03

정 재 웅*
블루팬넷 CFO

암호화폐의 역사와 기술, 그리고 분산금융

금융위기 직후인 2008년 10월 31일, 사토시 나카모토(Satoshi Nakamoto)라는 이름의 사람이 인터넷에 "Bitcoin: A Peer-to-Peer Electronic Cash System"이라는 제목의 문서를 공개했다. 이 문서는 중앙은행 혹은 다른 금융중개기관(Financial Intermediaries) 없이 개인과 개인이 자유로운 금융 거래를 할 수 있는 방법을 제시했다. 비트코인은 글로벌 금융위기 이후 중앙은행과 정부에 불만을 가진 사람들을 대상으로 급격하게 퍼져나갔으며, 이러한 사람들의 기대와 열망은 암호화폐 버블로 표출되었다. 이러한 버블의 붕괴에도 불구하고 암호화폐의 기술의 발전은 현재 진행형이고, 블록체인 기술을 금융과 접목하려는 시도 역시 지속적으로 이루어지고 있다. 블록체인 기술을 이용하면 해킹이나 위·변조를 막을 수 있어 금융에 있어 필수적인 신뢰를 향상시킬 수 있기 때문이다. 이러한 블록체인 기술은 다음의 셋에 기반을 두고 있다 : 채굴과 보상을 통한 인센티브, 비잔틴 장군 문제(Byzantine Generals Problem) 해결을 위한 작업 증명, 그리고 블록체인 분산원장을 통한 기록의 보관. 그러므로 이러한 블록체인 기술의 원리를 알아보고, 암호화폐 산업에서 이루어지는 탈중앙화 금융 시도에 대한 연구는 앞으로 금융이 발전하는 데 상당한 시사점을 줄 수 있다.

※ 본고의 내용은 필자의 개인 의견으로 한국주택금융공사의 공식적인 견해와 다를 수 있습니다.

* 아주대학교 대학원 금융공학과에서 박사학위를 받고 현재 블록체인 핀테크 스타트업인 블루팬넷에서 CFO로 재직 중이다. (yanwenry1333@gmai.com)

I. 서론

성경에 보면 "처음에는 보잘것없겠지만 나중에는 훌륭하게 될 것일세"[1]라는 구절이 있다. 일반적으로 대기만성을 의미하는 구절로 많이 사용되곤 하는데, 2019년 10월 12일 현재 시가총액 178조에 달하는 비트코인이나 여기서 파생된 다른 암호화폐 역시 이 말이 적용된다고 할 수 있다. 그 시작이 정말로 단순하고 미약했기 때문이다. 금융위기 직후인 2008년 10월 31일, 사토시 나카모토(Satoshi Nakamoto)라는 이름의 사람이 인터넷에 "Bitcoin: A Peer-to-Peer Electronic Cash System"이라는 제목의 문서를 공개했다. 이 문서는 중앙은행 혹은 다른 금융중개기관(Financial Intermediaries) 없이 개인과 개인이 자유로운 금융 거래를 할 수 있는 방법을 제시했다. 3개월이 지난 2009년 1월 3일, 사토시 나카모토는 비트코인의 제네시스 블록(Genesis Block)을 생성했고, 그 다음날에는 C++로 만들어진 비트코인의 소스코드를 이메일로 다수의 사람에게 배포했다. 비트코인의 최초 50개 채굴자는 사토시 나카모토고, 그에 이어 채굴을 한 사람은 사토시 나카모토에게 10 비트코인을 송금받은 할 피니(Hal Finny)다. 만약 할 피니가 없었다면 비트코인, 그리고 그에서 파생된 암호화폐는 시작할 수조차 없었을 것이다.

이처럼 초라하게 시작한 비트코인은 현재 대표적인 암호화폐가 되었고, 이후 나온 모든 암호화폐 혹은 블록체인 토큰은 비트코인의 블록체인 메커니즘에서 분기되어 탄생했다. 즉 비트코인은 모든 암호화폐의 기원이다.[2] 그렇기에 거의 모든 암호화폐는 채굴이라는 과정을 거쳐서 사용할 수 있으며, 블록에 기록된 거래가 최종적으로 승인되기 위해서는 합의 알고리듬을 거쳐 승인을 받아야 하고, 이러한 내역은 분산원장에 기록되기에 시스템에 참여한 모든 사람이 열람할 수 있으며, 위조나 변조가 불가능하다. 이러한 이유에서 비트코인을 비롯한 암호화폐는 금융시장을 혁신할 수 있으리라는 기대를 사람들로 하여금 갖게 했지만, 아직까지 그 혁신은 요원한 실정이다. 금융시장 참여자 및 일반 시민의 위와 같은 금융 혁신에 대한 기대와 열망이 표출된 사건이 지난 2017년 하반기에 시작되어 2018년 상반기에 꺼진 비트코인 버블이다. 2017년 1월 1일, 1 비트코인의 가격은 972.95 달러에 불과했으나, 곧 가파르게 상승하여 2017년 12월 17일에는 무려 19,535.70 달러가 되었다. 하지만 이후 가격은 다시 곤두박질쳐서 2018년 2월 7일에는 7,386.63 달러까지 하락했다. 이러한 극적인 상승과 하락은 비트코인을 비롯한 암호화폐와 이들이 기반한 블록체인 기술이 금융시장을 혁신하고 더 나아가 일상에서 상거래를 혁신할 수 있으리라는 시장 참여자의 기대의 변화를 보여준다고 할 수 있다. 물론 이에는 비이성적 과열(irrational exuberance), 투기심리, 군중심리 등도 포함되어 있다.

하지만 암호화폐에는 이를 단순하게 한때의 버블로만 볼 수 없는, 금융시장에 대한 여러 시사점이 존재한다. 암호화폐가 탄생하게 된 배경이 2007년 글로벌 금융위기이기 때문이고, 암호화폐가 기반한 기술이 금융시장에서 활발하게 논의되고 있으며, 페이스북에서 추진하는 프로젝트인 리브라(Libra)를 둘러싼 미국 의회와 규제당국의 반응에서 알 수 있듯이 암호화폐의 지급결제 기능은 여전히 논란의 중심에 있다. 그리고 무엇보다 최근 암

1) 공동번역성서, 욥기 8장 7절.
2) 예를 들어 이더리움 역시 비트코인의 소스코드에 기초한 암호화폐다.

호화폐에서 부상하고 있는 기능은 탈중앙화 금융(Decentralized Finance, DeFi)이다. 암호화폐 버블 여부와 상관없이 진행되고 있는 이러한 여러 논의는 결국 금융시장의 혁신과 연결된다. 금융위기로 인해 기존 금융 시스템에 대한 일반 대중의 불신이 초래되었고, 그 결과 탈중앙화를 기치로 내세운 비트코인을 비롯한 암호화폐가 등장하게 되었으며, 금융시장은 이러한 블록체인을 수용하여 어떻게 혁신을 이끌어낼지 지속적으로 연구하고 있으며, 암호화폐는 다시 기존 금융의 기능을 대체할 수 있는 탈중앙화 금융을 추진하는 등 암호화폐와 금융시장의 상호 혁신은 현재 진행형이다.

그러므로 이 연구에서는 상기한 암호화폐의 역사와 기술, 그리고 분산금융에 대한 논의를 진행하고, 이러한 기술이 주택금융에 끼치는 영향에 대해 분석하고자 한다. 2장에서는 먼저 비트코인을 비롯한 암호화폐가 나오게 된 배경인 2007년 글로벌 금융위기에 대해 간략하게 알아보고, 3장에서는 비트코인과 이더리움을 비롯한 암호화폐의 기술적 메커니즘에 대한 논의를 진행할 것이다. 이어서 4장에서는 암호화폐의 금융시장 혁신 시도인 탈중앙화 금융에 대해 살펴본 후, 5장에서 주택금융에 끼치는 영향을 다각도로 생각해보고 결론을 내리는 순서로 진행하고자 한다.

II. 암호화폐 등장의 기원 : 2008년 글로벌 금융위기

비트코인에서 시작되는 암호화폐와 금융시장에 끼친 영향을 살펴보기 이전에, 우리는 왜 이러한 디지털화된 자산 혹은 화폐가 나올 수밖에 없었는지를 먼저 살펴보아야 한다. 그래야만 암호화폐의 기술과 지향하는 바를 명확하게 알 수 있기 때문이다. 그리고 그 시작은 2008년 글로벌 금융위기다.

주지하다시피 금융위기는 2008년 9월 투자은행 리먼 브라더스(Lehman Brothers)가 파산하면서 시작되었다. 리먼 브라더스의 파산은 비우량주택담보대출(Sub-Prime Mortgage) 부실로 인한 주택담보대출의 채무불이행에서 비롯되었고, 이 비우량주택담보대출의 부실은 연방준비은행이 2000년대 초반부터 이어온 저금리를 2007년 9월부터 인상한 데서 비롯되었다.

그렇다면 우리는 먼저 왜 미국 연방준비은행이 저금리 기조를 장기간 유지해왔는지를 살펴보아야 한다. 이에 대해서는 시카고 대학교 경제학과 교수이자 전 인도 중앙은행 총재인 라구람 라잔(Raghuram Rajan)이 그의 저서 "폴트라인(Fault Line)"에서 정치적 이유라고 밝힌 바 있다. 미국 연방정부와 연방준비은행은 경기를 부양하기 위해 인위적 저금리 정책을 펼쳤는데, 이 인위적 저금리 정책의 연장선상에서 그 전까지는 주택담보대출을 받을 수 없었던 저신용자 계층을 대상으로 한 비우량주택담보대출이 활성화 되었다. 정부와 연방준비은행의 인위적 저금리 정책으로 인해 비우량주택담보대출은 대부분 변동금리로 계약되었는데, 연방준비은행이 금리를 인상하자 이들이 채무를 변제할 수 없게 되어 위기가 시작되었다.

그렇다면 왜 연방준비은행의 금리 인상이 문제를 야기했는가. 그 이유와 과정에 대해서는 프린스턴 대학교의 아티프 미안(Atif Mian)과 시카고 대학교의 아미르 수피(Amir Sufi)가 공저한 "빚으로 지은 집(House of Debt)"에 설명되어 있다. 아티프 미안과 아미르 수피에 따르면, "미국인들에게 홈 에쿼티(home equity, 소유하

고 있는 주택 가격에서 부채를 뺀 금액)는 유일한 재산인 경우가 많다."[3] 그렇기 때문에 주택 가격이 하락하게 되면 이는 곧 상당수 미국인들에게 그들이 보유한 유일한 자산 가격이 하락함을 의미하며, 이와 같은 자산 가격 하락은 주택 구입 과정에서 차입금을 많이 사용한 저신용계층이나 저소득계층일수록 더 심해진다. 예를 들어 저축 1만 달러와 이를 바탕으로 한 4만 달러의 모기지 대출을 이용해 5만 달러의 주택을 구입한 저소득층 주택 구매자의 경우를 살펴보자. 만약 주택가격이 20% 하락해서 4만 달러가 될 경우, 이 사람의 홈 에쿼티는 0이 된다. 주택 가격과 모기지 대출 금액이 동일해지기 때문이다. 이처럼 대출자의 자산 가치가 0이 되는 상황에서도 모기지 대출을 해준 금융회사와 이 금융회사에 자금을 공급한 예금주는 대출자의 자산 가치 하락과 상관없이 4만 달러의 대출금을 그대로 회수할 수 있다.[4] 이를 통해 우리는 주택 가격이 급격하게 하락하는 상황에서 주택담보대출은 가난한 채무자에게 모든 위험을 전가하며, 금융기관 혹은 여기에 자금을 공급한 예금자는 거의 위험을 부담하지 않음을 알 수 있다. 금융위기 상황에서 가난한 사람이 더 큰 위험을 부담한 것이다. 하지만 문제는 이게 끝이 아니다. 주택 가격의 하락은 단순히 자산 가격의 하락으로 끝나지 않고 저소득층이 직장을 잃고 소비를 줄이는 또 다른 재앙으로 이어진다. 그렇다면, 위기의 상황에서 저소득, 저신용 계층의 상황을 더욱 악화시키는 부채가 확산된 이유는 무엇인가.

2001년 미국 연방준비제도 이사회 의장 앨런 그린스펀은 향후 연방준비제도의 금리 기조에 대해 다음과 같은 발언을 한다 : "The FOMC stands prepared to maintain a highly accommodative stance of policy for as long as needed to promote satisfactory economic performance." 앨런 그린스펀의 이 발언은 연준이 경제활동을 촉진하기 위해 저금리 기조를 상당 기간 유지할 것임을 시사하였고, 이에 금융시장은 합당하게 반응했다 – 미국 국채를 대신할 수 있는 다른 투자자산을 찾기 시작했다.

금융시장이 발견한 새로운 투자자산 중 하나는 부채담보부증권(Collatralized Debt Obligation, CDO)이다. 주택담보대출은 집을 구입하고자 하는 사람에게 비교적 낮은 금리로 10년 이상 장기에 걸쳐 대출을 제공하는 상품인데, 이자율이 낮고 상환기간이 길기에 채무자 입장에서 안정적으로 이자와 원금을 상환할 수 있을 뿐만 아니라, 채권자 입장에서도 채무불이행 사태가 발생할 경우 주택을 차압하여 다시 경매를 통해 판매할 수 있어서 손실을 최소화할 수 있다. 하지만 이러한 장점에도 불구하고 채권자인 은행에게는 문제 하나가 발생하는데, 이는 대출과 상환 간 불균형이다. 이러한 비대칭 문제를 해결하기 위해 은행은 자산유동화증권(Asset Backed Security, ABS)의 한 종류인 주택담보대출저당증권(Mortgage Backed Security, MBS)을 발행한다. 이 증권을 발행함으로써 은행은 증권 금액을 받고 거래에서 완전히 빠질 수 있게 되며, 채무자가 지급하는 원금과 이자는 주택담보대출저당증권을 구입한 투자자에게 지급된다. 그런데 마찬가지로 이러한 주택담보대출저당증권을 구입한 투자자 역시 투자금과 상환금의 불일치 문제를 해결하기 위해 다시 이를 기초자산으로 한 증권을 발행하는데, 이게 상술한 부채담보부증권이다. 이러한 파생금융상품은 주택담보대출이 신용도가 높은 프라임 등급 대출자에게 한정되어 이루어졌을 때까지만 해도 높은 수익률을 보장하는 안정적인 금융상품이었다.

3) Mian, Atif. and Amir Sufi, House of Debt, The University of Chicago Press, 2014(한국어판, 박기영 옮김, 『빚으로 지은 집』, 열린책들 2014), pp. 34.
4) Mian, Atif. and Amir Sufi, ibid, pp. 34-35.

문제는 저신용자를 대상으로 한 서브프라임 주택담보대출이 이루어지면서 시작되었다. 서브프라임 주택담보대출이 활성화되기 이전에는 주택담보대출을 받기 위해서 소득 증명과 자산 증명이 필요했다. 그런데 서브프라임 주택담보대출이 활성화되자 은행은 이를 소득 선언과 자산 증명으로 완화했다가, 나중에는 소득 선언과 자산 선언으로 변경했다. 즉 저신용자는 자신의 수입과 자산을 증명하는 서류를 준비할 필요 없이 자신이 대출을 상환할 수 있는 충분한 수입과 자산이 있다고 서류에 명시하는 것만으로 주택담보대출을 받을 수 있게 되었고, 드디어 나중에는 NINA(No Income, No Asset) 대출까지 등장하게 되었다.

이러한 허술한 주택담보대출 시스템에서 발생하는 문제를 더 심화시키는 일이 주택담보대출에 기반한 파생금융상품 설계에 적용되었다. 금융회사는 트랜칭(Tranching)과 풀링(Pooling)을 사용하여 투기등급의 부채담보증권을 투자등급으로 만들 수 있었다. 부채담보증권도 금융상품이니만큼 신용평가를 받고, 투자등급부터 투기등급까지 다양하게 평가를 받는다. 트랜칭은 최소한 하나 이상의 투기등급 증권에 대해 이 증권이 높은 신용등급을 받도록 하여 자본조달비용을 절감하는 것인데, 이를 위해 가장 많이 활용된 방법이 신용보강(Credit Enhancement)이다. 신용보강은 기대손실 규모를 파악한 후 이러한 기대손실에도 불구하고 원리금 가치가 유지될 수 있도록 신용등급을 향상시키는 방법인데, 가장 대표적인 구조가 'Senior-Mezzanine-Equity'로 구분하는 것이다. 이 구조에서 후순위인 Equity는 모든 신용위험을 부담하게 되지만, 선순위인 Senior는 원리금 상환을 보장받을 수 있다. 어처럼 불리한 조건인 후순위부채담보증권도 풀링을 통해 위험의 성격이 바뀐다. 예를 들어 하나의 Equity가 10퍼센트의 확률로 100% 손실을 입는다면, 10개의 Equity를 풀링하면, 각 Equity의 부도확률이 상호 독립이라는 가정 하에, 이 풀링 상품의 부도 확률은 0.00000001%로 낮아진다. 투기등급 상품이 풀링이라는 단순한 과정을 거쳐 투자등급 상품이 되는 것이다. 게다가 이론적으로는 상술한 트랜칭과 풀링을 반복하면 부도 위험이 낮은 안전한 파생금융상품을 지속적으로 만들 수 있다.

문제는 상술한 후순위 증권의 부도확률이 완전히 독립적이지도 않고, 외부 요인의 변화에 극히 취약하다는 데 있다. 그리고 그 외부 요인의 변화에서 야기된 충격이 가해지자 우리가 아는 2008년 금융위기가 발생했다.

2007년 9월 금리 인상으로 인해 비우량주택담보대출의 부도가 증가하였고, 이러한 비우량주택담보대출을 기초자산으로 한 파생상품에 가장 많은 투자를 한 금융회사가 리먼 브라더스였다. 이러한 파생상품 투자에서 야기된 부실로 인해 리먼 브라더스는 2008년 9월 14일 파산했다. 하지만 이게 끝이 아니었는데, 리먼 브라더스에서 발행한 CDS를 가장 많이 인수한 회사가 미국 굴지의 보험사 AIG이기 때문이다. "자산이 1조 달러가 넘는 AIG는 리먼보다 규모가 50% 이상 더 컸다. 이 회사는 130개국 이상에서 영업을 했고, 세계적으로 7,400만이 넘는 개인과 법인 고객들을 확보하고 있다. AIG는 미국 근로자 총수의 3분의 2에 해당하는 1억 600만 명을 고용한 18만 개의 중소기업 및 여타 법인체에 상업보험을 제공하고 있었다. 이 회사의 여러 가지 보험 상품들은 수많은 지방자치체와 기금을 보호하고 401(k)에 가입한 사람들을 보호했다. AIG의 붕괴는 미국과 해외 양쪽에서 더 많은 초대형 금융회사들의 도산을 촉발할 가능성이 농후했다."[5] 결국 미국 연준과 재무부는 더 큰 금융위기를 막기 위해 의회의 반대에도 불구하고 AIG에 대한 구제금융을 결정한다. 하지만 AIG의 파산 보호 신청 소식

5) Bernanke, Ben S., op. cit, pp. 11.

에 주식시장은 패닉에 빠졌고, 여파는 포드, 크라이슬러, GM 등 대기업에까지 전파되었다. 이에 미국 연준은 채권시장에서 미국 재무부 채권을 직접 매입하는 양적완화를 세 차례에 걸쳐서 실시하게 되었다. 이러한 구제금융과 양적완화를 통해 미국 연준과 재무부는 금융위기를 수습하고 경제를 다시 활성화시킬 수 있었지만, 일각에서는 중앙은행과 정부가 주도하는 통화 정책이 화폐 가치의 불안정을 가져온다는 불만을 갖게 되었는데, 이러한 불만을 가진 사람들을 시작으로 암호화폐가 주목받기 시작했고, 그 경과는 우리가 아는 바와 같다.

III. 암호화폐와 그 기술

금융위기의 발생과 그 극복과정에서 구제금융과 양적완화를 비롯한 정부의 정책은 금융위기로 인해 야기될 수 있는 경기침체를 예방하는 데 분명 큰 역할을 했지만, 그와 반대로 일반 납세자 중 일부는 자신의 세금이 금융위기를 야기한 대기업을 구제하는 데 사용되거나 혹은 양적완화를 통한 경기부양에 사용되는 데 불만을 품게 되었다. 금융위기 발생과 극복 과정에 대한 소수의 이러한 불만은 다시 중앙은행이 화폐를 발행하고 통제하는 현행 법정화폐 시스템과 미국 달러화가 기축통화로 기능하는 국제 금융 시스템에 회의로 연결되었고, 그 결과 비트코인이 등장하게 되었다.

사실 비트코인 이전에도 이와 비슷한 시도는 많았다. 1980년대 데이비드 차움(David Chaum)은 거래 당사자 간 신원을 모르는 상태에서도 거래가 가능한 익명 거래 시스템을 제안했고, 이를 바탕으로 하여 1990년에 digicash라는 회사를 설립했으나, 기술적 한계와 사회적 여건의 미비로 인해 1998년 회사가 파산하였다. 한편 1993년 미국의 수학자 에릭 휴즈(Eric Hughes)는 티모시 메이(Timothy May), 존 길모어(John Gilmore)와 함께 사이퍼펑크 선언[6]을 발표하고 국가와 대기업으로부터 프라이버시를 보호할 수 있는 암호화된 거래 시스템을 제안했다. 이러한 사이퍼펑크 사상에 기반하여 1997년에는 아담 백(Adam Back)이 Hashcash라는 가상화폐를 만들었고, 1998년에는 웨이 다이(Wei Dai)는 B-Money라는 가상화폐를, 닉 재보(Nick Szabo)는 bit gold라는 가상화폐를 각각 제안했으나, 기술적 한계로 인해 모두 무산되었다.

이러한 실패의 기반 위에 상술한 바 있듯이 2008년 10월 31일 사토시 나카모토라는 가명을 사용하는 사람에 의해 비트코인 백서가 발표되었고, 2009년 1월 3일 비트코인의 제너시스 블록이 생성되었다. 하지만 이후에도 상당히 오랜 기간 비트코인은 지불 수단으로서 기능하지 못하고 데이터상으로만 채굴되어 보관되는 존재에 불과했으나, 2010년 5월 소위 '비트코인 피자데이'[7]로 불리는 작은 사건을 통해 지급결제 수단으로 사용될 수 있음이 증명되었고, 비로소 가격 상승과 투자자 간 거래가 시작되었다.

6) 사이퍼펑크는 중앙화된 국가나 권력구조에 저항하는 사회운동으로 그 근간은 암호화 기술이다. 암호를 뜻하는 단어인 cipher를 cypher로 바꾸고, 그 뒤에 권력에 대한 저항을 의미하는 punk를 붙여서 만든 단어다. 이 사이퍼펑크 운동의 기본 강령인 사이퍼펑크 선언은 프라이버시를 위한 암호기술의 활용과 개발을 주로 언급하고 있다.

7) 비트코인 피자데이는 5월 22일이다. 2010년 5월 22일 미국 플로리다에 거주하는 라스즐로 한예츠(Laszlo Hanyectz)라는 프로그래머는 당시 가격으로 40달러에 해당하는 10,000비트코인을 이용하여 피자 두 판을 구입했는데, 이 사건으로 인해 사람들은 비트코인이 현실에서의 결제에도 사용될 수 있다는 사실을 알게 되었고, 이때부터 비트코인 가격이 폭등하기 시작했다. 이후 암호화폐 시장 참여자들은 이 날을 비트코인 피자데이라 명명하고 기념하고 있다.

이전의 다른 가상화폐와 달리 본격적인 지급결제 수단이자 투자자산이 되었을 뿐만 아니라 암호화폐라는 신조어까지 탄생시킨 비트코인의 기술은 크게 다음의 셋이다 : 채굴과 보상을 통한 인센티브, 비잔틴 장군 문제(Byzantine Generals Problem) 해결을 위한 작업 증명, 그리고 블록체인 분산원장을 통한 기록의 보관.

먼저 채굴과 보상을 통한 인센티브부터 살펴보자. 비트코인을 비롯한 암호화폐뿐만 아니라 모든 화폐는 많은 사람의 사용을 통해 보편성을 획득해야만 가치를 지닌다. 한 주권국가의 법정화폐는 중앙은행이 발행하고 그 가치 유지를 보증하기 때문에 화폐로서 받아들여지고 가치가 유지된다. 만약 중앙은행이 발행하더라도 가치 유지에 대한 신뢰가 붕괴된다면 그 국가의 화폐는 가치를 상실하는데, 대표적인 예가 짐바브웨다. 이코노미스트 보도에 따르면 짐바브웨의 인플레이션은 2008년 사분기에만 7.3×10^{22}% 폭등했다.[8] 짐바브웨의 예처럼 부정부패로 인한 정치 불안정, 경제정책 실패로 야기된 경기침체, 그리고 이로 인한 정부 및 중앙은행 정책에 대한 신뢰 붕괴는 화폐 가치의 붕괴를 가져온다. 그렇기에 화폐 가치의 유지를 위해서는 무엇보다 중앙은행과 정부 정책에 대한 신뢰가 전제되어야 한다. 2007년 글로벌 금융위기에도 불구하고 미국 달러화가 글로벌 기축통화로 기능하는 이유는 미국이라는 초강대국과 연방준비제도에 대한 신뢰가 있기에 가능하다. 그렇다면 이러한 국가와 중앙은행에 의한 화폐 독점에 반대하는 암호화폐는 어떻게 가치를 유지할 수 있는가. 그 답이 채굴과 보상을 통한 인센티브 메커니즘이다. 비트코인은 채굴이라는 과정을 거쳐 획득되는데, 채굴은 SHA-256[9]해시 알고리듬에 따라 정해진 문제의 해를 가장 먼저 찾는 네트워크 참여자가 비트코인 블록체인 네트워크의 새로운 블럭의 소유권을 획득함으로써 이루어진다. 참여자는 자신이 보유한 컴퓨터의 계산 능력을 비트코인 블록체인 네트워크를 위해 사용하고 그 보상으로 새로운 블록, 곧 비트코인을 받는데, 이러한 인센티브를 통해 많은 참여자를 유지한다. 상술한 비트코인 피자데이가 중요한 이유도 단순히 흥미로 비트코인 블록체인 네트워크에 참여하고 채굴하던 참여자에게 그가 채굴한 비트코인이 현실에서 사용가치가 있음을 최초로 증명하였기 때문이다. 이처럼 채굴을 통해 새로운 비트코인의 소유권을 가질 수 있으며, 이 비트코인을 현실에서 지급결제 수단으로 사용할 수 있다는 사실은 사람들에게 이 네트워크에 참여할 충분한 인센티브가 되며, 이를 통해 비트코인은 – 비록 법정화폐, 특히 미국 달러화처럼 전 세계적으로 보편적 사용가치를 지니는 화폐는 아닐지언정 – 제한된 생태계 내에서 지급결제 수단으로 사용되는 화폐로서의 가치를 획득할 수 있었다. 그렇다면 자연스럽게 이 네트워크를 해킹하거나 공격하여 소유권을 조작하려는 시도가 가능하며, 그럴 경우 비트코인의 화폐로서 가치는 비록 그 인센티브에도 불구하고 상실될 수 있다는 우려를 가질 수 있다. 이러한 문제의 가능성을 예방하여 네트워크의 신뢰도를 높이는 방법이 작업 증명이다.

작업 증명(Proof of Work, POW)은 말 그대로 비트코인 블록체인의 새로운 블록을 생성해서 연결하는 작업을 완료했다는 사실을 증명하는 것을 말한다. 위에서 간략하게 서술한 바 있듯이 비트코인의 새로운 블록을 생성해서 기존 체인에 연결하기 위해서는 그 새로운 블록의 블록 해시를 계산해야 하는데, 이 블록 해시를 계산

8) "Spot the difference," The Economist, 2016. 04. 02(https://www.economist.com/the-americas/2016/04/02/spot-the-difference)

9) SHA는 Secured Hash Algorithms(보안된 해시 알고리듬)의 약자로 미국 국가안보국에 의해 1993년 처음 설계되었으며 미국 국가 표준으로 지정되었다. SHA-256은 그중에서 32 바이트 워드를 사용하는 해시 함수다.

하기 위해서는 블록 헤더 정보 중 하나인 논스(nonce) 값[10]을 구해야 한다. 논스 값을 통해 구하는 블록 해시는 32 바이트(Byte)[11]의 숫자인데, 이 값은 시스템을 통해서 정해진다. 즉 채굴량이 증가하면 난이도를 상승시키고, 채굴량이 감소하면 난이도를 하락시키는 방법을 통해서 채굴량이 일정하게 유지되도록 조정된다. 논스 값을 찾아 블록 해시를 찾는 계산은 컴퓨터의 연산 능력을 이용해야 하는데, 가장 빨리 블록 해시를 찾는 네트워크 참여자가 보상을 받기에, 즉 참여자가 수행한 연산을 통해 새로운 보상을 받을 수 있는 자격을 증명하기에 이 과정을 '작업 증명(Proof of Work, POW)'이라 한다. 이러한 자격 증명은 단순히 새로 채굴된 블록의 소유권을 인정받는 일 이외에도 중요한 기능을 하는데, 바로 해커에 의한 공격이나 위조 혹은 변조를 예방하는 기능이다. 네트워크를 통해 생성되고 전파되며 소유권이 인정되기에 비트코인은 해커에 의한 공격 혹은 위조나 변조의 우려가 큼을 부인할 수 없다. 예를 들어 블록의 기록을 해킹하여 비트코인의 소유권을 다른 사람에게 이전할 수도 있기 때문인데, 이러한 우려를 예방하는 기능이 바로 작업 증명이다. 사실 이러한 해킹 우려는 수학에서 상당히 오래된 문제 중 하나로 흔히 비잔틴 장군 문제(Byzantine Generals Problem)라고 불린다. 이 문제가 비잔틴 장군 문제라 불리는 이유는 다음과 같다 : 적군의 성을 공격하려는 비잔티움 제국의 군대가 지리적인 이유로 인해 다수의 장군이 지휘하는 여러 부대로 나뉘어져서 행군을 하고 있으며, 이 장군 사이 연락은 적에게 사로잡힐지 모르는 전령에 의해서만 이루어진다. 이 장군 중에서 충성스러운 장군은 사전에 합의된 규칙 – 예를 들어 공격 일자, 공격 시간, 공격 방법 등 – 을 충실하게 따르는 반면, 배신자는 규칙에 얽매이지 않고 자유롭게 행동할 수 있으며, 심지어 적과 내통할 수도 있다. 그렇다면 이 배신자의 존재에도 불구하고 공격을 성공시키기 위해서는 충직한 장군이 전체 장군 중 얼마나 있어야 하는지에 대한 문제가 비잔틴 장군 문제다. 이 문제에 대한 답을 보통 일반적으로 비잔틴 장애 허용(Byzantine Fault Tolerance, BFT)[12]이라 하는데, 기본적인 해결 방법은 Lamport, Shostak, and Pease(1982)[13]에서 제시되었다.[14] 보통 일반적으로 네트워크에서 비잔틴 장애 허용을 달성할 수 있는 방법은 2/3 이상의 신뢰할 수 있는 노드를 확보하는 것이다. 하지만 분산 원장 시스템에 자율적인 참여자로 구성되는 비트코인 네트워크에서는 신뢰할 수 있는 노드를 확보하는 일이 어렵다. 그래서 만들어진 방법이 합의 알고리듬으로서 작업 증명이다. 상술한 바 있듯이 작업 증명은 새로 채굴된 비트코인의 소유권을 보유하는 방법이지만, 동시에 합의 알고리듬이다. 상술한 논스를 이용한 블록 해시 계산은 네트워크 사이에 합의된 수학적 채굴 방식으로 이를 통해 새로운 블록이 채굴되었다는 사실은 곧 새로운 블록을 받아들여도 좋다는 의미다. 그렇기에 이 새로운 블록 생성은 모든 네트워크 참여자, 곧 노드에게 전파되고 기록된다. 그리고 이렇게 생성된 블록은 이전 블록의 정보를 지니고 있으며, 이 블록의 정보는 바로 다음 블록에 기록된다. 그렇기에

10) 논스 값이란, 이 값을 입력 변수로 계산해서 나온 해시값이 특정 숫자보다 작아지게 만드는 값을 말한다. 그리고 SHA-256 해시 함수의 특성상 논스 값은 특정 값에서 역으로 연산을 해서는 절대 구할 수 없고, 결과가 특정 값이 될 때까지 trial and error를 통해서만 찾을 수 있는데, 해시 함수의 특정 값을 찾는 입력값 중에서 유일한 변수가 바로 논스다.

11) 바이트는 컴퓨터의 저장 단위다. 1비트(bit)는 0 혹은 1로 정보를 표시하는 컴퓨터 정보 저장의 최소 단위인데, 비트 8개를 하나로 묶은 단위가 바이트다. 그렇기에 바이트는 인 256 종류의 정보를 저장할 수 있다.

12) 배신자, 즉 네트워크에서 악성 노드가 존재해도 네트워크가 정상적으로 작동할 수 있는 최소 허용값을 말한다.

13) Lamport, Leslie, Robert Shostak, and Marshall Pease, The Byzaantine Generals Problem, ACM Transactions on Programming Language and Systems, Vol. 4, No, 3, July, 1982, pp. 382-401.

14) 예를 들어, t명의 장군이 배신자일 경우, 전체 장군의 수인 n은 언제나 $n > 3t$이어야 한다.

만약 해커 혹은 네트워크 공격자가 블록 하나를 변조하려면 이와 연결된 모든 블록의 정보를 변경해야 하는데, 그러는 동안에도 블록은 계속 생성되어 연결되기에 사실상 블록에 기록된 내용을 변경하기는 불가능하다. 이처럼 비트코인은 비잔틴 장군 문제를 해결하여 네트워크 신뢰도를 높이기 위해 작업 증명을 사용한다.

작업 증명이 네트워크 신뢰도를 향상시키고 비잔틴 장군 문제를 해결할 수 있는 이유는 비트코인이 블록체인을 이용한 분산원장 시스템을 채택했기 때문이다. 만약 비트코인이 중앙화된 서버에서 모든 거래를 기록하고 통제한다면, 아무리 작업 증명을 통해 새로운 블록을 채굴하더라도 이에 대한 네트워크 공격이나 해킹을 통해 기록의 위조 혹은 변조가 가능하다면 신뢰를 획득하기 어렵다. 하지만 비트코인은 블록체인 분산원장을 통해 채굴과 거래 기록을 모든 노드에 분산해서 기록하였기에 만약 기록을 위·변조하려면 연결된 모든 기록을 변경해야 하며, 이는 상당한 수준의 연산 능력을 필요로 한다. 실제로 이러한 공격이 성공하기 위해서는 네트워크 전체 연산 능력의 51%를 보유해야 하지만, 이는 사실상 불가능하다. 비트코인 네트워크의 경우 지속적으로 블록이 추가되면서 규모가 증가하고 있기에 전체 연산 능력의 51%를 보유하기에는 막대한 비용이 소요될 뿐만 아니라, 만약 51% 연산 능력을 보유해서 네트워크 공격에 성공하더라도 그 즉시 비트코인의 가격이 폭락할 것이기에 오히려 공격자가 손해를 보게 된다.

이에 더해 작업 증명은 '이중지불(double spending)' 문제 역시 해결할 수 있다. 이중지불 문제는 비트코인을 비롯한 모든 전자화폐에 반드시 수반되는 문제로 이러한 화폐가 실물이 아닌 컴퓨터 데이터로 존재하기 때문에 발생하는 문제다. 즉 A라는 사람이 B라는 사람에게 비트코인을 송신하여 거래를 하는데, 이 비트코인 파일을 복사하여 저장했다가 C라는 사람에게 다시 송신하여 거래를 하는 일이 발생할 수 있는데, 이 문제가 바로 이중지불 문제다. 기존에 이중지불 문제를 해결하기 위한 방법은 신뢰할 수 있는 중개기관을 두고, 여기에 모든 데이터를 위탁하여 거래를 체결하는 시스템인데, 이는 현실에서 중앙은행의 재현일 뿐만 아니라, 이 중개기관이 해킹당할 경우 모든 데이터가 다 손실된다는 심각한 문제점이 있다. 비트코인은 이러한 이중지불 문제를 작업증명을 통해 해결했다. 상술한 바 있듯이 작업증명은 비트코인에서 채굴 알고리듬이자 합의 알고리듬이다. 즉 하나의 비트코인 거래는 새로운 블록에 탑재되며, 이렇게 새로 생성되는 블록은 작업증명 과정을 통해 가장 먼저 해시값을 찾아낸 참여자에게 소유권이 귀속된다. 만약 한 사람이 동시에 두 거래를 시도했다 하더라도 두 거래 중 하나만 기록된 블록치 채굴되어 기존 네트워크에 연결될 수 있기에 다른 거래는 자연스럽게 취소된다. 이중지불을 막을 수 있는 이러한 작업증명 메커니즘은 블록체인 네트워크의 신뢰도를 향상시킨다.

이상과 같은 세 메커니즘을 통해 비트코인은 기존에 전자화폐의 문제점으로 지적되어 온 문제를 해결했고, 그 결과 암호화폐의 대표 주자가 될 수 있었다. 하지만 비트코인의 상술한 기술적 발전에도 불구하고 여전히 부족함을 느끼는 사람은 많았는데, 그 중 한 명이 비탈릭 부테린(Vitalik Buterin)이다. 2013년, 19살의 청년 비탈릭 부테린은 비트코인에 사용된 블록체인 기술에 화폐 거래 기록 및 그와 관련된 정보뿐만 아니라 계약 관련 정보까지 기록할 수 있으며, 특히 블록체인 기술을 이용하면 거래 당사자 외 중개기관이나 보증기관이 개입되지 않고도 계약의 체결과 이행이 가능한 스마트 계약(smart contract)이 가능하다는 사실을 알게 되었다. 이에 비탈릭 부테린은 스마트 계약 플랫폼인 이더리움(Ethereum)을 제안하였다.

경제학적 측면에서 본다면, 블록체인 분산원장보다 스마트 계약의 등장이 더 혁신적인데, 그 이유는 이를 통해

거래비용을 획기적으로 절감할 수 있기 때문이다. 한 경제 체제 참가자 간 계약에서 중개자가 개입하고, 법원 등 공공기관의 인증이 필요한 이유는 그 이행을 강제하고 원활한 계약 체결을 보장하기 위함인데, 이러한 과정은 모두 거래비용을 증가시키는 결과를 야기한다. 예를 들어 부동산 임대차 계약을 생각해보자. 주택 임대인과 임차인이 중개자 없이 계약을 체결하고 이행한다면 이는 가장 이상적인 형태일 것이지만, 실제로는 여러 종류의 사기 – 예를 들어 집주인이 아니면서 집주인 행세를 하는 등 – 가능성이 높으며, 신뢰할 수 있는 제3자의 공증이 없는 형태의 계약은 그 신뢰성뿐만 아니라 법적 유효성을 인정받기도 힘들다. 그렇기에 부동산 임대차 계약에서 중개인이 개입되어 거래의 이행을 보증하고, 확정일자를 통해 신뢰받는 제3자인 정부가 개입하는 등 거래비용이 발생한다.[15] 이러한 부동산 임대차 계약에 만약 스마트 계약을 응용한다면, 거래 당사자 간 계약이 체결되는 즉시 이 계약은 블록체인 분산원장에 기록되어 위·변조가 불가능하게 되며, 특정 계약 조건 – 예를 들어 잔금의 납입 및 약정된 입주 일자 등 – 이 만족되면 자동으로 계약은 이행되며, 역시 마찬가지로 특정 조건 – 기한의 만료 혹은 계약 조건의 불이행 등 – 이 발생하면 계약은 자동적으로 만료된다. 즉 거래비용을 증가시키는 중개자의 개입 없이도 계약의 이행과 종료가 자동적으로 이루어진다. 부동산 임대차 계약만이 아니다. 거래 상대방 간 신뢰가 특히 중요한 금융 거래의 경우, 특정 조건이 충족되면 주식에 대한 배당금이 지급되거나 채권에 대한 쿠폰이 지급되는 형태로 스마트 계약의 작성이 가능하며, 보험 역시 특정 조건 – 병원 진단 혹은 사고 기록 – 이 충족된다면 보험금이 지급되도록 스마트 계약을 작성할 수 있다.

뿐만 아니라 이더리움은 블록체인 네트워크의 장점인 동시에 문제점인 작업증명을 지분증명(Proof of Stake, POS)으로 전환시켰다. 작업증명은 분명 획기적인 방법이지만, 많은 컴퓨팅 파워를 필요로 하기 때문에 전기 소모가 많고 하나의 거래가 승인되기까지 10분 정도 시간이 소요되는 문제가 있었다. 반면에 이더리움이 채택한 지분증명은 주식회사에서 지분에 따라 투표권을 갖는 것과 마찬가지로 전체 네트워크에서 더 많은 지분을 보유한 사람일수록 더 많은 영향력을 갖는다. 게다가 지분증명은 네트워크에 대한 공격 시도 역시 효율적으로 막을 수 있는데, 51% 공격을 하기 위해 지분을 취득하는 비용도 막대할 뿐만 아니라, 공격이 성공할 경우 신뢰의 붕괴로 인해 이더리움의 가치도 하락하기 때문에 굳이 막대한 비용을 투입하여 네트워크를 해킹할 이유가 없어진다.

경제사 연구에 계량경제학적 방법을 적용한 공로로 1993년 노벨 경제학상을 받은 더글러스 노스(Douglass North)는 그의 저서인 "경제사의 구조와 변화(Structure and Change in Economic History)"에서 인류의 역사적 발전과 경제적 발전을 연구하며 인류의 발전은 거래비용을 절감시키는 방향으로 이루어져 왔다고 서술한 바 있는데, 스마트 계약은 더글러스 노스의 이러한 통찰이 현재에도 여전히 유효함을 보여준다.

15) 물론 그 이전에 신뢰할 수 있는 거래 상대방과 중개인을 탐색하는 데 들어가는 비용도 무시할 수 없음은 주지의 사실이다.

Ⅳ. 탈중앙화 금융(Decentralized Finance, DeFi) : 블록체인의 금융 혁신 시도

상술한 바 있듯이, 블록체인 기술을 이용한 암호화폐의 기초인 비트코인은 2007년 글로벌 금융위기의 발생과 그로 인한 구제금융 및 양적완화에 대한 반발에서 시작되었지만, 적어도 2019년 현재 관점에서 보면 실패한 듯 보인다. 법정화폐를 사용하는 기존 금융 시스템은 여전히 정상적으로 작동되고 있으며, 은행이나 금융회사의 개입이 없는 개인 간 송금 및 금융거래를 목적으로 한 비트코인은 그 원래 목적을 이루지 못하고 투자자산으로서의 기능만 수행하고 있기 때문이다. 오히려 그와 반대로 기존 금융 시스템에서 블록체인 기술을 적용하여 금융을 혁신하려는 시도가 늘어나고 있다. 미국의 대표적 대형 은행인 JP Morgan Chase는 은행 간 거래 및 주식과 채권 거래에 사용할 달러 연동 암호화폐인 JPM Coin을 개발 중이라고 발표한 바 있으며,[16] 미국에서는 블록체인을 이용한 자산 토큰화를 통해 투자 자금을 모집하기도 했다.[17] 비록 비트코인이 처음 등장했을 때의 목표처럼 기존 금융 시스템을 암호화폐 시스템이 완전하게 대체하지는 못했지만, 금융 시스템의 이러한 변화는 긍정적이다. 블록체인 기술을 통해 기존 시스템보다 더 접근성이 좋고 투명한 금융 시스템을 만들었기 때문이다. 상술한 자산 토큰화가 대표적 예다. 값비싼 예술품이나 부동산에 투자할 수 있을만큼 여유 자산이 풍족하지 않은 투자자라도 자산 토큰화를 이용해서 예술품이나 부동산의 일정 지분을 소유할 수 있고, 이를 통해 수익을 올릴 수 있는 시스템의 등장과 보편화는 분명 블록체인 기술로 인해 가능할 수 있었다.

이에 더해 블록체인 자체적인 금융 서비스 시도도 있는데, 최근 대두되는 탈중앙화 금융(Decentralized Finance, DeFi)가 대표적 예다. 탈중앙화 금융은 은행이나 금융회사가 개입하지 않은 상태에서 블록체인 네트워크를 통해 금융 서비스가 이루어지는 시스템을 말한다. 사실 암호화폐 기반 금융 서비스는 암호화폐 발행 회사에 의해 이미 제공되고 있는데, 메이커 다오(Maker DAO)가 제공하는 이더리움 담보대출 서비스가 대표적 예다. 메이커 다오는 이더리움을 담보로 하여 암호화폐인 다이(DAI)를 발행한다. 이러한 담보대출은 상술한 스마트 계약을 통해 이루어지며, 시스템 안정성을 위해서 초과 담보(Over Collateralization)와 강제 청산(Forced Liquidation)이 적용된다.[18] 초과 담보는 말 그대로 대출하고자 하는 다이보다 더 많은 이더리움을 담보로 예치하도록 하는 제도로, 보통 담보 가치의 60%에서 70%에 해당하는 양만 대출이 가능하다. 예를 들어 어떤 사람이 100이더리움을 담보로 다이를 대출하고자 한다면 그 사람은 70이더리움에 해당하는 다이만 대출받을 수 있는 것이다. 강제 청산은 금융시장에서 레버리지를 이용한 거래에서 행해지는 그것과 적확하게 동일한 메커니즘이다. 즉 담보로 예치된 이더리움의 시장가격이 대출 비율보다 아래로 하락할 경우 즉시 이를 시장에서 매각하고

16) "JPMorgan plan to coin it on the blockchain", Financial Times, 2019. 02. 15 (https://www.ft.com/content/0bafd9d6-307e-11e9-8744-e7016697f225).

17) "Tokenization, 암호화폐시장의 새로운 변화," Weekly IBK 경제브리프(633호), IBK 경제연구소, 2019. 05. 07.

18) 이에 더해 암호화폐 가치 유지를 위한 교환비율 조정도 이루어진다. 예를 들어 발행 당시 1 다이의 가격이 1 이더리움으로 설정되어 있는 상황에서 만약 다이 가격이 1 이더 이상으로 상승했을 경우, 메이커 다오는 담보물에 대한 다이 발행량을 증가시킬 수 있다. 이러한 발행량 조정이 이루어지면 동일한 이더리움을 담보로 하여 더 많은 다이를 발행할 수 있어서 신규 계약자가 시장에 진입하고, 기존에 다이를 발행한 사람은 자신이 보유한 다이를 상환하고 이더리움을 돌려받아 더 낮은 담보비율로 더 많은 다이를 발행할 인센티브가 생긴다. 이로 인해 시장에 유통되는 다이 발행량은 증가하여 가격은 안정화된다. 반대의 경우도 마찬가지다. 이러한 메커니즘은 중앙은행에서 공개시장조작을 통해 화폐 가치를 일정하게 유지하는 것과 비슷하다고 할 수 있다.

그 금액으로 다이를 구입해서 계약을 청산한다. 금융시장이라면 이러한 담보대출 혹은 레버리지 거래 메커니즘에 금융회사가 계약 당사자로 개입한다면, 암호화폐 시장은 암호화폐 발행 회사와 스마트 계약을 통해 모든 거래가 이루어진다. 즉 암호화폐 발행 회사와 시장 참여자가 양 계약 당사자라면 이들 간 계약의 체결은 중개자 없이 스마트 계약을 통해 이루어진다. 스마트 계약을 통한 이러한 금융 서비스 메커니즘은 신뢰받는 중간자로서 금융회사가 필요했던 이전과는 다른 시스템이다.

이러한 탈중앙화 금융은 분명 기존 금융과는 다른 서비스로, 은행을 비롯한 금융 서비스에 대한 접근이 어려운 사람에게 하나의 선택지가 될 수 있다. 즉 암호화폐에 기반한 탈중앙화 금융은 은행이나 금융 서비스가 미비한 개발도상국 혹은 은행이나 금융 서비스 이용이 어려운 저소득 계층이나 저신용자가 믿고 이용할 수 있는 금융 서비스를 제공할 수 있다. 기존 금융 서비스를 이용하기 위한 은행 잔고 조회 혹은 신용평가 없이 블록체인을 이용한 스마트 계약을 통해 – 비록 법정화폐가 아니라 그 이용에 제한이 따르는 암호화폐지만 – 금융 취약 계층이 금융 서비스를 이용할 수 있기 때문이다.

이러한 금융 서비스의 중요성은 여러 금융경제학자에 의해 일찍부터 강조되어 왔는데, 가장 대표적인 학자가 라구람 라잔(Raguram Rajan)과 루이지 징갈레스(Luigi Zingales)다. 이들은 저서 "Saving Capitalism from the Capitalists"에서 "튼튼하고 경쟁적인 금융시장은 일반 대중들에게 더 많은 기회를 제공하고, 사회에 만연된 빈곤을 몰아내는 데 있어 놀라우리만치 효과적인 도구임"[19]을 논증한 바 있다. 또한 에릭 포스너(Eric Posner)와 글렌 웨일(Glen Weyl)은 그들의 저서 Radical Markets(2018)에서 불평등을 완화하기 위한 하나의 방법으로 윌리엄 비크리(William Vickery)의 경매 이론에 기반을 둔 시장 메커니즘을 제시한 바 있다. 즉 에릭 포스너와 글렌 웨일은 자산에 대한 개인의 항구적인 소유권을 인정하는 대신, 자산에 대한 경매 시스템을 도입하여 누구라도 현재 소유주가 지불한 가격보다 더 높은 가격을 지불하는 사람에게 해당 자산의 소유권을 이전하는 대신, 그 차액을 사회적 약자를 위해 사용하는 메커니즘을 제안했다. 에릭 포스너와 글렌 웨일의 이러한 주장은 일견 극단적으로 보임을 부정할 수는 없지만, 다른 한편으로는 시장 메커니즘을 이용해 장기적으로 지속되는 지대 추구를 예방하는 동시에 사회에 만연한 빈곤과 부의 불평등을 해소할 수 있는 한 방법으로 생각해볼 가능성도 충분히 있다. 예를 들어 현재 한국에서 문제가 되는 부동산을 생각해보자. 에릭 포스너와 글렌 웨일에 의하면, 부동산 가격 상승으로 인해 그 소유주가 얻는 이득은 전형적인 독점에 의한 지대 추구(rent seeking) 행위다. 만약 모든 사람이 자신이 소유한 부동산에 대해 '공동 소유 자기 평가세(Common Ownership Self-Assessed Tax, COST)'를 적용한다고 가정해보자. 공동 소유 자기 평가세는 쉽게 말해 부동산 소유자 스스로 자신이 보유한 부동산의 가치를 평가해서 세금을 지불하고, 누구든지 소유자가 평가한 가치보다 더 높은 돈을 지불하는 사람에게 그 소유권을 이전하는 제도다. 얼핏 황당하게 들리는 이 주장은 윌리엄 비크리의 경매이론과 역시 노벨 경제학상을 받은 로저 마이어슨(Roger Myerson)과 마크 새터스웨이(Mark Satterthwaite)의 연

19) Rajan, Raghuram G. and Luigi Zingales, Saving Capitalism from the Capitalists: Unleashing the Power of Financial Markets to Create Wealth and Spread Opportunity, Princeton University Press, 2004(한국어판, 고승익 옮김, 『시장경제의 미래』, 앤트출판, 2008), pp. 1.

구에 기초하고 있다.[20] 이러한 가격 책정과 경매 방식에 있어 반드시 필요한 것은 투명한 기록과 신뢰할 수 있는 시스템인데, 여기에도 블록체인 기술을 이용한 탈중앙화 금융 시스템을 적용할 수 있다. 즉 분산원장을 통해 모든 거래와 그 내역, 그리고 각 소유자가 책정한 자산 가치와 세금을 공개하여 더 투명하고 신뢰받을 수 있는 경매 시스템을 구축할 수 있다.

라구람 라잔과 루이지 징갈레스, 에릭 포스너와 글렌 웨일의 주장처럼 빈곤과 불평등을 완화하기 위해서는 기존 금융 서비스의 혁신과 함께 시장 메커니즘에 대한 근본적 차원에서의 고찰과 혁신이 이루어져야 한다. 그중에서도 특히 금융은 그 특성상 보수적인 성향을 가질 수밖에 없는데, 기존 금융 서비스에서 저소득층 혹은 저신용자 계층이 그 수혜자에서 제외되어 왔음은 부인할 수 없는 사실이다. 그렇다고 해서 섣불리 이들을 기존 금융 서비스로 편입할 경우, 상술한 것처럼 2007년 글로벌 금융위기 같은 금융위기가 다시 발생할 가능성이 높다. 그렇다면 기존 금융 서비스에서 소외되어 온 사람을 대상으로 하여 암호화폐 기반의 탈중앙화 금융 서비스를 제공한다면 위험을 최소화하면서 금융 서비스의 사각지대를 제거할 수 있을 가능성이 있다. 이러한 메커니즘을 통해 가장 가난한 사람조차 생활수준을 향상시킬 수 있는 금융 서비스를 제공한다면 경제 전체적인 효용도 향상될 것이다.

V. 결론

이 논고에서 우리는 2007년 글로벌 금융위기의 기원과 그 극복과정을 살펴보고, 그 과정에서 생겨난 현행 법정화폐 시스템과 금융 시스템에 대한 불만에 기초하여 등장한 암호화폐와 그 기술, 그리고 이러한 기술이 금융시장 및 주택금융에 적용될 수 있는 방법에 대해 알아보았다. 사실 글로벌 금융위기의 극복에 있어 위기를 초래한 금융회사에 대한 미국 정부의 구제금융과 경기침체를 막기 위한 양적완화가 큰 역할을 했음은 부인할 수 없는 사실이다. 그렇지만 이러한 구제금융이나 양적완화에 대한 납세자로서 시민 일반의 불만은 상당했고, 이는 결국 탈중앙화를 기치로 내건 비트코인을 비롯한 암호화폐에 대한 열광으로 표출되었다. 2017년 하반기부터 2018년 상반기까지 암호화폐는 마치 롤러코스터를 타는 듯한 놀라운 상승과 하락을 보여주었고, 현재까지도 이러한 암호화폐의 여파는 진행 중이다.

암호화폐가 기반한 기술은 블록체인 분산원장과 이러한 분산원장 시스템 하에서 비잔틴 장군 문제를 해결할 수 있는 합의 알고리듬이다. 이러한 기술을 통해 암호화폐는 데이터의 위·변조나 해킹 등 문제를 해결할 수 있어 시스템의 신뢰도를 향상시켰으며, 이에 더해 스마트 계약은 암호화폐가 더 보편적인 사용가치를 지닐 수 있도록 도약하는 계기가 되었다.

20) 이와 관련하여 상세한 논의는 Posner, Eric A., and E Glen Weyl, Radical Markets: Uprooting Capitalism and Democracy for a Just Society, Princeton University Press, 2018(한국어판, 박기영 옮김, 『래디컬 마켓』, 부키, 2019), pp.75-130 참조.

암호화폐의 현재 모습은 비트코인이 최초에 등장할 때 사토시 나카모토가 백서에서 언급한 "금융회사를 방문하지 않고서도 개인 간 금융거래가 가능한 순수한 개인 간 전자화폐"[21]의 이상과는 상당히 거리가 멀지만, 그럼에도 불구하고 암호화폐의 등장과 관련 기술의 발달은 금융시장의 혁신을 촉진하고 있다. 금융시장의 혁신은 은행을 비롯한 금융회사가 기존 업무에 블록체인 기술을 응용하는 것부터 시작해서 암호화폐를 이용한 다양한 탈중앙화 금융까지 다양한 방법으로 이루어지고 있다. 물론 현재는 이러한 금융 혁신이 규제와 충돌하거나 혹은 규제의 사각지대에 위치하고 있음을 부인할 수는 없지만, 적정한 규제가 이루어진다면 더 많은 사람에게 더 편리한 금융 서비스를 제공할 수 있을 것이다. 파생금융상품도 규제를 회피하기 위해 혹은 규제의 사각지대에서 금융 소비자의 다양한 요구를 충족시키며 투자와 헤지 수단을 제공하기 위해 시작되었음을 상기해보면, 암호화폐와 탈중앙화 금융의 이러한 행태도 새삼스러운 모습은 아니다. 무조건적인 규제나 금지 일변도 정책보다도 다양한 가능성을 열어두고 정부와 금융회사와 블록체인 핀테크 업계가 지속적으로 소통을 한다면 분명 현재보다 한 단계 더 발전한 금융 서비스가 가능할 것이다.

참고문헌

- Bernanke, Ben S., The Courage to Act: A Memoir of a Crisis and Its Aftermath, W. W. Norton & Company, 2015(한국어판, 안세민 옮김, 『행동하는 용기』, 까치, 2015).
- Lamport, Leslie, Robert Shostak, and Marshall Pease, The Byzaantine Generals Problem, ACM Transactions on Programming Language and Systems, Vol. 4, No. 3, July, 1982, pp. 382–401.
- Mian, Atif. and Amir Sufi, House of Debt, The University of Chicago Press, 2014(한국어판, 박기영 옮김, 『빚으로 지은 집』, 열린책들 2014).
- Posner, Eric A., and E Glen Weyl, Radical Markets: Uprooting Capitalism and Democracy for a Just Society, Princeton University Press, 2018(한국어판, 박기영 옮김, 『래디컬 마켓』, 부키, 2019).
- Rajan, Raghuram G. and Luigi Zingales, Saving Capitalism from the Capitalists: Unleashing the Power of Financial Markets to Create Wealth and Spread Opportunity, Princeton University Press, 2004(한국어판, 고승익 옮김, 『시장경제의 미래』, 앤트출판, 2008).
- Satoshi Nakamoto, "Bitcoin: A Peer–to–Peer Electronic Cash System", 2018.
- "Tokenization, 암호화폐시장의 새로운 변화," Weekly IBK 경제브리프(633호), IBK 경제연구소, 2019. 05. 07.
- "JPMorgan plan to coin it on the blockchain", Financial Times, 2019. 02. 15(https://www.ft.com/content/0bafd9d6–307e–11e9–8744–e7016697f225).
- "Spot the difference", The Economist, 2016. 04. 02(https://www.economist.com/the–americas/2016/04/02/spot–the–difference)

21) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2018.