가상화폐 비트코인의 핵심기술인 블록체인에 관한 연구

남수태 · 김도관 · 진찬용

원광대학교(융복합창의연구소)

A Study on the Blockchain as the Core Technology of Bitcoin

Soo-tai Nam · Do-goan Kim · Chan-yong Jin

Wonkwang University (Institute of Convergence and Creativity)

E-mail : stnam@wku.ac.kr

요 약

최근 사회적 화두가 된 비트코인은 블록체인 기술을 활용한 수평적 및 분권적 디지털 가상화폐라 불리기도 하며 암호화폐의 일종이다. 블록체인은 피어-투-피어(P2P) 네트워크상에서 공유되는 분산원장이라고 할 수 있는 블록체인은 비트코인에서 먼저 사용되었다. 이러한 기술은 다른 분야에서도 다양하게 응용 가능한 기술이라고 하여 높은 사회적 관심을 받고 있다. 최근 비트코인 등 가상화폐 시장 동향을 살펴보면 작년 일본정부가 가상화폐를 결제의 수단으로 인정한 이후 가격 변동성 높아졌다. 따라서 혁신적 기술을 바탕으로 한 비트코인의 핵심기술인 블록체인 기술을 조망을 통해 이론적 실무적 함의를 제시하고자 한다.

ABSTRACT

Recently in Bitcoin raising a social issue is sometimes called a horizontal and decentralized digital virtual currency utilizing the Blockchain technology such as a type of password currency. On the other hand, the Blockchain, which is a distributed ledger shared on P2P networks and it was first used in Bitcoin. These technologies are regarded as technologies that can be applied diversely in other fields, and are attracting high social interest. Looking at recent trends in the virtual currency market such as Bitcoin, price movements have increased since the Japanese government approved the virtual currency as a means of settlement last year. Therefore, we try to present theoretical practical suggestion through the viewpoint of the Blockchain technology which is core technology of Bitcoin based on innovative technology.

키워드

비트코인, 블록체인, 가상화폐, 암호화, 혁신기술

I. 소 개

블록체인 기술은 비트코인 디지털 화폐를 지원하는 기술에 부여된 이름으로 불린다. 전통적인 디지털 화폐는 전자 데이터에 가치를 제공하기 위한 특정 메커니즘에 집중되어 있으며 메커니즘의 통제 아래에 있는 영역에만 배포된다. 역으로 비트코인의 데이터는 분산된 시스템에서 관리된다. 전자 데이터의 가치는 모든 개인에 의해 공통적으로 인정되는 시스템의 사용과 관련된다고 볼 수 있다. 비트코인은 전 세계 최초로 유통되는 디지털 화폐로 소개되고 있다. 이러한 혁신적인 시스템의 중심에는 블록체인이라는 기술이 여기에 속한다[1]. 블록체인 기술이 작동하는 방법에 대해 논의하면 다음과 같다. 일반적인 금융거래에서 은행의 계좌와 동일한 개념이며, 비트코인의 맥락에서 보면 주소라고 말할 수 있겠다. 입력 주소의 소유자가 제공한 디지털 서명은 거래가 소유자의 의도적인 행위와 일치함을 보증한다. 또한 중복지불 문제를 피하기 위해 피어-투-피어(P2P) 비트코인 네트워크를 통해 변환이 전송되고 해당 네트워크의 모든 참가자가 유효성을 검사하게 된다. 10분마다 기록되는 합법적인 트랜잭션 블록을 가진 데이터 세트를 블록이라고 하고 블록체인은 연대순으로 연결된 여러 개의 블록에 대응하게 된다[1]. 새로운 블록은 마이너에 의해 생성되고 운영되어 진다. 특정 임계 값 이하의 해시 값을 가진 블록을 설계하는 마이너는 인센티브로 비트

코인을 받게 된다. 마이너들은 블록을 만들기 위해 무한 경쟁을 한다. 특정 주소를 가진 도메인에 할당된 번호를 임의로 변경하면 블록의 해시 값도 임의로 변경되게 된다. 임계 해시 값은 평균 10분 단위로 하나의 조각이 발생하도록 설정되어 있다. 해시 값은 다음 블록에 통합되므로 다음 블록이 모두 다시 계산되지 않으면 이전 데이터가 수정 될 때 일관성을 보장 할 수 없다. 따라서 블록체인을 변경하는 것은 사실상 불가능하다. 또한 P2P 비트코인 네트워크에 참여하는 모든 노드는 고유한 블록체인을 공유하므로 동시에 높은 가용성을 실현하게 된다. 비트코인 트랜잭션은 개별적으로 관리되지만 고유하고 일관된 블록체인에 통합되어 변조방지 및 가용성이 높은 정보를 공유하는 시스템을 실현하게 된다.

II. 연구방법

비트코인의 개발자인 나카모토 사토시가 2008년 논문을 발표하였고 그 논문을 바탕으로 비트코인이 개발되었다. 비트코인 이전의 인터넷에서의 상거래는 거의 금융기관을 제 3자 신용기관으로 하는 전자 지불 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 발생시키는 요인으로 작용한다. 이러한 문제를 해결하기 위해 신용보다는 암호화 기술을 기반 한 전자 지불 시스템을 이용하여 두 거래자가 제 3자인 신용기관 없이도 직접적인 거래를 가능하게 구현하였다. 네트워크 적으로 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 피어-투-피어 분산 네트워크 기반의 거래를 통해 이중지불의 문제를 방지하는 해법을 제시하였다[2].

비트코인 네트워크에서 사용하는 암호화 방식은 공개키 암호화 방식에서 주소가 공개키가 되는 것이고 개인키는 사용자의 PC에 저장된다. 이는 대중적으로 익히 알고 있고 사용하고 있는 PKI (Public Key Infrastructure)와 비교할 수 있다. PKI에서는 국가에서 신뢰하는 공인 인증기관(CA)에서 키를 만들어 개인이나 단체에게 인증서를 발급한다. 이 인증서에는 그 공인 인증기관의 공개키가 포함되어있다. 또한 각각의 피어(Peer)에게는 개인키가 발급된다. 공인 인증기관 에서는 이 피어에게 할당된 개인키 및 공개키를 적법한 절차를 통해 인증서를 발행하게 되며 공인 인증기관이 이를 보증한다[2]. 그러나 비트코인에서 사용하는 공개키 방식은 공인 인증기관이 별도로 존재하지 않는다. 공개키와 개인키는 한 쌍을 이루어져 있지만 이것을 보증해주는 공식적인 기관은 없다는 것이다. 오직 개인키를 담고 있는 지갑과 주소라는 이름으로 사용되는 공개키는 이것을 이용하는 사용자의 서명으로 거래를 입증하게 된다.

III. 결 론

국제사회는 가상화폐 규제를 위한 국제공조 방법을 모색하고 있으며 아울러 블록체인 기술을 법정통화에도 적용하는 방법을 모색하는 중으로 보인다. 한국에서도 가상화폐에 대한 투기열풍이 금융시장과 부동산 시장에서 소외되어 있는 2030세대를 중심으로 옮겨 붙어 결국 가상화폐 거래 실명제 등 정부의 규제정책으로 이미 이어졌다[3]. 업계와 전문가는 가상화폐가 거래소 인허가제도 및 양도소득세 과세 등의 방법으로 제도화될 것이라 전망하나 제도화의 구체적인 방법론에서는 정부부처와 전문가 사이에서 이견이 여전히 존재한다. 한편 비트코인은 피자구매와 실크로드 사건으로 교환수단의 가능성을 보였지만 가격변동성이 심화되어 현재는 해당기능이 약화되었다[3]. 또한 2013년 유로존 위기는 기존 법정통화에 대한 대안으로 비트코인을 주목받게 하였으나 마운트 곡스 파산 등으로 인해 비트코인 거래 제도의 안전성 문제가 크게 부각되었다[3]. 앞으로 비트코인 등 유사 가상화폐는 중앙은행 디지털 화폐와 경쟁이 불가피한 현실임을 직시하여야 할 것이다.

참고문헌

[1] J. Kogure, K. Kamakura, T. Shima and T. Kubo, “Blockchain Technology for Next Generation ICT,” *FUJITSU Science Technology Journal*, vol. 53, no. 5, pp. 56-61, Sep. 2017.

[2] J. H. Lee, S. H. Lee, D. E. Lee, W. C. Kim and M. S. Kim, “Effective Vitalization Plan of Electronic Cash using Bitcoin,“ *Journal of Convergence Security*, vol. 16, no. 4, pp. 79-90, 2016.

[3] B. K. Min, Y. J. Seong and W. I. Park, “Issues and policy implications of Bitcoin and Blockchain,” *Problem & diagnosis of Gyeonggi Research Institute*, vol. 1, no. 307, pp. 1-27, 2018.