

부정행위가 없더라도 거래소 및 기타 네트워크 중단 서비스 제공자는 비  
그에 취약하다. 6장의 앞부분에서 언급한 쿼드리가CX 문제는 단순한 코딩  
오류로 인해 1,400만 달러를 회수할 수 없는 경우였다. 최근 패리티Parity 지  
갑 서비스는 사용자가 (분명히) 실수로 특정 버전의 소프트웨어를 사용하는  
모든 스마트 컨트랙트에 접근할 수 없도록 하는 명령을 실행한 후 1억 6,000  
만 달러 상당의 이더가 갇혀 있는 것으로 나타났다.<sup>50</sup>

쿼드리가CX와 마찬가지로 패리티는 초기 결함을 수정하려고 지갑 소프  
트웨어를 업데이트할 때 버그를 제출했다. 이 초기 문제로 인해 해킹은 토큰  
판매로 보급된 3,000만 달러 상당의 이더를 훔칠 수 있었다. 그리고 패리티  
는 블록체인 초보의 회사가 아니다. 이더리움의 전 수석 기술자인 개빈 우드  
 Gavin Wood가 공동 설립했다. 거래소의 마찬가지로 지갑은 일반 사용자가 암호  
통패를 편리하게 나눌 수 있도록 하기 위한 중앙 집중식 양이다. 지갑 보유  
승환은 시간이 지남에 따라 개선될 것이지만 시범들이 네트워크 중단 시비

스 제공자에 의존하는 한 위험은 여전히 남아 있을 것이다.  
중단 서비스 제공자에 대한 신뢰와 또 다른 측면은 이러한 서비스 제공자  
가 트랜잭션을 통제할지 여부를 결정할 수 있다는 것이다. 만약, 도박, 정부  
살인에 대한 비트코인 거래는 피사 거래와 동일한 방식으로 처리된다. 신용  
적인 금융 거래에서 지급결제 처리업체(예: 비사Visa 및 마스터카드Mastercard 회  
원 등)는 정부가 불법 거래를 차단하도록 압력을 가할 수 있는 통제 지점이  
다. 지급결제가 비트코인으로 이루어지면 지급결제 사체에 관여하는 사람이  
없고 단지 분산된 채굴자들의 네트워크만 있다. 그러나 트랜잭션이 네트워  
크 중단 서비스 제공자를 기치면 법적 집행의 대상이 될 수 있다. 이는 서비  
스의 위치와 관리자의 신원을 숨겼는지에 따라 이루어질 수 있지만 불가능한  
것은 아니다. 가장 유명한 예는 2장에서 논의한 링크로드였다.

상황에 따라 다양한 수준의 보안과 안정성이 필요하다. 은행은 소매 소비  
자 거래에 종사하는 상인보다 특정 위험에 더 우려할 것이다. 블록체인의 의  
료 기록은 다이아몬드 공급망 기록과는 위험 프로파일이 다를 것이다. 이러  
한 변화는 블록체인에만 국한된 것이 아니라 기존의 중앙 집중식 시스템에