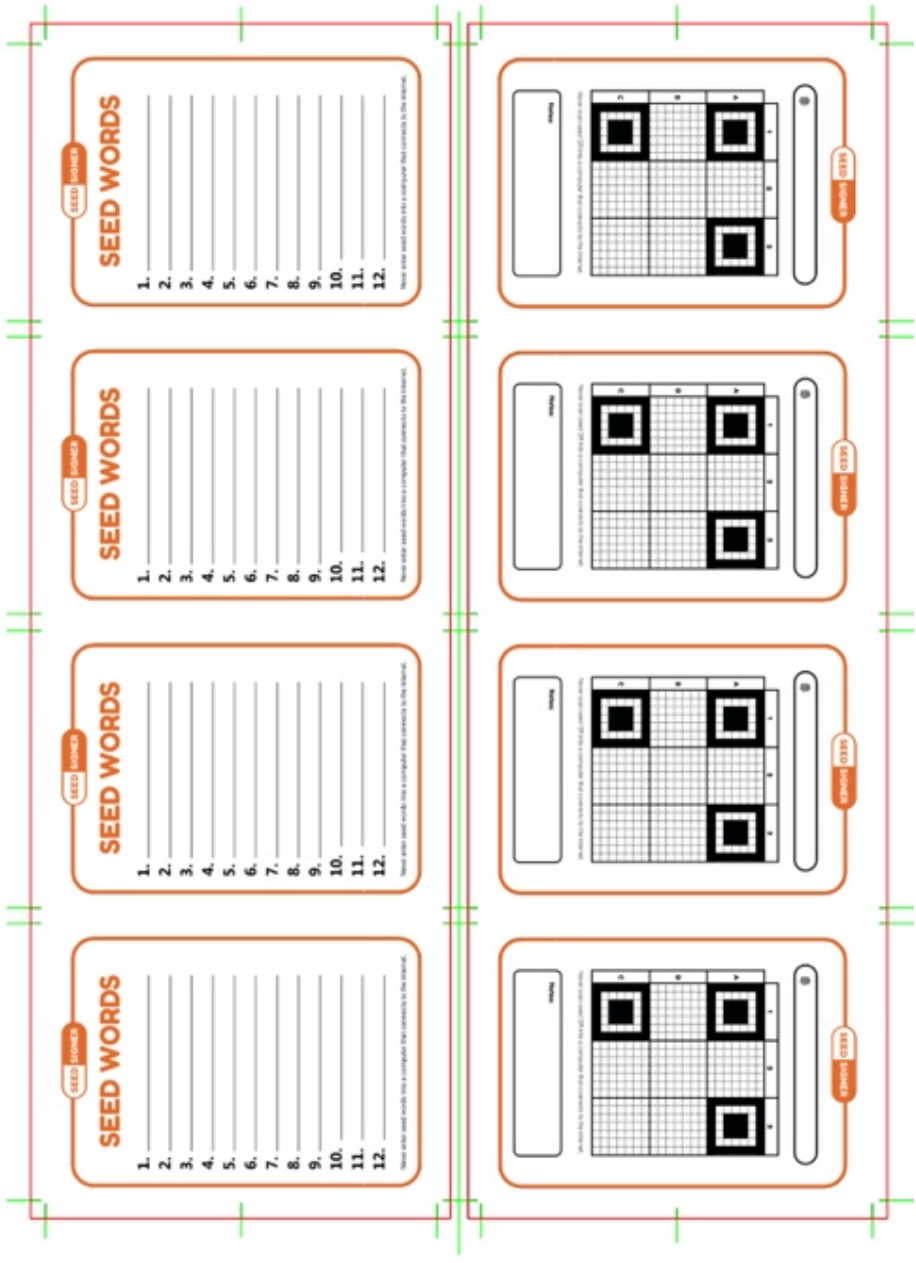
시드 QR 제작

시드사이너는 램(휘발성 저장공간)을 제외하고 저장장치가 없다. 따라서 니모닉이 저장되지 않기 때문에 매번 장치를 켤 때마다 니모닉을 입력해야 한다. 시드사이너를 쓸 거라면 니모닉을 외우는 것을 추천한다(당연히 니모닉을 물리적으로 백업한 상태에서 말이다).

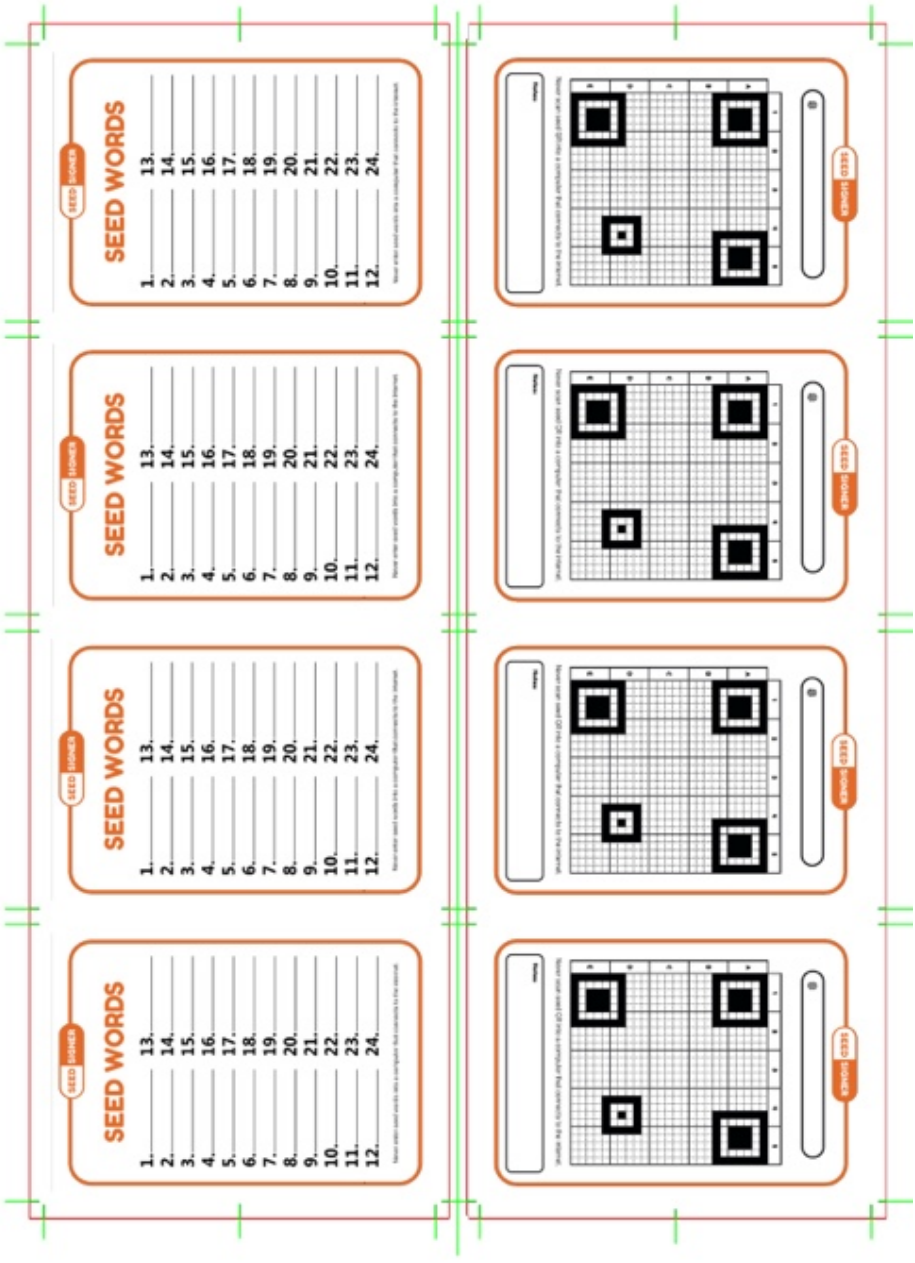
그러나 매번 니모닉을 입력하는 게 귀찮을 수도 있다. 그런 사람들은 시드 QR을 활용할 수 있다. 시드 QR을 만들어놓으면 이 QR 코드를 스캔했을 때 바로 니모닉을 불러온다(시드 QR도 니모닉 단어와 마찬가지로 보관에 주의를 기울여야 한다).

시드 QR 만드는 방법을 알아보자. 이미지에 대한 링크(QR 코드)는 다음 페이지에 첨부했다. 이미지를 먼저 인쇄하자.

시드 QR 21 × 21:



시드 QR 25 × 25:



홈 화면 → [Seeds] → [Backup Seed] → [Export as SeedQR]을 선택한다.

QR은 25×25와 21×21 중 선택할 수 있다. 25×25는 Standard QR (표준 QR)이고, 21×21은 Compact QR (압축된 QR)이다. 만약 니모닉이 24단어라면 Standard QR은 29×29, Compact QR은 25×25가 된다. Standard QR은 스마트폰 카메라로 찍으면 엔트로피 숫자가 그대로 인식되어 데이터가 노출되는데(※ 주의: 자신이 사용할 니모닉이라면 절대 시도하지 말 것. 스마트폰에 니모닉 정보가 노출된다), Compact QR은 스마트폰 카메라로 스캔해도 데이터 노출이 안 된다. 따라서 Compact QR이 좀 더 안전하고, 칸이 적어서 그리기도 쉽다. 필자는 이번에 25×25를 선택하여 QR 코드를 그려보겠다. 니모닉을 백업할 때와 마찬가지로 주변에 카메라가 전혀 없는 곳에서 진행하라.

[I Understand] → [Begin 25×25]를 선택한다.

그러면 칸마다 색칠해야 할 부분을 보여줄 것이다. 잘못 색칠하면 처음부터 다시 색칠해야 하므로 주의하자.

색칠이 완료되었다. 팔이 매우 아프다.

이 사진에 나와 있는 시드 QR을 스캔하여 지갑을 생성하지 말 것. 이 시드 QR은 테스트용으로 쓰였으며 온라인에 노출되었다. 이 시드에서 만들어지는 주소에 비트코인을 보내면 영영 되찾지 못할 수도 있다.
또한, 자신이 만든 시드 QR을 스마트폰 카메라로 스캔하지 말 것. 니모닉이 온라인에 노출될 수 있다.

Seed QR이 잘 인식되는지 확인하면 끝이다. [Confirm SeedQR]을 선택한다.

카메라로 직접 만든 QR 코드를 스캔한다. 스캔이 성공적으로 잘 됐다는 안내문이 나오면 [OK]를 누른다.

니모닉 입력하기 or 시드 QR 스캔하기

시드사이너는 어떤 데이터도 저장하지 않는다. 그래서 껐다 켤 때마다 니모닉을 새로 입력해야 한다.

이제 시드사이너에 니모닉을 불러올 것이다. 시드사이너 홈 화면 → [Seeds]에 들어간다.

[Scan a SeedQR]은 시드 QR을 스캔해서 니모닉을 불러오는 것이다. 시드 QR을 스캔하는 경우 그냥 홈 화면에서 [Scan]을 누르고 바로 시드 QR을 스캔해도 된다.

[Enter 12-word seed]는 12단어 니모닉을 입력하는 경우 사용한다.

[Enter 24-word seed]는 24단어 니모닉을 입력하는 경우 사용한다.

시드 QR을 스캔하거나 니모닉을 입력한다. 니모닉을 입력할 때는 조이스틱을 상하좌우로 움직이고, 조이스틱을 수직으로 누르면 단어가 선택된다. 오른쪽에 단어들이 뜨면 오른쪽 위아래 버튼을 이용해 이동할 수 있고, 오른쪽 가운데 버튼을 누르면 그 단어가 선택된다.

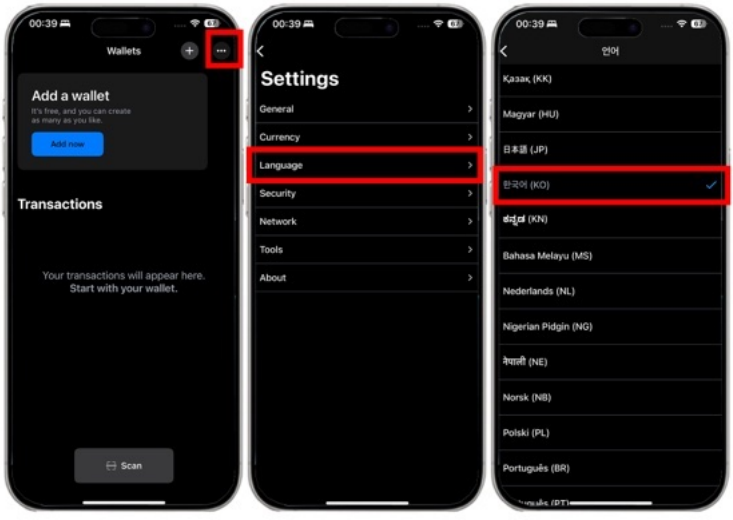
(상) 시드 QR 스캔, (하) 니모닉 입력

블루월렛에 확장 공개키 내보내 워치-온리 지갑 만들기

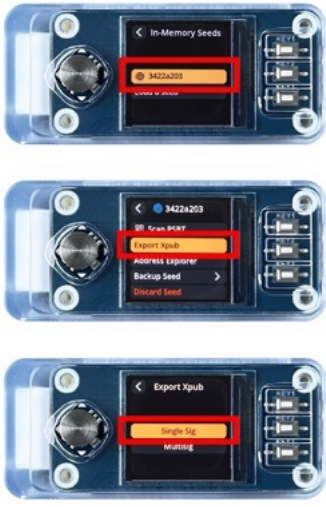
스마트폰에서 사용하는 워치-온리 지갑에는 크게 블루월렛과 넌척, 코코넛 월렛 등이 있다. 블루월렛은 잔오류가 많다는 단점이 있지만, 현재 한국어를 지원하기 때문에 영어가 불편한 사람들은 편하게 사용할 수 있다. 넌척은 블루월렛보다 훨씬 안정성이 있지만 한국어 지원이 안 돼서 영어를 못하는 경우 불편하다. 코코넛 월렛은 한국의 포우팀에서 개발한 지갑으로, 당연히 한국어가 지원되고 기능도 많다(심지어 고객센터도 있다). 워치-온리 지갑은 어느 하나만 사용하는 것보다는 두 가지 이상을 사용하며 교차 검증하는 것이 좋다.

블루월렛과 넌척, 코코넛 월렛을 먼저 설치하자. 구글 플레이스토어나 애플 앱스토어에서 BlueWallet, Nunchuk, 코코넛 월렛을 검색하고 다운로드한다. iOS 기준으로 설명하지만, 안드로이드도 크게 다르지 않다.

블루월렛 앱을 실행한다. 한국어가 편하다면 언어 설정부터 바꾸자. 오른쪽 위 점 세 개 → [Language] → [한국어]를 선택하고 뒤로 가기를 누른다.



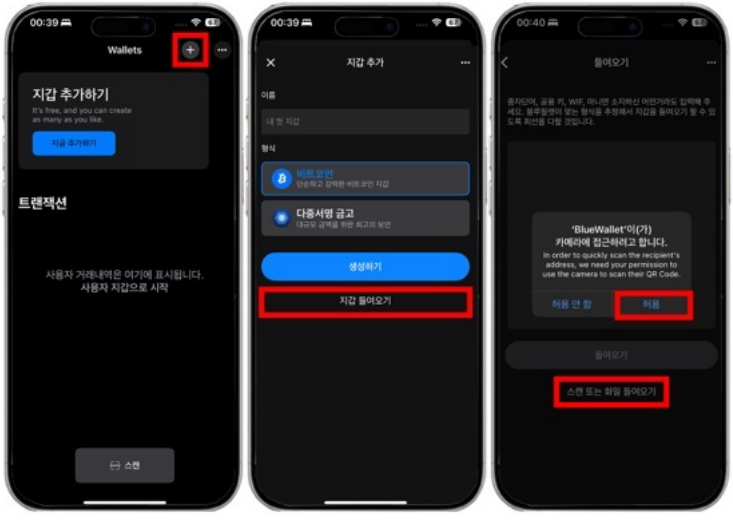
시드사이너에 니모닉을 입력했다면 'Seeds'에 들어갔을 때 MFP를 선택할 수 있다. MFP를 선택하고, [Export Xpub] → [Single Sig]를 선택한다.



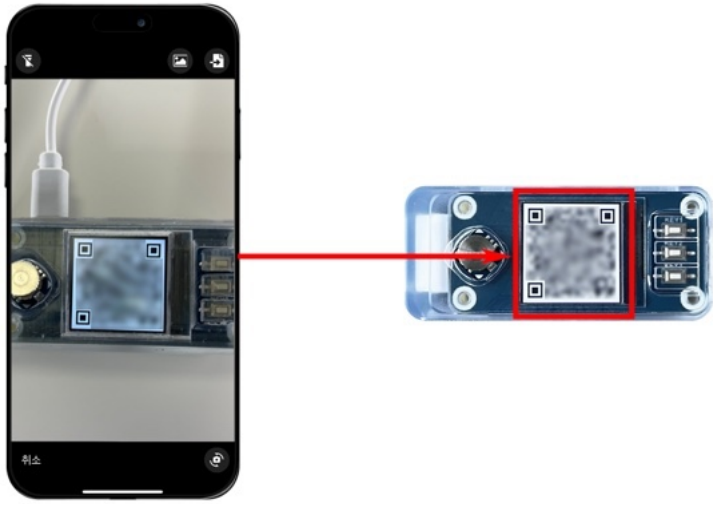
이제 블루월렛에 확장 공개키를 내보낼 것이다. [Native Segwit] → [BlueWallet] → [I Understand]를 선택한다.

[Export Xpub]을 누르면 QR 코드가 나온다. 조이스틱을 위로 밀어 밝기를 더욱 밝게 할 수도 있다.

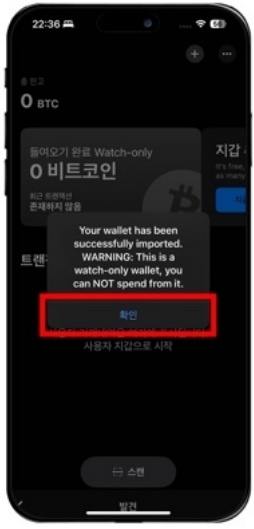
스마트폰의 블루월렛에서 우측 상단 [+] → [지갑 들여오기] → [스캔 또는 화일 들여오기] → 카메라 [허용]을 누른다.



블루월렛에서 카메라 화면이 뜨면 시드사이너에 나오는 QR 코드를 찍는다. 이것이 확장 공개키를 내보내는 과정이다.



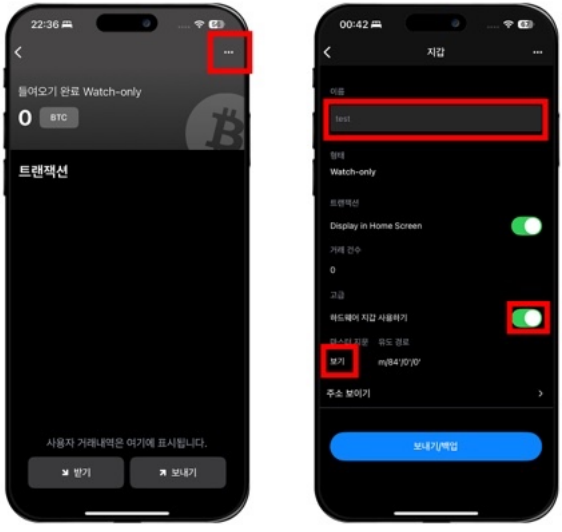
시드사이너를 스캔하면 자동으로 지갑이 만들어질 것이다.



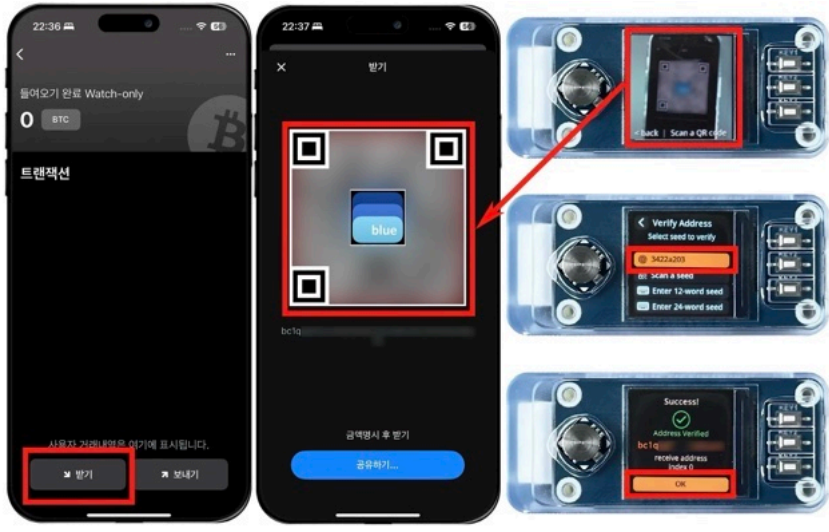
지갑에 들어와서 오른쪽 위 점 세 개를 누른다. 지갑의 이름을 설정한다.

[하드웨어 지갑 사용하기]를 켠다. 앞에서 나온 경고창이 이 옵션 때문에 떴던 것이다. 이 옵션을 켜야 시드사이너에서 서명을 받아올 수 있다.

마스터 지문 아래에 있는 [보기]를 눌러 MFP를 확인한다. 시드사이너에서 확인했던 MFP와 동일한지 확인한다. 대소문자는 상관없다.



시드사이너는 주소 검증하기가 쉽다. 블루월렛에서 [받기]를 눌렀을 때 나오는 QR 코드를 시드사이너로 스캔하기만 하면 된다. 시드사이너 홈 화면에서 'Scan'을 눌러 블루월렛이 보여주는 QR 코드를 스캔한다. MFP를 선택하면 이 주소가 지갑에 속한 주소인지 자동으로 검색해 준다.

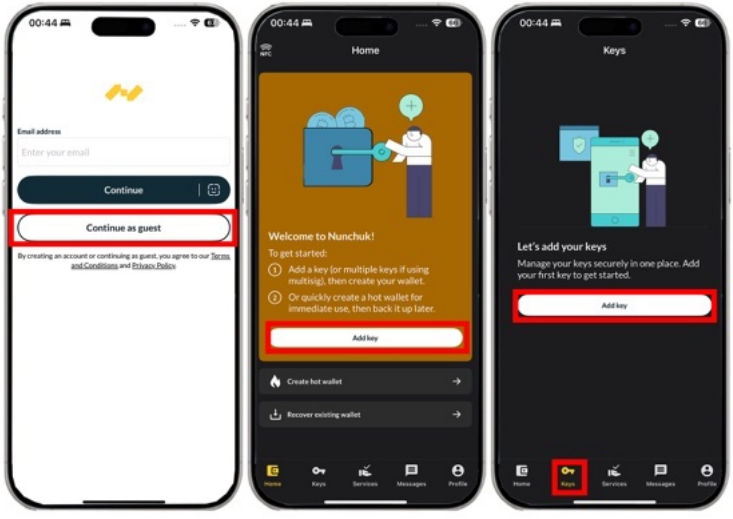


이제 워치-온리 지갑인 블루월렛과 시드사이너 연동이 끝났다. 앞으로 블루월렛에서 '받기'를 누르고 비트코인을 받으면 된다. 하지만, 일단 소액만 보내보고 서명 연습을 한 뒤에 본격적으로 사용하길 바란다.

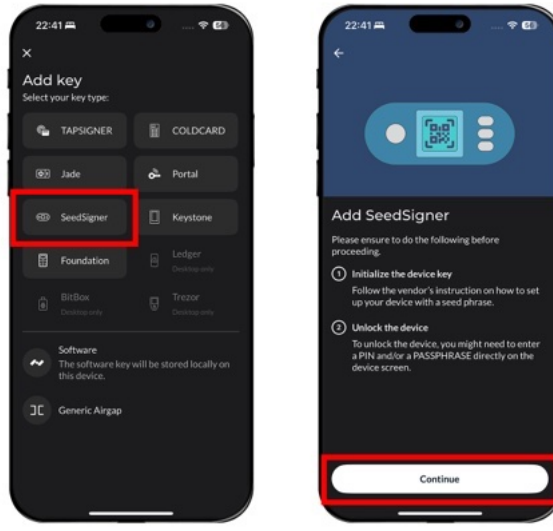
넌척에 확장 공개키 내보내 워치-온리 지갑 만들기

이제 워치-온리 지갑인 넌척과 시드사이너를 연동해 보자. 앞에서 설치했던 넌척을 켠다. 우리는 게스트 모드로 넌척을 사용할 것이다. 어차피 얼마든지 시드사이너와 넌척을 연동할 수 있으므로 로그인이 필요 없기 때문이다. [Continue as guest]를 누른다.

이후에 화면에서 [Add key] 버튼이 보인다면 바로 누르고, 안 보인다면 아래 탭에서 [Keys]를 누른 뒤 [Add key]를 누른다.



기기를 선택하는 창이 나오면 [SeedSigner]를 선택한다. 이후에 [Continue]를 누른다.

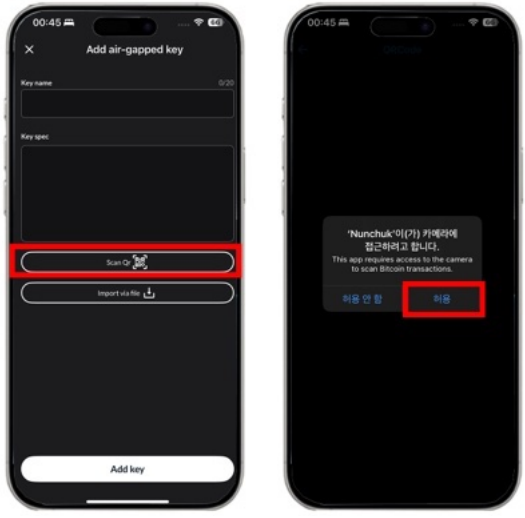


시드사이너에 니모닉을 입력했다면 'Seeds'에 들어갔을 때 MFP를 선택할 수 있다. MFP를 선택하고 [Export Xpub] → [Single Sig]를 선택한다.

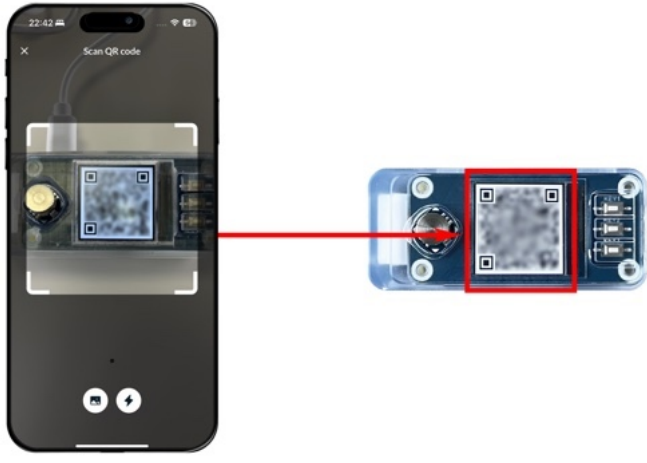
이제 넌척에 확장 공개키를 내보낼 것이다. [Native Segwit] → [Nunchuk] → [I Understand]를 선택한다.

[Export Xpub]을 누르면 QR 코드가 나온다. 조이스틱을 위로 밀어 밝기를 더욱 밝게 할 수도 있다.

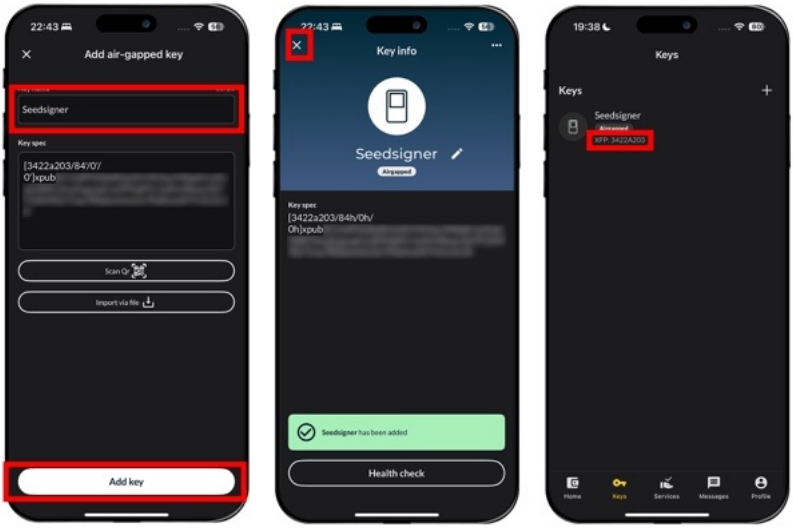
넌척에서 [Scan Qr]을 누른다. 카메라 접근 권한을 요구하면 [허용]을 누른다.



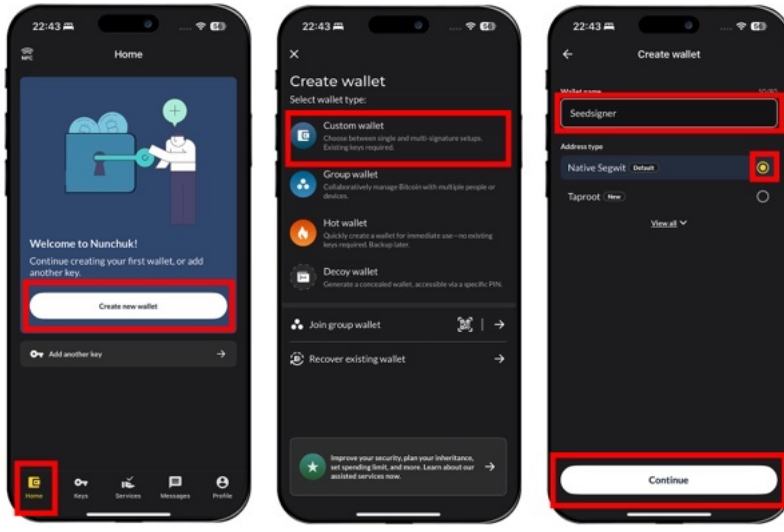
넌척에서 카메라 화면이 뜨면 시드사이너의 QR 코드를 스캔한다.



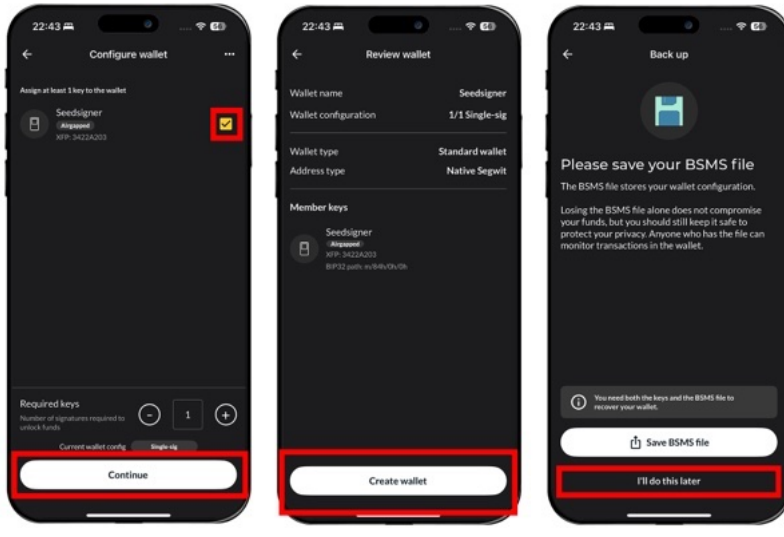
지갑 이름을 설정하고 [Add key]를 누른다. 그러고 [x] 버튼을 눌러 나가면 MFP (XFP)가 적혀있다. 이것이 시드사이너에서 확인했던 MFP와 동일한지 확인하자.



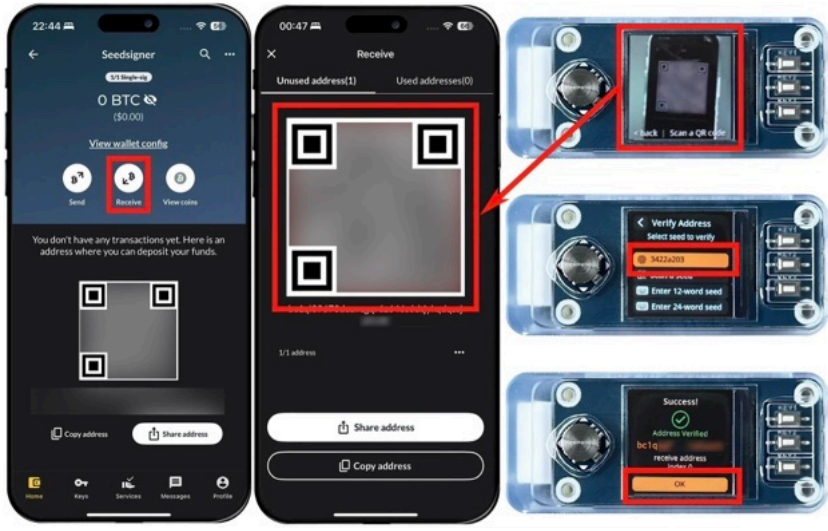
이제 넌척의 아래 탭에서 [Home]을 선택하고 [Create new wallet]을 누른다. [Custom wallet]을 누르고 지갑 이름을 입력한다. 다 되면 [Continue]를 누른다.



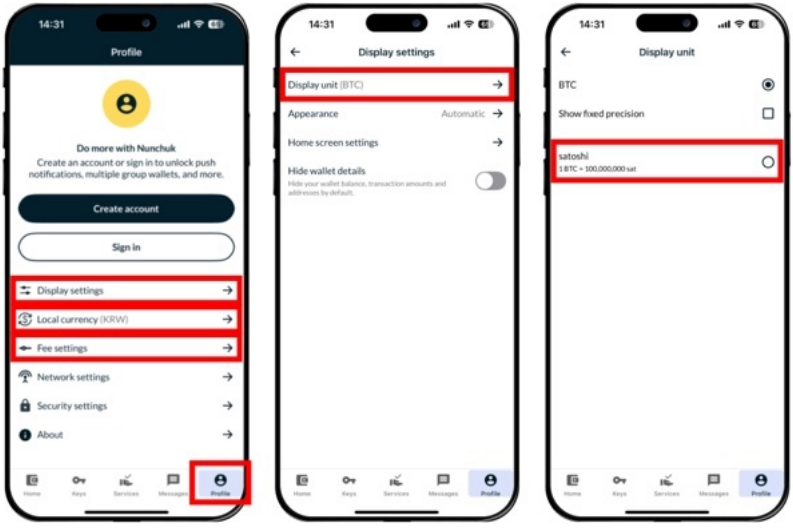
앞에서 추가했던 Key를 선택하고 [Continue]를 누른다. [Create wallet]을 누르고 [I'll do this later]를 누른다. 그러면 이제 넌척에 확장 공개키를 내보내는 것도 완료되었다.



넌척에서 [Receive(받기 주소)]를 누르면 나오는 QR 코드를 시드사이너로 스캔하면 주소 검증이 된다. 시드사이너 홈 화면에서 [Scan]을 눌러 넌척이 보여주는 QR 코드를 스캔한다. MFP를 선택하면 이 주소가 지갑에 속한 주소인지 자동으로 검색해 준다.



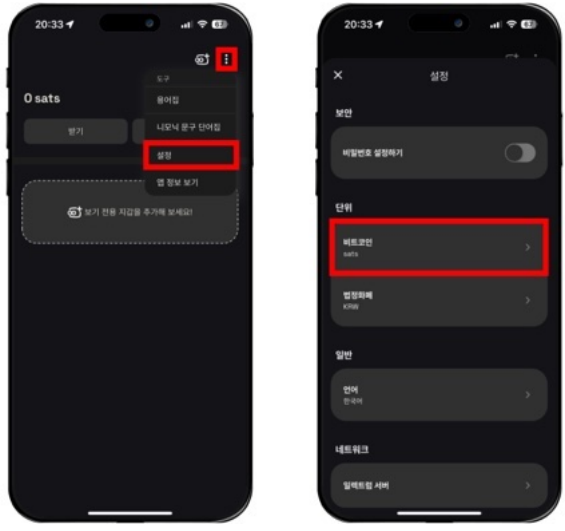
참고로 넌척 하단 탭의 [Profile]을 선택하면 몇 가지 설정을 할 수 있다. [Display settings]에서 일상적인 단위인 sat로 변경할 수 있다. [Display unit]을 누르고 [satoshi]를 선택하면 된다. 이 외에도 [Local currency]에서 [South Korean Won (KRW)]를 선택해 통화 단위를 바꿀 수 있고, [Fee settings] → [Default fee rate] → [Priority]를 선택해 온-체인 수수료를 좀 더 많이 지불하는 대신 거래가 빠르게 컨펌되도록 할 수도 있다.



코코넛 월렛에 확장 공개키 내보내 워치-온리 지갑 만들기

이제 워치-온리 지갑인 코코넛 월렛과 시드사이너를 연동해 보자. 앞에서 설치했던 코코넛 월렛을 켠다.

일상적으로는 BTC 단위보다 sats 단위를 더 많이 쓰므로 단위를 바꿔보자. 코코넛 월렛 홈 화면에서 우측 상단 점 세 개 → [설정]을 누르고, 단위: 비트코인을 'sats'로 바꾼다.



시드사이너에 니모닉을 입력했다면 'Seeds'에 들어갔을 때 MFP를 선택할 수 있다. MFP를 선택하고 [Export Xpub] → [Single Sig]를 선택한다.

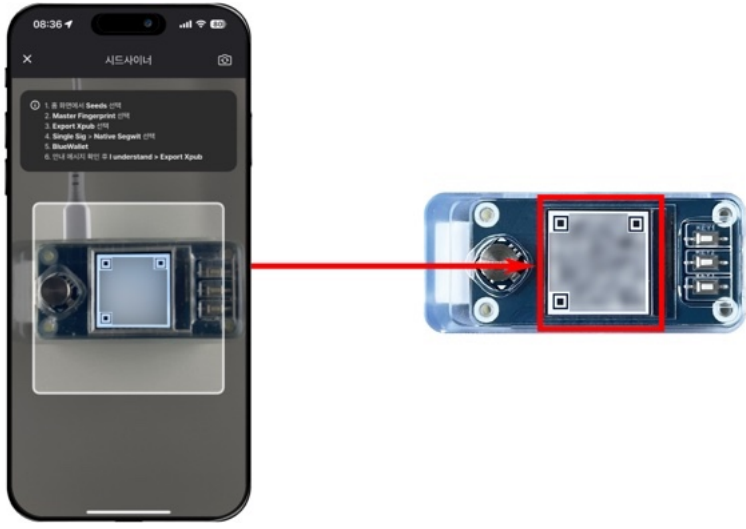
[Native Segwit] → [Nunchuk] → [I Understand]를 선택한다.

[Export Xpub]을 누르면 QR 코드가 나온다. 조이스틱을 위로 밀어 밝기를 더욱 밝게 할 수도 있다.

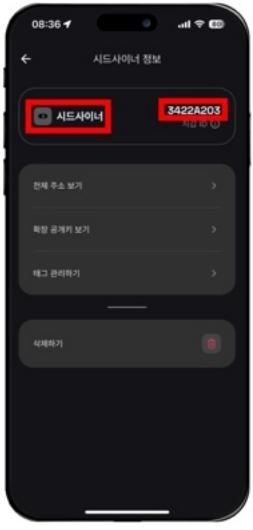
코코넛 월렛에서 오른쪽 위의 지갑 추가 버튼을 누르거나 아래의 [보기 전용 지갑을 추가해 보세요!]를 누른다.

지갑을 고르는 창이 나오면 [시드사이너]를 누른다. 카메라 접근 권한을 요구하면 [허용]을 누른다.

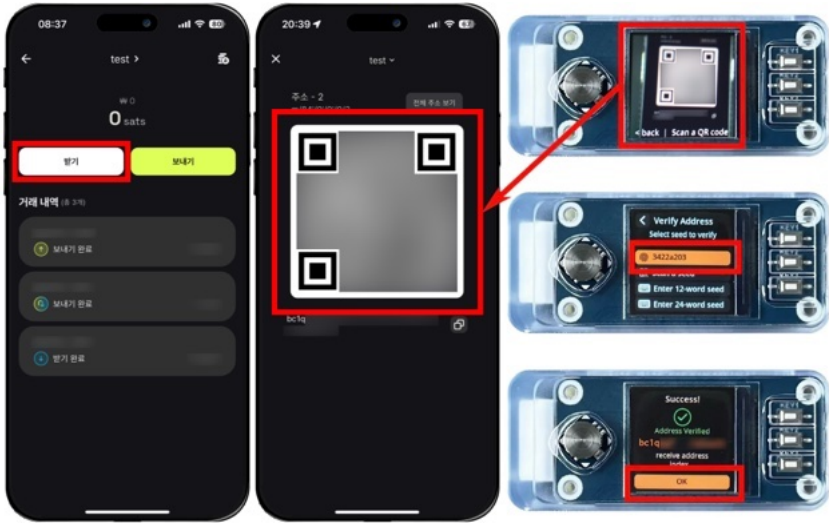
스마트폰의 코코넛 월렛에서 카메라 화면이 나오면 시드사이너에 나오는 QR 코드를 스캔한다.



바로 워치-온리 지갑이 불러와진다. 상단의 [시드사이너 〉]를 누른다. 먼저 오른쪽에 보이는 MFP가 시드사이너에서 확인했던 MFP와 일치하는지 확인한다. [시드사이너]를 누르면 지갑 이름을 설정할 수도 있다.



시드사이너는 주소 검증하기가 쉽다. 코코넛 월렛에서 [받기]를 눌렀을 때 나오는 QR 코드를 시드사이너로 스캔하기만 하면 된다. 시드사이너 홈 화면에서 'Scan'을 눌러 코코넛 월렛이 보여주는 QR 코드를 스캔한다. MFP를 선택하면 이 주소가 지갑에 속한 주소인지 자동으로 검색해 준다.



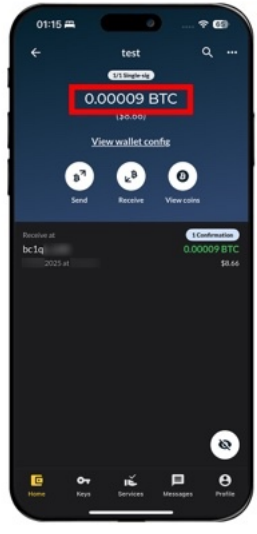
이제 워치-온리 지갑인 코코넛 월렛과 시드사이너 연동이 끝났다. 앞으로 코코넛 월렛에서 '받기'를 누르고 비트코인을 받으면 된다. 하지만, 일단 소액만 보내보고 서명 연습을 한 뒤에 본격적으로 사용하길 바란다.

블루월렛으로 서명 연습

본격적으로 비트코인을 지갑에 보관하기 전 꼭 해야 하는 것이 있다. 서명이 잘 되는지 확인하는 것이다. 비트코인을 다른 곳으로 보내려면 서명을 해야 한다. 만약 서명이 안 되면 다른 곳으로 보낼 수가 없으니 해당 주소에 모은 비트코인은 그림의 떡이 된다. 시드사이너는 니모닉 시드가 기기에 저장되지 않으므로 복구 연습을 할 필요는 없다. 기기를 켤 때마다 복구를 해야 하기 때문이다.

서명 연습 없이 덜컥 비트코인 모으기부터 시작하는 경우가 있는데, 이러면 나중에 거액이 들어간 상태에서 서명을 처음 해보다가 안 되는 경우 난감해질 수 있다.

서명 연습을 해보자. 서명을 연습하기 위해 9천 sats 정도를 지갑에 일단 보내보았다. 비트코인을 지갑에 보내는 방법은 뒤에 나오는 '거래소에서 지갑으로 비트코인 옮기기' 장을 참고하라. 블루월렛과 넌척 둘 다 금액이 잘 확인된다.

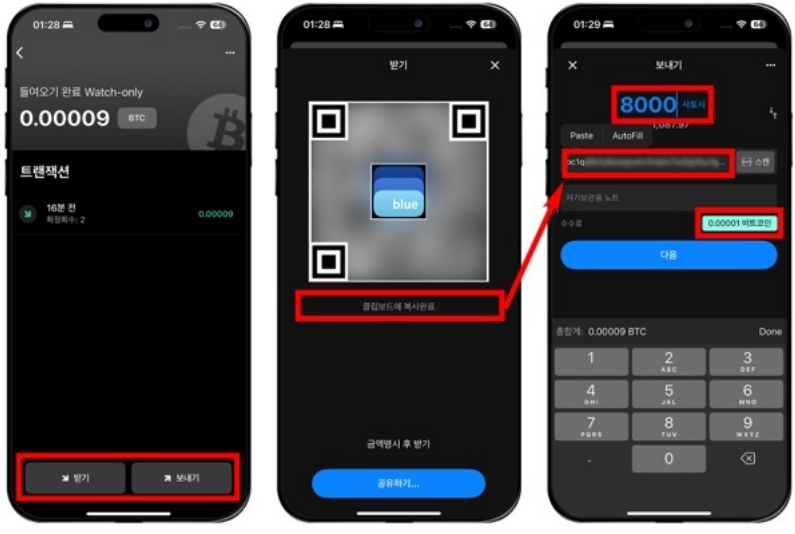


블루월렛에서 서명 연습을 해보자. 먼저 [받기] 버튼을 누르고 뜨는 주소를 복사한다. 프라이버시와 보안을 위해 주소는 재사용하지 않는 것이 좋은데, 블루월렛과 넌척, 코코넛 월렛은 안 쓴 주소를 자동으로 보여준다. 주소를 한 번 누르면 자동으로 주소가 복사된다.

이제 [x] 버튼을 누른 뒤 [보내기] 버튼을 누른다. 주소창에 아까 복사했던 주소를 붙여넣는다. 서명 연습을 하기 위해 내 비트코인을 다시 나에게 보내는 거래(트랜잭션)를 일으키는 것이다.

그 위에 있는 금액에는 수수료를 제외하고 보낼 금액을 입력한다. 비트코인 온-체인에는 수수료가 있기 때문에 2,000–3,000 sats 이상 제외하고 송금 연습을 해야 한다.

참고로 수수료 옆에 있는 민트색 박스를 누르면 수수료율을 자신이 직접 설정할 수도 있다. 멤풀을 보고 적정 수수료율을 설정하는 연습도 해보면 좋다.



이제 시드사이너를 켜고 지갑을 불러온다. 시드 QR로 지갑을 불러오거나, 니모닉을 입력해 불러오면 된다.

[Scan a SeedQR]은 시드 QR을 스캔해서 니모닉을 불러오는 것이다. 시드 QR을 스캔하는 경우 그냥 홈 화면에서 [Scan]을 누르고 바로 시드 QR을 스캔해도 된다.

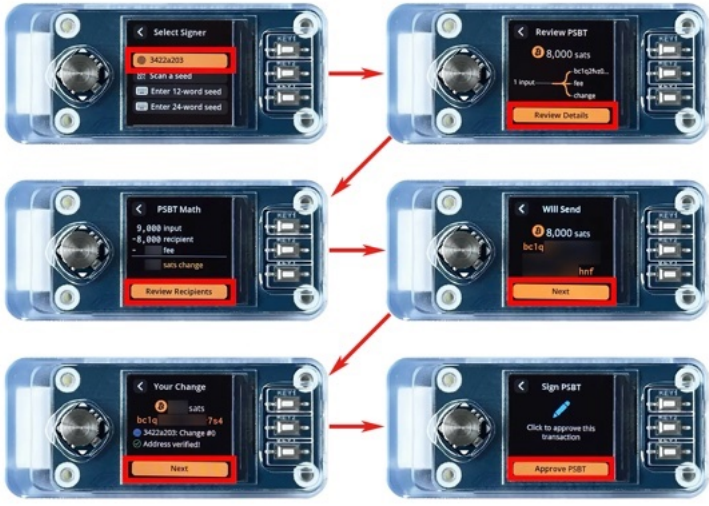
Enter 12-word seed는 12단어 니모닉을 입력하는 경우 사용한다.

Enter 24-word seed는 24단어 니모닉을 입력하는 경우 사용한다.

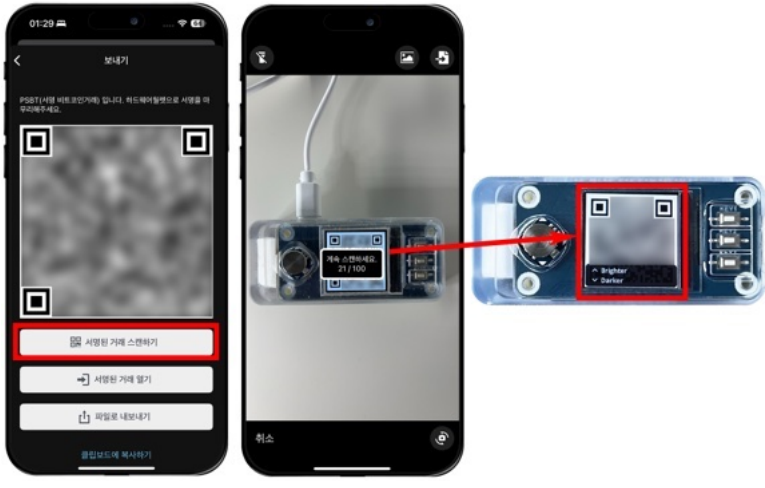
시드 QR을 스캔하거나 니모닉을 입력한다. 니모닉을 입력할 때는 조이스틱을 상하좌우로 움직이고, 조이스틱을 수직으로 누르면 단어가 선택된다. 오른쪽에 단어들이 뜨면 오른쪽 위아래 버튼을 이용해 이동할 수 있고, 오른쪽 가운데 버튼을 누르면 그 단어가 선택된다.

시드사이너에 니모닉을 입력해서 지갑을 불러왔으면 홈 화면에서 [Scan]을 선택한다. 카메라가 나오면 블루월렛 화면에 나오는 움직이는 QR 코드를 스캔한다.

시드사이너에서 MFP를 선택한다. 그러면 이제 거래에 관한 여러 가지 정보가 나온다. 정보들을 확인하고 맞으면 계속 다음으로 넘어간다.



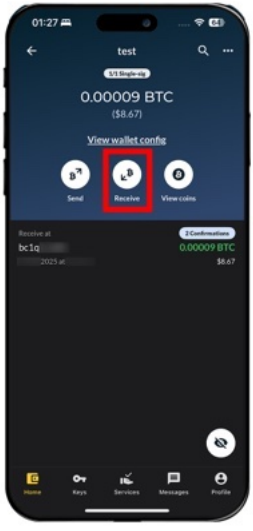
시드사이너에서 QR 코드가 나올 것이다. 블루월렛에서 [서명된 거래 스캔하기]를 누르고 시드사이너 화면을 스캔한다.



서명이 올바르다면 직렬화된 서명 데이터(나열된 숫자들)가 나타날 것이고, 여기서 [바로 보내기]를 누르면 네트워크에 전송된다.

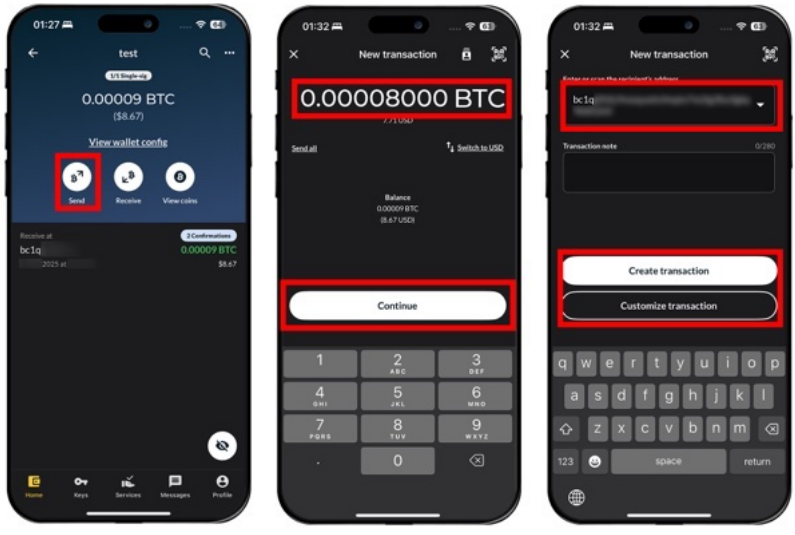
넌척으로 서명 연습

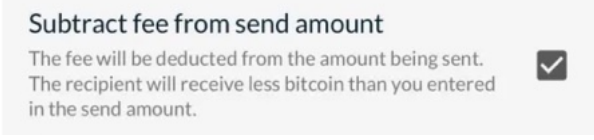
넌척에서 서명할 때도 블루월렛과 비슷하게 진행한다. 먼저 [Receive(받기)]를 누르고 [Copy address]를 눌러 주소를 복사한다.



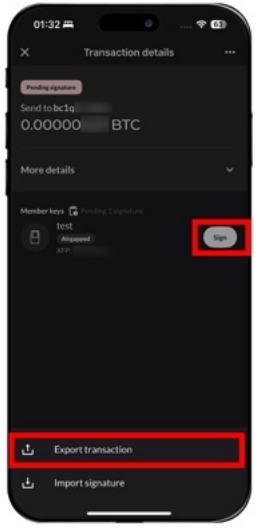
이제 [Send]를 누르고 보낼 금액을 입력한다. 이때 수수료는 제외하고 보내야 한다. [Continue]를 누른다. 아까 복사했던 주소를 붙여넣기하고 [Create transaction]을 누른다. 참고로 [Customize transaction]을 누르면 수수료율을 직접 설정하거나, 어떤 UTXO를 선택해서 보낼지 설정할 수 있다.

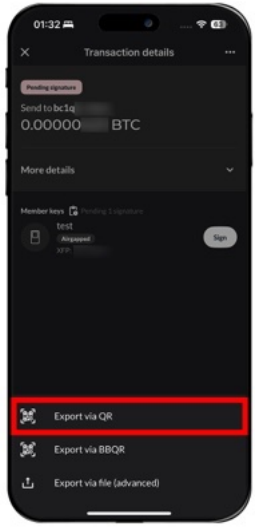
[Customize transaction]에서 [Subtract fee from send amout] 옵션을 체크하면 넌척이 보낼 금액에서 알아서 수수료만 차감하고 보낸다. 이렇게 하면 예상 수수료를 계산할 필요 없이 전액을 보내면 되기 때문에 편리하다.





[Sign]을 누르고, [Export transaction]을 누른다. 그다음에 맨 위에 있는 [Export via QR]을 누르면 QR 코드가 나올 것이다.





이제 시드사이너를 켜고 지갑을 불러온다. 시드 QR로 지갑을 불러오거나, 니모닉을 입력해 불러오면 된다.

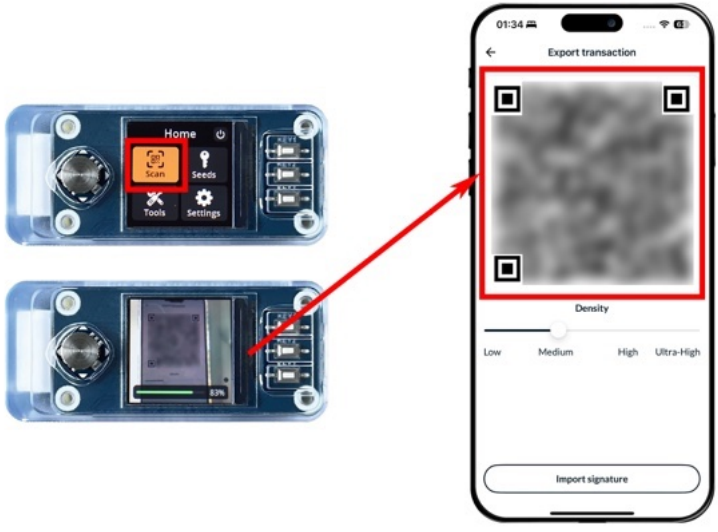
[Scan a SeedQR]은 시드 QR을 스캔해서 니모닉을 불러오는 것이다. 시드 QR을 스캔하는 경우 그냥 홈 화면에서 [Scan]을 누르고 바로 시드 QR을 스캔해도 된다.

Enter 12-word seed는 12단어 니모닉을 입력하는 경우 사용한다.

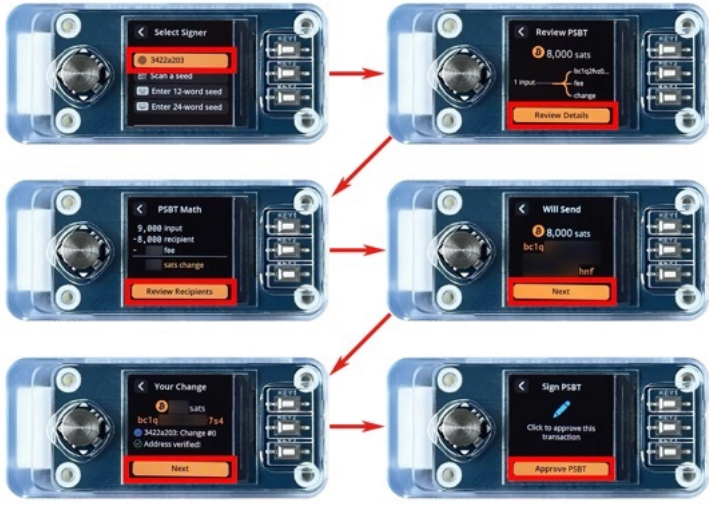
Enter 24-word seed는 24단어 니모닉을 입력하는 경우 사용한다.

시드 QR을 스캔하거나 니모닉을 입력한다. 니모닉을 입력할 때는 조이스틱을 상하좌우로 움직이고, 조이스틱을 수직으로 누르면 단어가 선택된다. 오른쪽에 단어들이 뜨면 오른쪽 위아래 버튼을 이용해 이동할 수 있고, 오른쪽 가운데 버튼을 누르면 그 단어가 선택된다.

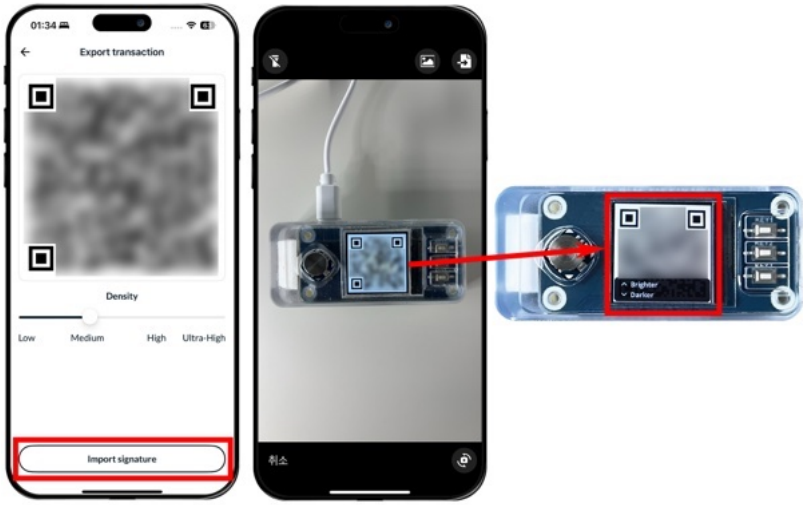
시드사이너에 니모닉을 입력해서 지갑을 불러왔으면 홈 화면에서 [Scan]을 선택한다. 카메라가 나오면 넌척 화면에 나오는 움직이는 QR 코드를 스캔한다.



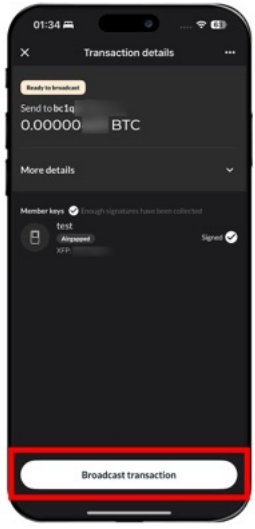
시드사이너에서 MFP를 선택한다. 그러면 이제 거래에 관한 여러 가지 정보가 나온다. 정보들을 확인하고 맞으면 계속 다음으로 넘어간다.

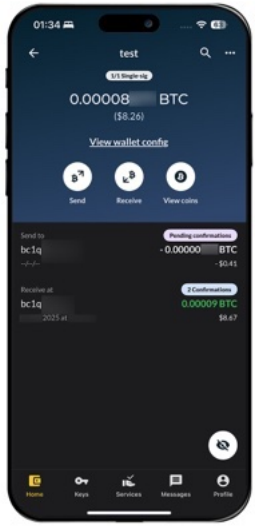


시드사이너에서 QR 코드가 나올 것이다. 넌척에서 [Import signature]를 누르고 시드사이너 화면을 스캔한다.



[Broadcast transaction]을 누르면 네트워크에 전파된다.

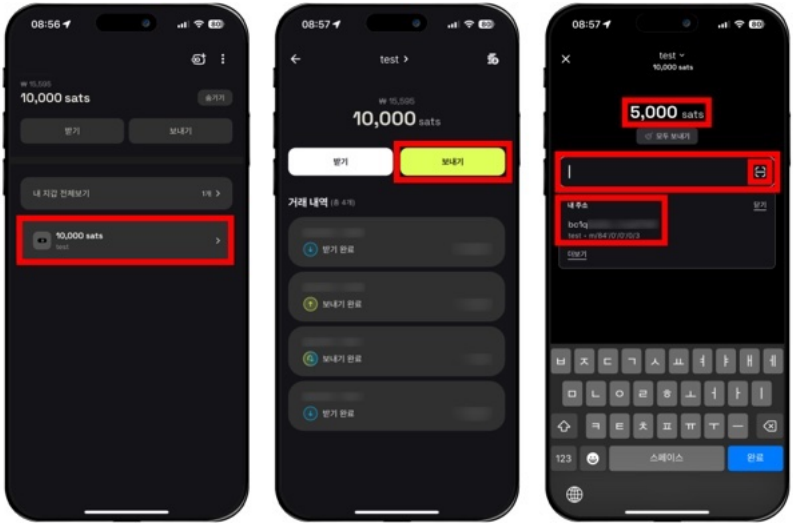




코코넛 월렛으로 서명 연습

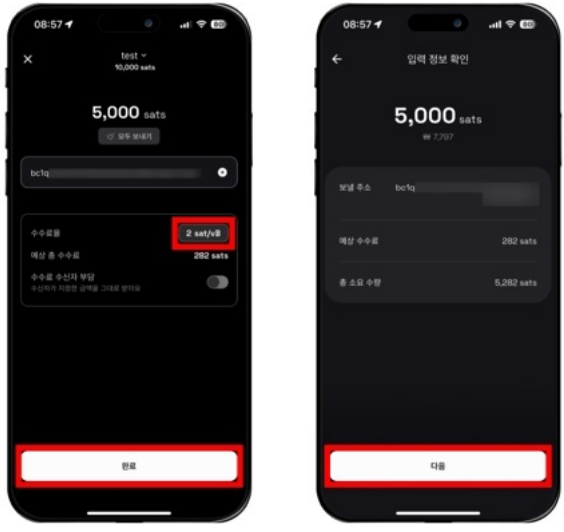
코코넛 월렛에서 서명하는 과정도 비슷하다. 코코넛 월렛 홈 화면에서 지갑을 선택하고 [보내기]를 누른다.

금액을 입력하고 아래 보낼 주소 입력창을 누른다. 코코넛은 다른 워치-온리 지갑들보다 서명 연습하는 것이 훨씬 편하다. 보낼 주소 입력창을 누르면 아래에 자신의 지갑 주소 목록이 나오기 때문이다. '내 주소' 아래에 있는 주소를 누른다.



코코넛 월렛에서는 바로 수수료율을 조정할 수 있다. 현재 적절한 수수료가 자동으로 입력되어 있지만 더 안정적으로 바로 다음 블록에 거래가 컨펌되게 하고 싶다면 수수료율을 높여도 좋다. 수수료율까지 설정했으면 [완료]를 누른다.

보낼 주소와 예상 수수료 등을 확인한 뒤 정보가 맞으면 [다음]을 누른다.



이제 시드사이너를 켜고 지갑을 불러온다. 시드 QR로 지갑을 불러오거나, 니모닉을 입력해 불러오면 된다.

[Scan a SeedQR]은 시드 QR을 스캔해서 니모닉을 불러오는 것이다. 시드 QR을 스캔하는 경우 그냥 홈 화면에서 [Scan]을 누르고 바로 시드 QR을 스캔해도 된다.

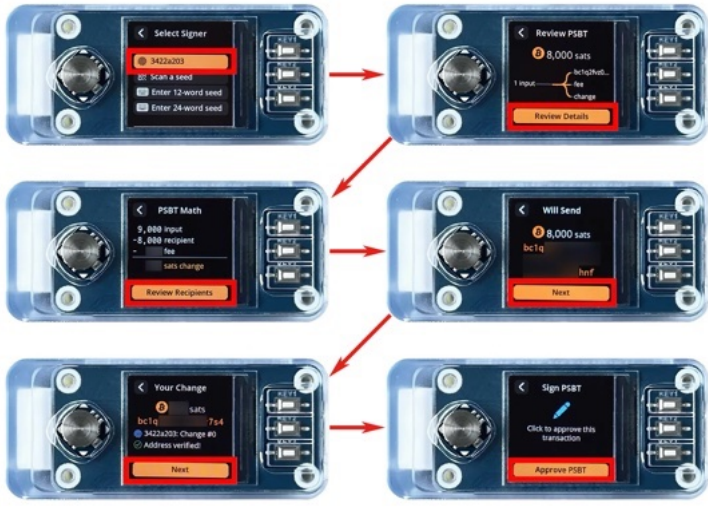
Enter 12-word seed는 12단어 니모닉을 입력하는 경우 사용한다.

Enter 24-word seed는 24단어 니모닉을 입력하는 경우 사용한다.

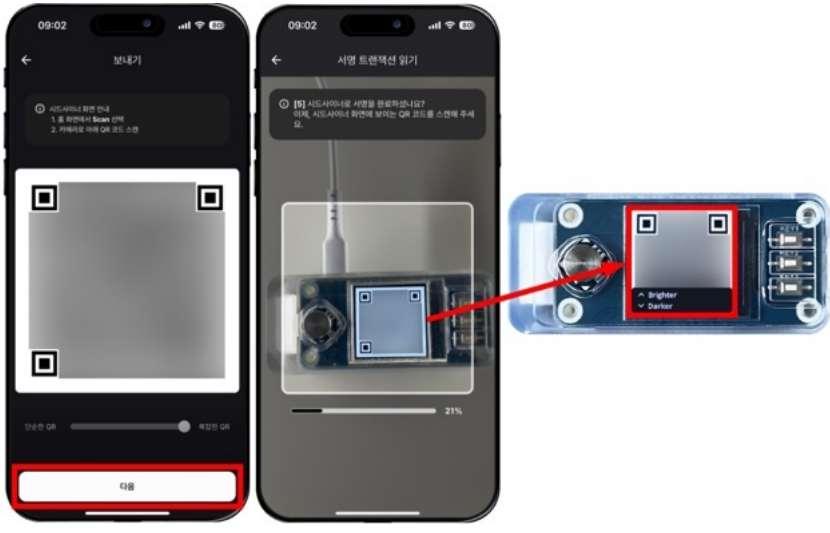
시드 QR을 스캔하거나 니모닉을 입력한다. 니모닉을 입력할 때는 조이스틱을 상하좌우로 움직이고, 조이스틱을 수직으로 누르면 단어가 선택된다. 오른쪽에 단어들이 뜨면 오른쪽 위아래 버튼을 이용해 이동할 수 있고, 오른쪽 가운데 버튼을 누르면 그 단어가 선택된다.

시드사이너에 니모닉을 입력해서 지갑을 불러왔으면 홈 화면에서 [Scan]을 선택한다. 카메라가 나오면 코코넛 월렛 화면에 나오는 움직이는 QR 코드를 스캔한다.

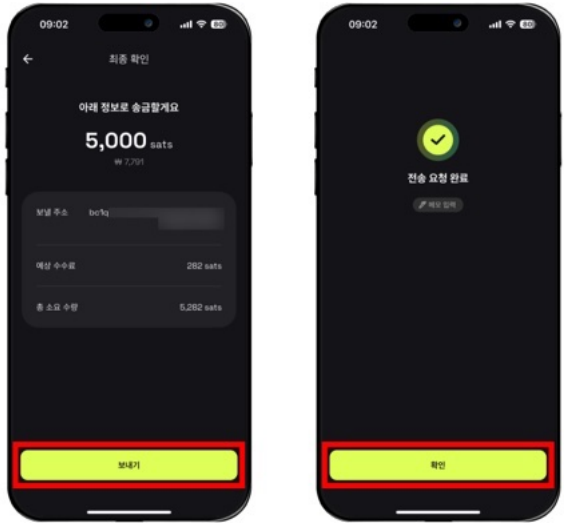
시드사이너에서 MFP를 선택한다. 그러면 이제 거래에 관한 여러 가지 정보가 나온다. 정보들을 확인하고 맞으면 계속 다음으로 넘어간다.



시드사이너에서 QR 코드가 나올 것이다. 코코넛 월렛에서 [다음]을 누르고 시드사이너 화면을 스캔한다.



거래 정보를 한 번 더 확인하고 [보내기]를 누르면 네트워크에 전파된다.



이로써 서명까지 잘 되는 것을 모두 확인해 보았다.

시드사이너를 게임기로 만들기

에어-갭 지갑은 그저 서명 기기일 뿐이다. 2024년 대한민국에서는 개인들의 거래 내역을 감시하기 위해 개인 지갑 신고 의무화 법안이 발의된 적이 있다. 이것이 얼마나 터무니없고 어려운 일인지 알게 하기 위해 이 절을 서술하게 되었다.

시드사이너가 설치된 마이크로SD카드를 꽂는 라즈베리파이 제로 보드는 온라인에 연결되지 않는 미니컴퓨터일 뿐이다. 따라서 다른 마이크로SD카드를 꽂는다면 시드사이너가 아닌 다른 기기가 되어버린다. 그렇다면 시드사이너는 마이크로SD카드를 말하는 것일까? 개인 지갑

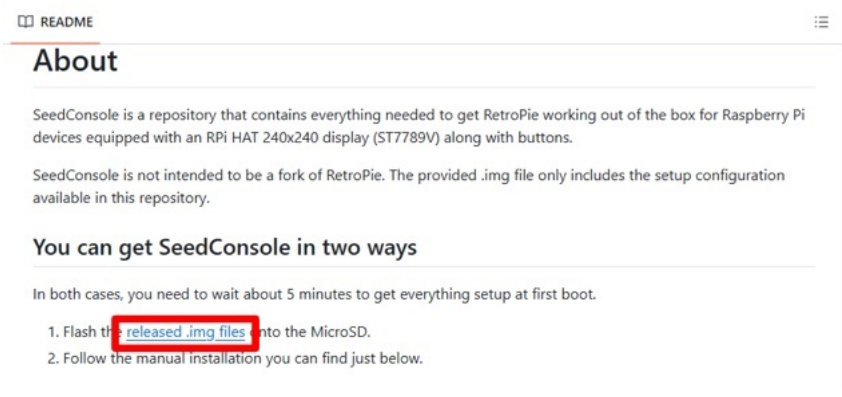
보유 여부를 신고하라고 하면 시드사이너가 담겨 있는 마이크로SD카드를 갖고 있다고 신고하면 되는 것일까? 시드사이너는 개인 지갑이 무엇인지 그 경계를 모호하게 한다.

이제 8GB 용량의 '다른' 마이크로SD카드에 미니게임 OS를 설치해 보자. '레트로파이'는 라즈베리파이 기기에서 고전 게임들을 구동할 수 있게 하는 프로젝트다. 어떤 사용자가 레트로파이에 게임 보이 게임 127개를 할 수 있도록 만든 '시드콘솔'이라는 프로그램이 있다. 이것을 설치해 보겠다.

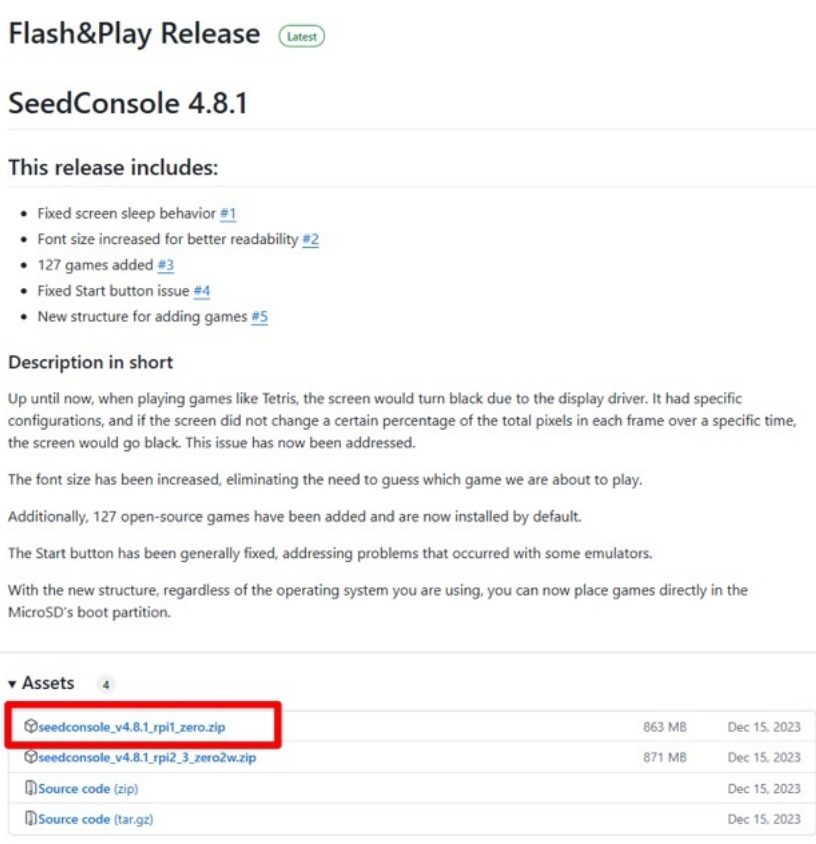
먼저 아래 링크에 들어간다.

https://github.com/DesobedienteTecnologico/seedconsole?tab=readme-ov-file#about

여기서 스크롤을 내려 'About'에 있는 [released .img files] 링크를 누른다.



들어가면 있는 릴리즈 버전 중 'Assets' 아래에 있는 seedconsole_v?.?.?_rpi1_zero.zip 파일을 다운로드한다.



Flash&Play Release Latest

SeedConsole 4.8.1

This release includes:

- Fixed screen sleep behavior #1
- Font size increased for better readability #2
- 127 games added #3
- Fixed Start button issue #4
- New structure for adding games #5

Description in short

Up until now, when playing games like Tetris, the screen would turn black due to the display driver. It had specific configurations, and if the screen did not change a certain percentage of the total pixels in each frame over a specific time, the screen would go black. This issue has now been addressed.

The font size has been increased, eliminating the need to guess which game we are about to play.

Additionally, 127 open-source games have been added and are now installed by default.

The Start button has been generally fixed, addressing problems that occurred with some emulators.

With the new structure, regardless of the operating system you are using, you can now place games directly in the MicroSD's boot partition.

▾ Assets 4

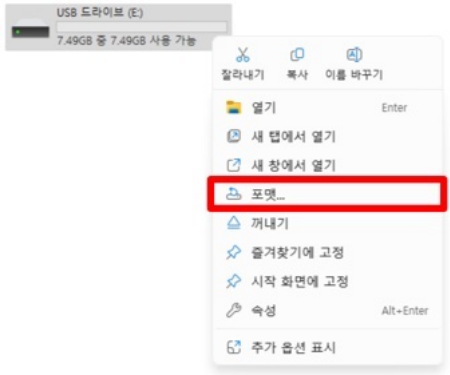
seedconsole_v4.8.1_rpi1_zero.zip	863 MB	Dec 15, 2023
seedconsole_v4.8.1_rpi2_3_zero2w.zip	871 MB	Dec 15, 2023
Source code (zip)		Dec 15, 2023
Source code (tar.gz)		Dec 15, 2023

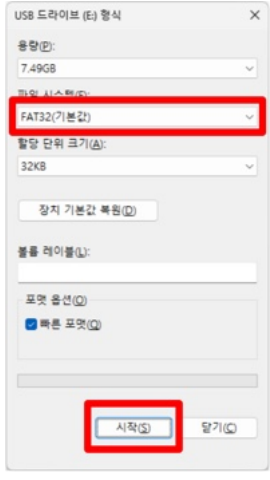
이제 다운로드한 파일의 압축을 푼다. 압축 풀기에 실패하면 이미지 파일을 지정해서 압축을 푼다.

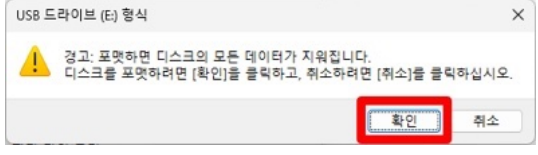
압축이 잘 풀렸다.

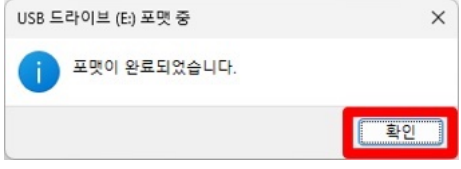
이제 컴퓨터에 여분의 마이크로SD카드를 꽂는다. 당연히 시드사이너가 설치된 마이크로SD카드가 아닌 다른 마이크로SD카드를 꽂아야 한다.

먼저 마이크로SD카드를 포맷한다.

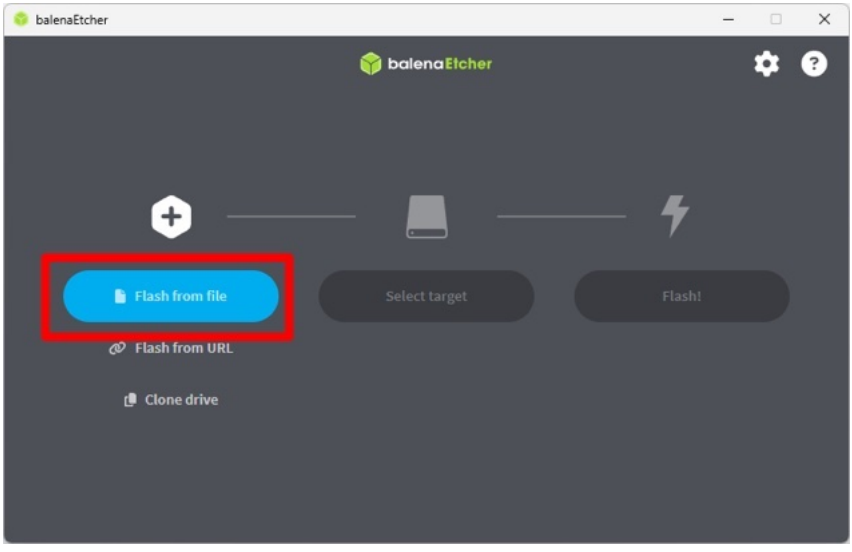


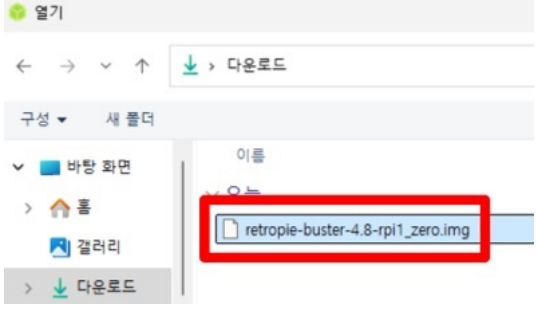




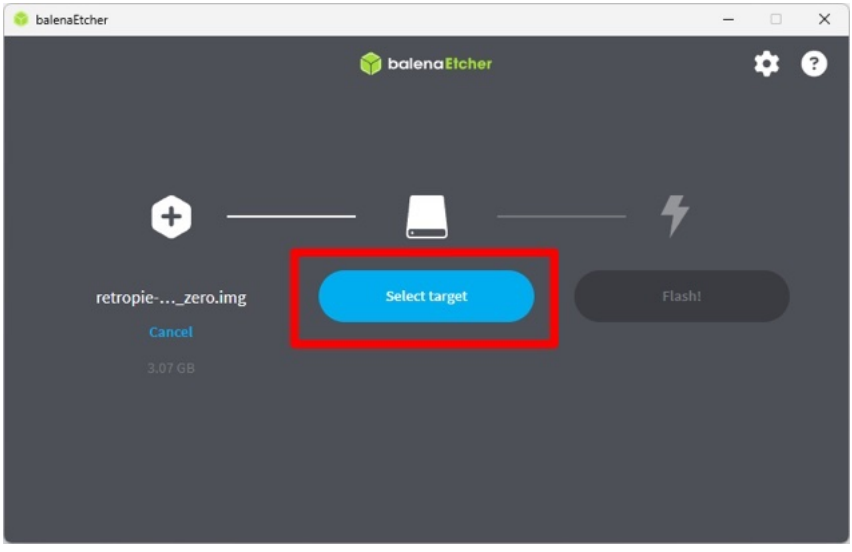


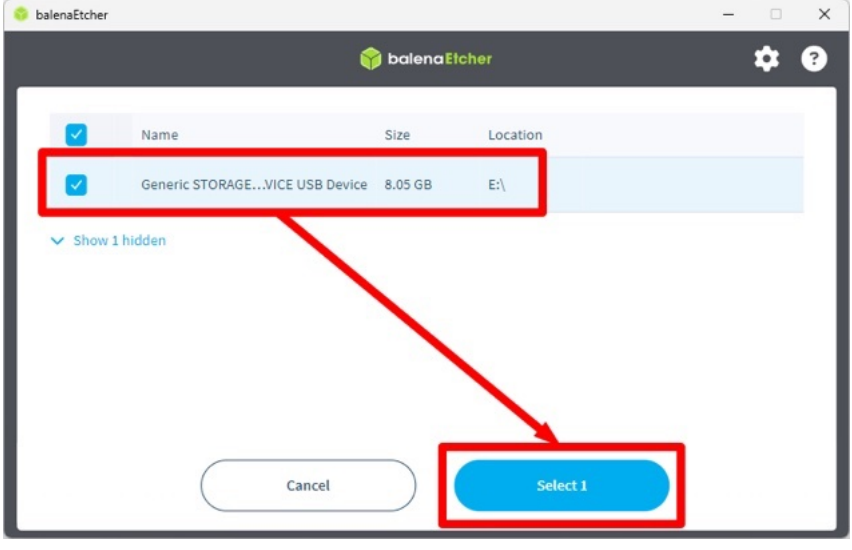
이제 발레나에처를 실행하고, [Flash from file]을 누르고 다운로드 한 파일을 선택한다.



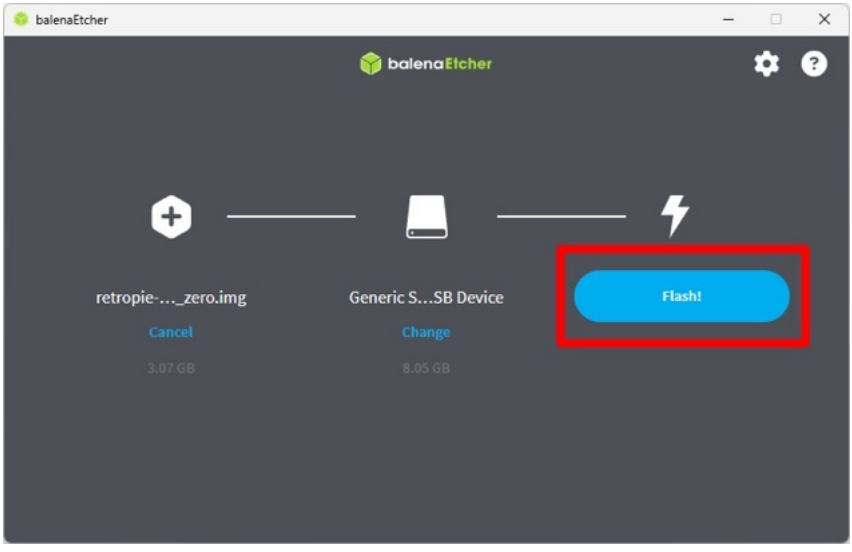


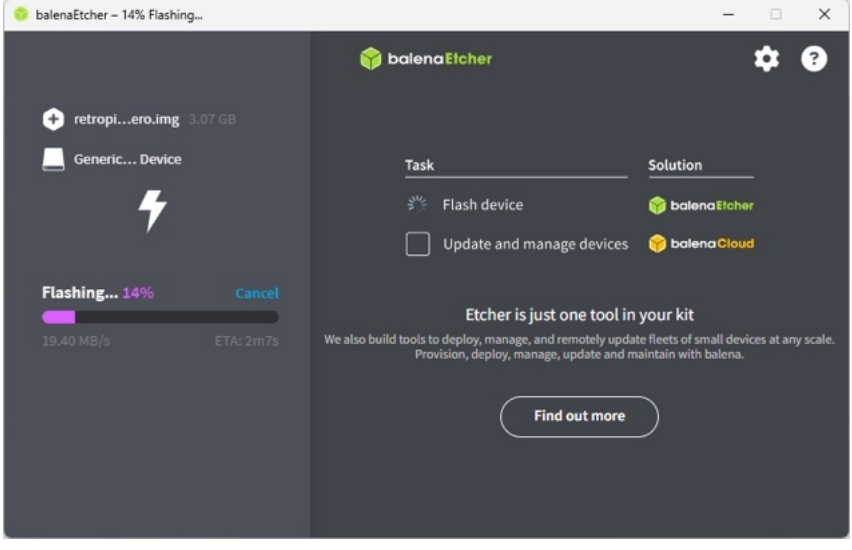
이제 [Select target]을 누르고 마이크로SD카드를 선택 → [Select]를 누른다.



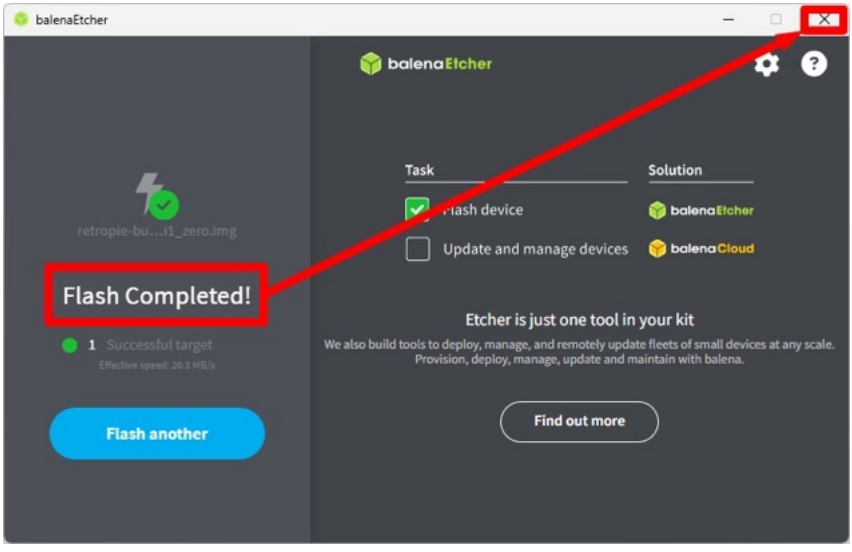


[Flash!]를 누르고 잠시 기다린다. 혹시 포맷하라는 창이 뜨면 무시하고 [X]를 누르면 된다. 앞에서 이미 포맷했기 때문이다.

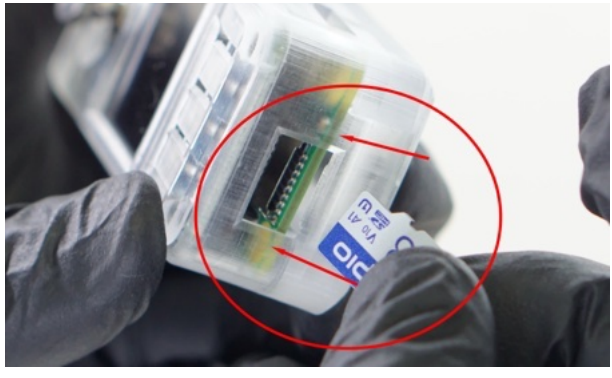




플래싱이 되었다면 [X]를 누르고 컴퓨터에서 마이크로SD카드를 뽑는다.



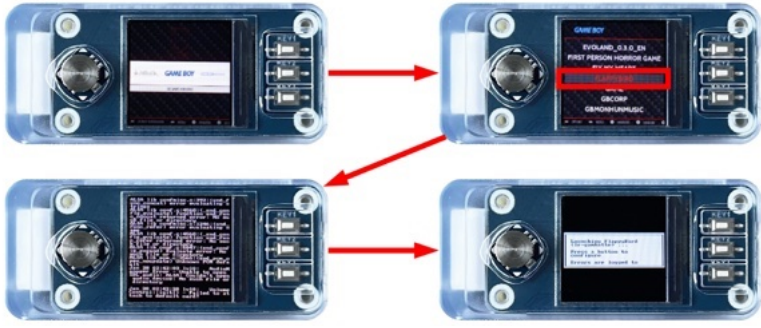
이제 마이크로SD카드를 시드사이너 기기에 꽂는다.



처음에 꽂으면 5분 정도 검은 화면에서 기다려야 한다. 저장 장치가 램을 제외하고 마이크로SD카드뿐이므로 게임에 필요한 파일들을 부팅 파티션에 복사해야 하기 때문에 시간이 걸린다.

왼쪽의 조이스틱을 수직으로 누르면 '선택', 오른쪽 맨 위 버튼은 'A', 중간 버튼은 'B', 맨 아래 버튼은 '시작' 버튼이다. 맨 아래 버튼과 조이스틱을 수직으로 동시에 누르면 '뒤로 가기' 입력이다. 'retropi'에서는 설정을 할 수 있고, 'GameBoy'와 'GameBoy Advanced'에 들어가면 게임을 할 수 있다.

예시로 'GameBoy'에서 'Flappy Bird'라는 게임을 플레이해보겠다. 이 게임은 2014년에 앱스토어 다운로드 수 1위를 할 정도로 매우 흥행했던 단순한 게임이다. [GameBoy] → [FLAPPYBIRD]를 누른다.



이제 시드사이너 기기는 시드사이너 지갑이 아니라 게임기가 되었다.

| 공기계 지갑

스마트폰 공기계를 콜드월렛으로 사용해 지갑 생성하기

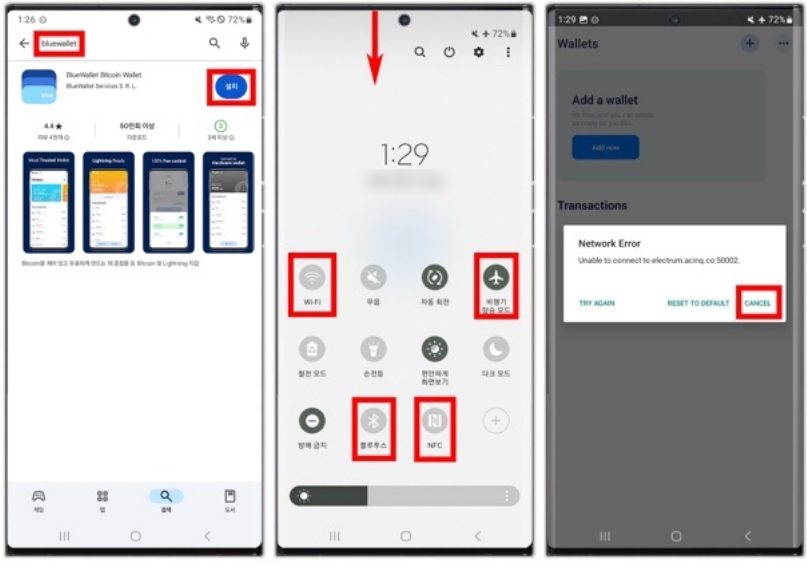
안 쓰는 스마트폰 공기계가 있다면 이 기기를 콜드월렛으로 사용할 수도 있다. 그러나 이런 옵션을 추천하진 않는다. 왜냐하면 와이파이나 블루투스 같은 통신 기능 자체가 아예 없는 것과 통신 기능이 있는데 꺼두는 것은 보안에 있어 완전히 다른 수준이기 때문이다. 오프라인 상태에서 OS나 앱의 보안 업데이트를 어떻게 할 것인지에 대한 문제도 남는다. 그러나 나이가 어린 학생이나 사정이 어려운 경우 지갑을 구매하는 것이 부담될 수 있고, 이런 상황에서 남는 스마트폰 공기계가 있다면 좋은 대안이 될 수 있다. 이렇게 했을 경우 비트코인을 조금 모은 후에는 콜드월렛을 구매하고 새 니모닉을 생성해 비트코인을 옮기는 것을 추천한다.

그러면 지금부터 공기계를 콜드월렛으로 사용하는 방법을 알아보자. 콜드월렛으로 쓸 스마트폰 공기계 한 대와 워치-온리 지갑 앱을 설치할 스마트폰이 필요하다.

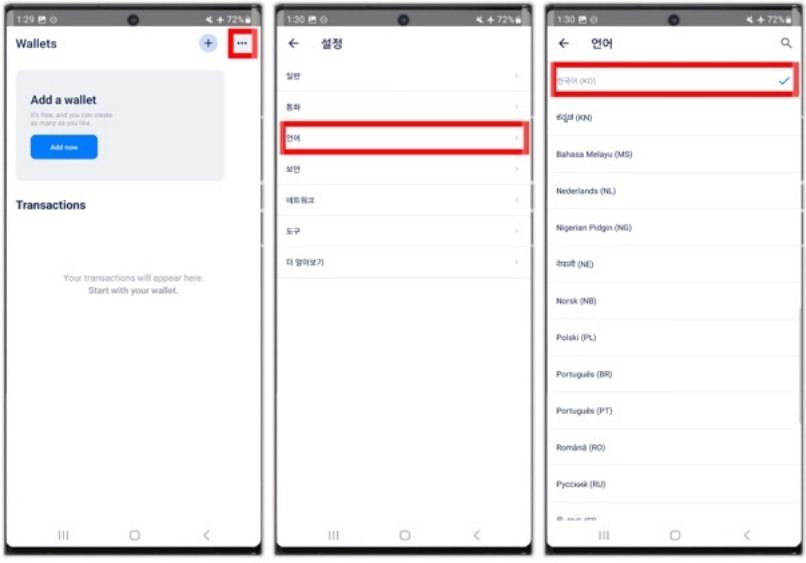
먼저 공기계에서 와이파이를 연결한 뒤 앱스토어나 구글 플레이스토어에서 'bluewallet'을 검색하고 다운로드한다.

그다음에 [Wi-Fi], [블루투스], [NFC] 등의 모든 통신 기능을 끄고 비행기 모드를 켠다.

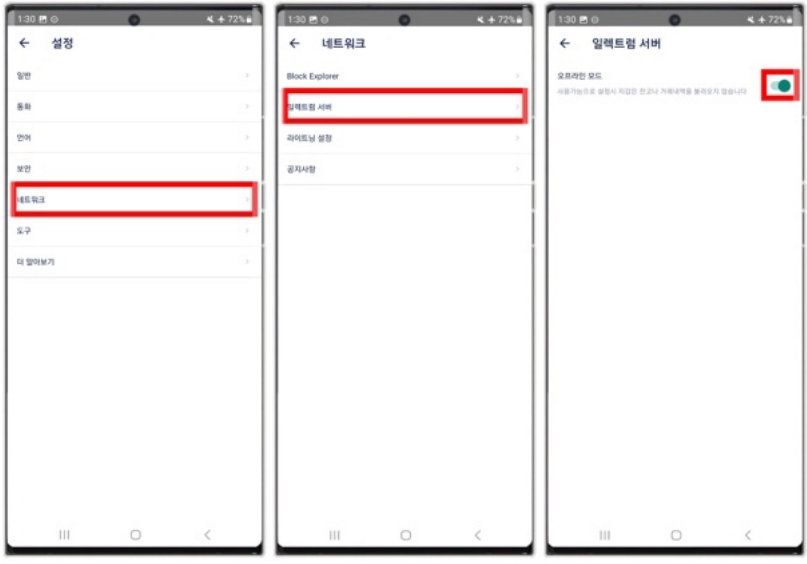
그러고 블루월렛을 켜면 네트워크 오류라는 메시지가 뜰 것이다. 비행기 모드를 켰으니 당연하다. [CANCEL]을 누른다.



먼저 언어 설정을 바꾸자. 블루월렛 홈 화면에서 오른쪽 위 점 세 개 → [언어] → [한국어]를 누른다.

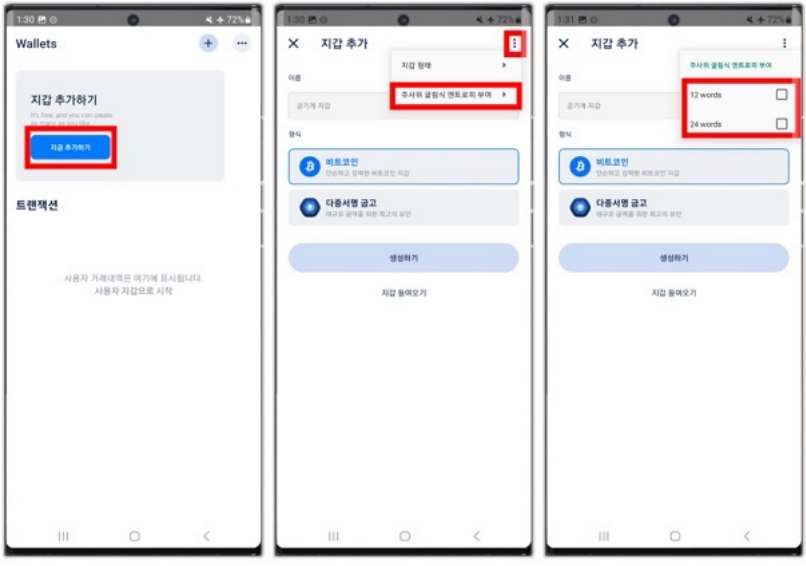


그다음으로는 네트워크에서 오프라인 모드로 설정할 것이다. 설정에서 [네트워크] → [일렉트럼 서버] → [오프라인 모드] 토글 스위치를 켠다.



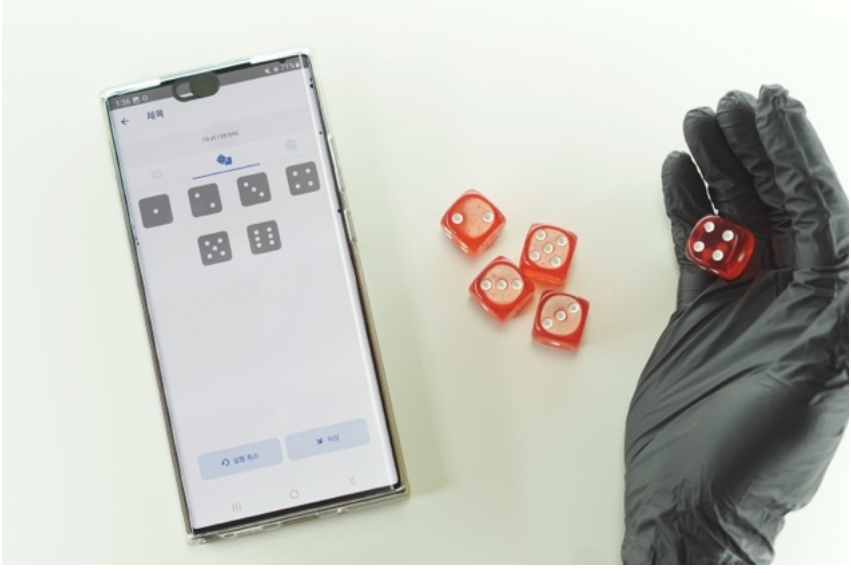
이제 지갑을 만들어보자. 홈 화면에서 [지갑 추가하기]를 누른다. 우리는 직접 주사위를 굴려서 니모닉을 만들 것이다. 오른쪽 위 점 세 개 → [주사위 굴림식 엔트로피 부여]를 누른다.

단어 수는 12단어와 24단어를 선택할 수 있다. 12단어로 할지 24단어로 할지 고민이 될 것이다. 필자는 주변인에게 셀프 커스터디를 알려줄 때 12단어는 충분한 것이고 24단어는 과도한 것이라고 말한다. 12단어도 똑같이 재현하는 것은 불가능하다. 그러나 보안에 있어서는 과도한 것도 나쁘지 않다. 12단어는 외우기 쉽다는 장점이 있으므로 자신이 선택하면 된다. 비트코인은 자신이 온전히 통제권을 갖는 것이므로 누군가 정해줄 수 없고 자신이 직접 선택해야 할 일이 많다.

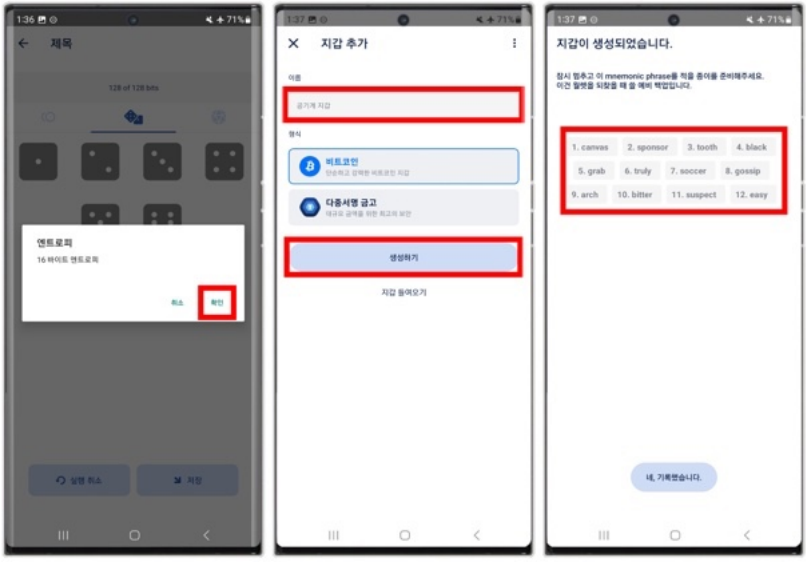


이제 주사위를 던져보자. 12단어 니모닉을 만들 것이라면 휴대폰에 뜨는 엔트로피가 128 bits가 될 때까지 주사위를 굴린다. 24단어 니모닉을 만들 것이라면 휴대폰에 뜨는 엔트로피가 256 bits가 될 때까지 주사위를 굴린다.

주의할 점이 있다. 주사위를 던지거나 니모닉을 기록할 때는 반드시 주변에 카메라가 없는지 확인해 보고 하라. 또한 전자기기가 있는 곳에서 주사위의 눈이나 니모닉을 소리 내 읽으면 안 된다. 필자는 니모닉을 만들 때 아무 전자기기도 없는 방에서 만든다.

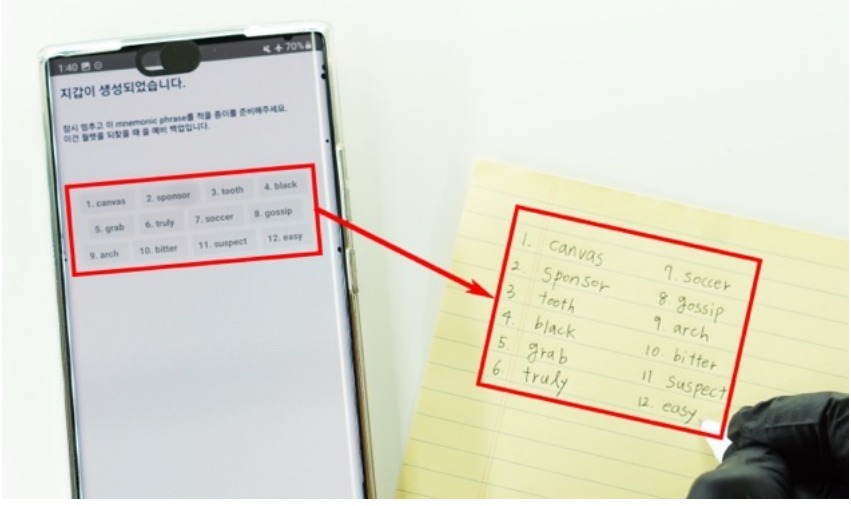


16바이트 엔트로피 혹은 32바이트 엔트로피라는 알림창이 나오면 [확인]을 누른다. 지갑 이름을 설정하고 [생성하기]를 누른다. 그러면 이제 니모닉 단어 목록이 보일 것이다. 이것을 잘 적어야 한다.

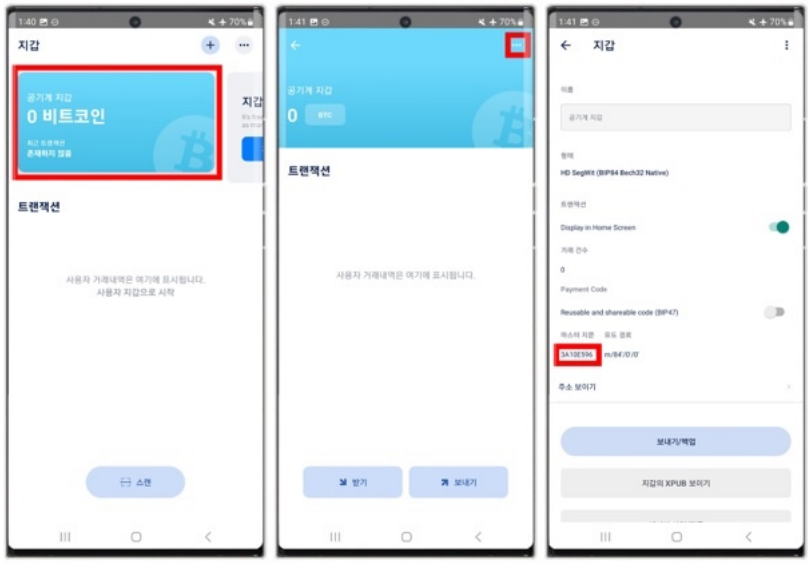


이 사진에 나와 있는 니모닉을 절대 사용하지 말 것. 이 니모닉은 테스트용으로 쓰였으며 온라인에 노출되었다. 이 니모닉에서 만들어지는 주소에 비트코인을 보내면 영영 되찾지 못할 수도 있다.

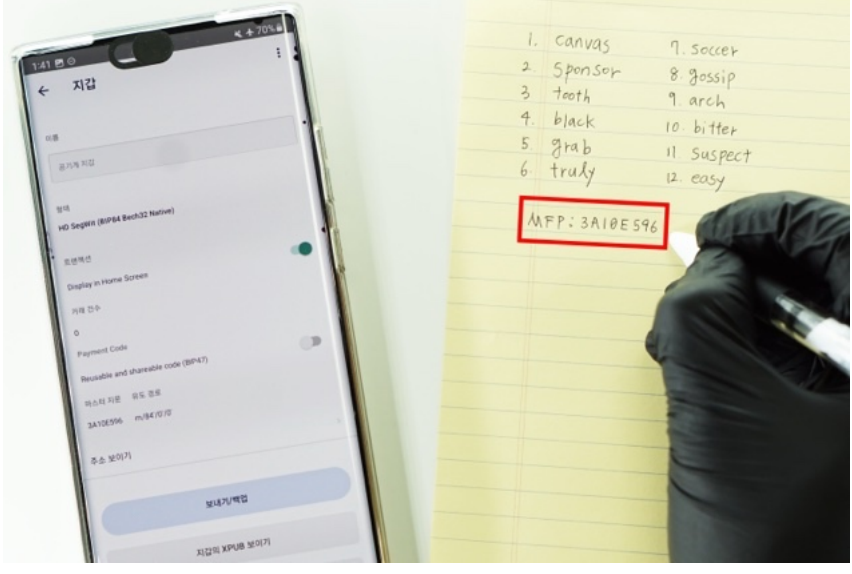
니모닉 목록을 종이에 잘 기록한다. 종이가 불에 탈 것을 염려해 철판 등을 사용할 수도 있다.



지갑이 다 만들어졌다. 지갑을 선택하고 오른쪽 위 점 세 개 → 마스터 지문 아래 [보기] 버튼을 눌러 MFP를 확인한다.



니모닉을 적은 종이에 MFP도 잘 적어놓는다.



지금까지 스마트폰 공기계를 콜드월렛으로 사용하여 지갑을 생성하는 방법을 알아보았다. 이제 워치-온리 지갑을 연결해 보자.

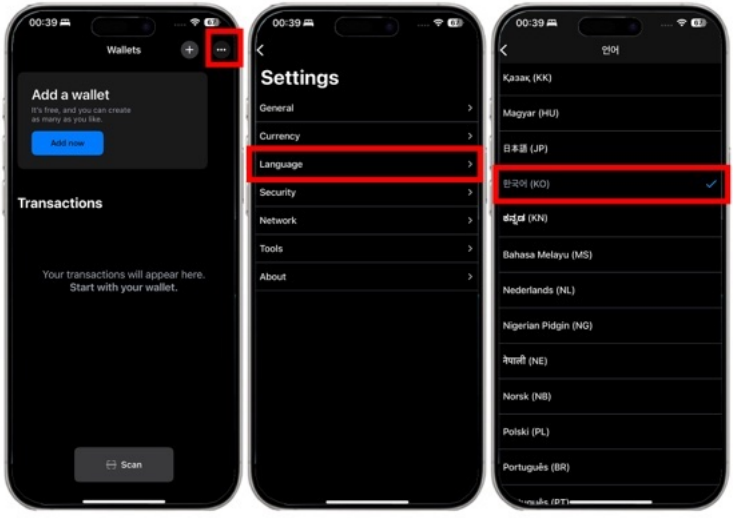
블루월렛에 확장 공개키 내보내 워치-온리 지갑 만들기

스마트폰에서 사용하는 워치-온리 지갑에는 블루월렛과 넌척, 코코넛 월렛 등이 있다. 블루월렛은 잔오류가 많다는 단점이 있지만, 현재 한국어를 지원하기 때문에 영어가 불편한 사람들은 편하게 사용할 수 있다. 넌척은 블루월렛보다 훨씬 안정성이 있지만 한국어 지원이 안 돼서 영어를 못하는 경우 불편하다. 코코넛 월렛의 경우 공기계에 블루월렛을 설치하여 콜드월렛으로 사용할 시, 서명된 PSBT의 QR 코드를 코코넛 월렛에서 읽지 못한다. 따라서 여기서 공기계 콜드월렛과 코코넛 월렛을 연동하는 방법은 다루지 않을 것이다. 워치-온리 지갑은 어느 하나만 사용하는 것보다는 두 가지 이상을 사용하며 교차 검증하는 것이 좋다.

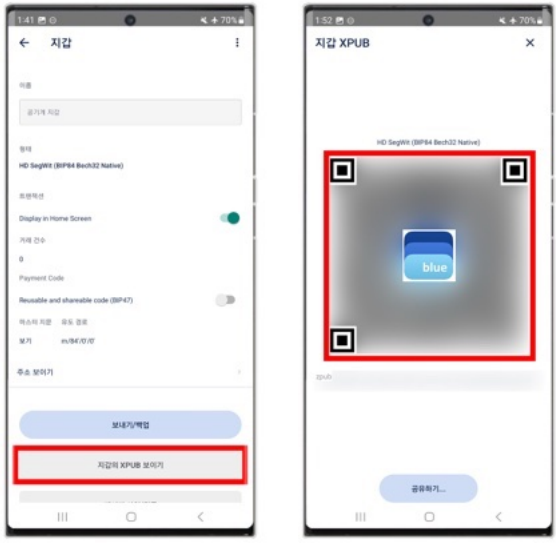
지금부터는 공기계가 아닌 인터넷이 연결되어 있는 다른 스마트폰을 사용해야 한다. 글에서 스마트폰의 모양에 주목하라. 가장자리가 각진 갤럭시 스마트폰은 콜드월렛으로 쓰는 공기계, 가장자리가 둥근 아이폰은 워치-온리 지갑 앱을 설치할 스마트폰이다.

워치-온리: 먼저 블루월렛과 넌척을 설치하자. 구글 플레이스토어나 애플 앱스토어에서 BlueWallet, Nunchuk을 검색하고 다운로드한다. iOS 기준으로 설명하지만, 안드로이드도 크게 다르지 않다.

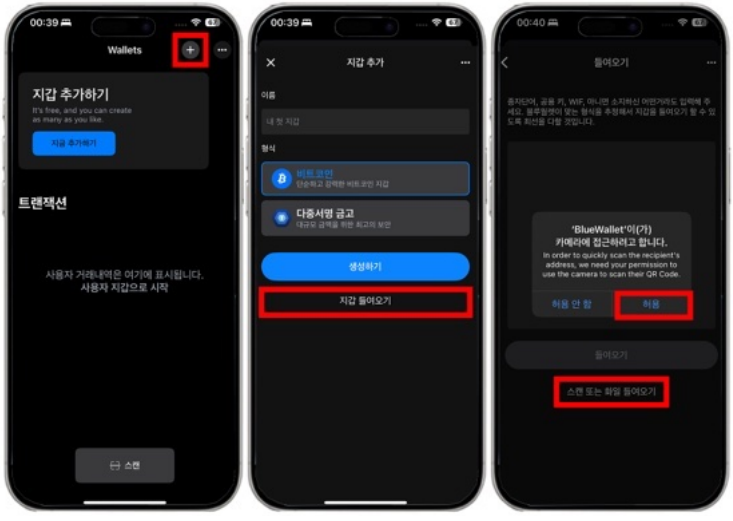
워치-온리: 블루월렛 앱을 실행한다. 한국어가 편하다면 언어 설정부터 바꾸자. 오른쪽 위 점 세 개 → [Language] → [한국어]를 선택하고 뒤로 가기를 누른다.



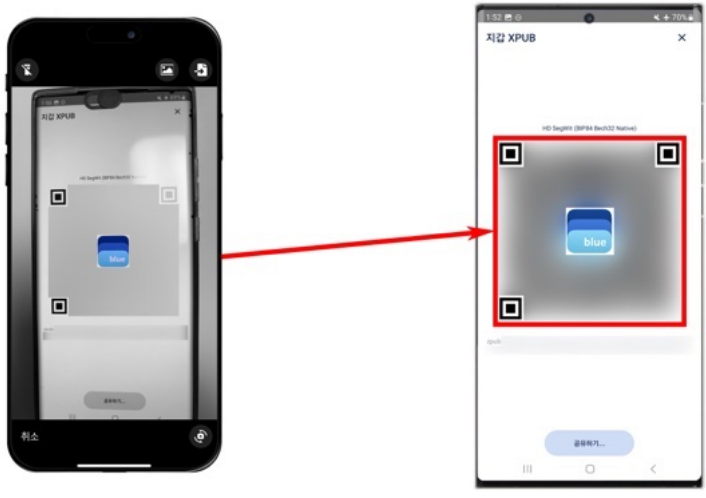
공기계: 블루월렛의 지갑 설정에서 [지갑의 XPUB 보이기]를 누른다.



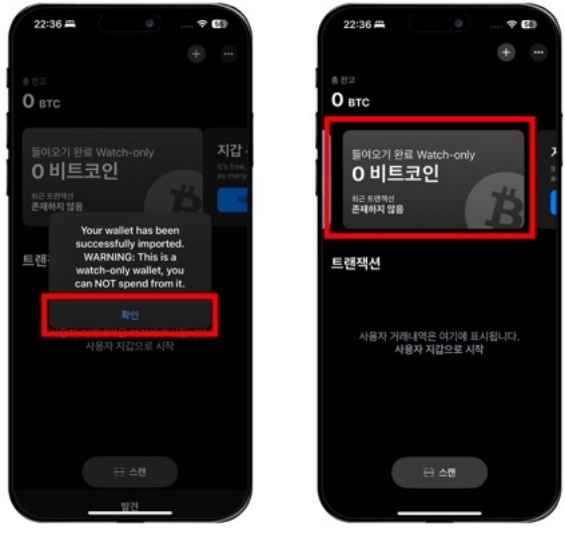
워치-온리: 스마트폰의 블루월렛에서 우측 상단 [+] → [지갑 들여오기] → [스캔 또는 화일 들여오기] → 카메라 [허용]을 누른다.



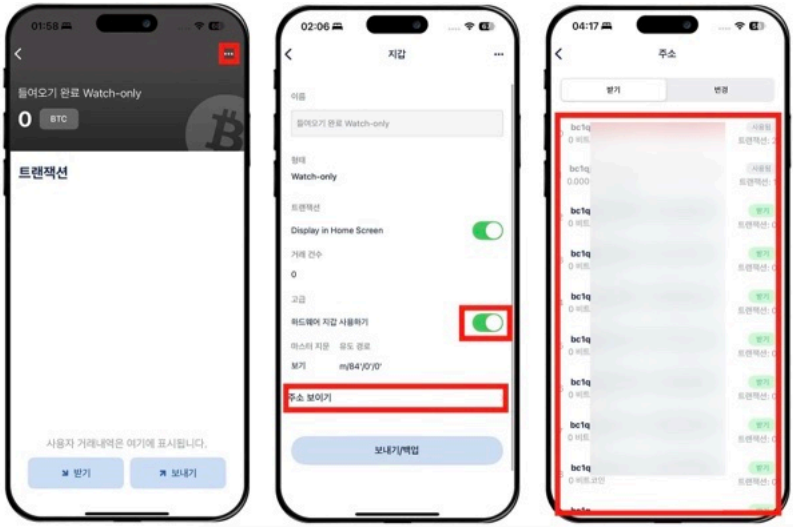
워치-온리: 블루월렛에서 카메라 화면이 뜨면 공기계 콜드월렛에 나오는 QR 코드를 찍는다. 이것이 확장 공개키를 내보내는 과정이다.



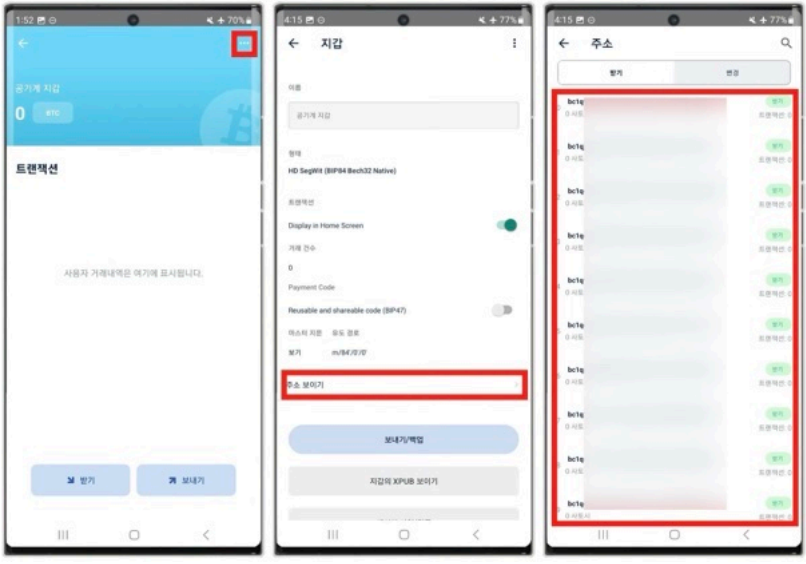
워치-온리: 공기계에 나오는 QR 코드를 스캔하면 자동으로 지갑이 만들어질 것이다.



워치-온리: 지갑에 들어와서 오른쪽 위의 점 세 개를 누른 후, [하드웨어 지갑 사용하기]를 켠다. 이 옵션을 켜야 공기계에서 서명을 받아올 수 있다. 이제 주소를 검증해 보자. 아래에 있는 [주소 보이기]를 누른다.



공기계: 공기계 콜드월렛의 블루월렛에서도 똑같이 한다. 오른쪽 위 점 세 개 → [주소 보이기]를 눌러 주소를 확인한다. 공기계와 워치-온리 지갑에서 나오는 주소 목록이 같은지 확인한다.



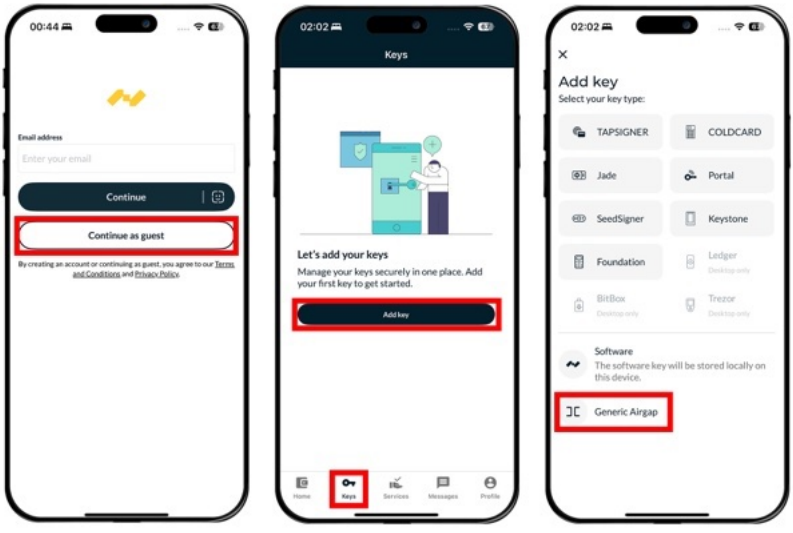
이제 워치-온리 지갑인 블루월렛과 공기계의 블루월렛을 연동하는 것이 끝났다. 앞으로 워치-온리 지갑인 블루월렛에서 '받기'를 누르고 비트코인을 받으면 된다. 하지만, 일단 소액만 보내보고 서명 연습을 한 뒤에 본격적으로 사용하길 바란다.

넌척에 확장 공개키 내보내 워치-온리 지갑 만들기

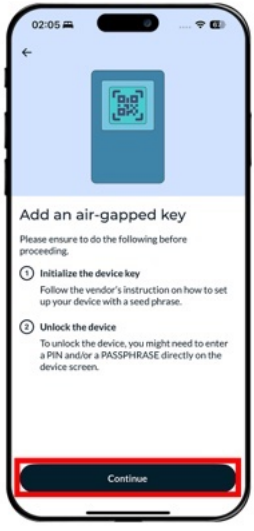
이제 워치-온리 지갑인 넌척과 공기계 콜드월렛을 연동해 보자.

워치-온리: 앞에서 설치했던 넌척을 켠다. 우리는 게스트 모드로 넌척을 사용할 것이다. 어차피 얼마든지 공기계와 넌척을 연동할 수 있으므로 로그인이 필요 없기 때문이다. [Continue as guest]를 누른다.

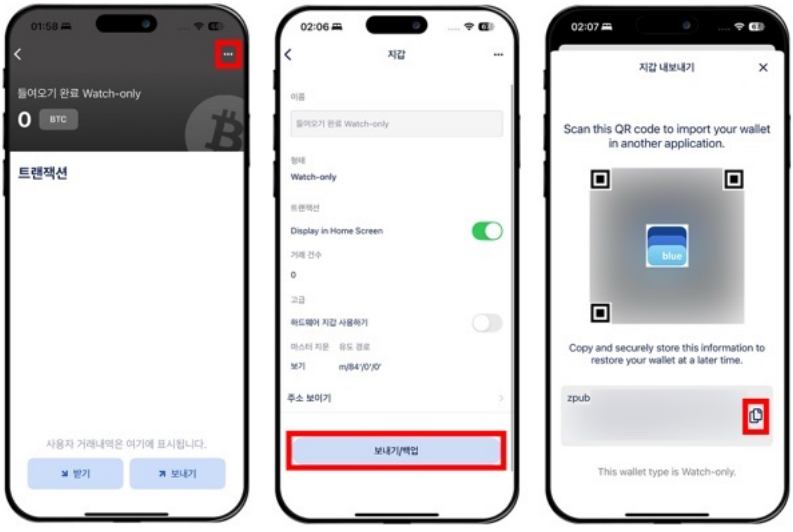
이후에 화면에서 [Add key] 버튼이 보인다면 바로 누르고, 안 보인다면 아래 탭에서 [Keys]를 누른 뒤 [Add key]를 누른다. 그다음에 [Generic Airgap]을 누른다.



워치-온리: [Continue]를 누른다. 그러면 확장 공개키를 입력하는 창이 나온다. 이때 확장 공개키를 내보내는 과정이 일반 과정과 다르다. 공기계의 블루월렛은 일반 확장 공개키를 QR 코드로 내보내지만, 넌척은 이를 읽지 못한다. 왜냐하면 넌척은 'Descriptor'라고 하는 추가 정보가 포함된 확장 공개키만을 읽을 수 있기 때문이다. 따라서 우리는 확장 공개키를 QR 코드로 내보내지 않고 다른 방법을 이용하여 확장 공개키를 내보낼 것이다.



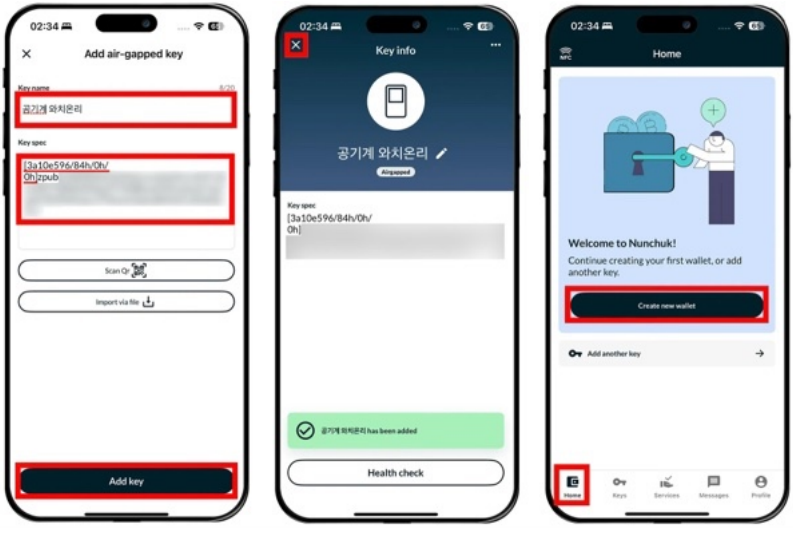
워치-온리: 블루월렛으로 들어가 워치-온리 지갑에서 오른쪽 위 점 세 개 → [보내기/백업]을 누른다. 그러면 확장 공개키인 zpub이 나온다. 옆의 문서 모양 버튼을 눌러 이 정보를 복사한다.



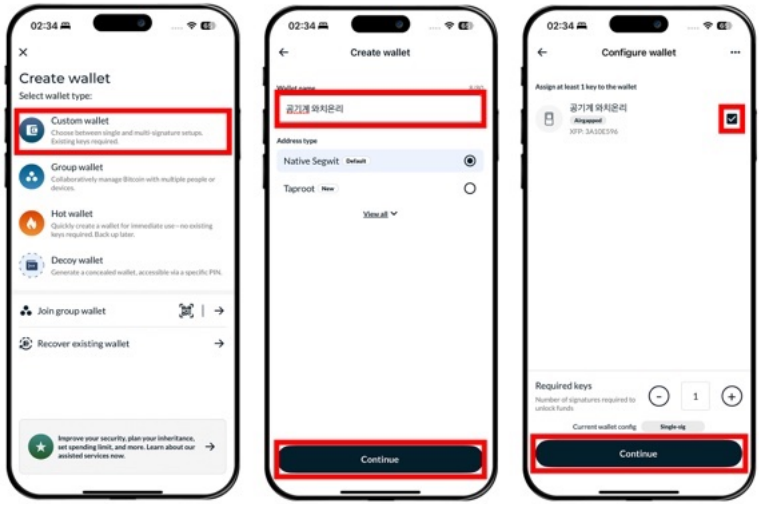
워치-온리: 이제 다시 넌척으로 돌아온다. 지갑 이름을 설정한다. 그 다음 'Key spec'에 블루월렛에서 복사했던 zpub 정보를 붙여넣기 한다.

여기가 중요하다. 이대로 [Add key]를 누르면 넌척이 인식을 할 수가 없다. 그래서 맨 앞에 '[MFP/84h/0h/0h]'를 붙여줘야 한다. MFP는 앞에서 지갑 만들 때 적었던 MFP를 소문자로 적어주면 된다. 사진의 예시에서는 '[3a10e596/84h/0h/0h]zpub…'을 적었다.
잘 적었다면 [Add key]를 누르고, [x] 버튼을 누른다.

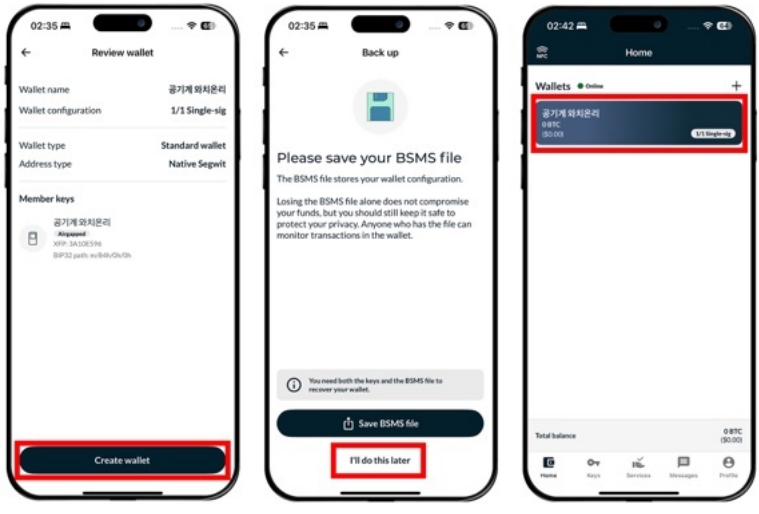
아래 탭의 [Home]에서 [Create new wallet]을 누른다.



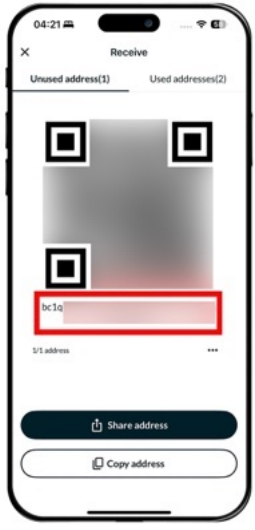
워치-온리: [Custom wallet]을 누르고, 지갑 이름을 설정한다. [Continue]를 누르고, 키를 선택한다. 다시 [Continue]를 누른다.

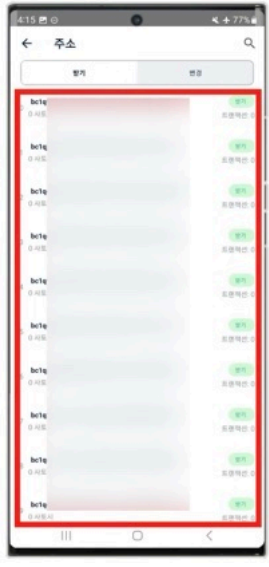


워치-온리: [Create wallet] → [I'll do this later]까지 누르면 넌척도 워치-온리 지갑 연동이 끝난다.

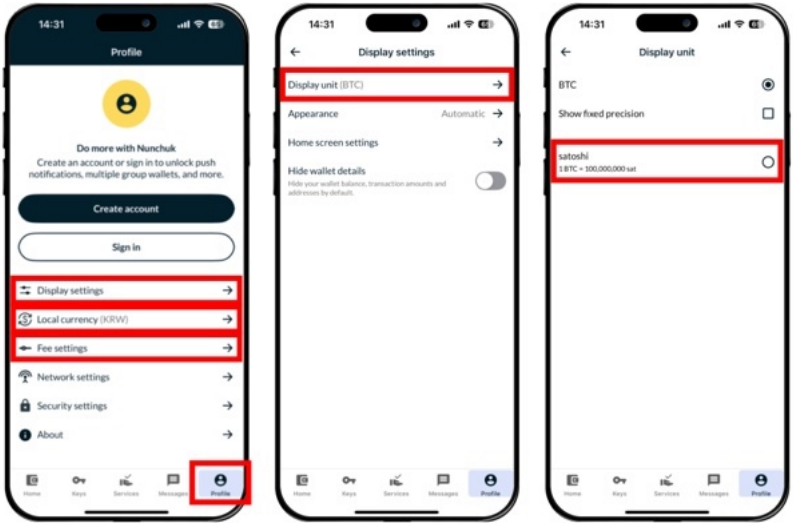


워치-온리: 넌척 지갑에서 [Receive]를 누르면 나오는 지갑 주소가 공기계의 블루월렛에서 [주소 보이기]를 누르면 나오는 주소 목록에 속하는지 확인한다.





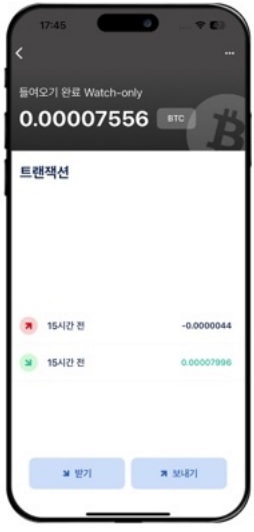
참고로 넌척 하단 탭의 [Profile]을 선택하면 몇 가지 설정을 할 수 있다. [Display settings]에서 일상적인 단위인 sat로 변경할 수 있다. [Display unit]을 누르고 [satoshi]를 선택하면 된다. 이 외에도 [Local currency]에서 [South Korean Won (KRW)]를 선택해 통화 단위를 바꿀 수 있고, [Fee settings] → [Default fee rate] → [Priority]를 선택해 온-체인 수수료를 좀 더 많이 지불하는 대신 거래가 빠르게 컨펌되도록 할 수도 있다.

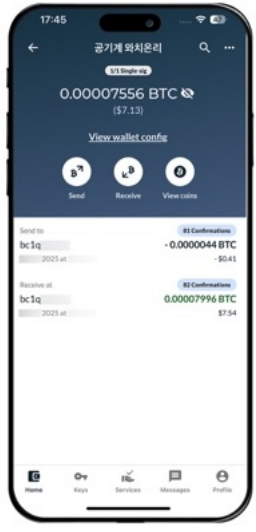


블루월렛으로 서명 연습

본격적으로 비트코인을 지갑에 보관하기 전 꼭 해야 하는 것이 있다. 서명이 잘 되는지 확인과 복구 연습을 미리 해봐야 한다. 이것을 안 하고 덜컥 비트코인 모으기부터 시작하는 경우가 있는데, 이러면 나중에 거액이 들어간 상태에서 서명이나 복구를 처음 해보다가 안 되는 경우 난감해질 수 있다.

워치-온리: 서명 연습을 해보자. 서명 연습을 하기 위해 7천 sats 정도를 지갑에 일단 보내보았다. 비트코인을 지갑에 보내는 방법은 뒤에 나오는 '거래소에서 지갑으로 비트코인 옮기기' 장을 참고하라. 블루월렛과 넌척 둘 다 금액이 잘 확인된다.





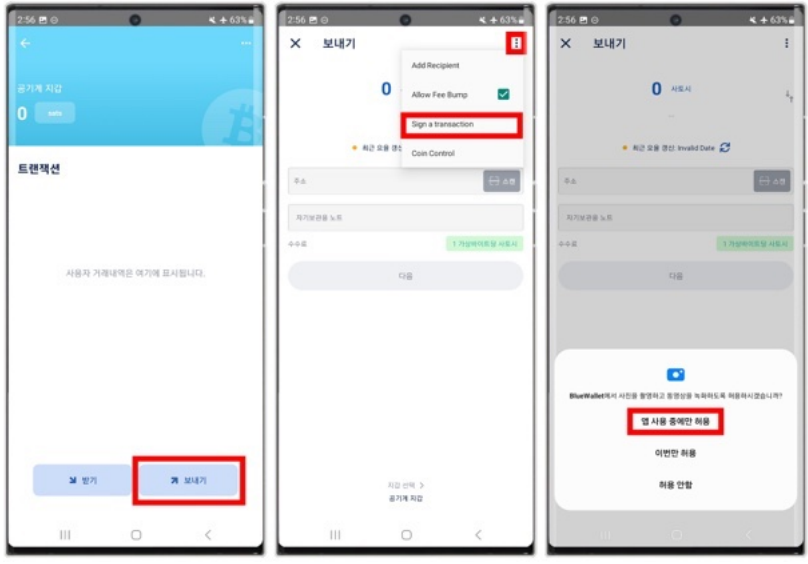
워치-온리: 블루월렛에서 서명 연습을 해보자. 먼저 [받기] 버튼을 누르고 뜨는 주소를 복사한다. 프라이버시와 보안을 위해 주소는 재사용하지 않는 것이 좋은데, 블루월렛과 넌척, 코코넛 월렛은 안 쓴 주소를 자동으로 보여준다. 주소를 한 번 누르면 자동으로 주소가 복사된다.

이제 [x] 버튼을 누른 뒤 [보내기] 버튼을 누른다. 주소창에 아까 복사했던 주소를 붙여넣는다. 서명 연습을 하기 위해 내 비트코인을 다시 나에게 보내는 거래(트랜잭션)를 일으키는 것이다.

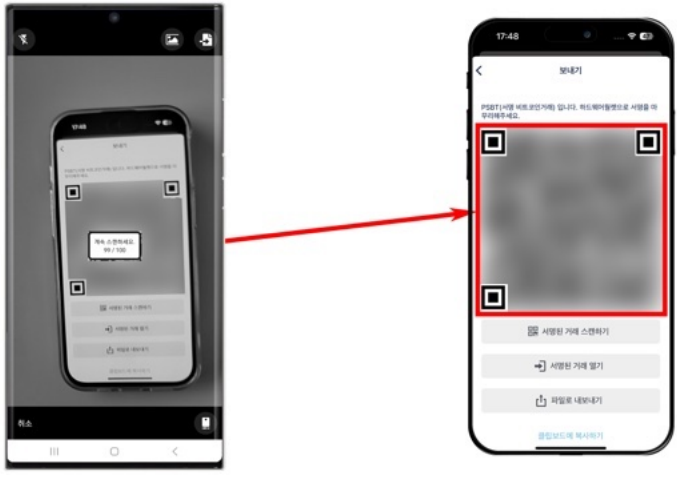
그 위에 있는 금액에는 수수료를 제외하고 보낼 금액을 입력한다. 비트코인 온-체인에는 수수료가 있기 때문에 2,000–3,000 sats 이상 제외하고 송금 연습을 해야 한다.

참고로 수수료 옆에 있는 민트색 박스를 누르면 수수료율을 자신이 직접 설정할 수도 있다. 멤풀을 보고 적정 수수료율을 설정하는 연습도 해보면 좋다.

공기계: 공기계 블루월렛에서 [보내기]를 누르고, 오른쪽 위 점 세 개 → [Sign a transaction (거래를 사인하세요)]를 누른다. 카메라 접근 권한을 요청하면 [허용]을 누른다.



공기계: 워치-온리 지갑(블루월렛)에 나오는 움직이는 QR 코드를 스캔한다.

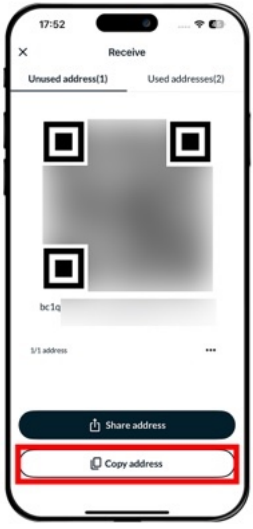


워치-온리: 블루월렛에서 [서명된 거래 스캔하기]를 누르고, 공기계 블루월렛에서 나오는 QR 코드를 스캔한다.

워치-온리: 서명이 올바르다면 직렬화된 서명 데이터(나열된 숫자들)가 나타날 것이고, 여기서 [바로 보내기]를 누르면 네트워크에 전송된다.

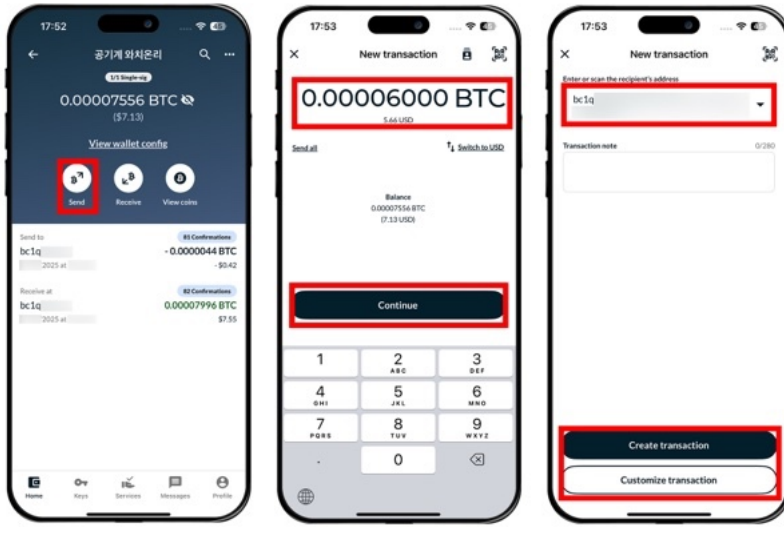
넌척으로 서명 연습

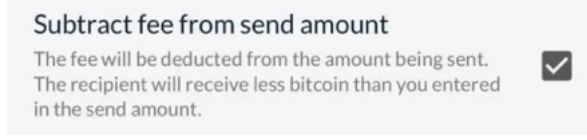
워치-온리: 넌척에서 서명할 때도 블루월렛과 비슷하게 진행한다. 먼저 [Receive(받기)]를 누르고 [Copy address]를 눌러 주소를 복사한다.



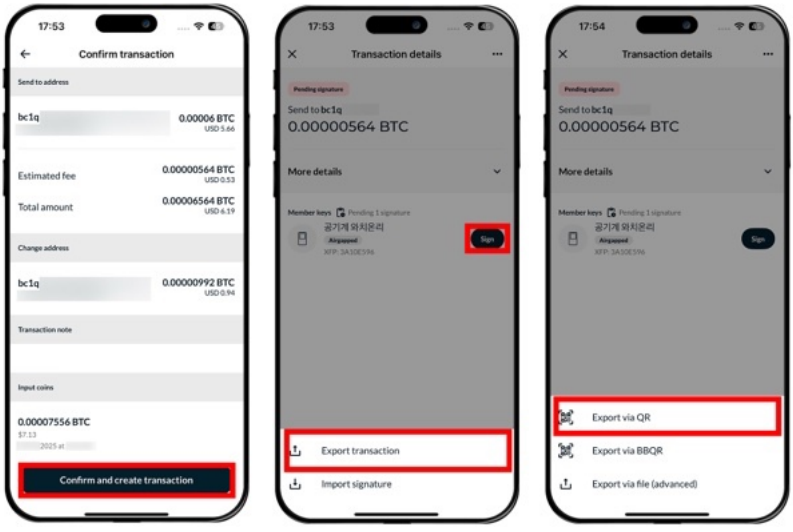
워치-온리: 이제 [Send]를 누르고 보낼 금액을 입력한다. 이때 수수료는 제외하고 보내야 한다. [Continue]를 누른다. 아까 복사했던 주소를 붙여넣기 하고 [Create transaction]을 누른다. 참고로 [Customize transaction]을 누르면 수수료율을 직접 설정하거나, 어떤 UTXO를 선택해서 보낼지 설정할 수 있다.

[Customize transaction]에서 [Subtract fee from send amout] 옵션을 체크하면 넌척이 보낼 금액에서 알아서 수수료만 차감하고 보낸다. 이렇게 하면 예상 수수료를 계산할 필요 없이 전액을 보내면 되기 때문에 편리하다.

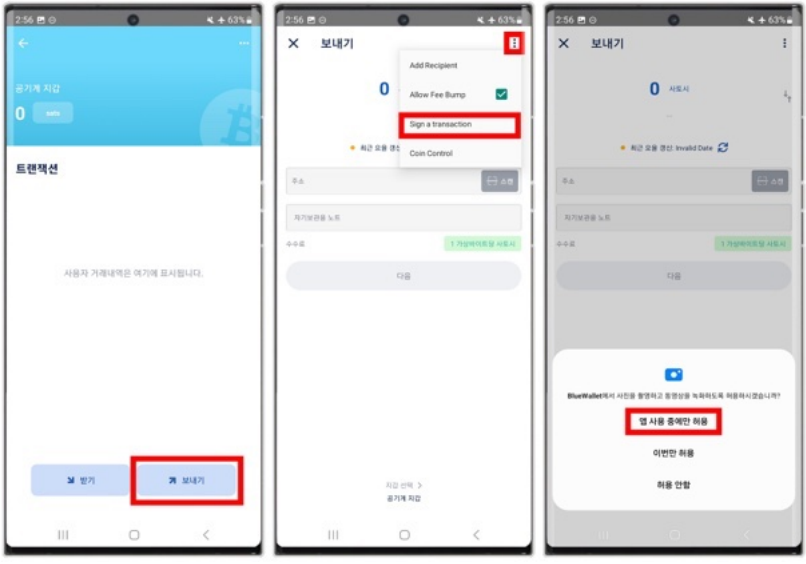




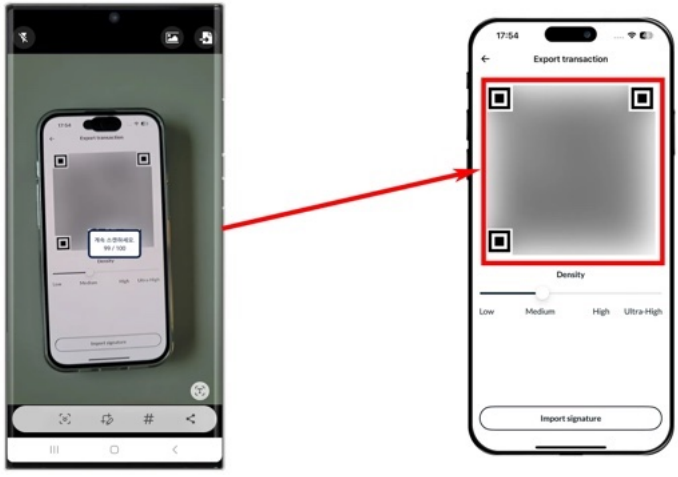
워치-온리: [Sign]을 누르고, [Export transaction]을 누른다. 그다음에 맨 위에 있는 [Export via QR]을 누르면 QR 코드가 나올 것이다.



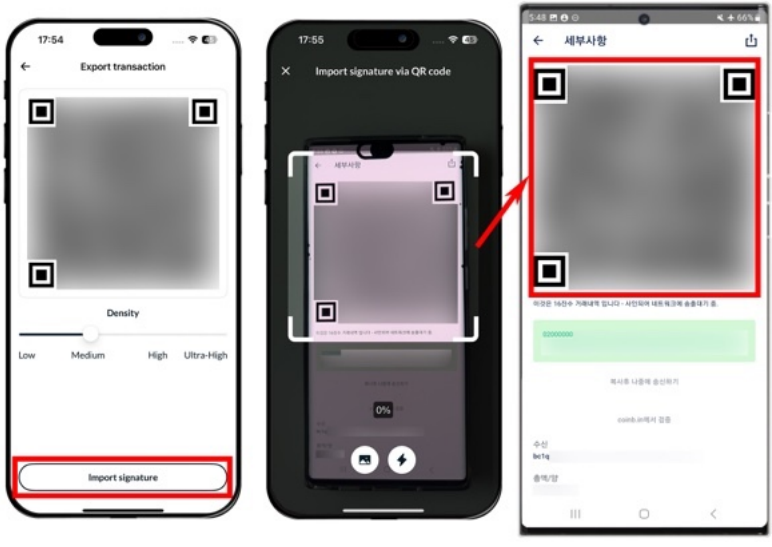
공기계: 공기계 블루월렛에서 [보내기]를 누르고, 오른쪽 위 점 세 개 → [Sign a transaction (거래를 사인하세요)]를 누른다. 카메라 접근 권한을 요청하면 [허용] 버튼을 누른다.



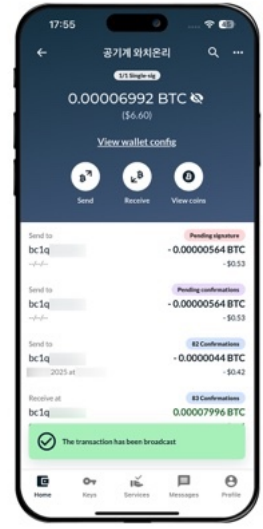
공기계: 워치-온리 지갑(넌척)에 나오는 움직이는 QR 코드를 스캔한다.



워치-온리: 블루월렛에서 [서명된 거래 스캔하기]를 누르고, 공기계 블루월렛에서 나오는 QR 코드를 스캔한다.



[Broadcast transaction]을 누르면 네트워크에 전파된다.



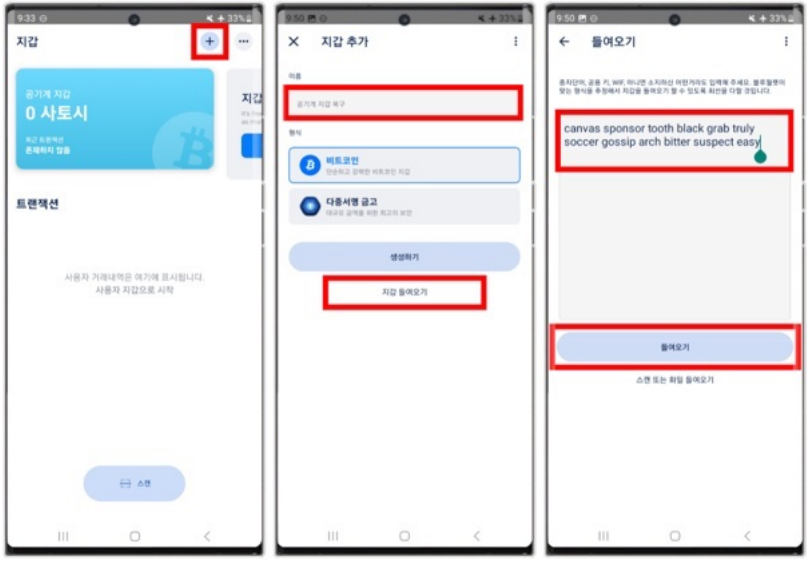
이로써 서명까지 잘 되는 것을 모두 확인해 보았다.

공기계 블루월렛에서 간접 복구 테스트

공기계에 블루월렛을 설치해 콜드월렛으로 쓰는 경우 지갑을 삭제하면 앱의 캐시 문제 등으로 복구가 제대로 안 되는 오류가 있다. 따라서 장기적으로 사용하기보다는 일시적으로 사용하다가 좀 더 돈이 모이면 에어-갭 콜드월렛을 하나 장만하는 것을 추천한다. 여기서는 공기계에 있는 블루월렛 앱에서 지갑을 삭제하는 대신, 지갑이 있는 상태에서 똑같은 니모닉으로 지갑을 불러옴으로써 '이미 존재하는 지갑입니다.'를 확인하여 간접적으로 복구 테스트를 해볼 것이다.

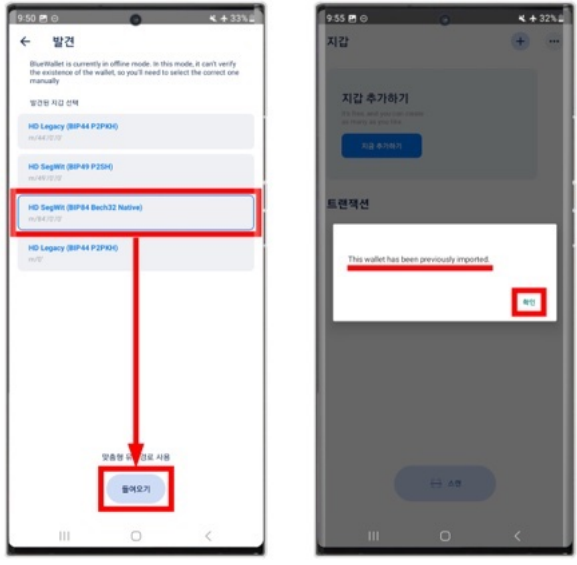
공기계: 블루월렛 홈 화면에서 우측 상단 [+] 버튼 → [지갑 들여오기]를 누른다.

입력창에 백업했던 니모닉을 입력한다. 반드시 공기계에서 입력해야 한다. 온라인에 연결된 워치-온리 지갑에서 니모닉을 입력하면 안 된다. 온라인에 연결된 워치-온리 지갑에 니모닉을 입력하면 핫월렛이 된다. 니모닉 단어를 순서대로 입력하고, 니모닉 단어와 단어 사이는 띄어쓰기로 구분하여 입력하면 된다. 오타가 나지 않도록 주의하자. 다 입력했으면 [들여오기]를 누른다.



파생 경로를 선택해야 한다. [HD SegWit (BIP84 Bech32 Native)]를 선택하고, [들여오기]를 누른다.

이미 있는 지갑을 불러왔으므로 'This wallet has been previously imported. (이 지갑은 이미 있습니다.)'라는 안내문이 나와야 정상이다. 그러면 니모닉을 제대로 백업했다는 뜻이다. 니모닉만 제대로 적었다면 다른 에어-갭 지갑에서 얼마든지 지갑을 복구할 수 있다.



공기계는 비트코인을 다른 곳으로 보낼 때 서명 과정에서만 사용할 것이다. 비트코인을 받을 때는 공기계가 필요 없다. 워치-온리 지갑만 있으면 된다. 여기까지 숙지했다면 이제 비트코인을 모으면 된다.

| 거래소에서 지갑으로 비트코인 옮기기

거래소에서 비트코인으로 환전하는 방법

원화를 비트코인으로 환전하는 방법은 크게 두 가지가 있다. 하나는 거래소를 통해 환전하는 방법이다. 다른 하나는 개인 간 거래(이하 P2P)를 통해 환전하는 방법이다. P2P로 환전하려면 먼저 비트코이너가 많은 디스코드, 텔레그램, 카카오톡 등의 채널로 가는 것이 좋다. P2P 거래는 대면 거래, 비대면 거래 등 다양한 형태의 거래가 있고 거래 당사자끼리 합의하여 거래하는 것이므로 방법은 생략한다. 다만, 대면 거래 시에는 물리적 공격을 조심해야 하고, 비대면 거래 시에는 사기의 위험이 있으니 조심해야 한다. 조금만 더 알아보면 에스크로 서비스도 있으므로 스스로 찾아보길 바란다.

지금부터는 거래소를 통해 환전하는 방법을 서술하겠다. 입문자들은 처음에는 대부분 이 경로를 통해 환전할 것이다. 그러나 이 방법은 P2P 거래에 비해 매우 번거롭다. 나중에 신뢰할 만한 P2P 거래 방법을 개발해 놓으면 그것이 훨씬 편하다는 것을 느끼게 될 것이다.

거래소에서 비트코인을 환전하기 위해서는 다소 번거로운 절차를 거쳐야 한다. 대한민국의 각종 규제 때문이다. 대한민국은 암호화폐에 대한 '트래블룰'을 세계 최초로 시행한 국가로, 국내 거래소에서는 신원이 일치하지 않는 다른 거래소로 출금할 수가 없다. 개인 지갑에 신원이 연결되어 있을 리가 없으므로, 국내 거래소에서 출금할 때는 신원이 일치하는 해외 거래소로 먼저 옮긴다.

또한, 국내 거래소나 해외 거래소는 각각 수수료 정책이 모두 다르다. 국내 거래소는 비트코인 출금 수수료가 대략 2만 사토시다. 반면 테

더의 트론 네트워크를 사용하여 해외 거래소로 보내면 수수료가 아예 없거나 매우 낮다. 따라서 국내 거래소로 옮길 때는 테더를 통해 해외 거래소로 보낸다. 이는 국내 거래소들이 라이트닝 네트워크를 지원하지 않기 때문이기도 한데, 라이트닝 네트워크를 지원한다면 테더를 쓸 이유가 없다.

이 글에서는 국내 거래소로 빗썸을 이용하고, 해외 거래소로 바이낸스를 이용할 것이다. 특정 거래소에 대한 광고는 절대 아니다. 필자는 거래소에 대해 부정적인 입장이다. 거래소에 있는 비트코인은 당신의 비트코인이 아니며 언제든 동결될 수 있다. 따라서 개인 지갑으로 옮기는 중간 경로로만 쓸 것을 권장한다. 심지어 옮기는 도중에 동결될 위험이 있다는 사실도 인지하고 있어야 한다.

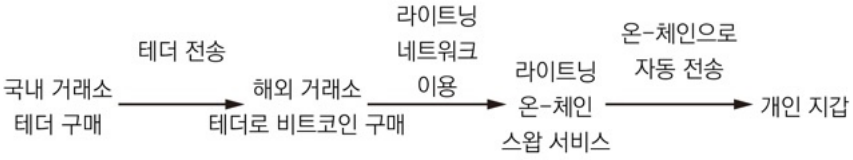
각각의 거래소를 선택한 이유를 들자면, 국내 거래소들 중에는 출금 시 자신들 마음대로 출금을 정지하거나, 자금을 소명하라거나, 머그샷처럼 사진을 찍어 보내야만 출금을 처리해 주는 거래소들이 있다. 이 글에서는 그나마 그런 일이 적은 빗썸을 선택했다. 해외 거래소는 준비금과 거래 대금이 제일 많은 바이낸스를 선택했다.

해외에는 라이트닝 네트워크 전송을 지원하는 거래소들이 많다. 라이트닝 네트워크를 이용한 비트코인 전송은 온-체인에서의 전송보다 수수료가 적고 빠르며, 소액 전송에 적합하다. 바이낸스에서 비트코인 출금 수수료는 비트코인 네트워크 상황에 따라 바뀌지만, 보통 3-4천 sats 정도다. 반면 라이트닝 네트워크를 이용하여 출금할 때는 수수료가 100 sats 정도다. 단, 1회 전송에 최대 약 99만 sats까지 전송할 수 있으며, 그마저도 99만 sats를 꽉 채워 보내면 출금 거절을 당해 70-80만 sats 정도로 낮춰 보내야 하는 경우가 많다.

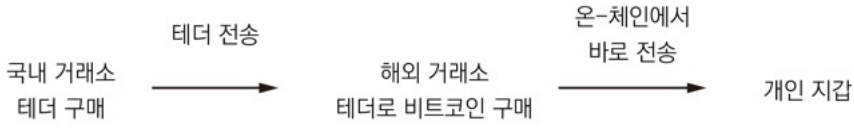
라이트닝 네트워크를 이용하여 개인 지갑으로 비트코인을 출금할 때는 라이트닝 → 온-체인 스와프를 이용해야 한다. 이는 라이트닝 네트워크로 보낸 금액을 온-체인으로 바꿔 전송해 주는 서비스다. 대표적으로 볼츠Boltz가 있는데, 볼츠의 경우 라이트닝에서 온-체인으로 스와프 시 0.5% 수수료에 온-체인 수수료 약 1천-2천 sats가 따로 들어간다(반대로 온-체인에서 라이트닝으로 스와프하는 것은 수수료가 0.1%다). 따라서 수수료 절감을 위해서는 출금 금액이 30만 sats보다 높은 경우에는 온-체인 출금을, 출금 금액이 30만 sats 미만인 경우에는 라이트닝 네트워크와 볼츠 스와프 서비스를 이용하는 것이 좋다.

라이트닝 네트워크를 이용하려면 자신이 라이트닝 노드를 운영하지 않는 이상 라이트닝 수탁 서비스를 이용해야 한다. 라이트닝 수탁 서비스에는 월렛 오브 사토시, 블링크, 스피드 등이 있다. 라이트닝 네트워크를 결제 목적으로 쓸 때는 월렛 오브 사토시를 이용할 것인데, 이는 다음 부에서 다룰 것이다.

정리해 보자. 30만 sats 이하를 거래소에서 개인 지갑으로 보낼 때 수수료를 최대한 절약하기 위해서는 다음과 같은 경로를 따른다. 국내 거래소(빗썸)에서 테더 구매 → 해외 거래소(바이낸스)로 테더 전송 → 해외 거래소(바이낸스)에서 테더로 비트코인 구매 → 해외 거래소(바이낸스)에서 라이트닝 네트워크와 볼츠 스와프 서비스를 통해 개인 지갑으로 전송.

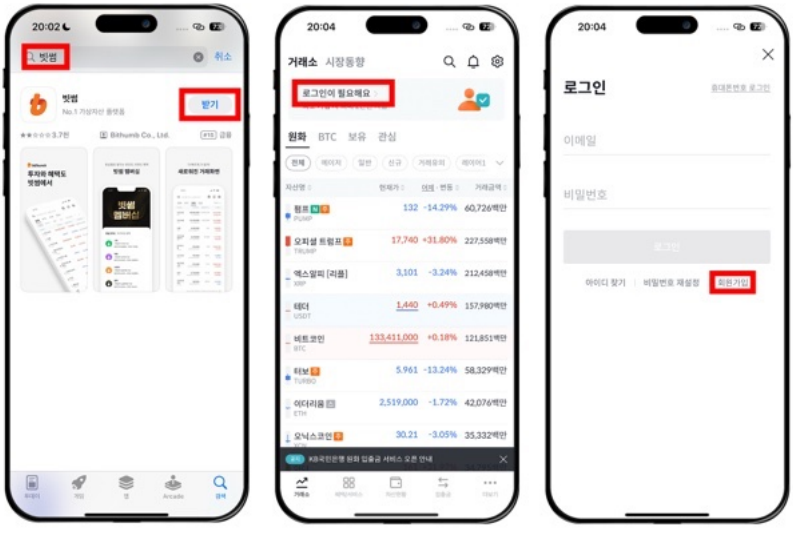


만약 30만 sats 이상의 금액을 보낸다면 다음과 같은 경로를 따른다. 국내 거래소(빗썸)에서 테더 구매 → 해외 거래소(바이낸스)로 테더 전송 → 해외 거래소(바이낸스)에서 테더로 비트코인 구매 → 해외 거래소(바이낸스)에서 온-체인 전송으로 바로 개인 지갑으로 전송.

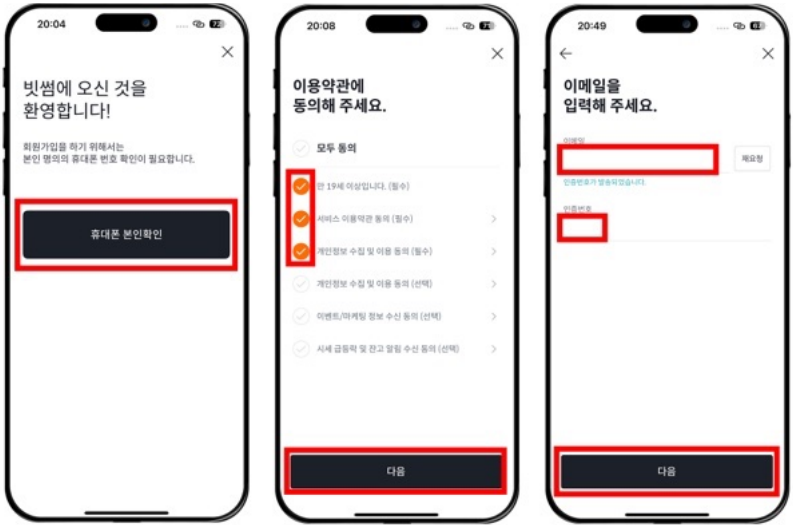


빗썸 가입 및 KYC 인증

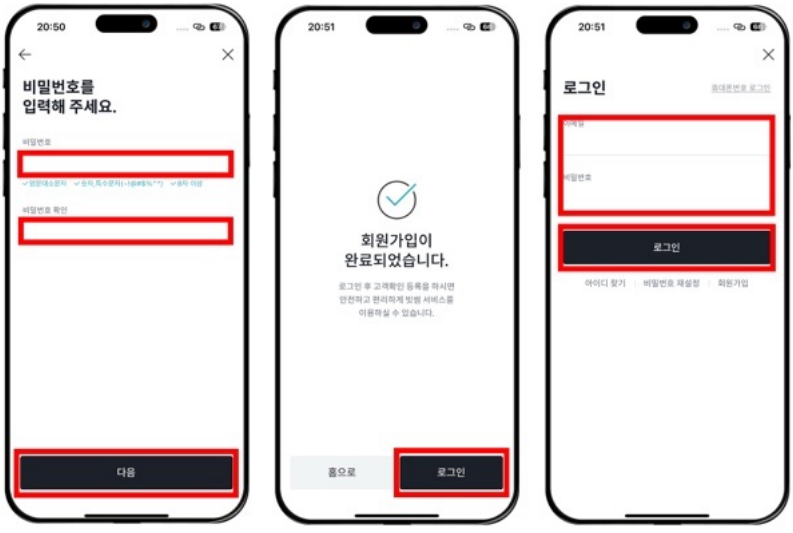
국내 거래소 중 빗썸은 KB국민은행과 연동된다. 따라서 KB국민은행의 계좌가 먼저 개설되어 있어야 한다. 먼저 앱스토어 또는 구글 플레이스토어에서 '빗썸' 앱을 다운로드한다. 빗썸을 켜고 로그인 화면에서 [회원가입]을 누른다.



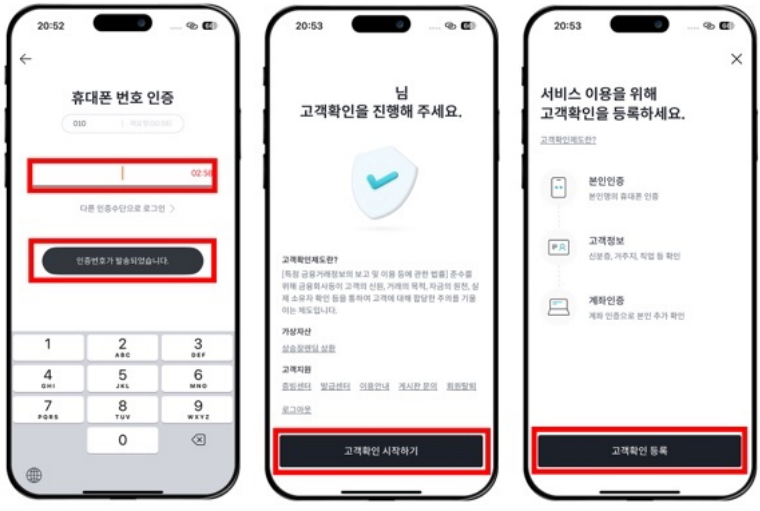
먼저 휴대폰 본인확인 절차를 마친다. 그다음에는 이용약관에 동의하고, 이메일 인증도 한다.



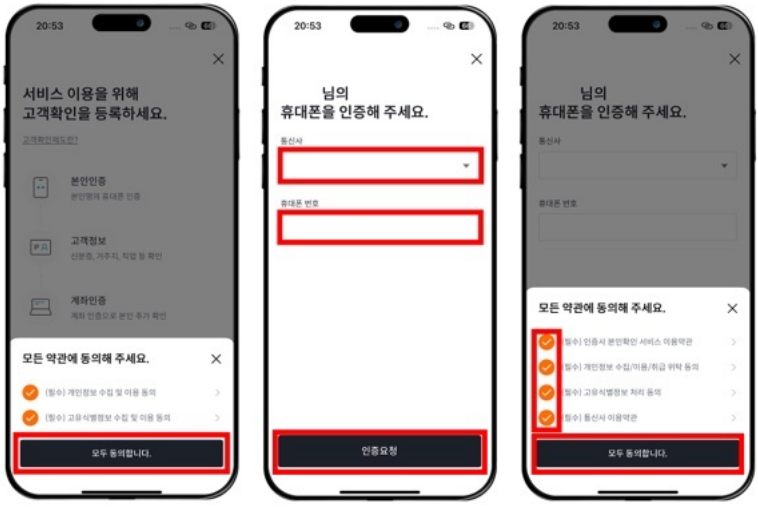
비밀번호까지 설정하면 회원가입이 완료된다. 이제 이메일과 비밀번호를 이용해 빗썸에 로그인한다.



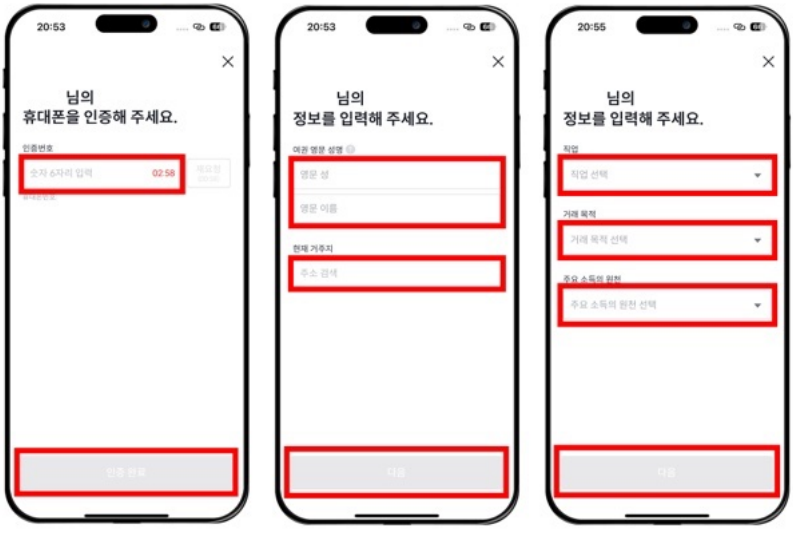
휴대폰 번호 인증을 하면 로그인이 될 것이다. 로그인하면 바로 고객확인(KYC) 창이 뜬다. [고객확인 시작하기] → [고객확인 등록]을 누른다.



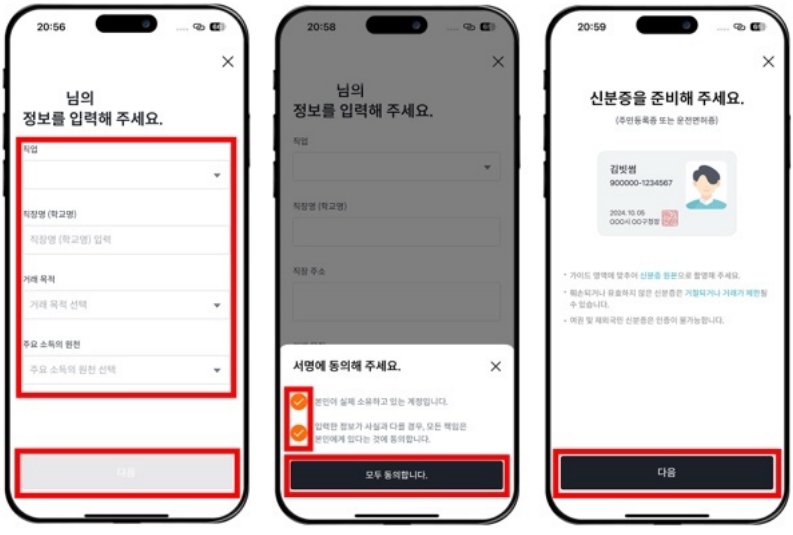
약관에 동의한 뒤 휴대폰 인증을 마친다.



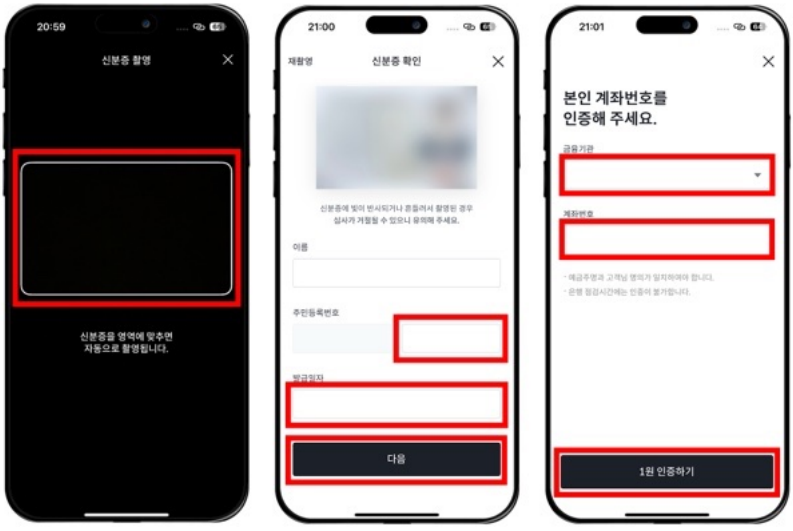
그다음에는 영문 성과 영문 이름을 입력해야 한다. 이때 여권이 있다면 여권상의 영어 성과 영어 이름을 써야 한다. 해외 거래소의 영문 이름이 빗썸의 영문 이름과 일치해야 하므로 주의하여 쓰자. 그리고 성을 먼저 써야 한다. 거주지와 직업까지 쓴다.



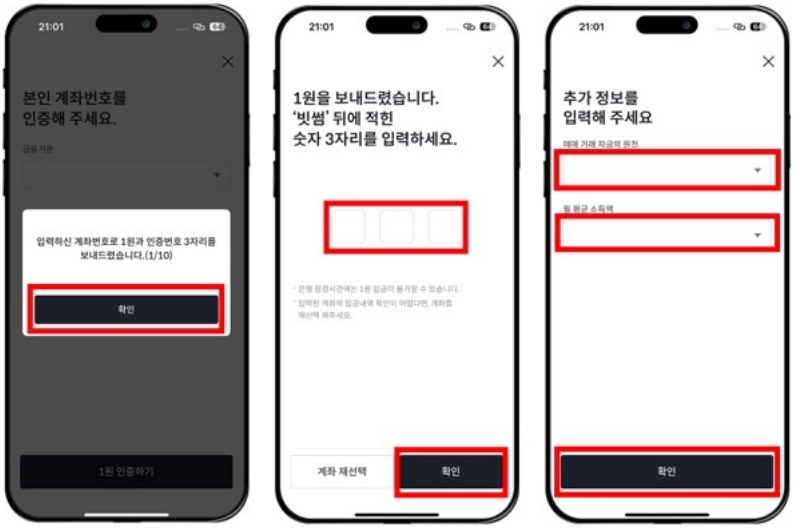
직장 정보까지 쓰고 나면 신분증 인증을 시작한다.



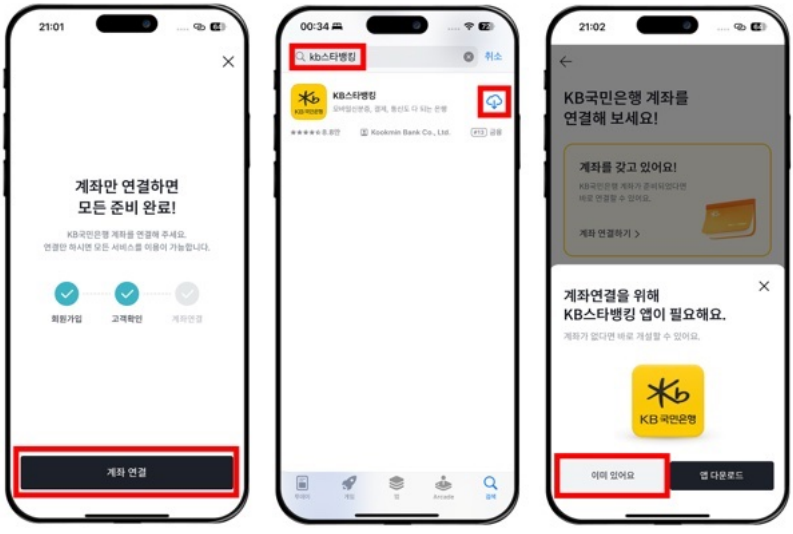
밝은 곳에서 신분증을 촬영하되 빛이 반사되지 않도록 주의한다. 신분증을 촬영하면 자동으로 이름과 주민등록번호가 기입된다. 주민등록번호 뒷부분을 쓰고, 발급 일자를 확인한 뒤 [다음]을 누른다. 이제 계좌번호를 인증해야 한다. 은행명과 계좌번호를 입력하고 [1원 인증하기]를 누른다.



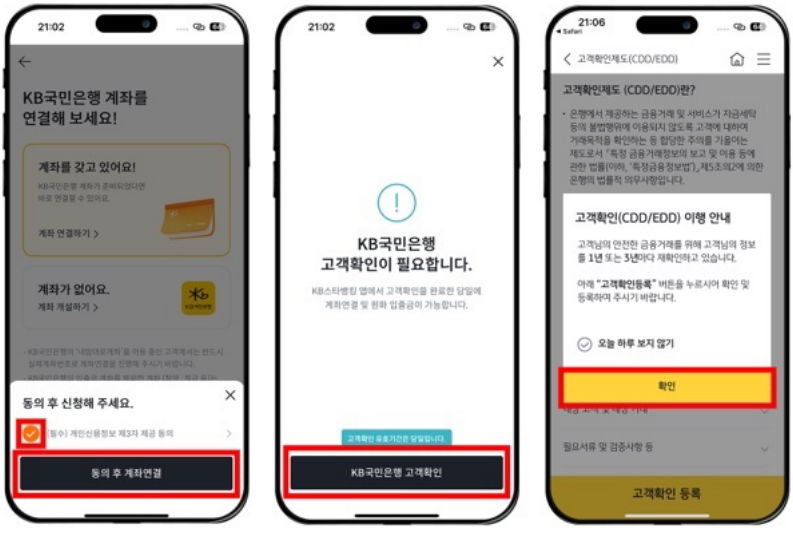
그러면 계좌에 1원이 입금되었을 것이다. 입금자 이름의 빗썸 뒤에 적힌 숫자 3자리를 입력한다. 계좌 인증까지 되었으면 매매 거래 자금 원천과 월평균 소득액을 적는다.



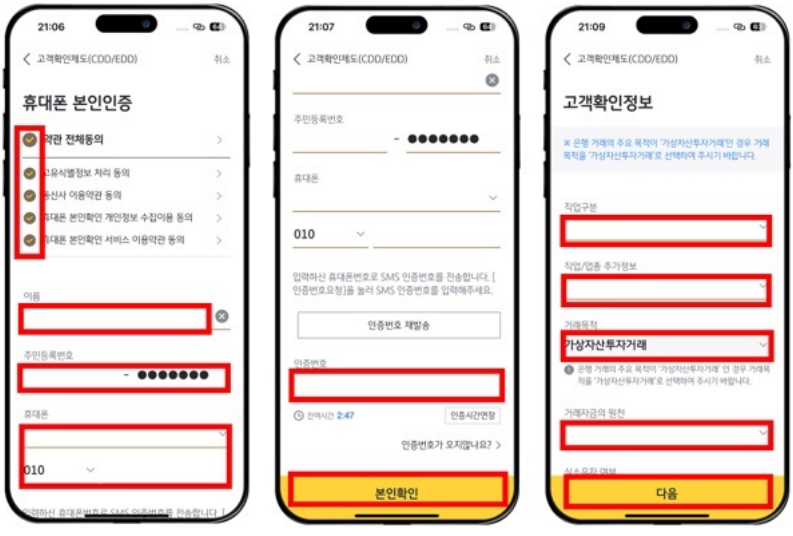
이제 국민은행 계좌를 연결해야 한다. 먼저 앱스토어 또는 구글 플레이스토어에서 'KB스타뱅킹' 앱을 다운로드한다. 다운로드하면 다시 빗썸으로 돌아와 KB스타뱅킹 앱을 설치했는지 물어보는 알림창에서 [이미 있어요]를 누른다.



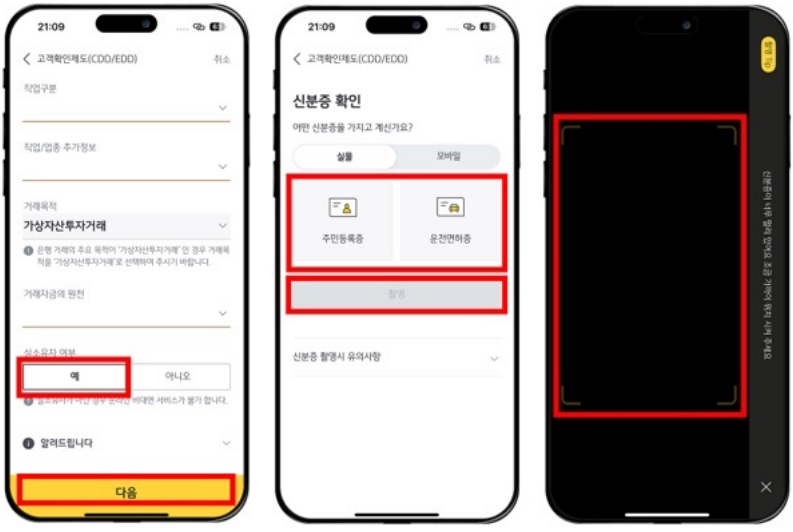
[동의 후 계좌연결] → [KB국민은행 고객확인]을 누르면 KB스타뱅킹 앱으로 넘어간다.



KB스타뱅킹 앱에서 약관에 동의하고, 이름, 주민번호, 휴대폰 번호를 적는다. 휴대폰 인증까지 마치면 [본인확인]을 누른다. 직업 정보까지 입력한다.

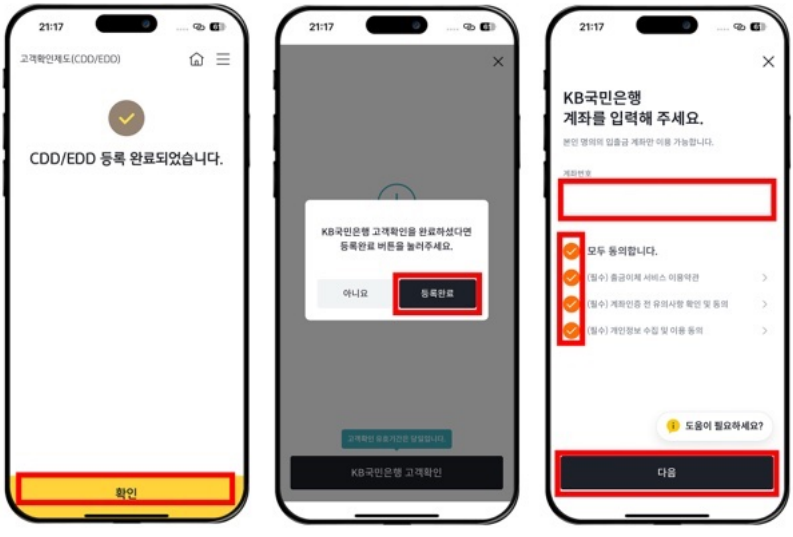


[다음]을 누르면 신분증을 촬영하는 단계로 넘어간다. 밝은 곳에서 신분증을 카메라로 촬영한다. 신분증에 불빛이 반사되지 않게 잘 찍는다.

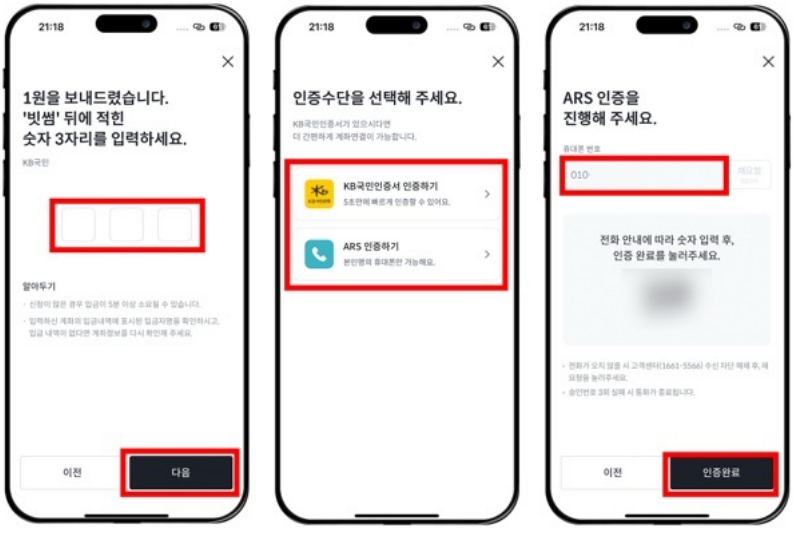


이름, 주민등록번호, 발급 일자가 모두 확인되었으면 [다음] → [다음]을 누른다. 이제 계좌 인증을 해야 한다. 국민은행 계좌를 선택하고 계좌 비밀번호를 입력한다. 입력했으면 [다음]을 누른다.

계좌 인증까지 되었으면 고객확인이 완료되었다. 다시 빗썸 앱으로 돌아와 [등록완료]를 누른다. 그다음에 연결할 국민은행 계좌를 입력하고, 약관에 동의한 뒤 [다음]을 누른다.



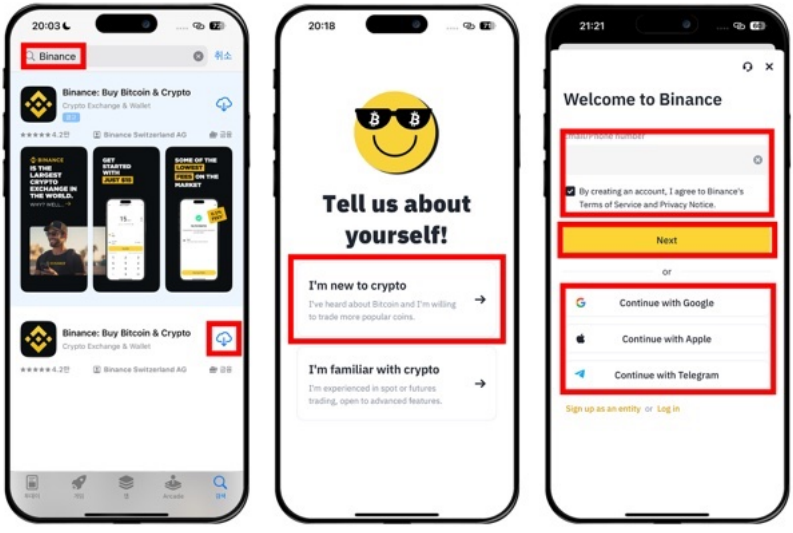
국민은행 계좌에 1원이 입금되었을 것이다. 입금자 이름의 빗썸 뒤에 적힌 숫자 3자리를 입력한다. 그다음에 KB국민인증서 또는 ARS 인증을 하면 되는데, 필자는 ARS 인증으로 진행했다. ARS 인증을 하면 전화가 오는데, 전화를 받고 빗썸 화면에 있던 숫자를 다이얼에서 입력하면 된다.



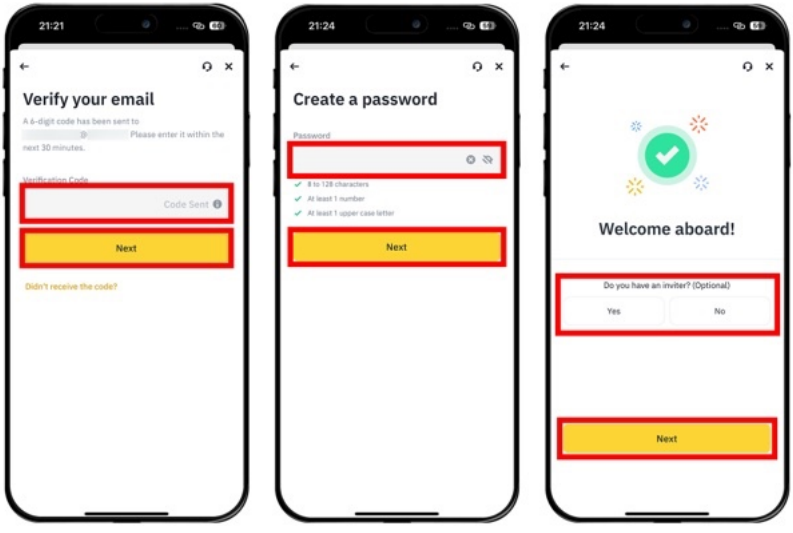
ARS 인증까지 하면 계좌 연결도 완료되었다. 빗썸 앱의 하단 탭에서 [더보기]를 누르면 고객확인이 완료되었다는 문구를 볼 수 있다.

바이낸스 가입 및 KYC 인증

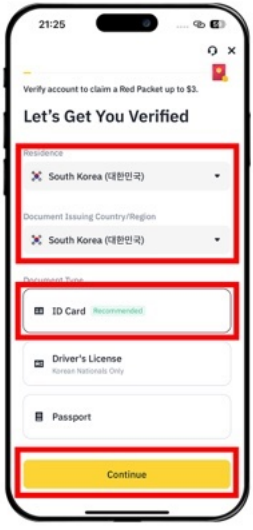
이제 해외 거래소인 바이낸스에 가입해 보자. 앱스토어 또는 구글 플레이스토어에서 'Binance'를 검색하고 앱을 다운로드한다. 처음 켠 화면에서 [I'm new to crypto]를 누른다. 그러면 가입하는 창이 뜨는데 이메일로 가입할 수도 있고, 구글이나 애플, 텔레그램 계정을 통해서 가입할 수도 있다. 필자는 이메일로 가입을 해보겠다.

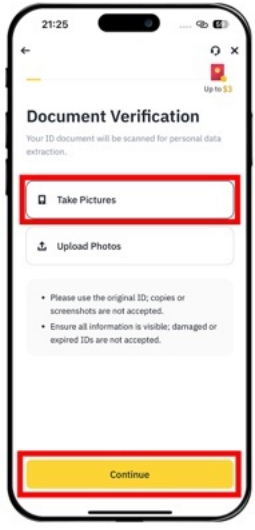


이메일 가입을 하면 입력한 이메일로 인증 번호가 온다. 인증 번호를 입력하고 [Next]를 누른다. 그다음에 비밀번호를 설정한다. 비밀번호는 8자리 이상의 문자열이어야 하고, 적어도 1개의 숫자와 1개의 대문자를 포함해야 한다. 그다음 화면에서는 추천인이 있는지 물어보는 창이 나오는데, 이는 레퍼럴을 입력하는 창이다. 필자는 바이낸스에서 자주 사고파는 것이 아니라 단지 중간 경로로 잠깐만 이용하는 것이므로 [Next]를 눌렀다.

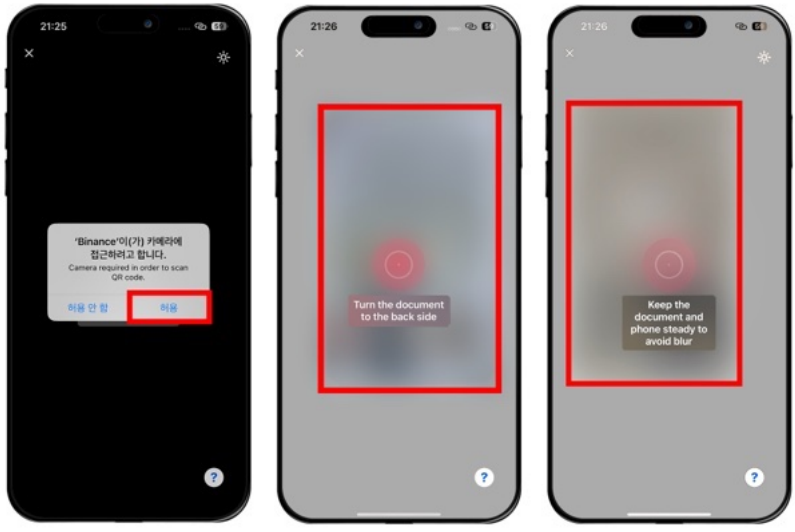


그러면 바로 KYC 인증하는 창으로 넘어간다. 국가를 입력하고, [ID Card]를 입력한다. 이는 주민등록증으로 인증하는 옵션이다. 그 아래 [Driver's License]는 운전면허증으로 인증하는 옵션이고, [Passport]는 여권으로 인증하는 옵션이다. [Continue] → [Take Pictures] → [Continue]를 선택한다.

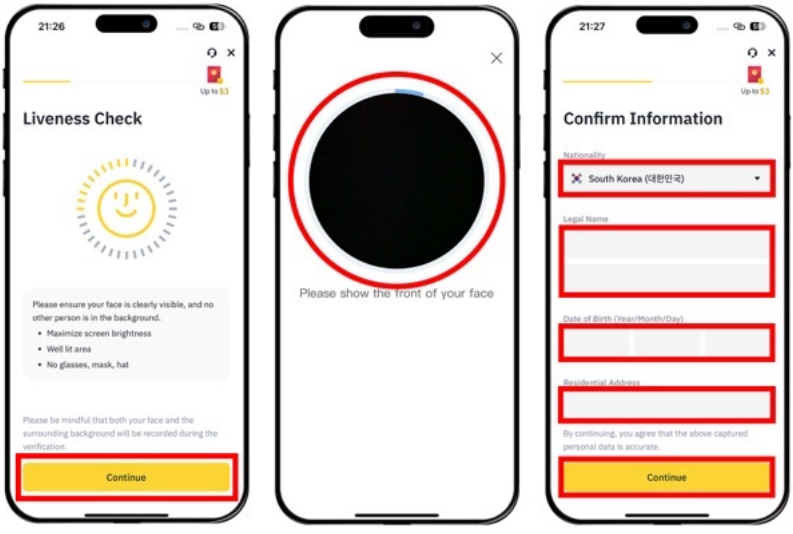




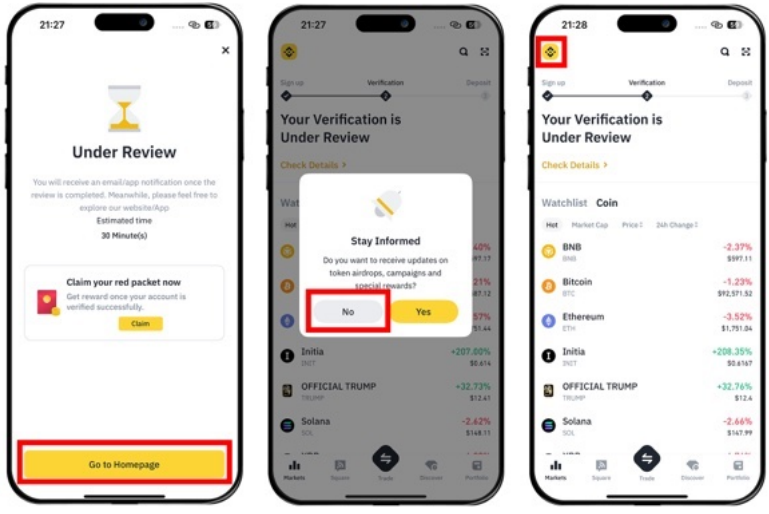
카메라 접근 권한을 허용하고 주민등록증을 촬영한다. 이때 앞면을 먼저 인식시키고 주민등록증을 뒤집어서 뒷면도 인식시켜야 한다.



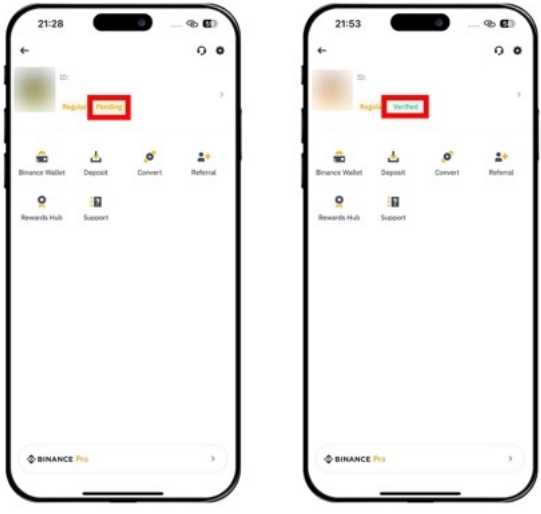
그다음에 얼굴 인증 창이 나온다. [Continue]를 누른 후 화면을 응시하고, 눈을 깜빡인 뒤, 고개를 좌우로, 위아래로도 흔들면 된다. 다음 창으로 넘어가면 신분증에 있던 이름이 자동으로 입력되었을 것이다. 여기서는 이름이 먼저고, 성이 그다음이다. 생년월일도 확인하고, 주소도 확인한다. 주소가 잘못되어 있으면 바르게 고친다. 다 됐으면 [Continue]를 누른다.



그러면 인증 신청도 완료되었다. [Go to Hompage]를 눌러 홈페이지로 간다. 하단 탭의 [Markets]을 누르고, 왼쪽 위의 바이낸스 로고를 누른다.



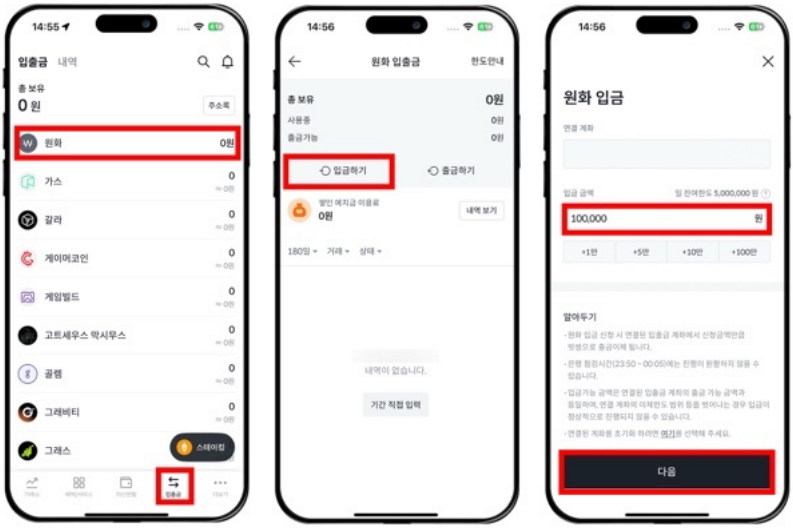
그러면 현재 인증 상태를 볼 수 있다. 처음에는 'Pending(보류)' 상태지만, 인증을 제대로 했다면 약 30분–하루 내로 'Verified(인증됨)'로 바뀐다.



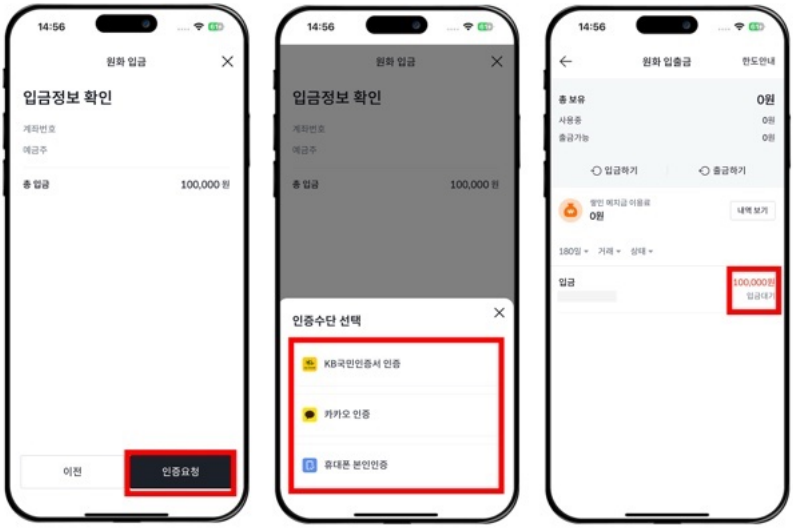
이로써 빗썸, 바이낸스 모두 가입이 완료되었다.

빗썸에서 원화 입금하고 테더 구매하기

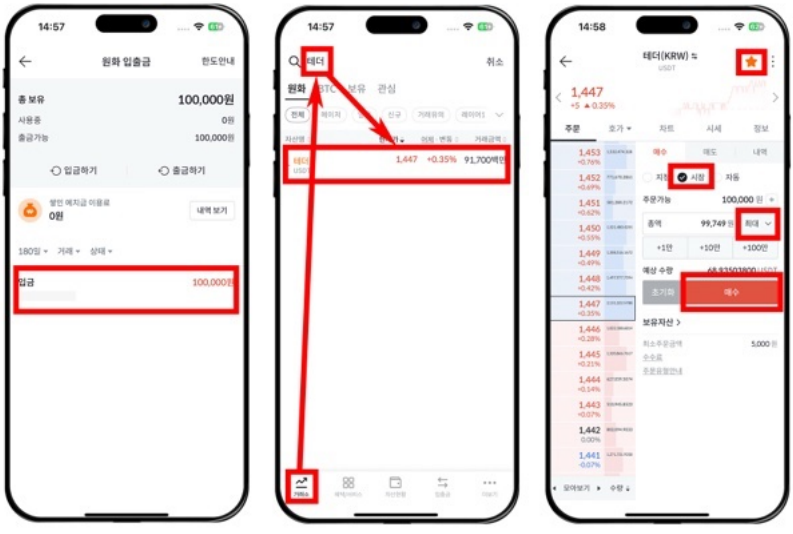
이제 빗썸에서 원화를 입금하고, 테더를 구매해 보자. 그 전에 원화가 빗썸과 연결된 국민은행 계좌에 들어있어야 한다. 먼저 하단 탭에서 [입출금]을 누른 후 [원화]를 누른다. [입금하기] → 금액 입력 → [다음]을 누른다.



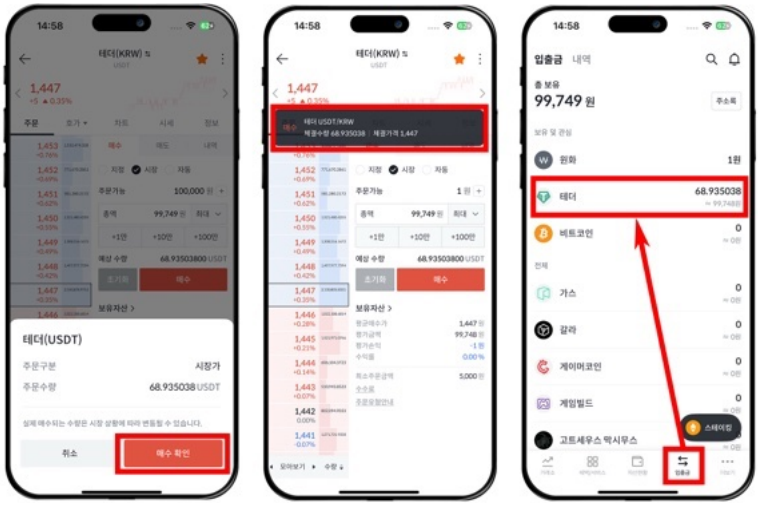
[인증 요청]을 누르고 원하는 방식의 인증을 마치면 '입금 대기' 상태가 된다.



잠시 기다리면 원화가 입금된다. 하단 탭의 [거래소]에서 '테더'를 검색하고 [테더]를 누른다. 호가창이 나오면 [시장]을 선택하고, [최대]를 선택한 후 [매수]를 누른다.

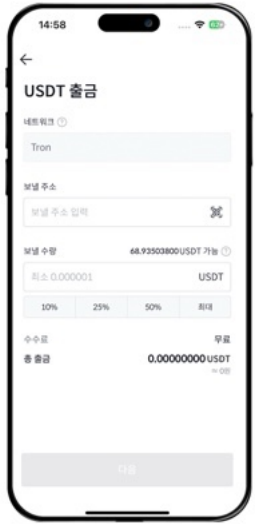


[매수 확인]을 누르면 상단에 체결되었다는 알림창이 뜬다. 이제 빗썸에서 바이낸스로 테더를 보낼 것이다. 하단 탭의 [입출금]으로 들어가 [테더]를 누른다.

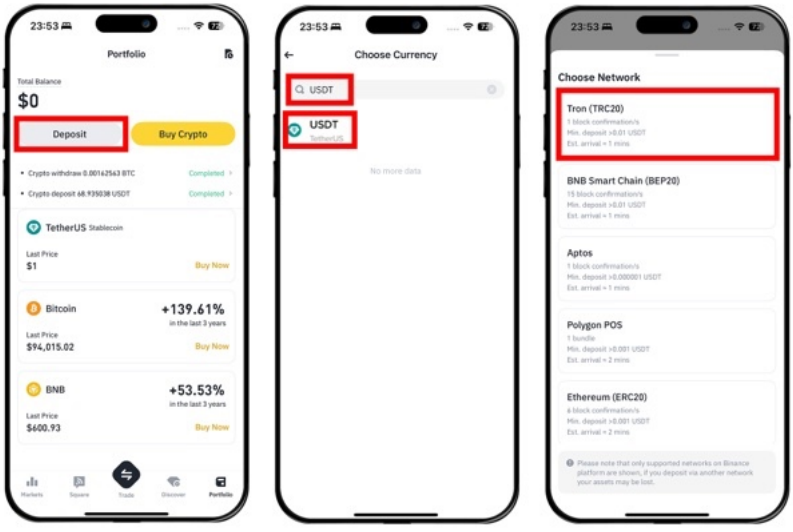


빗썸에서 바이낸스로 테더 보내기

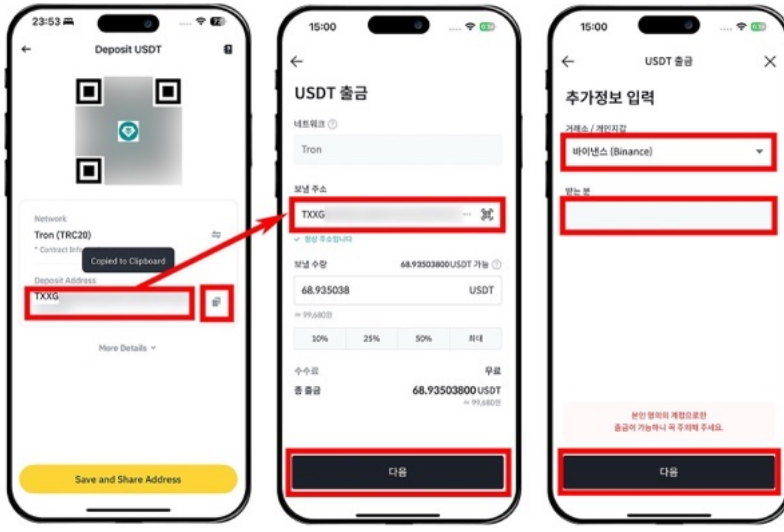
[테더]를 눌렀다면 오른쪽에 [출금하기] 버튼이 보일 것이다. 이 버튼을 누른다.



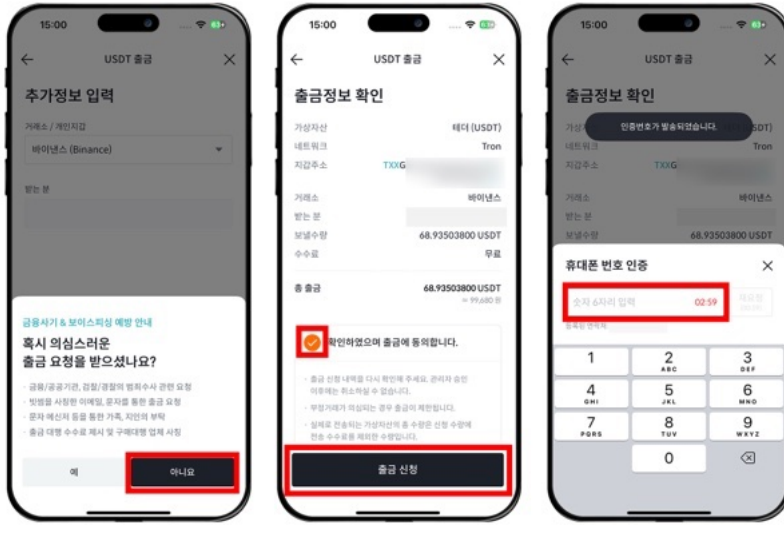
이제 바이낸스 앱을 켠다. 바이낸스 앱의 하단 탭에서 [Portfolio] → [Deposit (입금)]을 누른다(만약 이미 잔액이 있다면 화면이 조금 다른데 그때는 [Portfolio] → [Add Funds] → [Deposit Crypto]를 선택하면 된다). 검색창이 나오면 'USDT'를 검색하고 [USDT]를 선택한다. 그러고 네트워크를 선택하는 창에서 [Tron (TRC20)]을 선택한다.



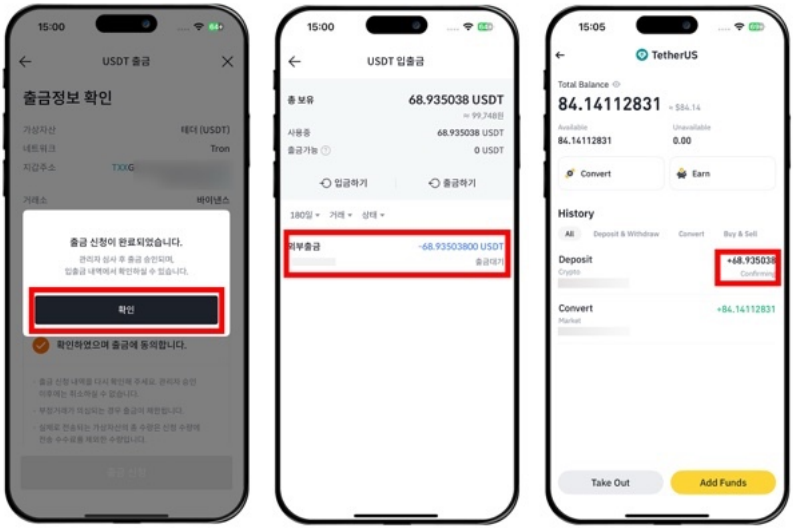
그러면 'Deposit Address (입금 주소)'가 나온다. 옆에 있는 문서 버튼을 눌러 입금 주소를 복사한다. 다시 빗썸 앱으로 가서 보낼 주소에 방금 복사한 테더 주소를 붙여넣기 하고 금액은 최대를 누른다. [다음]을 누르고, [바이낸스]를 선택한다. '받는 분'에 있는 이름이 바이낸스에 가입된 이름과 같아야 한다. 확인했으면 [다음]을 누른다.



보이스 피싱 알림 창이 나오면 [아니오]를 누르고, 약관에 동의한 뒤 [출금 신청]을 누른다. 휴대폰 인증 창이 뜰 것이다. 카카오톡 메시지나 문자로 온 인증 번호를 입력한다.



인증 번호까지 입력하면 출금 신청이 완료된다. 처음에는 출금 대기 상태로 나올 것이다. 바이낸스 화면에서는 입금 금액과 함께 'Confirming (확인 중)'이라는 문구가 뜰 것이다.



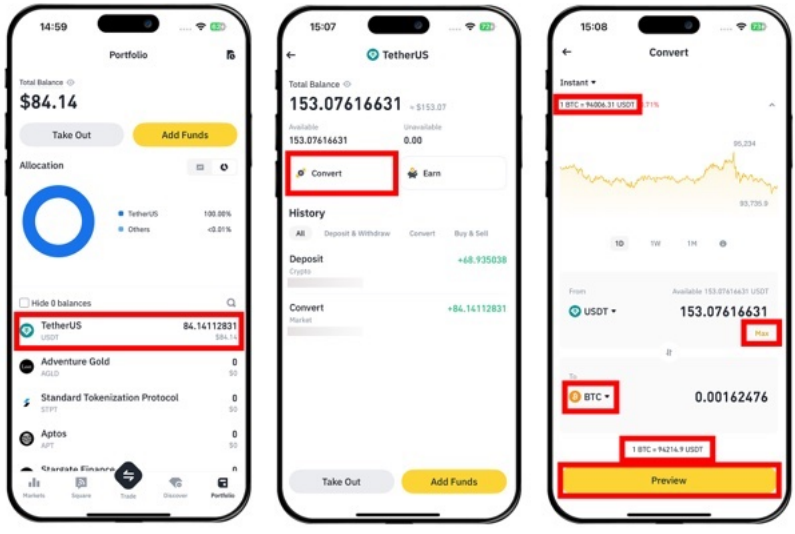
바이낸스에서 테더로 비트코인 구매하기 1: Convert 사용

테더가 바이낸스에 잘 입금되었다면 이제 테더를 비트코인으로 바꿔야 한다. 바이낸스에서 테더를 비트코인으로 바꾸는 방법에는 크게 두 가지가 있다. 하나는 Convert(변환)를 이용하는 것이고, 다른 하나는 마켓에서 시장가 매수를 하는 것이다.

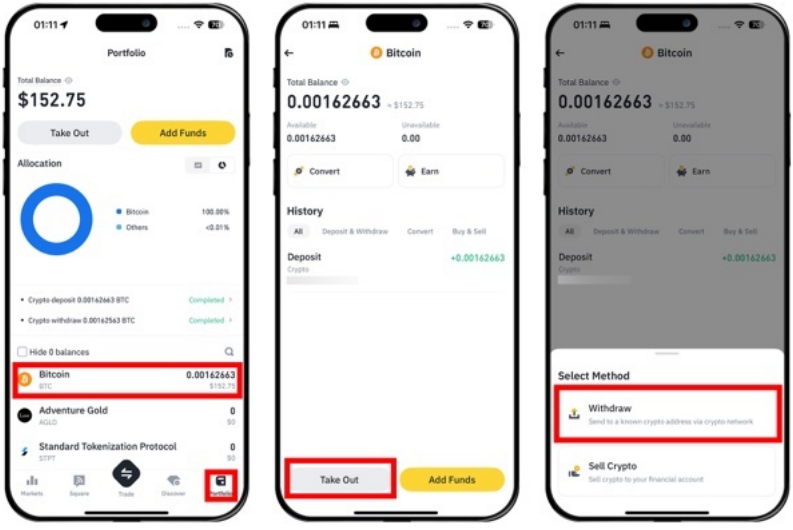
Convert는 좀 더 간편하지만, 시장가보다 0.2% 정도 더 높은 시세에 비트코인을 바꾸게 된다. 시장가는 더 저렴하게 바꿀 수 있지만 번거롭다. 두 가지 방법 모두 알아보자. 먼저 Convert를 이용해 테더를 비트코인으로 바꾸는 방법이다.

바이낸스 하단 탭의 [Portfolio] → [TetherUS] 선택 → [Convert]를 누른다. 왼쪽 위에 현재 비트코인 시세(사진에서 94006.31)가 나오고, 하단에 Convert 시세(94214.9)가 나오는 것을 볼 수 있다. 사진상에서는 Convert 시세가 0.22% 정도 좀 더 비싼 것을 알 수 있다. 간편한 대신 0.2% 정도가 더 비싼 것이다.

먼저 'To'에서 [BTC(비트코인)]를 선택하고, 금액은 [Max]를 누른다. 그다음에 [Preview(미리보기)]를 누른다. [Confirm(확인)]까지 누르면 변환이 완료된다.

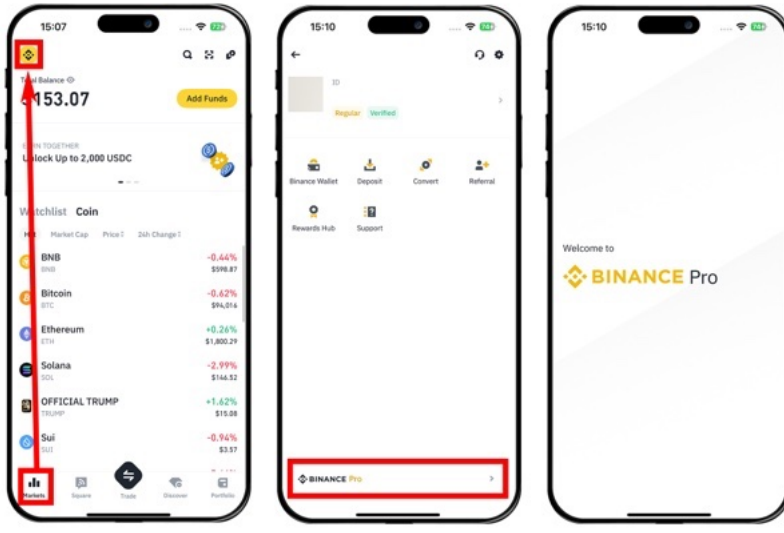


이제 하단 탭의 [Portfolio]에서 [Bitcoin]을 선택하고 [Take Out] → [Withdraw]를 누른다. 여기까지 했다면 바로 '바이낸스에서 온-체인을 통해 바로 개인 지갑으로 전송하기' 혹은 '바이낸스에서 라이트닝 네트워크와 볼츠 스와프 서비스를 통해 개인 지갑으로 전송하기' 절로 넘어가면 된다.

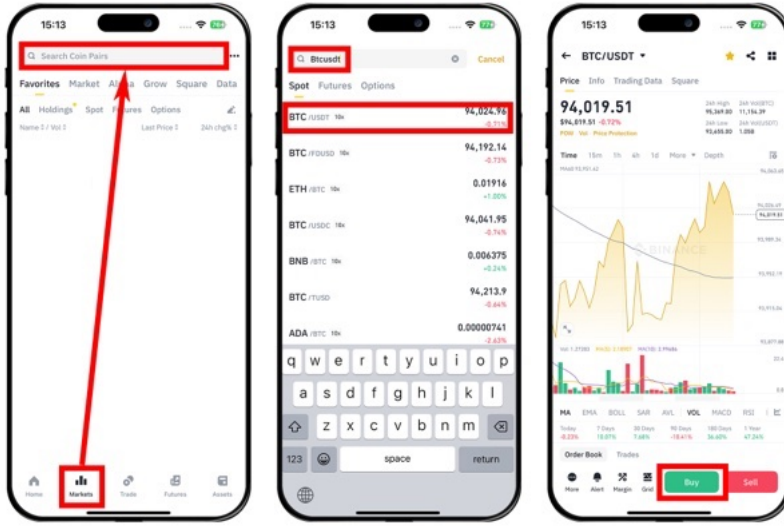


바이낸스에서 테더로 비트코인 구매하기 2: 시장가 매수

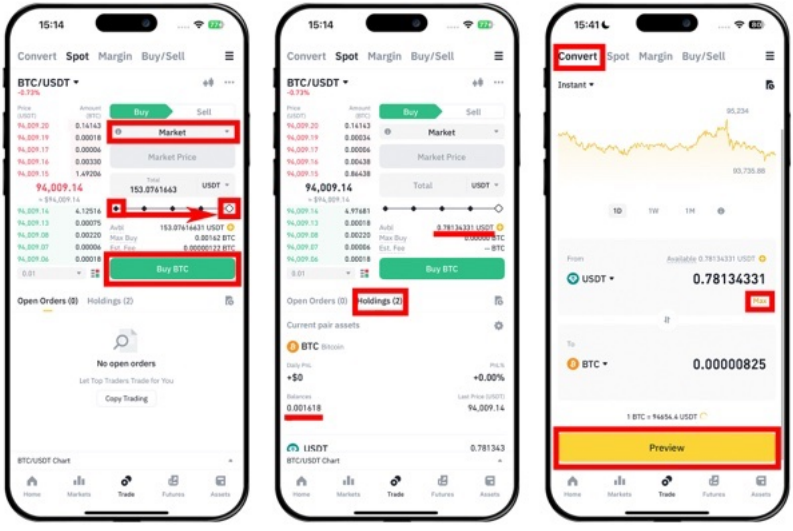
바이낸스에서 테더로 비트코인을 구매하는 다른 방법에는 마켓에서 시장가로 매수하는 방법이 있다. 시장가로 매수하려면 먼저 바이낸스 버전을 Lite 버전에서 Pro 버전으로 바꿔야 한다. 하단 탭 → [Markets] → 왼쪽 위 바이낸스 로고 버튼 → [BINANCE Pro]를 누른다.



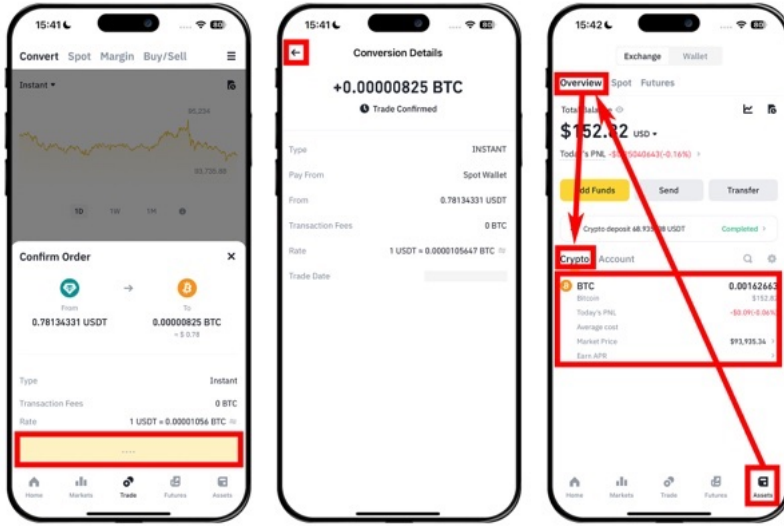
하단 탭의 [Markets]에서 'BTCUSDT' 페어를 검색하고, [BTC/USDT]를 누른다. 그다음 [Buy(구매)]를 누른다.



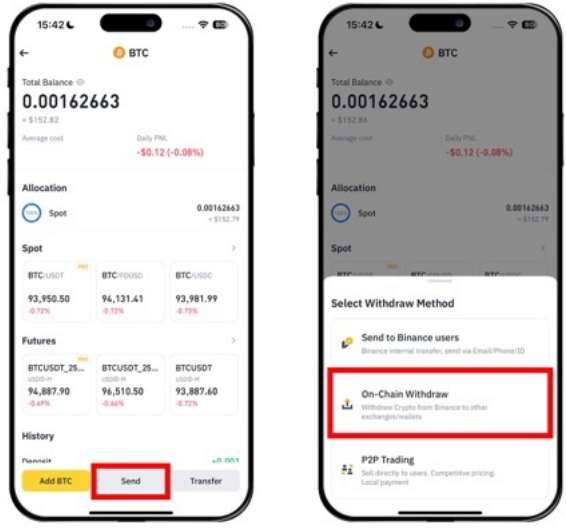
'Limit(지정가)'를 'Market(시장가)'으로 바꾸고, 슬라이드를 오른쪽으로 밀어서 금액이 100%가 되도록 한다. 이제 [Buy BTC]를 누르면 구매가 완료된다. 그런데 아직 테더가 조금 남은 것을 볼 수 있다. 남은 테더는 Convert를 이용해 바꿔야 한다. 왼쪽 위 [Convert]를 누른다. 테더 금액 아래에 있는 [Max]를 누르고 [Preview]를 누른다.



[Confirm(확인)]을 누르면 나머지 테더까지 깔끔하게 비트코인으로 바뀐다. 뒤로 가기 버튼을 누르고, 하단 탭 [Assets]에서 [Overview] → [Crypto]에서 [BTC]를 누른다.

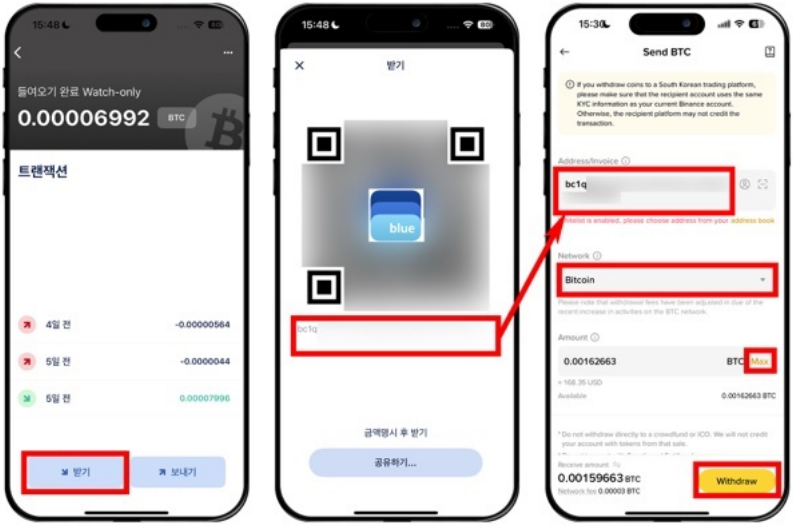


아래에서 [Send(보내기)] → [On-Chain Withdraw(온-체인 출금)]를 선택한다.

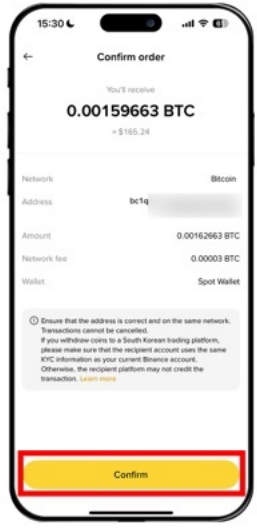


바이낸스에서 온-체인을 통해 바로 개인 지갑으로 전송하기

이제 블루월렛, 넌척 혹은 코코넛 월렛에 들어가 [받기]를 누르고 나오는 주소를 눌러 복사한다. 그 주소를 바이낸스의 'Address/Invoice'에 입력한다. 그 밑에 'Network'는 [Bitcoin]을 선택한다. 이걸 선택해야 온-체인으로 전송하는 것이다. 그 밑에 'Amount' 옆의 [Max]를 눌러 모든 금액을 전송한다. 다 되었으면 [Withdraw]를 누른다.



다음 화면에서 [Confirm]을 누르면 온-체인으로 전송된다. 거래가 블록에 담겨 채굴되면 개인 지갑으로 비트코인이 잘 전송될 것이다.



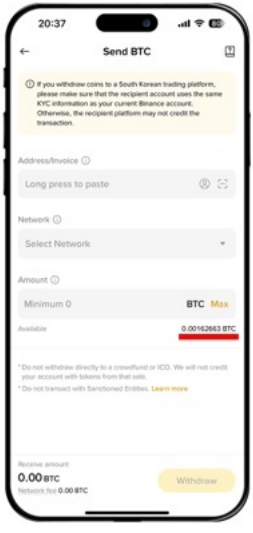
바이낸스에서 라이트닝 네트워크와 볼츠 스와프 서비스를 통해 개인 지갑으로 전송하기

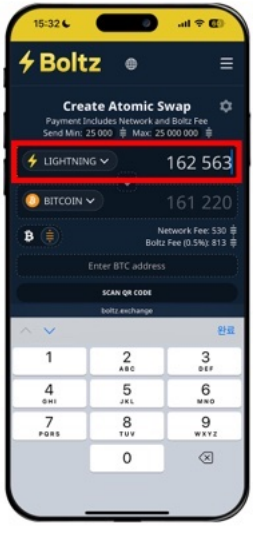
이번에는 온-체인으로 바로 전송하지 않고 라이트닝 네트워크와 볼츠 스와프 서비스를 이용해 개인 지갑으로 전송하는 방법을 알아보자. 참고로 이 방법을 이용할 때 최소 출금 금액은 약 25,100 sats이며 1회 최대 출금 금액은 99만 sats이다. 볼츠의 출금 금액이 25,000 sats 이상 2,500만 sats 이하이고, 바이낸스의 라이트닝 네트워크를 이용한 최대 출금 금액 한도가 약 99만 sats이기 때문이다.

바이낸스 출금 창에서 'Avalable (출금 가능 금액)' 옆에 있는 내가 가진 비트코인 금액을 잘 기억해 놓자. 사진상에서는 162,663 sats가 있는 것을 확인할 수 있다. 바이낸스에서 라이트닝 네트워크를 이용한 출금 수수료는 100 sats인데, 그러면 이를 제외한 출금 금액은 162,563 sats가 되리라는 것을 알 수 있다.

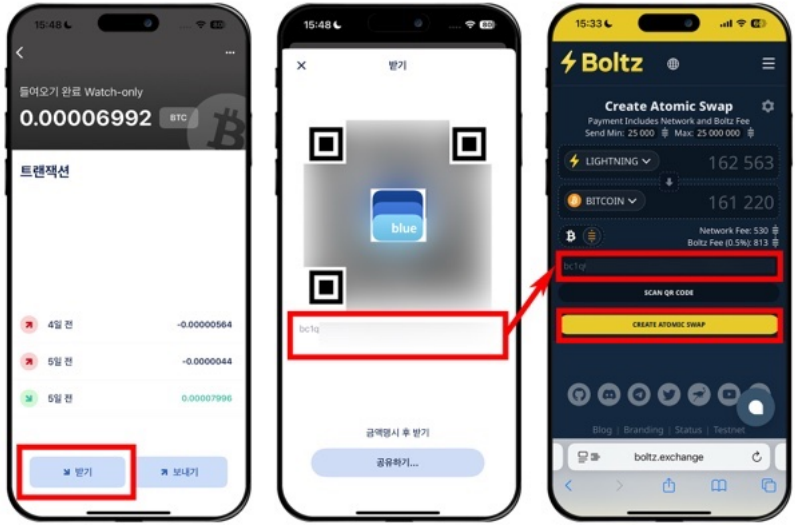
볼츠 웹사이트에 들어가 'LIGHTNING' 옆에 바이낸스에서 수수료 100 sats를 제외한 금액을 입력한다. 볼츠 웹사이트 주소는 다음과 같다.

https://boltz.exchange/

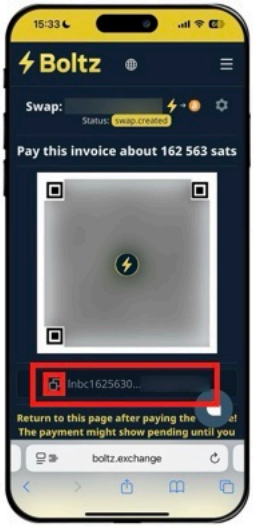


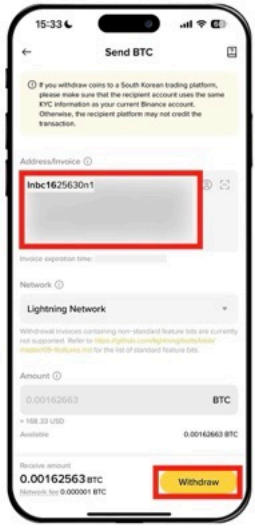


이제 블루월렛, 넌척 혹은 코코넛 월렛에 들어가 [받기]를 누르고 나오는 주소를 눌러 복사한다. 그 주소를 볼츠에서 금액 밑에 'Enter BTC address'에 입력한다. 다 되었으면 [CREATE ATOMIC SWAP]을 누른다.

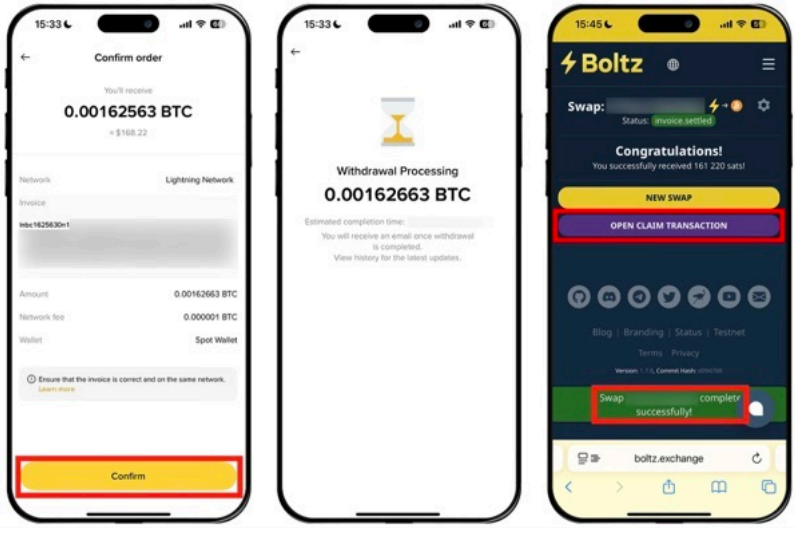


그러면 QR 코드와 함께 'lnbc'로 시작하는 어떤 텍스트가 나온다. 이를 '인보이스'라고 한다. 왼쪽에 있는 문서 모양의 복사 버튼을 누르고, 바이낸스 창의 'Address/Invoice'에 입력한다. 그러면 자동으로 'Network'와 'Amount'가 선택된다. [Withdraw]를 누른다.





다음 화면에서 [Confirm]을 누르면 라이트닝/온-체인 스와프가 완료된다. [OPEN CLAIM TRANSACTION]을 누르면 멤풀 웹사이트에서 해당 거래의 상태를 확인할 수 있다. 거래가 블록에 담겨 채굴되면 개인 지갑으로 비트코인이 잘 전송될 것이다.



이로써 국내 거래소에서 해외 거래소를 거쳐 개인 지갑으로 비트코인을 보내는 방법을 알아보았다.

| 지갑에서 거래소로 비트코인 옮겨 원화 출금하기

비트코인을 모으다 보면 종종 비트코인을 원화로 환전해서 써야 할 일이 있다. 비트코인을 원화로 환전하는 방법은 크게 두 가지가 있다.

1. 개인 간 거래(P2P)
2. 거래소(빗썸, 업비트 등)로 옮겨서 환전

개인 간 거래가 훨씬 간편하지만, 구매자가 없는 경우 거래소를 통해 비트코인을 원화를 환전할 일도 있을 것이다. 따라서 이번에는 비트코인을 지갑에서 거래소로 옮겨서 환전하는 방법에 대해 알아보자.

개인 지갑에 있는 비트코인을 원화로 환전하려면 해외 거래소를 거쳐 한국 거래소로 입금해야 한다. 이는 앞서 언급했던 트래블룰 때문이다. 트래블룰 때문에 한국 거래소에 입금하기 위해서는 신원 인증이 되어있고 신원이 일치하는 거래소에서만 입금할 수 있다.

전송 경로

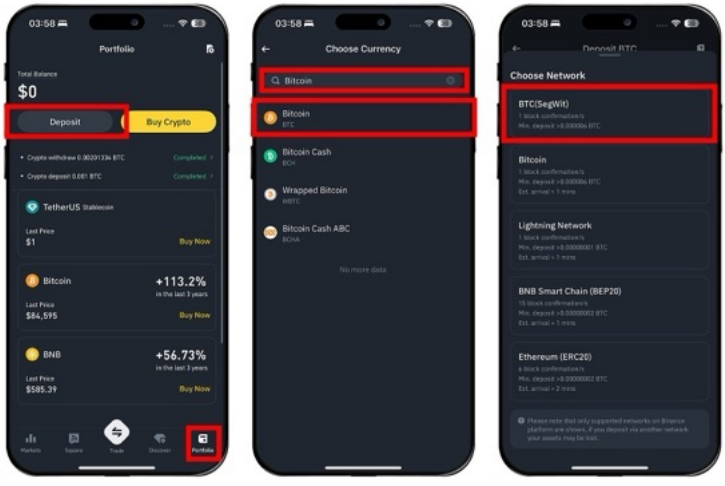
해외 거래소를 거쳐 원화로 환전하는 방법은 다음과 같다.

> 개인 지갑 → 해외 거래소 → 테더(USDT)로 환전 → 국내 거래소 → 원화로 환전 후 계좌로 출금

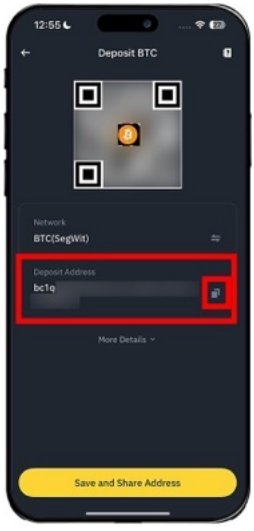
중간에 테더를 사용하는 것을 알 수 있다. 이는 현재 한국 거래소들이 라이트닝 네트워크를 지원하고 있지 않기 때문이다. 한국 거래소들도 라이트닝 네트워크를 지원하기 시작하면 테더는 사용하지 않아도 될지도 모른다.

개인 지갑에서 해외 거래소로 전송

개인 지갑에서 바이낸스로 전송하는 방법을 알아보자. [Portfolio] → [Deposit] → 'Bitcoin'을 검색해서 누르고, [BTC(SegWit)]를 누른다 (만약 이미 잔액이 있다면 화면이 조금 다른데 그때는 [Portfolio] → [Add Funds] → [Deposit Crypto]를 선택하면 된다).



'Deposit Address (입금 주소)' 옆에 있는 종이 모양을 누르면 이 주소가 복사된다. 워치-온리 지갑에서 이 주소로 비트코인을 보내면 된다. 블록이 채굴되어 컨펌되고 나면 바이낸스에 비트코인이 입금될 것이다.

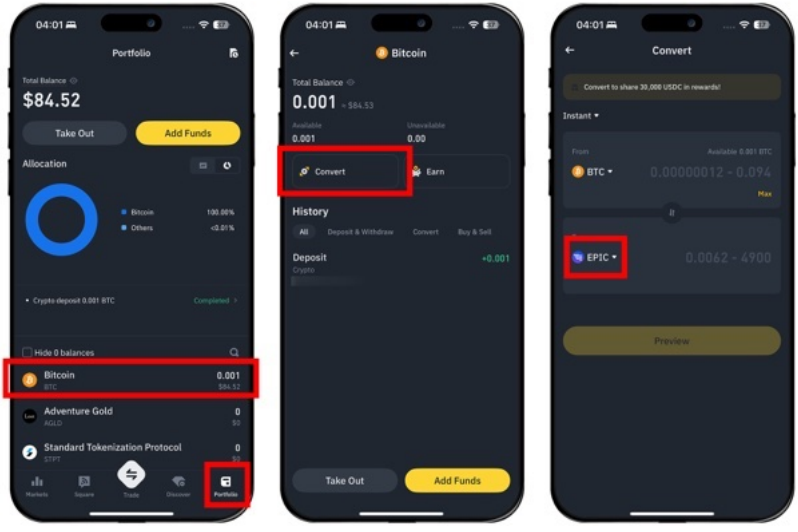


해외 거래소에서 국내 거래소로 전송

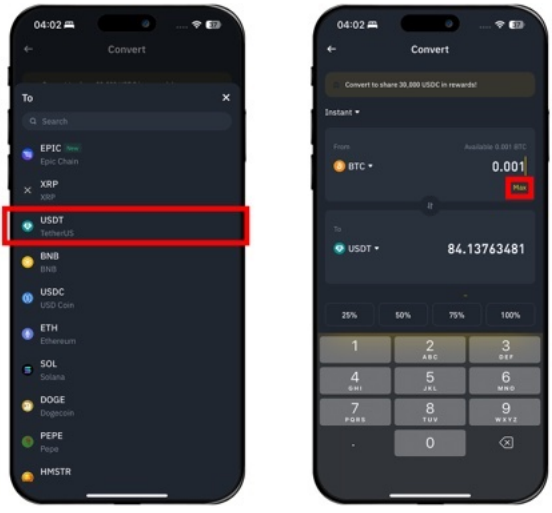
이제 앞에서 말한 대로 해외 거래소에서 비트코인을 테더로 변환한 뒤 국내 거래소로 전송할 것이다. 비트코인을 테더로 변환하는 방법부터 알아보자.

먼저 [Portfolio]에서 [Bitcoin]을 누른 후 [Convert]를 누른다. 비트코인을 테더로 변환할 때는 'Convert'로 변환하거나 'Markets(시장)'에서 BTC/USDT 페어에서 지정가/시장가 매도로 바꿀 수 있다. Convert는 제공된 환율로 체결되고 간편하다는 장점이 있다. 지정가/시장가 매도는 상황에 따라 Convert보다 이익일 수도 있다.

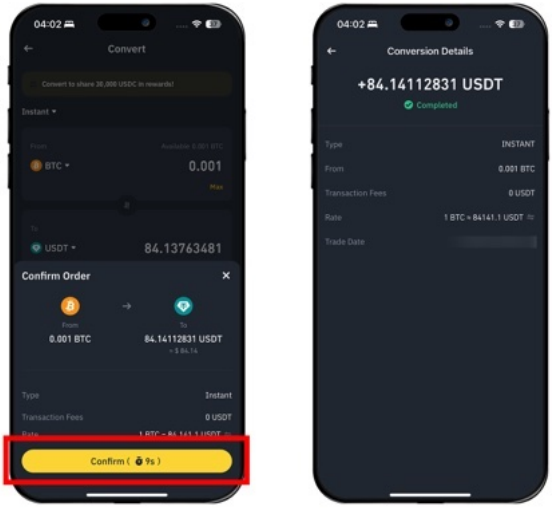
BTC 아래에 뜨는 심볼(사진상에서 EPIC)을 누른다. 이것을 테더(USDT)로 바꿔주어야 한다.



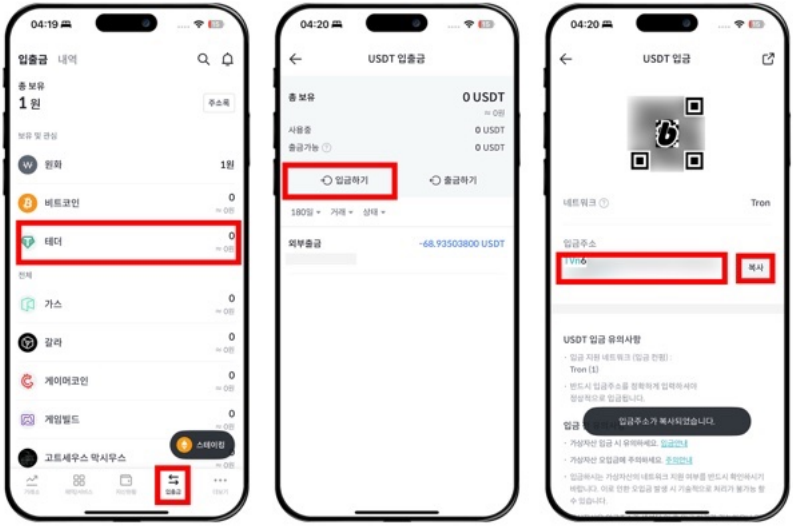
[USDT]를 찾아서 누른다. BTC 아래에 작게 노란 글자로 되어있는 [Max]를 누르면 바꿀 수 있는 모든 비트코인이 자동으로 입력된다.



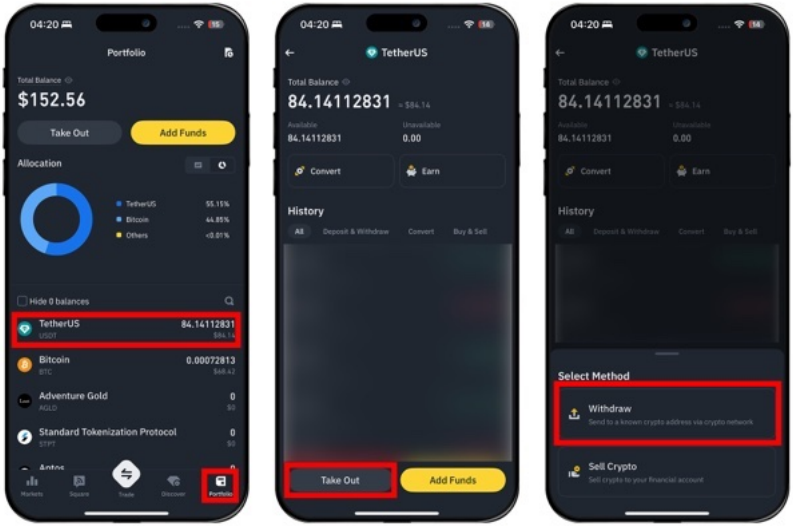
[Preview]를 누르고 [Confirm]을 누르면 테더(USDT)로 변환이 완료된다.



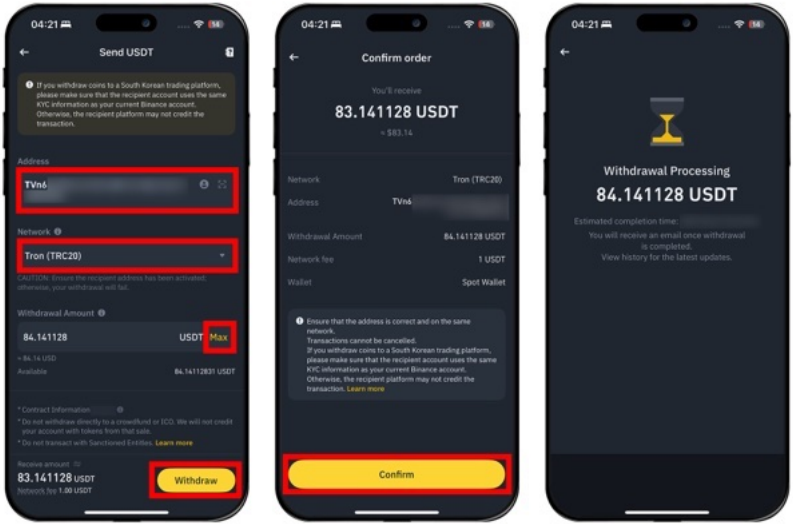
이제 국내 거래소로 테더를 전송해 보자. 빗썸에서 진행하는 방법을 알아보겠다. 앱에 로그인한 뒤 [입출금] 탭으로 들어간다. [테더]를 누르고 [입금하기]를 누른다. 그러면 테더 입금 주소가 나온다. 옆에 있는 [복사]를 눌러 이 주소를 복사하자.



다시 바이낸스로 들어가 아래 [Portfolio] 탭에서 [TetherUS(테더)]를 누른다. [Take Out]을 누르고, [Withdraw]를 누른다.

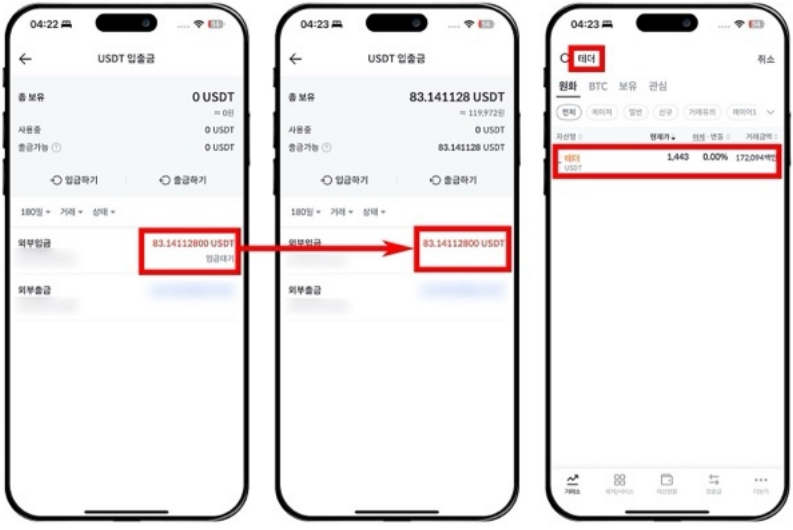


'Address'에는 국내 거래소에서 복사했던 주소를 붙여넣는다. 'Network'는 [Tron (TRC20)]을 선택한다. 노란색 글자로 되어있는 [Max]를 누르면 테더 전체 금액이 자동으로 입력된다. [Withdraw]를 누르고, [Confirm]을 누르면 된다.

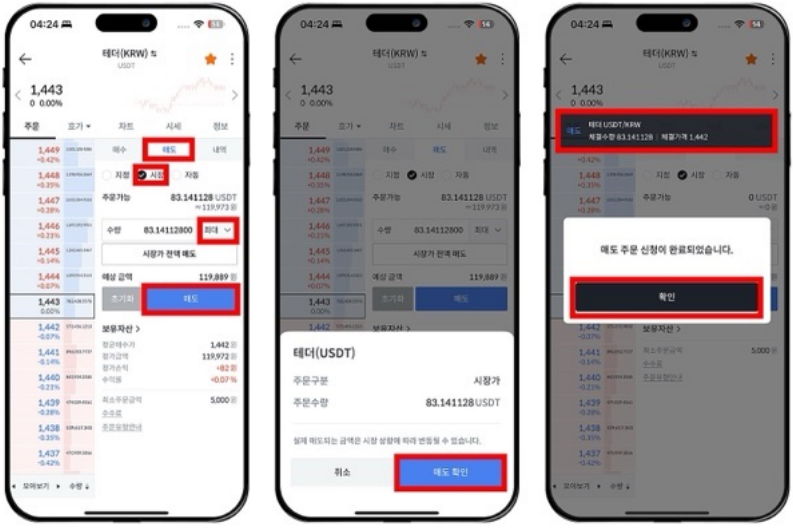


국내 거래소에서 원화 환전 후 은행 계좌로 출금

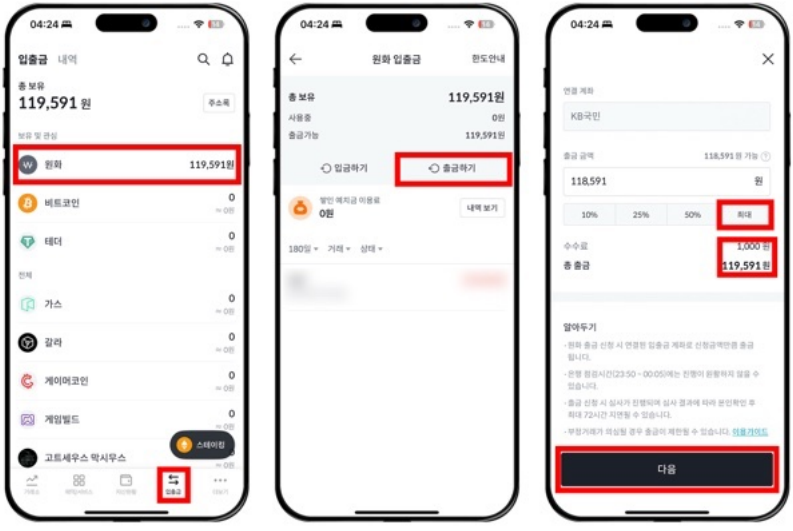
빗썸의 [입출금] → [테더] 화면을 보면 입금 대기 중이었다가 입금이 완료되는 것을 알 수 있다(새로고침이 안 되면 뒤로 나갔다가 다시 들어와 보자). 이제 빗썸의 아래 탭 [거래소]에서 '테더'를 검색하고 [테더]를 선택한다.



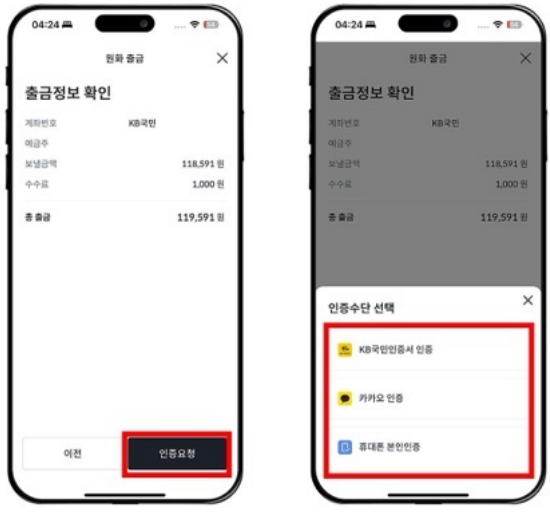
먼저 [매도] 탭을 누른다. [시장]을 체크하고 금액은 [최대]를 선택한다. 아래에 있는 [매도]를 누르고 [매도 확인]을 누르면 원화 환전이 완료된다.



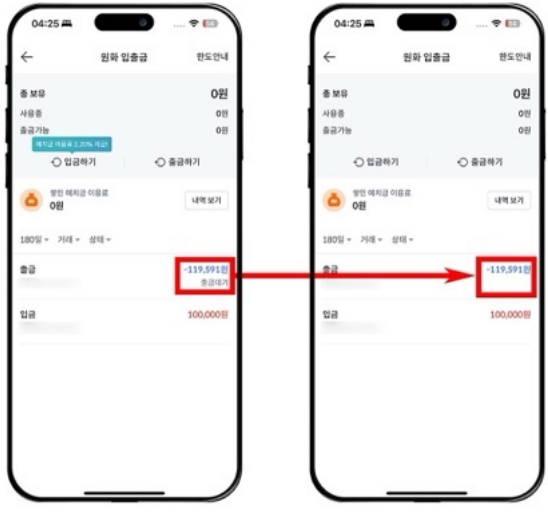
이제 원화를 은행 계좌로 출금해 보자. 아래 탭의 [입출금]에서 [원화]를 누른다. [출금하기]를 누르고 금액 입력창 아래에 있는 [최대]를 누른다. 그러면 수수료를 제외하고 출금할 수 있는 최대 금액이 자동으로 입력된다. [다음]을 누른다.



[인증요청]을 누르고 인증을 완료한다.



잠시 기다리면 출금 대기 중이던 상태가 출금 완료 상태가 되는 것을 알 수 있다.



이로써 거래소에서 원화로 환전하는 방법까지 모두 알아보았다.