BOScoin White Paper 2.0

2018. 11. 01.

Disclaimer

본 문서는 BOScoin팀(이하 “BOS팀”)의 BOScoin 생태계의 현황과 계획에 대하여 정리한 'BOScoin 백서 2.0'(이하 “본 백서”)이다. 본 백서는 오직 향후 계획 및 정보의 제공 목적을 갖고 있고, 향후 계획을 약속하는 것이 아니다. 구체적으로 명시된 것이 아니라면, 본 백서에서 정리해 놓은 혁신 기술은 아직 개발 중인 단계에 있고, 완전하게 적용되지 않은 것이다. BOS팀은 이러한 기술, 또는 혁신의 개발과 실행에 대한 성공이나 본 백서에 나와있는 어떤 활동에 대한 결과에 있어서도 보증 혹은 확약 및 진술을 작성·제공하지 않는다. 그리고 본 백서에 포함된 정보는 BOS팀이 믿을 수 있다고 생각한 출처의 자료들을 참고하였지만 해당 정보의 정확도, 완전성, 적합성과 관련하여서는 BOS팀이 보증 혹은 확약 및 진술을 작성·제공하는 것은 아니다.

본 백서로 BOS팀이 BOScoin의 가치를 보증 또는 승인하는 것이 아니고, 투자 원금을 보장하는 것도 아니다. BOS팀은 법이 허용하는 범위 내에서 투자자의 투자와 관련된 책임을 부인한다. 즉, BOS팀은 본 백서와 관련하여 투자자의 과실, 부주의 등으로 인해 발생한 투자의 손실이나 피해에 대해 법적 책임이 없다. 본 백서의 저자, 자문단, 기여자 역시 전술한 사항에 대하여 법적 책임이 없다고 할 것이다. 즉, 투자자는 투자를 결정하는 데 있어, 본인의 지식, 조사, 판단과 평가에만 의존해야 하고, 해당 투자 결정에 대해서는 본인이 책임을 진다. 따라서 상술된 위험성을 고려하여 투자에 신중을 기하여 주기 바란다.

본 백서는 https://boscoin.io/에서만 이용할 수 있으며 BOS팀의 사전 서면 동의 없이 어떤 목적으로든 일부 혹은 전체를 다른 사람에게 재분배, 복제 혹은 전달하거나 출판을 할 수 없다. 본 백서를 배포하는 행위는 특정 국가에서 법 혹은 규제에 의해 제한될 수 있다. 본 백서를 소지한 사람들은 해당 사항에 대하여 인지하여야 하고 이러한 제한을 준수하여야 하며, 본 백서를 접함으로써 수취인은 앞서 제시한 사항에 대하여 동의한 것으로 간주한다.

Abstract

BOS팀은 기존 백서에 제시한 전략을 보완한 본 백서를 제안한다. 블록체인/암호화폐 시장을 둘러싼 다양한 담론과 비즈니스 확대는 새로운 전략을 요구하고 있다. 이에 BOS팀은 글로벌 커뮤니티 참여자에 의한 신용창출 체계를 갖춘 글로벌 금융 시스템을 구축함으로써 기존 경제 패러다임에 신선한 충격을 줄 수 있는 기술적, 사회경제적 의미를 지닌 프로젝트를 만들고자 한다.

지난 50여년 간 풍요의 시대를 이끈 현 자본주의 체제는 지난 2008년 미국발 세계 금융 위기를 기점으로 한계에 봉착하였다. 피케티가 간결한 공식으로 증명하였듯(Capital in the Twenty-First Century, 2017), 주식회사 제도가 야기한 경제적 불평등(부의 편중) 심화, 기술 발전 등에 따른 노동(일자리) 소멸과 소비 축소, 가속화되는 금융주권 소외 등은 현 상태로 사회가 지속되기 어렵다는 사실을 보여준다. 이에 우리는 기존 경제 체제에 새로운 출구를 만들 수 있는 3가지 대안-암호경제, 커먼즈 운동, 임팩트 투자-에 주목하였다. 새롭게 창발하고 있는 암호경제 그리고 이미 십여 년 전부터 시작된 커먼즈(Commons) 운동과 임팩트 투자를 결합함으로써, 우리는 소수 주주들에게만 부가 집중되는 주주 자본주의를 넘어서 다수의 참여와 의사결정으로 신용창출이 가능하고, 창출된 신용으로 만들어진 부가가치를 커뮤니티가 사용할 수 있는 공공금융(Public Financing, 이하 PF)을 제안하고자 한다. 커먼즈 운동이 자본주의의 핵심 원리를 부정하지 않으면서도 자본주의의 편협한 소유권 제도를 넘어선 것처럼, 우리 역시 자본주의의 핵심 원리와 장점을 부정하지 않으면서 가장 자본주의적인 방법으로 그 한계를 넘어서고자 한다. 이를 위해서 우리가 제시하는 전략이 바로 PF다. PF는 기존 ICO와 다른, BOScoin의 비전, 정체성이자 핵심 경쟁 전략이다.

PF는 중앙은행이나 기존 금융기관이 아닌 실제 신용을 사용하고 거래하는 개인들의 집단적인 의사결정으로 신용을 창출하는 방식이다. BOS팀은 이미 백서 1.0에서 참여자의 의사결정 권한을 보장하기 위해 의회 네트워크(Congress Network)라는 거버넌스 시스템을 도입하였다. 의회 네트워크를 통해 BOScoin 커뮤니티는 BOScoin의 모든 정책을 수정, 삭제, 추가할 수 있다. 이것은 당연하게도 BOScoin의 발행 규모, 추가 발행 시점의 기준 가격, 발행량 배정, 발행된 물량의 분배 등에 대한 의사결정을 포함한다. 특히 BOScoin 추가 발행을 통해 만들어진 자산 그리고 이를 활용한 사업으로 획득한 유무형의 자산은 커먼즈(커뮤니티 공동의 것)이기에, 커뮤니티는 이 자산의 용도를 제안하고 결정할 권한을 갖는다. BOScoin의 Trust Contracts는 이와 같은 의사결정이 반드시 실행되도록 보장할 것이다. 이는 곧 BOScoin 내에서 금융주권은 특정 소수가 아닌 커뮤니티 구성원 전체에 귀속되어 있다는 사실을 의미한다. 이 같은 이유로 우리는 PF를 공공성(public)이 있다고 주장한다.

한편, 커뮤니티가 어떤 문제에 직면했을 때 이를 잘 이해하고 해결하기 위해서는 멤버 각자가 의견을

개진하고 참여하는 것이 중요하다. 그러나 기존 주식회사 방식인 1주 1표 또는 블록체인에서 코인을 많이 가진 사람에게 더 많은 권한을 부여하는 PoS(proof of stake)나 DPos(Delegated Proof of Stake) 방식처럼, 많은 자원을 가진 이가 영향력을 발휘하고 시스템을 지배할 수 있도록 만든다면 부의 집중과 불평등 심화를 불러올 것이다. 이것을 방지하기 위해 그리고 커뮤니티 구성원 전체가 의사결정 권한을 가지도록 하려면, 근대 민주주의가 수 백 년간 실험과 투쟁으로 만들어낸 1인 1표 무기명 투표 시스템을 도입하는 것이 현재 시점에서는 가장 적절한 방법일 것이다. 그런데 1인 1표를 구현하기 위해서는 개인 식별이 필요하다. 즉 우리가 풀어야 하는 숙제는 탈중앙화된 네트워크 상에서 프라이버시(익명성)가 보장된 1인 1표 시스템을 구축하는 것이다. 우리는 이를 해결하기 위해 동형암호 기술에 기반한 Congress Voting 시스템을 구축하기로 했다. 동형암호는 암호화된 상태로 존재하는 데이터의 암호를 풀지 않고, 암호화된 데이터들을 직접 연산하여 암호화된 결과값을 얻어낼 수 있는 최신 암호화 솔루션이다. 동형암호 기술을 활용함으로써, 우리는 커뮤니티 내에서 한 사람은 단 하나의 ID만을 가질 수 있으며(singularity), 동시에 커뮤니티 내에서 완전한 무기명 투표(Anonymous voting)가 가능하도록 하는 기술을 도입하고자 한다.

우리는 현 자본주의 체제가 가진 한계를 암호경제와 커먼즈 운동이 가진 잠재력과 폭발성을 통해 극복함으로써, '가장 자본주의적인 방법으로 자본주의를 해킹하고자' 하는 우리의 목표를 달성할 것이다. PF와 Congress Voting은 이를 가능하게 해주는 중요한 디딤돌이다. 본 백서에서 다루지 못한 Generic Trust Third Party(이하 GTTP), BOScoin 경제 모델 등은 이어서 나올 백서 개정판에서 다룰 예정이다.

서문

우리는 백서 1.0에 다 담지 못한 우리의 과제와 비전을 재정립하는 차원에서 본 백서인 'BOScoin 백서 2.0'으로 명명한 작업을 시작했다. 백서 1.0에서는 암호화폐 플랫폼 중 이더리움의 한계를 극복하는 대안 모델로서 BOScoin을 규정하고, FBA기반으로 오픈 멤버십을 수용하는 mFBA, Smart Contracts의 취약한 보안 문제를 해결하기 위한 Trust Contracts, 거버넌스 문제를 해결하기 위한 Congress Network, 지속 가능한 에코시스템을 위한 자금을 지원하는 Commons Budget, 그리고 메인넷과 동시에 출시되는 관련 응용 서비스 등을 제안하였다. 그리고 성공적인 ICO 과정을 통해 우리는 우리의 플랜이 당시 암호화폐 플랫폼들이 풀어야 하는 문제들을 어느 정도 제대로 진단했다고 평가한다. 하지만, ICO 이후 암호화폐 시장이 풀어야 할 과제와 변화에 대해 분석하고 고찰하면서 또한 BOScoin의 향후 비전, 전략, 사업 방향을 재정립하면서 우리는 기존 전략의 보완이 불가피하다고 결론을 내렸다. 보완된 전략 중심에는 기존 암호경제의 ICO와 대비되는 PF(Public Financing)와 1인 1표 기반의 Congress Voting이 있다.

본 백서는 BOS팀이 풀고자 하는 문제와 그 해결책으로서 '공공금융(PF)' 개념 제안에 중점을 두었다. PF는 뒤에 소개하겠지만 Congress Network의 투표에 의해서 실행된다. 이를 위해 우리는 한국스마트인증(KoSAC)과 함께 동형암호에 기반한 Congress Voting을 도입하기로 했다. 본 백서는 PF와 Congress Voting을 중심으로 작성되었다. 백서 개정판에서는 온라인 외에 오프라인 세계와 연계되는 고리로서 GTTP 개념을 제안할 예정이다.

BOS팀은 지금까지 진행되어 왔던 오픈소스 문화의 정신을 이어받아, 블록체인 기술을 활용해 세상을 근본적으로 바꿀 수 있다는 믿음을 가진 사람들이 모여 프로젝트를 진행하고 있다. 그렇다면 BOS팀은 어떤 일을 하고자 하는가? 프로젝트 리더인 예준은 달라스 밋업에서 이렇게 대답했다 :'우리는 GNU 선언,Creative Commons 운동에 이어 가장 자본주의적인 방법으로 자본주의를 해킹하고자 한다'. 이 말이 의미하는 것은 BOS팀은 블록체인과 암호화폐를 통해 글로벌 규모의 신뢰를 구축하고 조직화하며, 이를 통해 기존 금융자본주의 체제를 대체할 수 있는 새로운 유형의 신용창출 체계를 만들겠다는 것이다.

이제 BOS팀이 풀고자 하는 문제를 자세히 살펴보자.

1. 서론: 배경

인류는 유사 이래 가장 풍요로운 세상에 살고 있다. 그 풍요는 기술 발전에 따른 생산성 향상에 의한 것이기도 하지만, 과거 다른 체제와 달리, 사회의 신용창출 능력을 극대화한 자본주의 체제에도 기인한다. 특히 1971년 돈의 규칙을 통째로 바꾼 금본위제 폐지에 따른 명목화폐의 전 세계적 도입, 그리고 그 명목화폐를 중심으로 한 금융제도의 도입으로 만들어진 신용창출 능력이 만들어낸 효과는 눈부셨다. 또한 자본주의 국가들은 위기관리를 통해 몇 차례 발생했던 전 세계적 공황 등 심각한 경제 위기를 극복하였고, 이러한 경험들은 자본주의 경제 체제는 위기가 찾아오더라도 그 위기를 극복할 수 있는 체제라는 믿음을 만들었다. 하지만,2008년 세계 금융 위기 이후 그 믿음에 큰 균열이 생겼다.

현재 경제 상황은 자본주의 체제가 근본적으로 부의 분배에 실패하고 있으며, 이는 생산-소비-재생산이라는 자본 순환의 생태계를 무너뜨려 자본주의 체제의 존립 자체조차도 위험하게 만들 것이라는 위기의식을 낳고 있다. 이러한 분배 구조의 악화에 따른 시장 실패와 더불어 다른 한편에서 진행되고 있는 기술 발달, 특히 정보기술의 발달은, 새로운 기술이 새로운 일자리를 창출했던 과거와 달리 전체 산업에서 인간 노동의 필요성을 줄이고 있다. 이는 곧 노동 소득의 축소로 그리고 전반적인 인간 노동 질의 하락으로 이어진다. 기술 발달에 따른 노동 소득 감소로 노동자가 소비자 역할을 하지 못한다면 자본주의 체제는 어떻게 유지될 수 있을까? 유지될 수 없다면 대안은 무엇인가? 블록체인 기술을 어떻게 유용하게 사용할까 진지하게 고민하는 사람들이라면, 사회 전체가 직면하고 있는 이러한 문제를 회피하기 어려울 것이다. BOS팀 역시 BOScoin 프로젝트를 통해 이 문제를 해결하고자 한다.

이런 의미에서, 본격적으로 우리의 이야기를 하기 전에 사회 전체가 직면한 자본주의 체제의 문제점을 자세히 살펴 보고, 이를 극복하기 위해 노력했던 여러 대안을 살펴보고자 한다. 지금까지 진행되어 왔던 노력과 대안들에 대한 분석을 통해, 현재 자본주의 체제가 가진 문제를 극복하기 위한 새로운 암호화폐 경제 체제를 제안하고자 한다.

1.1 현재 경제 상황에 대한 우리의 이해

분배 실패에 따른 소비 시장 붕괴와 주식회사 제도

산업혁명 이후 자본주의 체제에서 비록 갈등과 위기가 있었지만 생산성이 향상되면 대부분 노동 소득은 증가하였다. 노동 소득 증가로 다수의 중산층, 상당한 구매력을 보유한 소비자층이 탄생했고 이들을 기반으로 경제가 지속적으로 성장하였다. 반면 1980~2000년에 들어서는 노동 소득 증가가 거의 일어나지 않았지만

경제는 별 문제 없이 성장하는 것처럼 보였다. 이 시기를 자세히 살펴 보면, 선진국 노동자들은 소득이 늘어나지 않은 상태에서 낮은 금리의 빚으로 소비를 유지해 왔다. 선진국 노동자들은 금융을 통해 소득 없이도 거의 모든 상품과 서비스를 소비할 수 있었다. 이를 '경제의 금융화(Financialization)'라 한다. '경제의 금융화'를 통해 선진국 중심으로 금융 서비스 부분이 크게 성장하였고, 이 때문에 경제는 호황인 것처럼 보였다. 이 시기에 자본가와 상위 소득자들은 자본소득을 통해 부를 크게 축적했고, 대부분 노동자는 빚으로 소비를 유지하는 불안한 상태가 지속되었다. '경제의 금융화'를 기반으로 하는 현 자본주의 체제(소위 '신자유주의'라 칭함)는 과거 자본주의 체제보다 더 큰 문제를 일으켰다. 2008년 전세계를 강타한 서브프라임 모기지(Subprime mortgage) 사태는 이 모든 상황들을 설명해 주는 상징적 사건이다.

분배 실패의 원인은 여러가지가 있겠으나 우리는 중요한 원인 중 하나로, 주주 이익 극대화를 추구하는 주식회사 제도에 있다고 분석한다. 주식회사는 주식 발행을 통해 자금을 조달하여 설립되며, 주주들에게 더 많은 이익을 분배하는 것이 그 설립 목적이다. 따라서, 대부분 주식회사는 생산비용을 최대한 낮추고 판매가격을 가능한 높이는 사업 방식을 택해 왔다. 이러한 사업 방식은 필연적으로 단위 노동당 생산성을 높이는 방향으로 나아가며, 그 결과는 대부분 단위 사업장에서 노동 비용을 최대한 줄이는 양태로 나타난다. 주식회사가 탄생한 지 400년 동안 인류는 주식회사가 만든 혁신을 통해 혜택을 누려 왔는데, 문제는 그러한 생산성 향상에 따른 부가 (주주 자본주의 체제에서는) 소수 주주에게 집중되며, 생산된 상품과 서비스를 소비할 다수 노동자에게는 돌아가지 않는다는 점이다. 이 주식회사 제도가 분배를 실패로 내몰고 있고, 주식회사가 만든 생산물을 소비해야 하는 노동자 집단의 몰락을 가속화하고 있다. 특히 정보기술과 정보재가 생산에서 점점 더 비중이 커지고 있는 근래에는 주식회사 형태의 글로벌 플랫폼 기업들이 탄생했는데, 이 기업들에 의해 국가 단위 부의 집중화를 넘어선 글로벌 규모에서 부의 집중화가 일어나고 있다 (Piketty and Ganser, 2015).

금융에 대한 의사결정 문제 : 금융 주권 문제

자본주의 체제에서 신용창출을 담당하는 금융이 중요하다는 것은 모두가 잘 아는 사실이다. 하지만, 금융에 대한 의사결정 권한이 일반 시민에게 주어지지 않는 사실에 대해서는 무감각하거나 당연하게 받아들인다. 하지만 신용창출의 기반이 다수 일반인의 작은 신용이 모여서 마련된다는 사실을 감안하면, 금융에 대한 의사결정 권한이 왜 소수 금융인들에게 맡겨져야 하는가에 대해 의문을 제기할 수 있다. 이러한 구조의 문제점은, 소수가 금융에 대한 의사결정 권한을 독점하고 그로 인해 창출되는 대부분의 이익을 독점하나, 이 의사결정으로 인해 발생하는 실패의 책임은 의사결정에 참여할 권한 조차 없는 다수의 평범한 사람들이 감당하게 된다는 사실이다. 리먼브라더스의 파산을 야기했던 의사결정은 소수 금융인이 내렸지만, 책임은 신용을 제공했던 전체 사회가 부담할 수밖에 없었다. 일반 상업은행에 의해 수행되는 대출이라는 신용창출 역시 소수 금융인들에 의해 판단되고 결정되고 집행되고 있다. 사토시 나가모토가 2009년 1월 3일

생성한 첫 블록(Genesis block)에서 “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”(2009 1월 3일, 타임즈: 재무부 장관, 은행들을 위한 두번째 구제금융 임박)이라고 넣은 것은 바로 금융 주권이 박탈된 현실을 꼬집은 것이다.

그런데 자본주의 하에서는 다수의 개인들이 주식회사의 주주로 참여할 수 있지 않느냐고, 개인들의 경제 참여 기회는 열려있지 않느냐고 반문할 사람이 있을 것 같다. 그런데 현재 금융 제도하에서 일반인이 주식회사의 주주로 참여할 기회는 그리 많지 않다. 현재 스타트업 제도-높은 위험을 감수하고 초기 투자를 감행한 후 M&A나 주식 상장을 통해 높은 수익을 얻을 수 있는 구조-를 예로 들어 보자. 통상 스타트업들은 벤처캐피털 투자에 의해 시작하고 성장한다. 조금 더 성장하면 사모펀드와 투자은행 등을 통해 대규모 자금이 투입된다. 이 자금들을 기반으로 구글, 페이스북 같은 글로벌 플랫폼 기업들이 탄생한다. 그 이후 통상적으로 주식 상장의 과정을 거친다. 상장이 되어야 비로소 일반 개인들이 주식에 접근할 기회가 생긴다. 상장 전까지 벤처캐피털, 사모펀드, 투자은행 모두 소수에 의한 결정으로 투자가 진행된다. 비록 높은 투자 위험이 있지만 성공하면 높은 자본 이익을 얻을 수 있는 기회를 일반인들은 거의 가지지 못한다.

2016년 핀테크 열풍이 불면서 P2P 대출과 크라우드 펀딩 시장이 성장하기 시작하자, 미국 등 주요 국가에서는 P2P 대출과 크라우드 펀딩의 개인 투자 한도(상한액)를 설정했다. 개인이 적극적으로 투자에 대한 위험을 안고 높은 투자 수익을 얻고자 하는 기회를 '투자자 보호'라는 명목으로 막은 것이다. 이는 한편으로는 국가가 개인들을 보호하려는 행위의 일환으로 볼 수 있지만, 동시에 이는 일반인에게 금융 영역의 의사결정 권한을 주지 않으려는 과도한 규제로 해석할 수도 있다. 개인들에게 투자 기회를 충분히 열어주면서도 현명하게 투자하도록 유도하는 장치들은 아주 다양하게 만들 수 있기 때문이다. (예를 들어 얼마 전 러시아가 일반인들에게 ICO 참여액의 상한선을 정하고 더 투자하고 싶은 사람들은 공인된 기관에서 일정한 교육을 받고 자격을 획득하라고 한 정책 등은 적어도 일괄적인 개인 투자 상한액을 설정하는 제도보다는 훨씬 현명한 방법이다.) 일괄적으로 개인 투자 상한액을 설정하는 등의 방식으로 일반인들의 고위험-고수익 투자 참여를 막으려는 시도는 ICO 시장에서도 비슷하게 반복되고 있다. 따라서 자본주의와 경제적 자유주의 체제하에서 일반 노동자와 시민에게는 자신들에게 막대한 영향을 미치는 금융에 대한 의사결정 권한 즉 '금융 주권'이 없다고 할 수 있다.

기술의 발전과 정보재 : 인간 노동의 필요성 감소에 따른 노동소득 감소 혹은 종말

과거 산업화 시대에 생산의 주요 요소는 토지, 자본, 노동이었다. 그러나 산업이 발달하면서 경영과 기술의 중요성이 커지고 이들이 생산의 주요 요소로 자리 잡았고, 기술에 의한 생산성 증대는 임금 상승으로 이어졌다. 앞서 살펴본 1980년~2000년대에 중요한 변화가 있었는데, 바로 기술이 가진 위상의 변화다. 과거에는 기술이 인간 능력을 보완하고 증가시켜 노동생산성을 높여왔다면 (Brynjolfsson and Saunder,

2009), 지금의 기술은 인간을 복제하여 인간의 정신 노동과 신체 노동을 모두 대체하는 방향으로 발전하고 있다(Brynjolfsson, and McAffee, 2014).

최근 글로벌 플랫폼 기업(아마존, 구글, 페이스북, 우버, 에어비앤비 등)의 주식 가치에서 보듯이, 정보기술과 정보재를 생산의 주요 요소로 활용하는 산업의 영향력이 커지고 있다 (Cusumano, 2017_1; Cusumano 2017_2). 또 물리적 상품을 만들어 제공하는 기업도 기존 상품에 정보기술과 정보재를 활용해 상품 가치를 높이고 있다. (예를 들어 나이키 제품은 헬스케어라는 데이터를 통해 상품 개념을 바꾸고 있다. 이런 움직임은 점차 늘어갈 것으로 예상한다.) 앞서 살펴본 바와 같이 주식회사 체제는 주주의 자본 이득을 높이기 위해 정보기술을 활용해 인간 노동을 대체한다. 정보기술을 적용하지 않는 주식회사는 자본 간의 경쟁 관계에서 도태될 수밖에 없다.

한편, 정보기술을 활용한 중개자 역할을 하는 주식회사 형태의 플랫폼 기업들은 경제학에서 말하는 긍정적 외부효과 즉 정보재를 바탕으로 성장한다. 긍정적 외부효과란 예를 들어 아마존 사이트에 들어가서 디지털카메라, 옷 또는 책을 구입하면 우리의 선택이 기록으로 남아 다른 아마존 이용자들 선택에 도움을 주어 매출과 이익이 늘어나는 효과를 말한다. 주주 자본주의 경제 체제에서는 이러한 긍정적 외부 효과 즉 정보재를 통해 창출된 부의 대부분을 기업이 가져간다. 그리고 이렇게 창출된 이윤의 대부분을 소수 주주가 가져가는 구조다. 반면 이러한 기업들의 혁신은 기존 산업을 파괴하고 파괴된 산업의 일자리는 감소한다. 앞서 예로 든 아마존의 경우, 현재 미국 유통 시장을 재편하고 있으며 이 영향으로 수많은 오프라인 기반의 작은 유통업체들이 문을 닫고 있다. 이 일련의 과정에서 아마존은 '정보기술'을 주로 이용하는 소수의 일자리만 창출한다. 하지만, 그 성장에 기여한 더 많은 소비자이자 노동자는 아마존이 성장함에 따라 역설적으로 일자리를 잃고 있다. AI(Artificial Intelligence)와 빅데이터(Big Data)로 정형화된 새로운 기법은 이러한 경향을 가속화하고 있다. 단언컨대, 이 경향은 결코 바뀌지 않을 것이다.

요컨대, 현재는 토지, 자본, 노동 등의 전통적인 생산요소보다 정보기술과 정보재가 생산요소로서 더 중요하게 작용하는 시대다. 정보기술과 정보재는 쉽게 복제되는 특징이 있어서, 추가 투입이 되더라도 추가 비용이 거의 들지 않는 속성을 갖고 있다. 이러한 속성 때문에 생산성 향상을 위해 정보기술은 지속적으로 적용되고, 적용된 개별 산업 분야에서는 노동의 필요성이 점차 감소한다. 정보기술은 투자 대비 수익이 나는 영역부터 인간 노동을 차례로 제거하는 중이다. 노동이 제거되지 않은 영역은 아직 투자 대비 수익이 나지 않는 영역이다. 그나마 그 영역에서도 점차 임금이 낮은 일자리들만 인간들에게 할당되는 추세로 가고 있다. 하지만 정보기술이 더 발달하여 특정 산업 영역이 투자 대비 수익이 나는 상황이 된다면 그 영역도 정보기술이 어김없이 적용될 것이다. 또한 정보재를 획득하는 체계를 갖춘 플랫폼 기업은 정보재를 통해 사용자 편의성을 높이는 방향으로 상품/서비스를 제공하지만 그 혁신은 기존 산업을 재편하면서 노동의

필요성을 감소시킬 것이다. 이는 기존 경제 위기와는 차원이 다른 국면을 초래한다.

3가지 문제와 새로운 경제 체제의 방향성

우리는 새로운 경제 체제가 앞서 살펴본 3가지 문제를 해결할 수 있어야 한다고 생각한다. 즉, 풍요를 가져온 자본주의의 신용창출 능력을 활용하되, 1) 주주 자본주의가 가진 문제를 극복하여 다수가 쉽게 참여할 수 있는 방안을 만들어야 하고, 2) 그 경제 체제의 신용을 제공한 참여자 다수가 금융 및 신용창출에 대한 의사결정에 참여할 수 있어야 하고, 3) 정보기술과 정보재 발달에 의해 인간 노동이 점차 감소되는 방향으로 갈 수밖에 없다면 그러한 생산 체계를 참여자의 공동 자원(커먼즈)으로 보고 그를 이용한 생산 결과물에 대한 혜택을 보장받을 수 있는 방법을 가지고 있어야 한다.

자본주의의 근본 문제에 대해서 경제학계에서는 글로벌 자본세 도입과 기본소득 혹은 기본 배당을 도입하자는 주장이 나오고 있다. 이러한 방법들은 과감한 정치적인 의사결정이 이루어져야 가능한 사안이다. 그런데 정치적 의사결정이 전제되지 않은 채, 다른 해결책을 만들려는 실험들이 이미 존재한다. 그 접근 방법들을 살펴보자.

1.2 현재 경제 체제의 대안들

현재 경제 체제의 대안은 여러 가지가 있는데, 여기서는 새로운 방향성을 제시하는데 도움이 되는 3가지, 즉 암호경제(Crypto Economy), 커먼즈 운동(Commons Movement), 임팩트 투자(Impact investment) 등을 검토하고자 한다.

암호경제

2017년 전 세계적으로 암호화폐 시장에 대한 관심이 높아졌다. 암호화폐를 기반으로 한 경제 체제를 암호경제라 부르며 이를 새로운 경제 체제의 대안으로 보는 시각도 있다. 암호화폐 프로젝트들은 대부분 1) 블록체인 기술을 통해 탈중앙화를 보장하고, 2) 암호화폐를 통해 해당 경제 생태계 참여자에게 보상할 수 있는 구조를 가지고 있고, 3) 기존 투자 체계와 달리 ICO(Initial Coin Offering)를 통해 누구나 쉽게 투자에 참여할 수 있는 특징이 있다. 이러한 특징을 통해 주주 자본주의가 가진 문제를 극복할 수 있다는 측면에서 암호경제가 주식회사 제도의 대안으로 부상하고 있다. 암호화폐는 앞서 살펴본 새로운 경제 체제의 3가지 조건-낮은 참여 문턱, 다수의 의사결정 참여, 생산수단의 공유에 부합하는 면도 있다. 이러한 기대에 힘입어 2017년 암호화폐 시장은 폭발적으로 성장하였다. 기존에는 벤처캐피털(Venture Capital, 이하 VC)의 투자 하에 새로운 스타트업들이 등장했다면, 요즘은 암호화폐를 매개로 한 ICO를 통해 스타트업들이 대거 등장하였고 ICO기반 스타트업에 투자하는 VC도 나타났다.

BOScoin은 이러한 암호경제에서 참여자의 의사결정 권한을 보강하기 위해서 Congress Network를 도입했다. 그럼에도 백서 1.0에서의 BOScoin을 포함한 현재 암호화폐 대부분이 새로운 경제 체제의 3가지 조건을 충분하게 만족하진 못하고 있다. 특히, 생산체제의 Commons화를 통해 생산수단을 공유하는 등은 거의 고려되지 않고 있다. 한편 인류 공동 노력의 산물로 탄생된 생산 체계를 공동 자원으로 보고 다수가 향유할 수 있도록 만들려는 움직임이 있는데, 바로 '커먼즈 운동'이다. 이제 '커먼즈 운동'에 대해 살펴보자.

커먼즈 운동

백서 1.0에 소개된 Commons Budget은 Common Budget이 아니라, Commons Budget이다. BOScoin의 Commons Budget은 아직 세부 정의와 그 운영 방안이 마련되지 않았지만, 커먼즈(Commons) 운동의 정신을 계승한 부분이 분명 있다. 커먼즈란 공기, 물, 지구와 같은 천연 물질을 포함하여 모든 사회 구성원이 이용할 수 있는 문화 및 천연 자원을 말한다. 이러한 자원은 개인 소유가 아니라 공동 소유이며 커먼즈는 공동체 혹은 사용자 집단이 개인 및 집단 이익을 위해 공동으로 관리하는 자원으로 정의된다. 이러한 흐름들 중에서 정보기술과 정보재를 인류 공동의 저작물이라는 관점에서 커먼즈화 하려는 시도가 특히 돋보이는데, 대표적인 사례가 GNU와 Creative Commons 그리고 이것을 확장한 Commons 운동이 있다.

정보기술과 정보재가 상품의 부가가치를 만들어내는데 많은 부분을 차지한다면 다음 2가지 질문을 던질 수 있다. 첫째, 정보기술과 정보재를 기업이 독점하고 그것을 통해 창출된 부를 독점할 수 있는가? 둘째, 정보기술과 정보재가 생산물의 부가가치에서 차지하는 비율이 높아지고, 일자리를 없애면서 소비 기반이 사라져 전체 경제가 작동하지 않는 환경이라면, 정보기술과 정보재에 의해 창출되는 부가가치를 공동체와 사용자 집단이 공유하는 것은 어떨까? 정보기술과 정보재가 활용된 생산체계를 '커먼즈'로 해석하는 '커먼즈 운동'은 새로운 경제 체제의 3번 생산 체계인 공동 소유 및 사용의 보장 방식을 푸는 중요한 해결책이 될 수 있다.

어떤 공동체와 사용자 집단이 특정 자원을 커먼즈라고 합의한다면, 우리는 그 공유 자원(커먼즈)을 기반으로 생산된 부는 공동체와 사용자 집단이 커먼즈로 공유할 당위성이 있다고 생각한다. 또한 정보기술과 정보재에 의한 노동 소득 기회의 소멸로 소비 기반이 사라지고 있는 현 경제 체제의 악순환을 해결할 수 있는 근본적이고 효과적인 대안이라고 우리는 평가한다. 1.3에서 커먼즈 운동에 대해서 분석하고, 그 철학을 계승한 우리의 제안을 제시할 예정이다.

임팩트 투자

커먼즈 운동과 더불어 적정 수익률과 사회적 가치를 동시에 추구하는 임팩트 투자가 있다. 기존 투자가

경제 및 재무 성과에 집중한 반면, 임팩트 투자는 경제 및 재무 성과를 넘어 사회적·환경적 성과도 함께 추구하는 투자를 말한다. 공공 예산만 갖고 더 이상 사회 문제를 해결하기가 어렵다는 인식 하에 비즈니스를 통해 사회 문제를 해결하겠다는 색다른 시도다. 2012년 투자은행인 골드만삭스가 미국 뉴욕 시가 편 청소년 재범률을 낮추는 사업에 960만 달러를 투자한 사례 등 다양한 사회문제 해결을 위한 임팩트 투자가 최근 활발해지고 있다. 대한민국에도 이같은 임팩트 투자가 상륙하면서 새로운 조류로 떠오르고 있다. 예를 들어 임팩트 투자에 나서는 VC가 생겼고 한국사회투자, 엘로우독 등 임팩트 투자사도 등장했다. 또 부동산 투자 및 관리회사인 공공그라운드는 건축물(부동산)의 문화적(사회적) 가치와 수익을 함께 추구하는 목표를 내걸고 하나하나의 건축물이 독립적으로 사회 문제 해결의 플랫폼으로 작동하도록 만드는 미션을 갖고 있다.

임팩트 투자는 커먼즈를 공동체가 확보할 수 있는 좋은 방법이지만, 소수에 의한 투자 재원이라면 현 경제 체제의 문제를 해결할 수 있는 충분한 방법이 아니라고 생각한다. 다만 임팩트 투자를 통해서, 투자 행위로 사회적 가치를 증대시키는 것이 가능하다는 중요한 사실을 확인했다는 것만 언급하고자 한다.

1.3 대안의 분석과 새로운 방향성

앞서 살펴본 암호경제와 커먼즈 운동이 각각 새로운 경제 체제의 해결책을 제시한다는 것을 살펴 보았다. 1.3에서는 현재의 커먼즈 운동과 암호경제의 한계를 분석해 보고, 보완점과 2가지 대안을 융합하는 방법을 살펴보고자 한다.

커먼즈 운동 대상으로서 화폐와 금융 : Money as Commons

취지가 좋은 것과 현실에서 효과적으로 작동할 것인가의 여부는 별개의 문제이다. 현재 커먼즈 운동은 커먼즈 기반 P2P 생산방식 확대를 추진하고 있는데, 이 방식이 커먼즈 운동의 이상과 목표를 달성할 수 있는지 검토가 필요하다.

무엇보다, 커먼즈가 국가와 시장보다 더 커지기를 바란다면, 특정 영역에서는 국가 단위의 시장에서 혹은 글로벌 단위의 시장에서 경쟁할 수밖에 없다. 예를 들어 우버의 문제점을 해결하기 위해서 협동조합 형태의 플랫폼을 만든다고 하자. 과연 그 플랫폼 협동조합은 우버와 경쟁하여 살아남을 수 있을까? P2P 기반 생산 방식의 제품이 로봇이 만드는 제품과 경쟁할 수 있을까? 감히 예단하건대, 쉽지 않을 것이다. 규모의 경제가 만들어내는 경쟁력을 소규모 생산자 집단이 따라잡기는 쉽지 않을 것이다.

물론, 특정 분야에서는 커먼즈 기반 P2P 생산방식이 의미 있는 성취를 거둘 것이다. 커먼즈 운동의 성공 사례인 GNU와 위키피디아를 분석해 보자. 두 프로젝트는 다음과 같은 공통적인 성격이 있다. 1) 두 프로젝트

모두 초기에 명확한 기여자와 주체가 있었고, 2) 혼자서 할 수 없는 대규모 협업이 필요한 프로젝트였으며, 3) 기여자들은 평판이라는 1차 인센티브와 그 평판에 힘입은 경제적 인센티브도 얻을 수 있는 구조였다. 특히 그 결과물은 기존 자본주의 기업의 결과물과 비교해도 탁월했다. 그렇다면 이 두 가지 프로젝트가 성공할 수 있었던 동력은 어디에 있을까? 첫번째 공통점은 어느 프로젝트나 초기에 명확한 기여자와 주체가 있어야 시작된다는 점에서 성공의 동력이라기 보다는 성공의 조건이라고 보는 것이 타당할 것이다. 세번째 공통점은 비록 평판과 약간의 경제적 인센티브를 얻을 수 있었지만, 그것이 개인들의 참여 동기를 이끌어낼 만큼 큰 것은 아니었기에 성공의 동력으로 보기 어렵다. 우리는 두 프로젝트가 성공할 수 있었던 근본적인 메커니즘은, 기존 자본주의 기업이 동원할 수 있는 협업보다 더 많은 사람들의 협업을 만들어낼 수 있었기 때문이라고 본다(<Nonzero: The Logic of Human Destiny> 참조). 따라서 아마도 (커먼즈 운동이 사회의 지배적인 한 축을 차지하기 전까지는) 사회의 모든 영역이 커먼즈 운동의 대상이 되기는 쉽지 않을 것이다. 대규모 협업을 이끌어 낼 수 있는 영역은 따로 있기 때문이다. (블록체인 기술이 이미 나와 있으니 하는 말이지만) 또한 그러한 대규모 협업에 모든 개인들이 의심하지 않고 참여할 수 있도록 대규모 협업의 신뢰와 안정성을 보장해주는 도구가 필수적이다.

그렇다면 과연 어떤 영역에 커먼즈 운동이 적용되어야 자본주의 문제를 효과적으로 해결할 수 있을까? 우리는 금융이 커먼즈 운동에 가장 필요한 영역이라고 본다. 앞서 살펴 보았듯이 자본주의 체제 하의 자본과 금융 문제를 근본적으로 해결하지 못하면 인류는 현재의 풍요를 더이상 누릴 수 없을 것이다. 신용협동조합 사례에서 볼 수 있듯이, 역사적으로 일반 시민들의 대규모 협업이 금융 영역에서도 없었던 것은 아니다. 다만 과거에는 신뢰를 다룰 수 있는 기술이 부족하여 GNU나 위키피디아 같은 대규모 협업을 만들어내기 어려웠다. 그러나 블록체인과 암호경제가 도입되면 얘기가 달라진다. 우리는 블록체인을 기반으로 한 암호경제를 통해 글로벌 규모의 협업을 이끌어낼 수 있으며, 이를 통해 현재 금융기관들이 창출하는 신용의 크기보다 더 큰 신용을 창출할 수 있다고 생각한다. 나아가 암호경제를 기반으로 대규모 신용을 창출하고, 창출한 신용으로 부가가치를 만들어내는 생산수단들을 커먼즈화 하는 전략이 가능할 것이라고 본다. 이미 BOScoin은 Commons Budget을 도입하여 커먼즈 개념을 일부 반영했었다. 다만 백서 1.0에서 제시했었던 방법론은 이와 같은 목표를 달성하기에 다소 부족한 면이 있었다고 판단한다. 이제 현재 암호경제 현황을 검토하면서 보완할 부분을 제시하고자 한다.

암호경제의 현재 문제점

현재 암호경제가 가지고 있는 한계를 이야기하자면 기술적 한계를 빼놓을 수 없다. 느린 처리속도, 빈번한 해킹 사고로 이어지는 불안전한 스마트 컨트랙트 개발 환경, 일반인들은 그 내용을 알 수 없는 소프트웨어 코드 어딘가에 들어 있는 계약 내용 등. 그러나 이러한 암호화폐의 기술적 한계는 향후 하나씩 극복될 것으로 예상한다. 특히 우리는 이러한 기술적 한계에 대해서는 백서 1.0에서 mFBA와 Trust

Contracts라는 대안을 제시한 바 있다. 우리는 백서 1.0의 기술 전략이 여전히 유효하다고 보고 이를 구현하기 위해 최선의 노력을 기울이고 있다. 따라서 본 백서에서는 기술적 측면보다 사회경제적 관점에서 현재의 암호경제 시장의 전략과 정책을 검토하고 그 문제점을 분석하고자 한다.

1) 사전 확정된 총발행량에 따른 희소성에 의해 발생하는 가격 변동성. 암호화폐 가격이 가진 큰 폭의 변동성은 해당 암호화폐의 성장에 기인하는 측면도 있지만, 가장 큰 원인은 사전에 정의된 총발행량으로 인해 희소성이 기대되기 때문이다. 2008년 금융위기 이후 각국 중앙은행은 이를 타개하기 위해 무분별하게 통화를 발행(양적 완화)했고 이에 따른 화폐 가치 하락에 반발한 사람들이 사전 정의된 총발행량 계획과 탈중앙화된 화폐 체계를 가진 비트코인을 기존 법정화폐의 대안으로 삼고 지지하기 시작했다. 사전에 정의된 총발행량으로 생태계 참여자가 늘수록 희소성에 의해 암호화폐 가치가 오르는 메커니즘(이를 '희소성 메커니즘'이라 하자)으로 암호화폐가 주목받기 시작했고, 2016년 스마트 컨트랙트로 블록체인/암호화폐의 적용 범위를 확대한 이더리움 이후 암호화폐 투자자 수와 투자액이 전 세계적으로 크게 늘어났다. 이러한 희소성 메커니즘은 암호화폐 생태계 참여 유인이자 투자 유인으로 중요하지만, 암호화폐 가격의 큰 변동성을 야기한다. 암호화폐 가격의 큰 변동성은 화폐 기능의 한 축인 지급 결제 수단으로서는 장애 요인으로 작용한다는 시각이 많다. 가격이 오르는 상황이면 암호화폐를 보유하고자 할 것이고, 가격이 내리는 상황이면 암호화폐를 받는 쪽에서 꺼리기 때문이다. 이를 극복하기 위해 법정화폐에 연계된 가치안정 토큰(Stable token) 등의 다양한 시도가 있으나 해당 암호화폐의 가격 변동성을 줄이는 근본 해결책은 아니다. 단일 경제 생태계를 위한 암호화폐의 경우도 가격 변동성 문제가 복잡한데, 동일 플랫폼 위에 다양한 암호화폐를 동시에 사용해야 할 경우는 문제가 더 복잡해진다. 이 문제는 암호화폐 플랫폼들의 Dapp-ICO 전략을 통해 살펴 보자.

2) Dapp-ICO 전략에 따른 화폐 공간의 분절화. 이더리움이 Dapp과 Dapp용 토큰을 발행할 수 있는 기능(ERC20)을 제공하면서 수많은 ERC20 기반 토큰과 ICO가 일어났다. 이더리움은 최근 DAO 해킹 사태 이후 DAO의 문제점을 보완한 DAICO를 소개하였다. 이더리움의 전략은 토큰 발행 플랫폼으로서 암호화폐 시장에 포지셔닝하고 있다. 이더리움뿐 아니라, 이더리움의 한계를 극복하려는 플랫폼형 암호화폐 프로젝트들 대부분이 이러한 Dapp 전략을 취하고 있다. 이러한 Dapp 전략은 초기 플랫폼 확대 전략에는 효과적이다. 특정 암호화폐 프로젝트팀이 모든 걸 할 수 없으니 경제적 인센티브를 통해서 플랫폼에 다양한 프로젝트팀을 참여시키는 유인 전략으로 적절하다. BOScoin 역시 초기에는 이러한 전략에 동의했고 이를 백서 1.0에 반영했다. 하지만, 우리는 Dapp-ICO 전략이 사용처와 사용자를 분절화시켜 플랫폼 암호화폐의 화폐 공간을 축소시킬 가능성이 높다고 판단한다. 화폐는 플랫폼과 유사해서 다수의 사용자, 보유자, 투자자 등이 있고 사용처가 다양하게 존재할 때 가치가 있다. 현재 Dapp-ICO 전략은 동일 암호화폐 네트워크 리소스를 쓴다고 할지라도 화폐 공간을 분절화시킨다. 암호화폐 보유자가 투자자로서 거래소를 가끔씩 이용하는데 큰 불편은 없겠지만, 일상 생활의 빈번한 지급결제를 위해 다양한 암호화폐를 보유하고 사용하는 것은 소비자

입장에서는 매우 불편하다. 현재 암호화폐 보유자 대부분은 암호화폐를 디지털 투자 자산으로 보는 경향이 강하기 때문에 다양한 암호화폐의 등장에 대해 불만을 갖지 않는다고 예상할 수도 있다. 하지만, 우리는 암호화폐 플레이어들이 펴고 있는 Dapp-ICO 전략을 통한 화폐 공간의 분절화가 암호화폐가 현실 세계에 단단하게 뿌리내리는 데 중대한 장애 요인으로 작용할 것으로 예상한다. 이러한 Dapp-ICO 전략은 초기 확산에는 유리한 듯 보이지만 법정화폐의 신용창출 체계와 비교하면 문제가 있다.

3) 분절화된 신용창출 체계. 분절화된 화폐 공간을 방지하기 위해서 BOScoin은 Commons Budget을 통해 Dapp 개발을 추진하였다. 그런데 협업을 위해 많은 기업을 만난 결과 우리는 상황을 냉정하게 파악하게 되었다. 그것은 많은 기업들에게 BOSnet 자체(블록체인 인프라)도 중요하지만 ICO를 통한 신용창출이 더 긴요하다는 사실이었다. 또한 BOSnet 자체는 어떤 사업 모델에는 필수적이지만 또 다른 사업 모델에는 부차적인 역할을 한다는 사실도 알게 되었다. 나아가 협업을 원하는 기업들에게 필요한 신용창출 규모가 Commons Budget만으로는 감당하기 어려운 규모가 있다는 사실도 확인하였다. 기존 법정화폐는 중앙은행이 본원화폐를 발행하고 시중 상업은행의 지불준비금 제도를 통해 신용을 창출한다. 시중 상업은행은 창출된 신용을 바탕으로 또다른 신용을 창출하는 대규모 신용창출 메커니즘을 가지고 있다. 법정화폐를 기반으로 한 금융시스템의 신용창출 체계는 금융자본주의의 핵심이다. 현재 암호경제는 ICO를 통한 최초 신용창출 외에 현 자본주의 금융시스템과 같은 신용창출 체계가 존재하지 않는다. 또한 암호화폐 플랫폼 플레이어가 Dapp-ICO를 통해 창출한 신용을 다른 Dapp-ICO에 전이하기도 어렵다. 즉, 현재의 Dapp-ICO 전략으로는 암호경제가 기존 법정화폐를 기반으로 한 자본주의 신용창출 체계를 뛰어넘기 어렵다고 본다. 암호경제가 확대되어 기존 금융자본주의가 가진 신용창출 체계를 넘어서려면 Dapp-ICO 전략을 대체할 무엇이 필요하다는 뜻이기도 하다.

4) 중앙집중화 문제. 대부분 암호화폐는 경제적 인센티브에 의해 네트워크가 운영된다. 비트코인은 초기 탈중앙화되었다고 각광받았지만 해시파워를 가지고 있는 채굴자 연합체에 의해 전체 네트워크가 좌지우지되는 상황에 처했다. 낮은 수수료가 책정된 거래는 언제 처리될지 모르는 상황에 처했고, 빠른 거래 처리를 위해서는 비싼 거래 수수료를 지불해야 한다. 애초 탈중앙화로 거래수수료가 낮아질 것이라는 암호화폐 찬성론자들의 기대와 다른 상황이 벌어진 것이다. PoS나 DPos 방식 역시 중앙집중화 문제가 PoW와 유사하게 일어날 것으로 예상된다. EOS의 사례에서 우리는 이미 이러한 중앙집중화 문제가 발생한다는 사실을 확인했다. 분산화된 네트워크 합의 과정을 경제적 인센티브에 기반 한 시장 메커니즘에 맡기자 집중화가 일어난 것이다. 이러한 중앙집중화는 우리가 암호화폐 경제 체제에서 바라는 바가 아니다. 더욱이 거버넌스 체계가 없는 암호화폐들은 중앙집중화 문제를 해결하는 데 매우 어려운 상황에 직면해 있다. 중앙집중화 문제는 심지어 거버넌스 체계를 갖춘 BOScoin에서도 보완해야 할 부분이 많다.(이것에 대한 문제 해결은 백서 개정판에서 다루고자 한다.)

2. 제안

서론의 내용을 정리하면 다음과 같다. 정보기술과 정보재가 중요해진 현재 자본주의 체제에서는 분배 문제를 해결하기 힘들고, 노동 소득이 줄어드는 경향이 있다. 이는 소비 기반이 무너지는 것을 뜻하며 소비 기반 없이 자본주의 체제는 작동하지 않는다. 이러한 문제를 해결하기 위해서는 분배 문제를 해결할 수 있는 체계가 필요한데, 암호경제를 기반으로 이에 대한 해결책을 만들 수 있을 것이라고 생각한다. 하지만, 현재 암호경제의 Dapp-ICO 전략으로는 분절화된 화폐공간과 분절화된 신용창출 체계가 양산될 가능성이 높고 분절화된 신용창출 체계로는 BOS팀이 풀고자 하는 문제를 해결하기 어렵다는 결론을 도출했다.

공공금융(Public Financing). 앞서 살펴본 Dapp-ICO 전략으로 인한 분절화된 신용창출 체계 문제를 해결하기 위해 우리는 공공금융(PF)을 제안한다. PF는 중앙은행이나 정부가 아닌, 실제 신용을 사용하고 거래하는 개인이 집단적으로 의사결정하여 신용을 창출하는 방식을 뜻한다. 즉 커뮤니티가 신용창출의 주체가 된다. 다른 암호화폐 플랫폼과 달리 BOS 플랫폼이 공공금융을 제안할 수 있는 것은 Congress Network라는 거버넌스 체계를 갖추고 있기 때문이다. 자본주의 체제에서는 법정화폐와 제도화된 금융 체계에 의해 소유한 자본에 비례하여 금융에 대한 의사결정이 이루어지며, 체제에 참여하는 구성원 대부분은 자신의 의지와 상관없이 그 의사결정을 따라야 한다. 하물며 체제를 탈퇴하기도 어렵다. 반면 BOScoin을 포함한 암호화폐는 커뮤니티 화폐로서, 커뮤니티의 의사결정에 커뮤니티 구성원들의 의사가 반영되지 않으면 커뮤니티를 탈퇴할 수 있다. 즉 커뮤니티 구성원들의 의사를 반영하지 못하는 커뮤니티는 성장하기 어려운 것이다. 따라서 암호경제를 확장하고자 한다면 커뮤니티 구성원의 다수 의사가 반영될 수 있는 구조를 최대한 보장하는 것이 바람직할 것이다. 하지만 백서 1.0에서 제안한 BOScoin Congress Network의 투표 방식은 BOScoin 다수 보유자가 다수의 Node를 만들 수 있으며, 이를 통해 많은 노드를 운영할 수 있는 사람이 커뮤니티 의사결정에 더 많은 영향을 줄 수 있는 구조이다. 이러한 문제를 해결하기 위해서 1인 1표가 가능한 시스템을 만들어야 한다. 1인 1표가 최선의 방법인지에 대해서는 반론의 여지가 있을 것이다. 그러나 우리는 최소한 1인 1표에서 출발하지 않고 예컨대 1주 1표와 같은 방식으로 출발한다면, 향후 더 나은 거버넌스 구조를 구축하는 것은 불가능하다고 생각한다. 이런 측면에서 1인 1표는 최종 해답은 아니지만 가장 좋은 출발점이다. 그런데 1인 1표를 부여하기 위해서는 개인 식별을 해야 하고, 개인 식별을 하는 순간 프라이버시와 의사표현의 자유를 침해할 수 있다는 점에서, 백서 1.0을 쓰는 당시 이 난제의 해결책을 찾지 못하였고, 제대로 된 Congress Network의 의사결정 구조를 짜는 문제는 해결 과제로 남아 있었다. 우리는 KoSAC과 함께 이 문제를 검토하였고, 이에 대한 해결책으로 동형암호 기반 Congress Voting을 제안한다. 이에 대해서는 2.2 Congress Voting 에서 자세히 다룬다.

2.1 Public Financing

배경

PF를 도입한 배경은 앞서 서론에서 살펴본 바와 같다. 요약하면, 현재 경제 체제의 문제점을 해결하기 위한 여러 대안 중 암호경제가 자본주의 신용창출 메커니즘을 활용하고 분배 문제를 해결하는 데 있어서 가장 효과적이라고 우리는 평가했다. 다만 현재 암호경제 시장의 Dapp-ICO 전략은 화폐공간을 분절화시키므로 자본주의 체제의 대안이 될 만한 새로운 신용창출 메커니즘으로 적절치 않다.

정의와 의미

PF는 BOScoin 커뮤니티가 실물경제의 다양한 자산을 획득하기 위한 신용창출 수단으로 커뮤니티 외부의 제3자로부터 투자를 받는 것이 아닌, 커뮤니티 자체적으로 BOScoin을 추가 발행하는 것을 뜻한다. 즉, 추가 발행의 주체는 커뮤니티다. 커뮤니티 스스로가 Congress Network를 통해 추가 발행과 정책을 제안, 검토, 투표, 결정한다. 이렇게 결정된 내용은 BOScoin의 Trust Contracts를 통해 실행된다. 그리고 Trust Contracts를 통해 실행된 PF를 통해 확보한 실물경제의 다양한 자산 및 투자의 결과물은 커뮤니티에 귀속되고 별도로 커뮤니티 구성원에게 분배되지 않으며, 그 운용 역시 커뮤니티 스스로 주체가 되어 결정한다. 이러한 일련의 과정을 우리는 공공금융(PF)이라고 정의한다.

PF가 Commons Budget과 다른 점은 다음과 같다. 첫째, 백서 1.0에서 정의된 50억 개 BOScoin의 발행 플랜 이외에 커뮤니티가 의사결정을 통해 추가 coin을 발행한다는 점이다. 둘째, Commons Budget이 비용 개념에 가깝다면, PF는 투자 개념에 가깝다. 셋째, 투자 개념에 가까우므로 커뮤니티가 추가 발행한 BOScoin은 발행량에 대응하는 자산(투자된 대상이 보유한 자산)이 대부분 존재할 것이다. 넷째, Commons Budget은 이익 공유를 고려하지 않은 모델이지만, PF는 이익 공유를 고려해 설계해야 하고 해당 로직을 넣어야 실행된다. 미래의 이익에 대한 공유 계획이 없으면 커뮤니티 구성원들이 해당 PF를 BOSnet 내에서 집행할 이유가 없기 때문이다.

'Public Financing'이라는 용어는 기존 투자은행들의 비즈니스 모델인 'Project Financing'에 대비하여 만든 용어로서 2가지 측면에서 공공적(Public)이다.

첫째, 금융주권 즉 금융과 관련한 의사결정 권한이 커뮤니티 구성원 다수에게 있다. 이때 Public의 의미는 '공공재에 투자'한다는 개념보다는 Project Financing을 기존 금융기관만 하는 것이 아니라, 'BOScoin Community 멤버들의 합의에 의해서 신용을 창출(money creation by the BOScoin Community people)한다'는 개념에 가깝다. 이러한 커뮤니티의 의지와 의사결정에 의한 신용창출 방식은 서론에서

살펴본 자본주의 체제 문제 중 하나인 '금융주권' 문제를 해결한다. BOSnet에서 PF가 가능한 이유는, BOScoin이 Congress Network이라는 거버넌스 체계를 갖췄기 때문이다.

둘째, 확보한 실물경제 자산을 커먼즈로 본다는 것은 발생한 부를 경제적 의미에서 커뮤니티 공동의 것(public)으로 본다는 뜻이다. 즉, 커뮤니티가 PF를 통해 커먼즈를 확보하고 커먼즈를 통해 발생하는 부를 커뮤니티 멤버들과 공유할 수 있다는 점에서 공공적('Public')이라고 할 수 있다. 이는 서론에서 언급한 자본과 기술에 의해 발생하는 노동 소득 감소 혹은 종말이라는 자본주의 체제의 당면한 문제를 해결할 수 있는 방법이라고 생각한다.

BOScoin 커뮤니티가 Congress Network에 발의한 PF 안건은 PF 정책과 목적, 기대효과 외에 발행 규모, 발행 조건과 커뮤니티 멤버들과의 이익 공유, 지속 가능한 경제 시스템에 대한 재투자 등을 포함할 것이다. 그리고 구체적인 투자 전략은 개별적인 PF 안건에 의하여 정해질 것이나, 단순한 금전의 대여나 이와 유사한 형태의 대출은 지양할 것이며, BOScoin Network 참여 기업에 대하여 불가피하게 금전적 지원이 필요한 경우에는 이자를 수취하지 않는 방법의 지원이 이루어질 것이다. 이처럼 BOScoin Network의 참여자 모두에게 실질적인 이익을 공유할 수 있게 하는 PF는 암호화폐 시장에서 다른 프로젝트들과 차별화되는 BOScoin의 vision, 정체성이자 경쟁 전략이다. 또한 백서 개정판에서 소개할 BOScoin Network 참여 기업인 GTTP의 생태계 구축을 위한 메커니즘이기도 하다.

우리는 실제 PF에 대한 경험을 토대로 보다 현실적인 방안을 만들기 위해, 일정 규모의 PF를 Pilot 형태로 진행할 수 있도록 할 예정이다. 이러한 Pilot 프로젝트를 통해 세부적인 Process와 다양한 데이터를 커뮤니티에 제공하여 의사결정의 질을 높인 뒤 본격적인 Congress Network 투표 프로세스를 적용할 계획이다. 이 Pilot 프로그램은 RIPP(Reverse ICO Partner Program)의 형태로 구체화되었다.

Reverse ICO Partner Program

PF는 그 목적에 따라, 투자를 위한 SME(Small and Medium Enterprise) PF, 커뮤니티 보상을 위한 Reward PF, BOScoin 인프라 구축을 위한 Infra & System PF 등으로 분류할 수 있다. 그 중, SME PF의 경우에는 파트너사의 비즈니스 모델 검증, 사업 역량 검증, BOScoin과의 시너지 효과 검증 등의 과정이 수반되어야 한다. 따라서 PF 이전에 파트너사에 대한 일련의 검증 절차로서 Reverse ICO 과정을 포함하는 RIPP(Reverse ICO Partner Program)를 개발하였다. 파트너사는 RIPP 단계를 거치면서 비즈니스 모델과 사업 역량을 커뮤니티에 검증 받게 되고, 이를 통해 커뮤니티는 최종적으로 Congress Voting을 통해 해당 파트너사의 PF 참여 여부를 결정할 수 있다.

2.2 Congress Voting

배경

블록체인은 코드화된 프로토콜이며 기술로서 분권화되었고, 불변이며, 신뢰가 불필요한 데다 비정치적으로 특정된다. 이에 블록체인은 인프라에 의한 거버넌스(governance of the infrastructure)라고 칭송받았다.(Sclavounis O., 2017) 하지만 블록체인 프로젝트에서도 사람의 역할은 존재한다. 시스템 창조와 관리는 커뮤니티에 속한 다양한 이해관계자에 의해 이루어지며, 이는 인프라에 대한 거버넌스로 정의될 수 있다.(De Filippi, P. & Loveluck, B., 2016) BOScoin의 자기 진화를 향한 의사결정은 '사람들'에 의해 이루어지며 여기서 '자기 진화'란 사람들의 토론과 의사결정으로 이루어진다.
모든 블록체인은 두 가지 층의 거버넌스를 가지고 있다.(Myungsan Jun, 2018) 블록체인에서 데이터에 대한 합의 과정은 직접민주주의 원칙에 따라 이루어진다. 모든 노드는 자유롭게 들어와서 거래를 확인하고 합의하기 위해 평등하게 참여한다. 합의가 51% 또는 2/3 기준 등으로 만들어질 것인지는 선택의 문제다. 핵심 아이디어는 모든 참여 노드가 합의에 이르기 위해 동등한 권리와 참여 기회를 부여받는다는 점이다. 그런데 두번째 거버넌스의 경우, 초기 암호화폐 프로젝트들은 변화를 수용하기 위한 공식 의사결정 장치가 거의 존재하지 않았으며, 혹은 있더라도 이러한 노력 대부분이 블록체인 외부(Off-chain)에서 행해진다. 블록체인은 힘(계산력)의 논리로 시작되었다. 채굴이란 규모의 경제를 따르는 비즈니스이기에 자연독점 현상이 예견되었고, 거대 채굴사업자로 세력이 집중되었다.(Ehrsam F., 2017) 사용자나 개발자와 같은 다른 참여자들은 이 세력 구성에서 제외되었다.

문제는 중앙집중화만이 아니다. 시스템 품질이 떨어지거나 구성원 이익을 감소시킬 때, 구성원은 탈출(다른 프로젝트로 이동하거나 하드포크) 외에 다른 선택지가 없으며, 이는 곧 네트워크 효과의 감소로 이어진다.(Albert O. Hirschman. 1970) 만약 참여하는 모든 멤버가 의견을 개진하고, 그들의 이익을 증대시키는 변화를 만드는 데 참여할 수 있는 통로가 있다면, 멤버 유지율은 더 높아질 것이다. 또한 커뮤니티가 문제를 더욱 잘 이해하고, 당면한 문제를 해결하기 위해 보다 많은 의견과 해결책을 제시하는 것이 시스템의 발전에도 도움이 된다. 효과적인 거버넌스 시스템을 통해 더 많은 네트워크 참여자의 목소리를 포함하고 극대화 할 수 있다.(Duncan L., 2017)

암호화폐 프로젝트들은 이를 인식하고 다양한 기제를 도입하기 시작했다. 마스터노드 투표와 DGBB(탈중앙화 거버넌스 블록체인 예산) (Wiecko Robert., 2018) 혹은 지분 기반의 투표 시스템이 대표적인 사례다. 이와 같은 노력이 인프라에 의한 거버넌스(governance of the infrastructure, 이하 “인프라 거버넌스”)에 보완적인 분권화 계층을 추가했다. 그러나 이같은 시스템은 많은 자원을 가진 이가 큰 영향력을 행사하는 주식회사 제도에 가깝다. 소수의 부자가 시스템을 지배하게 되면, 커뮤니티는 부자들에게 점점 더

이득을 주는 쪽으로 변화가 이뤄질 가능성이 크다. 이것은 부의 집중과 불평등이 심화되는 자기 강화 시스템을 만들고, 일반 멤버는 자신이 만들어내는 가치에서 점점 더 멀어지는 결과를 낳는다.

우리가 네크워크 상에서 모든 사람이 평등하게 대표성을 띠어야 한다고 생각한다면 네트워크는 각 개인을 식별해야한다. 이 과정 없이는 시빌 어택(Civil attack)에 취약하기 때문이다. 시빌 어택이란 공격자가 P2P 네트워크에서 다수의 가짜 아이덴티티를 구축하여 비정상적으로 큰 영향력을 끼치는 것이다. 그런데 시빌 어택을 방지하기 위해 개인 식별 정보를 수집하는 순간 사용자의 프라이버시가 침해된다. 프라이버시와 접근성을 희생하지 않으면서 블록체인에서 실존재를 수용할 수 있는 해결책이 없다면, 인프라 거버넌스(governance of the infrastructure)에 동일한 가치를 적용하는 것은 여전히 숙제로 남고 블록체인의 약속 또한 절반의 약속에 그치고 말 것이다.

정의

BOScoin의 탈중앙화되고 민주화된 인프라 거버넌스(governance of the infrastructure)는 우리가 Congress Network(의회 네트워크)라고 부르는 플랫폼으로 현실화될 것이다. 의회 네트워크는 BOSnet에서 온전히 기능하는 민주적인 의사 결정 기구가 될 것이다. 의회 네트워크는 완전한 익명성을 보장하면서 시빌 어택을 방지하기 위해 참여 개체를 식별하고 확인할 수 있는 최신 암호화 솔루션을 도입할 것이다. 의회 네트워크는 군중의 지혜(Surowiecki J., 2005)를 최대화하고, 다양하고 독립적인 의견을 가장 잘 반영해 이를 합법적인 방식으로 집계하기 위해 여러 단계의 의사결정 과정을 거친다. 의제 설정, 제안서 제출, 토론 촉진 및 투표의 모든 층위에서 탈중앙화가 일어날 것이다. 이하 BOSnet상에서 Congress Network를 적용하기 위하여, 각 준거 국가의 개인정보 관련 법령에 따른 제반 절차를 준수할 것임을 전제로 한다.

동형암호

완전동형암호, 또는 간단히 동형암호란, 1978년에 이미 Rivest, Adleman, Dertouzos에 의해 구상되고 2009년에 Craig Gentry에 의해 처음으로 구현된 암호화 방법의 한 종류를 말한다. 동형암호는 비밀키에 대한 접근을 필요로 하지 않고 암호화된 데이터에서 직접 연산을 할 수 있다는 점에서 통상적인 암호화 방법들과 다르다.(Homomorphic Encryption Standardization homepage, 2018) 반면 기존 암호기술은 복호화에 필요한 키가 물리적으로 연산이 이루어지는 서버에 보관되거나 외부에서 평문으로 변환된 데이터를 제공해야 하며, 키가 탈취되거나 평문 상태로 데이터가 유출되는 등의 취약성을 갖는다.

비대칭 암호문

`E = (KeyGen, Encrypt, Decrypt)`

은 다음의 연산이 가능하면 동형적이라 할 수 있다.

메세지 상 + 연산 (곱셈과 같은 다른 연산도 가능하다)

공개키 pk와 두개의 암호문 c1, c2에 '더하기' 알고리즘하여 새로운 암호문 s를 도출해내는것

정확성에 대한 조건은 모든 메세지 m1, m2에 대해 d= m1+m2이 반환되어야 한다.

```
(pk, sk) ← KeyGen(); c1 ← Encrypt (pk, m1); c2 ← Encrypt (pk, m2);
f(c1, c2) = Encrypt{pk, f(m1, m2)} (Bernhard D., Warinschi B., 2014)
```

가입

개인(entity)이 의회 네트워크에 참여하려면 먼저 의회 멤버십을 획득해야 한다. 누구나 의회 구성원이 될 수 있다. 국적이나 성별 등은 중요하지 않다. BOS 커뮤니티에 속한 사람이라면 BOSnet 이해관계자로서 커뮤니티에 기여할 수 있도록 진입 장벽이 낮아야 한다. 또한 접근성만큼 중요하게, 거버넌스에 참여하는 개인 Identity의 유일성을 확인함으로써 시빌 공격 가능성을 차단해야 한다. 다만 이것이 네트워크에 참여한 사람이 누구인지 개인의 정체성을 식별해야 함을 의미하지는 않는다. 단지 이 사람이 네트워크 구성원이고 단 한 사람의 Identity라는 것, 즉 한 사람이 복수의 Identity를 가지고 있지 않다는 확인만 하면 된다. 따라서 우리의 목표는 최소한의 개인 정보를 활용하여 유일성을 검증하며 이 과정을 검증 사실을 증명하는 토큰 발급 단계와 분리함으로 프라이버시와 Identity의 유일성을 보장하는 것이다. 토큰을 발급하는 어카운트는 블록체인 상에 형성되며 멤버는 토큰으로 자신의 유일성과 의회 멤버십을 증명할 수 있게 되며 IDA 라는 공개주소를 가진다.

단기적으로는 여권 등의 인증서가 사용되겠지만, 장기적으로는 개인의 물리적인 존재와 유일무이성을 홍채와 같은 생체인식기술로 인증할 것이다. 이것의 가장 큰 장점은 이름, 주민번호, 주소 등의 개인정보 없이도 '1 to n' 매칭이 가능하다는 점이다.(B. Thiyaneswaran, S. padma., 2012) 신원확인 데이터는 TTP의 생체정보 저장소에 기록되며, 신원확인 정보 저장소(Repository)에서 Identity 역추적을 불가능하게 만들기 위해 동형 해시 알고리즘이 적용된다. 신규로 등록되는 모든 신원확인 데이터는 기존 데이터베이스에 동일한 혹은 상당히 비슷한 데이터가 있는지 비교하는 과정을 거친다. onboarding request에서 유입된 데이터와 일치하는 것이 발견되면 해당 request는 거부된다. 신원확인 정보 저장소는 블록체인 외부의 데이터베이스로, 중앙집중형 클라우드 서비스로 구현될 것이다. 비록 이 부분에서 Third Party에 대한 어느 정도의 신뢰가 필요하지만, 이것은 확장성에 장점이 있으며 모든 데이터가 항상 암호화된 형태로 보관되므로 보안 위험 없이 손쉽게 배포할 수 있다. 또한 Third Party 생체정보 저장 서비스는 그 자체가 블록체인 거래나 의사결정 과정에 전혀 관여하지 않기 때문에, BOSnet이나 의회 네트워크가 이 TTP에 의존하지 않는다는 것을 의미한다.(Zyskind, Nathan, Pentland, 2016) 또한, 위 정보는 개인정보는 블록체인 상에 포함되거나 또는 어카운트와 결합하여 간접적으로 개인을 식별할 수 있는 형태로 보관되지 않도록 조치된다.

투표

투표가 실행되기 위해, 해당 주제에 대한 투표 프로그램(공개주소 IDV)이 생성된다. 각 멤버는 IDA와 IDV별 단 하나의 투표지(BallotStamp)를 발행 받으므로 단 하나의 투표권이 주어진다.

- Requirements
  1. Eligibility / 투표권: 유권자 여부, 즉 투표에 참여할 자격이 있는 사람인지 확인할 수 있어야 한다.
  2. Privacy / 비밀투표: 투표를 한 사람 본인 외에는 누가 어떻게 투표하였는지 알 수 없어야 한다. 즉 투표자와 투표 결과를 연결지을 수 없어야 한다.
  3. Unforgeability / 위조불가능성: 투표 용지와 투표 결과를 위조할 수 없어야 하고 투표 내용을 조작할 수 없어야 한다.
  4. Uncoercibility / 강요불가능성: 투표를 강요하거나 투표권을 매매할 수 없어야 한다.
  5. Singularity / 중복투표배제: 하나의 Proposal에 대해 한 사람은 하나의 투표권만 행사할 수 있어야 한다. 투표 진행 기간 중, 즉 투표 마감 전까지는 기존 결정을 번복할 수 있도록 허용한 경우, 개표 시에 마지막 투표 용지만 집계되어야 한다.
  6. Completeness / 완전성: 투표용지가 누락 또는 삭제되지 않아야 하며 유효한 투표 용지가 정확하게 투표 결과에 반영되어야 하고 유효하지 않은 투표 용지는 결과에 반영되지 않아야 한다. 투표 결과가 정확히 집계되어야 한다.
  7. Fairness / 공정성: 투표 진행 과정에 투표권 행사가 다른 사람의 투표권 행사에 영향을 받지 않아야 한다. 즉, 중간 투표 결과가 전체 투표에 영향을 미치는 일이 없어야 한다.
  8. Verifiability / 확인가능성: 투표자가 자신의 투표권 행사 내용이 투표 결과에 제대로 반영되었는지 확인할 수 있고, 전체 투표가 공정하게 이루어졌음을 누구나 확인할 수 있어야 한다. (Fujioka A., Okamoto T., Ohta K., 1993), (Çetinkaya O., Doganaksoy A., 2007)

- Voting Preparation : Getting a Ballot Stamp

  등록 과정을 통해 구성원들은 계정 모듈(1. Eligibility 보장)과 투표 프로그램에 연결되어 있는 개인 멤버 지갑을 획득하게 된다. 개인 지갑은 일회성 PKI 열쇠를 생성한다. 가입 단계에서 확인된 유권자의 자격 여부는 IDA 으로 확인한다.

  멤버는 투표지를 신청할 수 있다. 신청 시, 유권자에게 랜덤값이 보내지고, 유권자는 이를 자신의 개인 키로 동형암호화 해서 투표 프로그램으로 보낸다. 투표 프로그램은 동형암호의 성질을 사용해서 Encrypt(RE)를 바탕으로 BallotStamp를 생성한다.

  $$Encrypt(BallotStamp) = f\{IDA, IDV, Encrypt(RE), RA\}$$

  이 투표지는 신뢰할 수 있는 영역에서 만들어지지만 이를 생성하는 투표 프로그램조차 자신이 생성한

값의 평문화 값을 알지 못하여 어떤 개인과도 연결시킬 수 없다(2. Privacy 보장). Ballot Stamp는 공개된 영역에서 만들어지지만, 이를 풀어서 사용할 수 있는 것은 해당하는 프라이빗 키(private key)를 가지고 있는 유권자뿐이다.

해당 투표지 생성 요청 단계와 투표 행위를 분리함으로써 두 사건에 대한 시간의 연결성을 없앨 수 있다(2. Privacy 보장).

- Casting Votes

  투표지가 멤버에게 전달되면 멤버는 그가 가진 프라이빗 키를 이용하여 투표지를 해독하고 암호화된 채널을 통해 투표지와 함께 자신이 결정한 사항을 투표 프로그램에 직접 전송한다. 평문 투표지는 당사자 이외에 다른 누구에게도 알려지지 않기 때문에, 사용자는 임의로 복수 투표지를 만들어 여러 번 투표해도 투표프로그램은 투표지만으로 복수 투표 여부를 구별할 수 없다. 이러한 상황을 방지하고 Ballot Stamp에 대한 소유권을 가진 키를 보유한 개인이 정상적으로 복호화한 값을 투표프로그램 쪽에서 확인할 수 있게 투표프로그램은 멤버에게 태그값 형태로 투표지를 전송한다.

  ```
  Tag =f{sk, Encrypt(BallotStamp)}
  ```

  sk는 투표프로그램만이 아는 비밀값으로 Encrypt(BallotStamp)에 대한 키를 가진 사람 이외에는 유추가 불가능하다. f는 공개되어 있고 XOR연산 또는 Blind Signiture 방식 등이 활용될 수 있다. 동형성질을 지닌 연산이기에 다음과 같은 예시가 가능하다.

  ```
  Encrypt(BallotStamp)*sk1+sk2 = Encrypt(BallotStamp * sk1 +sk2)
  ```

  멤버는 sk 값을 풀어 투표지, 결정와 함께 투표프로그램으로 전송한다. sk가 올바르다면 투표 프로그램은 BallotStamp, 투표 결과, sk을 추후 확인 가능하도록 저장한다(3. Unforgeability 보장). sk값은 BallotStamp와 계산되기 전에 해시하여 공개할 수 있다. 이를 통해 추후 투표 프로그램의 완전성을 확인할 수 있다.

  멤버는 BallotStamp를 여러 번 신청할 수 있지만 시스템은 매번 같은 값의 BallotStamp를 생성한다. 즉, 사용자는 투표기간 내 같은 Ballotstamp로 여러 번 투표에 참여할 수 있다. 투표 기간에 새로운 정보가 나올 수 있고, 유권자는 자유롭게 자신의 결정을 바꿀 수 있어야 하기 때문이다. 또한 원격 투표에서 발생할 수 있는 강압 투표의 가능성을 차단할 수 있다. (4. Uncoercibility 보장)

- Tallying the votes

  선거 기간이 끝나면 투표 시스템은 투표 결과를 저장한다. 각 투표 날짜와 시간은 보관되며, 같은 투표지가 중복으로 행사된 경우, 마지막 투표만 최종 결과로 집계된다 (5. Singularity 보장). 이

프로세스와 결과는 검증이 가능하기에 결과가 블록체인에 기록되며 유효 투표가 누락되지 않는다 (6. Completeness 보장). 투표가 완료된 후에 집계가 실시되기 때문에, 투표에 영향을 줄 수 있는 부분 집계는 공개되지 않는다 (7. Fairness 보장).
결과 집계가 완료되면, 모든 결과는 블록체인에 보관된다. 회원 자신이 일반 텍스트 투표 스탬프를 알고 있으므로 회원은 투표가 제대로 고려되었는지 확인할 수 있다 (8. Verifiability 보장).

이러한 과정을 통해 Congress Voting 프로토콜은 위에서 설명한 모든 요구 사항을 충족시킨다.

3. 결론

경제학자 케인스는 이런 말을 남겼다. "새 아이디어를 생각해내는 것이 아니라 옛 아이디어에서 벗어나는 것이 어렵다."

그렇다면 중앙은행과 기존 금융기관만 신용창출을 할 수 있다는 시선에서 벗어나 보면 어떨까? 암호화폐 플랫폼이 현재의 금융자본주의 시스템보다 우수한 신용창출 체계를 갖춘다면 어떨까? 암호화폐는 극심한 등락폭 때문에 교환 매개 수단, 지급 결제 수단, 가치 저장 수단으로 적절하지 않기 때문에 화폐가 아니라는 비판을 받고 있다. 앞선 분석과 같이 기존 암호화폐는 주권화폐와 비교하여 신용창출 능력이 떨어진다. BOScoin은 이를 보완하기 위하여 다른 암호화폐와 달리 Congress Network라는 거버넌스 체계를 갖추고 기존 ICO와 대비되는 공공금융(PF)이라 명명한 커뮤니티에 의한 신용창출 체계를 도입하고자 한다.

또한 커뮤니티가 PF를 통해 창출한 신용으로 확보한 실물경제 자산(부)을 '공동의 것'(커먼즈)으로 보고, 커뮤니티의 합의에 따라 이를 사용할 수 있는 시스템을 만들어 편중된 부의 분배 문제를 해결할 수 있도록 할 것이다. 우리는 자본과 기술에 의해 발생하는 노동 소득 감소 혹은 종말이라는 자본주의 체제의 근본 문제를 PF로 해결할 수 있다고 믿는다.

아울러 이러한 PF를 실행하기 위해 필요한 Congress Network는 개인을 식별해야 한다. 우리는 개인을 식별하는 과정에서 발생할 수 있는 프라이버시 침해를 막기 위해 투표의 익명성을 보장하고 다수의 가짜 아이덴티티를 구축하여 비정상적으로 영향을 끼치고자 하는 시빌 어택을 차단할 수 있도록 동형암호를 이용한 Congress Voting을 도입하고자 한다. 이를 통해 커뮤니티에 의한 신용창출 과정에서 화폐 보유량이 아닌, 사람 기준으로 1인 1표를 부여 받고 커뮤니티 구성원은 안심하고 참여함으로써 군중의 지혜를 극대화하며, 다양하고 독립적인 의견을 공유할 수 있는 시스템을 구축할 것이다.

우리는 이어 본 백서에 담지 못한 내용을 백서 개정판에 실을 계획이다. 백서 개정판은 온라인 외에 오프라인 세계와 연결하는 고리로서 GTTP 개념과 함께, 보다 나은 자본주의를 향한 BOScoin 경제 모델을 담는다. 우리는 옛 아이디어에서 벗어나 새 아이디어를 제안하여 가장 자본주의적인 방법으로 자본주의를 해킹할 것이다. 우리는 모든 역사적 성취들이 성취가 가시화 하기 직전까지는 언제나 '불가능한 꿈'이었다는 사실을 알고 있다. 2018년, 탄생 200주년을 맞이한 마르크스는 자본주의 체제의 각종 폐해가 드러날수록 끊임없이 호명되고 반추되고 있다. 자본주의 발달이 경제적인 풍요를 불러왔지만 불평등과 노동 소외, 분배 문제 등을 해결하지 못했기 때문이다.

우리는 새로운 암호경제 체제의 초석을 다지는 BOScoin 프로젝트를 통해 세상을 근본적으로 바꾸는 혁신에 동참할 것이다. 이 프로젝트는 기술혁신과 사회혁신을 연결하여 사회적 신뢰 체계를 새롭게 구축하는 것을 목표로 한다. 세상에는 잠시 멈춰 세울 수는 있어도 돌이킬 수 없는 커다란 흐름이 존재한다. 우리는 블록체인/암호화폐가 그러한 흐름의 하나라고 생각하며, 많은 사람들이 기술과 사회를 혁신할 수 있는 프로젝트에 함께 하기를 희망한다.

Reference

- Piketty, T. Capital in the Twenty-First Century. Belknap Press, 2017.
- Brynjolfsson, E., and McAffee, A. The Second Machine Age: Work Progress, and Prosperity in a Time of Brilliant Technologies. W.W. Norton and Company, 2014.
- Brynjolfsson, E., and Saunders, A. Wired for Innovation: How Information Technology is Reshaping the Economy. The MIT Press, 2009. Cusumano, M.A. "The sharing economy meets reality," Communications of the ACM, 61 (1): 26-28, 2017. Cusumano, M.A. "Amazon and whole foods; follow the strategy (and the money)," Communications of the ACM, 60 (10): 24-26, 2017.

Congress Voting

- Myungsan Jun (2018) Blockchain Government: A next form of infrastructure for the twenty-first century. CreateSpace Independent Publishing Platform June 15, 2018 (https://boscoin.io/blockchain-government-free-download/)
- Sclavounis O. (2017) Understanding Public Blockchain Governance. Oxford Internet Institute. Retrieved March 18, 2018 from https://www.oii.ox.ac.uk/blog/understanding-public-blockchain-governance/
- De Filippi, P. & Loveluck, B. (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review, 5(3). Retrieved March 18, 2018 from https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure
- Ehrsam F. (2017) Blockchain Governance: Programming our future. Retrieved March 18, 2018 from https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74
- Albert O. Hirschman. 1970. Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States.Cambridge, MA: Harvard University Press. Retrieved March 18, 2018
- Duncan L. (2017) Thoughts on Governance and Network Effects. Medium. Retrieved March 18, 2018 from https://blog.aragon.one/thoughts-on-governance-and-network-effects-f40fda3e3f98
- Wiecko Robert. (2018) Understanding the Governance and Budget System. Dash Official Documentation. Retrieved March 18, 2018 from https://dashpay.atlassian.net/wiki/spaces/DOC/pages/8585240/Understanding+the+Governance+and+Budget+System
- Surowiecki J. (2005) The Wisdom of Crowds: Why the many are smarter than the few and how collective wisdom shapes business, economies, societies, and nations. Anchor. Retrieved March 18, 2018
- Homomorphic Encryption Standardization homepage, Retrieved March 18, 2018 from http://homomorphicencryption.org/introduction/
- Bernhard D., Warinschi B. (2014) Cryptographic Voting — A Gentle Introduction. In: Aldini A., Lopez J., Martinelli F. (eds) Foundations of Security Analysis and Design VII. Lecture Notes in Computer Science, vol 8604. Springer, Cham, Retrieved March 18, 2018 from https://link.springer.com/chapter/10.1007/978-3-319-10082-1_7 [10] B. Thiyaneswaran, S. padma. (2012) Iris Recognition Using left and right Iris feature of the Human Eye for Bio-metric Security system.
- IJCA, vol 50 No. 152. Retrieved March 18, 2018 from http://www.gjimt.ac.in/wp-content/uploads/2017/11/Vijay-Kumar-Sinha_Enhancing-Iris-Security-by-Detection-of-Fake-Iris_Paper.pdf [11] Zyskind, Nathan, Pentland (2016)

Decentralizing Privacy: Using Blockchain to Protect Personal Data. Retrieved March 18, 2018 from https://enigma.co/ZNP15.pdf

- Fujioka A., Okamoto T., Ohta K. (1993) A practical secret voting scheme for large scale elections. In: Seberry J., Zheng Y. (eds) Advances in Cryptology — AUSCRYPT '92. AUSCRYPT 1992. Lecture Notes in Computer Science, vol 718. Springer, Berlin, Heidelberg. Retri eved March 18, 2018
  from https://link.springer.com/chapter/10.1007/3-540-57220-1_66
- Çetinkaya O., Doganaksoy A. (2007) A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network, Availability Reliability and Security 2007. ARES 2007. The Second International Conference on, pp. 432-442, 10–13 April 2007. Retrieved March 18, 2018
  from http://ieeexplore.ieee.org/document/4159833/

보스코인 백서 2.0 저자, 자문, 기여자 명단

저자 (Wrtier)

김종현 : 블록체인OS CSO / 백서 2.0 총괄진행, Public Financing Concept Creator 및 집필

전명산 : 블록체인OS CGO / Congress voting 집필

문기봉 : 한국스마트인증 CEO / Congress voting 집필

한하원 : 한국스마트인증 Researcher / Congress voting 집필

자문 (Advisory)

최예준 : 블록체인OS CEO / 백서 2.0 자문위원

배민효 : 블록체인OS CTO / 백서 2.0 자문위원

강준구 : 한국스마트인증 CTO / Congress voting 자문위원

김기배 : ARIST(블록체인OS 연구소) Researcher / Public Financing 자문위원

기여자 (Contributor)

강순국 : 블록체인OS Developer / 백서 2.0 운영위원

이준석 : (전) 블록체인OS Developer / 백서 2.0 운영위원

정태권 : (전) ARIST(블록체인OS 연구소) Researcher / 백서 2.0 운영위원

김재오 : 블록체인OS PF Manager / 백서 2.0 편집

박호정 : 블록체인OS PF Manager / 백서 2.0 편집(영문)

최규철 : 블록체인OS PF Manager / 백서 2.0 편집

한글감수

김이준수

영문번역

여승욱

영문감수

Scott Matheina : 블록체인OS Community Manager