모바일 환경에서 M-비트코인 채굴 및 거래 서비스에 관한 연구 - 비트코인과 비교하여 -

김웅보*, 박석천**, 박동민***
*가천대학교 일반대학원 모바일소프트웨어학과
**가천대학교 컴퓨터공학과 정교수(교신저자)
*** 모코엠시스 ICT사업부 개발팀 대리
e-mail:cryingbo_@naver.com

A Study on Mobile-Bitcoin for Mining And Trading Service in Mobile Environment - Comparison of Bitcoin -

Woong-Bo Kim*, Seok-Cheon Park**, Dong-Min Park***
*Dept of Mobile Software, Gachon Uiniversity
**Dept. of Computer Engineering, Gachon University(Corresponding Author)
*** Dept. of ICT Div. Development Team, MOCOMSYS

요 약

가상화폐는 법정통화가 금융위기나 통화정책 등에 심각하게 영향을 받아 발생하는 문제점으로 시작하여 국가나 신용기관에 독립적인 전자지급결제시스템을 갖추는 것을 목표로 등장하게 되었다. 대표적인 가상화폐인 비트코인은 국제적인 유통수단으로 활용되고 있으며, 일부 국가에서는 납세 및 기타 법률과 같은 규제를 통해 관리되고 있을 정도로 영향력이 있는 가상화폐이다. 본 연구에서는 비트코인의 개념 및 현 상황에 대해서 분석한 후, 모바일 환경에서 채굴되는 M-Bitcoin을 제안하였다. 그리고 M-Bitcoin이 암호통화로써의 가치를 가질 수 있도록 신뢰성 확보를 위한 기술을 적용하고, 차후 현실에서 서비스되는 과정에 대해 연구하였다.

1. 서론

가상화폐(Virtual Currency)란 '특정한 가상사회에서 통용되는 디지털 민간화폐'를 의미한다. 가상화폐는 강제적 통용성이 없다는 점에서 '민간 화폐'이자, 실물이 존재하지 않는다는 점에서 '디지털 화폐'의 특성을 가지며, 민간 화폐는 공식적인 화폐로 인정되지는 않지만 현실 세계에서 유통 및 지불 수단으로서 기능한다는 점에서 넓은 의미의 화폐에 포함된다[1].

급격한 IT 기술의 발전으로 민간차원에 발행되는 가상화폐들이 출현하고 있는데, 전자금융거래법에서 인정된 국내 공식 전자화폐인 K-Cash와 별도로 온라인 사이버 머니 등 다양한 민간 가상화폐가 통용되고 있다. 최근에는 발행 기관이 존재하지 않고 익명성이 보장되는 글로벌 네트워크 화폐인 비트코인이 출현하며 이슈가 되고 있는데, 그 유통규모가 점차 확대되면서 기대와 우려가 증폭되고 있다.

따라서 본 논문에서는 가상화폐 중 가장 활발히 통용되는 비트코인에 대해 분석한 후 모바일 환경에서 적용할 수 있는 M-Bitcoin을 정의하고, 이를 채굴하고 거래할 수 있는 서비스에 관해 연구하였다.

2. 관련연구

2.1 비트코인의 개념

비트코인 시스템은 2008년 나카모토 사토시(Satoshi Nakamoto)라는 프로그래머에 의해 소개되었는데, 그는 비트코인은 신용(trust)이 아닌 수학적 증거(cryptographic proof)를 기반으로 하는 지불시스템이라고 정의하였다. 비트코인이 등장하게 된 가장 큰 요인은, 금융위기에 대비하여 은행이나 국가 그리고 신용기관과는 독립적으로 기능하는 금전지급시스템을 구축하고자 하는데 있었다. 즉, 중앙정부의 강제력에 구속되지 않는 전자지급결제시스템을 갖추는데 그 등장배경이 있다[2].

비트코인은 금이나 은과 달리 귀금속이나 산업용도로서는 사용되지 못하고 오로지 가상공간에서만 존재하는 가상화폐의 일종으로 볼 수 있다. 세계 각 국에서 통용되는 명목화폐(fiat money)는 비록 내재적 가치가 없음에도 중앙정부의 권위에 근거하여 강제 통용력을 갖는 이른바 법정통화(legal tender)에 해당하는데, 비트코인을 이와 동일하게 보아야 하는지 또는 어떻게 구별해야 할지가 중요한 문제가 된다.

게임 머니나 마일리지와 같은 기존의 가상화폐는 거래실적에 따라 얻게 되거나 또는 법정화폐를 이용하여 구입

할 수 있는데, 해당 사이트 내에서 물품이나 서비스를 구입하기 위해 사용될 뿐, 실물 화폐로 환전할 수는 없다. 또한 기존의 가상화폐는 해당 기업이 관리를 해오면서 주로 마케팅의 수단으로 활용하고 있다. 즉, 기존의 가상화폐는 법정 화폐제도를 극복하거나 위협하기 위해 등장한 것이 아니고, 대부분이 관련 법령의 범위 내에서 인정되고 있다. 반면, 비트코인은 오프라인에서도 그 사용이 가능할 뿐만 아니라 특정한 공간 외에서도 사용이 가능하기 때문에 구별될 수 있다[3].

2.2 비트코인의 취득

비트코인은 2,100만 개의 한정된 양이 존재하는 자원으로 이를 취득하는 방법은 3가지이다.

첫 번째는 비트코인을 채굴(mining)하는 것이고, 두 번째는 채굴한 비트코인을 법정화폐로 구매하는 것이며, 세 번째는 물건을 판매하면서 그 대금으로 비트코인을 얻는 방법이다.

비트코인의 채굴(mining)이란 컴퓨터 네트워크를 활용한 채굴 시스템을 통해 클라이언트(miner)의 PC자원을 사용하여 고도의 수학적 암호를 푸는 것을 의미한다. 이후 클라이언트는 암호 계산을 완료하면 일정량의 비트코인을 획득하게 되고, 이를 화폐로 사용하는 절차를 갖는다.

2.3 비트코인의 채굴

채굴은 단순히 새로운 비트코인을 공급하는 작업이 아니라, 블록체인이라는 공유된 거래기록을 해커나 사기꾼으로부터 안전하게 보호하는 역할을 한다.

비트코인 거래가 발생하면 거래는 비트코인 네트워크에 참여하는 노드에게 알려진다. 이렇게 알려진 거래를 기록하고 공식화하는 과정이 비트코인 채굴(mining)이다. 이 과정은 블록 단위로 일어난다. 블록(block)은 비트코인 거래를 약 10분 단위로 모은 것이며, 블록체인(block chain)은 현재까지의 블록이 모두 이어진 것으로 현재까지 일어난 모든 비트코인 거래가 시간 순으로 기록된 장부이다. 새로운 블록은 규칙에 따라 채굴자(mining node)들이 처리를 하게 되며 가장 먼저 처리를 끝낸 채굴자가 처리의 증거(proof of work)와 함께 “이것이 원본이다”라고 이웃 채굴자에게 알리고 이를 채굴자들이 확인하고 받아들이는 과정을 거치게 된다. 이렇게 받아들여진 블록은 기존의 블록체인을 이어가는 것이다. 이렇게 블록 및 블록체인을 공식화하는 과정이 바로 채굴이다[4].

2.4 비트코인의 거래 추이

2009년에 처음 발행되기 시작한 비트코인은 높은 변동성을 가진 화폐이다. 국내의 경우 비트코인 거래소(Korbit)의 원화 거래가격은 2013년 11월에 155만원까지 급등하였다가 현재 32.6만원으로 하락하였지만 점차 가격이 안정화되고 있으며, 거래규모도 점차 증가하고 있는 추세이다. (그림 1)은 비트코인 등장 이후의 거래가 및 거래량 추이를 나타내고 있다.

(그림 1) 비트코인 거래가 및 거래량 추이[5]

3. M-Bitcoin

3.1 연구배경

가상화폐는 비즈니스 모델의 발전, 스마트 소비 트렌드 확산에 따라 유형 간 융합이 가속화되며 꾸준히 진화할 것으로 전망된다. 특히 비트코인은 2,100만개라는 한정된 자원이라는 특징으로 인해 전문가들은 금융상품으로 진화를 예상 할뿐만 아니라, 지역에 상관없는 특징으로 인해 세계적으로 활발히 거래되는 대표적인 가상화폐이다. 앞으로도 다양한 방법을 통해 가상화폐가 등장하고 통용될 것이라 예상된다.

따라서 모바일 기기의 자원을 활용하여 채굴된 가상화폐인 M-Bitcoin을 정의하고, 신뢰성 확보방안 및 서비스 구조에 대해서 설명할 것이다.

3.2 M-Bitcoin 정의 및 신뢰성 확보방안

M-Bitcoin이란 Mobile-Bitcoin의 약자로 모바일 기기의 자원을 활용하여 채굴된 가상화폐를 의미한다. 가상화폐는 실물이 존재하지 않고 중앙정부의 권위에 근거하지 않는 민간화폐이기 때문에, 현실에서 쓰이기 위해서는 신뢰성이 있어야한다. 따라서 P2P간 신뢰성을 확보한 암호통화(cryptocurrency)로서의 가치를 갖기 위해 해시, 공개키-암호화 및 전자서명을 적용하였다.

3.2.1 해시(Hash)

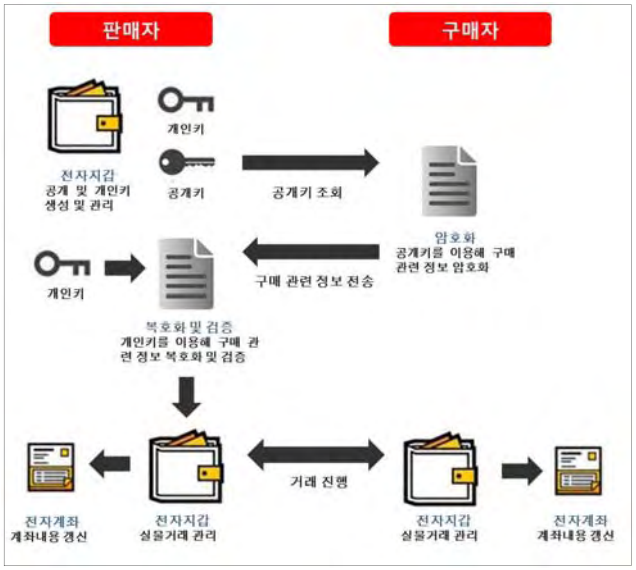
해시는 단순하게는 원본의 고정된 길이의 요약본이라고 할 수 있다. 컴퓨터 분야에서 다양한 용도로 사용되는데, 일반적으로 해시는 모든 경우의 수를 비교하지 않는 이상 결과 값을 통해 원본을 찾는 것이 불가능하다. 따라서 M-Bitcoin에서는 Secure Hash Algorithm을 적용해 거래 시 발생하는 데이터 및 메시지 변조를 막아 무결성을 확보하는 역할을 한다.

3.2.2 공개키 암호화(Public Key Encryption)

M-Bitcoin의 거래를 위해서 공개키 암호화 방식을 적용하였다. 공개키 암호화 방식은 대칭키 암호화 방식에 비해 처리속도가 느리지만, 키 배송문제를 해결하여 보안성

이 뛰어난 장점을 가지고 있다.

거래의 핵심은 개인별 전자계좌에 부여된 M-Bitcoin Address에 해당되는 값을 변경하는 것으로, 전자지갑 어플리케이션은 공개키와 개인키를 생성하고 관리한다. 아래 (그림 2)는 판매자와 구매자 사이의 비트코인 거래 시나리오를 나타내고 있다.



(그림 2) 공개키 암호화 방식을 이용한 비트코인 거래 시나리오

판매자의 전자지갑은 공개키와 개인키를 가지고 있다. 구매자는 판매자의 공개키를 조회하고, 이 키를 이용해 구매에 필요로 정보들을 암호화하여 판매자에게 전송한다. 판매자는 암호화된 정보를 자신의 개인키를 통해 복호화하고, 이상이 없다면 전자지갑은 해당 정보를 사용하여 구매와 판매에 관한 거래를 진행하게 된다.

3.2.3 전자서명(Digital Signature)

M-Bitcoin은 P2P기반의 분산형(decentralized) 네트워크로 구성되기 때문에 해킹에는 안전하지만 구매자와 판매자간의 거래내역을 다른 피어(Peer)들에게 알려야하는 단점이 있다. 따라서 M-Bitcoin에서는 전자서명을 통해 거래내역을 다른 클라이언트에게 알리고, 부인방지 역할을 한다.

M-Bitcoin의 거래가 발생하면 판매자는 구매자의 M-Bitcoin Address를 명시하여 자신의 개인키를 사용해 전자서명하고 구매자 및 Peer들은 판매자의 공개키를 통해 이를 해석하여 거래결과를 업데이트하게 된다.

3.3 M-Bitcoin 획득 및 거래절차

M-Bitcoin의 채굴을 위해서는 M-Bitcoin을 저장하기 위한 전자계좌를 등록해야한다. 전자계좌는 자신의 비트코인을 저장하고 전자지갑과 연동되어 거래를 위해 사용된다.

전자계좌를 등록하면 M-Bitcoin을 획득할 수 있는 권한이 생기며, 이를 위한 방법은 2가지가 있다.

첫 번째는 자신의 모바일 기기의 자원을 통한 획득이다. 전자계좌와 연동되는 전자지갑 어플리케이션은 채굴의 기능을 포함하고 있다. 모바일 기기는 고도의 수학적인 암호를 백 그라운드에서 작업하며 완료하는 시점에 일정량의 M-Bitcoin을 획득할 수 있다. 개인은 해당 어플리케이션을 통해 모바일 기기의 자원 할당량/비율을 설정할 수 있으며, 많은 자원을 할당한 기기는 더 빠르게 비트코인을 획득할 수 있다. 두 번째는 M-Bitcoin 거래소를 통한 구매로 타인의 기기를 통해 생성된 비트코인을 공식 거래소를 통해 거래하는 방법이다.

두 획득경로를 통해 생성된 M-Bitcoin은 전자지갑에 저장되며 사용자는 QR코드 또는 전자지갑 내에서 지원하는 결제 방식을 통해 거래한다.

아래의 (그림 3)는 M-Bitcoin 획득 및 거래 절차를 나타내고 있다.

(그림 3) M-Bitcoin 획득 및 사용절차

4. 결론

비트코인과 같은 가상화폐는 법정통화가 금융위기나 통화정책 등에 심각하게 영향을 받아 발생하는 문제점으로 시작하여 국가나 신용기관에 독립적인 전자지급결제시스템을 갖추는 것을 목표로 등장하게 되었다. 현재 비트코인은 국제적인 유통수단으로 활용되고 있으며, 일부 국가에서는 납세 및 기타 법률과 같은 규제를 통해 관리되고 있을 정도로 영향력이 있는 가상화폐이다.

따라서 본 연구에서는 비트코인이 PC의 자원을 활용하여 생산되는 것에 착안하여 모바일 환경에서 채굴되고 활용되는 가상화폐인 M-Bitcoin에 관해 연구하였다. 연구를 통해 M-Bitcoin이 암호통화로서의 가치를 갖기 위해

공개키 암호화방식, 해시 및 전자서명을 적용하였고, 획득 및 거래절차에 대해서 규정하였다.

M-Bitcoin이 활용되기 위해서는 IT에 한정된 연구뿐 아니라 정책에 관련된 부분들이 병행되어야 할 것이다. 특히 모바일 기기는 현재의 데스크 탑에 비해 성능이 떨어지므로 채굴을 위한 수학적 암호레벨 및 모바일기기에 사용되는 H/W의 성능향상에 관한 연구들이 필요할 것으로 판단한다.

사사의 글

본 논문은 미래창조과학부의 2015년 고용계약형 SW석사과정 지원사업(H0116-15-1003)을 지원받아 수행한 결과입니다.

Acknowledgement

This research was supported by SW Master's course of hiring contract Program grant(H0116-15-1003) funded by the Ministry of Science, ICT and Future Planning.

참고문헌

[1] 현대경제연구원. "국내 가상화폐의 유형별 현황 및 향후 전망", VIP리포트 563호, 2014

[2] Satoshi Nakamoto. "Bitcoin : A Peer-to-Peer Electronic Cash System," 2008

[3] 남기연. "Bitcoin의 법적 가치에 관한 연구", 법학논총 제38권, 2014

[4] 노상규. "비트코인 채굴과 선순환 구조",
http://organicmedialab.com

[5] Korbit 차트자료
https://www.korbit.co.kr