정 보 보 호 학 회 지
제28권 제3호, 2018. 6

블록체인개발 현황과 보안이슈 변화 동향

정 현 준*, 이 흥 노**

요 약

암호화폐가 세계적으로 주목받으며 핵심기술인 블록체인에 대한 관심이 증가하고 있다. 블록체인은 블록을 P2P 방식을 기반으로 생성된 체인 형태의 연결고리로 분산 저장되어 있으며 임의로 수정할 수 없고 누구나 변경의 결과를 열람가능하다. 블록체인의 공개 형태에 따라 공개형 블록체인과 허가형 블록체인으로 나뉘어 연구되고 있다. 이 논문에서는 세대별 블록체인의 개발 현황과 특징에 대해서 알아본다. 또한 블록체인 공개형태에 따른 특징과 보안성에 대하여 알아보고자 한다.

Ⅰ. 서 론

블록체인(Blockchain)은 비트코인(Bitcoin)의 등장과 함께 세상에 알려졌다. 비트코인은 2009년 등장하여 최근 가격이 급격히 증가함에 따라 암호화폐(Cryptocurrency)가 세계의 주목을 받고 있다. 그리고 암호화폐의 기반기술인 블록체인에 대한 기술적 분석과 블록체인을 접목한 비즈니스가 양성되고 있다.

미국 애리조나주에서는 블록체인 기록 등의 법적 유효성 목적의 입법을 진행하였다. 이 입법에서 블록체인 기술이란 분산, 탈중앙화, 공유, 복제의 성질을 가진 분산화된 원장이라고 정의하였다. 미국 하와이주에서는 블록체인 산업의 진흥의 목적 입법을 진행하였다. 이 입법에서 블록체인이란 새로운 P2P 네트워킹 및 탈중앙화의 분산 데이터 저장 기술이라고 정의하였다. 한국은행은 블록체인을 거래정보를 기록한 원장을 특정 기관의 중앙서버가 아닌 P2P 네트워크에 분산하여 참여자가 공동으로 기록하고 관리하는 기술이라고 정의하였다[1]. 블록체인이란 1) 통제에 대한 탈중앙화를 목적으로, 2) 분산화된 구조를 가지며, 3) 데이터의 저장할 수 있는 구조를 말한다.

블록체인 기술은 비트코인의 기반기술로 알려져 있다. 블록체인은 새로운 정보화 기술로써 산업 전반에 걸쳐 영향을 미칠 기술이다. 일반적인 시스템에서는 클라이언트 서버 모델(Client-server model)을 적용한다. 이 모델은 서비스 요청자인 클라이언트와 서비스 자원의 제공자인 서버 간에 작업을 분리해주는 네트워크 아키텍처이다. 블록체인은 중개자 없이도 개인 (peer)간의 거래, 가치, 자산 등을 교환할 수 있는 신뢰 프로토콜을 제공한다. 기존의 서버는 신뢰 프로토콜을 유지하기 위하여 비용과 노력이 필요하다. 서버에 저장하고 있는 데이터(혹은 코인)는 공격자의 타깃이 된다. 시스템 관리자는 공격자의 공격을 막기 위하여 보안을 지속해서 관리해야 한다. 블록체인은 지켜야 하는 데이터를 모두에게 공개하여 서로를 감시하게 하여 무결성을 유지한다. 암호화폐에서 블록체인은 모든 거래 내용을 공개하고 인터넷에 분산 저장한다. 즉, 블록체인이란 공개 장부를 공정하게 만들고 관리하기 위한 기술이다. 공개 장부에 한 번 기록된 것은 변경할 수 없으며 위조할 수 없기 때문에 화폐에 응용 가능하다.

비트코인의 가격이 2017년 1월 1BTC 가격은 약 600만원에서 2018년 1월 약 2500만원까지 상승하였다. 한국 정부에서는 암호화폐의 가격의 변동성이 심해지자 신규계좌의 생성을 막는 등의 제재를 실행했다. 블록체인과 암호화폐에 대한 사회적 관심이 증가하였으며 급격한 가격변동으로 인해 우려도 증가하였다. 블록체인의 공개 형태에 따라 공개형 블록체인(Public Blockchain)과 허가형 블록체인(Private Blockchain)으

이 논문은 2018년도 광주과학기술원의 재원으로 “과학기술응용연구단의 실용화연구개발사업”의 지원을 받아 수행된 연구임.
* 광주과학기술원 센서지능화 연구센터 연구원 (junghj85@gist.ac.kr)
** 교신저자, 광주과학기술원 전기전자컴퓨터공학부 교수 (heungno@gist.ac.kr)

로 개발되고 있다.

이 논문은 블록체인 공개형태에 따른 블록체인의 특징과 보안 연관성에 대해서 알아본다. 2장은 세대별 암호화폐를 구분하여 특징을 정리한다. 3장은 공개형태에 따라 공개형 블록체인과 허가형 블록체인의 특징을 정의하고 비교한다. 4장은 블록체인에 적용할 수 있는 암호화폐를 분류한다. 5장은 결론으로 블록체인을 이용한 비즈니스가 나가야할 방향에 대하여 말한다.

Ⅱ. 세대별 암호화폐

암호화폐는 비트코인을 시작으로 현재까지 수백개가 제안되었다. 암호화폐는 단순 결제 기능의 화폐성 1세대 암호화폐(표 1)와 스마트 계약이 가능한 2세대 암호화폐(표 2)로 구분한다. 이 논문에서는 1.5세대 암호화폐(표 3)를 1세대 암호화폐의 기본 기능에 추가기능을 넣은 암호화폐, 2.5세대 암호화폐(표 4)를 2세대의 한계를 극복하고자 나온 암호화폐로 구분하였다.

암호화폐는 세대로별로 진화할수록 기능에 초점을 맞춰 발전되고 있다. 예를 들어, 새로 제안되는 암호화폐는 비트코인의 확장성, 거래 속도 향상을 위하여 기존의 구성요소를 변경 혹은 추가하여 구성한다. 하지만 신규 암호화폐의 새로운 기능과 속도를 위한 구조로 인하여 보안성이 약해지는 경향이 있다.

〔표 1〕 1세대 - 단순 결제 기능의 화폐성 암호화폐

이름	발행 or ICO	특징
비트코인 (BTC)	2009. 1.3	사토시 나카모토가 제안한 최초의 코인〔2〕. 전자 화폐를 디지털 서명의 체인으로 정의함. 코인 소유자는 거래 내역에 디지털 서명을 한 후 다음 사람에게 전달하고, 이를 받은 사람은 자신의 공개 키를 코인 맨 뒤에 붙임.돈을 받은 사람은 앞사람이 유효한 소유자였다는 것을 확인가능.
비트코인 캐시 (BCH)	2017. 8.1	비트코인에서 하드포크 되어 생성된 알트코인이다〔3〕. 한계 속도를 극복하기 위해 블록 크기를 2~8MB까지 유동적으로 늘리는 편법 정책을 적용함.
비트코인 골드 (BCG)	2017. 10.25	비트코인에서 하드포크 되어 생성된 알트코인임〔4〕. 그래픽카드(GPU)로 채굴할 수 있음.
비트코인 다이아몬드 (BCD)	2017. 12	블록 크기 제한을 8MB로 변경하여 트랜잭션 용량이 향상되고 블록이 5배 빠르게 생성된다〔5〕. 거래 전송 시에 금액을 암호화하여 개인정보를 보호함.
리플 (XRP)	2012	블로체인 기반 송금 시스템임. 중앙 통제식(채굴이 존재하지 않음)이며 국제간 화폐 거래를 이용한 프로그램을 지원하여 수수료 및 환율 시세차익을 얻음〔6〕. 암호화폐의 기본 이념인 탈규제, 탈중앙화, 익명에 정면으로 반대되는 코인임.
스텔라 루멘 (XLM)	2014. 7	리플에서 하드포크 하여 개발된 암호화폐이다〔7〕. 비영리 기업 스텔라 재단에서 운용하는 화폐이다. 리플은 기업 간의 자금 송금을 목적으로 하고 스텔라루멘은 개인 간의 거래를 위하여 만들어짐.
라이트 코인 (LTC)	2011. 10.7	비트코인을 중심에 두고 개발되었음. 비트코인보다 약 4배 빠른 거래가 이루어진다〔8〕. 라이트닝 네트워크는 비트코인과 라이트코인에 복수 적용될 예정임. 이를 통해 아토믹스왑이 실현 가능해질 예정임.

〔표 2〕 1.5세대 - 1세대 암호화폐의 기본 기능과 추가 기능을 넣은 암호화폐

이름	발행 or ICO	특징
제트 캐시 (ZEC)	2016. 10.28	트랜잭션의 프라이버시와 선택적 투명성을 제공하는 분산형 오픈소스 코인임〔9〕. 제트캐시 지급은 영지식 증명 기술(zero-knowledge proof) 기반으로 공개 블록체인에 개시되지만 거래의 보낸 사람,받는 사람 및 금액은 사적으로 유지됨.
모네로 (XMR)	2014. 4.18	CryptoNight이라는 독자적 작업증명 기법을 사용하여 채굴기와 이를 소유한 자본에 의한 탈중앙화(decentralization)적 가치가 훼손되는 것을 막음〔10〕. 거래내역이 비공개로 되어있어, 누가 누구에게 얼마를 보냈는지 알 수 없음.
대시 (DASH)	2014. 2.14	Dash 전송을 요청하면 마스터노드가 3개 이상의 거래 내역을 섞어서 보내는 코인조인(coinjoin) 방식을 사용함〔11〕. 마스터 노드는 Dash를 1,000개 이상 가진 사람이며 향후 대시의 개발 및 운영 방향에 대한 투표권을 가짐.

이름	발행 or ICO	특징
팩텀코인 (FCT)	2015. 9	데이터(문서)의 투명성과 지속성을 위하여 제안된 플랫폼[12]. 팩텀 블록에는 문서/기록의 고유값을 저장할 수 있음.
지코인 (XZC)	2016. 10.6	CPU와 GPU를 통해 채굴할 수 있음[13]1. 공용코인 소유자는 개인코인을 주조할 수 있음. 개인코인 사용 시 송금 이력 추적이 불가능함(영지식 증명 기반).
나브코인 (NAV)	2014. 6	비트코인 코어를 개량하여 만들어진 코인임[14]. 빠른 전송속도(블록타임 30초, 블록사이즈 20mb 확장)와 익명성(Navtech라는 이중블록체인 기술이용)이 특징이며 aDapp(익명화된 분산 어플리케이션)을 지원하는 플랫폼으로서 역할을 함.
시아코인 (SC)	2015. 6	클라우드 데이터 저장 서비스임. 블록체인을 이용한 스토리지 서비스를 제공함[15]. 컴퓨터의 저장공간을 다른 사람에게 임대하고 사용료를 받음. 기존 상용 클라우드서비스보다 평균 10배 이상 저렴함.
버스트 코인 (BURST)	2014. 8	PoC(Proof of Capacity)를 사용하여 채굴함[16]. PoC는 컴퓨터에 남아있는 잉여부분의 하드디스크를 사용하여 채굴하는 방식임.
스토리지 (STORJ)	2017. 7.2	이더리움 기반으로 만들어진 분산화된 클라우드 저장 플랫폼임[17]. 하드디스크의 남은 용량을 크라우드 형태로 임대하고 코인을 획득함.
NEM코인 (XEM)	2015. 3.31	약 90억 개의 고정된 통화 발행으로 인플레이션이 제로인 코인임. 자바, 자바스크립트로 코드가 작성됨[18]. NEM 코인에 적용된 PoI (Proof of Importance) 알고리즘은 코인의 유동성과 거래참여 기여도를 측정하여 채굴자의 중요도를 결정하고 중요도에 비례하여 보상 함.
버트코인 (VTC)	2014. 1	NIST5기반의 Lyra2Re 체인 알고리즘을 제안하여 마이닝 중앙 집권화를 방지함[19]. 지금까지 2차례 PoW를 변경함.
디지 바이트 (DGB)	2014. 1.10	다섯 개의 마이닝 알고리즘을 사용하여 마이닝 중앙 집중화를 방지함[20]. 초당 280회의 트랜잭션을 처리할 수 있음. DGB 코인을 보상으로 지급하는 게임서비스를 제공함.

[표 3] 2세대 - 계약 기능을 포함한 암호화폐

이름	발행 or ICO	특징
이더 리움 (ETH)	2015. 7.30	블록체인 기술을 기반으로 스마트 계약 기능을 구현하기 위한 분산 컴퓨팅 플랫폼과 탈중앙화된 앱 개발 환경 제공[21]. 비탈리크 부테린(Vitalik Buterin)이 개발함. P2P 컴퓨터 네트워크를 데이터 및 코인거래 내역을 블록체인에 저장하는 것은 물론, 스마트 계약이 설정된 코드도 실행할 수 있는 컴퓨팅 플랫폼 제공.
퀀텀 (QTUM)	2016	비트코인 블록을 사용하여 이더리움의 스마트 계약 엔진을 연결한 플랫폼임[22]. 비트코인의 디자인을 사용하고 이것을 블록체인에 코드로 비즈니스 규칙을 저장하고 EVM(이더리움 Virtual Machine)과 연결함. 채굴방식으로 PoS (Proof-of-Stake, 지분 합의 증명)을 택했음.

[표 4] 2.5세대 - 2세대의 한계를 극복하고자 나온 암호화폐

이름	발행 or ICO	특징
아이오타 (IOTA)	2016	사물인터넷을 위한 수수료 없고 채굴자 없이 데이터 무결성을 추구하는 블록체인. 탱글(방향성 비사이클 그래피)이라는 새로운 분산장부 작성 기술을 사용[23]. 이 기술은 서버사용으로부터의 탈중앙화를 유지하며 채굴자 없이 즉 수수료 없는 거래가 가능케 함.
카르다노 (ADA)	2017. 10.1	암호화폐 개발 언어로 적합한 하스켈언어로 만들어진 블록체인임[24]. 하스켈은 함수형 언어이며 카르다노 백서에 제시된 수학적 표현을 완벽하게 설명하고 입증함. 카르다노는 회계(Accounting)와 컴퓨팅(Computing)을 분리하여 구현되어있음. 우로보로스(Ouroboros)라는 PoS 증명 알고리즘을 사용함.
이오스 (EOS)	2017	이더리움의 PoS에 비해 빠른 트랜잭션 처리가 가능한 비잔틴장애허용 DPoS(Delegated Proof Of Stake)방식을 사용함[25]. 이오스 Dapp은 사용자는 수수료를 지급하지 않고 개발자가 이오스를 지급함.

Ⅲ. 공개형 블록체인과 허가형 블록체인

블록체인 기술은 서로 신뢰할 수 없는 인터넷 환경에서 사람이나 사물들이 중개인 없이 돈이나 자산을 안전하게 교환하는 것이다. 거래들이 기록되어 있는 분산화된 원장을 안전하고 위변조 될 수 없게 관리하기 위한 분산 데이터베이스 및 관련 기술을 말한다. 분산화된 원장은 암호화키를 이용하여 체인 형태로 연결되어 있어 위변조가 불가능(혹은 난이도가 높음)하다. 기존 시스템에는 거래명세을 독점하여 데이터를 보호하고 무결성을 검증하였다. 반대로 블록체인은 거래명세을 모두가 공유하고 내용에 대해 수정이 있는지 서로 감시하고 검증한다. 블록체인 검증에 참여하는 노드들이 많아야 하며 참여, 검증, 저장에 대해 보상이 필요하다.

노드들은 특정 기간(예, 비트코인 매 10분)에 일어난 거래 기록을 담은 블록(block) 단위로 저장한다. 블록을 조작하는 것을 막기 위하여 공동 관리하고 블록들을 해시 함수(예, sha256)를 이용하여 요약하고 연결체인을 만든다. 연결 체인은 이전 블록의 요약을 다음 블록에 추가하여 다음 블록이 완성되면 이전 블록을 수정할 경우 바로 확인할 수 있다. 분산 원장은 모든 블록을 가지고 있어서 내용을 확인할 수 있지만 변경할 수 없다. 위의 특징을 이용하여 P2P 구조로 모든 사람이 변경되지 않은 데이터를 가질 수 있으며 확인할 수 있다. 비트코인 등의 암호화폐의 블록체인은 금전 거래(트랜잭션)를 저장하고 있다. 금전 거래뿐만 아니라 다른 기록 정보를 원본 그대로 보존하는 목적으로 이용할 수 있다.

블록체인 네트워크는 비트코인, 이더리움 등과 같이 분산 원장에 누구나 참여할 수 있는 공개형 블록체인과 권한을 가진 이들만 참여할 수 있는 허가형 블록체인으로 나뉜다. 허가형 블록체인은 운영 규칙에 따라 운영 주체 또는 특정 몇 명만 원장을 만들 수 있다. 허가형 블록체인은 현재 운영하는 시스템에 블록체인을 적용하기 위한 특수한 형태이다.

기업이 허가형 블록체인을 도입하는 이유는 공개형 블록체인(예, 비트코인, 이더리움)을 그대로 적용할 경우 기존 시스템과 맞지 않기 때문이다. 그래서 자신에게 맞는 형태로 변경하여 적용하고 싶기 때문에 허가형 블록체인의 수요가 유지되고 있다. 기업이 허가형 블록체인을 적용하는 이유는 다음과 같다.

1. **거래 처리 시간 단축**: 비트코인은 하나의 블록이 생성되기 위해서는 10분이 소요된다. 블록의 기록이 안정되기 위해서 5개의 블록이 필요하다고 가정한다면 50분이 필요하다. 블록이 생성되는 시간이 비즈니스에서 필요한 요구 시간보다 길기 때문에 보다 적은 시간을 요구한다.
2. **트랜잭션 비용(Transaction fee) 조정**: 블록체인은 데이터를 P2P로 저장하기 때문에 트랜잭션을 저장하기 위해서 일정한 비용을 요구한다. 일반적인 은행 계좌일 경우 송금 시에 보내는 쪽이나 받는 쪽 정책에 따라 일정량의 수수료가 책정된다. 일반적인 암호화폐(예, 비트코인, 이더리움)의 수수료는 송금자의 수수료 납부 정책에 의해 결정된다. 이는 거래를 인증해주는 노드(채굴자)가 네트워크상에 반드시 존재해야 하기 때문이다. 하지만 암호화폐의 가격이 급격히 상승하고 거래량이 증가하여 송금 자가 낮은 수수료 책정 시 채굴 노드에 의해 승인되지 않거나 시간이 오래 걸리는 문제가 발생한다. 기업에서 비즈니스로 발생한 트랜잭션이 트랜잭션 비용 때문에 저장이 늦어지거나 거부될 경우 문제가 발생할 수 있다.
3. **해킹 범죄 감소**: 기업은 블록체인을 적용하여 해킹 범죄를 감소시킬 수 있다. 기존의 서버를 공격하여 진행되었던 사이버 공격 대상이 P2P 전체를 대상으로 바뀌었으며 해킹을 위하여 투입되는 비용이 증가한다. 기업은 보안을 위해 소요되는 비용보다 블록체인을 도입으로 인한 유지비용이 적다면 블록체인 도입을 고려할 수 있다.
4. **위-변조 불가능한 프로세스 공유**: 일반 사용자들은 기업에서 저장하고 있는 데이터의 무결성에 관해서 확인할 수 있는 방법은 없었다. 기업은 블록체인을 이용하여 데이터를 저장하고 관리하는지에 대하여 프로세스를 공유할 수 있다. 기업과 사용자는 운용하고 있는 데이터에 대한 신뢰성에 대한 공유와 지속적인 관리가 가능하다.

블록체인 표준화 생태계는 하이퍼레저 프로젝트(Hyperledger Project)와 EEA(Enterprise Ethereum Alliance) 그리고 R3CEV로 구성되어있다. 하이퍼레저 프로젝트는 모든 산업에서 사용할 수 있는 블록체인 기술의 표준화 및 발전을 위한 오픈소스 커뮤니티이다. 리

눅스 재단, IBM, VM웨어, 레드햇, 오라클 등이 모여 오픈소스 프로젝트로 진행 중이다. 현재 200개 이상의 회원사가 참여하고 있으며 국내에서는 한국거래소, 예탁결제원, 코스콤 등이 포함되어 있다. 하이퍼레저 프로젝트 중 하이퍼레저 패브릭이 가장 빠르게 성장하고 있으며 159명의 개발자와 IBM과 인텔을 포함한 28개의 기업에서 패브릭 플랫폼을 지원하고 있다. EEA는 이더리움 기반 허가형 블록체인 컨소시엄이다. 150개 이상의 회원을 확보하고 있다. 삼성SDS, SK텔레콤, 더루프, 코인플러그 등이 참여하고 있다. EEA는 이더리움을 엔터프라이즈급 기술로 발전시켜 개인정보, 기밀성, 확장성, 보안 등 다양한 영역에서 연구 및 개발을 제공한다. 또한, 실시간 트랜잭션 처리 등 다양한 플랫폼 프로젝트들이 있다. R3 CEV는 글로벌 은행 컨소시엄이다. 100개 이상의 회원을 확보했다. 하나, 신한, 우리, 국민, 농협은행 등이 회원이다. 하지만 초기 참여자인 골드만삭스 등 대형 금융사의 이탈하여 상황이 좋지 않다.

표 5는 블록체인 유형별 특징을 보인다. 개방형 블록체인과 허가형 블록체인은 큰 차이점은 네트워크에 접근권한이다. 개방형 블록체인은 누구나 네트워크에 참여하고 거래를 형성하고 승인할 수 있다. 허가형 블록체인은 승인된 사용자만 참여가 가능하며 승인된 기관만 거래를 생성이 가능하다. 악의적 참여자에 의한 해킹에 대해서 허가형 블록체인이 공개형 블록체인보다 안전하다.

〔표 5〕 블록체인 유형별 특징

	개방형 블록체인	허가형 블록체인
특징	- 네트워크에 자유로운 참여 가능 - 암호화폐를 이용한 네트워크 유지 및 공유경제 - 트랜잭션을 모든 노드와 공유, 안전한 거래 처리를 위한 프로세스 유지	- 네트워크 노드 참여자를 승인 및 제한 - 암호화폐 부재 - 신속한 트랜잭션 처리, 데이터에 대한 프라이버시 중심
보안성	- 높은 수준의 보안성 유지 - 해킹을 위해 큰 비용 소모 요구	- 낮은 수준의 보안성 유지 (불투명성) - 참여자를 식별하여 해킹방지 - 데이터를 일반인에게 공유하지 않음
적용영역	- 탈중앙형 트랜잭션 처리가 요구되는 영역 - 암호화폐를 이용한 서비스가 가능한 영역 - 일반인들의 참여와 데이터의 공개가 가능한 영역	- 중재자의 역할이 필요하며 트랜잭션 처리가 필요한 영역 - 기업/기관 등 참여자를 사전에 특정할 수 있는 서비스

공개형 블록체인은 채굴을 해서 거래를 증명하고 보상에 대해서 약속한다. 채굴방식으로 PoW(작업증명), PoS(지분증명), DPoS(위임지분증명), PoI(기여증명) 등을 사용한다. 공개형 블록체인은 다수의 사람이 이용하기 때문에 대형 네트워크가 형성되고 다수의 사람이 검증한다. 반면에 허가형 블록체인은 소수의 승인 기관이 거래를 검증 및 수정을 한다. 허가형 블록체인은 작은 네트워크 크기로 인해 거래를 통제 가 가능하지만 투명성과 보안성이 부족하다.

Ⅳ. 결 론

이 논문에서는 블록체인 개발현황과 특징에 대해서 알아보았다. 세대가 증가할수록 기능과 거래 속도 등을 강조하였지만 상대적으로 보안성은 낮아지는 특징을 보였다. 블록체인은 공개형태에 따라서 공개형 블록체인과 허가형 블록체인으로 분류된다. 공개형 블록체인은 사람들에게 네트워크에 자유롭게 참여 가능하여 트랜잭션을 모든 사람과 공유하며 안정적인 거래가 가능하다. 허가형 블록체인은 네트워크에 허가된 사용자만 참여할 수 있으며 변형된 형태의 블록체인을 사용한다. 블록체인의 공개형태에 따라 네트워크 크기가 다르며 투명성과 보안성이 달라졌다. 향후 연구로 마이닝 방법 즉, 작업증명(PoW, Proof -of-work)과 지분증명(PoS, Proof-of-stake) 등에 따른 보안성에 대해 연구를 진행할 예정이다.

참 고 문 헌

[1] 박선종, 김용재, 오석은, "중앙은행 디지털화폐 연구 - 제1부 중앙은행의 디지털화폐 발행 시 법률적 쟁점", 한국은행 금융결제국]

[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008)

[3] https://www.bitcoincash.org/

[4] https://bitcoingold.org/

[5] http://btcd.io/
[6] https://ripple.com/
[7] https://www.stellar.org/
[8] https://litecoin.com/
[9] https://z.cash/
[10] https://getmonero.org/
[11] https://www.dash.org/
[12] https://www.factom.com/
[13] https://zcoin.io/
[14] https://navcoin.org/
[15] https://sia.tech/
[16] https://www.burst-coin.org/
[17] https://storj.io/
[18] https://nem.io/
[19] https://vertcoin.org/
[20] https://www.digibyte.co/
[21] https://www.ethereum.org/
[22] https://qtum.org/
[23] https://www.iota.org/
[24] https://www.cardano.org/zh/home-3/
[25] https://eos.io/

〈저자소개〉

정 현 준 (Hyunjun Jung)
2008년 2월 : 삼육대학교 컴퓨터과학과 졸업
2010년 2월 : 숭실대학교 컴퓨터학과 석사
2017년 8월 : 고려대학교 컴퓨터전파통신공학과 박사
2017 9월~현재 : 광주과학기술원 센서지능화연구센터 연구원
관심분야 : 사물인터넷, 인공지능, 블록체인

이 흥 노 (Heung-No Lee)
정회원
1993년 : University of California 전기공학과 졸업
1994년 : University of California 전기공학과 석사
1999년 : University of California 전기공학과 박사
1999년~2002년 : HRL Laboratories Research Staff Member
2002년~2008년 : University of Pittsburgh Assistant Professor
2009년~현재 : 광주과학기술원 전기전자컴퓨터공학부 교수
관심분야 : 정보이론, 신호처리, 통신/네트워크, 무선 통ㅅ인 및 네트워킹, 압축센싱