블록체인 혁명!

GIST 이흥노 교수
2018년 1월 3일

지난 시간에는 Bitcoin 기술을 살펴보았습니다.

소유권과 이중거래 검증을 마친 거래를 장부에 기록하고
장부를 인터넷에 공개하여 관리하는 블록체인기술이
뛰어난 보안과 신뢰성을 인정받고 있으며,
이로 인해 Bitcoin이 통화로써의 지위를 확고히하고 있다는
내용이었습니다.

오늘은 Bitcoin의 핵심, 즉 블록체인 기술을 살펴보겠습니다.
즉 어떻게 거래내용을 장부에 기록하며, 어떻게 한 번 기재된 내용은 임의로 수정하지 못하게 보호할 수 있는지 설명하겠습니다.

핵심 기술의 올바른 이해는 매우 중요합니다.
이해부족에서 기인한 불필요한 기술규제를 방지하며
새로운 응용분야와 비즈네스모델 개발에 크게 도움이 될 것입니다.

1Mbyte 사이즈의 파일을 하나를 블록이라고 칭합니다.
이 파일 안에 최근 10분 안에 발생한 거래의 내용과
시간을 기록합니다.
이런 파일들을 시간의 순서대로 연결합니다.
블록은 파일이고, 여기서 핵심은 연결입니다.
앞블록을 한 줄로 요약하고 그 요약을 뒷 블록의 내용에
포함시킴으로써 블록과 블록을 연결합니다.
블록체인은 시간 순으로 연결된 거래를 담은 파일들의 묶음입니다.

“A가 B에게 코인 두 개를 지불합니다,”

“B가 C에게 코인1개를 지불합니다,”
“C가 D에게 코인 0.5개를 지불합니다,” 와 같은
코인거래내용이 체인안에 기록됩니다.

이 체인을 들여다보면 누가, 언제, 누구에게, 얼마만큼의 동전을 이전하였는지 알 수 있습니다.
그러므로 블록체인은 거래장부입니다.
이 장부는 인터넷에 공개됩니다.
누구나 이 장부를 열람할 수 있으며,
어떤 코인이 누구에게 속해 있는 지,
소유권의 귀속상태를 곧 바로 파악할 수 있습니다.

그러나 오해는 금물입니다.
블록체인은 암호화 되어 있습니다.
따라서 해당 동전의 소유권자가 누구인지 확인 할 수는 있으나,
소유권자가 아니면 그 권한을 행사 할 수는 없습니다.

동전의 소유권은 사실 사람이 아닌 public key 라 불리는
암호주소에게 귀속되어 있는 것 입니다.
해당 public key를 푸는 private key를 갖고 있는 사람만이
해당 동전의 소유권을 행사 할 수 있습니다.

즉, 위의 예에서 A라는 사람만이
해당 동전의 public key를 풀 수 있는
private key를 갖고 있으며,
“A가 B에게 코인 두개를 지불합니다” 라는 메시지에 전자서명을 붙일 수가 있는 것입니다.
Private key를 잊어버리면 권리 행사를 못 하게 됩니다.

이렇게 암호화된 거래기록을 담은 공개된 장부가 블록체인입니다.
이제 거래내역이 들어있는 이 디지털파일 묶음을
누군가가 공격할 의도를 가지고 아무도 눈치 채지 못 하게
그 내용을 위 변조하기 쉽지 않은가? 라는
매우 중요한 문제를 생각 해 보겠습니다.

블록체인은 새로운 방식으로 이 문제의 해결책을 제시하였습니다.
새로운 거래기록을 담은 블록을 생성할 때
작업증명을 붙이도록 설계한 것입니다.

작업증명이 없는 블록은 체인에 연결될 수 없습니다.
그런데 이 작업증명을 10분 안에 완수하려면, Bitcoin 네트워크에 속한 컴퓨터가 모두 동원할 때 가능하도록 설계 한 것입니다.
원할한 작업증명 결과를 얻기 위해서 많은 컴퓨터의 참여가 필요하고, 이를 위해 작업증명을 마친 컴퓨터에게 보상으로 Bitcoin을 수여합니다.

핵심 사항을 정리 해 드리면,
한대의 컴퓨터 혹은 협력하는 여러 대의 컴퓨터 무리로는
정해진 시간 내에 이 작업증명을 끝낼 수 없도록 설계하였습니다.
전 세계에서 수많은 컴퓨터가 참여할 때,
그들 중 최소 한 대 이상의 컴퓨터가 작업증명에 성공 할 수 있도록 작업증명문제를 설계한 것 입니다.

정리해 보면, 한 대의 컴퓨터로는 절대 못 마치는 일을 백 만대의 컴퓨터가 동원되었을 때는, 10분 안에 완료하도록 설계된 것이 작업증명입니다.

작업증명으로 보안을 높이는 해결책은 블록체인으로 파일들이 묶여

있을 때 더 위력을 발휘합니다.
앞에서 언급 했던 데로, 하나의 블록은 그 다음 블록과 연결되어 있습니다.
앞 블록의 한 줄 요약을 다음 블락의 내용에 집어넣는 것이지요.
체인연결이 되면, 어느 한 블록의 내용을 바꾸면 그 뒤에 따라 오는 모든 블록의 내용도 바뀌게 됩니다.
블록의 내용이 바뀌면 블록의 작업증명들도 모두 연차적으로 다시 해야 합니다.

하나의 작업증명을 완료하는 데에도 네트워크에 속한 컴퓨터들
모두가 동원되어야 가능했던 것을 상기해 보면,
체인 안에 깊숙이 자리 잡은 내용을 다른 컴퓨터들이 눈치 채지 못하게 바꾸는 것은 불가능 한 것임을 쉽게 이해 할 수 있습니다.
즉, 소수의 컴퓨터 무리가 필요한 작업증명을 제한된 시간 내에 완성하고 다수의 컴퓨터를 기만하는 것은 거의 불가능하게 됩니다.

결론적으로, 작업증명요구 때문에, 블록체인 속에 기록된 거래내용은 위변조가 불가능 하게 됩니다.

블록체인 기술은 은행이나 중간자의 개입 없이
거래한 기록을 확보하고 보존할 수 있는 기술입니다.
이 거래기록 보존 기술은 그 용도가 매우 다양합니다.
사회활동을 하다보면 병원진료기록, Copyright 및 특허, 투표권의 행사, 부동산 계약 등과 같이 위변조의 위험 없이 기록 관리 되어야 것들이 많이 있습니다.

하나만 예를 들어 본다면, 병원 진료기록의 보존입니다.
의료사고가 발생 했을 때
위변조가 불가능하게 보존된 진료기록 있다고 하면,

그 기록의 열람을 통해 책임소재를 분쟁 없이 가려낼 수 있습니다.
블록체인 기술이 불필요한 분쟁을 막을 수 있는 것 입이다.

블록체인 기술은 그러나 아직은 완성되었다고 보기는 어렵습니다.
작업증명에 너무 많은 cpu자원과 전기를 낭비해야 하는 등 추가적인 연구를 통해 개선해야 할 점이 많이 있습니다.

블록체인 기술 연구와 응용분야 개발은 적극 추진해야 합니다.
이를 위해서 GIST에서 저는 블록체인 연구센터 설립과 교과목 신설을 준비하고 있습니다.

이 자리를 빌어 많은 관심과 성원을 부탁드립니다.

끝