



블록체인 프로젝트가 놓치고 있는 문제

2007년부터 미국경제는 서브프라임 모기지(Subprime Mortgage) 사태로 인해 휘청거리기 시작해 2008년 리먼 브라더스의 파산을 계기로 뿌리째 흔들리게 된다. 세계 4위의 IB였던 리먼 브라더스는 뉴욕 연방법원에 파산보호를 신청하고 당대 경제 시스템의 주축을 이루는 매릴린치, AIG 등의 기업들 역시 연이어 인수, 파산하게 된다. 대출의 원금을 갚을 수 없는 서민층, 중산층들은 기업들이 줄줄이 파산해 악순환의 고리를 겪었으며 많은 사람들이 일자리를 상실하고 집을 잃었다.

글_황병대



부동산 거품의 붕괴로 가계 자산 19조 200억 달러가 순식간에 증발했으며 기업이 무너졌다. 이런 파생상품을 산 기업들은 물론이며 중국 등의 내수 위주 신흥부국을 제외하곤 수출과 금융으로 먹고 살던 국가들 역시 무너졌다. 이에 미국은 2008년 10월 7000달러 규모의 부실자산매입프로그램(TARP)을 통한 구제금융 계획을 발표했고 그들의 탐욕이 부른 사태를 국민의 혈세로 막기 시작했다. 하지만, 이에 그치지 않고 기업들의 CEO와 임원들이 보너스 파티 등으로 배를 불려가는 모습에 국민들은 분노할 수 밖에 없었다. 이런 신자유주의의 문제가 극명화해진 시점에 나타난 것이 사토시 나카모토의 Bitcoin: A Peer-to-Peer Electronic Cash System 백서다.

나카모토의 백서는 시대의 흐름에 맞게 등장해 빛을 발했다. 탈중앙 경제 시스템과 이것을 가능하게 하는 시스템 구성은 많은 개발자와 사상가가 공감했으며 2008년 11월 9일 비트코인(Bitcoin) 프로젝트가 SourceForge.net에 등장하고 불과 2개월 만인 다음 년 1월 3일 Genesis Block이 피어를 통해 전달됐다. 이 디지털 암호화폐 시스템은 진정한 공유 경제 세상이 가능함을 증명하는 서막을 열었으며 기존의 중앙집중적인 지배 구조를 깨버리는 '운동(Movement)'이 됐다.

두 대의 컴퓨터와 Genesis Block으로 시작된 비트코인 코어 프로그램은 글을 쓰는 2018년 10월 3주차 현재 1만66개의 노드가 참여하고 있다. 이 놀라운 결과가 가능한 이유는 세계의 문제를 정확하게 지적하고 이행된 운동이기 때문이다. 세계 경제 시스템에 대한 비판론과 오픈 진영의 힘은 시스템 확장에 불을 붙였고 현재의 가치를 만들 수 있었던 근본적인 이유라 할 수 있다.

코어(Core) 소프트웨어 프로그램의 실행을 통해 참여 가능한 시스템은 스스로 규모를 성장시켜 나갔다. 참여자 서로가 거래에 대한 증명을 했으며, 나름의 이유 있는 게임을 통해 정해진 통화를 발행했다. 멀리서 보면 단순히 통화를 발행하고 거래 내역 명세를 교환, 검증, 저장하는 것이 이 시스템이다. 하지만 이 프로젝트가 담고 있는 의미는 상당히 복잡하다. 개발된 코어 소스 코드의 복잡도를 말하는 것이 아니다. 탄생에 대한 이유가 대단했으며 너도 나도 '탈중앙화'에 대한 운동에 참여하고 있기 때문이다. 아마 신뢰 사회에 대한 의문이 없었다면 비트코인은 그저 복잡한 구조를 가진 포인트 시스템이 됐을 가능성이 크다. 비트코인의 탈중앙화 운동에 대한 역할은 금융 시스템에 한정된 것은 아니었다. 이 운동을 시작으로 많은 오픈 진영 팀과 개발자들이 다양한 가치에 가상화폐를 연결하기 시작했고 컬러드코인(ColoredCoin), 네임코인(NameCoin), 메타코인(MetaCoin) 등의 프로젝트들이 존재했다. 비트코인을 화폐 외의 가치와 연결하기 시작했으며 다양한 도전들이 존재했다. 이런 도전의 움직임 중 탄생한 프로젝트의 대표격은 비탈린 부테린(Vitalik Buterin)의 이더리움(Ethereum) 프로젝트다. 비트코인 프로젝트에서 활동하던 그는 비트코인의 스크립트(Script) 언어를 활용한 문제 해결 방법에 다른 방안을 제시했고, 그것이 지금의 스마트 컨트랙트(Smart Contract)가 됐다. 이것은 단순히 암호해독을 통해 화폐의 소유를 검증하는 방법이 아닌 튜링 완전한(Turing Completeness) 언어를 제공해 참여자가 불변하는 시스템을 만들어 공유하는 것을 그려냈다. 이것은 탈중



황병대

인공지능을 접목한 블록체인 DAIOS 프로젝트 진행 중 (현), 인공지능&블록체인 전문 개발회사 DAIB의 CTO(현), 외주 블록체인 컨설팅 및 개발 프로젝트 진행, 모의해킹, 국/외산 솔루션 엔지니어, 보안 솔루션 개발 등 7년차 보안 엔지니어, 블록체인의 기술과 철학을 공유하는 커뮤니티와 스타터를 운영 중

양화 운동의 한 획을 그은 운동이 되었다. 2014년 참여자에게 이더(Ether)를 분배하는 식으로 크라우드소싱(Crowdsourcing)이 진행됐고 2015년부터 동작하기 시작한 이 프로젝트는 현재 어떠한 블록체인 프로젝트보다 활발하게 성장하고 있다. 비트코인과 이더리움은 각각 1세대, 2세대 블록체인이란 수식어가 붙어있다. 당당하게 세대를 구분할 만한 혁신적인 운동이 있었기 때문이다. 이 운동에는 탈중앙화란 강력한 메시지가 붙어있었으며 많은 사람에게 감동을 주어 빠르게 성장했다. 하지만, 지금의 블록체인 업계는 이것을 놓치고 있다는 생각이 많이 든다. 과도하다 싶을 정도로 많은 프로젝트가 나타났고 무분별한 ICO(Initial Coin Offering)가 진행됐다. 탈중앙화라는 핵심적인 가치를 지닌 가상화폐 시스템에 중앙화된 거래소가 등장해 많은 이윤을 가져갔으며, 2016년부터 뜨거워지기 시작했던 수 많은 선동들과 감동 없는 이코노미(Economy) 시스템이 시장의 가능성을 선점해 가져갔다. 그렇게 점점 엇나간 운동의 모습은 탈중앙화의 가치를 열려갔다.

금융자산으로 매치하기 힘든 가치를 가상화폐로 풀어내는 것은 의미 있는 일이다. 하지만 지금의 수 많은 공모 프로젝트, 지금은 하나의 트렌드로 잡힌 리버스(Reverse) ICO들을 보면 많은 의문이 든다. 꼭 그렇게 대규모의 캡(Cap)으로 프로젝트가 진행돼야 하는 것일까. 꼭 블록체인으로 시스템화 돼야 하며 릴리즈(Release)된 프로그램이 기존의 시스템에서 사용자의 이주를 유도할 수 있을 것인가. 대부분의 이런 프로젝트가 투자자의 수익성에 맞춘 그저 돈을 안겨줄 시큐리티(Security)에만 포장이 돼 있다. 시스템을 공정하게 하는 것보다 운영되는 네트워크 내에서의 양털깎기에 눈이 멀어버린 것이다. 이런 프로젝트에 어떤 참여자가 붙을 것이며 또 함께 개발해 가치 있는 시스템으로 나아갈 것인지 탈중앙화된 세상에서 살아갈 우리는 날카롭게 지켜볼 필요가 있다.

업계 여러 사람들은 1세대, 2세대 코인 프로젝트가 가지고 있는 속도와 용량문제, 에너지 효율성에 대한 문제해결을 목표로 진행되는 프로젝트를 3세대 코인 프로젝트라 부르고 있다. 대표적인 프로젝트로 이오스(EOS)가 있으며 암호화폐에 관심이 있다면 모두가 들어봤을 프로젝트이다. 이오스는 성공에 대한 경험이 존재하는 설계자 댄 라리머(Dan Larimer)가 진행하는 프로젝트로 신뢰와 투자 수익에 대한 기대감으로 40억 달러라는 엄청난 규모의 공모를 달성한 이력이 있다. 중요한 것은 론칭(Launching) 시점에 확인된 코인 분배 결과인데, 전체 코인 발행량의 절반 가까이가 10개의 계좌에 몰려있었다는 것이다. 이오스와 같이 지분을 통해 블록 생성자가 결정되는 구조에서는 치명적인 중앙화 문제를 내포하고 네트워크가 시작되는 것이다. 이는 이오스만의 문제가 아니다. 많은 메인넷(Main Net) 프로젝트가 tps(Transaction Per Second)를 올리기 위해 지분 증명 형식으로 합의 알고리즘을 구성하며 설계를 한다. 하지만 이미 공모 단계에서 수 많은 양의 코인들이 실물 경제 상위 층에 속하는 사람들이 소유하게 되며 공정해야 할 블록체인 네트워크가 중앙화되어 단합을 야기한다. 뿐만 아니라 블록에 대한 보상 역시 편중화 되어 '부익부 빈익빈'이 너무나도 명확하게 그려진다.

많은 개발자들이 속도와 용량문제, 에너지 효율성 등의 기능적인 해결안을 제안하는 블록체인 프로젝트를 3세대 코인으로 규정해야 하는 지에 대한 의문을 가진다. 물론 이런 문제를 해결하면 블록체인 시스템이 기존 시스템을 대체 하는 많은 변화를 이룰 수 있을 것이다. 하지만 2세대의 크립토 3.0의 모습에는 이미 이러한 것들이 모두 포함돼 주류 시스템을 대체할 수 있는 제안이 됐고 많은 기술적 도전이 계속되고 있다. 그렇기에 탈중앙화를 버린 기능적 해결 만으로는 세대 교체의 제안이 힘들며 투자자의 수익을 앞당길 것 같다는 심리적 기대감 외에는 감동이 없다. 이런 현상의 근본적인 문제는 아마 코인 자체가 가지는 '증권성'에 있을 것이다. 무분별하게 각 팀의 기준으로 공모가 진행이 됐으며 거의 대부분의 프로젝트가 투자자 위주로 세일즈를 해왔다. 과도한 보너스 코인, 에어드랍(AirDrop) 그리고 마케팅, 상장피 등 실제 탈중앙화 네트워크의 행동 유도와 보상으로 쓰여야 할 코인 가치가 쓸데 없이 낭비가 됐다. 이런 무너진 경제 시스템은 우리가 지적할 필요가 있다. 코어는 개발자가 만들지 투자자가 만들지 않는다.

블록체인은 끝이 없는 가치를 가진 성장 기대형 기술이다. 중앙 제어되지 않는 신뢰 평가가 가능한 시스템 속에서 우리의 노동의 가치가 온전히 인정받을 수 있기 때문이다. 그렇기에 '탈중앙화'가 무너진 네트워크는 의미가 없으며 참여자를 기대할 수 없고 발행되는 코인 역시 가치가 없다. 만약 가치 있는 코인을 얻고 싶다면 그것이 얼마나 탈중앙화 된 생태계를 지향하고 있는지 그리고 비트코인, 이더리움 이후 혁신적인 세상을 만들 수 있는 새로운 '운동'을 불러일으킬 것인지를 지켜볼 필요가 있다. ☺

