Market Talks
교육 센터

블록체인 · 초급 · 13강 중 9강

시드 문구와 백업

지갑 전체를 다시 만들어 낼 수 있는 12개 또는 24개의 단어, 안전하게 보관하는 법, 그리고 그것을 노리는 사람들

읽는 시간 6분　　퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 9강

시드 문구와 백업

한 문장 요약

시드 문구는 지갑의 모든 개인 키를 다시 만들어 낼 수 있는 평범한 단어 12개 또는 24개의 목록입니다. 잘 보관하면 기기를 잃어버리거나 고장 나도 복구할 수 있습니다. 유출되면 누구든 모든 것을 가져갈 수 있고, 되돌릴 방법은 없습니다.

모든 키를 위한 하나의 백업

8강에서 지갑은 결제마다 새 주소를 만들고, 각 주소는 저마다의 개인 키에서 나온다는 것을 보았습니다. 수십 개의 키를 하나하나 백업하는 것은 악몽일 것입니다. 요즘 지갑들은 모든 키를 **시드**(seed, 씨앗)라고 부르는 하나의 시작 숫자에서 만들어 내는 방식으로 이 문제를 해결합니다.

시드는 지갑을 처음 설정할 때 단 한 번, 12개 또는 24개의 단어 목록으로 보여집니다. 이것이 바로 **시드 문구**이며, 복구 문구라고도 부릅니다. 같은 단어를 거의 모든 최신 지갑 앱에 입력하면 정확히 같은 키를 같은 순서로 다시 만들어 내고 같은 코인을 찾아냅니다. 휴대폰이나 하드웨어 기기는 잃어버리거나 도난당하거나 고장 날 수 있습니다. 그래도 단어만 가지고 있다면 비트코인은 사라지지 않습니다.

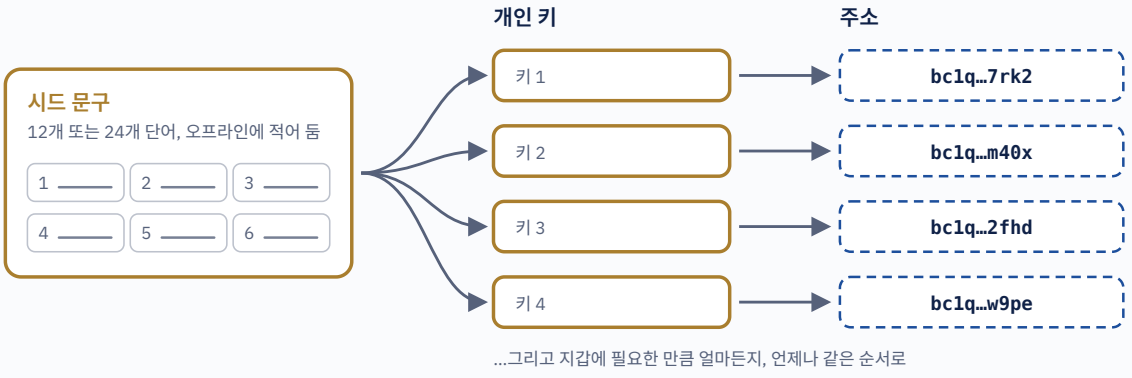


그림 1. 시드 문구 하나가 지갑의 모든 개인 키를 만들고, 각 키는 주소 하나를 만듭니다. 호환되는 어떤 지갑에서든 문구를 복구하면 같은 키와 코인이 돌아옵니다.

비유: 사진 필름 원판

필름 카메라 시절에는 어떤 인화 사진보다도 필름 원판(네거티브)이 더 중요했습니다. 사진을 잃어버려도 원판만 있으면 어느 사진관에서든 원하는 만큼 다시 뽑을 수 있었습니다. 시드 문구는 지갑의 원판입니다. 휴대폰의 앱은 인화된 사진 한 장일 뿐입니다. 하지만 원판을 손에 넣은 사람이라면 누구든 자기 사진을 뽑을 수 있습니다.

왜 단어이고, 왜 하필 이 단어들인가

사실 시드는 아주 큰 무작위 숫자일 뿐입니다. 이를 숫자와 글자 64자로 받아 적다 보면 실수하기 쉬우므로, 널리 쓰이는 표준이 이 숫자를 간단한 영어 단어 2,048개로 이루어진 고정된 목록의 단어들로 바꿉니다. 단어 하나하나가 숫자의 한 부분을 나타냅니다.

이 목록은 신중하게 만들어졌습니다. 영어 버전에서는 첫 네 글자가 같은 단어가 하나도 없어서, 끝부분이 번져도 알아볼 수 있습니다. 마지막 단어는 내장된 검사 역할도 합니다. 단어 하나를 잘못 옮겨 적으면 지갑은 보통 빈 지갑을 조용히 여는 대신 문구가 유효하지 않다고 알려 줍니다.

단어는 내가 아니라 지갑이 무작위로 고릅니다. 이것이 핵심입니다. 12단어 문구는 약 3.4 × 10의 38제곱, 즉 39자리 숫자만큼의 조합 중 하나가 될 수 있습니다. 직접 지어낸 문장이나 노래 가사는 흔한 문구 수백만 개를 시험하도록 만들어진 프로그램에 금방 맞혀집니다.

일부 지갑은 passphrase라고 부르는 선택적인 추가 비밀번호도 설정할 수 있게 해 줍니다. 이를 설정하면 12개나 24개의 단어만으로는 지갑을 열 수 없습니다. 보호는 강해지지만, 이 비밀번호를 잊어버리면 단어도 소용이 없습니다.

보관: 오프라인으로, 튼튼하게, 찾을 수 있게

좋은 백업은 세 가지 위협을 견뎌야 합니다. 도둑, 화재나 물 같은 사고, 그리고 몇 년 뒤의 내 기억력입니다. 흔한 방법들을 비교하면 다음과 같습니다.

보관 장소	강한 점	약한 점
종이에 적어 집에 보관	인터넷에 닿지 않으니 해커에 강함	불, 물, 그리고 발견하는 누구에게나
금속판에 새김	해커, 불, 물에 강함	잘 숨기지 않으면 발견하는 누구에게나
은행 대여 금고 등 다른 곳에 두 번째 사본	한 번의 재난으로 유일한 사본을 잃는 것	사본이 많을수록 유출될 곳도 많아짐
사진, 스크린샷, 메모 앱, 이메일, 클라우드	종이가 더 잘하지 못하는 것은 없음	계정 해킹, 동기화된 백업, 이미지를 훑는 악성 코드

무엇을 고르든 단어를 순서대로 적고, 번호를 매기고, 하나하나 화면과 대조하세요. 그다음 복구 훈련을 하세요. 지갑에 소액만 둔 상태에서 지갑을 지우거나 다른 기기를 이용해 단어를 다시 입력하고, 같은 주소가 나타나는지 확인합니다. 지금 실수를 발견하면 비용이 적게 듭니다. 비상시에 발견하면 그렇지 않습니다.

정상적인 누구도 결코 요구하지 않는다

시드 문구는 모든 것을 열 수 있기 때문에 암호화폐 사기의 주요 표적입니다. 수법은 다양하지만 요구는 언제나 같습니다. 단어를 어딘가에 입력하라는 것입니다. 메시지로 오는 고객지원 담당자일 수도 있고, 지갑을 '동기화'하거나 '인증'해야 한다는 팝업일 수도 있고, 앱 스토어의 가짜 지갑 앱이나 무료 에어드롭을 약속하는 웹사이트일 수도 있습니다.

규칙은 단순하고 예외가 없습니다. 시드 문구는 오직 내 지갑을 직접 복구할 때, 내 지갑에만 입력합니다. 지갑 회사도, 거래소도, 개발자도, 채널 관리자도 그것이 필요한 경우는 절대 없습니다.

실제 사례: 가짜 '교체용' 지갑

2020년 하드웨어 지갑 제조사 Ledger의 데이터베이스가 침해되었고, 12월에는 고객 약 27만 2천 명의 이름, 집 주소, 전화번호가 인터넷에 공개되었습니다. 몇 달 뒤 일부 고객은 진짜 Ledger 포장처럼 보이는 소포를 받았는데, 기기가 안전하지 않으니 '교체용' 기기를 동봉한다는 편지가 들어 있었습니다. 안내문은 복구 문구를 입력하라고 했습니다. 기기는 조작되어 있었고, 단어는 곧장 도둑에게 넘어갔습니다.

트레이더에게 왜 중요한가

- **트레이딩 단체방은 사기꾼의 사냥터입니다.** 사기꾼들은 활발한 암호화폐 단체방에 들어와 관리자의 이름과 사진을 베끼고, 개인 메시지로 도움이나 '지갑 점검'을 제안합니다. MARKET TALKS는 시드 문구, 개인 키, 비밀번호를 절대 요구하지 않으며, 진짜 팀이라면 어디도 마찬가지입니다.
- **거래소 계정에도 시드 문구 같은 비밀이 있습니다.** 거래소 계정은 시드 문구를 쓰지 않지만, 2단계 인증 백업 코드가 비슷한 역할을 합니다. 누군가 이 코드와 비밀번호를 함께 손에 넣으면 계정을 탈취할 수 있습니다. 시드 문구처럼 오프라인에 보관하세요.
- **내 뒤에 남을 사람을 위해 계획하세요.** 연구자들은 이미 수백만 개의 비트코인이 영원히 사라졌다고 추정하는데, 상당수는 키를 아는 유일한 사람이 세상을 떠났거나 잊어버렸기 때문입니다. 의미 있는 금액을 보유하고 있다면, 오늘 누구에게도 접근 권한을 주지 않으면서 언젠가 믿을 만한 사람이 복구할 수 있는 방법을 생각해 두세요.

핵심 용어

시드	지갑이 모든 개인 키를 만들어 내는 하나의 큰 무작위 숫자.
시드 문구	12개 또는 24개 단어로 적은 시드. 지갑의 모든 키를 다시 만들어 낼 수 있습니다. 복구 문구라고도 합니다.
단어 목록	시드 문구의 단어를 뽑는 2,048개 단어의 고정 목록으로, 호환되는 어떤 지갑이든 읽을 수 있게 해 줍니다.
체크섬	마지막 단어에 담긴 내장 검사로, 문구를 잘못 옮겨 적었을 때 지갑이 알아차리도록 돕습니다.
Passphrase	시드 문구에 덧붙이는 선택적인 추가 비밀번호. 이것이 없으면 단어만으로는 지갑을 열 수 없습니다.
복구 훈련	지갑에 큰돈을 넣기 전에, 적어 둔 시드 문구로 복구를 미리 연습해 보는 것.

핵심 정리

1. 요즘 지갑은 모든 키를 하나의 시드에서 만들며, 시드는 12개 또는 24개 단어의 시드 문구로 보여집니다.
2. 시드 문구가 있으면 예전 기기를 잃어버리거나 고장 나도 새 기기에서 지갑을 다시 만들 수 있습니다.
3. 단어는 2,048개 단어의 고정 목록에서 지갑이 무작위로 고르며, 마지막 단어는 실수를 잡아내는 검사 역할을 합니다.
4. 문구는 오프라인에 튼튼하게 보관하고, 사진, 메모 앱, 이메일, 클라우드에는 절대 두지 말며, 소액으로 복구를 시험해 보세요.
5. 시드 문구를 요구하는 사람은 누구든 도둑질을 하려는 것입니다. 시드 문구는 오직 내 지갑에만 입력합니다.

실력 점검

각 문제에 답을 하나씩 표시하세요. 해설이 포함된 정답은 다음 페이지에 있습니다. markettalks.info에서 온라인으로 퀴즈를 풀고 바로 점수를 확인할 수도 있습니다.

1. 시드 문구로 무엇을 할 수 있나요?

A 거래소 비밀번호를 재설정한다
B 지갑의 모든 개인 키를 다시 만든다
C 거래를 더 빠르게 한다
D 이미 보낸 결제를 취소한다

2. 지갑 앱이 깔린 휴대폰을 도난당했습니다. 시드 문구는 적어 두었습니다. 어떻게 해야 하나요?

A 다른 기기에서 시드 문구로 지갑을 복구한다
B 비트코인 고객센터에 연락한다
C 코인을 잃었다고 받아들인다
D 거래소에 도난을 되돌려 달라고 요청한다

3. 좋아하는 명언으로 시드 문구를 직접 만들면 안 되는 이유는 무엇인가요?

A 지갑은 문장을 읽지 못한다
B 거래가 느려진다
C 사람이 지어낸 문구는 프로그램이 쉽게 맞힌다
D 명언은 저작권이 있다

4. 시드 문구를 보관하는 가장 안전한 방법은 무엇인가요?

A 사진첩의 스크린샷
B 이메일 임시 보관함의 메모
C 클라우드 드라이브의 파일
D 오프라인으로 적거나 새겨, 불과 도난으로부터 안전한 곳에 보관

5. 시드 문구의 마지막 단어는 어떤 도움을 주나요?

A 지갑의 비밀번호를 정한다
B 옮겨 적는 실수 대부분을 잡아내는 검사 역할을 한다
C 지갑이 어떤 코인을 담을지 정한다
D 지갑의 잔고를 보여 준다

6. 트레이딩 단체방의 누군가가 시드 문구를 알려 주면 지갑을 고쳐 주겠다고 메시지를 보냈습니다. 무슨 일일까요?

A 정상적인 고객지원 절차다

B 잔고를 확인하려면 필요하다

C 사기다. 정상적으로 돕는 사람은 시드 문구가 필요 없다

D 본인 확인을 하는 것이다

정답 및 해설

1 B

지갑의 모든 개인 키를 다시 만든다

시드 문구는 모든 키를 만들어 내는 시드를 글로 적은 것입니다. 호환되는 어떤 지갑이든 이를 이용해 같은 키를 다시 만들고 같은 코인을 찾을 수 있습니다.

2 A

다른 기기에서 시드 문구로 지갑을 복구한다

코인은 휴대폰이 아니라 블록체인 위에 있습니다. 시드 문구로 복구하면 통제권을 되찾고, 곧바로 새 지갑으로 자금을 옮기면 안전하게 지킬 수 있습니다.

3 C

사람이 지어낸 문구는 프로그램이 쉽게 맞힌다

보안은 엄청난 수의 조합 중에서 단어를 무작위로 고르는 데서 나옵니다. 사람이 고른 문구는 훨씬 예측하기 쉽습니다.

4 D

오프라인으로 적거나 새겨, 불과 도난으로부터 안전한 곳에 보관

인터넷에 연결된 계정이나 기기에 저장된 것은 무엇이든 해커나 악성 코드가 닿을 수 있습니다. 튼튼한 오프라인 사본은 그 위험을 피합니다.

5 B

옮겨 적는 실수 대부분을 잡아내는 검사 역할을 한다

마지막 단어의 일부는 나머지 단어에서 계산되므로, 단어 하나를 잘못 적으면 지갑이 보통 문구가 유효하지 않다고 알려 줍니다.

6 C

사기다. 정상적으로 돕는 사람은 시드 문구가 필요 없다

시드 문구가 있으면 지갑의 모든 것을 가져갈 수 있습니다. 진짜 고객지원팀은 절대 요구하지 않으므로, 요구 자체가 사기라는 증거입니다.

출처

- 비트코인 개선 제안 39, 키 생성을 위한 니모닉 코드 (GitHub): https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BleepingComputer, 암호화폐를 훔치려 조작된 Ledger 기기를 우편으로 보내는 범죄자들: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency
- Cointelegraph, 최대 400만 개의 비트코인이 영원히 사라졌을 수 있다 (Chainalysis 추정): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

계속 학습하기

다음: 10강
수탁: 거래소 계정 또는 개인 지갑

이 강의는 MARKET TALKS 교육 센터의 무료 블록체인 과정에 속합니다. 초급, 중급, 고급 강의로 구성되며 강의마다 퀴즈와 다운로드 가능한 PDF가 제공됩니다.

교육 센터
기초 원리부터 고급 주제까지 다루는 강의

시장 분석
주요 시장에 대한 기술적 분석과 기본적 분석

리포트
비트코인, 금, 은, SPX 등

markettalks.info

텔레그램 @MARKET_TALKS

교육 목적으로만 제공됩니다. 이 문서의 어떤 내용도 투자 조언이 아닙니다. © 2026 MARKET TALKS. 이 PDF는 수정 없이 자유롭게 공유하실 수 있습니다.