Journal of Information Technology and Architecture
Vol. 15. No. 3, September 2018, Pages 357-364

블록체인 기술 및 응용사례

유재필[1] · 신현준[2,*]
[1]KIS채권평가 채권평가실
[2]상명대학교 경영공학과
jaepilryu@kispricing.com; hjshin@smu.ac.kr

(2018년 9월 7일 접수; 2018년 9월 18일 수정; 2018년 9월 25일 채택)

요약: 컴퓨팅 분야에서 다섯 번째 혁신으로 불리는 블록체인 기술 또는 분산원장기술은 최근 몇 년 동안 많은 주목을 받아왔다. 본 논문은 문헌을 바탕으로 최근 세계적으로 관심이 높은 블록체인 기술에 대해서 조사 연구를 하였다. 본 논문은 해외의 다양한 논문에서 기본적인 블록체인에 대한 이론적 배경들을 취합하고 블록체인 기술의 상위적인 종류에 대해서 기술한다. 또한 블록체인의 대표적인 알고리즘인 작업증명 알고리즘, 지분증명 알고리즘 그리고 비잔틴 장애 허용 알고리즘에 대해서 설명하고, 이러한 블록체인 기술이 적용되는 대표적인 분야들에 대해서 그 응용사례를 제시한다.

주제어: 블록체인, 암호화폐, 분산원장기술, 작업증명, 지분증명

Blockchain Technologies and Applications

Ryu Jaepil[1] and Shin Hyun Joon[2,*]
[1]Center for Bond Pricing, KIS Pricing
[2]Dept. of Management Engineering, Sangmyung University

(Received September 7, 2018; Revised September 18, 2018; Accepted September 25, 2018)

Abstract: Blockchain or distributed ledger technology, the fifth innovation in computing, has received much attention in recent years. Based on the literature, this paper has recently investigated the block chain technology, which is of interest to the world. This paper surveys the theoretical backgrounds of basic blockchain in various papers and describes representative blockchain techniques. In addition, we address the typical algorithms of the blockchain, such as the proof-of-work algorithm, the equity proof algorithm, and the Byzantine fault tolerance algorithm, and give examples of blockchain applications in various industry sectors.

Keywords: Blockchain, Cryptocurrency, Distributed Ledger, Proof of Work, Proof of Stake

1. 서 론

초기의 블록체인 기술은 비트코인(Bitcoin), 라이트코인(Litecoin), 피어코인(Peercoin) 등의 상호간의 이체와 이들 스스로의 화폐 기능을 하는 암호화화폐(Cryptocurrency)에 적용되었는데 이는 마치 법정화폐(Fat Currency)처럼 투자나 온라인 이체 그리고 가치의 저장 수단 등으로 이용되었다. 이처럼 블록체인을 기반으로 하는 암호화화폐는 상호간의 연결 그리고 화폐의 환전 및 결제 등을 만족시켰기 때문에 빠른 속도로 발전하게 되었다. 물론 정부 규제 및 보안성 문제 등 아직까지 풀어야할 과제들이 많이 있는 것은 사실이지

*Corresponding author
This research was supported by a 2017 Research Grant from Sangmyung University.

만 블록체인 기술이 가져올 미래 가치는 분명한 것이 사실이다[9]. 때문에 전 세계적으로 블록체인과 관련한 스타트 업(Start Up) 회사들이 많이 생겨나고 있으며 많은 투자 기관에서 블록체인에 대한 투자를 확대하고 있다.

블록체인 시장 규모는 연 평균 약 79%가 성장하여 2022년에는 약 76억 8천만 달러를 넘을 것으로 예상하고 있으며, 이와 파생되는 부가가치는 그 이상일 것으로 전망하고 있다.

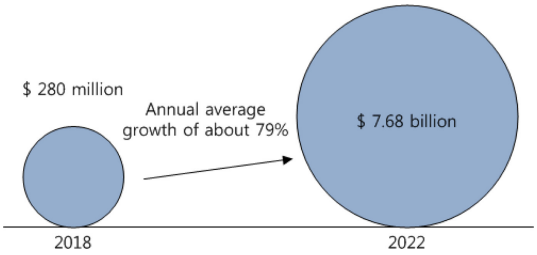

Figure 1. Growth Forecast of the Blockchain

블록체인 기술의 가장 큰 장점은 중앙 데이터 저장 시스템이 아닌 탈중앙화를 지향한다는 것에 있다. 이는 데이터 저장에 있어서 분산화를 해서 거래 장부와 거래 증서를 모든 사용자의 컴퓨터에 분산 저장하며, 새로운 거래가 발생할 때 구성원들이 해당 거래를 인증하기 때문에 보안에 매우 강하다.

Pilkington[12]의 논문에서는 블록체인의 출현과 함께 암호 경제학은 함께 발전해 왔는데 이는 블록체인을 기반으로 한 암호화화폐가 현 제도에서 어떻게 적용될 수 있는지를 자세하게 설명하고 있다. 또한 이 논문은 무허가형 블록체인(Permissionless Blockchain)에서 허가형 블록체인(Permissioned Blockchain)으로 옮겨가는 것에서 신뢰가 가장 중요하며, 무허가형 블록체인 기술의 보안 위험을 해결하는 것은 무엇보다 중요하다고 설명하고 있다.

오랜 기간 동안 비트코인이라는 용어와 블록체인이라는 용어는 서로 혼합되어 사용됐다. Swan[16]은 블록체인 기술의 운영체제, 비트코인 알고리즘 그리고 비트코인을 이용한 거래 등에 대해서 기술하면서 블록체인 기술은 가장 낮은 층을 형성하고 중간층에는 비트코인 알고리즘 그리고 최상층에는 비트코인 거래가 있다고 정의하였다. 또한 디지털 통화 애플리케이션은 블록체인 1.0, 탈중앙화 어플리케이션(Decentralized Applications)은 블록체인 2.0 그리고 최종적으로 통화 및 경제 활동 적용은 블록체인 3.0의 형태로 발전해 가고 있다고 설명한다. Peters[10]의 연구에서는 새롭게 등장하는 블록체인 아키텍처(Architecture), 기존의 데이터베이스와의 차별화 그리고 상호간의 전자화폐 거래 시스템에서 블록체인의 역할에 대한 포괄적인 개요를 상세하게 설명하고 있다.

4차 산업혁명으로 다양한 영역의 융합적 기술이 발전하면서 데이터의 보안 및 관리 등이 중요해지고 있으며, 이에 따라 블록체인 기술을 다양한 분야에 적용시키는 것에 대한 필요성이 높아지고 있다[6].

블록체인 기술의 성장과 함께 가상화폐 시장이 크게 발전하였는데 최근 가상화폐 거래소의 보안 문제 및 정부의 불명확한 규제 등으로 인해서 블록체인에 대한 기술적 내공을 쌓아야 한다는 비판의 여론도 나오고 있다. 이처럼 급속도로 증가한 가상화폐의 투기 열풍으로 인해서 블록체인에 대한 국내 학술적 연구는 해외에 비해서 매우 미흡한 실정이다. 따라서 본 연구는 해외의 블록체인과 관련된 다양한 논문과 보고서 등을 통해서 블록체인에 대한 서베이(Survey) 연구를 진행하고자 하며 이를 바탕으로 향후 다양한 연구가 진행되기를 기대한다.

본 논문의 2장에서는 블록체인의 상위적인 분류를 Satoshi Nakamoto[13], Buterin[1]의 학술 자료 등을 토대로 설명하고, 3장에서는 블록체인에 대한 기본적인 알고리즘에 대해서 설명한다. 그리고 4장에서는 블록체인이 적용되는 분야에 대해서 Zyskind[21]와 Sharples[14] 등의 학술 자료를 바탕으로 설명하고, 5장에서는 블록체인 기술의 향후 과제에 대해서 Trevor Kiviat[17], Peters[10] 등의 학술 자료를 바탕으로 논의한다. 그리고 마지막으로 6장에서는 결론을 제시하고자 한다.

2. 블록체인의 분류

Nakamoto[13]에 의해 제안된 블록체인의 기본적인 핵심 기술은 분산원장기술(Distributed Ledger Technology)이다. 원장(Ledger)은 상호간에 거래를 기록하는 장부인데 이는 각 각의 주체가 독립적으로 기록하고 보관하거나 중앙 관리자 또는 제 3자의 신뢰기관(Trusted Third Party)이 관리한다. 반면 분산원장(Distributed ledger)은 Figure 2에서 보이듯이 네트워크상에서 허가된 참여자가 원장을 함께 기록하고 보관하며, 동일한 전체 원장을 모든 참여자들이 동일하게 공유하고 복제하는 방식이다. 따라서 분산원장은 원장 데이터를 참여

자 모두가 함께 보관하기 때문에 중앙 기관의 보완적 위험을 제거하게 된다는 장점이 있다.

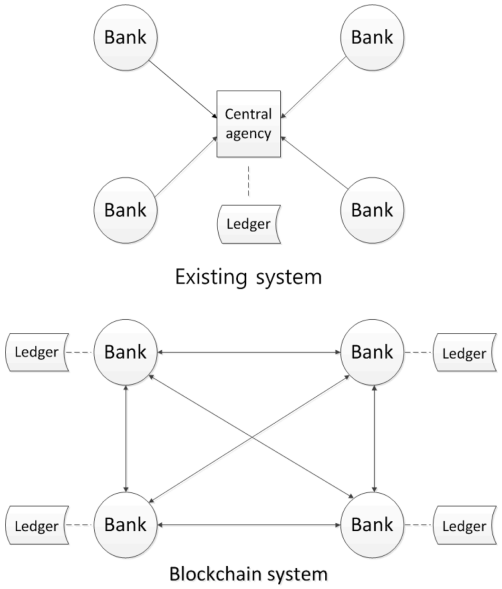

Figure 2. Concept of Distributed Ledger

일반적으로 블록체인은 네트워크에 누가 접근하는지 혹은 블록체인 데이터를 수정할 수 있는 권한이 어떻게 배정되는지 등에 따라서 퍼블릭 블록체인(Public Blockchain)과 프라이빗 블록체인(Private Blockchain)으로 나눠진다. 여기서 전자의 경우에는 무허가형 분산원장(Permissionless Distributed Ledger) 그리고 후자의 경우에는 허가형 분산원장(Permissioned Distributed Ledger)이라고도 정의할 수 있다.

Buterin[1]의 연구에서는 현실 세계에서 퍼플릭 블록체인과 프라이빗 블록체인의 다양한 사례에 대해서 기술하였으며, 더 나아가 컨소시움 블록체인(Consortium Blockchain)의 실효성에 대해서 자세하게 설명하고 있다. Xu[20]의 논문에서는 블록체인 시스템에서 다양한 아키텍처를 구성하는데 블록체인 기술의 적용 가능성 등에 대해서 설명하고 있다. 다음 절에서는 앞서 기술한 퍼블릭 블록체인과 프라이빗 블록체인에 대해서 기술하고자 한다.

2.1 퍼블릭 블록체인

Huaiqing Wang[7]에 의하면 퍼블릭 블록체인은 참여자 모두에게 개방되어 있으며, 누구든지 거래를 할 수 있으며 암호화화폐의 경우에는 채굴에도 참여할 수 있다. 이처럼 퍼블릭 블록체인의 경우에는 누구나 블록체인의 데이터를 읽고, 쓰고 그리고 검증할 수 있는데, 가장 대표적인 사례가 비트코인이다.

비트코인은 참여자 모두가 블록체인을 조회할 수 있으며 데이터의 과거 기록까지 확인할 수 있다. 그러나 퍼블릭 블록체인의 경우에는 다양한 한계점을 내포하고 있다. 퍼블릭 블록체인에서 채택하고 있는 분산합의 알고리즘으로 작업증명(Proof of Work, PoW)이나 지분증명(Proof of Stake, PoS)을 사용하려면 내부 화폐가 필요하다. 퍼블릭 블록체인에서 분산합의 목표는 결국 거래 내역을 검증해 신뢰할 수 있는 블록을 만들 수 있는 노드(Node)를 선택하는 것이며 이러한 수고를 하는 대가가 필요한데 이러한 과정을 채굴(Mining)이라고 한다. 또한 퍼블릭 블록체인 형태의 가상화폐는 익명성(Pseudonymity) 및 투명성(Transparency)을 기반으로 하기 때문에 은행 등의 금융권에서는 도입에 근본적인 부작용이 발생할 수 있다. 더불어 비트코인의 거래는 10분 간격으로 블록을 통해 기록되는데 각 블록에 기록할 수 있는 데이터의 크기는 최대 1MB로 크기가 매우 작다. 기존 금융시스템의 결제(Settlement) 속도보다는 빠르겠지만 지급(Payment) 속도보다는 매우 느린 것이 현실이다. 예컨대 은행 거래의 경우에는 이체를 하면 수령인이 즉시 출금을 할 수 있지만 블록체인에서는 최소 약 10분에서 60분이라는 시간이 소요된다. 거래 시스템 또한 비트코인의 경우에는 초당 4번에서 7번의 거래를 처리하지만 일반 비자카드(visa card)의 경우에는 초당 약 1만 번 이상의 결제를 처리하기 때문에 이와 비교했을 때 비트코인이 글로벌(Global) 지급 시스템이 되기엔 어려움이 있다.

2.2 프라이빗 블록체인

영국의 클리어매틱스(Clearmatics)는 비트코인이나 이더리움과 같은 퍼블릭 블록체인의 한계점을 극복하기 위해서 금융기관을 대상으로 블록체인을 개발하는 대표적인 기업이다. Buterin[1]도 연구를 통해서 금융기관을 위한 프라이빗 블록체인의 필요성이 점점 커지고 있으며 이에 맞는 블록체인 환경이 발전해야한다고 주장했다.

프라이빗 블록체인은 읽기, 쓰기 그리고 참여할 수 있는 참여자를 사전에 지정할 수 있으며, 특정 주체를 새로 참여시키거나 기존 참여자를 제거할 수 있다. 또한 목적에 따라서 참여자 모두가 자료를 조회할 수 있

고 기록은 특정 참여자만 가능하게 할 수 있으며, 읽기와 쓰기 모두를 특정 참여자만 가능하게 하는 경우 등 다양한 설계가 가능하다는 장점이 있다. 즉 프라이빗 블록체인은 접근 권한에 있어서는 유동성이 퍼블릭 블록체인보다 높다.

Table 1은 퍼블릭 블록체인과 프라이빗 블록체인의 차이점을 나타내는 표인데 대체적으로 퍼블릭은 앞서 설명했듯이 읽기, 쓰기 등에서의 권한이 프라이빗 블록체인에 비해서 자율적인 것을 알 수 있다.

Table 1. Types and Differences of BlockChain

	Public Blockchain	Private Blockchain
Read	All participants	Allowed Participants
Verification	All participants	Allowed organizations
Save	All participants	Trading partner
Agreement	PoW, PoS	BFT series
Scalability	Limited	Flexible
Speed	7~20 TPS	More than 1000 TPS
Example	Bitcoin, Etherium	R3 Corda, DAH

더 나아가 프라이빗 블록체인은 현재 금융기관들이 보유하고 있는 신용 및 유동성 그리고 운영 및 법률 등에 대한 위험을 최소화 할 수 있을 것이다. 특히 막대한 자금이 은행에 묶일 필요가 없어지고 대금이 부족할 경우 결제가 발생하지 않기 때문에 유동성 위험이 줄 것이다. 그리고 다양한 금융 기관의 암호학적으로 증명된 거래 기록들이 비가역적인 단일성 원장에 기록되고 규제 기관들이 실시간으로 그 거래들을 확인 및 열람할 수 있기 때문에 자금세탁과 법적 분쟁 등의 법률적 위험들도 축소될 것으로 예상한다. 이 밖에도 원장 데이터베이스를 분산화해서 저 비용으로 해킹에 대한 보안성을 유지할 수 있고, 계약의 조건 및 과정을 표준화(Standardization)하면 스마트 계약(Smart Contract)을 적용해 업무를 단순 및 자동화할 수 있다.

3. 블록체인의 알고리즘

Cachin[2]의 보고서는 다양한 블록체인의 합의 알고리즘을 설명하고 있는데 대표적으로 작업증명(PoW)와 지분증명(PoS)가 있다. 본 장에서는 이러한 합의 알고리즘에 대해서 가상화폐에 적용하여 설명하고자 한다.

3.1 작업증명 알고리즘

작업증명 알고리즘은 비트코인에서 사용되는 합의 알고리즘으로써 특정한 트랜잭션(Transaction)이 발생했을 때 해당 트랜잭션의 신뢰성 여부에 대한 검증역할을 수행한다.

일반적으로 채굴은 임의의 넌스(Nonce) 값을 대입하여 블록 해시(Hash) 결과 값을 생성하고 이 값이 제시된 목표 값(Target)보다 작은 블록 해시를 찾는 과정이다. 여기서 정확한 목표 값을 찾기 위해서는 넌스의 값을 0부터 1씩 더하면서 목표 값보다 작은 결과 값이 나오기까지 무한적으로 반복 작업을 한다.

이처럼 일련의 과정들을 1초에 몇 번을 수행할 수 있는지에 대한 정량적 정보를 해시파워(Hash Power)라고 정의하며, 해시파워가 높은 사용자가 더욱 많은 문제를 풀 수 있기 때문에 보다 더 많은 목표 값을 찾을 수 있다. 즉 해시파워가 높은 참여자가 더욱 많은 보상을 받을 수 있으며 이것이 작업증명 알고리즘의 특징이다[4]. 그러나 이러한 작업증명 알고리즘은 채굴 난이도가 높아지면서 연산에 필요한 고 사양 장비가 필요하며, 이를 작업하기 위한 전력 소모비용이 높다는 단점이 있다.

3.2 지분증명 알고리즘

지분증명 알고리즘은 앞서 기술한 작업증명의 한계점(i.e., 과도한 컴퓨팅 파워)을 보안하기 위해 고안되었는데 이는 단지 가상화폐를 지갑에 넣고 온라인 상태를 유지하게 된다면 일정 시간이 지난 후 해당 화폐의 지분을 증명한 것에 대한 보상을 받는다는 개념이다. 이 보상은 참여자가 갖고 있는 지분의 양과 비례한다. 즉 특정 화폐에 대해서 소유한 지분에 따라서 블록 생성 권한이 결정되는 알고리즘이다. 예컨대 어떤 참여자가 특정 화폐의 20%의 지분을 갖고 있다면 다음 블록을 만들 확률이 20%라는 것을 의미한다. 또한 어떠한 블록이 진짜인지를 의사 결정하는 것에서도 지분을 활용한다[12]. 이는 주식 시장에서 보다 더 많은 주식을 보유한 주주가 더 높은 의결권을 갖는 것과 유사하다. 단 지분증명 알고리즘은 Nothing at Stake 문제가 발생한다. 이는 두 블록이 동시에 만들어지면 어떠한 블록이 진짜인지 투표하는 과정에서 양쪽 모두에게 투표하는 것이다. 이는 자기 자신의 지분과 모두 동일하기 때문에 양쪽 모두에게 투표해도 손해 보는 일이 없다.

또한 해시파워에 의존하는 합의 알고리즘을 보안하기 위한 것도 있지만 지분을 많이 참여자에게 집중화가 될 수 있다는 단점도 내포하고 있다.

3.3 비잔틴 장애 허용 알고리즘

블록체인은 비잔틴 장군 문제(The Byzantine Generals Problem)와 밀접한 연관을 갖고 있다. 비잔틴 장군 문제는 다수의 아군 장군들이 동일한 목표 지점을 동시에 공격하면 전쟁에서 승리할 수 있는데 이를 합의하는 과정에서 첩자가 정보를 장군들에게 잘못 전달해서 발생하는 문제를 뜻한다.

블록체인 네트워크상에서도 새로운 블록이 생성되는 과정에서 악의적인 공격으로 인해서 잘못된 블록이 생성될 수 있다. 이는 블록 안에 트랜잭션이 변형되어 막대한 손실로 이어질 수 있기 때문에 이를 해결할 수 있는 합의 알고리즘이 필요하다.

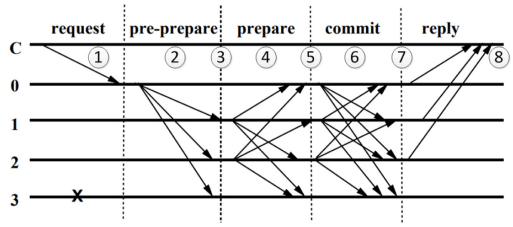

Figure 3. The process of settlement of PBFT

프랙티컬 비잔틴 장애 허용(Practical Byzantine Fault Tolerance; 이하 PBFT) 알고리즘의 핵심은 일부 특정한 노드의 결과 값이 달라도 어느 정도 이상의 값이 동일하면 합의된 것으로 간주하는 것이다. 즉 다수결의 원칙에 의존하는 합의 알고리즘이다. PBFT는 Miguel Castro[8]에 의해서 처음으로 공개되었는데 Figure 3는 해당 논문에서 명시한 그림을 참고했다.

Figure 3의 ①~⑧ 과정을 간략하게 설명하면 다음과 같다.

①: Client가 현재 상태에 대한 confirm을 Primary 노드에 요청함.
②: Primary 노드는 트랜잭션을 모아서 생성한 블록을 다른 노드들에게 모두 보냄.
③: 모든 노드가 Primary 노드로부터 블록을 수령함.
④: 블록을 받은 노드들은 자신이 블록을 받았다는 것을 다른 노드들에게 보냄.
⑤: 각 노드는 다른 노드들이 블록을 받았는지 여부를 취합하고, 이 수가 2/3 이상이면 블록을 검증함.
⑥: 블록의 유효성을 검증하고 결과 값을 다른 노드들에게 모두 보냄.
⑦: 각 노드는 다른 노드들이 보내준 블록에 대한 유효성 검증 정보를 취합하고, 전체의 2/3를 초과하여 동일한 결과 값을 보냈을 경우 해당 결과 값을 참으로 인지함.
⑧: 현 상태(State) 값을 Client에게 보내줌.

하지만 PBFT 알고리즘은 적은 노드 수를 유지해야 하며, 탈중앙화를 지향하지는 않는다는 단점이 있다. PBFT 알고리즘을 사용하고 있는 대표적인 암호화화폐는 NEO가 있다.

4. 블록체인 기술의 적용

최근 몇 년간 세계적으로 비트코인에 대한 관심이 높아지면서 블록체인 기술도 함께 발전해 왔다[3]. 또한 비트코인과 유사한 NXT, Open Assets, Colored Coins 등과 같은 가상화폐들도 탄생했다.

Pilkington Mark[12]도 블록체인 기술이 가상화폐를 넘어서 투표, 상품 거래, 교육 등 다양한 산업에 적용이 가능하다고 주장했다. 이런 동향(Trend)에 맞게 미국의 대표적인 75개의 금융기관들 중에서 약 50% 이상이 이미 블록체인 기술에 투자했다고 발표했다. 이러한 사실은 블록체인 기술이 가상화폐를 넘어서 다양한 분야에서 시도되고 있다는 것을 의미한다. 본 장에서는 이처럼 블록체인 기술이 적용 가능한 다양한 분야에 대해서 간단하게 설명하고자 한다.

4.1 가상화폐

전 세계적으로 많이 사용되고 있는 통화에는 크게 미국 달러, 영국 파운드 등 정부에 의해 그 가치가 보장되는 화폐이다. 이러한 통화는 물리적 인 다른 자산에 의존하지 않는다. 상품 화폐는 금이나 은과 같이 다양한 시장에서 합리적인 거래가 가능한 제 2의 화폐이다. 그러나 비트코인과 같은 가상화폐는 앞서 기술한 화폐의 어떠한 범주에도 해당하지 않는다[17].

가상화폐는 암호화 방식을 사용하여 거래를 안전하게 할 수 있다. 이는 기존의 전통적인 화폐들보다 저장 비용을 최소화 할 수 있다. 현재 가상 화폐는 약 1,300개이며, 이들에 대한 시가총액은 약 4,500억 달러에 달

한다. 이 중에서 비트코인의 시가총액이 약 5%를 차지하고 있다. 아직 정부의 규제 및 법률 등에 의해서 실효성은 다소 부족하지만 다양한 화폐들이 갖고 있는 잠재적 기능은 환전 수수료, 결제 등에 있어서 큰 이점을 갖고 올 것이라는 것은 명백하다.

4.2 교육 분야

Sharples[14]는 세계적으로 보수적으로 발전해온 교육 분야에 블록체인 기술을 적용하면 큰 혁신을 갖고 올 것으로 예상하고 있다. 교육 기관에서는 교과과정을 블록체인 상에서 구현할 수 있고 학생들은 스스로 필요한 교과과정을 수료하면서 맞춤형 교육을 받을 수 있다. 또한 이 과정에서의 보상 시스템도 객관적인데 모든 평가는 교육 기관의 정성적인 판단이 없이 직접적인 평가로 진행되기 때문에 더욱 좋은 교육을 제공한 교육자와 더 좋은 학업 성적을 받은 학생은 더 많은 보상을 받게 된다. 더불어 학생들은 교육 과정에서의 결과물을 업로드(Upload)하는 등 구체적이고 객관적인 관리를 받을 수 있다. 이런 블록체인 기술에 기반을 둔 교육 시스템은 높은 비용과 물리적인 접근성으로 인해서 교육을 받지 못했던 사람들에게도 기회를 줄 수 있다.

4.3 금융 분야

비트코인에 대한 관심이 높아지면서 처음에 대부분의 많은 금융 기관에서는 블록체인 기술이 큰 위협으로 여겨졌다. 하지만 지난 몇 년 동안 금융 기관들은 블록체인 기술을 그들에게 유리한 방식으로 적용될 수 있도록 많은 노력을 하였다[5]. IBM에서는 전 세계 은행의 약 65%가 3년 이내에 블록체인 기술을 도입할 것이라고 예측했다. 블록체인 기술을 통해서 금융 거래에 있어서 소요되는 시간을 최소화할 수 있고 인증과 검증과정에서 필요한 중개 또는 중앙기관의 역할이 축소되면서 매매 비용이 절감될 것이다. 또한 거래 과정의 모든 자료를 기록하고 공유되기 때문에 거래 상대방에 대한 위험과 부정 거래 등을 줄일 수 있다. 더불어 실시간으로 거래 과정을 관찰할 수 있기 때문에 감독의 효율성도 높아질 수 있다. 이미 비자카드는 기업을 대상으로 당일 해외송금 서비스를 조만간 제공할 예정이며, 이는 미국의 Chain 사와 공동 개발한 ChainCore 기술을 적용하였다. 마스터카드(Master Card) 또한 마스터카드 연구소에서 블록체인 API 서비스를 제공하고 있다. 중국의 Union pay 사는 IBM 사와 블록체인 기술을 적용해서 고객의 포인트 점수를 다양하게 사용할 수 있는 시스템을 개발하고 있다. 그 외 HSBC, CITI 은행 그리고 SC 은행은 블록체인 기술에 의한 금융 거래를 은행 간 서로 공유하는 환경을 개발하기로 합의했다. 그밖에 Peters G.W[11]의 논문에서 블록체인 기술이 금융 분야에 끼칠 기대 효과에 대해서 자세하게 기술하고 있다.

4.4 의료 분야

블록체인 기술은 의료 분야의 많은 범위에 적용가능하다. 특히 환자의 진료 기록, 신양 개발에 대한 임상실험, 의약품의 배송 관리, 인간의 유전학적인 정보 기록 그리고 의료 보험 청구 및 심사 등이 있다. 현재 환자의 진료 기록은 전자기록저장(Electronic Health Records, EHR)이나 종이 차트에 기록하고 있다. 그러나 블록체인 기술을 적용하면 신뢰성, 보안성, 접근성 등을 높일 수 있으며, 개개인의 의료 정보를 탈중앙화 방식으로 중간 판매상 없이 정보 활용이 가능해진다[18]. 예컨대 23andMe 사는 약 300만 명에 달하는 유전 정보를 갖고 있으며 이 정보를 제약사를 통해서 수익을 창출하고 있지만 이 정보를 원천적으로 제공한 사람들은 전혀 판매 수익을 얻을 수 없다. 또한 운동, 금주, 금연 등 건강한 몸을 유지하기 위한 암호화화폐의 보상제도 등을 통해서 시민들에게 동기부여를 제공할 수 있다. 실제 미국의 헤이버(Hayver)나 소버코인(Sovercoin)을 통해서 금주를 유도하고 소변검사 등을 통해서 금주를 성공하면 이러한 가상화폐로 보상하기도 한다. 그리고 오래 걸은 만큼 스윗코인(Sweatcoin)을 지급하는 경우도 있다. 이처럼 블록체인 기술은 제도적, 기술적 그리고 사회적으로 다양한 난제를 해결하면 의료 분야에서 다양하게 활용되어 질 것이며, 이는 기존의 의료 서비스 환경에서 다소 부족한 환자들의 권한과 의사결정권 등을 더욱 강화할 것으로 기대된다[19].

4.5 기타 분야

본 연구에서 설명한 분야 말고도 블록체인 기술은 매우 다양한 분야에 접목시킬 수 있다. 예컨대 투표, 과세, 스마트시티(Smart City) 등이 있다[15]. 특히 중국과 미국에서는 주거 환경 및 도시 공공 서비스에 블록체인

기술을 적용시키기 위해 많은 투자를 집행하고 있다. 중국은 약 1,000여 개에 달하는 스마트시티 조성계획을 수립하였고 미국의 델라웨어(Delaware)주는 2016년에 이미 블록체인 이니셔티브(Delaware Blackchain Initiative)를 발족하였다. 이는 델라웨어 주의 공공 서비스 영역에서 블록체인 기술인 스마트 계약(Smart Contract)을 활용할 수 있도록 설계되었다. Peters G.W[11]와 Huaiqing Wang[7]의 논문에서는 앞서 설명한 블록체인 기술의 적용 분야 외로 다른 분야에 대해서도 자세하게 설명하고 있다.

5. 결 론

블록체인 기술의 혁신성은 수많은 실험과 논쟁에서 이미 검증되었다. 때문에 이 기술을 정부기관 및 기업에 적용시키기 위해서 많은 투자와 연구가 병행되고 있다. 그러나 블록체인 기술의 발전 속도가 규제를 넘어서면서 많은 부작용이 발생할 수 있다는 비판의 목소리가 많다[2]. 예컨대 비트코인 거래를 통해서 마약 거래, 자금 횡령 등의 불법적인 활동은 비트코인 거래가 가능해지면서 지속적인 증가를 보이고 있다. 또한 비트코인 가격의 변동성이 높기 때문에 화폐의 기능이 떨어지며 이미 투기성이 높은 거래 시장의 환경이 조성되어 졌다. 따라서 앞으로 블록체인 기술과 연관된 모든 것에 대한 구체적인 규제를 정부에서 수립해 가는 것이 중요하며 이를 바탕으로 블록체인 기술이 병행적으로 함께 발전해 가야 할 것으로 사료된다.

본 연구에서는 블록체인 기술이 매우 다양한 분야에 적용되는 것을 감안해서 블록체인 기술의 상위적인 이론적 배경에 대해서 설명하고 해외 다양한 논문, 학술자료 등을 참고하여 논문을 구성하였다. 따라서 블록체인에 대해서 관심이 있는 많은 독자들이 본 논문을 통해 블록체인 기술의 기본적 이해를 도모하고 기술 발전의 현황을 점검할 수 있는 계기가 되길 바란다.

REFERENCES

[1] Buterin, “On Public and Private Blockchains”, blog.ethereum.org/2015/08/07/on-public-and-private-blockchains, 2015.

[2] Cachin et al., “Blockchain, cryptography, and consensus”, IBM Research, 2017.

[3] Crosby et al., “BlockChain Technology : Beyond Bitcoin”, Applied Innovation Review, No. 2, 2016.

[4] Decker and Wattenhofer, “Information Propagation in the Bitcoin Network”, International Conference on Peer-to-Peer Computing, 2013.

[5] Fanning, “Blockchain and Its Coming Impact on Financial Services”, The Journal of Corporate Accounting and Finance, Vol. 27, No. 5, pp. 53-57, 2016.

[6] Hyeong-seog Kho, Hong-je Lee, Hwa-yeon Lim, Kyeong-seok Han, “A Study on the Strategies of Big Data Resource Management in the 4th Industrial Revolution”, Journal of Information Technology and Architecture, Vol. 15, No. 2, pp. 119-131, 2018.

[7] Huaiqing Wang and Kun Chen and Dongming Xu, “A maturity model for blockchain adoption”, Financial Innovation, 2016.

[8] Miguel Castro and Barbara Liskov, “Practical Byzantine Fault Tolerance”, Appears in the Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999.

[9] Park Yeon-a, Kim Jong-hyun, Kim In-kyu, “A Case Study on the Application of Ethereum-Blockchain Technology for Electronic Voting System”, Journal of Information Technology and Architecture, Vol. 15, No. 2, pp. 201-218, 2018.

[10] Peters, G. and Vishnia Guy, “Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges”, ASTRI, 2016.

[11] Peters, G. W. and Panayi, E., “Understanding Modern Banking Ledgers Through Blockchain Technologies : Future of Transaction Processing and Smart Contracts on the Internet of Money”, Banking Beyond Banks and Money, pp. 239-278, 2016.

[12] Pilkington Mark, “Blockchain Technology : Principles and Applications”, Research Handbook on Digital Transformations, 2016.

[13] Satoshi Nakamoto, “Bitcoin : A Peer-to-Peer Electronic Cash System”, http://www.bitcoin.org, 2008.

[14] Sharples, M. and Domingue, J., “The Blockchain and Kudos : A Distributed System for Educational Record”, Adaptive and Adaptable Learning, 2016.

[15] Sun et al., “Blockchain-based sharing services What blockchain technology can contribute to smart cities”, Springer, 2016.

[16] Swan Melanie, “Blockchain : Blueprint for a new Economy”, 2015.

[17] Trevor Kiviat, “Beyond Bitcoin : Issues in Regulating Blockchain Transactions”, HeinOnline.org, 2015.

[18] Xia et al., “Trust-less Medical Data Sharing Among

Cloud Service Providers Via Blockchain", IEEE, Vol. 5, pp. 14757 - 14767, 2017.
[19] Xiao Yue et al., "Healthcare Data Gateways : Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control", Journal of Medical Systems, 2016.
[20] Xu et al., "A Taxonomy of Blockchain-Based Systems for Architecture Design", International Conference on Software Architecture, 2017.
[21] Zyskind et al., "Decentralizing Privacy : Using Blockchain to Protect Personal Data", 2015 IEEE Security and Privacy Workshops, 2015.

유재필(Jae Pil Ryu)
상명대학교 학사, 석사, 박사
현재 : KIS채권평가 채권평가실 선임연구원
관심분야 : 금융공학, 데이터마이닝, 블록체인
이메일 : jaepilryu@kispricing.com

신현준(Hyun Joon Shin)
고려대학교 학사, 석사, 박사
미국 Texas A&M 대학교 연구원
(주)삼성전자 책임연구원
현재 : 상명대학교 경영공학과 교수
관심분야 : 금융공학, 조합최적화 응용, 데이터마이닝, 블록체인
이메일 : hjshin@smu.ac.kr