BHC COIN

WHITE PAPER Ver. 2.0

2021.05.31.

주식회사 비에이치

(www.bhcc24.com)

01. 서론

가상자산 열풍 이후 금융 시장에서 블록체인 기술을 활용한 증권형 코인에 대한 관심이 증대되고 있다. 비트코인(Bitcoin)으로 대표되는 암호화폐(현 '가상자산')(cryptocurrency) 열풍은 "암호화폐에 화폐의 지위를 부여할 수 있냐"는 논란을 거쳐 엄청난 가치상승과 뒤이은 폭락으로 불안정한 금융 거품의 속성을 보여주고 있다.(박주환 2019) 암호화폐는 새로운 화폐가 아닐 뿐만 아니라 실체가 없는 투기 대상에 불과하다고 주장하는 입장은 암호화폐에 대한 정부의 강력한 규제를 요구하고 있다. 반면에 4차 산업 혁명 시대에 블록체인 기술을 활용한 암호화폐의 가능성 자체를 부정하는 것은 어려우므로 부작용에 대한 규제와 더불어 적극적인 지원 육성 정책이 동시에 필요하다는 주장도 있다.

금융시장에서는 암호화폐의 불안정한 가치 변동을 보완하는 방법으로 일정한 수익을 발생시키는 실물 자산에 기초한 증권형 코인에 대한 논의를 활발하게 진행 중에 있다. 시장에서의 단기 가치 상승에 기초한 암호화폐 투자는 실제 수익 창출로 연결되지 않았기 때문에 급격한 가치 하락을 겪을 수 밖에 없다. 이에 비해 부동산·지식재삭권 등 안정적인 현금 흐름을 확보한 실물 자산을 코인에 연동시킨 증권형 코인은 가치의 확고한 기반을 마련할 수 있었다. 자산 유동성 증대를 가장 큰 장점으로 지닌 증권형 코인은 비유동적인 자산을 증권형 코인으로 만들었을 때 가장 효과적인데 대표적인 사례로 부동산이 주로 언급되고 있다.

2007년 금융 위기에서 알 수 있듯이 경기 침체 상황에서 부동산 시장을 금융시장과 결합시키는 부동산 유동화는 상당한 사회경제적 영향력을 발휘하고 특히 가치하락으로 암호화폐로 흘러 들어가지 못한 투자자금이 증권형 코인으로 몰릴 수 있으므로 부동산 유동화 수단으로 블록체인 기술을 어떻게 활용할 수 있을지 검토가 필요한 상황이다.

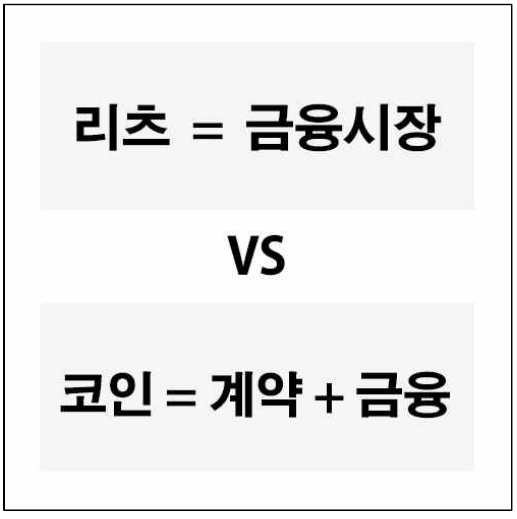
증권형 코인이 단순히 블록체인 기술을 적용한 새로운 금융기법에 지나지 않는다면 증권형 코인을 통한 부동산 유동화는 암호화폐 언저리에 머물러 있는 과잉 유동성을 불러일으킬 가능성이 있다. 반면에 증권형 코인을 통해서 기존에는 가능하지 않았던 부동산 유동화를 실현할 수 있다면 부동산 시장의 혁신·발전을

선도할 수 있다.

부동산 서비스, 특히 부동산 등기, 부동산 중개업 등에서는 정책적 측면에서 4차 산업혁명의 변화를 활발하게 논의중이고 4차 산업혁명이 부동산 시장의 변화를 이끌어가는 핵심 요인이라는 점을 고려할 때, 증권형 코인을 개인 투자자의 관점이 아니라 사회적 활용 차원에서 정책적으로 접근하는 사회적 상황에서 BHC를 개발했다. BHC는 부동산운용전문코인으로써 부동산매매 및 임대료 지급 전문코인이다.

02. 스마트 계약과 증권형 코인

부동산 코인화에는 블록체인 기술 뿐만 아니라 스마트 계약과 증권형 코인이 활용된다. 거래 정보를 네트워크에 기록하는 블록체인 기술 개발 이후 계약관계에서는 스마트 계약이 금융 시장에서는 증권형 코인이 부각 되고 있다. 증권형 코인을 금융시장 측면에서만 보면 부동산 증권과 큰 차이가 없으므로 계약 관계에서 스마트 계약을 분석하는 작업이 리츠와 코인의 비교를 위해 상당히 유용하다. 블록체인 기술의 활용이 리츠와 같은 기존 방식과 질적으로 다른 부동산 유동화를 가능하게 했는지를 파악하기 위해서는 스마트 계약의 개념과 효과에 대한 이해가 필요하다.

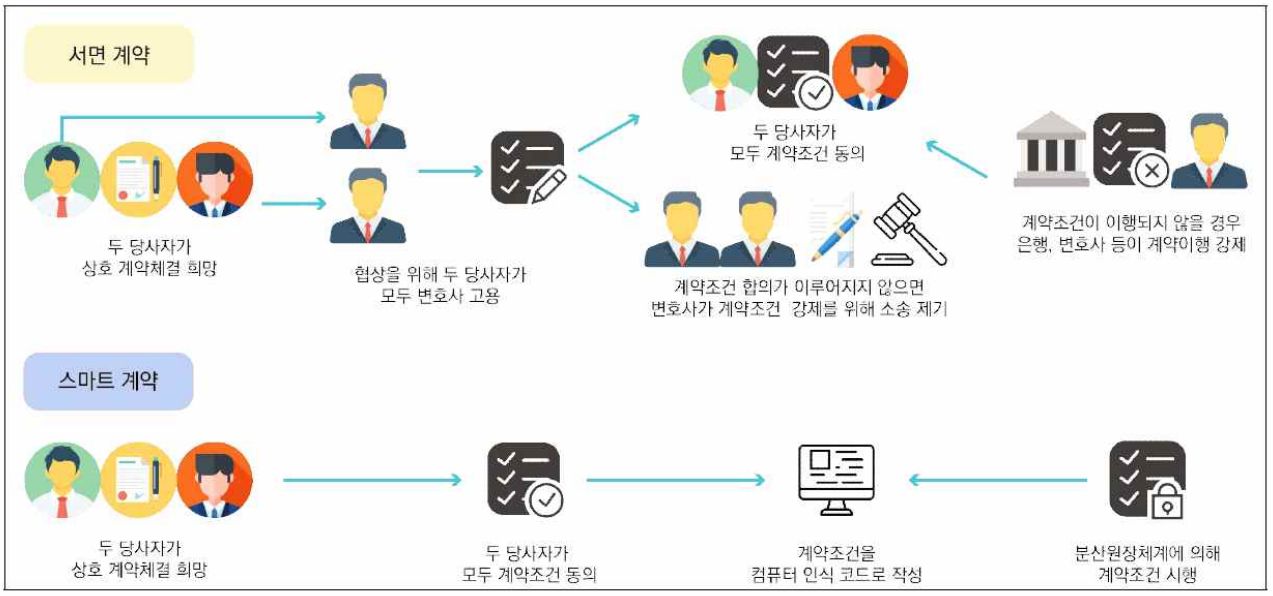


2.1. 스마트 계약

스마트 계약은 계약의 성립 및 이행을 블록체인 기술에 결합한 ‘블록체인 2.0’이다. 통상 스마트 계약은 ‘스스로 이행이 되는 자동화된 약정’으로 불린다. 스마트 계약은 블록체인 플랫폼의 소프트웨어 코드로서 미리 정해진 조건이 성취된 경우 블록체인 플랫폼에 기재된 자산에 대하여 계약 내용을 자동적으로 이행한다. 블록체인 기술을 통해 계약의 조건 성취 여부를 대리인과 같은 제 3 자 개입 없이 P2P 네트워크로 투명하게 확인이 가능하다. 이처럼 거래 기록의 증명 뿐 만 아니라 계약의 체결과 이행까지 블록체인 기술을 활용하므로 스마트 계약을 ‘블록체인 2.0’으로 부른다. 현재 계약의 체결과 이행이 필요한 거의 모든 분야, 예를 들어 증권 거래소・보험・특허 관리 등에서 스마트 계약이 활발하게 활용 된다.

알고리즘 계약의 경우 인간이 미리 계약의 내용 및 조건을 설정하면 인간이 아닌 컴퓨터가 계약 조건의 성취 여부를 판단해서 계약 내용을 처리하는 방식이다. 대표적인 사례로는 증권업계의 알고리즘 매매가 있는데, 특정한 조건을 만족하는 매매 기회가 발생하면 컴퓨터가 알아서 증권의 주문을 집행하는 것이다. 스마트 계약이 기존의 알고리즘 계약과 큰 차이를 보이는 부분은 P2P 네트워크에 기초한 분산화된 자치조직을 활용한다는 점이다. 블록체인기술에 의해 서로 모르는 사람들이 중앙 기관의 관여 없이 사건의 발생 여부에 관해 투명하게 의견 일치를 이뤄내는데, 이러한 특성은 스마트 계약이 대부분 2명으로 이뤄진 당사자 간의 계약 뿐만 아니라 회사설립, 펀드 모금 등 다수의 사람들이 참여하는 합동행위에 적용하기 용이하다는 것을 의미한다.

계약에서 가장 큰 위험 중 하나는 상대방이 계약 조건이 성취됐음에도 불구하고 계약 내용을 이행하지 않는 불이행 문제이다. 이와 같은 불이행 문제를 고려해서 기존 서면 계약에서는 계약서를 작성할 때 법률전문가를 고용해서 계약의 조건・내용을 명확하게 기술하고 이것들을 소프트웨어로 전환하기 위해서는 비용이 발생하지만, 종이 계약과 다르게 불이행 문제를 고려한 계약의 증명과 불이행 문제를 해결하기 위한 강제 집행에는 비용이 전혀 들어가지 않는다.



출처: 이정훈 2018.

2.2. 증권형 코인

자산형 코인이 주로 주식·채권 등 금융 자산에 기초하는데 비해, 증권형 코인은 부동산·지적재산권 등 실물 자산을 코인에 연동시킨 디지털 자산이다. 증권형 코인의 소유는 곧 코인에 연동된 자산에 대한 소유권을 의미하며 이에 따라 코인 발행 주체가 창출하는 수익에 대한 배당 청구 및 의사결정 권리를 포함한다.

ICO는 발행 주체가 제공하는 '서비스'를 이용하기 위해 코인을 판매했지만 SCO(Security Coin Offering, 증권형 코인 발행)는 비즈니스 모델에서 발생하는 수익을 배당금으로 제공하는 코인을 발행한다. SCO를 실행하기 위해서는 투자자들에게 배당금을 지급할 수 있는, 달리 말해 수익을 낼 수 있는 비즈니스 모델이 존재해야 한다. 자산의 수익에 기초해서 수익청구권 및 의사 결정권을 발행한다는 점에서 증권과 유사하다.

ICO가 비즈니스 모델의 빈약한 수익 창출로 큰 곤경을 겪은 반면, SCO는 수익을 창출하는 자산, 특히 실물 자산에 기초한다는 점에서 상대적으로 자금 조달에 유리하기 때문에 금융시장에서 ICO의 대안으로 각광을 받는다. 확실한 비즈니스 모델에 기초한 SCO는 ICO보다 자금 조달 규모가 크고 투자 리스크도 상대적으로 낮다.

<금융시장의 자금조달 방식 비교>

유형	IPO(최초기업공개)	ICO(최초코인발행)	SCO(증권형 코인 발행)
증권유형	증권	코인	증권
기반자산	실물유가자산	체인상 자산	실물 유가 자산
기업리스크	비교적 작음	상당히 큼	적정
자금조달규모	큼	중소형	큼
투자 리스크	중간	높음	상대적 높음
적격투자자 여부	O	X	O
투자자 보호수준	높음	낮음	보통

출처 : 이후빈. 2020

2.3. 코인과 리츠의 비교

부동산 소유권에 기초해서 증권을 발행할 때는 소액 단위로 분할할 경우 다수의 소액투자자들이 투자할 수 있고, 이에 따른 수요 증가로 자산의 유동성이 증대한다. 부동산을 직접 투자하기 위해서는 상당한 초기 자본이 필요하므로 부동산 소유로 자본이득을 향유 할 수 있는 계층은 제한된다. 하지만 리츠를 활용해서 소액 단위 증권을 발행함으로써 소액투자자들도 부동산에 간접적으로 투자하는 것이 가능해지고 이에 따라 부동산 가격 상승시 자본 이득 향유가 가능하다.

리츠를 통한 부동산의 증권화는 부동산 시장을 증권시장에 연계시킬 수 있고, 이로 인해 부동산 시장으로 증권 시장의 풍부한 자금이 유입될 수 있다. 증권시장으로의 접근성 향상에 따라 증권 시장의 자금이 유입되기 쉽고, 특히 금융 위기의 저금리 구조에서는 안정적 수익에 기초한 리츠로 증권 시장의 자금이 쏠릴 수 있다. 리츠는 다른 자산 특히 주식과 상관관계가 낮으므로 포트폴리오에 리츠를 편입시켜서 분산투자의 효과를 누릴 수 있다. 주식시장이 하락할 때 안정적인 부동산 자산에 기초한 리츠의 포토폴리오 효과가 높아질 수 있다. 특히 경기의 영향을 상대적으로 덜 받는 임대형 부동산 리츠가 높은 포트폴리오 효과를 가질 수 있다.

구분	내용
소액화에 따른 유동성 증대	- 소액 단위로 증권을 발행해서 다수의 소액투자자 투자 가능 - 리츠를 활용한 간접투자로 소액투자자로 자본인득 향유 가능
금융 시장과의 연계	- 리츠를 통한 부동산의 증권화로 부동산 시장과 금융 시장 연계 - 부동산 시장으로 금융시장의 풍부한 자금 유입 가능
포트폴리오 효과	- 포트폴리오에 리츠를 편입시켜서 분산투자의 효과 향유 - 안정적인 부동산 자산에 기초한 리츠의 포트폴리오 효과

출처 : 이후빈. 2020

거래 비용 절감과 확장 기능 이외에 코인과 리츠는 금융 시장 측면에서 큰 차이가 없다. 증권형 코인의 장점으로 언급됐던 부분 소유권, 자금 유입, 상호 운용성은 모두 리츠에서도 실행 가능한 특징이다. 부동산 소유권을 잘게 쪼개서 소액 투자를 가능하게 한다는 점에서 동일하고 암호화폐시장과 증권시장의 차이만 있을 뿐 금융 시장에 풍부한 자금이 유입된다는 점에서 동일하다. 또한, 증권화를 통해 다른 자산과 분산 투자가 가능하게 된다는 점에서도 동일하다.

국제적 접근성은 코인과 리츠의 본질적 차이라기 보다는 새로운 기법인 코인에 아직 규제가 적용되지 않았기 때문에 코인이 누리는 상대적 이점으로 볼 수 있다. 블록체인기술을 활용한 거래 비용 절감과 확장된 기능 활용은 리츠에서는 불가능하고 코인에서만 가능한 특징이다. 특히 스마트 계약은 계약의 체결과 이행을 인간의 개입 없이 블록체인으로 실행하는 방식으로 새로운 계약 관계를 형성할 뿐만 아니라 불이행 문제를 남기지 않으므로 거래비용의 획기적 절감도 초래할 수 있다. 따라서 코인과 리츠는 실물 자산을 금융상품화 한다는 측면에서 다양한 특징들을 공유하지만 블록체인기술을 활용한 코인은 스마트 계약과 같은 혁신적 거래 방식으로 비용을 절감할 수 있다는 측면에서 차별적이라고 할 수 있다.

구분		코인	리츠
자산 유동성 증대	**소액화**	- 전자 화폐의 분절 가능성 - 소액자본투자 가능	- 소액 단위 증권 발행 - 소액투자자의 간접투자
	자금 유입	- 암호화폐의 엄청난 가치 상승 - 증권형 코인으로 부의 이전	- 동산 시장과 증권 시장 연계 - 부동산 시장으로 유동성 유입
	국제적 접근성	- (규제가 없다는 전제) 어디서나 구매 가능	
비용감소		- 블록체인 기술을 활용한 거래 비용의 절감	
새로운 기회창출	**상호운용성**	- 다양한 자산의 일괄 관리 - 효율적인 금융구조 설계	- 안정자산(부동산)에 기초 - 리츠의 포트폴리오 효과
	확장 기능	- 스마트 계약과 같은 블록체인 기술만의 장점 활용가능	

출처 : 이후빈. 2020

부동산 유동화를 위한 새로운 방식으로 구분소유권 거래 및 이에 기초한 SCO에 주목할 필요가 있다. 새로운 방식은 단순한 비용 절감을 너머 스마트 계약과 증권형 코인의 융합처럼 블록체인 기술만으로 할 수 있는 방식으로 이전과 다르게 부동산을 유동화 시키는 것을 가리킨다. 소유권의 일부 만을 판매하는 구분소유권 거래는 완전히 새로운 방식이라고 볼 수 없지만, 스마트 계약을 통한 구분 소유권 거래의 활성화는 부동산 시장의 새로운 변화라고 할 수 있다.

<구분 소유권에 기초한 새로운 방식의 부동산 유동화>

스마트 계약 활용 구분 소유권 거래		구분 소유권 거래에 기초한 SCO
거래 비용 절감에 따른 거래 활성화	→	빚 없이 거주 지속하면서 현금 확보

비용 절감을 넘어 부동산 유동화의 질적인 변화

2.4. 구분 소유권 거래

구분 소유권 거래는 블록체인 기술 활용이 부동산 거래에 일으키는 상당히 중요한 변화이다. Granglia and Mellon(2018)은 부동산 거래에 블록체인 기술이 적용되는 방식을 크게 8단계로 구분해서 설명했다.

<부동산거래에서 블록체인 기술 적용의 발전단계>

구분		설명
1	블록체인 기록	- 부동산 거래에 블록체인 기술 적용 - 부패 우려 지역에 블록체인 기술을 도입하면 기록 조작이 어려워짐
2	스마트 워크 플로우	- 거래 참여자가 볼 수 있도록 거래 진행 상황 기록 - 기존 작업과정의 속도를 높이고 이를 더욱 투명하게 만드는데 기여
3	스마트 에스크로(escrow)	- 스마트 계약을 통해 에스크로 대체 - 모든 계약조건이 충족되었을 때 블록체인을 통해 소유권 이전
4	블록체인 동기	- 블록체인이 기존 등기 시스템 대체 - 이전 세 가지 단계들이 블록체인으로 보완되는 중앙집중식 데이터베이스인데 비해, 4단계는 사적 허가 블록체인으로 완전한 시스템 구축
5	권리 분할	- 권리를 분할한 다음 블록체인을 통해 개별 관리 - 모든 거래는 블록체인 시스템을 통해 추적 가능
6	구분소유권	- 투자자가 특정 자산의 일부분(share)을 구매 - 블록체인 기술의 활용을 통해 거래 비용이 상당히 낮아짐
7	P2P거래	- 중개인 없이 구분소유권을 개인 간 거래 - 빠른 청산과 낮은 비용으로 거래 가능, 단 법적 권리의 명료화 필요
8	상호운영성	- 여러 블록체인들의 병합운영 - 물리적 공간과 법률적 권리에 대한 통일된 정의 필요.

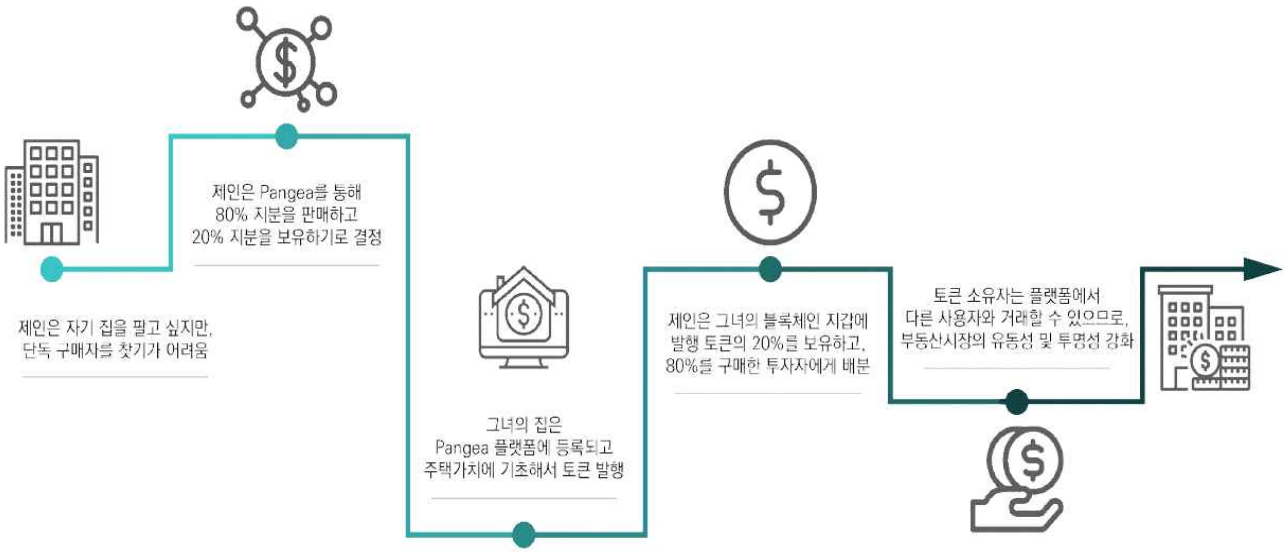
위의 표와 같은 단계 구분은 병렬적인 변화가 아니라 순차적인 변화를 가르키는데, 특정 단계의 실현은 이전 단계들의 완료를 전제로 한다. 예를들어 2단계 스마트 워크 플로우는 1단계 블록체인 기록을 바탕으로 가능해진다. 1~4단계까지는 부동산 거래에서 기존 방식의 효율성을 높이는 수준이라면 5단계부터는 상대적으로 새로운 방식의 부동산 거래를 나타낸다. 새로운 변화의 분기점으로 작용하는 것이 바로 권리 분할에 기초한 구분 소유권 거래의 활성화이다. 자산의 일부분만을 구매하는 구분소유권 거래 자체가 완전히 새롭다고 볼 수는 없지만 거래 비용 절감에 따른 구분 소유권 거래의 일상화는 부동산 거래의 새로운 변화라고 할 수 있다.

03. 해외 사례

3.1. Meridio

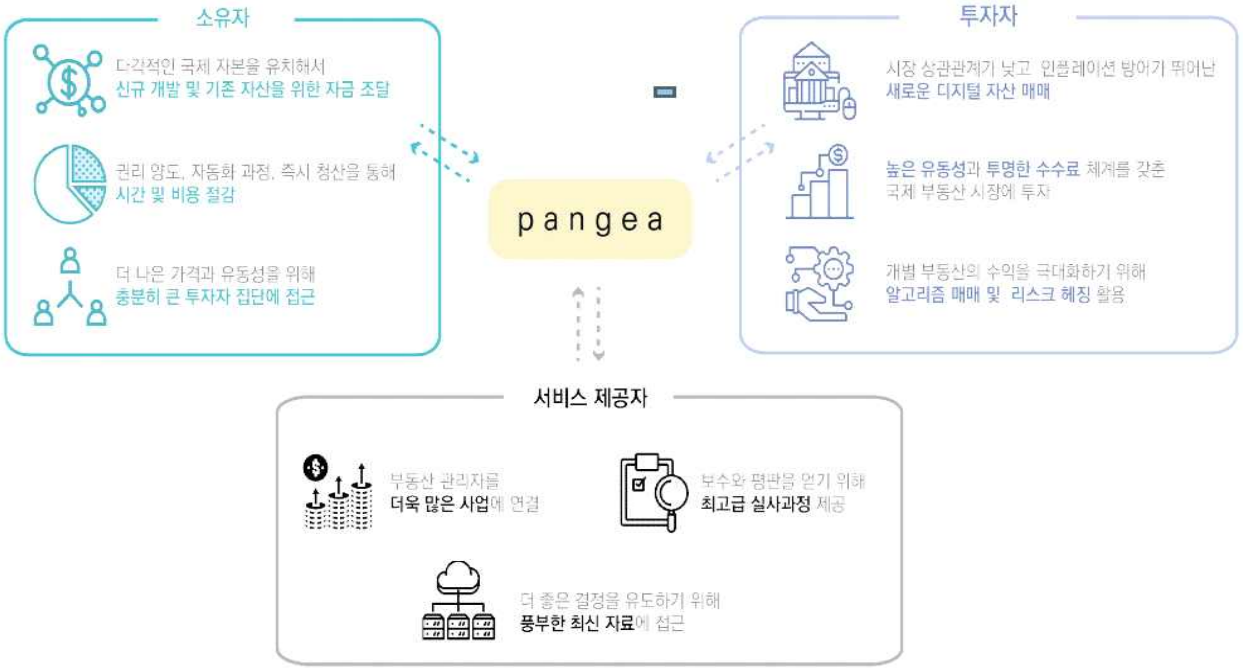
스마트 계약을 활용한 부동산 거래 및 투자 지원플랫폼으로써 블록체인 소프트웨어 회사인 컨센서스가 개발한 부동산 거래/투자 플랫폼이다. 이 플랫폼은 부동산의 높은 중개 비용, 진입장벽, 낮은 유동성을 문제점으로 지적하며 개발됐다. 먼저 스마트 계약을 활용해서 거래 비용을 절감하고 거래의 투명성 증진을 유도한다. 또한 부동산 개발, 기존 부동산 중개시장, 부동산 가치에 대한 실시간으로 자료를 제공한다. 투자자는 서비스를 통해 소규모 자본금을 부동산에 투자할 수 있는 다양한 기회, P2P 거래를 통한 거래 비용 절감 효과 등을 얻을 수 있다. 소유자는 상대적으로 더 큰 투자자 집단에 접근할 수 있으므로 자산의 유동성을 높일 수 있다. 특히 스마트 계약을 활용해서 구분소유권 거래의 활성화를 시도하고 있는데 소유자가 부동산 소유권의 일부분만을 코인으로 만들어서 투자자에게 판매한다.

Meridio는 블록체인 기술을 활용한 구분소유권 거래방식을 제시하고 있다.



위 그림에서 알 수 있듯이 주택 소유주는 자신이 원하는 만큼, 예를 들어 80%의 소유권을 코인으로 만든 다음 이 코인을 '판게아' 플랫폼에서 P2P 방식으로 세계적 투자자들과 거래할 수 있다. 부동산의 온전한 소유권을 잘게 쪼개서 자산의 유성을 높이는 한편, 스마트 계약과 P2P거래로 거래 비용을 절감하면서 거래의 투명성을 증진한다. 구분소유권을 거래하는 것은 블록체인 기술을 활용하지 않더라도 현재 방식으로도 충분히 가능한데 예를 들어 구분소유권에 대한 종이 계약서를 작성하고 공증을 받은 다음 해당 구분소유권으로 증권 또는 주식을 만들어서 증권거개소에서 거래를 한다. 하지만 블록체인 기술을 활용하면 소유권의 분해・기록・거래에서 발생하는 여러 가지 비용들을 감소시킬 수 있다. 단적으로 증권거래소를 통하지 않는 탈중앙화된 시스템은 구분소유권을 더 저렴한 비용으로 더 투명하게 거래할 수 있도록 해준다. 즉 거래 비용의 감소는 구분소유권 거래를 활성화시키고 규모를 확대할 수 있다.

<Meridio의 구분 소유권 거래>



3.2. QuantmRE

QuantmRE는 구분 소유권에 기초한 증권형 코인을 발행하고 있다. 주택 소유주는 구분 소유권 거래로 빚을 지지 않고 현금 확보가 가능한데 주택 소유주가 주택 지분 일부를 양도하는 대가로 이자 지급 없이 당장 현금을 확보할 수 있고 최대 30년까지 현재 주택에서 거주가 가능하다. 이 비즈니스 모델의 핵심은 주택담보대출과 같은 빚을 떠안지 않고 주택 지분에 기초해서 현금을 추출하는 구분 소유권 거래에 있다. 주택 소유주는 자신의 원하는 만큼 소유권의 일부를 'QuantmRE'에게 양도하는 대신 그에 합당하는 현금을 바로 손에 쥘 수 있다.

QuantmRE의 수익구조는 현재와 미래 사이 부동산 지분의 가치 차이에 기초하고 있다. QuantmRE는 구분 소유권의 가치를 현재보다 미래에 더 높게 산정해서 일정한 이윤을 확보할 수 있다. 예를 들어 10%만큼 구분소유권을 양도받으면서

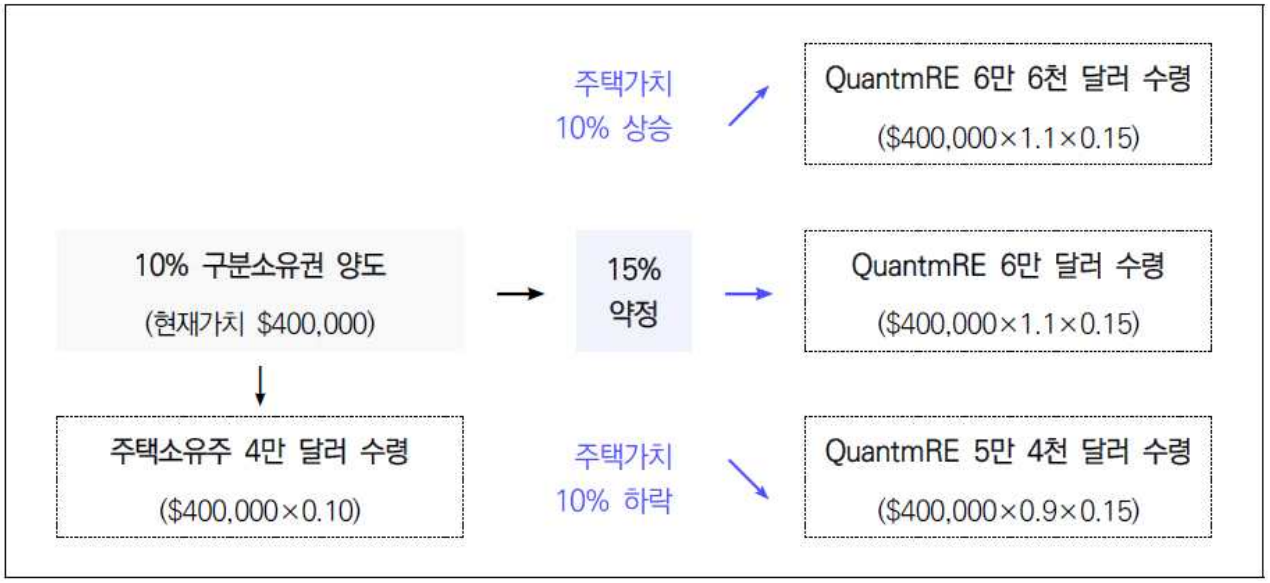
차후에 주택소유가가 주택을 실제로 매각할 때 그 매각 대금의 15%를 요구할 수 있는 권리를 약정할 수 있는데, 이때 현재가치의 10%와 미래가치의 15%차이가 QuantmRE이 벌어들이는 수익의 근원이다. 미래의 불확실성에도 불구하고 이와 같은 거래가 가능한 이유는 채무불이행 문제를 남기지 않는 스마트 계약 덕분인데, 만약 스마트 계약이 없다면 QuantmRE는 불확실한 미래에 대비하기 위해 추가적인 법률 조치들을 취해야 하고, 이와 같은 거래 비용의 증가는 구분소유권 거래의 활성화를 어렵게 만든다.

QuantmRE는 포트폴리오에 기초한 'EQRE' 코인 발행 예정에 있다. 'EQRE'이라고 불리는 증권형 코인은 미국 1인 가구 소유 또는 점유하고 있는 주택의 주식을 조합해서 만든 포트폴리오에 기초해서 발행한다. 투자는 개별 부동산에 직접 투자하거나 EQRE 코인을 구매할 수 있다. 증권형 코인의 가치는 유동화 또는 판매 실적에 따라 실시간으로 변하며, QuantmRE는 분기별로 자산에 대한 재평가를 실시해서 공표한다. 이렇게 기록된 다양한 가치 정보를 바탕으로 금융 전문가가 코인의 구매자에게 최적의 포트폴리오 구성을 제시한다.

QuantmRE는 구분소유권 양도에 기초해서 증권형 코인을 발행하는 비즈니스 모델을 제안한다. 주택소유주는 자신이 원하는 만큼 구분소유권을 양도하고 이에 대한 애가로 양도한 구분소유권 가치 만큼 현금을 즉시 수령한다. QuantmRE는 서로 다른 주택의 구분 소유권들을 섞어서 부동산 포트폴리오를 구성한다음 증권형 토큰 발행으로 투자자금을 유치한다. 투자자는 증권형 코인의 소유자로써 QuantmRE로부터 정해진 배당금을 수령한다.

이 모델의 핵심은 주택소유주로부터 15%의 미래가치를 10%의 현재가치로 구매하는 스마트계약에 있다. 주택소유주와 QuantmRE는 구분소유권 양도 계약에서 구분 소유권을 양도하는 현재 시점과 주택 매각으로 구분소유권의 가치를 실현하는 미래시점을 구분한다. 주택의 일부 소유권만을 양도하는 것이므로 주택소유주는 여전히 해당 주택에서 거주할 수 있고, 반대로 구분소유권을 구입한 QuantmRE는 주택 소유주가 주택을 매각해서 대금을 받는 수간에야 구분소유권자로써 일정한 현금을 수령 할 수 있다. 구분소유권을 양도한 주택소유주는 당장 현금을 받지만, 구분소유권을 넘겨받은 QuantmRE는 주택 매각이 이뤄지는

미래에야 현금을 받을 수 있다. 이런 비대칭성은 구분소유권의 현재가치와 미래 가치의 차이로 보상된다. 이 차이는 주택 가치 상승 여부에 따라 더 커질 수가 있다. 불이행 문제를 남기지 않는 스마트 계약을 통해서 불확실한 미래에도 불구하고 별도의 법률적 보호 장치 없이 저렴한 거래 비용으로도 계약을 체결 할 수 있다.



04. 코인 특징

4.1 CryptoNote 란

“비트코인은 p2p 전자 화폐를 성공적으로 현실화한 사례이다. 전문가들과 대중들은 public transaction과 proof-of-work 방식을 신뢰할 수 있는 모델로 평가했다. 현재 사용자 기반의 전자 화폐는 꾸준히 성장하고 있다. 일반 소비자들은 전자화폐의 낮은 수수료와 익명성에 이끌리고 있으며, 상인들은 예견이 가능하고 분산화된 화폐 발행을 긍정적으로 생각한다. 비트코인은 전자화폐가 지폐처럼 단순하고 신용카드처럼 편리하다는 사실을 효과적으로 입증했다.

하지만, 비트코인에는 몇 가지 단점이 존재하는데, 예를 들어 시스템의 분배는

경직되어 있으며, 모든 네트워크 이용자들이 클라이언트를 업데이트 해야만 새로운 기능이 도입될 수 있다. 단점을 빨리 개선할 수 없다는 점은 비트코인의 확산을 막고 있다. 이러한 경우에는 기존의 것을 개선하는 것보다 아예 새로운 프로젝트를 만드는 것이 효율적이다.

이 문서에서, 비트코인의 주된 단점에 대한 해결책을 제시하고자 한다. 이러한 해결책을 통하여 전자 화폐 시스템은 건전한 경쟁을 할 수 있을 것이다. “CryptoNote” 라는 우리의 전자화폐를 통해서, 전자화폐는 혁신될 수 있을 것이다.

4.2 비트코인의 단점들과 가능한 해결책들

4.2.1 트랜젝션의 추적 가능성

전자화폐에서 프라이버시와 익명성은 가장 중요한 측면들이다. 개인 간 거래는 제3자로부터 숨겨질 것이며, 이는 전통적인 은행의 거래 방식과 대조된다. 특히 T. Okamoto와 K. Ohta는 이상적인 전자화폐의 6가지 특성을 서술하였는데, 그 중 하나는 “프라이버시로, 사용자 간의 관계와 구매 내역은 어느 누구도 볼 수 없어야 한다.” Okamoto와 Ohta의 완전히 익명적인 전자화폐 개념을 충족하기 위해서 2가지 특성을 이끌어 내었다.

비추적성 : 각각의 수신 트랜젝션에서 누가 보냈는지 알 수 없다.

비연결성 : 임의의 2개의 발송되는 트랜젝션에 대해서, 같은 사람에게 전송되었다는 것을 입증할 수 없다.

안타깝게도 비트코인은 비추적성에서 벗어난다. 네트워크의 참가자들의 트랜젝션이 모두 공개되기 때문에, 발송자와 최종 수신자가 모두 공개될 수 있다. 만약 간접적으로 거래를 하더라도, 경로 추적 기술을 이용하면 발송자와 수신자를 확인할 수 있다.

비트코인이 2번째 속성도 충족하지 않는 것처럼 보인다. 일부 연구자들에 의한 블록체인에 대해 자세히 분석하면, 비트코인 네트워크의 이용자들과 트랜젝션 사이의 관계를 알게 될 가능성이 존재한다. 많은 방법들이 부정되었지만, 공개된 데이터베이스로부터 숨겨진 개인정보가 알려질 가능성이 크다.

비트코인은 위에 서술된 2가지 속성을 충족하지 못하며, 따라서 익명성을 가장한 전자 화폐 시스템이라는 것이다. 사용자들은 이러한 단점을 빠르게 극복하고자 한다. 두 가지의 직접적인 해결방법은 “화폐세탁 서비스”와 공개된 트랜젝션과 중간 주소를 이용하는 것으로서, 제3자가 필요하다는 단점이 있다.

최근에, I.Miers는 새로운 계획을 제시하였다. “Zerocoin”은 단방향의 암호 축적 방식을 이용하며, 사용자들로 하여금 비트코인을 제로코인으로 바꾸게 하고, 디지털 서명 및 공개 키 대신에, 익명 소유권 증명으로 전송된다. 그러나, 이러한 증명 방식은 상당히 많은 용량이 필요하며, 현재의 피트코인이 30kb인 것을 고려하면 실용적이지 않다. I.Miers는 이러한 방식이 대다수 비트코인 유저로부터 외면받을 것이라고 예상했다.

4.2.2 proof-of-work 의 작동 방식

비트코인 제작자인 Satoshi Nakamoto는, proof-of-work에 대한 의사결정 방식을 “1cpu당 1표”로 설명하였고, CPU에서 시작되는 가격 결정 방식(double SHA-256)을 주장하였다. 이용자들은 트랜젝션 기록을 바탕으로 투표를 하게 된다. 이 과정이 제대로 되어야 전체 시스템이 잘 작동할 수 있다.

이러한 모델의 보안은 두 가지 단점을 지니고 있다. 첫째로는 정직한 유저의 통제 하에 두려면 51퍼센트의 네트워크 마이닝 파워가 필요하다. 두 번째로, 해당 시스템의 발전 과정(버그 수정, 보안 수정 등)을 하려면 대다수의 사용자가 변화에 지지하고 동의해야만 한다. (사용자들이 지갑 소프트웨어를 업데이트 해야 하기 때문이다. 동일한 투표 방식은 또한 일부 기능의 도입에 대한 설문조사에서 활용된다.

이러한 모델을 통해 proof-of-work 가격 방식의 속성을 이해할 수 있다. 이러한 방식은 네트워크 내의 특정 참가자가 지나치게 강한 힘을 갖는 것을 방지해야 한다. 일반적인 하드웨어와 고비용의 커스텀 장치가 서로 동등해야 한다. 최근 비트코인에서 사용되는 SHA-256 방식의 경우 고성능 CPU보다 뛰어난 고성능 GPU와 ASIC의 등장으로 인해 이러한 동등성은 상실되었다.

비트코인의 경우 CPU소유자보다 GPU 및 ASIC 채굴자들이 더 많은 투표력을 갖기 때문에, 실제 투표력과 차이가 발생한다. “1CPU 1투표” 원칙을 어기기 때문이다.

일부에서는 적지 않은 참가자들이 의사결정을 행사하기 때문에, 해당 문제가 보안과 관련된 사항은 아니며, 대신에 의사결정 참가자들의 정직성이 중요하다고

주장한다. 이러한 주장에 대한 반론이 존재하는데, 값이 저렴하며 채굴에 특화된 하드웨어가 존재할 가능성 때문이다. 예를 들어, 만약 악의적인 채굴업자가 값싼 하드웨어로 채굴을 하게 된다고 가정해보자. 그리고 전세계의 해쉬레이트가 감소했다고 가정해보자. 잠깐일지라도 그는 chain fork 및 double-spend가 가능해진다. 이러한 상황의 가능성이 충분하다는 것을 이 글에서 설명할 것이다.

4.2.3 불규칙적인 생성

비트코인의 생성속도는 기존에 정해져 있다. 각 블록을 채굴하면 고정된 액수의 코인을 얻을 수 있다. 약 4년마다 이러한 보상은 반으로 줄어든다. 원래의 의도는 완만하게 지수함수형 붕괴(exponential decay) 하도록 하는 것이었으나 현실은 구분적선형(piecewise linear) 의 형태로 중단점(breakpoint)에서 비트코인 인프라에 대한 문제점이 발생할 수 있었다.

문제점이 발생하면, 기존의 보상에 비해서 절반의 가치만을 얻게 된다. 12.5와 6.25 BTC의 차이(2020년에 예상)는 그래도 괜찮아 보인다. 그러나, 50과 25BTC의 차이는 2012.11.28.에 발생하였으며, 채굴 업계에서 상당히 부적절한 일로 비춰졌다. 그림에서는 11월 말 네트워크 해쉬레이트가 급격히 감소했다는 상황을 나타내며, 보상이 절반으로 감소한 직후 일어난 일이었다. 악의적인 개인이 double spending attack을 일으킬 완벽한 순간이다.

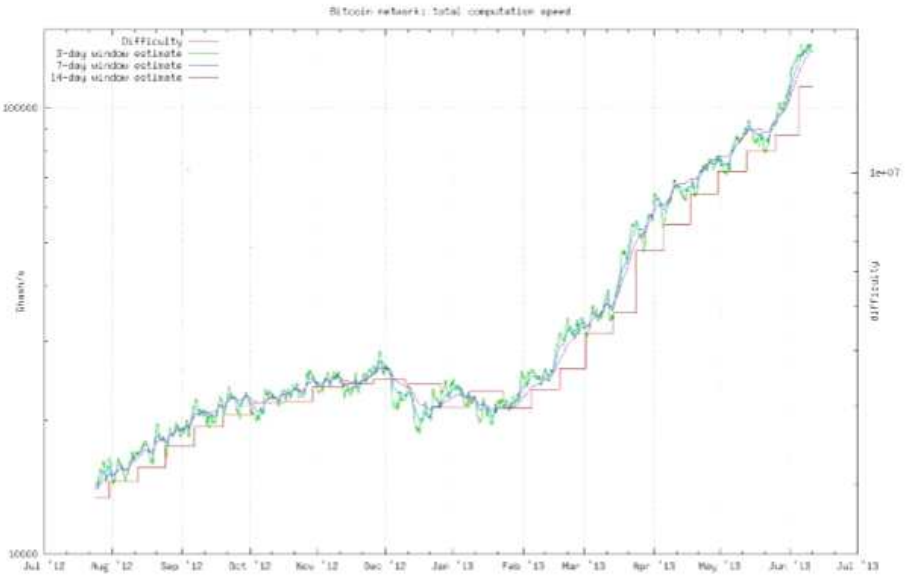


Fig. 1. Bitcoin hashrate chart
(sourced from bitcoin.sipa.be/block_name% on 2018-11-01

4.2.4 수정의 어려움(Hardcoded Constants)

비트코인은 수정이 어렵다는 단점이 존재하고, 원래의 디자인(block frequency, 최대 통화 공급량, 확인의 개수 등)에 문제가 있다. 특히 가장 큰 문제는 단점을 빠르게 개선하지 못한다는 점이다. 적시에 수정하지 못할 경우 끔찍한 결과가 발생할지도 모른다.

수정이 어려운(hardcoded) 문제점 중 하나는 블록 사이즈 리미트가 250kb라는 것이다. 약 10,000건의 일반 거래를 감당하기에는 충분하다. 2013년 초기에 거래량이 이 정도에 도달하였으며, 리미트를 올리고자 합의하였다. 지갑 버전 0.8에서 도입되었으며, 결과적으로 24-block chain split과 double-spend attack이 발생하게 되었다. 비트코인 프로토콜 자체에는 버그가 없었으나, 데이터베이스 엔진에 문제가 있었으며, 만약에 인위적인 블록 사이즈 제한이 없었다면 스트레스

테스트를 통해서 미리 알 수 있었을 것이다.

Constant는 또한 중앙화로 유도하기도 한다. 비트코인은 p2p 방식이지만, 대다수의 node가 특정 그룹에서 만들어낸 공식 클라이언트를 활용하고 있다. 이 특정 그룹은 프로토콜을 변화시키려 하며, 대다수의 사람들은 "정확성"과 관계없이 이러한 변화를 받아들이나. 일부 결정 과정에서 토론은 과열되었으며 보이콧되기도 하였다. 커뮤니티와 개발자들이 특정한 부분을 반대할지도 모른다는 점을 나타낸 것이다. 따라서 이용자가 조장할 수 있는 변수를 가진 프로토콜을 사용하는 것이 논리적인 해결책으로 보여졌다.

4.2.5 방대한 스크립트

비트코인의 스트립트 시스템은 방대하고 복잡한 기능이다. 잠재적으로 한 객체는 복잡한 트랜젝션을 만들어낼 수 있으며, 일부 기능은 보안상의 이유로 제한되었고, 일부는 전혀 이용된 적이 없다. (송신자와 수신자 부분을 포함하여) 비트코인의 대다수의 트랜젝션은 다음과 같이 사용된다.

<sig> <pubKey> OP DUP OP HASH160 <pubKeyHash> OP EQUALVERIFY OP CHECKSIG.

이 스크립트는 164 바이트의 길이이지만, 유일한 목적은 수신자가 그의 서명을 확인하기 위한 암호 키를 가지고 있는지를 체크하는 것이다.

4.3 크립토노트 기술

4.3.1 추적 불가능한 트랜젝션

우리는 비추적성, 비연결성 조건을 모두 충족하는 완전히 익명의 트랜젝션 방식을 제안한다. 여기서 핵심적인 부분은 자주성이다. 송신자는 트랜젝션을 위해 다른 사용자 또는 신뢰할 수 있는 제3자와 협력할 필요가 없으며, 따라서 각각의 참가자들은 독립적으로 거래를 한다.

4.3.2 타원곡선 파라미터(Elliptic curve parameters)

우리는 EdDSA를 이용하려고 하며, 이 내용은 D.J. Bernstein에 의하여 개발되었다. 비트코인의 ECDSA와 유사하게 타원곡선 로그 문제(elliptic curve logarithm problem)에 근거하고 있으며, 우리의 방식은 미래에 비트코인에도 적용될 수 있을 것이다.

일반적인 파라미터는 아래와 같다.

q: a prime number; $q = 2^{255} - 19$;

d: an element of $\mathbb{F}_q$; $d = -121665/121666$;

E: an elliptic curve equation; $-x^2 + y^2 = 1 + dx^2y^2$;

G: a base point; $G = (x, -4/5)$;

l: a prime order of the base point; $l = 2^{252} + 27742317777372353535851937790883648493$;

$\mathcal{H}_s$: a cryptographic hash function $\{0,1\}^* \to \mathbb{F}_q$;

$\mathcal{H}_p$: a deterministic hash function $E(\mathbb{F}_q) \to E(\mathbb{F}_q)$.

4.3.3 용어

private ec-key is a standard elliptic curve private key: a number $a \in [1, l-1]$;

public ec-key is a standard elliptic curve public key: a point $A = aG$;

one-time keypair is a pair of private and public ec-keys;

private user key is a pair (a, b) of two different private ec-keys;

tracking key is a pair (a, B) of private and public ec-key (where $B = bG$ and $a \neq b$);

public user key is a pair (A, B) of two public ec-keys derived from (a, b);

standard address is a representation of a public user key given into human friendly string with error correction;

truncated address is a representation of the second half (point B) of a public user key given into human friendly string with error correction.

트랜젝션 구조는 비트코인의 구조와 유사하다. 트랜젝션 아웃풋이 가능하며, 대응하는 개인 키로 서명하여 다른 주소로 보낼 수 있다.

비트코인과의 차이점은, 한 유저가 독특한 개인 키와 공개 키를 가지고 있을 경우에, 송신자는 수신자의 주소와 랜덤 데이터에 근거해서 1회용 공개키를 만들어낸다. 이러한 방식으로, 동일한 수신자에 대한 트랜젝션은 1회용 공개 키를 통해 이루어진다. 특정 주소로 바로 전송되지는 않으며, 정당한 수신자만이 개인 키 부분을 복원하여 자금을 수신할 수 있다. 수신자는 ring signature을 이용하여 자금을 소비할 수 있으며, 소유권을 유지하면서 익명성을 유지할 수 있다. 프로토콜의 자세한 부분은 다음 항목에서 설명된다.

4.3.3 비연결성 지불

전통적인 비트코인 주소는, 일단 발행된 후에, 돈을 지불할 수 있는 추상적인 identifier가 되며, 둘을 서로 묶게 되며, 수신자의 가명(pseudonyms)으로 연결

(tie)된다. 만약 누군가 연결되지 않은(untied) 트랜젝션을 수신하려면, 그의 주소를 송신자에게 사적인 채널을 통해서 전송해야 한다. 만약 어떤 사람이, 같은 사람인지 증명되지 않은 다양한 트랜젝션을 수신하려 하면, 모든 다양한 주소를 생산해야 하며, 그 자신의 가명(pseudonym)으로 공개해서는 안된다.

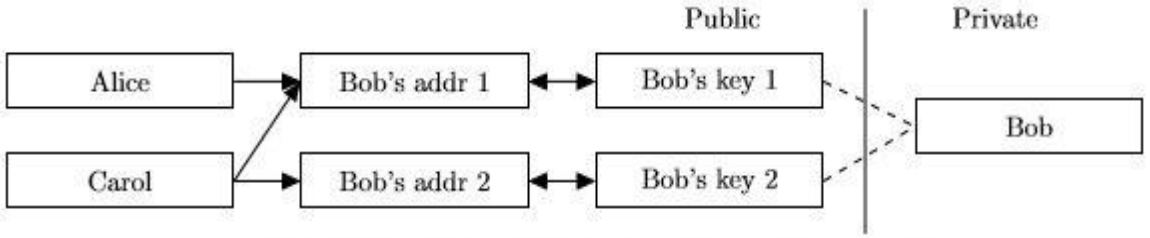


Fig. 2. Traditional Bitcoin keys/transactions model.

사용자가 단일 주소를 공개할 수 있으며, 무조건적으로 비연결성의 지불을 받을 수 있는 단일 주소를 발행할 수 있는 방식을 제안한다. 각각의 크립토노트 output은 기본적으로 공개 키 방식이며, 수신자의 주소와 송신자의 랜덤 데이터로부터 발생한다. 비트코인과의 주된 차이점은 모든 destination key가 기본적으로 독특하다는 것이다. (동일한 송신인이 동일한 데이터를 동일한 수신인에게 보내는 경우를 제외). 따라서, 이러한 방식에서 "주소 재사용"에 대한 문제는 없으며, 제3자가 특정 주소에 대한 전송을 확인할 수는 없다.

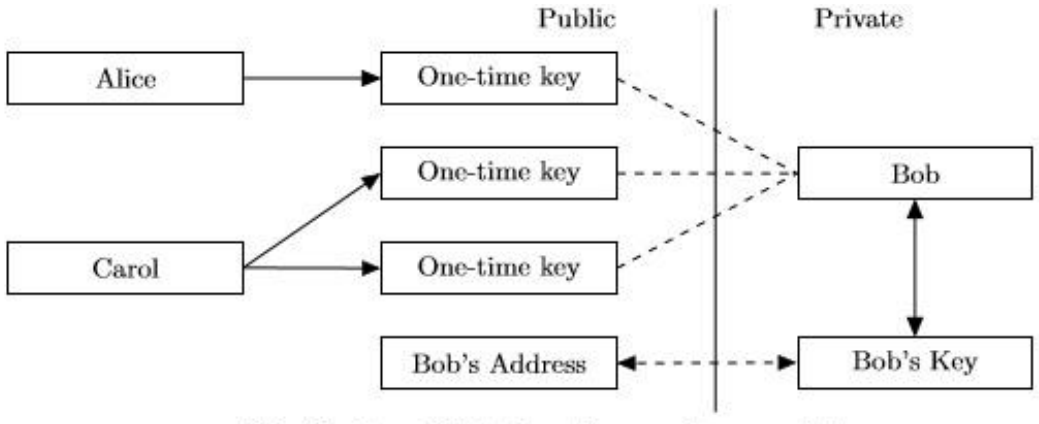


Fig. 3. CryptoNote keys/transactions model.

첫째로, 송신자는 Diffie-Hellman 교환을 이용하여 그의 데이터의 비밀을 공유하며, 수신자의 주소의 절반을 얻게 된다. 그리고 나서 공유된 비밀과 주소의 나머지 절반을 이용하여 1회용 destination key를 계산한다. 이러한 2단계의 과정에서 수신인은 2개의 서로 다른 ed-key를 준비해야 하며, 따라서 일반적인 크립토노트 주소는 비트코인 지갑 주소보다 거의 2배 정도 길다. 수신자는 또한 Diffie-Hellman 교환을 수행하여 상응하는 비밀 키를 해독해야 한다.

일반적인 거래 과정은 다음과 같다.

1. Bob은 표준 주소를 공개하였으며, Alice가 Bob에게 전자화폐를 보내고자 한다. Alice는 주소를 분석하고 Bob의 공개키를 얻는다. (A,B)
2. Alice는 랜덤의 r(1,-2 중 하나)을 만들어내고, 1회용 공개키를 계산해낸다. 공개키 P = Hs(rA)G + B.
3. Alice는 output에 대해서 P를 destination key로 사용하고, R 값을 해석한다. R=rG(Diffie-Hellman 교환의 일부) 또 다른 공개 키를 활용하여 다른 output을 만들어낼 수도 있다. (수신인의 키가 다르면(Ai, Bi), 동일한 r에 대해서도 서로 다른 Pi가 도출된다.)

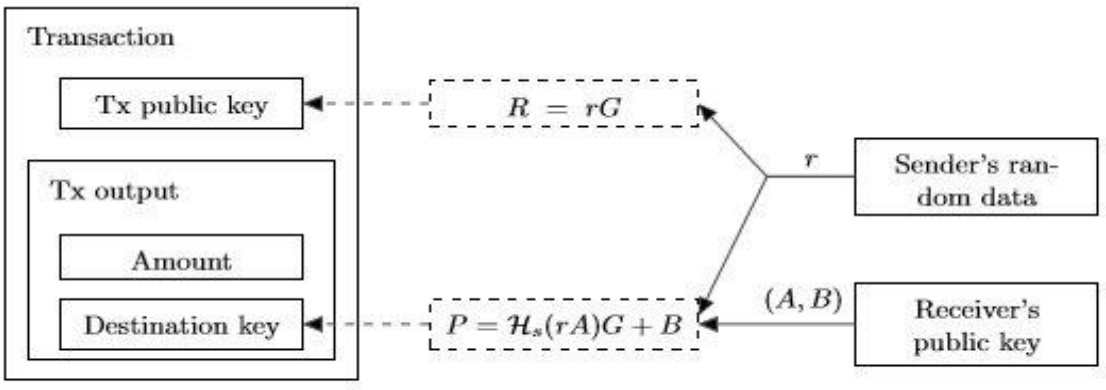


Fig. 4. Standard transaction structure.

4. Alice는 트렌젝션을 전송한다.

5. Bob은 개인키(a,b)를 이용하여 트랜젝션을 체크하며, P0 = Hs(aR)G + B라는 내용을 계산한다. 만약 Alice와 Bob의 트렌젝션이라면 aR = arG = rA and P’ = P.

6. Bob은 상응하는 1회용 개인 키를 얻을 수 있다. x = Hs(aR) + b. 따라서 P = xG가 되며, x로 서명함으로써 원할 때에 output을 전송할 수 있게 된다.

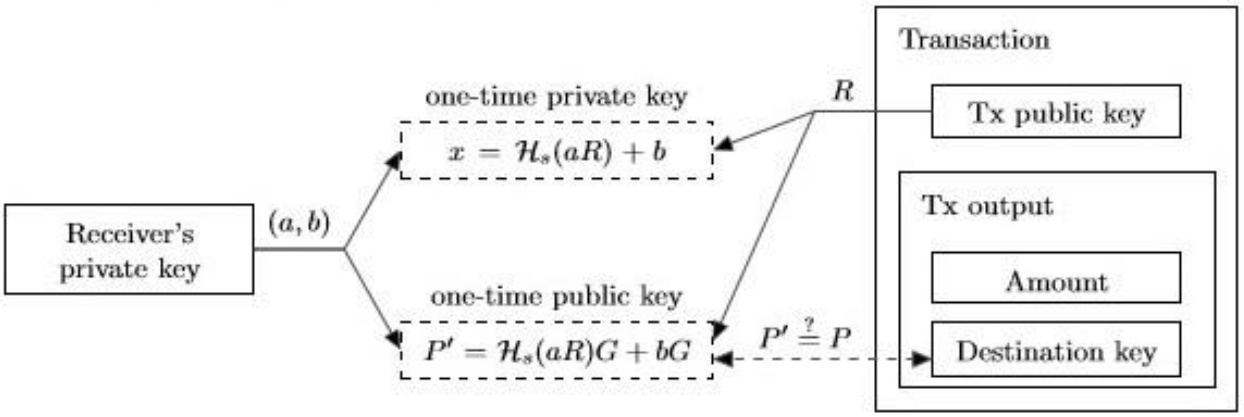


Fig. 5. Incoming transaction check.

결과적으로 Bob은 전자화폐를 지불받게 되며, 제3자는 연결 불가능한 1회용 공개 키가 활용된다. 추가적으로,

* Bob이 스스로의 Transaction을 “인지”하면(step 5) 실질적으로 그의 개인정보의 절반만을 이용한다. (a, B). 이 한 쌍은 또 tracking key로 알려져 있으며, 제3자 (Carol) 에게 전달될 수 있다. Bob은 새로운 트랜젝션에 대한 진행을 Carol에게 위임할 수 있다. 특히 대역폭이 낮거나 성능이 떨어지는 경우(스마트폰, 하드웨어 지갑 등) 유용하게 사용이 가능하며, Bob의 개인 키가 없다면 1회용 비밀 키를 알 수 없으므로, Carol을 완전히 신뢰하지 않아도 된다.

* 만약 Alice가 Bob의 주소로 보낸 트랜젝션을 확인하려면, r을 공개하거나, zero-knowledge protocol을 사용하여 그녀가 r을 안다는 것을 입증하면 된다. (예

를 들어 트랜젝션을 r로 서명할 수 있다.)

* 만약 Bob이 연결 가능하고, 조사 가능한 주소를 원한다면 tracking key를 공개하거나, 생략된 주소를 사용하면 된다. 이 주소는 단지 하나의 공개 ec-key만을 의미하며, 프로토콜이 요구하는 나머지 부분은 다음과 같이 도출된다. a = Hs(B) 그리고 A = Hs(B)G. 두가지의 경우 모두에서 모두들 Bob이 트랜젝션을 수신했다는 것을 알 수 있다. 그러나 물론 비밀 키 b를 알지 못하면 어느 누구도 해당 자금을 소비할 수 없다.

4.3.4 일회용 ring signature

1회용 ring signature에 기반하면, 이용자들은 무조건적인 비연결성을 갖게 된다. 안타깝게도 일반적인 암호화폐의 암호화된 서명을 통해 개별적인 송신인과 수신인들에게 추적할 권한을 얻을 수 있다. 기존 전자화폐와 차별화된 서명 방식을 사용한다는 것이 해결책이다.

우선 전자화폐와는 별도로 ring signature 알고리즘을 설명하겠다.

1회용 ring signature은 4개의 알고리즘을 포함한다. (GEN, SIG, VER, LNK):

GEN: takes public parameters and outputs an ec-pair (P, x) and a public key I.

SIG: takes a message m, a set $\mathcal{S}'$ of public keys $\{P_i\}_{i \neq s}$, a pair (P_s, x_s) and outputs a signature σ and a set $\mathcal{S} = S' \cup \{P_s\}$.

VER: takes a message m, a set $\mathcal{S}$, a signature σ and outputs "true" or "false".

LNK: takes a set $\mathcal{I} = \{I_i\}$, a signature σ and outputs "linked" or "indep".

프로토콜 이면의 아이디어는 상당히 단순하다. 한 사용자가 1개의 특정한 공개키가 아니라 여러개의 공개키 세트로 체크될 수 있는 서명을 한 사용자가 생성한다. 소유주가 동일한 열쇠 짝을 이용하여 두 번째 서명을 발행하지 않는 한, 서명자의 아이덴티티는 공개 키의 동일한 세트 중에서 구별할 수가 없다.

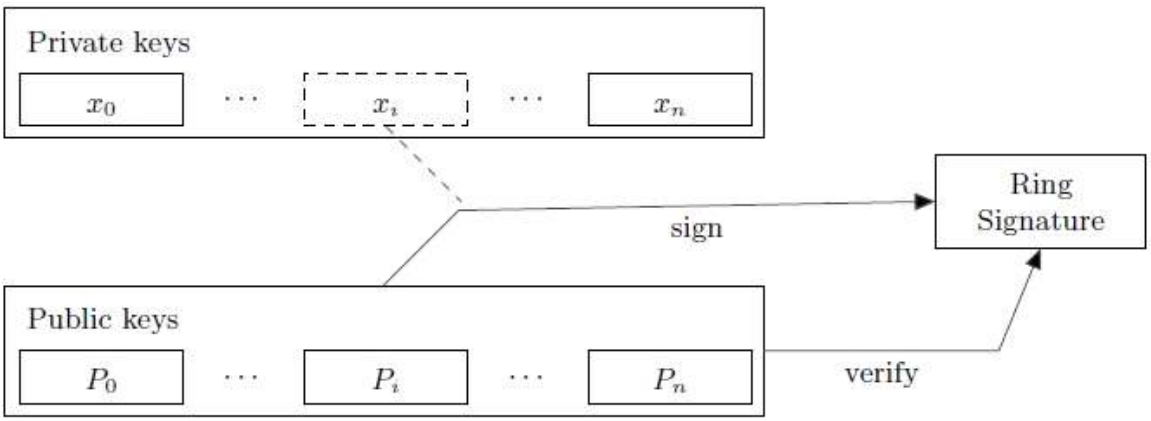


Fig. 6. Ring signature anonymity.

GEN : 서명인은 랜덤한 비밀키 x ∈ [1,l−1]를 선택하며, 상응하는 공개키 P = xG를 계산한다. 추가적으로 또 다른 공개키 I = xHp(P)를 계산해야 하며, 이러한 것을 “키 이미지”라고 부른다.

SIG : 서명인은 기술을 활용하여 1회용 ring signature를 비상호작용적인 zero-knowledge proof와 함께 생성한다. 서명인은 다른 이용자들의 공개 키Pi, 자신만의 keypari (x,P), Key image I로부터 랜덤한 하위집합 S0를 선택한다. S (그의 공개키는 Ps)에서의 서명인의 비밀 인덱스를 0 ≤ s ≤ n 라고 하자.

서명인은 랜덤의 {qi ¦ i = 0...n}를 선택하며 (1...l)로부터 {wi ¦ i = 0...n,i 6= s}를 선택하며, 다음의 변환에 적용된다.

$$L_i = \begin{cases} q_i G, & \text{if } i = s \\ q_i G + w_i P_i, & \text{if } i \neq s \end{cases}$$

$$R_i = \begin{cases} q_i \mathcal{H}_p(P_i), & \text{if } i = s \\ q_i \mathcal{H}_p(P_i) + w_i I, & \text{if } i \neq s \end{cases}$$

The next step is getting the non-interactive *challenge*:

$$c = \mathcal{H}_s(m, L_1, \ldots, L_n, R_1, \ldots, R_n)$$

Finally the signer computes the *response*:

$$c_i = \begin{cases} w_i, & \text{if } i \neq s \\ c - \sum_{i=0}^{n} c_i \mod l, & \text{if } i = s \end{cases}$$

$$r_i = \begin{cases} q_i, & \text{if } i \neq s \\ q_s - c_s x \mod l, & \text{if } i = s \end{cases}$$

The resulting signature is $\sigma = (I, c_1, \ldots, c_n, r_1, \ldots, r_n)$.

VER : 역변환을 이용하여, 확인자는 서명을 체크할 수 있다.

$$\begin{cases} L'_i = r_i G + c_i P_i \\ R'_i = r_i \mathcal{H}_p(P_i) + c_i I \end{cases}$$

결과적으로, 확인자는 위 그림을 찾게 되며,

만약 등식이 성립한다면, 알고리즘 LNK를 작동하게 된다. 그렇지 않다면 확인자는 서명을 거부한다.

LNK : 확인자는 I가 이전의 서명에서 사용되었는지를 조사한다. 다중의 사용들

에서 두 개의 서명들이 같은 비밀 키에서 만들어졌다는 것을 시사하게 된다.

프로토콜의 의미 : L 변환을 적용함으로써 서명자는 그러한 x가 적어도 Pi=xG라는 사실을 입증하게 된다. proof를 반복 불가능하게 하기 위해서 키 이미지를 I=xHp(P)로 설정한다. 서명인은 같은 계수(ri,ci)를 활용하여 거의 동일한 명제인 "그러한 x가 적어도 Hp(Pi)=I · xˆ-1이라는 사실을 안다." 는 것을 증명한다.

만약 x에서 I로의 대응이 injection mapping이라면
1어느 누구도 키이미지로부터 공개키를 복원할 수 없으며, 서명인을 알 수 없다.
2서로 다른 I들과 동일한 x를 가지고 두 개의 서명을 만들어낼 수 없다.

4.3.5 표준 크립토노트 트랜젝션

비연결적 공개키와 비추적성의 ring signature이라는 2가지 방법을 결합하면, Bob은 원래의 Bitcoin 방식과 비교하여 발전된 수준의 프라이버시를 갖게 된다. Bob은 개인키 하나 (a,b)만 가지고 있으면 충분하며, (A, B)를 공개하여 익명의 트랜젝션을 송수신할 수 있게 된다.

각 트랜젝션을 유효화하기 위해서, Bob은 추가적으로 단지 2개의 타원곡선(elliptic curve)을 다중 발행하고, Bob 소유의 트랜젝션인지를 확인하기 위하여 output 당 1개를 추가하게 된다. Bob은 각각의 output에 대하여 1회용 keypair (pi, Pi)를 복원하며, 지갑에 저장하게 된다. 단일한 트랜젝션인 경우에만 동일 소유주의 input으로 확인될 수가 있다.

ring signature에 대해서 Bob의 input은 효과적으로 익명성이 유지될 수 있다.

트랜젝션이 누구의 것인지에 대한 추론이 어려우며, 이전의 th유주인 Alice 또한 다른 제3의 관찰자와 같이 정보가 없다.

만약 Bob이 n개의 외부로의 output을 같은 금액으로 전송하고, 섞어 버린다고 가정하자. Bob 스스로는 (어느 누구라도) 이러한 지불 중 어느 것이 전송되었는지 알 수가 없다. output은 수천 개의 서명에서 추상적인 요소(ambiguity factor)로 활용될 수 있으며, 숨김의 대상이 될 수는 없다. 이미 사용된 키 이미지 집합으로부터 체크함으로써, LNK 단계에서 double spend 검사가 발생된다.

Bob은 추상 정도(ambiguity degree)를 스스로 설정할 수 있다. n=1이라는 의미는 그가 output을 전송했을 확률이 50퍼센트라는 의미이다. n=99일 때는 1퍼센트의 확률을 나타낸다. 결과적인 서명은 선형적으로 O(n+1)로 증가된다. 따라서 Bob의 익명성 비용이 향상되면 트랜젝션 수수료가 높아진다. 또 Bob은 n=0이라고 설정할 수 있으며, 스스로의 ring signature를 단지 하나의 구성요소로도 만들 수 있다. 하지만 이러한 경우 그는 익명성을 전혀 보장받을 수 없다.

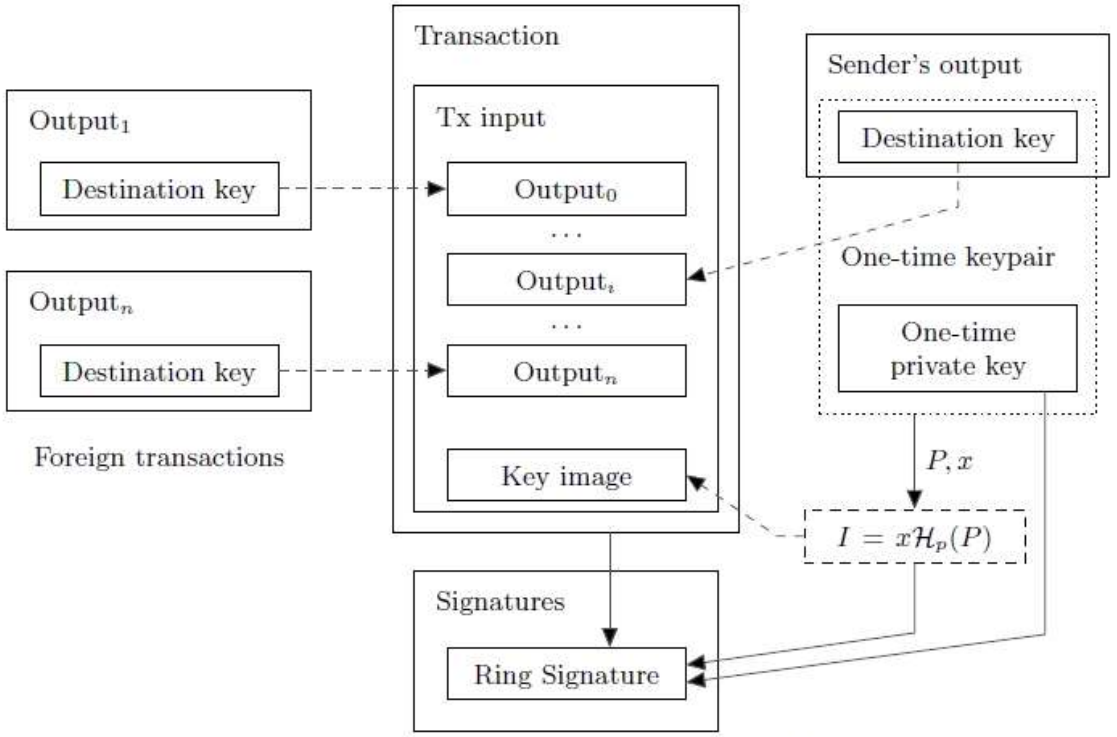


Fig. 7. Ring signature generation in a standard transaction.

4.3.6.1 평등화된 Proof-of-work

이 부분에서 새로운 proof-of-work 알고리즘을 제안하고자 한다. CPU(다수) 마이너와 GPU/FPGA/ASIC(소수) 마이너 사이의 차이를 줄이기 위한 것이다. 일부 마이너가 우위를 선점하는 것은 적절한 일이지만, 그들의 투자는 power에 대해서 적어도 선형적으로 증가해야 한다. 일반적으로 특수 목적의 장치들(주 : ASIC 등)은 가능한 수익성이 적어야 한다.

4.3.6.1 Related works

원래 Bitcoin의 proof-of work 프로토콜에서는 CPU에 중점을 둔 가격 결정 함수 SHA-256을 사용하였다. 주로 basic logical operators로 구서되었으며, 프로세

서의 계산 속도에 따라서면 바뀌기 때문에 multicore/conveyer 의 적용에 완벽히 적절하였다.

하지만 현대적인 컴퓨터의 경우 초당 operation 숫자에 의해서만 제한되는 것이 아니라, 메모리 사이즈에 의해서도 제한을 받는다. 프로세서 간의 속도 차이가 상당할 수는 있으나 메모리 사이즈는 큰 차이가 없다.

메모리를 기준으로 가격을 결정하는 함수는 Abadi에 의하여 맨 처음 소개되었으며 "주로 메모리에 접속한 시간에 의하여 계산 시간이 결정되는 함수"라고 정의되었다. 핵심적인 아이디어는 큰 블록 데이터인 스크래치패드를 상대적으로 느리게 접속될 수 있는 메모리(ram 등)에 할당하는 알고리즘을 만들고, 그 안에서 "예측 불가능한 sequance of locations의 접속을 수행"하는 것이다. 블락이 충분히 커야만 각각의 access 마다 다시 계산하는 것보다 저장하는 것이 유리해진다. 이 알고리즘은 내부적인 병렬성(internal parallelism)을 방지해야 하며, 따라서 N의 동시적인 쓰레드는 N배 많은 메모리를 요구해야 한다.

Dwork는 이러한 접근 방식에 대해 연구 및 체계화하였으며, 이를 통해 가격 결정 함수의 또 다른 방식인 "Mbound"가 탄생할 수 있었다. F.Coelho은 가장 효과적인 솔루션 "Hokkaido"를 제안했다.

현재 보편적으로 거대한 array 내에서 유사 난수 검색(pseudo-random searches)을 하는 방식은 "scrypt"라고 일컬어진다.(C. Percival) 이전의 함수들과 달리 핵심적인 derivation에 주목하고 있으며, proof-of-work system과 차이점이 존재한다. 이러한 사실에도 불구하고, scrypt는 우리의 목적을 충족할 수 있는데, 부분적인 해쉬 변환 문제에서 가격 결정 함수로 잘 작동한다는 것이다. 예를 들면 Bitcoin에서의 SHA-256이 있다.

현재 이미 Litecoin에 scrypt는 적용되었으며 일부 다른 Bitcoin 포크들에도 적용되었다. 그러나 이러한 적용은 사실상 메모리 기반의 접근방법이 아니다. “메모리 접속 시간 / 총 시간” 은 공간이 충분하지 않은데, 단지 128KB만을 사용하기 때문이다. 이를 통해 GPU 채굴자들은 거의 10배 더 효율적으로 채굴이 가능하며, 저렴하면서도 채굴효율이 좋은 장비가 등장할 가능성이 충분하다.

게다가, 스크립트를 작성하는 것으로 인해, 스크래치패드의 모든 블록이 이전의 것으로부터 발생되기 때문에, 메모리 사이즈와 CPU 속도가 반비례적으로 움직이게 된다. 예를 들어, 모든 두 번째 블록을 저장할 수 있으며, 필수적인 경우에만 다른 모든 블록들을 느린 방식으로 재계산할 수 있다. 유사 난수 인덱스(pseudo-andom index)들은 일괄적으로 배분되는데, 따라서 추가적인 블록의 재계산은 기댓값은 1/2N이다. (N은 반복수). scratchpad를 준비하고 모든 반복에 대해서 해시하는 작업과 같은 시간 독립적(constant time) operation들로 인해서 전체적인 계산 시간은 절반보다는 덜 증가하게 된다. 2/3의 메모리 사용을 줄이려면 N의 추가적인 재계산이 필요하다. 9/10을 줄이려면 4.5의 추가적인 재계산이 요구된다. 정리하면 만약 모든 블럭의 1/s만을 저장하게 되면 (s-1)/2 만큼을 곱한 것보다 덜 증가하게 된다. 바꾸어 말하면, 현대의 CPU보다 200배 빠른 CPU는 320 byte의 scratchpad 만을 저장할 수 있다.

4.3.6.2 새로운 알고리즘의 제안

proof-of-work 가격 설정 함수에 대해서 새로운 메모리 기반(memory-bound) 알고리즘을 제안한다. 느린 메모리에 대한 랜덤 엑세스에 의존하게 되며, 레이턴시 의존성을 강조한다. 스크립트와는 다르게, 모든 새로운 블록(64바이트 길이)은 이전의 모든 블록에 의존적이다. 결과적으로 메모리 절약기

(“memory-saver”)는 계산 속도를 기하급수적으로 증가시킬 것이다.

우리의 알고리즘은 다음의 이유로, 인스턴스당 2MB 정도를 요구한다.

1. 최신 CPU의 코어당 L3캐쉬에 적당하며, 몇 년 안에 주류가 될 CPU의 사양이다.

2. 최신 ASIC 파이프라인에 대해서 1MB의 내부 메모리는 부적절하다.

3. GPU의 uddn tnqor의 인스턴스를 동시에 처리할 수 있으나, GDDR5 메모리는 CPU의 L3캐쉬보다 느리고, 대역폭은 넓지만 랜덤 엑세스 속도는 낮다.

4. scratchpad가 확장되면 필연적으로 반복적 계산이 증가하게 되며, 전체적인 시간이 증가하게 된다. 신뢰성이 낮은 p2p 네트워크에서 많은 계산량은 심각한 취약점으로 남을 수 있는데, 왜냐하면 node는 모든 새로운 블록의 proof-of-work에 대하여 체크할 의무가 있기 때문이다. 만약 node에서 각각의 해쉬 평가에 대해 상당한 시간을 소모한다면, 임의 작업 데이터로 가득 찬 가짜 오브젝트들로 인한 Ddos 공격에 취약해진다. (nonce value)

5. 더 많은 장점들.

6. 안정적인 통화량 발행

크립토노트 전자 코인의 상한값(upper bound)은 MSupply = 2^54 -1 원자단위(atomic units)이다. 이러한 것은 기술적인 제한값이며 “N개의 코인이 충분하다” 라는 직관적 방식에서 계산된 것이 아니다.

발행 과정을 안정적으로 유지하기 위하여 블록 리워드에 대해 다음과 같은 공식을 사용한다.

BaseReward = (MSupply − A) >> 18

여기에서 A는 이전에 생산된 코인의 양을 의미한다.

4.3.7 수정 가능한 파라미터

4.3.7.1 난이도

크립토노트에서는 모든 블록마다 난이도를 변경시킨다. 네트워크 해쉬레이트가 급격하게 성장하거나 감소할 때에 대한 반응시간이 낮아질 수밖에 없고, constant block rate로 고착된다. 원래의 Bitcoin 방식에서는 마지막 2016개의 블록간의 목표 기간과 실제 기간을 비교하게 되고, 이를 현재의 난이도에 대한 배수(multiplier)로 적용한다. 이러한 비트코인의 방식에 따르면 난이도가 급증 급락한다는 점이 단점이다.

크립토노트의 기본적인 알고리즘은 node에 의하여 계산된 모든 work를 합하고, 그들이 소비한 시간으로 나누는 것이다. 일의 단위는 각각의 블록의 난이도 값에 상응한다. 하지만 time stamp에서의 부정확성과 비신뢰성 때문에 블록 사이의 정확한 시간 간격을 알아내기는 어렵다. 만약 한 유저가 time stamp를 미래로 전환한다면 다음의 interval은 감소하거나 심지어 음수가 될 것이다. 이러한 사례가 거의 없을 것으로 생각되며, 단지 time stamp를 정리하고 초과분을 소거할 것이다.(20퍼센트 정도) 나머지 값들의 범위는 80퍼센트의 상응하는 블록에

대하여 소비한 시간 값이다.

4.3.7.2 사이즈 제한

사용자들은 블록체인을 저장하는 것에 대하여 지불하며, 사이즈에 해당하는 투표 권한을 가진다. 모든 채굴자들은 수익과 지용의 균형 사이에서 절충을 선택해야 하는데, fee와 블록을 만드는 것에 대한 자신만의 “soft-limit”에 대한 균형이다. 또 위조 트랜젝션을 막기 위해서 최대 블록 사이즈에 대한 핵심 규칙은 필수적이다. 하지만 이러한 값은 수정할 수 있어야 한다.

Mn이 N블록 사이즈에 대해서 중간 값이라고 가정하자. 그러면 블록을 받아들이는 데에 대한 “hard-limit”은 2 · MN이 된다. 이러한 것을 통하여 블록체인의 bloating을 방지하며, 시간에 맞게 서서히 성장하도록 허락한다.

트랜젝션 사이즈는 명시적으로 제한될 필요가 없다. 블록의 사이즈에 따라 달라지며, 만약 누군가가 수백개의 input / output을 이용하여 거대한 트랜젝션을 보내고자 한다면 (혹은 ring signature에서 큰 추상성을 가질 경우), 충분한 수수료를 지불함으로써 트랜젝션을 진행할 수 있다.

4.3.7.3 트랜젝션 스크립트

크립토노트는 굉장히 최소화된 스크립트 서브시스템을 가지고 있다. 송신자는 특정한 표현 Φ = f (x1, x2, . . . , xn)을 규정하는데, n은 destination 공개 키 C:\Users\ddd\AppData\Local\Temp\Hnc\BinD 의 숫자이다. 5 binary의 오퍼레이터

만 지원되며, min, max, sum, mul, cmp이다. 수신자들이 이 지풀을 소비하게 되면, 0 ≤ k ≤ n 의 서명을 생산하고, 트랜젝션 input으로 전송하게 된다. 확인 과정은 단순히 s Φ with xi = 1를 평가하여 공개키 Pi에 대한 유효한 서명을 체크하며, Xi=0임을 확인한다. 확인자는 만약 Φ > 0인 경우에 proof를 받아들인다.

간단함에도 불구하고, 이러한 방식으로 가능한 모든 경우에 대처할 수 있다.

o multi-/threshold 서명. 비트코인 스타일의 “N 개중 M ro” multi 서명(수신자는 적어도 0 ≤ M ≤ N 의 유효한 서명을 공급해야 한다.) Φ = x1+x2+. . .+xN ≥ M 가중 threshold 서명(일부 키는 다른 키보다 중요할 수 있음)은 Φ = w1 · x1 + w2 · x2 + . . . + wN · xN ≥ wM로 표현될 수 있다. 마스터키는 Φ = max(M · x, x1 + x2 + . . . + xN) ≥ M에 상응한다. 이러한 방식으로 복잡한 상황을 간단하게 표현할 수 있다.

o 암호의 보호. 비밀 암호 s를 보유한 것은 개인 키에 대한 지식을 보유한 것과 동등하며, 확정적으로 암호 k=KDF(s)로부터 도출된다. 따라서 수신자는 k key 하의 또 다른 서명을 제공함으로써 비밀번호를 안다는 사실을 입증할 수 있다. 송신자는 단순히 자신의 output에 상응하는 공개 키를 추가하면 된다. 이러한 방식은 Bitcoin에서 사용되는 “transaction puzzle”보다 상당히 안전하다.

o Degenerate cases. Φ = 1인 상황에서는 어느 누구든지 돈을 사용할 수 있다. Φ = 0인 상황에서는 해당 output이 영원히 사용 불가능함을 나타낸다.

만약 공개키와 통합된 output script가 송신자에게 지나치게 클 경우에, 특별한 output type을 이용할 수 있다. 송신자가 단지 그것에 대한 해쉬를 공급하는 반

면 수신자는 이 데이터를 그의 input으로 보내게 될 것이다. 이러한 접근은 Bitcoin의 “pay-to-hash”와 유사한 방식이다. 새로운 스크립트 명령을 추가하는 대신에, 데이터 구조 수준에서 이러한 케이스를 다룬다.

05. 결론

코인과 리츠는 부동산을 금융상품으로 만든다는 측면에서 큰 차이가 없다. 비유동적인 부동산을 금융시장에서 거래할 수 있게 되면 유동성 증대, 자금 유입, 포트폴리오 효과를 누릴 수 있는데, 이런 측면에서 코인과 리츠의 차이는 암호화폐시장과 증권시장의 차이로 귀결된다. 하지만 거래 비용 절감과 스마트 계약 활용은 블록체인 기술을 활용한 코인만의 장점으로 볼 수 있다. 따라서 스마트 계약고 같은 블록체인 기술만의 장점을 코인과 결합하면 리츠와는 차별되는 즉 질적으로 다른 부동산 유동화가 가능할 수도 있다.

코인을 활용하면 구분소유권 거래에 기초해서 빚 없이 주택 지분 일부으 현금화가 가능하다. 블록체인 기술을 활용하면 소유권의 분해・거래・기록에 대한 비용을 감소시킬 수 있고, 이에 따라 구분소유권 거래의 활성화 및 규모화가 촉진될 수 있다. 주택소유주는 미래의 주택 매각 시점에서 일정한 가치를 지급하는 구분소유권 양도 계약을 통해 이자 지급 없이 자신의 주택 지분 일부를 미리 현금화 할 수 있다. 이와 같은 구분소유권 거래는 여전히 그 집에서 살면서 alw을 늘리는 것 없이 현금을 확보할 수 있다는 측면과 역모기지 등과 같이 부채를 활용한 기존 부동산 유동화와 차별화 될 수 있다.

06. BHC 코인 발행 및 배포

BHC Coin은 총 100억 개를 발행할 계획이다. 특히, 비즈니스와 접목하여 업무를 활용하는 동안에 다양한 아이템을 운영하도록 하여 콘텐츠의 공급과 수요를 창출하고, 향후 모든 업무를 통합하므로 인한 다목적이고 빅테이터로의 풍부한 플랫폼으로 발전하고자 한다. 부동산 운용 전문 가상자산으로서 투명한 부동산

매매와 임대료 지급 프로세스를 갖추는 것을 목표로 하며 다양한 콘텐츠(업무) 및 디지털 마케팅의 생태계에서 비지니스와 유관 회사 그리고 이용자가 투명한 형태로 비즈니스와 콘텐츠(또는 아이템)를 활용하고 수익을 창출할 수 있도록 나아갈 것이다.

07. 플랫폼

BHC Coin은 2021년 02월 초순부터 베타 테스트를 거친 후 2021년 02월 24일부터 유통 가능합니다.

BHC Coin은 2021년 02월 27일 14:00(한국표준시간)을 DBX 거래소에 직상장하여 거래를 시작할 것입니다.

08. P2P(개인 대 개인)의 거래

BHC Coin은 고객이 제3자 대신 서비스를 제공할 사람을 직접 선택하고 상호 소통하는 개인 대 개인 플랫폼입니다. 이 플랫폼은 안전하고 빠른 결제 서비스를 제공할 것입니다.

09. 중립적인 서비스의 거래

BHC Coin은 짧은 시간에 이뤄야 하는 리얼타임의 단순한 거래에서부터 전문적인 서비스를 필요로 하는 전문서비스에 이르기까지 다양한 서비스를 할 수 있도록 하여 모든 지불과 계약의 업무에 적합합니다. BHC Coin은 다양한 서비스를 위하여 다양한 기술을 사용자에게 제공합니다.

BHC Coin은 모바일 서비스, 오프라인 서비스, 일회성 작업, 주기적인 그룹 예약 대해서 유연하게 대처할 수 있는 기능을 제공합니다.

10. 자금 운용 계획

BHC Coin의 법적 비용에는 법률 연구를 포함되어 있습니다.
기본적으로 각종 인증, 승인, 허가 등의 라이선스 비용과 실제 법률적 근거를 찾기 위한 연구비, 사례 연구비 등이 포함될 것입니다.

11. 변동성에 대한 보호

희소성을 가진 코인은 투기로 인해 발생되는 변동성 때문에 선호되는 가상화자산이 아닙니다. BH Coin은 먼저 거래소 상장을 통하여 입증된 가치를 지키고 BH Coin의 가치를 유지하기 위한 BH Coin의 소각 및 상장된 BH Coin의 회수 등을 활용하여 변동성을 막을 계획입니다. 코인이 가상자산으로 활용되는 동안 그 가치가 보장됩니다.

시장 가격이 합산되고 비정상 값이 제거되어야 올바른 결과를 얻을 수 있습니다.

12. 카드결제

코인의 경우 현재 일반 매장에서 사용할 수 있는 인프라 구축이 부족한 상황입니다. 가상자산이 실제로 시장에서 통화로서 가치를 지니

기 위해서는 통용이 되어야 할 것입니다. 때문에 점진적으로 화폐가 실물 자산에서 가상자산으로 이동하는 과도기에서 사용자들이 현금과 가상자산을 모두 사용할 수 있도록 시스템을 구축할 예정입니다. 즉 은행을 통해 코인 사용자에게 카드를 발급해주고 일반 매장에서 카드 결제시 사용자가 보유한 코인 만큼 거래소에서 코인과 현금이 자동 거래 되어 실시간으로 현금 결제도 가능하도록 시스템을 구축할 것입니다.

13. 코인 판매 및 환불

코인

BHC Coin은 증권, 주식 또는 이익 분배 메커니즘이 아닙니다. 코인 판매 참가자는 코인을 구입할 때 위험 요소를 이해하고 참여하기 전에 BHC Coin의 백서 전체를 읽어야 합니다. 코인 판매에 참여하는 것은 BHC Coin의 판매 및 구매 약관의 적용을 받습니다.

기술적인 위험

BHC Coin의 계약은 CryptoNote 표준을 기반으로 합니다. 계약서에 기술적 오류가 없도록 모든 노력을 기울이고, 메인넷 3.0을 준비하였습니다. 참가자는 이 위험을 이해하기 위해 블록체인 기술을 숙지해야 합니다. 참가자는 개인키 저장 및 전송과 관련된 위험을 이해해야 합니다.

해커와 형사상의 개입

BHC Coin의 계약 주소는 http://www.bhcc24.com을 통해 제공됩니다. 범죄의 행위 중 잘못된 주소를 통해 돈을 보내도록 컴퓨터와 이메일 서버를 인수하려는 시도가 있습니다. 여기에는 사회 공학이 포함될 수 있습니다. BHC Coin은 잠재적인 공격을 막기 위해 모든 모범 사례 보안 조치를 구현합니다. 참가자는 올바른 계약 주소를 다루는 모든 합리적인 노력을 기울여야 하며, BHC Coin의 모든 지침을 준수해야 합니다. 참가자는 BHC Coin을 대표하는 척하는 사기를 일으킬 수 있으므로 http://www.bhcc24.com 외에 외부 게시된 계약 주소를 사용해서는 안 됩니다. 참가자는 BH Coin의 지시에 따라 모든 보안 모범 사례를 따라야 합니다.

세금 및 규제 위험 요소

코인 구매자는 자신의 관할권에 있는 가상자산의 세금, 증권 및 기타 규정에 관한 모든 현지 법률을 준수하는지 확인하기 위해 자체 실사를 수행해야 합니다. BHC Coin의 판매는 향후 추가 규제의 대상이 될 수 있습니다.

환불

환불은 처리되지 않습니다. 일단 판매가 되면 취소할 수 없습니다.

14. 법적 고지 사항

BHC Coin은 유가증권이 아니며, 소유권을 나타내지 않습니다. 따라서 이 백서의 내용은 금융 프로모션의 용도로 사용되지 않습니다. 백서에 기술되어 있는 내용을 기반으로 계획에 맞도록 BHC Coin을 운영할 예정입니다. (객관적이고 합리적인 의사결정에 따라 개발 변경 사항이 적용될 수 있습니다.)

귀하가 BHC Coin의 사업에 참여하기 위해서 다음과 같은 내용을 정확히 확인, 완벽히 이해하시고 아래의 내용에 대하여 합의하시기 바랍니다.

1. BHC Coin은 어떤 관할권에서도 유가증권을 구성하지 않습니다.
2. 이 백서의 모든 내용은 어떠한 형태로든 투자 활동을 유도하거나 초청의 용도로 사용하지 않습니다.
3. 본 백서의 내용을 임의적으로 해석하고 이해해서는 안 됩니다. (BHC Coin, 거래소 및 관련 Platform 포함)
4. 본 백서에 포함된 모든 정보와 BHC Coin으로부터 현재 또는 미래에 공지되는 내용은 발생 시점과 관계없이 어떠한 형태로의 이익 또는 이익의 보장으로 해석되어서는 안 됩니다.
5. 큰 가격 변동성, 가상자산 시장이 가지는 특유의 위험성 등 가상자산과 연관된 위험이 있음을 인정하며, 이는 자금적 손실도 포함합니다.
6. BHC Coin의 사업의 운영, 가상자산의 판매 등과 관련하여 위험이 있을 수 있습니다.
7. BHC Coin의 사업들은 현재 개발 중이며, 출시 후에도 수시로 변화가 있을 수 있습니다.
8. 때에 따라 BHC Coin에서 귀하에게 e-mail을 발송할 수 있음을 인정합니다. 그리고 이러한 e-mail 통지는 귀하의 기밀정보를 요구하지 않습니다. 따라서 이와 관련하여 사기, 피싱 시도 및 악의적인 의도의 접근 가능성이 있습니다.

이에 비공식적인 문의에 대해서는 응답하지 마십시오.

9. BHC Coin에서는 코인 사업의 운영 기간을 보증하지 않을 수 있습니다. BHC Coin 사업은 대중의 관심 부족 또는 솔루션 개발을 위한 자금 부족과 같은 여러 가지 이유로 중단될 수 있습니다.

10. BHC Coin 소지자는 결코 BHC Coin에 대한 어떠한 유가증권이나 지분도 소유함을 의미하지 않습니다.

귀하 및 BHC Coin의 상호 이익과 분쟁을 방지하기 위하여 상기의 법적 면책 조항을 명확하게 이해하시고 이를 합의 인정하시기 바랍니다.

-- (끝) --