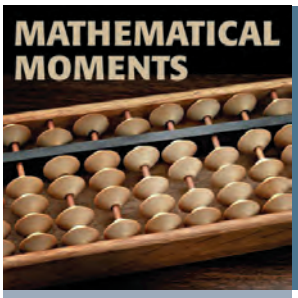

화폐 없이 화폐 거래하기

많은 거래가 온라인상에서 이루어지지만, 대부분은 표준통화를 기반으로 합니다. 비트코인은 디지털 지불시스템 또는 암호화폐의 한 예인데, 전자적으로만 존재하고 사용자의 익명성을 유지하며 은행이나 정부와 같은 중앙관리자가 없습니다. 비트코인은 공유된 컴퓨터의 네트워크를 사용하여 개개의 거래를 처리하고 검증하는데, 각 거래는 수학 공식을 이용하여 암호화되어 있고 '블록체인'이라고 부르는 전자장부에 입력됩니다. 블록체인은 거래 내역들을 연결하며 비트코인 소유자가 동일한 가치단위("코인")를 중복으로 이용하지 못하게 합니다. 각 비트코인 소유자는 수학 공식에 의하여 사용하기는 쉽지만 실제로 알아내기는 불가능한 고유번호를 갖습니다. 따라서 비트코인이 경화(hard currency)보다 덜 안전해 보일 수 있지만, 고유번호를 비밀로 유지하는 한 절도나 위조에 훨씬 덜 취약합니다.

블록체인의 아이디어는 배송과 같은 잠재적 응용분야가 많습니다. 세금 및 세관 서류를 작성하고 유지하는 현재의 작업은 배송비에 버금가는 비용이 들 수 있습니다. 더욱이 종이 문서는 변조되거나 갑자기 사라질 수 있습니다. 공개키 암호체계, 일방향 해시 함수, 작업 증명의 계산 복잡도와 같은 블록체인 뒤에 있는 수학으로 화주는 운송 중에 있는 물품을 추적할 수 있을 뿐만 아니라, 필요한 서류들에 대하여 안전하고 변경이 불가능한 디지털 기록을 확보하게 됩니다. 블록체인을 사용하는데 관심이 있는 것은 대기업들 뿐만이 아닙니다. 종종 자신들의 신원을 정부에 등록하기를 꺼려하는 난민들은 일종의 블록체인에 기록된 비상 신분증을 만듭니다. 이는 적대적일 수 있는 정부 조직에 자신을 드러내지 않으면서, 떨어져 있는 가족 구성원들과 전자적으로 연결하고 결국 실제로도 재결합할 수 있도록 해줍니다.

더 알아보기: "Bitcoins Maybe; Blockchains Likely," Peter J. Denning and Ted G. Lewis, *American Scientist*, November-December 2017.

Translation courtesy of the Korean Mathematical Society

Listen Up!

MM/134/KR