한국은행 THE BANK OF KOREA

금융결제 업무정보

금융결제국 결제연구팀
2022.8.11일(목)

블록체인의 확장성과 분절화

※ 국제결제은행(BIS)의 블록체인의 확장성과 분절화에 대한 보고서(Blockchain scalability and the fragmentation of crypto, 6.8일 발표)와 연례경제보고서(Annual Economic Report, AER, 6.21일 발표) 제3장 미래의 화폐시스템(The future monetary system)의 내용을 정리

◈ 암호자산 시장이 성장하고 관련 기술이 발전하고 있으나 비허가형 블록체인(permissionless blockchain)*의 태생적 한계로 인해 **블록체인 생태계의 분절화(fragmentation)**가 **발생**

* 블록체인을 사용하거나 검증자(validator)로 참여할 때에 허가가 필요하지 않은 시스템으로 누구든지 운영에 참여할 수 있는 블록체인 시스템

○ 이는 **신뢰할 수 있는 다수의 검증자 확보**를 위한 **인센티브 구조**로 인해 데이터 처리용량의 **확장성(scalability)이 제한**되는 데 기인

○ 검증자들의 **거래내용 조작 방지를 위해** 높은 수준의 **인센티브 제공**이 불가피한데 이를 해결하기 위해 **거래처리 건수를 제한**하고 있어, 이용자들은 빠른 거래처리를 위해 **더 높은 수수료를 부담**하게 됨

○ 높은 수수료 부담으로 인해 **대체 블록체인으로 전환하는 이용자가 증가하게 되며,** 블록체인마다 의사결정을 위한 합의 메커니즘이 상이하기 때문에 블록체인 간 **상호운용성*이 저하**

* 디파이 프로토콜과 검증자들이 서로 다른 블록체인에 접속하여 정보를 교환하고 거래내용을 검증할 수 있는 능력을 의미

◈ 상호운용성을 높이기 위해 **블록체인간 거래를 성립**시키는 **'크로스체인 브릿지(crosschain bridge)'와 하위 블록체인(레이어2)에서 거래를 처리**하고 이를 **메인 블록체인(레이어1)에 기록**하는 방법인 **'레이어2 기술'**이 등장하였으나, **보안의 취약성 및 중앙화(centralised)*** 현상을 피할 수 없는 상황

* 소수의 주체(중앙 서버, 검증자 등)가 데이터를 통제하는 현상

◈ 비허가형 블록체인은 사용자가 증가할수록 **확장성의 제한으로** 인해 **분절화**되는 **태생적 한계**를 가지고 있으므로 이를 기반으로 하는 **암호자산 및 디파이**는 **화폐시스템**으로 **기능하기 어려움**

⇒ 이와 달리 **중앙은행 디지털화폐(CBDC)**는 법화로서 네트워크 효과를 형성할 수 있고 국가 간 합의를 통해 상호운용성을 확보할 수 있어, 화폐로서 범용성에 한계를 가지는 **여타 암호자산과 차별화**

작성자 : 오건우 조사역(02-750-6636)

1 블록체인 생태계의 분절화 현황

□ 블록체인을 기반으로 금융기관의 중개 없이 알고리즘에 따라 암호자산을 대여 및 투자하는 디파이(DeFi) 시장이 크게 성장

○ **디파이**에 **예치된 총 자산규모**(Total Value Locked, TVL)는 20.12월 2백억 달러에 불과하였으나 21.12월에는 2천 5백억 달러로 10배 이상 **급증**

□ 디파이 시장이 커지면서 **다수의 블록체인이 등장**하게 되었으며 그 결과 **블록체인 간 상호운용성(interoperability)***이 **떨어지는 블록체인 생태계의 분절화(fragmentation)**가 **발생**

* 디파이 프로토콜과 검증자들이 서로 다른 블록체인에 접속하여 정보를 교환하고 거래내용을 검증할 수 있는 능력을 의미

○ 초창기 대부분의 디파이 프로토콜*은 이더리움 블록체인**을 이용하고 있었으나 2021년을 기점으로 **수수료가 저렴한 새로운 블록체인**(Binance, Avalanche 등)이 등장하면서 이들을 **이용**하는 **비중**이 빠르게 **증가**

* 이용자 간 암호자산의 대출, 매매 등 의 거래를 가능하게 하는 탈중앙화된 애플리케이션(dApp) 또는 이를 구성하는 코드를 의미

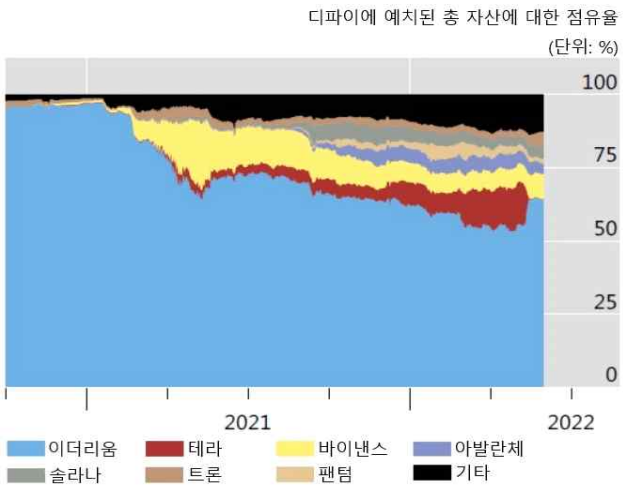
** 2015년부터 운영을 시작한 이더리움은 블록체인 내에 미리 설정한 조건을 충족할 경우 중개인 없이 자동으로 계약이 체결되게 하는 '스마트 계약'을 최초로 프로그래밍하여 디파이 시장을 선점

○ 그러나 새로운 블록체인 이용 확대 속도에 비해 기존 블록체인 및 여타 블록체인 간의 상호운용성 개선 작업이 더디게 진행

디파이에 예치된 총 자산규모(TVL)

자료: DeFiLlama

레이어1[1] 블록체인의 분절화



주: 1) 해당 블록체인에서 거래 검증 및 처리 가능한 블록체인

2 블록체인 간 상호운용성 제약 요인

□ 블록체인 간 상호운용성 제약은 비허가형 블록체인의 태생적 인센티브 구조에 기인

○ **비허가형 블록체인(permissionless blockchain)***은 **익명성**을 **특징**으로 하며 거래 검증에 대한 인센티브를 받는 **다수의 검증자**에 의해 **거래의 유효성**을 **확보**

* 블록체인 시스템을 사용하거나 블록체인 검증자(validator)로 참가할 때에 허가가 필요하지 않은 시스템으로 누구든지 운영에 참여할 수 있는 블록체인 시스템

— **암호자산 거래의 유효성**을 **검증***한 후 수정 불가능한 거래기록을 유지하기 위해 검증자들에게 **작업증명**(proof-of-work, PoW)을 요구하며, 이를 통해 **신규 블록 생성**에 성공한 검증자들에게는 **암호자산을 인센티브로 제공****

* 누구나 블록체인 데이터에 접근하여 거래기록을 위조할 수 있기에 검증자들에 의해 해당 거래의 유효성을 보장받을 필요

** 작업증명 과정에는 높은 비용(전력 및 시간)이 발생하기에 검증자들에게 경제적인 보상이 지급될 필요가 있으며, 이를 위해 거래 당사자들은 수수료를 지불

— 거래 당사자들은 **거래 검증**에 대한 **수수료**를 **지급**해야 하며 **이더리움**에서는 이를 **'Gas fee(단위: Gwei)'***라 지칭

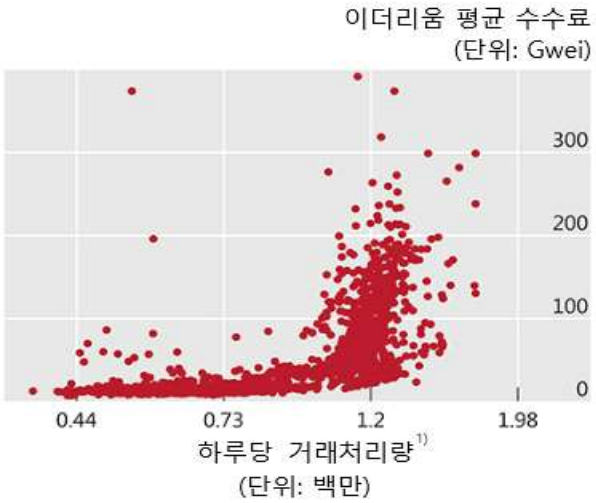
* 이더리움 시스템의 암호자산 단위는 이더(ether)라고 불리며, 1이더는 10^9 Gwei임

○ 비허가형 블록체인은 검증에 대한 **인센티브**가 축소될 경우 검증자들의 **참여도가 낮아지고** 그 결과 **검증에 대한 신뢰도** 역시 **하락해** 시스템의 **보안이 저해되는 취약점**이 존재

— **거래내용 조작 방지**를 위해서는 **다수의 검증자가 필요**한데, 이더리움은 **거래처리 건수를 제한**해 높은 수준의 **인센티브를 제공**하는 방식으로 **검증자를 확보**하고자 함

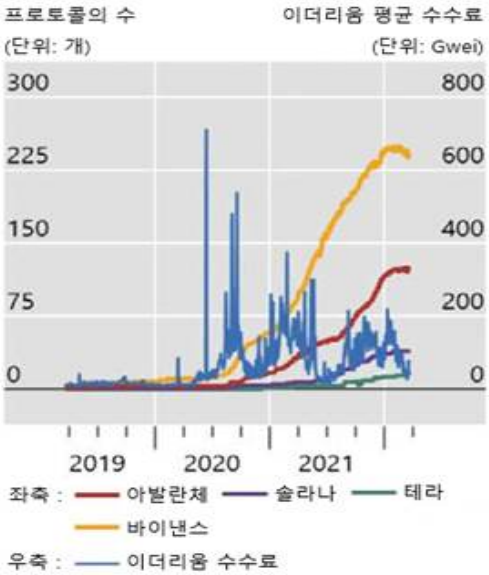
— 이로 인해 일정 시간 내 처리 가능한 거래 건수가 제한됨에 따라 **더 높은 수수료를 부담**하더라도 **빠른 거래처리**를 원하는 이용자가 증가하면서 **평균 수수료**가 급격하게 **상승**하는 효과(network congestion effect)가 발생

이더리움 블록체인의 수수료 분포



주: 1) 하루당 처리된 거래의 양을 로그 스케일로 표시

이더리움의 수수료 상승에 따른 대체 블록체인의 성장



⇒ 높은 수수료 부담으로 인해 **대체 블록체인으로 전환하는 이용자가 증가하게 되며,** 블록체인마다 의사결정을 위한 합의 메커니즘이 상이하기 때문에 블록체인 간 **상호운용성이 저하**

○ **이더리움의 수수료가 급등**한 2020년 및 2021년에 이더리움의 **대체 블록체인**인 바이낸스, 아발란체, 솔라나, 테라가 등장하였으며 차례로 **성장**

3 상호운용성 및 확장성 문제의 해결 방안과 한계

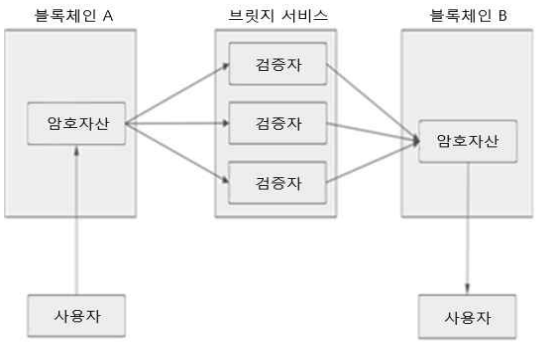
[해결 방안]

□ **(크로스체인 브릿지)** **외부 검증자들의 검증**을 거쳐 블록체인 간 암호자산 거래를 성립시키는 **'크로스체인 브릿지(crosschain bridge)'가** 등장

○ 이더리움 사용자가 **브릿지에** 자신의 **암호자산**(이더)을 **이전**하고 이에 대한 **검증 및 거래 기록**을 한 뒤 다시 브릿지에서 **다른 블록체인으로** 암호자산을 이전

○ 브릿지는 **소수 외부 검증자**들의 거래 검증을 거치므로 **빠른 거래처리**가 **가능**하며 블록체인 간 암호자산 이동을 가능하게 한다는 장점 보유

크로스체인 브릿지의 구조



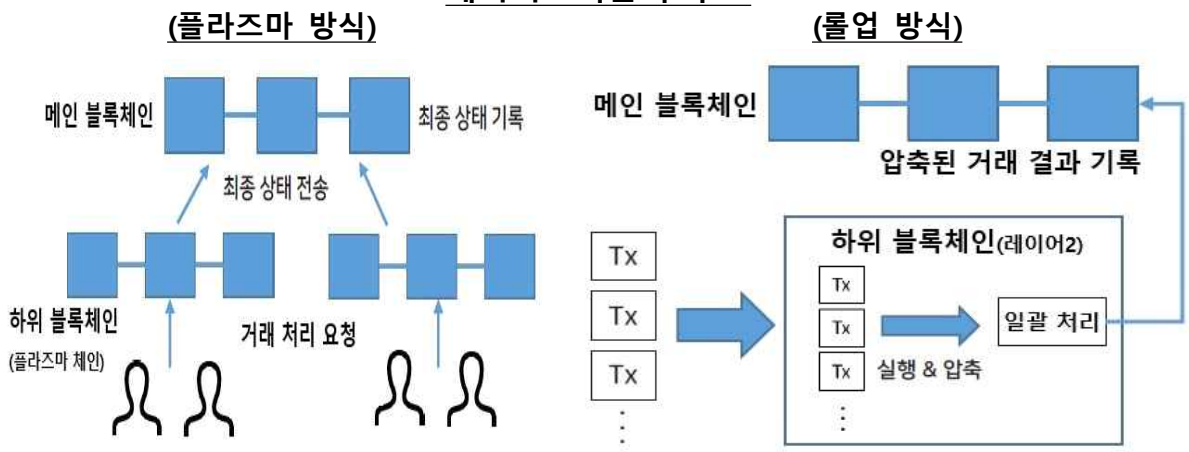
자료: Luniverse

□ **(레이어2 기술)** 메인 블록체인이 전체 거래를 검증하여 기록하는 레이어1 기술과 달리, **연계된 하위 블록체인**에서 일부 거래를 검증하고 해당 **결과만 메인 블록체인에 기록**하는 **레이어2 기술**도 등장

○ 레이어2 기술에는 **거래처리 결과만 요약**하여 **전달**하는 **플라즈마 방식**과 하위 블록체인의 **전체 거래기록을 압축**하여 **메인 블록체인에 전송**하는 **롤업 방식**이 존재

○ 레이어2 기술은 한계가 있는 메인 블록체인의 **거래처리 능력을 향상**시킴으로써 메인 블록체인에서의 **수수료 상승 문제**를 **해소**

레이어2 기술의 구조



자료: 한국은행, 중앙은행 디지털화폐 관련 주요 이슈 및 중앙은행의 과제, 지급결제제도 컨퍼런스, 2021.11

[한계]

□ 크로스체인 브릿지는 기존 블록체인보다 거래의 유효성을 검증하는 **검증자의 수**가 **적어** 소수의 주체가 데이터를 통제하는 **중앙화(centralised)** 현상이 발생하기에 **보안이 취약**하다는 문제*

* 현재 블록체인은 확장성, 보안성(security), 탈중앙화(decentralised)의 가치를 동시에 달성하지 못하는 트릴레마(Trilemma)에 봉착. 자세한 내용은 <참고> '블록체인의 트릴레마'를 참조

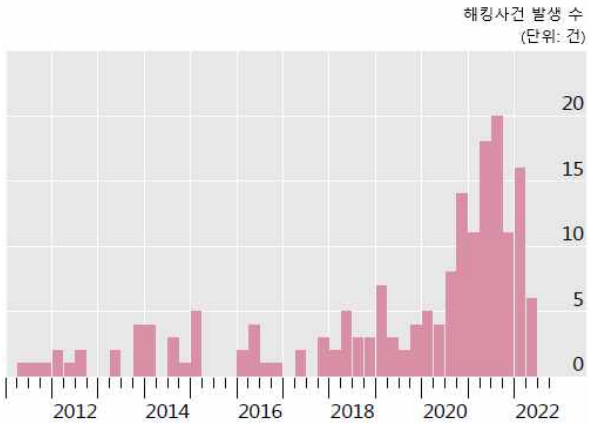
○ 이더리움과 로닌 블록체인을 연결하던 **로닌 브릿지**는 **검증자 9명**의 검증에 **의존**하여 **데이터의 중앙화**가 발생

— 그 결과 '액시인피니티'는 로닌 브릿지의 9명의 검증자 중 과반수인 5명의 개인 키를 도난당해 총 6억2천5백만 달러 상당의 이더리움을 유출하는 **보안상 취약점 노출**

○ 브릿지 등장 초기인 **2020년 1분기의 암호자산 해킹 건수**는 **5건**에 불과하였으나 **브릿지의 수가 증가**하며 **2022년 1분기**에는 **16건**으로 3배 이상 **급증**

크로스체인 브릿지의 증가 추이

암호자산 해킹 건수 추이



□ 레이어2 기술은 거래처리와 거래기록이 각각 다른 블록체인에서 진행되는 **구조**로 인하여 **거래 기록시 보안상 취약점**이 발생

○ **플라즈마 방식**은 메인 블록체인에서 최종 결과값만을 기록하기에 블록을 생성한 거래 **검증자가 유효하지 않은(invalid) 결과값**을 **메인 블록체인에 기록할** 경우 사용자들은 **거짓에 대한 검증(fraud proof)*이 불가능**하여 보안이 취약하다는 한계

* 메인 블록체인에 기록된 결과값을 하위 블록체인(플라즈마 체인)에 저장된 거래처리 내역들과 대조하며 거래의 유효성을 확인하는 작업을 의미하며, 하위 블록체인에서 처리된 거래 정보를 조작한 경우 결과값만을 가지고 거래의 진위를 알 수 없음

○ **롤업 방식**의 경우 **하위 블록체인**에서 **거래를 처리하고 압축**하여 일괄적으로 메인 블록체인에 기록하고 있기에 **데이터가 중앙화**되어 있으며, **하위 블록체인**에서의 **악의적인 거래 조작**이 일어날 수 있는 문제

4 시사점

□ **비허가형 블록체인**은 **사용자가 증가**할수록 **높은 수수료**로 인해 **분절화**된다는 태생적인 한계가 존재하며, **이를 기반으로 사용**하는 **암호자산** 및 **디파이** 역시 **분절화**되는 **현상** 발생

○ **인센티브**를 제공해 거래를 검증하는 구조는 이를 유지하기 위해 **높은 수수료**가 요구되고, 이로 인해 사용자들이 **대체 블록체인**을 **선택**하여 **시스템이 분절화**되기 쉬움

□ 따라서 **암호자산** 및 **디파이**는 **상호운용성이 저하되는 분절화 현상**으로 인해 **화폐시스템**으로 기능하기 **어려움**

○ **상호운용성이 저하**됨으로 인하여 **사용자들의 집중**을 통해 거래 비용을 절감하고 서비스 품질을 개선하는 **네트워크 효과(network effect)**를 형성하는 것이 **불가능**

○ 따라서 '네트워크 효과를 통한 새로운 사용자 유입'이라는 **선순환 구조(virtus circle)**를 형성할 수 **없어**, 암호자산이 **화폐로서 범용화**되기에 **한계**가 존재

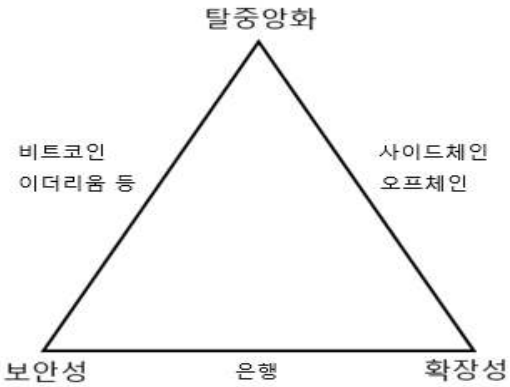
□ 이와 달리 **중앙은행 디지털화폐**(CBDC)는 법화로서 네트워크 효과를 형성할 수 있고 국가 간 합의를 통해 상호운용성을 확보할 수 있어, 화폐로서 범용성에 한계를 가지는 **여타 암호자산과 차별화**

○ **중앙은행에 대한 신뢰를 기반**으로 디지털 경제에 보편적 지급수단을 제공 가능

<참고>

블록체인의 트릴레마

트릴레마의 구조



자료: BIS, The future monetary system, Annual Economic Report, 2022.6

□ 비허가형 블록체인은 **'확장성', '보안성', '탈중앙화'**라는 3가지의 목표를 **동시에 달성할 수 없으며,** 이 중 하나의 목표는 포기하여야 하는 **트릴레마(Trilemma)**에 봉착

○ (**보안성 및 확장성**) **전통적인 금융 중개기관**(은행 등)은 직접 당사자 간 거래를 중개하여 보안성 및 확장성을 확보할 수 있으나 소수의 중개기관에 거래와 정보가 집중되어 **중앙화되는 문제**가 발생

— 이를 회피하기 위해 블록체인을 이용한 비트코인이 최초로 개발되었으며, 이후 스마트계약을 프로그래밍할 수 있는 이더리움 등 레이어1 블록체인 시스템이 등장

○ (**탈중앙화 및 보안성**) **레이어1 블록체인**인 이더리움은 다수의 검증자에 의한 **거래 유효성 검증**을 통해 **보안성과 탈중앙화**를 **달성**할 수 있었으나 이를 위한 **인센티브 구조**로 인하여 **확장성**에 대한 **한계** 존재

— 거래처리 건수를 제한해 검증에 대한 충분한 인센티브를 제공할 경우 **많은 검증자들의 참여**를 유도할 수 있어 보안이 강화되며 탈중앙화를 이룰 수 있음

— 그러나 이로 인해 일정 시간 내 처리 가능한 거래 건수가 제한됨에 따라 거래의 처리를 위한 수수료가 증가하게 되어 **수수료가 저렴한 대체 블록체인이 등장**하는 분절화 발생

○ (**확장성 및 탈중앙화) 브릿지**를 이용하는 사이드체인 및 **레이어2 기술**의 경우 메인 블록체인(레이어1) 외 **하위 블록체인(레이어2)을 이용하여 확장성 및 일부 탈중앙화**를 이룰 수 있으나 **보안이 취약**하다는 문제

— **브릿지를 이용하는 사이드체인**의 경우 암호자산을 이전할 때, **소수 검증자의 검증**에 의존하여야 하기에 레이어1 블록체인보다 중앙화되어 보안성에 취약점이 발생한다는 **한계**가 **존재**

— **레이어2 기술**의 경우 연계된 **하위 블록체인**에서 거래를 처리한 뒤 메인 블록체인에 이를 기록하기에 데이터 용량의 **확장성을 개선**하였으나 **거래처리 정보가 하위 블록체인**에 있어 이로 인한 **거래의 조작 가능성**이 존재