ISSN 2233-6583

18-01

KISDI

Premium Report

블록체인의 다변화: 채굴 없는 블록체인의 확산

남 충 현

정보통신정책연구원 부연구위원

KISDI 정보통신정책연구원

KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

KISDI
18-01
2018. 2. 19
Premium Report

블록체인의 다변화: 채굴 없는 블록체인의 확산

남 충 현
정보통신정책연구원 부연구위원

블록체인의 다변화: 채굴 없는 블록체인의 확산

남 충 현
정보통신정책연구원 부연구위원
*namch@kisdi.re.kr, 043-531-4180
*연세대학교 경제학과 학사, 동 대학원 석사
*University of Warwick 경제학박사

요약문

블록체인은 비트코인에서 중개기관을 거치지 않은 개인간의 P2P 거래의 신뢰성을 담보하기 위하여 처음으로 고안되었다. 비트코인은 승인을 기다리는 신규 거래들을 블록이라는 단위로 모아서, 작업증명이라는 채굴 과정을 거쳐 승인을 받게 하고, 이전에 승인받은 블록에 이어 붙여서 체인을 만드는 식으로 블록체인 네트워크의 신뢰성을 유지하도록 하였다. 그러나, 퍼블릭 블록체인으로 불리는 이러한 구조는 누구나 작업증명만 통과하면 승인권한을 가진다는 개방성을 부여하는 반면 거래 처리 용량의 제한으로 인한 확장성 부족 및 장부에 기입하는 데이터의 포맷 한정, 작업증명(채굴) 과정에서의 막대한 비용 발생 등과 같은 커다란 문제들도 초래하였다.

따라서, 비트코인에 처음 등장한 블록체인 기술이 금융, 의료, 무역, 공공행정 등 다양한 분야로 응용되는 과정에서는 프라이빗(Private) 블록체인이라 불리는 변형된 형태의 블록체인이 주를 이루게 되었다. 이는 비트코인 등의 퍼블릭 블록체인이 작업증명 등 채굴과정만 거치면 누구에게나 거래 승인권한을 주는 반면에, 네트워크의 운영주체 등 검증자(Validator) 역할을 하는 사람에게만 거래의 승인을 주는 시스템이며, 네트워크에 참여할 자격에도 제한을 두고 있다. 이러한 변형의 결과 작업증명을 통한 채굴 과정이 불필요하게 되었으며, 더욱 빠른 거래속도를 달성할 수 있게 되었다. 동시에 의료기록과 같이 용도에 맞는 특화된 데이터를 장부에 써넣는 것도 더욱 용이해진다.

그러나, 이러한 변형은 중개기관 등 중앙의 권위에 의지하지 않고서도 개방형 거래 네트워크의 신뢰를 확보한다는 원래의 원칙을 어느 정도 타협하는 것을 의미하며, 비트코인과 같은 개방성과 탈중앙화를 기대할 수는 없다. 그럼에도 불구하고, 프라이빗 블록체인 역시 장부가 다수에게 분산되어 보안성이 향상되며, 이미 쓰여진 기록을 사후에 무단으로 수정하는 것이 매우 어려워 기록의 신뢰성이 높아진다는 점에서는 블록체인의 고유한 장점을 유지하고 있다.

이렇듯 블록체인은 다양한 형태로 진화하고 있으므로, 블록체인 기술을 적용할 때는 무엇이 가장 목적에 적합한 형태인지를 잘 고려해야한다. 또한 프라이빗 블록체인의 경우에는 시스템 전체의 신뢰도는 운영 주체의 신뢰도에 의지하므로, 참여자의 신뢰를 얻을 수 있는 시스템 운영 가버넌스의 룰을 정립하는 것이 필수적이다.

1. 서 론

◆ 비트코인과 퍼블릭 블록체인

● 비트코인에서 금융기관 등 중앙의 권위에 전혀 의존하지 않는 완전한 P2P 온라인 거래를 달성하기 위해 블록체인 기술이 최초로 개발됨

– 중앙 서버가 없는 개인 간의 P2P 온라인 결제는 토큰이라 불리는 디지털 화폐를 한 개인이 다른 개인에게 이체한다는 송금 메시지가 다른 모든 참여자들에게 발송되는 방식으로 이뤄짐

※ 이 송금 메시지를 수신한 다른 참여자들은 자신이 보유한 거래내역 장부의 내용을 이 메시지에 맞추어 자동적으로 업데이트 함

– 같은 토큰을 두 번 사용하는 이중지불은 기존의 P2P 네트워크에서는 방지하기 어려웠음

– 비트코인은 블록체인 기술을 사용하여 중앙의 서버 등 관리주체 없이도 이중지불 문제를 해결한 최초의 완전한 P2P 결제 시스템이며, 누구나 거래 장부에 접근 권한을 가진다는 점에서 퍼블릭 블록체인에 속함

● 비트코인의 퍼블릭 블록체인 기술은 장부의 분산 및 기록의 비가역성으로 보안성의 향상을 가져오지만 과도한 채굴비용 등의 비효율성도 수반함

– 거래 장부가 특정 서버에 집중된 것이 아니라 모든 사용자의 컴퓨터에 분산되어 저장되며, 한번 쓰여진 기록은 다시 고쳐 쓸 수 없기 때문에 높은 보안성을 가짐

– 작업증명에 의한 채굴 과정을 통하여, 신뢰할 수 없는 참여자조차도 전체 네트워크의 신뢰성에 기여할 수 있는 인센티브 구조를 구현함

– 반면, 비트코인 채굴을 위한 대량의 컴퓨터 가동비용 및 막대한 전력 소모가 필요하며, 거래 처리량이 제한된다는 비효율적 요소도 있음

◆ 블록체인의 다변화

● 프라이빗 블록체인은 거래 장부를 분산한다는 점은 같으나, 작업증명과 채굴 과정을 생략하고 대신에 중앙의 관리주체가 거래의 승인 및 블록 생성 권한을 보유함

– 많은 연산을 필요로 하는 작업증명과 채굴 과정이 불필요해지므로 거래 속도의 대폭 향상 및 비용 절감이 가능해짐

※ 프라이빗 블록체인에도 토큰(가상화폐)가 존재하는 경우가 있으나, 비트코인과 달리 참여자가 직접 채굴하지 않고 시스템 관리주체에 의해 발행됨

– 거래 장부에 가상화폐 송금 내역 뿐 아니라, 의료정보 등 비금전적 데이터도 포함될 수 있음
– 해당 목적에 부합하는 특화형 설계가 보다 용이하며, 금융, 의료, 무역 등 다양한 분야에 폭넓게 응용이 가능함
– 그러나, 중앙의 권위에 의지하지 않고 모든 사람이 자유롭게 참여한다는 비트코인의 원칙은 타협하게 되었음

● 컨소시움 블록체인은 프라이빗 블록체인과 같이 참여 자격에 제한이 있지만 시스템의 관리 주체가 복수의 관계자의 협의체라는 점이 차별점임

– 채굴과정이 불필요하며 퍼블릭 블록체인보다 거래속도가 빠르다는 프라이빗 블록체인의 특징을 공유함
– 복수의 이해관계자와 운영주체가 장부 권리 권한을 공동으로 행사하면서 같은 거래 장부 데이터를 공유함

2. 블록체인의 개념

◆ 비트코인: 블록체인의 원형 제시

● 비트코인은 중개기관의 권위에 전혀 기대지 않으면서 거래 장부를 보유한 개인들 간의 직접적 거래가 이뤄지는 최초의 완전한 P2P 온라인 결제시스템임

– P2P 온라인 결제 네트워크에서는 토큰이라 불리는 디지털 화폐를 한 개인이 다른 개인에게 전송하며, 이 송금 메시지가 다른 모든 참여자들에게 전송되는 방식으로 송금이 이뤄짐

※ 토큰(디지털 화폐)의 보유자는 암호화된 고유키 (유료 SW의 인증번호와 유사)를 보유하며, 송금 메시지에 이 고유키가 포함되어야만 거래가 유효함

– 가지지 않은 토큰을 전송하는 부정행위는 전송된 토큰의 암호키를 확인하여(디지털 서명) 쉽게 방지 가능하지만, 실제로 보유한 토큰을 두 번 사용하는 이중지불을 방지하는 것은 매우 어려움

– 동일한 토큰의 전송 메시지를 두 번 발송한다면, 나중의 것을 취소해야 이중지불을 방지할 수 있지만, 중앙 서버가 존재하지 않는 P2P 네트워크에선 거래의 선후순서를 정확히 알 수 없음

● P2P 네트워크에서 시간의 표준을 부여하는 권위가 없기 때문에, 거래 기록을 모은 블록들을 순서대로 연결해 체인(블록체인)을 만드는 방식으로 거래의 선후 순서를 판정함

– P2P 네트워크에서는 거래 메시지가 모든 참여자(노드) 들에게 전송될 때 지연이 발생하며, 또한 서로 다른 시스템 시계(개별 컴퓨터에서 임의적 조작이 가능)를 가지고 있기 때문에 통일된 시간 기준이 부재함

– 비트코인에서는 P2P 상의 메시지 전달 지연을 감안, 약 10분 간격으로 최근 거래 메시지들을 모아 하나의 블록을 만들며, 나중에 만들어진 블록이 앞의 블록에 연결되며 체인(블록체인)을 구성함

- 블록이 새로 생성되는 시간 간격을 일정하게 하도록, 전체 네트워크가 참여해서 푸는데 약 10분이 걸리는 수학적 퍼즐을 풀어서 맞춘 참여자(노드)만이 새 블록을 생성할 권한을 부여함
- 이렇게 수학적 퍼즐[1]을 맞추어 새로운 블록을 만들고 승인 대기 중인 거래 메시지들을 써넣는 과정을 작업증명(Proof Of Work)이라고 함
- 블록들이 연결된 체인 내에서 같은 블록에 속하면 동시에 이뤄진 거래로, 더 앞의 블록에 소속된 거래는 더 먼저 발생한 거래로 간주함

● 작업증명은 거래들의 선후 순서를 조작하는 것을 어렵게 하여 이중지불을 억지하는 역할을 하며, 이에 참여하는 보상으로서 가상화폐(비트코인)를 지불함

- 작업증명을 하여 블록을 생성하기 위해서는 연산장치를 구동하기 위한 비용(전기료 등)이 들기 때문에, 새로 생성된 비트코인을 보상으로 제공하며 이를 비트코인 채굴(mining)로 부름
- 비트코인 네트워크에서 유일한 시간의 표준은 블록체인의 시작 블록에서부터 몇 번째의 블록에 위치하느냐의 여부임
- 서로 다른 두 개의 체인이 대립하면, 중앙의 권위가 진본을 판별해주는 대신에 더욱 길이가 긴 체인이 (더 오래전에 생성되었을 것이므로) 진본 체인으로 간주 됨
- 그러나, 전체 네트워크를 압도하는 연산능력으로 빠르게 블록을 만들어내서 진본 보다 더욱 긴 조작된 체인을 만들어내면 시간의 순서를 조작하여 진본(더 오래전에 만들어진)으로 승인될 위험이 있음
- Satoshi Nakamoto(2008)는 블록체인의 기록을 위조하려는 자는 그동안 전체 참여자들이 함께 쌓아온 거대한 누적 연산량과 대결해야하기 때문에 거의 불가능하다는 것을 보임

1) 비트코인의 작업증명은 Hash function(언제나 같은 길이의 숫자가 출력값)이라는 변환 함수를 활용하여, 일정한 목표치 이하의 출력 값을 산출하는 입력 값을 무작위로 찾아내는 식으로 이뤄진다(비밀번호를 모를 때 반복 시도해서 찾아내는 것과 유사함). 출력값의 목표치를 낮출수록 난이도가 높아지며, 채굴에 참여하는 컴퓨터들의 전체 연산력이 높아지면 이 난이도를 상향 조정한다.

◆ 비트코인의 블록체인의 특징

● 비트코인의 블록체인은 거래장부가 모든 참여자에게 공유되며, 누구나 자유롭게 거래 장부에 읽고 쓸 수 있는 퍼블릭(Public) 블록체인임

– 기존의 온라인 거래는 금융기관이나 PayPal과 같은 중개기관의 권위에 대한 신뢰에 의존하여 거래의 신뢰성을 보장하며, 따라서 권위를 인정받지 못한 참여주체들은 거래 장부에 대한 접근 권한이 제한 됨
– 반면, 비트코인은 작업증명 과정을 통해서, 그 누구도 장부를 위조하는 것이 본인에게 이익이 되지 않도록 함으로써 신뢰할 수 없는 참여자들 조차도 전체 네트워크의 신뢰도를 높이는데 기여하도록 함
– 라인홀트 니버가 도덕적 개인이 모여 비도덕적 집단을 만들 수 있다고 경고한 반면, 비트코인은 신뢰할 수 없는 개인이 모여 신뢰할 수 있는 네트워크를 만들어내는데 성공함
– 누구도 신뢰할 필요가 없기 때문에, 누구에게나 똑같이 자유롭게 거래 장부를 공유할 수가 있음

● 블록체인의 기록은 그 누구도 나중에 고쳐 쓰는 것이 거의 불가능한 비가역성을 가지며, 이로 인해 강력한 변조 방지 기능을 가짐

– 블록체인은 기존에 연결된 블록들의 체인에 새로운 거래를 추가할 수만 있을 뿐 기존의 블록의 거래 내용을 그 누구도 변경할 수 없음
– 나머지 전체 네트워크를 능가하는 연산력을 독점한 행위자가 있으면 이전 블록의 기록을 고쳐 쓴 후에 새로운 블록을 연속해서 추가하는 식으로 과거 기록의 변조가 가능하지만 가능성이 매우 낮음

◆ 비트코인의 블록체인의 문제점

● 거래 속도가 느리며, 블록에 써넣을 수 있는 내용이 한정되어 있음

– 거래 내역이 모든 참여자들에게 전파되고 새로운 블록에 쓰여지는 과정에 시간이 소요되어 전체 네트워크의 거래 처리 용량은 약 1초에 7회 정도로 제한되어있음

- 새로운 블록에 쓰여져 승인받기를 기다리는 거래들의 대기열이 증가하면서 거래의 승인에 걸리는 시간이 길어짐[2)]
- 블록의 용량이 제한되어있으며, 블록 안에 토큰 송금 내역 이외의 다른 복잡한 거래 내역을 써넣는데 한계가 있음

● 작업증명을 통한 비트코인 채굴(mining) 작업에 들어가는 비용이 과도하여 사회적 낭비를 발생시킴

- 비트코인의 마이닝 작업이 소모하는 전력량은 아일랜드 국민들 전체가 소모하는 전력량보다 더 높다고 함 (The Guardian, 2017. 11. 27)
- 비트코인은 장부 위조를 막기 위해서는 블록을 생성하는 비용을 높게 유지할 필요가 있기 때문에 마이닝에 참여하는 컴퓨터의 수가 늘어날수록 마이닝 비용이 증가하지만 이는 사회적 낭비임

2) 거래가 승인받기 이전의 대기시간 동안에는 물품을 인도받은 상대방이 고의로 이중지불을 시도하여 송금 거래를 무효화시킬 위험이 있음

3. 블록체인의 다변화

◆ 프라이빗 블록체인의 확산-개방성 원칙의 타협

● 프라이빗(Private) 블록체인은 비트코인과 달리 블록의 승인권한을 보유한 시스템 관리주체가 존재하며, 참여 자격도 제한됨

- 채굴과정을 거쳐 새로운 블록을 승인하는 것이 아니라 운영주체가 검증자(Validator) 역할을 수행하여 새로운 블록이 승인이 됨

※ 모든 참여자가 기록에 대한 동등한 읽기/쓰기 권한을 가진 퍼블릭 블록체인과 달리, 운영주체는 일반 참여자보다 더 높은 권한을 보유함

- 비트코인 등 퍼블릭 블록체인이 모든 참여자를 동등하게 불신하는 것과 달리, 검증자 역할을 하는 시스템 운영 주체는 일반 참여자보다 더욱 신뢰할 수 있다고 전제함
- 비금전적인 내용도 유연하게 장부에 써넣을 수 있으며[3], 금융, 무역, 의료, 공공 행정 등 가상화폐 결제 이외의 분야에 블록체인이 응용되는 경우는 주로 프라이빗 블록체인에 해당됨

※ 프라이빗이란 사기업 소유란 뜻이 아니라 모든 참여자가 자유롭게 장부에 기록을 써넣을 수 있는 퍼블릭 블록체인에 대비된다는 뜻이며, 공공부문도 프라이빗 블록체인의 운영주체가 될 수 있음

● 비트코인의 개방성의 원칙을 타협하는 대신에 거래속도 등의 효율성을 크게 증대시킴

- 전체 노드에 거래내역을 전송하고 합의를 구하는 절차를 생략하여 거래 처리속도를 크게 증가시킴
- 채굴이 필요 없게 되므로, 작업증명을 통한 채굴에 들어가는 전기료 등의 막대한 비용을 절약할 수 있음

3) 퍼블릭 블록체인의 경우에도 이더리움처럼 장부 내에 프로그래밍 코드 등 토큰 송금 내역 이외의 데이터 들을 써넣을 수 있는 경우가 있으나, 데이터의 제한이 보다 큰 편임

- 그러나, 이러한 효율성 증대의 반대급부로 전체 네트워크의 신뢰성은 전통적 시스템과 마찬가지로 특정한 관리주체의 신뢰성에 다시 의존하게 되었으며 탈중앙화와 개방화의 원칙은 타협하게 되었음
- 이로 인해, 프라이빗 블록체인은 진정한 블록체인이 아니라는 비판이 제기되었음

※ 프린스턴 대학의 Arvind Narayanan 교수(2015. 9. 18)는 프라이빗 블록체인이 기존의 데이터베이스의 공유형(shared) 버전과 근본적 차이가 없다고 비판함

※ 반면, Multichain의 Gideon Greenspan(2015. 10. 1)은 프라이빗 블록체인과 기존의 중앙집중식 데이터베이스는 분명히 다르며, 프라이빗 블록체인은 높은 신뢰성 등 여러 차별점을 가진다고 반박함

※ 이더리움의 창시자 Vitalik Buterin(2015. 8. 7)은 "블록체인을 구성하는데 단 한 가지의 올바른 방법이 있다고 믿는 것은 완전히 잘못된 것"이라고 지적함

- 또한, 거래 주체들 사이의 이질성이 매우 크고 데이터베이스를 공유하기 힘든 경우에는 오히려 퍼블릭 블록체인이 더욱 빠른 거래를 달성할 수도 있음

● 프라이빗 블록체인은 비트코인 등 퍼블릭 블록체인의 개방성을 타협한 대신 거래 장부의 분산 및 기록의 비가역성을 통한 보안성과 투명성 증대라는 특성은 유지함

- 장부가 다수의 참여자에게 공유되어 저장된다는 특성은 비트코인과 같으며, 이로 인하여 중앙 시스템이 해킹당하면 전체 데이터가 훼손되는 기존 시스템 대비 보안성이 증대될 수 있음
- 과거의 거래내역을 사후 수정하기 어렵게 하고[4], 사후 수정시 반드시 기록에 남도록 함으로서 감사 가능성 (Auditability) 이라는 블록체인의 특성을 유지함

4) 프라이빗 블록체인의 경우 Validator로서 관리 권한을 가진 주체에게 기존 기록의 수정 권한을 부여하는 경우도 있기 때문에, 기록의 비가역성은 퍼블릭 블록체인에 비해서는 덜 보장될 수도 있음

◆ 컨소시움 블록체인－관리 권한의 분산

● 컨소시움 블록체인은 프라이빗 블록체인과 유사하지만 다수의 관리 주체의 합의제로 운영된다는 점이 차별점

- 모든 사람에게 장부가 개방된 것은 아니라는 점에서 프라이빗 블록체인에 해당하지만, 새로운 블록의 승인 권한 등을 가진 검증자(Validator)의 역할이 다수의 관계자에게 분산되어있음
- 시스템 관리 권한을 가진 다수의 주체의 협의로 운영된다는 점에서 컨소시움 블록체인이라고 불리며, 이를 프라이빗 블록체인과 별개의 유형으로 분류해야하는가에 대해서는 이견이 존재함
- 시스템 관리 권력의 분산을 통한 견제와 균형을 통해 시스템 전체의 신뢰성을 증대시킬 수 있으며 단일 관리 주체의 시스템에 비해 투명성의 향상이 가능함
- 프라이빗 블록체인과 마찬가지로 채굴 작업을 생략하고, 노드 간의 합의 절차를 부분적으로 생략함으로서 효율성 향상이 가능함
- 퍼블릭 블록체인과 마찬가지로 장부가 다수에게 분산이 되어있으며, 거리기록의 비가역성으로 보안성 및 투명성 제고가 가능함

◆ 프라이빗 블록체인의 도입 사례

● 세계최대 해운사인 머스크(Maersk)사는 다수 이해관계자가 개입된 물류체인의 관리를 위하여 블록체인을 도입하려고 함

- 머스크 해운은 자사가 처리하는 화물의 전세계적인 이동을 블록체인을 통하여 추적하고 관리하는 시스템을 구축하기 위하여 IBM과의 제휴할 것을 발표함 (Shippingwatch, 2017. 3. 6)
- 해운의 경우 같은 컨테이너 안에 서로 다른 화물들이 있으며, 화물을 발송한 화주 측, 그 것을 받아볼 고객과 각국의 세관 등 다수의 관계자가 얽혀있어 물류 데이터 관리의 복잡성을 증가시킴

- 머스크 해운이 한 개의 컨테이너를 동아프리카에서 유럽까지 운반하는 과정에서의 서류 작업 처리를 위해 약 30명의 인원과 200건 이상의 비즈니스 인터랙션이 필요했다고 함 (MIT Technology Review, 2017. 3)
- 화주와 세관, 해운업계 등 특정 화물 아이템에 관계된 모든 주체들이 공유하는 분산형 장부를 만들면, 업데이트 되는 정보들을 새로운 블록에 추가하여 모든 관계자가 동시에 조회할 수 있음

● 구글 DeepMind는 블록체인 기술을 활용하여 의료기록을 관리하는 솔루션을 개발하기로 함

- 구글 DeepMind는 Verifiable Data Audit 이라고 불리는 의료 기록 관리 솔루션을 개발할 것이며, 이는 블록체인 기술을 기반으로 의료 데이터를 관리할 것이라고 발표함 (MIT Technology Review, 2017. 3)
- 이 경우, 참여자들이 공유하는 분산된 장부가 존재한다는 것은 비트코인과 같지만, 코인 송금 내역 대신에 환자의 의료 기록이 장부에 쓰여진다는 점이 차이점임
- 환자나 의사 등 접근권한을 보유한 참여자들만이 장부를 공유할 수 있는 프라이빗 블록체인 시스템이며, 장부에 쓰여진 의료기록을 조회하려면 반드시 로그인을 해야 함
- 환자 개인의 의료기록에 접근해서 사용한 경우 모두 기록에 남으며, 환자 몰래 접근해서 의료기록을 가져가거나 수정하는 것이 불가능하다는 것이 최대의 장점임

● IBM은 Batavia 라는 블록체인 기반 국제 무역 결제 시스템을 개발하였으며, UBS, Commerzbank 등의 금융기관 들이 참여

- Project Batavia는 IBM과 UBS가 공동으로 개발을 시작한 블록체인 기반 국제 무역 지불 결제 시스템이며, 무역상품이 국제간 이동하는 과정을 추적하면서 각 단계별로 자동적으로 대금 지불을 수행하게 됨

- Bank of Montreal, Caixabank, Erste Bank와 Commerzbank도 프로젝트에 참여하기로 발표하였으며, 2018년 초에 첫 거래를 시작하는 것을 목표로 함 (Financial Times, 2017. 10. 5)
- 국제 무역의 지불 결제에서는 구매자와 판매자, 거래 은행, 세관 등이 서로 다른 나라에 있으며, 이에 따라 결제 과정이 복잡하고 오래 걸릴 뿐 아니라 하나의 기관이 전 과정을 일관되게 규율하기 어려웠음
- Batavia는 국적이 다른 여러 기관의 컨소시움이 블록체인 형태로 물류의 흐름과 이에 따르는 결제 정보를 공유하고, 이로서 다수의 다국적 이해관계자 사이의 복잡한 거래를 투명하고 신속하게 조정함
- Batavia는 Maersk와 같은 단일 기관이 관리주체가 되는게 아니라 무역거래에 참여하는 다수의 기관들이 공동관리할 뿐 아니라 새로운 기관들의 참여에 문을 열어놓고 있음

4. 시사점

● 모든 참여자에게 개방된 퍼블릭 블록체인과 참여자격 및 접근권한에 제한을 두는 프라이빗 블록체인 사이에서 적절한 유형을 선택해야 함

– 퍼블릭 블록체인과 프라이빗 블록체인 사이의 양자택일이 아니며, 프라이빗 블록체인들 간에도 공개 범위나 관리주체의 권한 등에서 커다란 차이가 있음
– 블록체인 기술의 적용 대상 네트워크가 포괄하고자 하는 참여자의 범위, 요구되는 거래 속도와 처리용량 및 보안수준 등을 감안하여 최적의 유형을 선택해야 함
– 거래에 참여하는 주체가 이질적이고 다수일 경우에는 퍼블릭 블록체인 또는 보다 분산형의 프라이빗 블록체인(컨소시움 블록체인 등)이 보다 적합함
– 반면, 동질적인 주체간의 거래의 경우에는 블록체인 기술이 기존의 중앙집중식 데이터베이스보다 우월하지 않을 수도 있음[5)]

● 프라이빗 블록체인의 경우 투명하고 공정한 데이터 가버넌스 룰 설정의 필요성이 퍼블릭 블록체인보다 더욱 커짐

– 비트코인 등의 퍼블릭 블록체인은 시스템의 신뢰성이 참여자의 신뢰성에 의존하지 않는 반면, 프라이빗 블록체인은 시스템의 신뢰성이 시스템 운영 주체의 신뢰성에 의존함
– 프라이빗 블록체인의 신뢰성은 작업증명 등의 게임이론적 장치를 통해서가 아니라 시스템 운영 주체가 운영의 룰 설정에 모든 관계자들을 참여시키고 적극적으로 합의를 구함으로서 담보될 수 있음

5) 블록체인에서 장부의 복사본을 분산해서 보유하는 것은 데이터 중복으로 인한 속도 저하가 반대급부로 따름

● 다수의 기관들이 함께 참여하여 컨소시움 블록체인 네트워크를 구성하기 위해서는 데이터 포맷 및 데이터 공유정책의 조율 작업이 필수적임

– 블록체인 네트워크는 보다 이질적인 주체들을 포괄할수록 기존 중앙집중식 데이터베이스 대비 우위를 가지지만, 이는 이질적인 주체들 사이의 조정의 문제를 과제로 남김

– 서로 다른 기관들은 대부분 서로 다른 데이터 포맷과 데이터 공유정책을 가지고 있기 때문에, 이들 간에 합의에 도달해야 블록체인 네트워크 구축이 가능함

※ 예를 들어, 서로 다른 지역과 전공분야의 병원들이 제휴하여 의료기록을 공유하는 블록체인 네트워크를 구성하는 경우, 병원들마다 서로 다른 의료 관리 기록 및 데이터 공유 정책을 서로 맞춰서 합의에 도달해야 함

– 이러한 합의는 블록체인 기술이 자동적으로 가져다 줄 수 있는 것이 아니며, 각 주체간의 소통과 타협의 사회적 프로세스가 수반되어야 가능해지는 것임

참 고 문 헌

Financial Times (2017. 10. 5). "Banks team up with IBM in trade finance blockchain"

Gideon Greenspan (2015. 10. 1). "Private blockchains are more than "just" shared databases", Multichain

MIT Technology Review (2017. 3. 6). "The World's Largest Shipping Company Trials Blockchain to Track Cargo

_____(2017. 3. 9). "DeepMind's New Blockchain-Style System Will Track Health-Care Records"

Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System"

Narayanan, Arvind (2015. 9. 18). ""Private blockchain" is just a confusing name for a shared database", Freedom to Tinker.

Shippingwatch (2017. 3. 6). "Maersk Line and IBM form new digital partnership"

The Guardian (2017. 11. 27). "Bitcoin mining consumes more electricity a year than Ireland"

Vitalik Buterin (2015. 8. 7). "On Public and Private Blockchains", Ethereum Blog.