홀로체인—비트코인과 이더리움을 넘어서

- 저자 : Hank Sohota
- 원문 : Beyond Bitcoin and Ethereum—a fairer and more just post-monetary sociopolitical economy (2019. 1. 28)
- 분류 : 내용 정리
- 정리자 : 정백수

화폐는 사회적 구축물로서 사람들의 신뢰에 의존한다. 그 기능은 ① 가치저장 ② 교환수단 ③ 회계단위, 이 셋이다. 그런데 화폐가 큰 규모로 작동하려면 표준화가 필요하고, 이는 불가피하게 중앙집중화를 낳는다. 불행하게도 중앙집중화는 ‘ 화폐의 경화적 성격’(hardness of money)[가치의 안정성(‘uninflatability’)]과 사람들의 신뢰를 침식한다. 의사결정이 소수의 손에 맡겨지기 때문이다. 안타깝게도 이 소수는 그들의 책임을 오용해온 긴 역사를 가지고 있다.

화폐의 경화적 성격과 신뢰의 수준이라는 문제를 해결하기 위해서는 중앙집중화 문제를 해결해야 한다. 그 문제의식은, ‘ 중개자들 · 대표자들 · 경영자들 · 조직소유자들 없이 어떻게 시공간을 가로질러 연계하고 협동하고 협력하는가? ’ 이다.

이는 어떤 사람들에게는 ‘ 아나키 ’ 라는 성배(聖杯)를 나타낼 수도 있다. (여기서 ‘ 아나키 ’ 는 단순한 무법, 혼란, 무질서와 동의어로 간주되어서는 안 된다.)

[비트코인의 한계]

비트코인은 ‘ 경화(硬貨)의 중앙집중화 ’ 문제를 풀기 위한 시도이다. 이는 더 큰 그림에 넣고 보면 좋은 출발점이다. 비트코인은 이 일을 위해 해시체인(hashchain) 블록들의 분산된 원장을 사용해서 변경 불가능성을 부여하고, ‘ 하드 코딩 ’ 을 통해 가치의 안정성을 확보하며 탈중심화된, 그러나 온전히 분산되지는 않은 작업증명(Proof of Work, PoW)을 사용하여 단 하나의 네트워크 전체에 걸친 타임라인을 구축하고, 합의 메커니즘을 통해 검열 불가능성을 확보한다. 이렇듯 개별 주체나 행위자보다는 네트워크를 신뢰함으로써 ‘ 신뢰 부재(trustlessness)의 한 형태가 형성된다.

그런데 실용상의 한계 및 철학적 한계로 인해서 이 접근법은 부분적이고 비실용적인

해결책만을 제시한다. 충분히 분산되어 있지 않다는 것, 충분히 빠르지 않다는 것, 비용 효율이 충분히 높지 않다는 것, 충분히 규모를 키우지 못하다는 것이 그 한계이다. 더군다나 비트코인은 앞으로 재생 가능한 에너지의 생성에 재정적으로 큰 혜택을 주지 못하는 한, 아니 더 나아가 녹색에너지 기반시설의 구축에 재정적으로 기여하지 못하는 한, 코인 채굴에 들어간 전력 소비 때문에 기후변화를 잘못된 방향으로 너무 많이 밀어붙였다는 비난을 들을 수밖에 없다. 비트코인의 모든 중기 개선책들이 의도된 효과를 발휘한다고 하더라도 앞에서 말한 결점들은 여전히 남는다. 그렇더라도 비트코인의 네 핵심 특성들—변경 불가능성, 가치 안정성, 검열 불가능성, 몰수 불가능성(unconfiscatability)—은 역사적 성취로 남아있다.

[이더리움의 한계]

이더리움은 반드시 비트코인이 해결하려는 바로 그 문제를 해결하려는 것은 아니지만 비트코인과 근본적으로 동일한 원장 기술을 바탕에 깔고 있으며 따라서 동일한 한계를 가진다. 여기에 더 추가할 것으로서, 권력의 중앙집중화 문제, 비트코인에 비한 암호화페로서의 단점들, 스마트계약의 문제점들, 지분증명(Proof of Stake, PoS)이라는 합의 메커니즘으로의 이동 시도 등이 있다.

이더리움이 한 일은 수 천 개의 대안코인들을 출시한 것인데, 그 가운데 어느 것도 말이 되는 것 같지 않다. 또한 이 코인들이 주장된 목표를 달성할 수 있으리라는 확신도 주지 않는다. 이것이 새로운 자산계층과 규제되지 않는 시장에서 일어난 일임을 감안하다면, FOMO-FUD라는 ‘ 서부 ’ 가 출현하더라도 놀랄 것은 없다.[FOMO (Fear Of Missing Out) : 코인이 막 상승 중일 때 지금 사지 않으면 돈을 못 번다는 일종의 강박감에 추격매수하는 것을 이르는 말; FUD (fear, uncertainty and doubt) : 하락장에 막연한 두려움으로 팔아버리는 것을 이르는 말.— 정리자]

[상호적 자기주권(mutual self-sovereignty)—공정하고 정당한 사회정치적 경제의 토대가 되는 핵심 구축물]

경제는 인간의 사회 시스템의 번영 가능성(thrivability)에 강하게 집중해야 한다. 다소 단순화하자면, 번영 가능성의 핵심부에는 집단의 유대(solidarity)와 개인의 주권 사이의 변증법이 존재한다. 그런데 유대와 주권은 사실 동일한 동전의 양면이다. 이 둘은 서로를 구성하며 공생적으로 함께 진화한다. 이 둘은 ‘ 변증법적 특이성 ’ 을 구성하는데, 이는 상호적 자기주권을 통하여 조화에 도달한다. (음양의 상호작용과 같다.) 이 동학에서는 사회적 결속과 개인의 주권이 둘 다 강한 동시에 유동적이다. 이는 도교 철학에서 종종 물의 은유를 사용하여 나타내는 개념이다. 저자의 생각에 이 영속적인 동학을 통하여 인간의 사회 시스템의 ‘ 안티프래질 특성(anti-fragility)이 높아진다. 그리고 자아에 대한 인식과 정체성에 대한 인식이 영속적으로 출현/창발한

다. [‘anti-fragility’ 개념을 만들어낸 탈렙(Nassim Nicholas Taleb)에 따르면 ‘resiliency’(복원력)는 실패로부터 회복하는 능력이고, ‘robustness’(튼실함)는 실패에 저항하는 능력이며, ‘ 안티프래질 특성(anti-fragility)은 스트레스, 휘발성, 소음, 실수, 외부로부터의 공격, 실패의 결과로 번영할 수 있는 능력이 증가하는 속성을 가리킨다.—정리자]

더 나아가, 그리고 더 중요한 점으로서, 그런 모든 게임에서 규칙들은 창발적이고 자기조직적인 방식으로 참여자들에 의해서 시행되고 운용된다. 민중에 의한, 민중을 위한, 민중의 거버넌스이다. 규칙들의 상대성이 존중되어야 하며, 전체적 합의는 필요하지 않다. 만일 이런 합의가 필요하다면 우리는 다시 중앙집중화의 문제로 돌아가게 될 것이다.

이 모든 것이 의미하는 것은, 비트코인과 이더리움은 (특히 이들을 지탱하는 블록체인 기술은) 우리를 우리가 가야 할 곳에 데려다주지 않으리라는 것이다. 이들은 비판적이고 중요한 촉매가 될 수는 있지만, 그 실제 작동에 있어서는 충분하지 않기 때문이다. 처음에 비트코인의 분산된 원장 테크놀로지가 근본적으로 새로운 P2P 경제를 가능하게 하는 과제를 담당할 수단이 되리라는 생각에 고무된 사람들조차 지금은 그 한계를 인식하고 또 인정하고 있다. 따라서 이더리움 관련 개발자들 가운데 돈이 목적이 아닌 사람들은 환멸감을 느끼고 있다.

[홀로체인]

이와 달리 홀로체인(Holochain)은 우리를 우리가 가야 할 곳에 데려다 줄 것이다. 홀로체인은 인류의 역사에서 상호적 자기주권의 문제와 진정으로 씨름한 최초의 테크놀로지이다. 홀로체인의 효율과 효능은 네트워크의 사이즈가 커질수록 향상된다. 사실 홀로체인은 이더리움과 비트코인 이전에 이미 메타커런시(MetaCurrency)와 쎕터(Ceptr) 프로젝트의 필수적 구성부분으로서 등장했다.

홀로체인은 아나키를 출현시킬 수 있는 사회적 기술—생체모방(bio-mimicry)에서 영감을 얻고 소프트웨어에 기반을 둔 기술—을 제공한다. (여기서 아나키란 대규모의 중개/매개intermediation를 필요로 하지 않은 삶을 가리킨다.) 그리하여 홀로체인은 우리가 자산에 기반을 둔 수많은 상호신용 (암호)화폐—이들은 홀로체인에서 상호 운용 가능하다—를 통해 기존의 화폐가 지배하는 시기를 넘어서는 것을 가능하게 한다. 여기서 사용되는 통화(通貨) 정의는 훨씬 더 광범한 것이다. 통화는 가치 · 약속 · 평판의 흐름들을 형성하고 가능하게 하며 측정하는 형식적인 상징체계로서 정의된다. 저자 생각에 이는 하이에크의 사유에 대한 해석으로서 신자유주의적 해석보다 훨씬 더 계몽된 것이다.

모든 종류의 가치 흐름이 더 나은 방향으로 관리되기 전에 먼저 인정되어야 한다.

(GDP 관련 흐름만을 가시화한 것은 인류와 지구에 재앙이 되었다.) 그렇게 인정될 때에만 우리는 상호연관된 긍정적 흐름들은 강화시키거나 증폭시키고 상호연관된 부정적 흐름들은 완화시키거나 제거하는 작업을 창발적이고 자기조직적인 방식으로 시작할 수 있다. 그리하여 다수를 위해, 심지어는 모두를 위해, 더 의미 있고 더 인간적인 부와 번영을 창출할 기반을 만들 수 있다.

[대규모 탈매개(Disintermediation)]

대부분의 사람들에게 홀로체인이 가져올 경제적 및 사회정치적 혁명은 그 긴 역사에도 불구하고 하룻밤 사이에 일어나는 것처럼 보일 것이다. 이는 그것이 디지털화된 세계에서 오픈소스 소프트웨어를 통해 일어나는 것이기 때문이다. 홀로체인은 어떤 규모로든 빠른 속도로, 제로의 한계비용으로 이용될 수 있다. 그것은 라즈베리 파이(Raspberry Pi)에서 스마트폰, 태블릿, 노트북, 심지어는 서버에 이르기까지 그 어떤 컴퓨팅 장치에도 설치될 수 있다.

제일 처음 만들어진 h앱(hApp, Holochain dApp)은 홀로(Holo)이다. 이는 h앱들을 호스팅하기 위한 h앱으로서 홀로퓨얼(Holo Fuel)이라고 불리는 최초의 상호신용 암호화폐를 포함하고 있다. 이 화폐는 h앱들에 여벌의 컴퓨터나 아니면 현재 쓰는 장치의 저장 공간을 제공해주는 홀로 호스트들에게 보상해주는 데 사용된다. 이로 인해 모질라(Mozilla)의 파이어폭스(Firefox) 같은 표준적인 브라우저를 사용하여 웹에서 h앱들에 접근하는 것이 가능하다. 그런데 이런 식의 호스팅을 피할 수도 있다. 홀로체인을 돌리는 장치는 모두 사용자인 동시에 호스트이기 때문이다. 홀로의 목적은 현재의 서버 기반 웹과 미래의 (P2P이기에) 서버 없는 대안적 홀로체인 사이에 다리를 놓는 것이다. 궁극적으로는 메시 네트워킹(mesh networking)[각각의 노드가 직접, 수평적으로 네트워크에 데이터를 중개하는 네트워크 토폴로지. 모든 노드가 다른 모든 노드에 연결되는, 뿌리줄기적 연결방식이다—정리자]이 가능할 것이며, 이는 진정으로 그리고 완전하게 분산된 인터넷과 웹을 의미할 것이다.

더 나아가 홀로체인의 데이터 무결성 모델은 데이터 중심적(data-centric)이기보다는 행위자 중심적((agent-centric))이기를 지향함으로써 상호적 자기주권을 지원한다. 홀로체인은 소스체인(행위자가 소유하는 해시체인hashchains을 생각해보라)과 디지털 서명을 사용하고 분산된 해시 테이블을 확증한다(비트토렌트BitTorrent와 깃허브GitHub를 생각해보라). 이렇게 해서 프라이버시와 기밀성이 보장될 뿐만 아니라 가치실현과 가치소유가 가치를 추출하여 화폐화하려는 중개자들 · 대표자들 · 경영자들 · 조직소유자들이 아니라 현장에서 실제로 가치를 창출하는 사람들에게 완전히 귀속된다.

[궁극적 물음]

상호적 자기주권은 일단 작동 가능하고 실용적이며 어디에나 존재하게 되면 우리 삶의 모든 측면(사회적 · 정치적 · 경제적 · 예술적 · 문화적 측면)을 다시 규정하게 될 것이다. 가장 심층적 차원에서는 우리가 우리의 삶의 방향과 관련하여 스스로에게나 서로에게, 같은 세대 내에서나 서로 다른 세대 간에 하는 이야기들의 성격이 완전히 변할 것이다. 여기에 쎕터와 쎕터에 기반을 둔 인공지능은 말할 것도 없고 발전된 심층 및 강화 학습 인공지능이 가세하면 우리는 궁극적으로 21세기에 인간이 된다는 것이 진정으로 무엇을 의미하는지를 다시 파악하고 다시 정의하게 될 것이다.