디지털산업정보학회 논문지 제13권 제3호-2017년 9월
http://dx.doi.org/10.17662/ksdim.2017.13.3.001

비트코인에 대한 안정성 확보를 위한 문제점 분석

최 희 식*·조 양 현**

Problem Analysis to Secure Stability of Bitcoin

Choi Heesik · Cho Yanghyun

〈Abstract〉

Recently, Bitcoin which is digital currency and cryptocurrency is getting worldwide attention since Bitcoin has an ability to replace legal tender unlike other existing cyber currency. Especially, most Bitcoin trading is done between two traders such as P2P method and it does not require a third-party to make sure reliability and it records every transaction details, so it is more transparent then traditional financial trade, so the number of users is increasing. However, Bitcoin, which has been recognized for transparency, confidentiality and stability among traders has recently been threatened by illegal transactions such as money laundering and the attack on the exchange. These threats to Bitcoin are becoming social problems.

At first, it seems that most of the digital currency is difficult to get hacked due to the Blockchain technology. However, threats such as digital money leaks by user account hacking and paralyzing the servers are increasing.

In this paper, it will examine the features of the Bitcoin and the threatening elements to secure marketability of digital currency such as Bitcoin and receive more interest from public in domestic. The paper will examine the problems of Blockchain technology on speculative transactions and fraudulent behavior by analyzing the problems of Bitcoin transaction. Lastly, it will propose ways to make transparent and secure digital currency transactions.

Key Words : Bitcoins, Blockchain, Ransomeware, Digital Money, Cyber Money

Ⅰ. 서론

비트코인은 2009년 1월 3일 호주의 사업가 겸 컴퓨터공학자인 크레이크 스티븐 라이트(사토시 나카모토 : 창시 당시 사용했던 가명)가 블록체인 기술을 기반으로 암호화된 가상화폐 '비트코인'을 처음 공개한 이후 세상에 선보이게 되었다. 그러나 최근 가상화폐 시장을 주도하고 있는 비트코인은 몸값을 요구하는 랜섬웨어의 지급 수단으로도 널리 알려져 있으며 그에 대한 피해 사례도 증가하고 있다. 특히,

* 경민대학교 IT경영과 외래교수
** 삼육대학교 컴퓨터학부 교수(교신저자)

비트코인은 랜섬웨어와 같은 사이버 범죄의 주목적으로 이용되고 있어서 불법거래 및 투명하지 못한 거래에 이용되고 있는 것이 사회적으로 문제가 되고 있다. 뿐만 아니라 비트코인은 디지털 네트워크상에서 무형의 가치만으로 투기가 이뤄지고 있다는 점과 실제 거래자를 확인할 수 없다는 점에서 익명성을 바탕으로 전 세계 범죄자들의 '검은돈'이 현물로 돈세탁이 되고 있다는 주장 등으로 위험에 대한 경고의 목소리도 커지고 있다. 본 논문에서는 가상화폐 비트코인과 관련된 위험한 요소를 파악하여 피해를 최소화하고 비트코인에 대한 지불수단 위협과 부정거래와 관련된 문제점들을 알아보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 비트코인에 대한 특징에 대해서 살펴보고, 3장에서는 비트코인 위협적 요소에 대해서 알아보고, 4장에서는 비트코인 거래에 대한 문제점 분석에 대한 방안 제시, 5장에서 결론으로 마무리하고자 한다.

Ⅱ. 관련연구

2.1 비트코인 정의

2009년 처음 발행된 비트코인은 암호 화폐의 일종으로 기존의 사이버 머니 와는 다르게 수량 통제가 엄격히 이루어지는 등 법정화폐를 대체한다는 이유로 주목을 받았다. 또한, 비트코인은 중앙은행의 통제로부터 자유롭고, 국가 통화의 대안으로서 환전할 필요성이 없는 것이 특징으로 사용자가 늘어나고 있다. 비트코인이 최근 주목을 받은 가장 큰 이유로는 금융기관의 복잡한 가입 절차가 없다는 점과 P2P 방식과 같은 거래자와 거래자 간의 직거래 방식으로 거래가 되는 방식으로 운영되기 때문에 수수료를 줄일 수 있다는 것이다. 비트코인은 현재 가상통화 거래의 약 90%를 차지하고 있으며 이더리움, 리플, 라이트코인, 대시 등과 같은 새로운 가상화폐가 계속해서 생성되고 있다[1].

2.2 비트코인 특징

비트코인은 현재 세계적인 글로벌 공식 화폐로 인정은 되지 않지만 새로운 경제적 수단으로 비즈니스 모델 적인 투가 가치가 있는지에 대해서는 의견이 분분하다. 가상화폐인 비트코인이 가지고 있는 특징을 살펴보자.

① 국적을 초월한 발행 및 유통 시스템으로 인터넷만 연결되어 있으면 전 세계 누구와도 직접 거래가 가능하다.

② 거래 과정에서 개인정보를 요구하지 않는 가상화폐의 등장으로 개인정보 유출에 대해 우려를 하지 않아도 된다.

③ 거래하는 과정에서 은행, 카드회사 등 금융기관과 같은 실제 거래의 중간 과정을 거칠 필요가 없고, 발행 기관이 존재하지 않고 익명성이 보장되는 글로벌 네트워크 화폐이다.

④ 소액 콘텐츠 시장의 확장과 소상인들의 판매영역 확대를 가져올 수 있다.

⑤ P2P 거래의 활성화, 블록체인 기술로 인한 거래의 투명성에 대한 효과를 기대할 수 있다.

<표 1> 블록체인 용어[2]

특징	설 명
투명성	블록체인 내 모든 내용이 참여자들로 공유되어 있음
가용성	특정 노드가 서비스 불가하더라도 수많은 노드들에 의해 블록체인이 저장되어 유지
신뢰성	다수에 의해 결정되므로 결과를 신뢰할 수 있음
무결성	블록체인에 기록된 기록을 삭제하거나 조작할 수 없음

2.3 비트코인 동작

비트코인이 거래하기 위해서는 가장 기본적인 구성으로 비트코인이 소속되는 비트코인 주소(address)가 있어야 한다. 또한, 비트코인의 경우 매 거래를 블록체인이라 불리는 공개된 장부(public ledger)에 기록하며, 이를 공개키(public key) 방식으로 암호화하여 저장함으로써 보안과 익명성을 보장하는 형태를 취하게 된다[3]. 비트코인의 거래는 은행의 계좌 이체와 비슷하지만, 은행은 계좌 하나에 있는 돈 일부가 다른 계좌 하나로 이동하는 과정인 데 반하여 비트코인 거래는 입력의 비트코인이 모두 출력으로 옮겨져야 한다.

2.3 국가별 비트코인 동향

비트코인이 등장한 이후, 각 국가에서 비트코인을 규제하는 데에는 다소 견해 차이가 있다. 2013년 8월 독일은 비트코인을 사적 통화(private money)로 규정하고 비트코인 거래에 대해서는 과세를 부여하고 있다. 그러나 미국에서는 비트코인과 같은 가상통화 이용 자체에는 특별한 제약 없이 이용할 수 있지만, 비트코인 마이닝과 같이 통화를 생성하여 교환 및 판매하는 것은 규제 대상이다.

2.3.1 한국

한국은 국가 차원에서 비트코인 및 가상화폐 거래를 장려하지 않는 반면 거래량이 전 세계 비트코인의 8%를 차지한다. 비트코인 인기에 힘입어 그 뒤를 잇는 이더리움 클래식이나 이더리움, 대쉬의 상승을 한국에서 주도했다는 말이 나올 만큼 한국에서는 비트코인과 같은 가상화폐가 활발히 거래되고 있다[4].

2.3.2 미국

미국은 비트코인에 대한 수요는 트럼프 대통령과 관련된 심각한 정치적 불안과 주식 시장 등 어려운 상황에서 비트코인이 금과 함께 헤지 자산으로 고려되어 급속하게 증가하였다. 미국의 투자자와 거래자들의 비트코인에 대한 수요가 폭발적으로 증가함에 따라 비트코인 가격의 상승 추세도 일어나고 있다[5].

2.3.3 호주

호주 정부는 호주를 세계적인 금융 기술(FinTech) 허브의 중심지로 만들기 위해 비트코인을 구매할 때 세금을 내고, 비트코인으로 물건을 살 때 한 번 더 세금을 매기는 블록체인(Blockchain)과 관련된 이중과세 대상에서 제외했다. 또한, 호주 정부는 핀테크 산업을 세계 선두 주자로 삼을 새로운 패키지 계획안을 발표했는데 그것은 2017년부터 2018년까지 비트코인과 같은 디지털 가상 통화 기업이 호주에서 사업을 더 잘할 수 있는 방침이다[4].

2.3.4 러시아

러시아 정부는 금융 서비스 내 모든 참여자의 신분을 알고 있어야 하고, 가상화폐 결제 정보에 대한 접근 권한을 반드시 확보해야 한다며 2018년까지 비트코인 합법화에 대한 강경책 마련을 추진하고 있다. 즉, 가상화폐 거래가 이뤄진 경우, 은행과 마찬가지로 구매자와 판매자, 거래 중개자에 대한 모든 정보가 투명하게 제출되어야 한다며 비트코인 거래소에 제재를 강화하고 있다[5].

2.4 블록체인

가상화폐인 비트코인은 화폐를 주고받은 공통 거래기록 내용을 블록체인에 기록함으로써 거래가 이루어진다. 블록체인을 이용하면 모든 네트워크 참여자끼리의 모든 거래가 체인처럼 공유되므로 노드가 보관되어 거래의 투명성과 동시에 음성화를 차단할 수 있다. 또한, 이중지급에 대한 공격 및 외부 해킹 방어에 매우 효과적이어서 시스템의 안정성 향상에도 기여한다.

<표 3> 블록체인 장·단점

구분	특 징
장점	- 대부분의 거래가 P2P방식 임 - 참여자가 공동으로 내역을 공유하여 금융거래보다 투명함 - 중간과정을 거치지 않음 - 공증 없이도 개인 거래가 가능
단점	- P2P서비스로 다수의 사용자와 정보 교류가 이루어지므로 속도가 느림 - 기술적 오류 발생이나 업그레이드 속도가 느림

2.4.1 주소 생성

비트코인은 거래를 위해서 집 주소나 이메일의 주소와 같은 숫자와 문자가 결합한 형식의 주소가 반드시 필요하며, 각각의 거래를 위해서는 유일한 새로운 주소가 필요하다.

2.4.2 비트코인 구매

비트코인은 상품이나 서비스에 대한 대가로 비트코인을 지불받을 수 있으며 주변 사람이나 친구로부터 살 수도 있다. 또한, 보유하고 있는 실거래 은행계좌를 가지고 환전소에서 직접 비트코인을 살 수도 있다[2].

<표 2> 블록체인 용어[6]

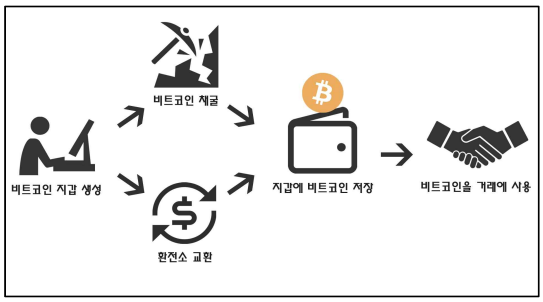
항목	내 용
블록체인	모두에게 나누어 공개된 공공원장으로 비트코인 네트워크는 이 원장을 토대로 진행되며, 확인된 모든 거래내역들이 블록체인이 포함되어 있음
개인키	블록체인에 기록되는 비트코인 지갑들 간의 가치의 이동을 위해 사용되는 비밀정보
서명	비트코인 거래가 승인된 이후에 거래가 타인에 의해 변질되지 않도록 방지 역할
채굴	새로운 비트코인이 통화 공급량에 추가

2.4.3. 지갑 생성 및 거래

비트코인 거래를 이용하기 위해서는 <그림 1>과 같이 블록체인으로 비트코인 지갑을 반드시 생성해야 한다. 비트코인 지갑은 은행에 해당하고 비트코인 주소는 계좌번호에 해당한다고 볼 수 있다. 대부분의 비트코인 지갑 생성 서비스는 공식적으로 운영되는 것은 아니고 대부분 개발자에 의해서 업로드되는 독립적인 방식으로 지갑의 정보를 잃어버리기라도 하면 사용자의 책임이 된다.

안전한 비트코인 거래를 위해서 비트코인 거래소가 있는데 비트코인을 실제 돈으로 매수하거나 비트코인을 매각해 돈으로 돌려받을 수 있는 서비스를 제공하는 업체이다. 즉, 비트코인을 손쉽고 안전하게 얻는 방법이 거래소를 통해 비트코인을 매수하는 것이다. 회원가입 절차를 거치고 이메일 및 휴대폰 인증을 거치면 지갑이 생성되고, 자유롭게 비트코인 거래 및 매수/매각을 할 수 있다. 세계적으로 가장 널리 사용되는 비트코인 거래소로는 코인베이스(Coinbase), 써클(Circle), 비트피넥스(Bitfinex), 오케이코인(OKcoin) 등이 있으며, 한국 비트코인 거래소로는 코빗(Korbit)과 코인플러그(Coinplug) 등이 많

이 이용되고 있다[7].



<그림 1> 블록체인 거래[8]

2.4.4 비트코인 송금

비트코인을 한 지갑에서 다른 지갑으로 송금하는 것도 가능하다. 이는 비트코인 간의 거래 방식으로 A 고객이 1BTC(비트코인)를 B 고객의 비트코인 지갑에 전송하여 송금이 이루어진다. 즉, 비트코인의 송금은 일반 금융거래와는 다르게 실제 돈이 사용되지 않는 비트코인 교환을 통해 송금이 이루어지는 가장 기본적인 기능이다[7].

2.4.5 비트코인 매수/매도

거래 이용자가 비트코인을 사거나 비트코인을 팔아서 돈을 받는 게 가능하다. 비트코인 매수/매도를 위해서는 비트코인 거래소를 통해서 비트코인을 돈으로 사고 팔수가 있다. 반면, 블록체인 지갑은 오직 비트코인의 보관과 비트코인 간의 송금만을 지원하게 되며, 웹사이트에서 비트코인을 돈으로 매수/매각하는 것은 불가능하다[7].

Ⅲ. 비트코인의 위험

비트코인을 이용한 결제는 직접적인 현금 거래와 마찬가지로 익명성이 높은 거래가 많다. 익명성 거래는 주로 마약류 등의 불법적인 온라인 거래 사이트 및 랜섬웨어와 같은 대가성 결제 지불 수단에서 주로 이용되고 있다. 그동안 거래자들 사이에서 비트코인에 따른 투명한 거래 및 비밀성 보장과 안정성을 인정받던 비트코인이 돈세탁과 같은 유형의 부정거래 및 거래소 해킹 공격 등으로 위협적인 요소가 드러나고 있다.

3.1 해킹 범죄 위협

대부분 가상화폐가 블록체인 기술을 이용하고 있어서 해킹이 어렵다고는 하나 최근 사용자 계정 해킹을 통한 가상화폐 유출 시도나 거래소 자체 서버를 공격하여 마비시키는 행위 등의 범죄 위협이 증가하고 있다. 그뿐만 아니라 국내 최대 가상화폐 거래소 직원의 PC가 사이버 공격을 당해 3만 명에 달하는 고객의 개인정보가 유출되었다. 유출된 정보에는 고객의 전화번호 및 이메일 주소 등이 포함되어 2차 피해가 우려되고 있다[9].

2011년 6월 29일에는 해커가 비트코인 거래의 대부분을 차지하고 있는 Mt. Gox에 침입하여 수십만 개의 비트코인을 확보하려는 시도가 있었다. 또한, 해커들이 랜섬웨어의 몸값으로 사용자 추적이 불가능한 비트코인을 지불수단으로 선택하고 있고 비트코인 이용자들을 대상으로 바이러스 등을 통해서 이용자의 비트코인 지갑에 접근하거나 혹은 노드로서의 권리를 가로채려는 시도도 여러 번 있었다[10].

3.2 투기 조장

최근 비트코인의 빠른 성장과 함께 비트코인의 가격 가치 상승으로 인한 투기를 목적으로 접근하는 투자자 및 기관들이 늘어나고 있다. 특히, 비트코인

은 일반적인 주식시장과 달리 24시간 운영되는 가상화폐 거래소마다 초 단위로 급등락을 거듭하는 등 가치에 대한 변동성이 너무 큰 것에 대한 위험성도 매우 높다. 그뿐만 아니라 비트코인은 공인된 금융투자 상품으로 분류된 것이 아니어서 가치가 급등락을 하더라도 투자자를 보호하기 위한 일시매매정지 제도 등과 같은 대책이 따로 마련되어 있지 않다[10].

3.3 이중지급 공격

이중지급 공격은 공격자가 기 지급된 비트코인을 회수하거나 재 지급하여 성공으로인 거래 승인을 완료하는 것으로 최종적으로는 지불받지 못한 자의 손실이 발생하게 된다. 공격의 종류로는 승인형 공격과 미승인형 공격이 있다.

① 승인형 공격 : 수신자가 블록체인을 통해 거래내용을 확인하는 정상지급 거래내용이 최장 블록체인에 포함되지 못하도록 방해하고 정상지불 거래내역이 블록체인에는 불포함시키는 공격 등이다.

② 미승인형 공격 : 돈을 받는 사람이 해당 거래내용이 블록체인에 포함되었는지를 미확인하여 발생할 수 있는 공격으로 레이스(Race) 공격, 피니(Finney) 공격 등이 있다[11].

3.4 익명성 거래

비트코인의 경우 익명성을 무기로 범죄 단체들의 검은돈이나 짧은 시간 큰 폭으로 변화하는 가치를 목표로 하는 투기성 자금이 밀려들고 있다. 즉, 비트코인을 투자의 개념으로 접근하여 익명성으로 거래를 시도하는 사람들이 늘고 있다. 세계 각국 관계자 말에 따르면 비트코인은 세금 탈세뿐만 아니라 범죄에도 연루되고 있다[12]. 특히, 세계 각국에서는 새로운 신종 랜섬웨어 악성코드 사태와 더불어 사용자의 컴퓨터 또는 데이터 파일을 사용자가 접근할 수 없도록 암호화하고, 암호해제를 빌미로 몸값을 요구하는 익명성 지급거래가 비트코인으로 이루어지고 있는 실정에서 익명성 거래는 매우 심각한 상태이다[13].

VI. 방안 제시

4장에서는 비트코인이 랜섬웨어 공격에 의한 대가성 몸값을 지급하는 비트코인과 관련된 투기성 거래에 대한 안전성 여부를 살펴본다. 또한, 비트코인 부정사기 거래에 대한 블록체인 문제점을 알아보고 비트코인을 좀 더 투명하고 안전하게 이용할 수 있는 비트코인 위험 요소에 대한 예방 방안을 제시한다.

4.1 보안 기능 강화

비트코인이 전 세계적 각 국가의 법정화폐로 인정받기는 거래적인 측면의 우려, 이용적인 측면의 우려, 일반인이 실질적인 화폐와 동등하게 통용할 수 없다는 측면에서 대중적으로 이용되기에는 시기가 필요하다. 또한, 새로운 가상화폐들의 생성으로 인해 채굴업자 간의 심각한 주도권 싸움이 일반인들에게는 더욱더 거래에 대한 경쟁성과 안전성을 떨어뜨리고 있다. 국내 가상화폐 전문가들까지도 비트코인이 국내에서 성공하는 낙관론보다 회의적인 측면에 좀 더 비중이 있는 것으로 추측되고 있다. 국내에서 비트코인과 같은 가상화폐가 좀 더 시장성 확보와 대중들로부터의 관심을 받기 위해서는 무엇보다 비트코인에 대한 올바른 사용과 왜곡을 막기 위해 좀 더 강력한 블록체인의 보안 기술이 접목되어

야 한다. 즉, 블록체인에 해쉬 암호 알고리즘의 보안 기능을 강화하여 계좌 및 비밀번호 등의 새로운 보안정책이 추가로 마련되어야 한다.

4.2 블록체인 수수료 인상

블록체인 이용 금액 및 이용 횟수에 대한 거래 수수료가 너무 싸다는 논란이 많다. 비트코인 거래 시 부담 없는 수수료 등이 불법 자금에 대한 부정 거래를 부추길 수 있다는 것이다. 즉, 거래가 빈번한 블록체인과 금액에 대한 1일 이용횟수 및 상한금액이 표시되어야 할 것이며 이용에 따른 수수료 정책을 높이는 개선 정책이 필요하다. 아직 가상화폐가 법정통화를 대체할 수 있는 수단으로는 다소 시간이 필요하다고 하였지만 디지털 시대에 가상화폐가 일부 국가에서는 법정통화로 인정되고 있는 시점과 비트코인과 같은 가상화폐가 빠르게 생성되어 유입되고 있는 시장 흐름을 고려해 볼 때 수수료 및 이용 횟수에 대한 수수료 지급 정책은 새롭게 개선되어야 한다고 본다.

4.3 신중한 투자

가상화폐의 높은 관심이 투기성 화폐로 전락하고 있는 위험한 상황이 전개되고 있다. 이와 비교되는 예가 2000년 초 인터넷 보급과 함께 닷컴 버블이 한참이었으나 말 그대로 흥하는 기업도 있었지만, 거품으로 많은 기업이 도산되는 시기이기도 하였다.

마찬가지로 2014년 비트코인 최대 거래소 마운트곡스가 해킹 및 배임 등을 이유로 파산하면서 비트코인의 가치는 반 토막 났다. 이어서 2015년 미국 비트코인 채굴업체와 스위스 비트코인 채굴업체도 결국 파산 신청을 냈다. 만약, 도산된 채굴업체가 영업적인 운영 면에 문제가 있거나 재정적으로 지급능력이 없는 채굴업체가 파산될 경우에는 투자된 돈을 전혀 돌려받지 못할 수도 있다. 즉, 주식 투자와 같이 투자 종목을 잘못 선택된 거와 마찬가지로 비트코인이 잘못 선택되어 투자했을 경우는 거래소와 사용자, 지갑 개발자와 채굴자 등 업계 관계자 상호간의 심각한 교착상태에 빠질 수 있다. 즉, 채굴시장의 가열과 경쟁이 치열한 상태에서 안전한 비트코인을 채굴하기 위해서는 각 국가적 가상화폐 매수/매도에 대해 꾸준한 시장 흐름을 파악하고 정보를 입수하여 건실한 채굴업체를 선정하여 블록체인을 공급받는 시간적 노력이 무엇보다 중요하다.

4.4 익명성 억제

미국과 유럽에서 비트코인의 사용자 수와 가맹자 수가 점차 늘어가는 이유는 바로 비트코인이 익명성이 강한 특징 때문이며, 금융거래 시 자금 이체가 편리하고 낮은 지급수수료 비용으로 분석된다. 또한, 무엇보다 주식과 같이 가격 상승이 동반할 수 있다는 투자 가치로서의 기대 수익도 한몫하고 있다. 그러나 비트코인이 자금출처가 불분명한 돈세탁과 같은 거래에 사용된다면 큰 문제가 아닐 수 없다. 또한, 익명성 거래가 공공연히 부정적으로 사용하게 된다면 세계적으로 비트코인에 대한 부정적 이미지와 가상화폐에 대한 부패가 토착화될 것이 자명하다. 특히, 익명성 거래의 목적은 불법적인 온라인 사이트를 통해 자신들의 거래 흔적이 남지 않길 원하는 사용자들이 대부분이다. 이러한 익명성 거래는 주로 도박, 성범죄, 무기매매 등의 범죄수단에 사용되거나 비자금 조성과 자금세탁 등에 악용되고 있다. 비트코인 익명 사용자들은 거래 시 영문과 숫자로 된 익명성의 주소로 거래가 제공됨으로 공공 주소의 이름을 네트워크에 알려지지 않고 온라인상에서 사용할 수 있는 비트코인과 같은 가상화폐를 익

명성으로 사용하게 된다. 이렇게 개설된 거래자 주인의 주소는 각종 불미스러운 사건을 유발할 수 있는 사기 거래에 이용되기도 한다. 더욱더 익명성 보장이 요구되는 마약류나 총기류와 같은 밀수 거래에 이용된다면 사회적으로 심각한 부작용을 초래될 수도 있다. 비트코인의 익명 거래를 막고 공정한 거래를 위해서는 거래 내용을 모든 사람이 시각적으로 판독 가능하게 하거나 보안이 강화된 블록체인 시큐어 기술이 도입되어야만 한다. 또는 보내는 사람과 받는 사람의 본인 인증 절차가 확인되는 거래에 대해서 공공주소가 투명하게 공개되는 인증 시스템이 국가적 차원에서 도입되어 비트코인 거래 시 조속히 적용될 수 있는 방안이 마련되어야 한다.

V.결 론

본 논문에서는 가상화폐 비트코인에 대해서 이해하고 국가적 비트코인 동향 및 규제에 대해서도 알아보았다. 위험성을 배제하고 안정성과 투명성을 위해 블록체인은 공정성 있는 주소 거래 기준을 따르는 것이 바람직하다. 하지만 랜섬웨어와 같은 사회공학적 공격으로 악성코드 감염에 의한 피해를 본 경우라면, 파일 복구를 위해 비트코인을 지급했다가 피해를 입은 경우가 대부분이다. 만약, 공격자의 계좌 추적과 투명한 거래를 위해 안전한 장치가 확보되었다면 충분히 공격자의 신원을 파악하여 구속 수사가 가능할 수 있다. 본 논문에서 살펴본 바와 같이 익명성을 가진 대부분의 피해 거래 유형이 비슷하다. 우리나라 비트코인 시장은 아직은 크지 않다. 그러나 시장 성장에 대한 잠재 가능성이 점차 커가고 있다. 비트코인이나 이더리움과 같은 가상화폐가 투자 가치 및 사이버상에서 가치를 지니는 거대한 화폐 시장으로 성장하기 위해서는 법적 분쟁이 발생할 수 있는 여러 상황에서 운용에 필요한 절차와 규제적 표준 방안이 필요하다.

참고문헌

[1] 이경미, 고은희, 주소현, “한국·미국·독일의 비트코인 활용 현황과 공유가치창출에의 함의 탐색,” 한국FP학회, 제9권, 3호, 2016년, pp. 86-87.

[2] https://bitcoin.org/ko/how-it-works

[3] 이종협, “비트코인의 가능성과 보안의 문제들,” 정보처리학회지, 제21권, 6호, 2014년, pp. 35-43.

[4] https://steemit.com/kr/

[5] https://www.ddengle.com/trading/1675927

[6] https://bitcoin.org/ko/how-it-works

[7] https://bitstand.com/

[8] https://blog.naver.com/PostView.nhn?blogId=ntscafe&logNo=220756269559&proxyReferer=https%3A%2F%2Fwww.google.ca%2F

[9] http://www.kinews.net/news/articleView.html?idxno=108746

[10] 전주용, “비트코인의 이해와 시사점,” 정보통신정책연구원, 제13권, 제8권, 2013년, pp. 9-10.

[11] 이혁준, 이수미, “비트코인의 신뢰구조와 이중지불의 위협,” 정보보호학회지, 제26권, 2호, 2016년, pp. 25-30.

[12] 양지연, 김소희, 김윤정, “비트코인 취약점 및 현 대응방안의 한계 분석,” 한국정보과학회 학술발표논문집, 2015년, pp. 1013-1015.

[13] 최희식, 조양현, “사례로 살펴본 렌섬웨어 공격에 의한 피해를 최소화하는 연구 고찰,” 디지털산업정보학회 논문지, 제13권, 1호, 2017년, pp. 103-111.

■ 저자소개 ■

최 희 식
(Choi Heesik)

2008년 9월 ~ 현재
경민대학교 IT경영과 외래교수
2006년 2월 숭실대학교 컴퓨터학과(공학박사)
2002년 2월 숭실대학교 컴퓨터공학과(공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터, IoT,
핀테크 금융보안
E-mail : dali3054@ssu.ac.kr

조 양 현
(Cho Yanghyun)

1997년 9월 ~ 현재
삼육대학교 컴퓨터학부 교수
2011년 2월 광운대학교 전자통신학과 (공학박사)
1985년 2월 광운대학교 전자통신학과 (공학석사)
1982년 2월 광운대학교 전자통신학과(공학사)

관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS
E-mail : yhcho@syu.ac.kr

논문접수일 : 2017년 8월 12일
수 정 일 : 2017년 8월 23일
게재확정일 : 2017년 8월 24일