비트코인을 활용한 효율적 전자화폐 활성화 방안

이준형* · 이성훈* · 이도은* · 김우철* · 김민수**

요 약

현재 통용되고 있는 '전자화폐'는 기존에 통용되던 실물화폐를 디지털화하여 사용할 뿐 물리적으로 통용되던 화폐를 벗어나지 못하고 있는 실정이다. 특히 비트코인의 경우 발행주체 없이 '채굴'이라는 행위에 의해서만 발행되며, 개인간 거래는 P2P 형태로 '블록체인(BlockChain)'을 통해 거래를 증명하는 형태로 몇몇 국가에서 화폐로써 인정을 받아 제법 활발히 통용되고 있지만, 비트코인이 갖는 특성들 때문에 여러 가지 문제를 안고 있다. 따라서 본 연구에서는 비트코인의 활성화 방안에 있어 정책적, 관리적, 기술적 문제점들에 대한 대안을 제시하고자 한다.

Effective Vitalization Plan of Electronic Cash using Bitcoin

Jun Hyung Lee* · Seong Hun Lee* · Do Eun Lee* · Woo Cheol Kim* · Minsu Kim**

ABSTRACT

It is current status that currently-used 'electronic cash' cannot go beyond the physically and commonly-used as it is used by digitalizing the existing commodity money. Especially in case of bitcoin, though it is issued only by the activity called 'mining' without the issuing body and used in some countries in relatively-active way as it is admitted as the currency in the way that proves the transaction through 'BlockChain' in the form of P2P for the transaction among the individuals, it has several issues due to the characteristics it has. So, this research is willing to suggest the alternative plan to matter of policy, managerial and technical problems regarding the vitalization plan of bitcoin.

Key words : 비트코인, 블록체인, 전자서명, 멀티시그니처, 전자화폐

접수일(2016년 6월 23일), 수정일(1차: 2016년 6월 30일, 2차: 2016년 6월 30일), 게재확정일(2016년 6월 30일)

* 경기대학교 융합보안학과
** 경기대학교 융합보안학과(교신저자)

1. 서 론

공동체 구성을 바탕으로 한 '국가'의 개념 등장과 이를 기반으로 구성원들은 보다 안전하고 체계적인 사회적 활동을 영위할 수 있게 되었다. 또한 발전적 사회 활동을 위한 기능적 수단으로 '화폐'가 등장하게 되면서 사회적 활동과 더불어, 경제적 활동이 국가 발전의 중요한 요소로써 한 국가의 발전적 척도로 자리매김하게 되었다.

이와 같은 화폐의 쓰임은 시대의 흐름에 따라 다양한 형태로 변모하였고, 각국의 중앙은행이 독점적으로 발행하면서 야기되는 극심한 인플레이션이 등의 문제점으로 인한 지금의 '실물화폐'는 지식정보사회의 패러다임과 발맞추어 '전자화폐'로의 전환을 꽤하고 있다.

그러나 현재 통용되고 있는 '전자화폐'는 기존에 통용되던 실물화폐를 디지털화 하여 사용할 뿐 물리적으로 통용되던 화폐를 벗어나지 못하였다. 이러한 반쪽짜리 전자화폐는 2009년 '나카모토 사토시'라는 익명의 프로그래머에 의해 '비트코인'이 처음 발행되면서 새로운 전환을 맞이하게 되었다.

비트코인은 실물과 발행주체 없이 '채굴'이라는 행위에 의해서만 발행되며, 개인 간 거래는 P2P 형태로 '블록체인(BlockChain)'을 통해 거래를 증명하는 형태로 몇몇 국가에서 화폐로써 인정을 받아 제법 활발히 통용되고 있는 실정이다.

하지만, 비트코인이 갖는 특성들 때문에 여러 가지 문제를 안고 있다. 우선 익명성을 보장해 프라이버시를 보호하고 있지만 이로 인해 불법적인 거래로 악용될 수 있으며, 해킹을 통한 도난의 위험성 그리고 매 4년마다 공급량이 줄어드는 구조로 인해 디플레이션을 유발, 실물경제에 악영향을 미칠 수도 있다. 이 외에도 다단계 거래의 특성을 가지고 있어 수요가 없으면 비트코인의 가치가 폭락할 수도 있어, 전자화폐로의 장점들 이면의 문제점들로 인하여 기존 통화를 대체할 수 있는 지급 및 결제수단으로 사용될 가능성에 대해서는 아직 결론을 내리기 어렵다는 것이 공통된 의견이다.

따라서, 본 연구에서는 비트코인의 활성화 방안에 있어 정책적, 기술적 문제점들에 대한 대안을 제시하고자 한다.

2. 관련연구

2.1 비트코인(Bitcoin)

비트코인의 개발자인 '나카모토 사토시'가 2008년 논문을 발표한 논문을 발표하였고 그 논문을 바탕으로 비트코인은 개발되었고 연구되었다. 비트코인 이전의 인터넷에서의 상거래는 거의 금융기관을 제 3자 신용기관(Trusted Third Parties)으로 하는 전자지불 방식에 전적으로 의존하였다. 대부분의 거래에 충분히 정상적으로 작동하고 있지만, 여전히 신용기반 모델이라는 내재적인 약점을 가지고 있다. 이러한 방식은 금융기관이 거래상 발생하는 분쟁을 중재해야하기 때문에 이것이 거래 수수료를 올리는 결과를 가져온다. 바로 이러한 문제를 해결하기 위해 신용보다는 암호화 기술에 기반한 전자지불 시스템을 이용하여 두 거래자가 제 3자인 신용기관 없이도 직접적인 거래를 가능하게 구현하였다. 네트워크적으로 번복이 불가능한 송금은 판매자를 가짜 지불로부터 보호할 수 있으며, 구매자는 에스크로 방식을 통해 보호받을 수 있다. 비트코인은 이러한 거래들의 시간 순서에 따라 입증하게 만들도록 하는 'P2P 분산 네트워크' 기반의 거래를 통해 이중지불의 문제를 방지하는 해법을 제시하였다[1].

2.2 비트코인 적용기술

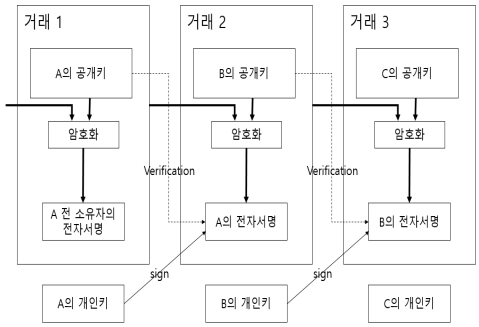
2.2.1 주소(address)

비트코인의 주소는 비트코인 네트워크 내에서 유일무이하며 공개키로 사용된다. 주소와 주소 사이의 비트코인 이동인 거래(transactions)은 블록체인 사이트에 모두 공개된다. 주소는 1또는 3으로 시작하는 34자리 알파벳과 숫자의 조합으로 이루어져 있다. 그 중 헷갈릴 수 있는 문자인 0,I,O,l(숫자 0, 대문자 I, 대문자 O, 소문자 l)은 사용하지 않아서 58가지 조합으로 33자리를 채워 312아승기 가지의 조합이 가능하다. 실제로 사용되는 비트코인의 예시는 '1FJWnwCiogjNAjE9JWxWBdGG7iprKUcuy3' 같은 식이다.

2.2.2 거래(Transaction)

전자화폐는 전자서명의 연속으로 정의된다. 각 공

개키와 개인키의 소유자들은 그 전까지의 거래 내역에 다음 소유자의 공개키를 덧붙인 뒤 자신의 개인키로 암호화하는 전자서명을 하고 넘긴다. 전자화폐를 받는 사람은 서명 소유자들의 체인과, 서명들을 검증할 수 있다[1].



(그림 1) 비트코인 거래[1]

위와 같은 구조를 가지더라도 '이중지불'이라는 큰 문제가 존재한다. 기존에 사용되던 해법은 모든 거래가 이중지불 되었는지 확인해줄 수 있는 중앙집권적인 TTP(Trusted Third Party)를 도입하는 것이다. 하지만 이러한 방식은 TTP에서만 직접 화폐를 발행하여 쓰도록 하기 때문에 화폐의 시스템 자체가 TTP에 너무 의존적이라는 문제를 가지고 있다.

비트코인에서는 이러한 문제를 해결하기 위해 돈을 받는 사람이 이전 소유자가 그 전에 어떤 거래에도 서명하지 않았는지를 확인할 수 있도록 하였다. 거래내역을 모두 검색하여 거래 내역이 하나라도 비어있는지 확인하여 거래 내역이 비어있지 않다면 이중지불이 되지 않았다고 판단하는 것이다. TTP를 거치지 않고도 이를 확인하려면 모든 거래가 공개되어 있고, 참여자들이 시간 순서에 따라 오직 하나의 거래내역만을 인정하는 시스템이 필요하다. 이를 위해 '블록체인'이라는 공개되어 있고 과반수이상의 참여자들이 거래내역이라고 인정하는 시스템을 사용하고 있다[2].

2.2.3 공개키 암호화 방식

비트코인 네트워크에서 사용하는 암호화 방식은 공개키 암호화 방식이다. 2.2.1에서 설명한 '주소'가 공개키가 되는 것이고, 개인키는 사용자의 PC에 저장된다. 이는 대중적으로 익히 알고 있고 사용하고 있는 PKI (Public Key Infrastructure)와 비교할 수 있다.

<표 1> 비트코인에서의 공개키와 PKI의 비교[3]

항목	공통점	차이점
비트코인 암호화	• 소인수분해에 기반한 RSA 알고리즘을 사용 • 개인키는 유출에 대비하여 암호화하여 보관	CA, Root CA가 필요 없음 인증서 대신 개인키 역할을 하는 '지갑' 존재
PKI		CA, Root CA가 필요 인증을 위한 인증서(Certificate)가 존재

PKI에서는 믿을만한 공인 인증기관(CA)에서 키를 만들었다는 인증서를 발급한다. 이 인증서에는 그 공인 인증기관의 공개키가 포함되어있다. 또한 각각의 피어(Peer)에게는 개인키가 발급된다. 공인 인증기관에서는 이 피어에게 할당된 개인키과 공개키가 '적법한 절차'를 통해 만들었다는 의미에서 인증서를 발행하게 되며, 이것은 공인 인증기관에 의해 보증된다[4][5].

반면 비트코인에서 사용하는 공개키 방식은 공인 인증기관이 추가로 존재하는 것이 아니다. 공개키와 개인키는 쌍을 이루지만 이것을 보증해주는 기관은 없다. 오직 개인키를 담고 있는 지갑과 주소라는 이름으로 사용되는 공개키를 이용한 서명을 통해 거래를 입증한다.

2.3 선행연구 분석

비트코인을 비롯한 전자화폐에 대한 연구는 올해 초 중국 인민은행에서 발표하였던 '독자적인 비트코인 개발'과 레딧(Reddit)과 같은 국외의 소셜 뉴스 웹 사이트 등과 같이 중앙은행, 소수의 참여자들에 의해 이루어져 왔다. 물론 심도 깊은 연구는 이들과 같은 전문가집단에서 이루어지는 것이 맞지만, 본 연구의 주제인 전자화폐 및 그 지불수단의 활성화 방안에 관한

연구는 전문가집단이 아닌 일반 소비자들의 심리를 연구해야한다. 이러한 연구 역시 한 축으로 진행되고 있다.

연구 결과 비트코인의 경제성은 인지된 유용성에, 호환성은 인지된 사용 편리성에 긍정적 영향을 미친다. 지불 편의성은 인지된 유용성과 인지된 사용 편리성 모두에 긍정적인 영향을 미친다. 이에 따라 인지된 사용 편의성은 인지된 유용성에 긍정적 영향을 미치고, 결과적으로 인지된 유용성과 신뢰성은 사용의도에 긍정적인 영향을 미친다고 나타났다[6][7].

3. 제안하는 방법

가상화폐는 현재 지급결제수단이자 투자대상으로 널리 사용되고 있다. 이에 각국은 가상화폐를 활용한 거래를 교환거래의 일종으로 간주하여, 그 거래에 대한 차익에 대해 과세를 하고자 하고 있다. 하지만 현재 각국의 세제상의 대응방안은 천차만별이고 우리나라는 별다른 대응방안도 없는 실정이다.

기존 연구의 경우 각국의 대응방안에 대한 특징과 장단점을 살펴보고 거래 관련 과세방향과 기본적 해결방안에 대해 검토와 가상화폐를 세법상으로 분류할 때 법정통화에 해당할 수 없어 신유형의 무형자산으로 분류할 수 있다는 점을 제시했으며, 이에 따라 외화와 같이 평가대상에 해당되는 자산은 아님을 밝혔다. 또한 가장 중요한 거래 흐름중 하나인 개인과 법인 간의 지급결제수단에 있어서의 과세에 대해 구체적인 흐름을 제시한다. 이 경우 법인은 가상화폐 사용여부를 국가에 등록하는 것이 필요하다는 것도 검토하며, 과세관청은 비트코인과 같은 가상화폐에 대한 과세거래 정보 수집이 필요 하는 것도 제시한다.

각 주요 국가들은 가상화폐의 성격에 맞게 대응방안을 구성해 과세 정책을 세우고 있지만 우리나라만 별도의 대응책이 없는 것의 문제점도 심각하게 논하고 있다. 비트코인과 같은 가상화폐는 '현금과의 교환' 또는 '재화나 용역과의 교환'에 대해 대다수 해당하므로 관련 경우에는 과세하는 것이 옳다. 하지만 과세관청과 납세의무자 간의 거래 정보비대칭 문제가 있으므로 가상화폐에 대한 과세는 매우 까다로우며 이를 해결하는 것이 해당 문제를 해결하는 것의 열쇠이다. 현재 우리나라는 ICT 인프라 배경이 매우 고도화되어 있고, 핀테크 산업 발전이나 다양한 ICT 기반의 지급결제수단 활용이 필요한 시점이므로 해당 문제는 시급히 해결해야할 사회적 이슈이며 계속적인 연구가 필요하다[8][9].

<표 2> 국가별 비트코인 규제 현황[10]

구분	국가	내용
적대적	중국	개인의 거래는 자신의 책임 하에 거래할 수 있으나 금융기관의 거래는 금지
	러시아	비트코인을 사용하는 것이 불법이며 이를 비롯한 모든 가상 화폐 사용을 불법으로 간주
우호적	독일	비트코인에 가장 친화적인 나라로 개인의 비트코인 사용 및 소지를 발 빠르게 인정하여 '비트코인의 수도'로 자리매김 하였으며 이에 대한 자본소득세 징수
	한국	한국정부는 중앙은행인 한국은행이 비트코인을 다룬 보고서를 내놓았지만 2013년 당시 아직은 화폐로써의 역할을 수행하기에는 부적절하다고 판단하였으며, 비트코인 규제안은 아직 없음

전담부서를 지정하여 국내의 거래상황 파악 및 경제적 측면을 담당해야하고, 보안/기술적 측면도 강화해야할 필요성이 있지만, <표 2>와 같이 우리나라는 비트코인을 비롯한 가상화폐에 대해서 특별한 규제정책 및 방침을 마련하고 있지 않다. 현재 가상화폐 거래가 증가하고 있는 상황에 비추어보면 활성화방안에 대한 정부당국의 역할이 부족한 실정이다[11].

3.1 정책적 제안

우리나라는 현재 비트코인을 포함한 라이트코인(Litecoin), 이더리움(Ethereum)과 같은 전자화폐에 대해 특별한 규제를 내놓지 않고 있다. 이러한 규제 및 과세 방안에 대한 논의는 지난 2013년 한국은행에서 이루어진 논의를 제외하면 전무하다시피하다. 한국은

행에서 2020년까지 추진하려는 '동전 없는 사회'와 궤를 같이하는 방법도 한국은행으로서는 이를 추진하려는 움직임은 아직 없다[12].

하지만 비트코인을 비롯한 전자화폐를 세금 징수대상만으로 보는 규제적 접근방식은 곤란하다. 비트코인은 기존에 거래되었던 상품들과는 다른 특성을 지니고 있으며 향후 금융 및 상거래의 패러다임을 바꿀 수 있는 가능성을 가지고 있기 때문이다[11].

비트코인에 대한 회의적인 시각도 많이 존재하지만 비트코인이 처음 활용한 기술인 블록체인은 큰 각광을 받고 있다. 세계적인 금융회사들의 블록체인 컨소시엄인 'R3 CEV'는 블록체인을 이용하여 기업어음의 발행 및 거래에 대한 과정을 실험하였다. 이 R3 CEV는 2014년 출범한 이래로 기존에 40개 은행이 참가하였으나 국내 은행은 참가하지 않고 있었다. 뒤늦은 올해 4월 하나은행이 국내 은행으로는 처음으로 참여를 하게 되었다. 세계적으로 유명한 은행들이 이처럼 블록체인 기술에 지대한 관심을 보이는 와중에 IT 강국이라고 자신하는 대한민국에서는 블록체인 기술에 큰 관심이 없다. 이것은 우리나라가 향후 대세가 될 수 있는 기술에 대한 주도권 및 경쟁력을 상실하는 결과를 낳게 될 것이다[13].

3.1.1 규제와 세금

앞서 밝혔던 것처럼 비트코인은 현재 국가로부터 공식적인 규제로부터 자유롭다. 이러한 결과를 가져올 수 있었던 것은 발행자가 없으며, 지급을 보장하지 않는 화폐는 인정할 수 없다는 법적 근거를 제시한 한국은행의 발표 때문이다. 앞으로 비트코인이 국내에서 가지는 법적 지위는 3가지 경우로 나누어볼 수 있다.

첫째, 기존의 법을 개정하여 비트코인을 일종의 화폐로 분류로 비트코인을 화폐로 인정하는 것은 기존 한국은행의 방침에 반하며, 대부분의 국가에서 비트코인의 사용을 인정하고는 있으나 심한 가격변동성을 이유로 공식 화폐로 인정하지 않는 것과 맥을 같이하기 때문에 어려울 것으로 보인다.

둘째, 비트코인을 화폐가 아닌 금과 같은 재화로 분류하여 관련법을 적용하는 것으로 비트코인을 마치 금과 같은 재화로 구분하는 것인데, 비트코인이 금과 비슷한 점은 2100만개만 발행되는 비트코인과 같이 희소성이 있으며, 투기 및 투자 수단으로 이용되어왔다는 것이다. 하지만 금과 달리 물리적 운송 및 보관이 불필요하며, 만약 금과 같은 취급을 받게 된다면 비트코인에도 부가가치세를 부과하게 되는 결과를 가져올 것이다. 비트코인에 부가가치세를 적용하는 것은 정부로서는 세수확대를 위한 매력적인 카드이겠지만 시장에는 악영향을 끼칠 것이다.

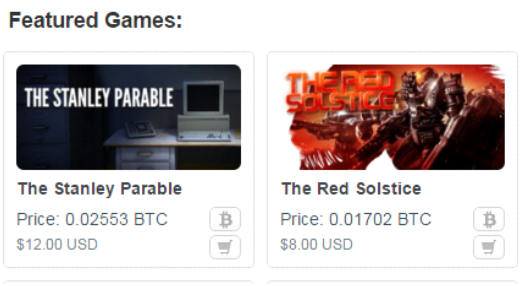
마지막으로, 비트코인과 관련된 법을 마련하여 이 비트코인을 위한 법의 테두리에 넣는 방안으로 비트코인과 관련된 법을 신설하는 것이 좋을 것이다. 비트코인과 블록체인 기술은 기존의 금융 및 상거래 방식의 비용과 시간을 획기적으로 줄일 수 있다[14].

3.1.2 인식의 변화

비트코인에 대한 대중의 인식은 "몇 달 사이에 가격이 수십 배 급등했다가 폭락한 투자대상"이 주를 이룬다. 많은 사람들이 비트코인을 단순 투자, 투기 대상으로 여겨 도박성을 가지고 있다고 생각한다. 겉으로 보이는 가격의 상승 및 하락에는 관심이 있으나 그 이면에 존재하는 가치에 대해 잘 알지 못하는 경우가 많다. 이러한 자극적인 정보보다 중요한 것은 비트코인과 블록체인이 가지는 가치와 그 무궁무진한 가능성이 가격변화보다 중요하게 조명이 되어야한다. 이미 비트코인은 우리가 주도권을 잡지 못하였지만 이더리움(Ethereum)과 리스크(Lisk)처럼 비트코인의 기술을 넘어 그 자리를 채울 수 있을 것으로 보이는 화폐들에 대한 주도권을 가져오는 것이 앞으로 더욱 중요해질 것이다.

(그림 2) 비트코인 시장가격[14]

이러한 주도권을 가져오기 위해서는 오직 소수의 전문가 집단에 의해서가 아니라, 많은 대중들이 비트코인과 블록체인이 가지고 있는 기술에 관심을 가지도록 하는 것이 필요하다. 이를 위해 비트코인과 블록체인에 대한 내용을 일반인들에게 교육하는 프로그램을 편성하거나, 실생활에서 비트코인이 사용될 수 있도록 하는 것이 중요하다. 이것을 국내 소비자들이 와 닿게 느낌 수 있었던 것은 유명 게임 플랫폼인 '밸브'의 '스팀(Steam)'을 통해서이다.



(그림 3) 비트코인 결제를 할 수 있는 스팀[16]

(그림 3)과 같이 스팀에서는 '$12 USD'라는 달러 가격과 '0.02553 BTC'라는 비트코인으로 환산된 가격표를 제공하며 이에 해당하는 비트코인을 송금하면 구입이 가능하다. 스팀에서 결제를 해본사람은 알겠지만 기존에 스팀에서는 페이팔(Paypal)을 이용하거나 해외결제 승인이 된 VISA 카드를 이용해야만 했다. 이것은 국내 사용자들에게는 아주 불편하게 느껴졌는데, 그 이유는 페이팔은 국내 사용자들 중 소수만 사용해보았고, VISA 역시 따로 카드를 신청해야하는 불편함을 겪었다. 때문에 수수료를 받고 결제를 대행해주는 사이트까지 있다.

3.1.3 정책적 변화

2016년 5월 8일 IT 전문매체인 엔가젯은 스위스의 '추크주(Zug)'에서 수도세 및 전기세와 같은 공공서비스 요금을 납부할 때 비트코인을 사용할 수 있도록 하였다. 추크주는 인구 3만 명 가량의 소도시로 주 정부 스스로가 '크립토벨리(Crypto Valley)'라는 브랜드를 자처할 정도로 핀테크와 블록체인 같은 금융기술에 대한 관심이 높다.

이러한 추크주의 파격적인 행보에 귀추가 주목되고 있는 것은 비트코인과 그 기술인 블록체인이 널리 전파되려면 소도시에서 사용하는 것이 문제가 없다는 것이 문제가 없다는 것을 먼저 증명해보여야 하기 때문이다. 추크주에서 비트코인을 통한 공공서비스 요금 납부가 성공적으로 이루어진다면 비슷한 방식의, 더 큰 규모로의 활용이 가능해질 것이다[16]. 추크주가 적극적으로 비트코인 및 블록체인 기술을 받아들이려고 노력하는 이유는 전자화폐 기술의 '헤게모니(Hegemony)'를 확보하기 위해서이다.

공공서비스 요금을 비트코인으로 받을 수 있었던 스위스는 극도의 지방자치제도와 소규모이며 금융중심이었던 추크주의 특성이 잘 결합되어 나타난 정책으로 우리나라에 적용하기에는 어려운 실정으로, 다음과 같은 정책적 변화가 필요하다.

첫째, 앞서 언급한 R3 컨소시엄에 최초로 가입한 하나은행의 경우처럼 R3 컨소시엄에 가입하기 위해선 가입 의사만 나타내는 것이 아니라 안정적이고 실효성 있는 기술에 대한 관심 및 투자가 있어야만 가입 자격이 부여된다. 국내의 은행은 컨소시엄 가입 조건은 충분하나 블록체인에 대해 관망적 태도를 보인고 있다. 이를 해결하기 위한 대책으로 블록체인을 연구 및 개발하는 기업에 대해 정부에서 세제해택을 마련하는 것이다.

둘째, 정부에서 시행하려는 '동전 없는 사회'를 비트코인을 이용하여 구현하는 것이다. 한국은행에서는 동전 없는 사회를 만들기 위한 방법으로 지폐를 내고 거스름돈을 주는 대신 거스름돈 카드에 거스름돈을 적립하는 식의 방법을 구상중이다. 하지만, 이 경우 일반적인 소비자들은 비트코인이 생소하여 현금으로 받기를 원할 수 있기 때문에 거스름돈을 비트코인으로 받을 시 추가 적립을 해주거나 응모권을 이용하여 일정량의 비트코인 당첨금을 지급하는 방법도 가능할 것이다. 또한 부가적으로 소액의 거스름돈은 사용자의 의사에 따라 기부(Donation)를 하기도 용이하다[12].

3.2 관리적 제안

3.1.3에서 제안한 거스름돈을 비트코인으로 적립 받기 위해 사용자마다 지갑(Wallet)을 만들어야할 것이다. 이 지갑에 부여된 주소에 거스름돈을 비트코인으

로 전송시켜주면 된다. 비트코인 주소는 길기 때문에 사용자가 외우고 다니기는 어려우며 입력 시 큰 불편이 따른다. 그래서 카드 형태의 지갑(Wallet)을 이용하거나 많은 사람들이 휴대하는 스마트폰에 QR코드를 활용하면 좋다[18].

(그림 4) 카드형태와 QR코드 형태의
비트코인 지갑주소[18]

하지만 여기에는 기술적으로 해결해야할 것이 남아있다. 비트코인은 지갑에서 지갑으로 비트코인이 이동하는 거래(Transaction)를 발생시키기 위해 수수료가 필요하다. 이 수수료는 없이 보낼 수도 있고 아주 큰 금액을 보낼 수도 있다. 이렇게 수수료를 차등적으로 적용하는 이유는 많은 수수료를 지불한 거래에 우선순위를 주기 위함이며, 수수료가 높은 거래일수록 먼저 전송된다.

국내 거래소들의 경우 주로 사용하는 수수료는 0.0002 BTC로 한화로는 약 100원 정도의 가치를 가진다. 거스름돈을 받을 때마다 수수료로 100원씩을 지불해야한다면 동전을 거슬러 받는 경우는 적게는 10원에서 많게는 990원 일 것인데 100원 미만의 경우는 배보다 배꼽이 더 큰 상황이 되며, 990원이 수수료라고 하더라도 100원은 무시할 수 없는 수치이다. 이를 막기 위해 블록체인에는 '팬아웃(Fan-out)'이라는 다수의 거래를 하나의 거래로 묶는 방법을 제공한다.

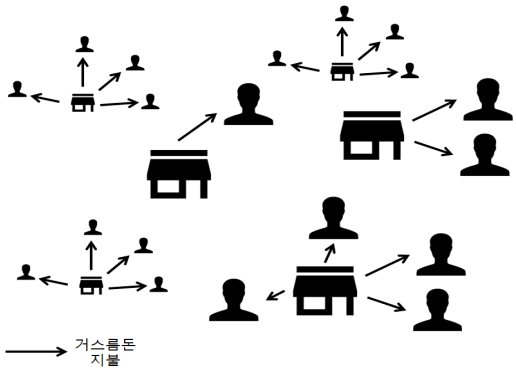
그러나 이 팬아웃 역시 어느 정도 수수료 문제는 해결할 수 있으나 묶어서 보낼 거래들이 모이는 동안 전송(Transaction)이 이루어지지 않고 대기해야한다는 문제점이 있다. 이를 해결하기 위해 점포들을 구획으로 나누어 각각의 구획마다 노드가 되는 주소를 두고 이 주소에서 사용자들에게 거스름돈을 팬아웃 해주는 방식이 필요하다.

3.2.1 팬아웃

팬아웃을 이용한 전송은 비트코인 네트워크인 블록체인에서 제공해주는 기술로 이미 채굴 풀(Mining Pool)과 거래소(stock market)에서 사용 중인 기술이다. (그림 5)처럼 전송이 빈번하게 이루어지는 거래소나, 일정시간마다 대규모의 사용자들에게 비트코인을 전송해야하는 채굴 풀 같은 경우 적게는 2개에서 많게는 수천 개의 거래를 하나로 묶는다.

(그림 5) 거래소에서 비트코인 전송시
사용한 팬아웃[19]

거스름돈을 비트코인으로 지불하는 것으로 돌아와보면, 우선 거스름돈을 지불할 상점과 이를 받을 고객이 존재할 것이다. 가장 단순한 방식으로 거스름돈 지불시마다 1개의 거래를 발생시키면 다음과 같은 그림처럼 될 것이다.



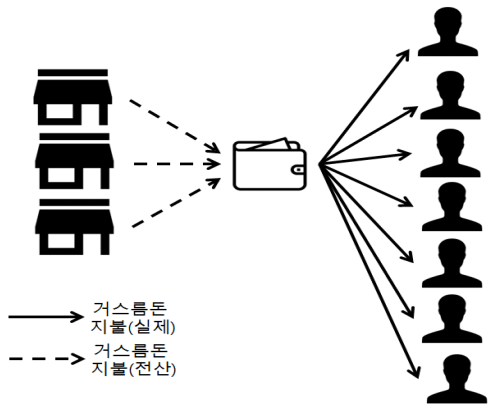
(그림 6) 일반적 지불거래 도식

(그림 6)은 매 거스름돈 지불마다 거래를 발생시키고 있다. 이것은 3.2에서 언급했던 것처럼 매 거래마다 수수료가 발생하여 거스름돈을 효율적으로 지불하기 어렵다는 문제점을 가지고 있다. 이것을 해결하기 위

해 상점에서 발생하는 거스름돈 지불을 묶어 팬아웃 시켜주는 것이 가능하지만 손님이 적게 방문하는 상점의 경우 일정 수 이상의 거스름돈 지불을 쌓아야 하기 때문에, 거래를 발생하기까지 오랜 시간이 걸릴 수 있다. 이것은 고스란히 소비자가 거스름돈을 늦게 돌려받는 피해로 이어진다. 이것 역시 막기 위해 팬아웃을 하되, (그림 6)처럼 상점별로 수행하는 것이 아닌 구획으로 나누어 해결할 수 있다.

3.2.2 지불거래 구획화

구획화를 위해서는 상점과 손님 사이에 같은 구획의 상점들이 공유하는 지갑이 하나 필요하다. 이 공유지갑은 각각의 상점에서 관리하거나 키를 가지고 있는 것이 아니라, 공유 지갑의 관리 및 키 보유는 컨트롤타워 역할을 하는 단체를 신설 혹은 지정하여 그곳에서 관리할 수 있도록 한다. 상점들은 실제 '거래'가 아닌 전산 상으로만 공유 지갑에 거스름돈 지불을 요청하고, 일정한 시간이 지나거나 혹은 지불 횟수가 쌓일 경우 실제 거래를 발생시킨다.



(그림 7) 구획화 지불거래 도식

3.3 기술적 제안

(그림 7)은 두 부분으로 나눌 수 있다. 상점에서 공유지갑으로 거스름돈을 전송하는 과정과 공유지갑으로부터 고객으로 거스름돈을 전송하는 과정이다. 후자는 비트코인의 블록체인을 통해 일어나는 거래이기 때문에 그 안전성은 검증이 되었다고 볼 수 있다[20]. 하지만 전자의 경우 전산상으로 처리를 해야 한다. 여기에는 여러 가지 보안 위험이 존재하며 이를 해결하기 위해 기존의 암호 및 통신 보안 기술로부터 해결책을 살펴보면 다음과 같다.

3.3.1 전자서명(Electronic signature)

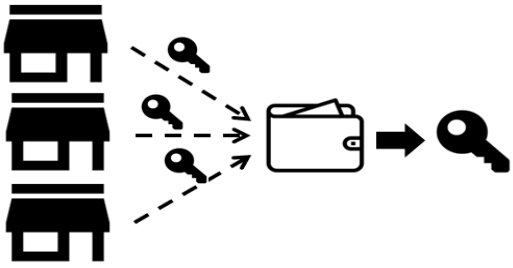
상점에서 공유지갑으로 전송할 때 누군가 전송되는 패킷을 가로채어 재연공격(replay attack)을 시도하거나 상점 주인이 거스름돈을 보내고 나서 자신이 한 행위가 아니라고 부인(repudiation)할 수 있다. PKI에서는 재연공격 및 부인을 방지하기 위해 전자서명을 사용한다. 이를 상점과 공유지갑 사이에도 적용하여 상점에서 지갑으로 보내진 데이터가 위변조 되지 않았다는 것을 증명할 수 있다.

3.3.2 멀티시그니처(Multisignature)

3.3.1에서 상점에서 공유지갑으로 보내지는 데이터의 유효성 검사는 전자서명을 통해 해결할 수 있다. 남아있는 한 가지 중요한 문제는 공유지갑의 개인키(private key)를 어디에 보관해야하는지에 관한 것이다. 공유지갑을 보관하고 있는 것도 어떠한 형태의 컴퓨터일 것이다. 이 컴퓨터로부터 개인키를 이용한 거래(transaction)가 발생해야하는 것은 분명하지만 이 개인키를 이 컴퓨터에 저장하는 것은 바람직하지 않다. 대부분 최소한의 안전을 위해 개인키를 암호화하여 보관하지만 이 개인키를 암호화한 '또 다른 키' 역시 보관해야할 곳이 필요하다. 이 또 다른 키를 보관하는 서버를 두는 방법도 있지만 이는 서버 해킹을 통해 여러 개의 공유지갑이 해킹당하는 대형 사고를 초래할 수 있다.

키 보관의 위험성을 피하기 위해 샤미르의 비밀 공유 방법(Shamir's secret sharing scheme)을 구현한 멀티시그니처를 이용한 방법으로 이미 비트코인 블록체인 보안 업체인 'Bitgo'에 의해 구현되어 서비스 중에 있다. 이외에도 파이썬으로 구현된 오픈소스 지갑인 아머리(Armory) 역시 멀티시그니처를 지원하고 있다. 멀티시그니처는 지갑에 사용되는 개인키를 하나만 사용하는 것이 아니라 샤미르의 비밀 공유 방법을 통해 여러 개의 개인키를 사용해야 거래의 발생이 가능하다[21].

멀티시그니처를 공유지갑에 적용하기 위해 몇 개의 개인키를 사용해야할지 정해야한다. 대략 전체 개인키의 3분의 2 가량을 사용하는 것이 일반적이다. 만약 10개의 상점이 하나의 지갑을 공유한다면 7개의 상점으로부터 개인키 전송이 필요하다. 이렇게 함으로써 키 보관의 위험성을 회피함과 동시에 상점의 전산망에 문제가 생겼을 경우에도 다른 상점들은 영향을 받지 않는 부수효과를 얻을 수 있다.

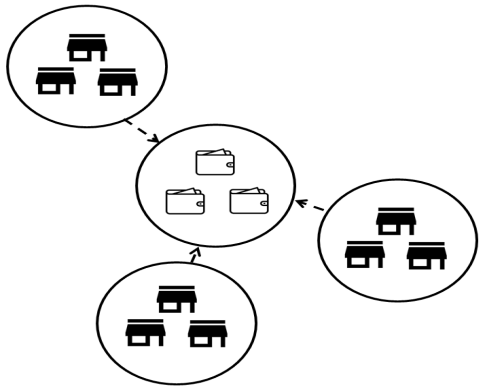


(그림 8) 상점으로 받은 개인키를 이용해 거래 발생이 가능한 실제 개인키 생성

상점들이 나누어 가지는 각각의 개인키는 일반적인 개인키 저장과 마찬가지로 상점 내부의 전산망에 암호화하여 저장하며 거래 발생이 필요할 경우 암호화하여 공유지갑으로 전달한다. 때문에 공유지갑을 해킹하기 위해서는 전체 개인키의 3분의 2를 해킹해야하기 때문에 위험성을 낮출 수 있다.

3.3.3 공유지갑의 공유

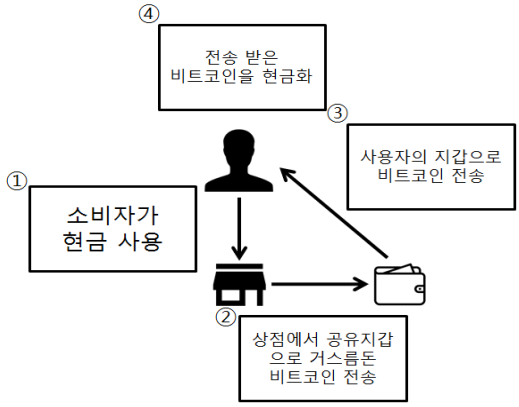
3.3.2에서 멀티시그니처 지갑을 사용해 얻을 수 있는 부수효과가 한 상점이 전산망에 장애가 생겼을 경우에도 지갑을 공유하는 다른 상점들은 영향을 받지 않을 수 있다고 했다. 하지만 지갑이 존재하는 컴퓨터에 문제가 생긴다면 문제가 발생한 지갑을 공유하는 상점들은 거스름돈을 지급하지 못하는 문제가 발생한다. 이런 위험이 존재하는 이유는 하나의 지갑에 모든 것이 집중되기 때문이다. 전형적인 서버-클라이언트 모델에서 발생하는 문제는 고스란히 안고 있는 것이다. 이를 막기 위해 공유지갑의 공유를 통해 하나의 지갑에 모든 것이 집중되지 않고, 문제가 발생하더라도 원활하게 지갑에서 거래가 발생할 수 있는 대체 작동 시스템(Failover)의 기술적 방법이 필요하다.



(그림 9) 공유지갑의 공유

(그림 9)는 공유지갑의 공유에 대한 그림으로 원 안에 있는 상점들은 하나의 공유지갑을 공유하는 구획 안에 있는 상점들이다. 총 3개의 구획이 3개의 지갑을 공유하고 있다. 3개의 지갑은 3개의 지갑 서버가 모두 가지고 있으며 하나의 지갑 서버가 장애가 생길 경우 다른 두 개의 지갑 서버를 이용해 거스름돈을 전송한다. 이때 반드시 지갑 서버들 사이에는 거스름돈의 리스트를 공유해야하며 그 리스트는 3.3.1의 전자서명을 이용하여 암호화하여 공유해야한다.

최종적으로 본 논문에서 제안한 내용을 사용자 입장에서 플로차트를 그려보면 (그림 10)과 같다.



(그림 10) 사용자가 비트코인을 받기까지의 과정

4. 비교 분석

블록체인과 공유지갑을 이용해 한국은행에서 2020년까지 추진 중인 '동전 없는 사회'를 뒷받침 할 수 있는 비트코인의 활성화 방안을 제안하였다. 한국은행의 동전 없는 사회를 구현하기 위해 거스름돈을 '충전식 선불카드'에 적립해 주는 방식을 제시하고 있다.

이러한 충전식 선불카드와 3.2에서 제안한 블록체인과 공유지갑을 이용한 거스름돈 지불 방식과 비교하면 <표 3>과 같다[22].

<표 3> 충전식 선불카드 방식과의 비교 [22]

구분	충전식 선불카드	제안된 방식
관리적 측면	중앙 집중적 지급결제 수단으로 인한 대규모 서버 운영 및 관리적 비용이 큼	소규모인 공유지갑으로 전산화의 운영 및 관리가 쉬움
기술적 측면	기존 지급결제 기술 적용	안정적 기술로 평가받는 블록체인 적용
위험도 측면	중앙 집중화로 인한 보안위협 항시 존재	전산망 분산으로 보안위협의 최소화
인프라 측면	기존에 있는 지급결제 인프라를 이용하므로 인프라 구축에 대한 비용부담이 적음	각 상점들 간 공유지갑을 연결하는 전산망에 대한 초기 인프라 구축 비용 발생
대중적 측면	익숙한 충전식 카드는 대중들에게 큰 거부감 없이 사용이 가능	생소한 전자화폐에 대한 거부감 존재

충전식 선불카드의 경우 인프라 측면에서 기존의 지급결제 방식을 사용하게 되므로 비용부담이 적으나 관리적 측면에서 중앙 집중적 지급결제 수단으로 서버 운용 및 관리 비용과 보안취약성에 노출되어 공격타킷이 될 가능성이 높다.

블록체인을 이용한 방식의 경우 전산망 구축에 대한 초기 인프라 비용이 발생하지만 소규모 전산화로 인한 운영 및 관리의 편리함과 더불어 전산망 분산으로 인한 보안위협을 최소화 할 수 있다. 또한 안정적 기술로 평가되어 세계 각국에서 사용하고 있는 블록체인의 적용으로 안정성을 확보할 수 있지만, 생소한 전자화폐에 대한 대중적 거부감이 있을 수 있기 때문에 인식변화에 대한 적극적인 노력이 필요하다.

5. 결 론

비트코인과 운용적 네트워크인 블록체인 짧은 기간 동안 획기적인 기술로 인정받으면서 점진적으로 그 영역을 넓혀가고 있지만, 아직은 대중적으로 사용하기에는 생소한 기술이다. 이러한 비트코인 기술에 대한 대중화를 위해 정책적, 관리적, 기술적 측면에 대하여 제안을 하였고, 한국은행에서 향후 제시하려고 하는 거스름돈에 대한 충전식 선불카드 적립 방안과의 비교를 통해 그 안정성과 실효성을 살펴보았다.

비트코인의 활성화를 위해 정책적 측면에서 R3 컨소시엄 가입을 조건으로 세제혜택과 더불어 사용자에게 적립 혜택 등을 적용하는 방안을 제시하였고, 관리적 측면에서 구획화를 통해 실제 '거래'가 아닌 전산상으로만 공유 지갑에 거스름돈 지불을 요청하고, 일정한 시간이 지나거나 혹은 지불 횟수가 쌓일 경우 실제 거래를 발생하는 방식이다. 기술적 측면에서는 공유지갑으로 전송할 때 누군가 전송되는 패킷을 가로채어 재연공격(replay attack)을 시도하거나 상점 주인이 거스름돈을 보내고 나서 자신이 한 행위가 아니라고 부인(repudiation)할 수 있는 방법으로 전자서명, 비밀공유 방법(Shamir's secret sharing scheme)을 구현한 멀티시그니처 방식 그리고 공유지갑의 공유를 통해 하나의 지갑에 모든 것이 집중되지 않고, 문제가 발생하더라도 원활하게 지갑에서 거래가 발생할 수 있는 대체 작동 시스템(Failover)의 기술의 적용이 필요하다.

이와 같이 본 연구에서 제안한 거스름돈 지급결제 방식은 충전식 선불카드 적립방식에 비해 전산망 구축에 대한 초기 인프라 비용이 발생하지만 소규모 전산화로 인한 운영 및 관리의 편리함과 더불어 전산망 분산으로 인한 보안위협을 최소화 할 수 있다. 또한 안정적 기술로 평가되어 세계 각국에서 사용하고 있는 블

록체인의 적용으로 안정성을 확보할 수 있지만, 생소한 전자화폐에 대한 대중적 거부감이 있을 수 있기 때문에 인식변화에 대한 적극적인 노력이 필요하다.

참고문헌

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electoronic Cash System,, https://bitcoin.org/bitcoin.pdf, 2008.

[2] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[3] C. Fromknecht, A Decentralized Public Key, Cryptology ePrint Archive, IACR, 2014.

[4] http://crazia.tistory.com/entry/PKI-PKI

[5] 강정희, "PKI(Public Key Infrastructure)", 영남대학교 @Xpert

[6] 신동희 외, "국내 소비자들의 비트코인 사용의도에 영향을 미치는 요인 연구", 한국콘텐츠학회논문지, pp.27, 2016.

[7] 신용도, "IC카드형 전자화폐 이용활성화를 위한 사용자 수용모형분석연구," IITA, pp.1-142, 2004.

[8] 정승영, "가상화폐(Virtual Currency)의 세법상 분류와 과세. 조세학술논집, pp.85-140, 2015.

[9] 김현동, "법인세법상 무형자산에 관한 규정의 문제점과 개선방안에 관한 연구", 한국세법학회, 조세법연구 제17-2집, 2011.

[10] http://www.bloter.net/archives/181894

[11] 김홍기, "최근 디지털 가상화폐 거래의 법적 쟁점과 운용방안 - 비트코인 거래를 위주로", 증권법연구, pp.377-431, 2014

[12] http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=003&aid=0007187961&viewType=pc

[13] Berkeley Univ, "BlockChain Technology:Beyond Bitcoin", http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[14] http://goodcounsel.blog.me/60207475164

[15] https://blockchain.info/ko/charts/market-price

[16] "Steam Bit Shop"https://steambitshop.com/

[17] https://coinone.co.kr/coinclip/posts/31/?page=1

[18] https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses

[19] https://blockchain.info/ko/tx/26ae4df3b837a6d22c8d77f361d6b9f2e2f98a173fa7f6b8690bbebb2f7021c1

[20] https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

[21] https://en.bitcoin.it/wiki/Multisignature

[22] http://www.yonhapnews.co.kr/bulletin/2016/04/25/0200000000AKR20160425106200002.HTML

[저 자 소 개]

이 준 형 (Jun Hyung Lee)

2016년 현재
경기대학교 융합보안학과 재학

email : lleellee0@kgu.ac.kr

김 우 철 (Woo Cheol Kim)

2016년 현재
경기대학교 융합보안학과 재학

email : kimwoo003@naver.com

이 성 훈 (Seong Hun Lee)

2016년 현재
경기대학교 융합보안학과 재학

email : leeseonghun313@nate.com

김 민 수 (Minsu Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : fortcom@hanmail.net

이 도 은 (Do Eun Lee)

2016년 현재
경기대학교 융합보안학과 재학

email : rayyo5720@gmail.com