Bitcoin, 도대체 무엇인가!

GIST 이흥노 교수
2018년 1월 3일

“비트코인 거래 국민 300 만명, 코인 한개 2000만원,
거래소서버 다운, 거래소 해킹, 재산 피해 심각...”

한 동안 방송매체를 장식했던 헤드라인들입니다.

지난 몇 일 동안은 다음과 같았지요.

“정부, 비트코인 등 암호화폐 규제 강화”,
"거래 실명제 실시“, ”거래소 폐쇄 검토“

오늘은 지난 시간에 이어,
도대체 Bitcoin이란게 무엇이기에
이렇게 세상을 떠들썩하게 하는 가 살펴보겠습니다.

Bitcoin은 디지털 화폐입니다.
통상적인 화폐와 대비해보면 이해가 쉽겠지요.

오늘날의 화폐는 신뢰에 기반 한 가치교환 수단입니다.
국가는 지폐나 동전의 모양으로 만들어진
한정된 양의 화폐를 발행하고 유통시킵니다.
종이나 구리로 만들어진 화폐 그 자체는 값어치가 없습니다.
카드와 계좌이체가 활성화 된 요즘에는,
화폐는 계좌에 찍혀진 숫자에 불과합니다.
그저 출금계좌에서 입금계좌로 숫자가 이동 할 뿐이지요.
화폐의 시장가치는 화폐를 발행한 국가의 존재에 있습니다.
불법적 화폐 발행과 유통을 적발하고 엄단하는

공권력을 행사하는 국가를 신뢰하는 것입니다.
이런 역할을 못 하는 국가가 발행한 화폐는 가치를 없습니다.
국가가 발행한 화폐를 소유한 주체는, 화폐 소유권 이전의 댓 가로
언제 어디서든지 필요한 서비스 및 제품을 제공 받을 수 있다는
신뢰가 있는 것 입니다.
신뢰를 확보한 화폐는 높은 값어치를 갖게 되는 것입니다.

Bitcoin은 인터넷상에서 통용되는 디지털화폐를 생산하고,
유통하며 거래를 관리하는 컴퓨터 알고리즘입니다.
2009년에 알고리즘과 논문이 공개되었지요.
국가의 개입이 없었음에도 불구하고, 화폐로써의 신뢰를 확보하고,
수요에 기반 한 시장가치를 창출하는데 성공한 것 입니다.
이 알고리즘은 Bitcoin 네트워크에 속한 모든 컴퓨터가
거래 검증 및 기록을 위해 상호 협력하도록 디자인 되었으며,
거래기록의 위조 및 이중거래를 차단하도록 설계되어 있습니다.

이 알고리즘은, "A가 B에게 코인 한 개를 지불 합니다" 같은
평범한 문자메세지가 수정 불가능하게 기록될 때,
A가 B를 직접 만나서 동전 한 개를 건네주는 것과 같은
지불수단의 역할을 할 수 있음을 보여 주었습니다.
국가나 은행과 같은 신뢰받는 제3자의 중개가 없어도,
누구나 안심하고 인터넷 상에서 신뢰거래를 할 수 있게 된 것이죠.

도대체 어떻게 설계된 알고리즘이기에 그런게 가능해진 것일까요?

해답은 의외로 너무나 간단한 것이었습니다.
즉, 거래의 내용과 시간이 수정 불가능한 방식으로 기록되고,
또 기록된 거래장부를 인터넷에 실시간으로 공개하여
누구나 열람 가능하도록 한 것 입니다.

즉 각각의 거래를 다음과 같은 절차로 인증하고,
인증된 거래만 장부에 기록하고,
장부에 기록된 거래는 절대 수정하지 못하게 하는 것입니다.

첫 째, 거래시점에 과연 A가 동전의 소유권을 갖고 있는 지 확인합니다.
둘 째, 동전의 소유권을 혹시 B가 아닌 C에게도 동시에 넘기고 있지는 않은지 검증합니다.
셋 째, 위와 같은 소유권 및 이중거래 문제가 없는 거래는 장부에 기록합니다.
이때, 한 번 장부에 기록된 정보는 임의로 수정하지 못하도록 관리합니다.

거래 장부를 인터넷에 실시간으로 공개하면,
소유권 검증과 이중거래 방지 문제는 방지될 것으로 생각됩니다.

그런데 세 번째 문제, 즉, 장부에 기록된 거래를 임의로 수정하지 못하게 보관하고 관리할 것인가의 문제는
블록체인이라는 새로운 기술의 개발로 해결한 것입니다.

Bitcoin기술은 국가의 개입이 없어도, 인터넷 상 거래를 실시간으로 관리 추적할 수 있고, 동시에 보안과 신뢰성을 크게 높일 수 있음을 보여주었습니다.

이 기술혁신에 전 세계가 주목하고 있습니다.
화폐 이외에 다른 문제에도 적용하여 효과를 크게 보고 있습니다.

Walmart는 식품이력 추적시스템 개발에 적용하고
문제가 되는 식품이 어떤 경로를 통해 납품되었는지
실시간으로 관리 하는 데 성공하였습니다.

에스토니아 정부는 블록체인을 기반으로 한
주민등록제도와 전자투표 시행을 예고하였습니다.

전 세계에서 블록체인기반 가상화폐와 또 다른 응용 분야 발굴에 박차를 가하고 있으며 지원하고 있습니다.

신기술 개발을 투기 목적에 사용하는 것은 마땅히 규제해야 합니다.
그러나 Bitcoin 기술을 활용하여 사회의 문제를 해결하고 그 응용 분야를 넓히는 연구를 지원하는 것은 더욱 중요합니다.

다음 시간에는 Bitcoin의 탄생을 가능케 한 블록체인을 보다 자세히 논의하도록 하겠습니다.

끝