

2017 한국인터넷거버넌스포럼(KRIGF) 워크숍 보고서

세션명	블록체인 기술의 이해와 활용		
일시	2017.9.15.(금) 10:45~12:15	장소	세종대학교 광개토관 소회의실 6
발표자	민경식(한국인터넷진흥원)		
플로어	약 17명 참여		

1. 블록체인의 개념

- 네트워크 내의 모든 참여자가 공동으로 거래 정보를 검증하고 기록, 보관함으로써 공인된 제3자 없이 신뢰성을 확보하는 기술
- 2008년 나카모토 사토시의 논문 “비트코인: 개인간 전자화폐 시스템”을 통해 금융기관에 의존하지 않는 비트코인의 블록체인의 개념이 처음 유입

(1) 블록과 체인

- 블록: 일정기간 내 거래가 기록된 장부로 각 블록의 헤더와 바디로 구성 되어 정보의 위변조를 확인하기 위한 해쉬값, 변경된 데이터의 암호와 저장, 참여자 확인을 위한 전자서명 기술이 활용되어 보안이 우수함
- 체인: 블록이 연결되어 있는 형태

(2) 비트코인

- 비트코인은 특정한 발행주체가 없는 P2P (Peer-to-Peer) 네트워크상에서 암호화 알고리즘에 따라 채굴 (minning) 을 통해 발행
- 비트코인의 총 발행량은 2,100만 BTC 로 정해져 있으며 채굴을 통해 발행되는 양은 (현재 12.5 BTC)은 약 4년마다 절반으로 줄어들도록 설계

(3) 비트코인 현황

- 비트코인의 거래 규모는 지속적으로 확대되고 있으며 2017년 5월 기준 전체 거래량은 약 13억 달러, 가격은 2,300만 달러를 기록
- 현재 약 7700개의 노드, 150 GB의 크기, 1500만 개의 지갑, 하루 약 26만 건의 거래가 이루어지는 블록체인 네트워크 존재

(4) 블록체인 페리다임의 진화 방향

- 암호화폐, 화폐 전송, 외환 송금, 전자 지불만 가능한 비트코인의 1세대 블록체인
- 스마트계약 (smart contract), 탈중앙화 자율 조직 (DAO) 라는 개념을 가진 이더리움 (Ethereum) 이 나타나며 2세대 블록체인의 금융 이외의 분야에서 활용 가능성 제시

2. 블록체인의 활용분야

- 2세대 블록체인 자산, 신뢰, 소유권, 화폐, 신원, 계약등 다양한 분야에 활용, 개발

(1) 블록체인 유형별 주요 특징

- 퍼블릭 블록체인 (Public Blockchain): 공개적 접근이 가능한 최초의 블록체인 활용 사례
- 프라이빗 블록체인 (Private Blockchain): 허가한 사용자만 접근 가능한 개인형 블록체인
- 컨소시엄 블록체인 (Consortium Blockchain): 허가한 그룹의 사용자만 접근 가능해 네트워크 확장이 용이하고 거래 속도가 빠름

(2) 정책 활용 사례

- 에스토니아의 블록체인을 활용한 “전자 시민권” 제도 투입해 신원 확인 및 정부 서비스에 접근을 인증하는 용도
- 영국의 “beyond blockchain” 모든 공공 서비스에 블록체인 및 스마트 계약 적용 추진

(3) 블록체인 활용 기대분야

- 신분 증명, 출생, 생존 증명, 학위 증명의 개인 인증
- 스마트 시티, 전자 거래, IoT 등 다양한 분야에 활용 가능
- 부동산 등기, 의료정부 관리, 공문서 관리들의 문서 관리

(4) 주요 서비스 구현 사례

- KT의 블록체인 기반 전자 서명 이미지 관리
- 한국조폐공사 (KOMSCO)의 공공분야 블록체인 플랫폼 개발

3. 블록체인 기반 디지털 신뢰 사회 구현

- 블록체인 글로벌 생태계가 빠르게 조성되고 있고 선진국에서는 금융, 물류, IoT를 포함하여 전 영역에 걸쳐 적용 확대중

(1) 부족한 블록체인 인프라

- 국내는 금융 분야를 중심으로 진행되고 있으나 정부 및 민간으로의 확장이 필요
- 블록체인 관련 글로벌 시장이 2021년 약 23억 달러로 빠르게 성장할 전망으로 국내 기업의 경쟁력 강화

(2) 정부의 정책 현황

- 정부는 “지능정보사회추진단” 발족, “블록체인 오픈 포럼” 출범 등을 통해 블록체인 산업 지원 토대 마련
- 비금융분야 블록체인 기술 적용 확산을 위한 범제도적 기반 마련 추진

질의	<p>(플로어)</p> <ul style="list-style-type: none"> - 하이퍼레저 퍼블릭의 성격이나 특징은 뭐가 있을까요? <p>(답변)</p> <ul style="list-style-type: none"> - 강의 내용에서 다시 설명을 드리자면, 일단 퍼블릭은 아니고 프라이빗한 형태를 가지고 있습니다. 또한 코인을 매체로 사용하지 않습니다. 상업용 기반으로는 코다도 있고 원자만 만드는 특수한 형태도 존재 하지만 구조적인 차이이고 하이퍼레저 퍼블릭은 데이터를 많이 나눌 수 있어 기업용이나 서비스 기반 등 다양하게 많이 쓰이고 있습니다.
-----------	--