불럭체인 풀렛폼의 한계, 그리고 법정화폐와 가상화폐의 발전과 공존에 대한 전망

서울대학교 명예교수 이천표

1절 서론

P2P 구조, 불럭체인기술(분산원장기술), 해시, 암호화, 작업증명 등
법정화폐 이야기는 없이 가상화폐만 이야기 해, 그런데 후자의 전자 대비 상대적 크기는 1% 내외, 꼬리가 몸통을 흔드는 격

2절 법정화폐와 가상화폐

2-1 의미의 재탐색

2-2 가상화폐의 매력 내지 장점

데이터 불가변경, 위조 변조 있을 수 없어
그러나 이는 일정한 제한 속에서 성립하는 것(뒤에 봄)

낮은 수수료
희망하고 예상하는 것, 그러나 아직 실현된 것은 아니야
다른 방법도 있어, 핀테크 송금

해시, 암호화, 승인(consensus achieving)이라는 3중의 안전장치

3절 불럭체인기술의 한계 및 약점

3-1 기반 기술로부터 유래하는 한계

P2P 구조: 모든 데이터 공개, privacy 유지 어렵고 영업비밀도 공개
해시기술: 암호화를 줄여 비용절감(암호학자에게는 크게 인상적)
그러나 작업증명을 하기 위해 들여야 하는 전기료를 무시해서는 안 돼

비트코인 풀랫폼에서의 작업증명의 한계점

확장성: 불럭완성에 10분, 안정화를 위한 6개 불럭이면 60분 필요
컴퓨팅 파워를 크게 늘려야, 그러면서 중국의 독주는 견제해야

효과성: 양당사간 거래, 노드들의 승인, 승인(consensus achieving)이라는데 무엇을 승인하는 것인가? 거래내용의 진실성을 보증하는 것은 아니야, 거래가 사회미풍양속에 반하지 않는 것이라는 것을 증명하는 것은 더더구나 아니야(불법자금의 거래를 여과못해, 양당사간 거래가 제3자의 이해를 해하더라도 이를 알 길이

없어 예방할 방도도 준비되어 있지 않아)

필요성: 작업증명이나 지분증명이 왜 필요한가?
micro efficiency, macro efficiency, invisible hand?
market failure를 인지하고 실패현상에 대응하는 간여를 함

반면 작업증명을 하는 것이 자원과 노력을 들이면서 작업을 했다는 것은 알겠으나 무엇을 위해 어떤 근거로 '어려운 수학문제를 푸는' 작업을 했는지에 대한 설명이 없어, 어떤 이유로 그것을 하면 consensus achieving을 이루게 되는지는 설명되어 있지 않아, 해시한 것을 복원해 본래의 데이터를 아는 것이, 또는 이를 위해 컴퓨터를 마련하느라 돈을 쓰고 운영을 위해 많은 전기료를 내는 것이, 어떤 논리 또는 어떤 이유로 승인하는 것이라고 하는가?

3-2 해킹에 대한 대비 불충분

불럭 생성의 단계, 그 이후 이용의 단계(wallet에 대한 해킹 많았음, 반론은 사토시의 wallet은 해킹당한 적이 없다고 함)
설사 앞의 단계에서 해킹이 없더라도 뒤의 단계에서 해킹이 많아 이들 둘을 함께 보면 해킹을 무시할 수 없어

3-3 미신의 극복

작업증명을 거쳤다고 해서 위변조가 불가능한 변경불가의 데이터가 되는 것은 아니야
작업증명이 끝난 후 10분 또는 60분이 경과하고 난 후에야 데이터의 불가변성이 주어지게 돼

불럭체인기술을 채택했다고 해서 무조건 데이터의 고결성이 보장되는 것은 아니야

3-4 기왕의 논의 및 한계 극복

기왕의 논의(돈 탭스콕 알랙스 탭스콧의 불럭체인 혁명 등) 및 평가
막대한 에너지 비용, 사회적 낭비

한계극복

한계극복방안이 없을 경우의 무력감(특히 시장실패)
governance(특히 해킹방지 및 사후수습)의 불분명 및 책임소재
비용절감은 미실현의 이익
결국 불럭체인기술은 아직은 미성숙된 것, 기대를 가지고 실험 중

4절 불럭체인기술의 이용 확장: 한계의 극복 및 선용방법의 모색

4-1 사적 불러체인의 선용

이것은 개방성 및 탈중앙성을 포기하는 것(중앙의 관리주체를 인정)
중앙의 관리주체가 validator, 승인자가 됨
그로써 거래속도를 높일 수 있어

건강관리, 부동산관리, 자율자동차 제도 관리 등에서 이용

4-2 스마트 계약 활용을 통한 융통성 확보

그러나 DAO의 파산, 스마트 계약이라는 장치를 했다는 것만 가지고는 문제가 해결되지 않아, 완벽한 스마트 계약을 할 수 있어야, 그런데 완벽한 스마트 계약이란 것이 가능한가? 이를 위해서는 미래를 예측하여 즉각적 자동적으로 프로그램 업그레이드 할 수 있게 되어야, 그리고 이를 위해서는 AI에 기대, 그런데 데이터 준비, 알고리즘의 마련?

이상적 스마트 계약을 할 수 있으면 좋으나 지금은 실현 불가능

4-3 여러 이용 예의 개발

4-4 불럭체인은 만병통치약이 아니야

삼성증권의 입력오류 및 그 이후의 사태, 불럭체인기술을 이미 도입했었더라면, 더불어 AI를 통해 대응하도록 했더라면 그 사태를 예방할 수 있었을 것이라는 희망이 피력되고 있어, 이러한 희망에도 불럭체인기술에 대한 과잉의 기대가 숨어 있어, 이때 필요한 것은 불럭체인기술이 아니라 비정상거래의 탐색 시스템임, 이런 시스템을 AI로 할 수 있게 한다면 매우 기동적일 것, 그러나 이러한 AI를 마련할 수 있나? 이번 사태처럼 비정상 중에도 비정상인 거래 탐색을 위한 알고리즘을 마련할 수 있어야 하고, 이런 알고리즘을 훈련시키기 위한 데이터도 마련해야 해, 그런데 이런 data analytics란 적어도 현재는 불가능(우리나라에서는 물론 미국에서도), 나아가 그러한 프로그램이 담아야 할 내용은 내부 '견제와 균형' 장치이고, 현재의 미국 AI 관련문헌은 이런 일은 사람이 해야 한다고 말하고 있어, 2045년 singularity를 이야기 하나 그 이전 또는 그 이후에도 상당한 기간 사람과 AI는 협력하며 공존해야 할 것으로 보여

5절 법정화폐와 가상화폐의 발전과 공존에 대한 전망

5-1 법정화폐에 대한 도전: 불럭체인, 핀테크(이것을 통해서도 낮은 수수료 시현)

5-2 Baclays의 연구

비트코인 가격등락, 가상화폐에 대한 통화당국 및 재정당국의 영향력,

가상화폐 이용 시 정보누출(privacy, 영업비밀), 시발점에서 잘못된 거래가 변경불가능하게 되면 심각한 문제 노출(원상회복 어려워)
무법 무정부 사회에서 가상화폐 선호 돼, 범죄와의 연관

5-3 법정화폐량의 증감, 가상화폐량의 증감
실물경제의 성장을 뒷받침, 기타 정책적 수요
ICO, 기왕에 발행된 가상화폐의 추가발행, alternative private token

5-4 ICO
IPO, 투자자 보호(백서의 실박화: 비즈니스 모델, 투자계획, 자금사용 및 수입에 대한 예산, 같이 일할 사람들, 알고리즘의 코드 공개 등)

ICO 담당자들의 위험(외환관리법, 현지에서의 횡령죄, 대외투자 신고 및 역외소득 신고의 의무)

ICO 가이드라인(스위스 금융감독청): 화폐, 자산, 유틸리티

미국의 ICO
(적격투자자에게 권고, 일반투자자에 주의할 것을 요구, 일반투자자에게는 차라리 reverse ICO를 권고)

우리나라의 ICO
(자금수요: IPO 및 벤처투자 방식으로의 자본조달의 어려움, ICO에서 숨통)
(자금공급: 낮은 이자율, 괜찮은 투자기회의 결여, 비트코인의 가격상승을 보고 투기이익을 감지, 그러나 투자규모는 크게 보아서는 제한적이었다고)

가상화폐가 더 늘어날 수 있는 소지: ICO 이외 가상화폐 거래소의 역할(가상화폐의 유통속도를 늘릴 수 있어)

5-5 가상화폐 거래소
딜러, 브로커 없이 거래소가 딜러, 브로커 및 거래종결이라는 3중의 역할을 모두 담당, 증권거래소에서 보이는 딜러, 브로커, 거레소 간의 견제와 균형이 실종되었어

가상화폐 시장이 경쟁시장이 되기 어려워(특히 정보비대칭)
외환관리와의 관계?(법정화폐와 가상화폐의 교환이 아누런 장애 없이 이루어지게 되고 수수료도 아주 낮다면 현재 방식의 외환시장은 존립할 수 없게 돼)

5-6 법정화폐의 반격

정책적 반격

특히 양적완화

손정의 Vision Fund

가치있는 신기술, 기술 활용 혁신, 법정화폐 기반 자금의 투자(1000억불), ICO를 통한 자금조달은 이것에 비해 보면 얼마나 초라한가?