정 보 보 호 학 회 지
제 32 권 제2호, 2022. 4

저사양 사물인터넷 디바이스를 위한 블록체인 기술 동향

허 신 욱*, 조 욱**, 김 금 보**, 권 율**, 김 호 원***

요 약

사물인터넷은 물류, 환경, 스마트 홈, 자율주행 자동차, 에너지 관리, 스마트시티, 농업 등 다양한 응용 분야를 가지며, 거의 모든 산업분야의 기본 인프라 사용되는 핵심 기술이다. 하지만, 사물인터넷은 쉬운 공격 노출과 다양한 보안 취약성, 다양한 센서로부터 수집되는 데이터에 대한 개인정보보호의 어려움 등 많은 문제점이 존재한다. 최근, 이러한 사물인터넷의 문제점들을 보완할 수 있는 기술로 블록체인 기술이 주목받고 있다. 사물인터넷과 블록체인을 접목하면, 블록체인의 높은 확장성과 공격에 대한 복원력, 신뢰성, 추적성 등을 통해 사물인터넷 서비스의 보안성, 신뢰성을 향상시킬 수 있다. 또한, 데이터 및 프로세스의 정형화, O&M 효율성 향상 등 다양한 장점을 가질 수 있으며, 블록체인이 접목된 사물인터넷 기술은 대부분의 산업분야에 혁신을 발생시킬 수 있다. 하지만, 사물인터넷 디바이스는 기본적으로 높은 자원 제약성을 가지고 데이터 처리에 높은 TPS 성능을 요구하기 때문에 기존 블록체인 기술과 통합되는 것이 쉽지 않다. 이에, 본 고에서는 사물인터넷과 블록체인의 융합을 위한 요구사항을 분석하고, 사물인터넷과 블록체인의 융합을 위해 필수적으로 요구되는 블록체인 스케일링 기술에 대해 알아본다.

Ⅰ. 서 론

다양한 디바이스를 통해 각종 데이터를 수집하고 디바이스들을 제어하는 사물인터넷 기술은 물류, 환경, 스마트홈, 스마트시티, 스마트팜 등 다양한 산업 분야에 기본 인프라로 사용되는 4차 산업혁명 시대의 핵심 기술이다[1]. 하지만, 사물인터넷은 다양한 디바이스 및 운영환경의 활용과 센서 및 액츄에이터 디바이스의 높은 자원 제약성으로 인한 쉬운 공격 노출, 단일장애점 문제, 개인정보보호 문제 등 다양한 보안 문제점이 존재한다[2][3]. 이에, 사물인터넷과 블록체인을 접목하는 사물 블록체인 기술이 최근 주목받고 있다[4]. 사물인터넷과 블록체인이 접목되면 블록체인의 높은 확장성, 공격에 대한 복원력, 신뢰성, 추적성, 피어와의 상호작용성 등에 의해 사물인터넷의 낮은 보안성 및 신뢰성 향상이 가능하다[5]. 또한, 데이터 및 프로세스의 정형화, O&M 효율성 향상 등의 다양한 장점을 가질 수 있다. 하지만, 사물인터넷시스템 구축에 활용되는 디바이스들은 기본적으로 높은 자원 제약성을 가지기 때문에, 기존의 블록체인 기술과 통합되는 것이 쉽지 않다[6]. 이에, 본 고에서는 경량 사물인터넷 디바이스에서 블록체인을 연동하기 위한 요구사항들을 분석한다. 또한, 저사양 사물인터넷 환경과 블록체인의 융합에 필수적인 스케일링(Scaling) 기술인 샤딩, 상태 채널, 플라즈마, 롤업 기술에 대해서 알아본다.

본 논문의 구성은 다음과 같다. 2장에서는 사물인터넷과 블록체인의 융합을 위한 요구사항과 필요 기술들을 분석한다. 3장에서는 온체인 스케일링 기술인 샤딩에 대해서 알아본다. 4장, 5장, 6장에서는 오프체인 스케일링 기술인 상태 채널, 플라즈마, 롤업 기술에 대해 알아본다.

Ⅱ. 사물 블록체인 요구사항 분석

사물인터넷과 블록체인의 융합을 위해서는 블록체인 트릴레마(Trilemma) 문제를 극복해야한다. 블록체인 트릴레마는 블록체인에서 확장성(Scalability), 탈중앙화(Decentralization), 보안(Security) 문제를 동시에

이 과제는 부산대학교 기본연구지원사업(2년)에 의하여 연구되었음.
* ㈜스마트엠투엠 IoT 보안팀 (팀장, shinwookheo@smartm2m.co.kr)
** 부산대학교 정보컴퓨터공학부 (대학원생, jouk@islab.re.kr, 대학원생, guembo@islab.re.kr, 대학원생, kwonyool@islab.re.kr)
*** 부산대학교 정보컴퓨터공학부 (정교수, howonkim@pusan.ac.kr)

해결하기 어렵다는 것을 뜻한다[7]. 일반적으로 확장성은 블록체인의 TPS(Transaction Per Second)를 나타낸다[8]. 탈중앙화는 블록체인 네트워크를 구성하는 노드, 피어가 분산되어 자율적으로 운영되는 정도를 뜻하며[9], 보안은 블록체인에 저장되는 데이터, 트랜잭션에 대한 기밀성, 무결성, 프라이버시 보호 등을 뜻한다.

블록체인 트릴레마 문제들을 해결하고 사물인터넷 서비스와 완벽히 융합되어 시너지 효과를 창출하기 위해서는 대용량/실시간 데이터 처리 기술, 경량 합의 알고리즘 및 스마트 컨트랙트 기술, 사물인터넷 데이터 신뢰성 보장 기술, 사물인터넷 시스템 보안 연동 기술, 사물인터넷 데이터 관리 및 플랫폼 연동 기술, 개인정보보호 기술이 필요하다.

2.1. 대용량/실시간 데이터 처리 기술

다양한 사물인터넷 디바이스에서 수집, 활용되는 실시간 데이터에 대한 처리를 위해서는 대용량/실시간 데이터 처리 기술이 필요하며, 이는 블록체인 확장성 문제와 직결된다. 비트코인(Bitcoin), 이더리움(Ethereum)과 같은 기존의 블록체인 기술은 합의 알고리즘 수행에 많은 계산량과 네트워크 상호 통신을 필요로 한다. 이 때문에 비트코인의 경우 약 7 TPS[10][11], 이더리움의 경우 약 20 TPS의 낮은 성능을 보이며 대부분의 사물인터넷 서비스에 적용하는 것은 불가능에 가깝다. 또한, 단순 복제 데이터베이스로 인해 과도한 저장 공간을 필요로 한다. EOS, Solana, IoTex와 같이 트랜잭션 처리 성능을 향상시킨 블록체인의 경우 2,000 TPS에서 3,000 TPS의 성능[12][13][14]을 보여 트랜잭션 관점에서 사물인터넷에 적용 가능하지만, 여전히 높은 저장 공간 요구사항으로 인해, 사물인터넷에 적용되기 어렵다.

2.2. 경량 합의 알고리즘 및 스마트 컨트랙트 기술

사물인터넷 디바이스의 높은 자원 제약성은 블록체인 블록체인의 신뢰성과 투명성, 탈중앙성, 보안성의 원천인 합의 알고리즘의 실현을 어렵게 한다[15][16]. 이에, 경량 디바이스 환경에서 원활히 동작하며, 보안 취약성이 없는 경량 합의 알고리즘 기술이 필요하며, 사물인터넷 환경에서 동작 가능한 스마트 컨트랙트 기술이 필요하다. 경량 환경에서 동작하는 합의 알고리즘과 스마트 컨트랙트 기술이 없을 경우, 일부 사물인터넷 게이트웨이나 서버에 노드가 집중되며, 이는 탈중앙화 문제를 발생시킬 수 있다[17]. 블록체인 플랫폼 중 Microchain은 사물인터넷에 블록체인을 결합하기 위해 소수의 허가된 검증자만을 가지는 합의 알고리즘을 제안했다[18]. Microchain은 검증자들이 현재 네트워크에서의 신용도에 기반하여 단 한번의 해시 퍼즐 값을 계산할 수 있도록 하는 PoC(Proof of Credit) 합의 알고리즘을 통해 낮은 리소스를 가지는 사물인터넷 디바이스라도 합의 알고리즘에 참여할 수 있도록 한다.

2.3. 사물인터넷 데이터 신뢰성 보장 기술

블록체인 관점에서, 외부에서 발생한 데이터는 신뢰할 수 없으며, 이것을 블록체인 오라클 문제라고 한다. 마찬가지로, 사물인터넷 센서를 통해 수집된 데이터는 블록체인 외부에서 발생한 데이터로 신뢰 할 수 없다[19][20]. 따라서, 사물인터넷 센싱 데이터에 대한 신뢰성을 제공할 수 있는 오프체인 기술, DID 기반 사물인터넷 디바이스 검증 기술, 저사양 사물인터넷 디바이스를 위한 경량 보안 프로토콜 및 데이터 검증 기술, 신뢰 실행 환경을 활용한 데이터 신뢰성 보장 기술 등이 필요하다. [21]에서는 신뢰 실행 환경인 TEE(Trusted Execution Environment)를 사용해서 저사양 디바이스에서의 신뢰성 문제 및 블록체인 오라클 문제를 해결하고 했다. TEE 내 보안 영역(Secure Zone)에서 구현된 TA(Trusted Application)는 API를 통해 비보안 영역에서만 호출할 수 있으며 비보안 영역에서 수정하거나 검사할 수 없다. 이처럼 TEE는 철저히 보안영역/비보안 영역을 나누어 프로그램의 무결성, 자산의 기밀성 등의 보안기능을 제공하는데 기존의 오프체인 오라클 문제를 TEE 기반으로 데이터를 관리함으로써 악의적으로 수정되는 것을 제한했다.

2.4. 사물인터넷 시스템 보안 연동 기술

블록체인 기반의 DID(Decentralized ID) 기술을 사물인터넷 환경에서 사용하기 위해선, DID와 기존 사물인터넷 ID 체계(OID, URN 체계 등)과의 통합, 연동이 되어야 한다. 또한, DID 기반의 사물인터넷 서비스의 접근제어 기술, 권한 관리 기술, IAM(Identity

and Access Management) 기술이 필요하다 [22][23][24]. 추가적으로, 다양한 사물인터넷 표준(oneM2M, OCF, LwM2M 등)에서 사용하고 있는 표준 보안 기술과의 연동 및 호환을 위한 기술들이 필요하다[25].

IoT 장치의 사이버 공격 방지를 위해서 소프트웨어 업데이트의 지속성은 매우 중요하다. 그러나 일반적인 업데이트 방식인 OTA(Over-The-Air)는 IoT 장치가 제조업체의 서버에서 업데이트를 받아오는 중앙집중식 펌웨어 업데이트 방식을 사용한다. 중앙집중식 펌웨어 업데이트 방식은 단일 장애점 문제를 만들 수 있다. [25]에서는 OCF (Open Connectivity Foundation)의 P2P 업데이트 프로토콜을 보안측면에서 개선한 블록체인 기반 OCF 펌웨어 업데이트 연구가 진행했다.

2.5. 사물인터넷 데이터 관리 및 플랫폼 연동 기술

사물인터넷 환경에서는 실시간으로 데이터가 발생하고, 이미지, 고화질 영상 데이터와 같은 대용량의 데이터가 많이 활용된다. 이를 블록체인 상에서 처리하기 위해 샤딩[7]이나 IPFS(InterPlanetary File System)[27]와 같은 분산 데이터베이스 기술을 활용되는데, 분산 데이터베이스를 활용할 경우 효율적인 데이터 접근, 조회를 위한 데이터 관리 기법이 필수적으로 요구된다. 또한, 사물인터넷 환경에서는 다양한 사물인터넷 표준, 플랫폼이 융합되어 서비스를 창출하는데, 이를 블록체인 상에서 처리하기 위해서는 이종 사물인터넷 플랫폼, 표준에서 정의하는 데이터 모델을 처리하거나 서로 다른 데이터 모델을 변환할 수 있는 기술이 필요하다.

분산 데이터베이스의 효율적인 데이터 접근, 조회를 위한 대표적인 블록체인 프로젝트로 더 그래프(The Graph)가 있다[28]. 더 그래프는 서브 매니페스트(manifest)라고 하는 서브그래프를 기반으로 이더리움 데이터를 인덱싱하는 방법을 학습한다. 서브 그래프 매니페스트가 배포된 후 데이터 흐름은 다음과 같다. 먼저 별도의 그래프 노드를 두어 이더리움의 새 블록과 해당 블록들에 포함될 수 있는 서브 그래프 데이터를 검색한다. 이런 블록들에서 서브 그래프에 대한 이더리움 이벤트를 찾고 데이터 엔티티를 생성 및 업데이터하는 WASM 모듈인 매핑 핸들러를 실행한다. DApp은 노드의 GraphQL endpoint를 사용하여 그래프 노드를 쿼리한다. 더 그래프 노드는 GraphQL 쿼리를 기본 데이터 저장소에 대한 쿼리로 변환 및 활용한다.

2.6. 개인정보보호 기술

스마트 홈, 스마트 헬스케어와 같은 사물인터넷 서비스를 블록체인을 활용하는 방안이 많이 연구되고 있으나, 동시에 블록체인 트랜잭션을 검증할 때 데이터의 노출과 분산 원장에 기록된 모든 데이터가 참여하는 모든 노드에 공개된다는 특징으로 인해 개인정보가 노출 될 수 있다는 문제점이 지적되고 있다[29]. 이러한 데이터 노출을 해결하기 위해 Hyperledger Fabric[30]은 네트워크내에 PDC(Private Data Collection) 오프체인을 이용해 같은 조직으로 정의된 노드들만 데이터에 접근이 가능하고 트랜잭션을 검증하는 노드들은 해시데이터를 검증하여 데이터의 노출을 최소화하며, ZCash[31]는 영지식 증명 zk-SNARK를 사용해 코인 거래시 전송자, 수신자, 금액, 시간 등의 정보를 볼 수 없도록 한다. Monero[32]는 영지식 범위 증명인 bulletproofs를 사용해 기존 RingCT(Ring Confidential Transactions)를 대체하여 검증과정에서 트랜잭션의 사이즈를 줄이고자 했다. 하지만 여전히 영지식 증명을 블록체인 네트워크 내에서 검증과정에 사용할 때 저사양 디바이스에서 동작시키기에는 아직까지 많은 컴퓨팅 리소스가 필요하기 때문에[33] 관련 암호 기술에 대한 최적화 기술 연구가 지속적으로 필요해 보인다.

Ⅲ. 샤딩(Sharding)

데이터베이스 관점에서 샤딩은 같은 테이블 스키마를 가진 데이터를 다수의 데이터베이스에 분산하여 저장하는 방법을 의미하지만, 블록체인 관점에서 샤딩은 단일 블록체인에서 처리하는 트랙잭션과 데이터를 복수의 체인으로 수평적으로 분할하여 처리하는 방법을 뜻한다. 예를들어, 이더리움에서는 샤드(shards)라고 불리는 새로운 체인을 생성하여, 분할된 샤드별로 트랜잭션을 처리하여 네트워크의 혼잡을 줄이고 트랜잭션 성능을 향상시킨다[34][35]. 대표적인 샤딩 기술로는 트랜잭션 샤딩, 상태 샤딩이 있다.

3.1. 트랜잭션 샤딩 (Transaction Sharding)

트랜잭션 샤딩은 트랜잭션을 발생시킨 주소, 트랜잭션 유형 등을 기준으로 분리하여 처리하는 기술이다. 트랜잭션 샤딩을 구현한 대표적인 블록체인 프로젝트로는 질리카(Zilliqa)가 있다[36]. 질리카는 트랜잭션 유형을 단순 송금 트랜잭션(유형 1), 스마트 컨트랙트 호출 트랜잭션(유형 2), 복수 스마트 컨트랙트 호출 트랜잭션(유형 3)으로 구분하여 처리한다. 유형 1, 유형 2의 트랜잭션의 경우 샤드노드에서 처리되며, 유형 3의 트랜잭션의 경우 유형 1, 유형 2의 트랜잭션의 검증후 샤드 마이크로 블록을 집계하고 트랜잭션 블록을 생성하는 DS(Directory Service) 노드에 의해 처리된다[37].

3.2 상태 샤딩 (State Sharding)

상태 샤딩은 전체 저장소를 여러 샤드로 나누고 분리된 부분을 소속된 샤드가 처리하는 기술이다[38]. 계정 기반의 모델을 위해 상태 샤딩은 특정 상태(state)의 일부만을 유지한다. 상태 샤딩 구현을 위한 목표는 크게 3가지로 분류된다. 서로 다른 샤드를 통한 데이터 처리는 샤드 간의 커뮤니케이션을 통한 트랜잭션 유효성 검증이 필요하며 단편화 상호작용은 샤딩 기술의 효율성을 감소시키며 높은 상호작용은 오버헤드를 유발한다. 또한, 노드를 장기간 재분배하지 않으면 트랜잭션의 중앙화를 유발하여 모든 분기(epoch)마다 네트워크 노드를 재구성해야 한다. 이 과정에서 지연이 발생되며 샤딩이 붕괴할 수 있다. 마지막으로 특정 샤드가 공격당해 문제가 생길 시 샤드는 전체 상태를 저장하지 않아 관련 트랜잭션 검증이 불가능하며 이는 시스템의 장애로 이어진다[35]. 이를 위해 백업 노드를 유지하지만, 이는 중앙화의 문제를 야기한다.

Ⅳ. 상태 채널(State Channel)

상태 채널은 레이어 2 솔루션 중 하나로, 레이어 1 메인넷의 모든 트랜잭션을 블록에 모두 포함 시키지 않고 채널 생성을 통해 오프 체인에서 거래를 수행하고 채널을 닫을 때의 상태 값을 레이어1의 블록에 기록하도록 설계된 기술이다[39].

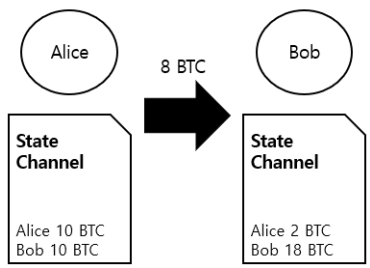
예를 들어 밥과 엘리스가 각각 서로 10 BTC씩 가지고 거래를 한다고 할 때, 밥과 엘리스는 오프체인 거래를 위해서 먼저 각각 10 BTC씩 예치해야 한다. 그 후 둘은 상태 채널을 생성해서 오프체인에서 거래한다. 거래가 진행될 경우에는 레이어 1에 기록하지 않고, 거래가 끝난 후에 엘리스와 밥의 잔고가 [그림 1]과 같이 각각 2 BTC, 18 BTC 상태를 레이어 1의 블록에 기록한다.

상태 채널의 주된 목적은 피어 간의 트랜잭션 속도를 높이는 것이다. 기존의 낮은 TPS를 가지는 퍼블릭 블록체인과는 다르게, 거래를 하는 두 사용자 간의 채널을 열어서 두 사용자간만 거래를 진행하기 때문에 매우 빠른 처리 속도를 가질 수 있다. 채널을 연다는 표현의 의미는 사용자 간 채널을 형성하며 레이어 1에 알리고 자신들이 예치한 자산을 생성한 채널에 담보를 걸어 앞으로의 거래를 약속하는 것을 말한다.

상태 채널에서 사용자끼리 거래가 이루어질 때 해당 거래는 채널이 생성되고 닫힐 때를 제외하고 는 레이어 1에서 수수료를 사용하지 않기 때문에 매우 적은 금액(최소 0.00000001BTC)의 잦은 거래도 가능하다. 레이어 1에서 동일하게 적은 금액을 거래하게 되면 높은 수수료를 계속해서 내야하는 단점이 존재한다.

상태 채널에서 이루어지는 거래는 누적되어 블록에는 최종 잔액이 한 번만 기록되고 또한 원할 때 블록에 즉시 반영시킬 수 있다. 레이어 1에 마지막 상태 업데이트를 제출하고 최신 잔액이 두 당사자에게 다시 전송된다. 레이어 1에서 두 사용자들이 최종적으로 한 서명과 최종 잔액을 확인하여 최종 상태의 유효성을 검증할 수 있다.

상태 채널은 대표적으로 비트코인을 개선한 Lightning Network와 이더리움의 ERC-20 토큰 전송 간소화를 위한 Raiden Network가 있다.



〔그림 1〕 State Channel 예시

4.1. 라이트닝 네트워크(Lightning Network)

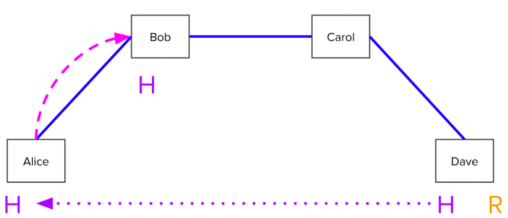
라이트닝 네트워크[40]의 비트코인을 하드포크한 블록체인으로 앞서 설명한 상태 채널처럼 상호 동의하에 열게 되는 결제(Payment) 채널을 생성해서 사용자 간 거래를 지원한다.

라이트닝 네트워크에서 모든 피어가 서로 연결되어 있지 않다. 직접 연결되어 있지 않은 피어가 서로 거래하기위해 라이트닝 네트워크는 우회 지불 방법을 사용한다. 우회 지불은 라이트닝 네트워크 내 피어가 네트워크 상에서 누군가와 연결되면 서로 제약없이 전송하기 위한 방법이다.

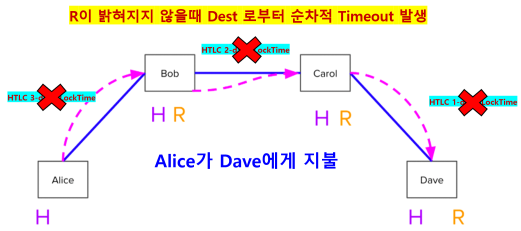
예를 들어 엘리스가 데이브에게 비트코인을 보낼 때 캐롤과 직접 라이트닝 지불 채널을 열 필요 없이 과거 참여자가 이미 열어놓은 지불 채널을 이용하여 우회 거래를 할 수 있다. 이와 같이 라이트닝 네트워크는 해시 타임락(Hashed time lock) 방법을 사용해 제삼자인 밥을 신뢰하지 않고도 우회 지불을 가능할 수 있게 만들었다.

[그림 2] 에서 엘리스가 데이브에게 돈을 지불하고 싶어 한다는 가정을 해보자. 데이브는 임의의 숫자(R)를 이용하여 해시(H)를 구하고 Alice에게 H를 제공한다. H를 받은 엘리스는 밥에게 3일 이내에 프리이미지(preimage)를 생성할 수 있으면 지불할 것을 약속한다. H를 받은 밥은 똑같이 캐롤에 2일 이내에 프리이미지를 생성할 수 있으면 지불할 것을 약속하고 캐롤은 데이브에게 1일 이내에 프리이미지를 생성할 수 있으면 지불할 것을 약속한다. 데이브는 R을 알고 있기 때문에 캐롤로부터 원하는 금액을 지불받고 연쇄적으로 밥, 엘리스로부터 지불받으며 이 거래는 성사된다. [그림 3]은 해시타임락에서 타임아웃 예외 상황이다.

또한, 라이트닝 네트워크를 이용한 비트코인 거래의 이미 사용 중인 Visa를 비교했을 때 현저히 떨어지는



〔그림 2〕 우회 지불



〔그림 3〕 우회지불 TimeOut

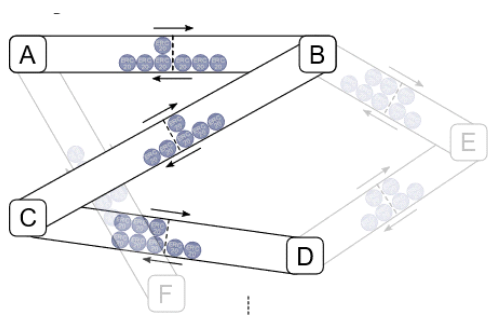
속도이지만 비트코인의 실생활 사용에 한층 더 가까워지고 있다는 평을 받고 있다.

라이트닝 네트워크는 몇 개의 문제가 존재한다. 우선 온체인 트랜잭션과 달리 인터넷에 연결되어 있지 않은 상황에서 라이트닝 네트워크 지불 시스템이 불가능하다. 라이트닝 네트워크 구조상 자신들의 자금을 안전하게 보관하기 위해서 지불 채널을 지속해서 모니터링 해야 할 필요가 있으며 대규모 지불에 적합하지 않다.

4.2. 라이덴 네트워크(Raiden Network)

비트코인에 라이트닝 네트워크가 있다면 [그림 4]의 이더리움 라이덴 네트워크[41]가 있다. 라이덴 네트워크는 이더리움 블록체인에서 호환되는 ERC-20 토큰들의 전송을 수행하기 위한 오프체인 확장성 솔루션이다. 라이트닝 네트워크와 유사하게 개인정보가 보호되며 빠르고 저렴한 전송을 가능하게 하는 특징이 있다.

라이덴 네트워크는 이더리움의 스마트컨트랙트를 이용해서 ERC-20 토큰을 예치 계좌로 전송하여 채널을 사용할 수 있도록 한다. 스마트 컨트랙트를 사용함으로써 라이트닝 네트워크보다 사용하기 용이하다는 장점이 있다. 라이덴 네트워크는 잔액 증명(Balance Proof)를 사용하는데 이는 채널을 생성할 때의 두 당



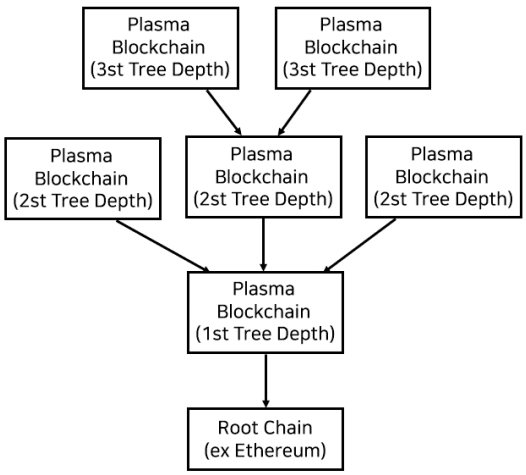
〔그림 4〕 결제 채널 네트워크

사자가 각자 예치해놓은 총 금액에 대한 증명으로, 두 당사자 간 거래시 잔액이 처음 예치한 금액의 한도를 넘지 않았음을 증명한다. 이후 채널을 닫을 때 최종 거래의 결과만을 레이어 1에 기록한다.

Ⅴ. 플라즈마(Plasma)

플라즈마 네트워크는 수많은 블록체인 네트워크가 트리구조로 이어진 레이어 2 솔루션이다[42]. 플라즈마 체인들은 주기적으로 블록 헤더의 머클루트 값을 상위 플라즈마 체인으로 커밋하여 상위 플라즈마 체인에 여러 하위 플라즈마 체인의 블록 정보를 저장한다. [그림 5]는 플라즈마 네트워크의 구조를 나타낸 것이다. 플라즈마 네트워크의 트리구조를 확장하는 이유는 루트체인의 수수료 절감이다. 예를 들어 모두 커밋 주기가 3인 플라즈마 체인을 사용 시 깊이가 1인 플라즈마 체인보다 깊이가 2인 플라즈마 체인은 3배의 트랜잭션을 하나의 머클루트 값으로 루트체인에 저장할 수 있다. 또한 Map-Reduce 방식을 사용하여 상위 플라즈마 체인 하에 하위 플라즈마 체인들을 둬 병렬트랜잭션 처리를 통한 고속화의 이점이 있다.

플라즈마 체인들은 지속적인 블록 유효성 검증이 아닌 하위 플라즈마 체인에서 사용되는 토큰이 상위 플라즈마 체인으로 출금(exit) 시 이더리움과 같은 루트 체인에서 사기증명(Fault Proof)을 진행한다. 루트체인을 제외한 모든 플라즈마 체인들은 신뢰할 수 없기 때문에 루트체인의 풀 노드가 출금 관련 트랜잭션



〔그림 5〕 Structure of Plasma Network

의 머클루트 값을 계산해 플라즈마 체인에서 커밋된 머클루트 값과 비교하여 사기증명을 진행한다. 플라즈마 네트워크가 충분히 활성화된다면 현재 이더리움 등에서 진행되는 DApp 프로젝트들을 개별적인 플라즈마 체인 위에서 진행될 수 있다.

5.1. 플라즈마 MVP(Plasma MVP)

플라즈마 MVP[43]는 플라즈마 네트워크 운영을 위한 기본적인 기능만을 구현한 UTXO 기반의 프로젝트이다. 플라즈마 체인의 동작은 입금(Deposit), 커밋(Commit), 출금(Exit) 세 가지로 구분된다.

입금은 참여자가 플라즈마 체인에 참여하기 위한 과정으로 루트체인을 통해 자신의 토큰(ex ETH)을 락업 후 플라즈마 체인에 동일한 양의 토큰을 발행 한다. 이후 플라즈마 체인 내에서 트랜잭션이 발생 시 임의의 블록 간격마다 관련 블록의 트랜잭션이 담긴 머클루트 값을 상위 플라즈마 체인으로 컴밋하며 위 과정을 반복하여 루트체인에 모든 플라즈마 체인의 트랜잭션 정보가 하나의 해시값으로 저장된다. 참여자가 상위 플라즈마 체인 및 루트체인으로 출금 시 루트체인을 제외한 모든 플라즈마 체인을 신뢰할 수 없기 때문에 루트체인에서 사기증명을 진행하는 Challenging 기간을 1~2주간 가진다. 이후 플라즈마 체인의 블록 생성자의 허위 UTXO 생성 가능성 배제를 위한 오래된 UTXO 순서로 출금이 진행된다. 출금 과정이 오래 걸려 소액의 경우 Atomic swap을 이용한 1대 1 토큰 스왑인 Fast withdrawal을 지원한다.

플라즈마 체인의 트랜잭션은 기존 블록체인 트랜잭션과 다르게 루트체인 커밋 완료 후 확인 서명을 제출하는 이중 서명 방식을 사용한다. 이중 서명을 위해 플라즈마 체인은 상위 플라즈마 체인의 블록 정보를 저장해야 하며 때문에 트리구조 깊이가 깊어질수록 하위 플라즈마 체인이 무거워지는 문제가 존재한다.

5.2. 플라즈마 캐시 & 데빗(Plasma Cash & Debit)

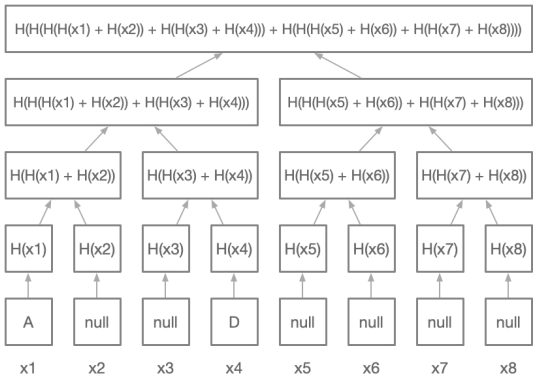
플라즈마 캐시(Cash)[44]는 플라즈마 MVP의 이중 서명, ERC-721을 사용한 NFT 토큰 미지원 문제 극복을 위해 사용된다. 트랜잭션은 UTXO 소유주, 블록 위치 등을 저장하던 Plasma MVP와 달리 모든 토큰을 NFT로 발행 후 일련번호 기반의 key-value 형태의

Sparse Merkle Tree를 이용한 토큰 거래 내역 정보를 저장한다. 머클트리와 달리 Sparse Merkle Tree는 효율적인 포함(inclusion) 및 미포함(non-inclusion) 트랜잭션 검증이 가능하다.

머클트리는 특정 트랜잭션이 블록에 포함(inclusion)된다는 것을 증명하기 위해 관련 Leaf Hash 값을 사용해 O(logN) 복잡도로 머클루트 생성이 가능하다. Sparse Merkle Tree는 [그림 6]과 같이 각 잎사귀(leaf)마다 key-value에 맞춰 값을 저장하며 값이 없을 시 null 값을 저장한다. 때문에 null 값을 사용한 머클루트를 이용해 미포함(non-inclusion) 트랜잭션 또한 O(logN) 복잡도로 계산할 수 있지만 관리 대상이 늘어날수록 머클트리 대비 Sparse Merkle Tree 사이즈가 증가하는 문제가 있다.

NFT 기반의 토큰 사용으로 인해 플라즈마 MVP의 확장성 문제를 유발한 이중 서명 문제를 해결하였다. 이 때문에 플라즈마 체인의 하위 레이어가 저장하는 상위 블록의 데이터 정보가 감소하였지만 NFT의 특성상 수수료 지급을 위해 기존 토큰을 분할하여 지급하며 이를 관리하는 토큰의 개수가 꾸준히 늘고 있다. 분할을 지속하여 토큰의 가격이 수수료의 가격보다 낮아지면 사용 불가능 토큰이 되며 NFT는 화폐로 사용하기 위해 가격의 조정이 힘든 문제가 존재한다.

NFT 기반의 플라즈마 캐시 거래 편의성 감소 해결을 위해 PoA 기반의 블록 생성자가 결제 채널을 지원하는 플라즈마 데빗을 사용한다 [45]. 참여자는 초기 입금 금액 v 내에서 0과 v 사이의 값 a를 임의로 전달할 수 있으며 모든 거래 과정은 블록 생성자가 구축한 결제 채널을 통해 이뤄진다. 이 과정에서 라이트닝 네트워크와 동일하게 일정 이상의 금액이 초기 결제 채널 생성 시 입금 및 잠기는 단점이 존재한다.



〔그림 6〕 Sparse Merkle Tree

Ⅵ. 롤 업 (Rollup)

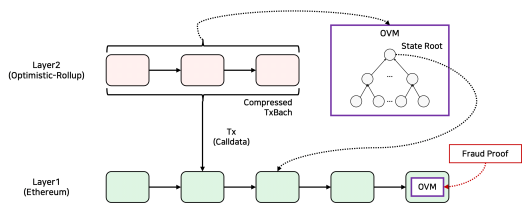
본 장에서는 롤업에 대해 살펴본다. 롤업은 돌돌 말아 올린다는 단어의 뜻처럼 레이어 2에서 분기에 발생하는 모든 트랜잭션을 수집하고(Aggregate) 압축된 형태로 레이어 1 메인넷에 올리는 레이어 2 솔루션이다. 롤업은 상태 채널과 플라즈마가 채널을 닫을 때의 상태 값 또는 분기별 변화되는 상태 값을 하나의 커밋값으로 레이어 1에 저장하는 것과는 다르게, 트랜잭션들을 압축된 계산 가능한 배치(batch) 형태로 레이어 1에 저장하는 것이 기존 두 방법과 다르다[46].

롤업 방식은 트랜잭션 검증 방식에 따라 대표적으로 Optimistic 롤업 방식과 ZK-롤업 방식으로 나눌 수 있다[48].

6.1. Optimistic 롤업(Optimistic Rollup)

[그림 7]은 이더리움 네트워크 기반 Optimistic 롤업 방식을 보여준다. 레이어 2에서 발생되는 트랜잭션들은 수집되어 배치 형태로 압축되어 트랜잭션을 반영한 상태 루트 값과 함께 레이어 1에 저장된다[48].

Optimistic 롤업은 트랜잭션을 검증하기 위해 사기증명(Fraud Proof)에 기반을 둔다. 사기증명이란 트랜잭션에 대한 상태 변화 값을 우선적으로 반영을 하고 일정 시간(약 1주일)의 논쟁기간 동안 사기 증명이 검증되지 않으면 현재 상태 값들에 대한 최종성(Finality)를 부여하는 증명 방식이다[49]. 사기증명은 블록체인 네트워크의 노드들을 풀 노드와 라이트 노드로 나누고 운영할 때, 라이트 노드가 풀 노드는 트랜잭션을 올바르게 검증할 것이라고 가정하기 때문에 발생하는 문제를 해결하기 위해, 상태 값의 최종성이 부여되기 전에 트랜잭션이 잘못 되었음을 주장할 수 있도록 만든 증명 방식이다. 하지만 라이트 노드가 사기증



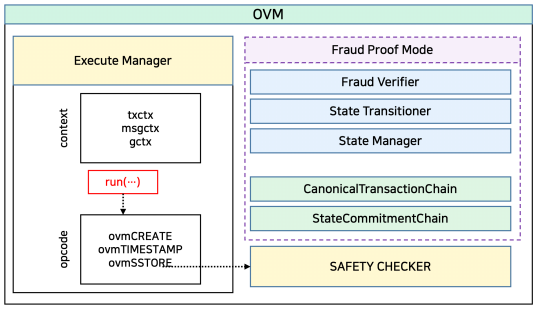
〔그림 7〕 Optimistic 롤업

명 데이터를 풀 노드에 요청해서 전달 받아야 하기 때문에, 풀 노드가 악의적이거나 데이터를 주지 않거나 네트워크의 문제로 데이터가 전달되지 못하는 데이터 가용성 문제(Data Availability Problem)가 여전히 존재한다[50]. 이러한 문제를 해결하기 위해 Optimistic 롤업은 레이어 2의 풀 노드가 레이어 1에 상태 값을 전달할 때, 트랜잭션들의 정보를 배치로 압축해 저장함으로써, 라이트 노드가 풀 노드에 의존하지 않고도 레이어 1의 등록된 배치 데이터를 통해 사기 증명을 수행할 수 있도록 한다. 또는 네트워크 내에 검증자 노드를 따로 둠으로써 지속적으로 배치와 상태 값을 검증하기도 한다.

사기증명을 레이어 1에서 실행하게 함으로써 데이터 가용성 문제를 해결했지만, 사기증명을 실행하게 되면 레이어 1에서 수수료 및 가스 비용이 들게 된다. 레이어 1에서 발생하는 비용을 최소화하기 위해 Optimistic 롤업은 담보금과 인센티브 정책을 사용한다[51]. 풀 노드로 참가하기 전 담보를 맡겨야 하며, 만약 잘못된 상태 값을 올린 것이 검증되면 담보금은 이를 검증한 노드에게 인센티브로 전달된다.

Optimistic 롤업은 네트워크에서는 컨텍스트(context)에 의존하는 opcode로 인해 사기 증명 검증 시 다른 결과를 가져올 수 있어 새로운 OVM(Optimistic Virtual Machine)을 정의한다. OVM은 레이어 1과 레이어 2에서 opcode 실행시 동일한 결과 값이 나오는 것을 보장한다[52]. [그림 8]은 Optimism의 OVM 구성 요소를 나타내며, [표 1]은 OVM 구성 요소들의 역할을 설명한다.

대표적인 Optimistic 롤업 프로젝트는 Optimism, Fuel Labs, OffChain Labs, Hubble 등이 있다.



[그림 8] OVM 구성요소

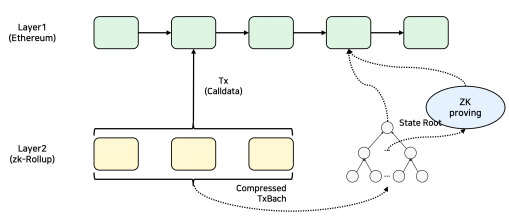
[표 1] OVM 구성요소 역할

구성요소	설명
Execute Manager	· L1과 L2 간의 결정적(deterministic) 스마트 컨트랙트 실행을 보장하는 샌드박스
Fraud Verifier	· 사기 증거 검증 프로세스 전체를 조정 · 새로운 사기 증거를 초기화하기 위해 State Transitioner를 호출 하고, 사기 증거가 성공적 이면 SCC 에서 분쟁 지점 이후에 게시된 배치를 제거
State Transitioner	· 사전 상태 루트로 분쟁 중인 경우 Fraud Verifier에 의해 배포됨 · Execute Manager 을 호출하고 규칙에 따라 온체인 트랜잭션을 실행 하여 분쟁 트랜잭션에 대한 올바른 사후 상태 루트를 생성하는 것
State Manager	· L2에서의 모든 상태에 저장 관리 · 사기 증거를 위해서 배치되고 분쟁 거래에 의해 영향을 받은 상태에 대한 정보만 포함하는 "임시" 상태 관리자
CanonicalTransactionChain (CTC)	· OVM 상태에 적용되는 트랜잭션의 append-only 로그 · 시퀀서는 L2의 트랜잭션 배치를 CTC에 추가
StateCommitmentChain (SCC)	· 사용가 CTC의 각 트랜잭션 결과라고 주장하는 상태 루트 목록을 포함 · SCC의 요소(Element)는 CTC 트랜잭션과 1:1 매칭 됨
SAFETY CHECKER	· execute Manager가 호출한 opcode가 맞는 opcode인지 확인 (1,0 반환)

6.2. ZK-Rollup

[그림 9]는 이더리움 네트워크 기반 ZK-롤업 방식을 보여준다. 레이어 2에서 발생되는 트랜잭션들은 수집되어 Batch 형태로 압축되고, 이를 영지식 증명(ZKP, Zero Knowledge Proof)을 통해 증명(Proof)를 생성하여 트랜잭션을 반영한 상태 루트 값과 함께 레이어 1에 저장된다. 레이어 1에 저장된 증명이 검증되면 상태 값을 업데이트한다[53].

ZK-롤업은 유효성 증명(Validity Proofs)에 기반을 두고 있는데, 배치를 통해 발생된 상태 값 변화가 올바르다는 증명을 영지식 증명을 이용해 생성하여 제출한다. 영지식 증명은 데이터를 공개하지 않고도 데이터



[그림 9] ZK-Rollup

를 가지고 있다는 사실을 증명하는 증명 방식 말한다. 제출된 증명은 레이어 1의 검증자가 스마트 컨트랙트를 통해 증명이 유효함을 검증한다. 여기서는 트랜잭션의 상태값 업데이트의 유효성만을 검증한다[53].

Optimistic 롤업과 비교해서 최종성 결정에 걸리는 기간과 출금 기간이 짧다는 장점을 가지고 있지만, 검증 컨트랙트의 사용에 대한 상대적으로 높은 가스 비용과 증명이 특정 유형의 거래에서만 사용이 가능하다는 단점이 존재한다.

대표적인 ZK-롤업 프로젝트는 zkSync, Aztec, STARKWARE, Loopring zkSwap 등이 있다.

Ⅶ. 결 론

블록체인의 높은 확장성, 공격에 대한 복원력, 신뢰성, 추적성은 사물인터넷 서비스의 보안성, 신뢰성을 향상시킬 수 있다. 이에, 본 논문에서는 사물인터넷과 블록체인의 융합에 있어서 걸림돌이 되는 문제점들과 요구사항을 도출하였다. 또한, 사물인터넷 서비스의 요구사항들을 만족시킬 수 있는 블록체인 기술 동향을 살펴보았다. 특히, 블록체인 분야에서 가장 활발히 연구되고 있으며 사물인터넷의 대용량/실시간 데이터 처리, 개인정보보호 등에 활용될 수 있는 샤딩, 상태 채널, 플라즈마, 롤업 기술에 대해 자세히 살펴보았다.

블록체인 기술과 사물인터넷의 융합은 모든 산업 분야에 혁신을 일으킬 수 있으며, 이와 관련된 다양한 서비스가 개발될 것으로 보인다. 따라서, 본 논문에서 도출한 대용량/실시간 데이터 처리 기술, 경량 합의 알고리즘 및 스마트 컨트랙트 기술, 사물인터넷 데이터 신뢰성 보장 및 시스템 보안 연동 기술, 사물인터넷 데이터 관리 및 플랫폼 연동 기술, 블록체인 상에서의 개인정보보호 기술들에 대한 지속적인 연구가 필요할 것으로 보인다.

참 고 문 헌

[1] Deloitte, "Internet of Things (IoT), The rise of the connected world", Confederation of Indian Industry, 2020

[2] KOUICEM, Djamel Eddine; BOUABDALLAH, Abdelmadjid; LAKHLEF, Hicham. Internet of things security: A top-down survey. Computer Networks, 2018, 141: 199-221.

[3] OZA, S.; MATHPAL, D. A study on Internet of things security and lightweight cryptography. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 2018, 3.3: 683-689.

[4] SALIMITARI, Mehrdad; CHATTERJEE, Mainak; FALLAH, Yaser P. A survey on consensus methods in blockchain for resource-constrained IoT networks. Internet of Things, 2020, 11: 100212.

[5] MAPLE, Carsten. Security and privacy in the internet of things. Journal of Cyber Policy, 2017, 2.2: 155-184.

[6] WANG, Wenbo, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks. Ieee Access, 2019, 7: 22328-22370.

[7] Ethereum. Sharding faq. https://github.com/ethereum/wiki/wiki/Sharding-FAQ. [Online, Accessed: Nov/19/2019].

[8] KIM, Soohyeong; KWON, Yongseok; CHO, Sunghyun. A survey of scalability solutions on blockchain. In: 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2018. p. 1204-1207.

[9] Vitalik Buterin. The meaning of decentralization. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. [Online, Accessed: Nov/19/2019].

[10] KIAYIAS, Aggelos; PANAGIOTAKOS, Giorgos. Speed-security tradeoffs in blockchain protocols. Cryptology ePrint Archive, 2015.

[11] KUMAR, Nallapaneni Manoj; MALLICK, Pradeep Kumar. Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 2018, 132: 1815-1823.

[12] EOS, “https://eos.io/“

[13] Solana, “https://solana.com/ko”

[14] IoTex, “https://iotex.io/”

[15] ZHENG, Zibin, et al. Blockchain challenges and

opportunities: A survey. International Journal of Web and Grid Services, 2018, 14.4: 352-375.

[16] SEHGAL, Anuj, et al. Management of resource constrained devices in the internet of things. IEEE Communications Magazine, 2012, 50.12: 144-149.

[17] YEOW, Kimchai, et al. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. IEEE Access, 2017, 6: 1513-1524.

[18] HAN, Xuan; YUAN, Yong; WANG, Fei-Yue. A fair blockchain based on proof of credit. IEEE Transactions on Computational Social Systems, 2019, 6.5: 922-931.

[19] CALDARELLI, Giulio. Understanding the blockchain oracle problem: A call for action. Information, 2020, 11.11: 509.

[20] FRANKENREITER, Jens. The limits of smart contracts. Journal of Institutional and Theoretical Economics, 2019, 175.1: 149-162.

[21] LIU, Chunchi, et al. Extending On-chain Trust to Off-chain--Trustworthy Blockchain Data Collection using Trusted Execution Environment (TEE). IEEE Transactions on Computers, 2022.

[22] LUECKING, Markus, et al. Decentralized identity and trust management framework for Internet of Things. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020. p. 1-9.

[23] FAN, Xinxin, et al. DIAM-IoT: a decentralized identity and access management framework for internet of things. In: Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure. 2020. p. 186-191.

[24] IoTex DID, “https://onboard.iotex.io/platform/did”

[25] LEE, Euijong, et al. A Survey on Standards for Interoperability and Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 2021, 23.2: 1020-1047.

[26] Witanto, Elizabeth Nathania, et al. "A blockchain-based OCF firmware update for IoT devices." Applied Sciences 10.19 (2020): 6744.

[27] ZHENG, Qiuhong, et al. An innovative IPFS-based storage model for blockchain. In: 2018 IEEE/WIC/ACM international conference on web intelligence (WI). IEEE, 2018. p. 704-708.

[28] the graph, “https://thegraph.com/en/”

[29] 이상현, 김용수, 김호원. 블록체인 프라이버시 보호 프로토콜 동향 및 분석. 한국통신학회논문지, 2019, 44.12: 2252-2259.

[30] Hyperledger Fabric Private Data Collection, “https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html?highlight=private”

[31] ZCash ZK-SNARK, “https://z.cash/technology/zksnarks/”

[32] Monero Bulletproofs, “https://web.getmonero.org/resources/moneropedia/bulletproofs.html”

[33] BOO, EunSeong; KIM, Joongheon; KO, JeongGil. LiteZKP: Lightening zero-knowledge proof-based blockchains for IoT and edge platforms. IEEE Systems Journal, 2021.

[34] ethereum on-chain scaling, “https://ethereum.org/en/developers/docs/scaling/#sharding”

[35] LUU, Loi, et al. A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016. p. 17-30.

[36] The Zilliqa Technical Whitepaper, “https://docs.zilliqa.com/whitepaper.pdf”

[37] Zilliqa Sharding Mechanism, “https://dev.zilliqa.com/docs/basics/basics-zil-sharding/”

[38] 1.Xi, J. et al. A Comprehensive Survey on Sharding in Blockchains. Mob Inf Syst 2021, 1–22 (2021).

[39] DZIEMBOWSKI, Stefan; FAUST, Sebastian; HOSTÁKOVÁ, Kristina. General state channel networks. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018. p. 949-966.

[40] POON, Joseph; DRYJA, Thaddeus. The bitcoin

lightning network: Scalable off-chain instant payments. 2016.
[41] HEES, Heiko. Raiden network: Off-chain state network for fast DApps. In: Devcon two. Ethereum Foundation, 2016.
[42] POON, Joseph; BUTERIN, Vitalik. Plasma: Scalable autonomous smart contracts. White paper, 2017, 1-47.
[43] Plasma MVP, “https://www.learnplasma.org/en/learn/mvp.html”
[44] KONSTANTOPOULOS, Georgios. Plasma cash: towards more efficient plasma constructions. arXiv preprint arXiv:1911.12095, 2019.
[45] “Plasma Debit: Arbitrary-denomination payments in Plasma Cash”, ethresearch, last modified Jan 19.2019, accessed Apr 06,2022,https://ethresear.ch/t/plasma-debit-arbitrary-denomination-payments-in-plasma-cash/2198/46
[46] SGUANCI, Cosimo; SPATAFORA, Roberto; VERGANI, Andrea Mario. Layer 2 blockchain scaling: A survey. arXiv preprint arXiv:2107.10881, 2021.
[47] MARUKHNENKO, Oleksandr; KHALIMOV, Gennady. The Overview of Decentralized Systems Scaling Methods. COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES, 2021.
[48] L2 − Deep Dive into OVM, “https://starli.medium.com/l2-deep-dive-into-ovm-e2229052ed00”
[49] AL-BASSAM, Mustafa; SONNINO, Alberto; BUTERIN, Vitalik. Fraud proofs: Maximising light client security and scaling blockchains with dishonest majorities. arXiv preprint arXiv:1809.09044, 2018, 160.
[50] Vitalik Buterin and Peter Todd Go Head to Head in the Crypto Culture Wars, “https://www.trustnodes.com/2017/08/14/vitalik-buterin-peter-todd-go-head-head-crypto-culture-wars”
[51] ethereum optimistic-rollup, “https://ethereum.org/ko/developers/docs/scaling/optimistic-rollups/”
[52] How does Optimism’s Rollup really work?, “https://research.paradigm.xyz/optimism”
[53] Zkstark medium, “https://medium.com/starkware/tagged/zkstark”

〈저 자 소 개〉

허 신 욱 (ShinWook Heo)
정회원
2015년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2018년 2월 : 부산대학교 전기전자컴퓨터공학과 박사과정 수료
2018년 2월~2021년 9월 : 부산대학교 전기전컴퓨터공학과 수료후 연구생
2021년 9월~현재 : (주)스마트엠투엠 책임연구원
<관심분야> 암호구현, 정보보호

조 욱 (Uk Jo)
학생회원
2012년 2월 : 광운대학교 전자공학 학사 졸업
2016년 2월 : 광운대학교 전자공학 석사 졸업
2020년 3월~현재 : 부산대학교 정보융합공학과 박사과정
<관심분야> 블록체인, 보안

김 금 보 (GuemBo Kim)
학생회원
2021년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2021년 3월~현재 : 부산대학교 컴퓨터공학과 석사과정
<관심분야> 블록체인, 보안

권 율 (Yool Kwon)
학생회원
2022년 2월 : 부산대학교 나노에너지 공학과 학사 졸업
2021년 3월~현재 : 부산대학교 컴퓨터공학과 석사과정
<관심분야> 블록체인, 보안

김 호 원 (Howon Kim)
종신회원
1993년 2월 : 경북대학교 공학사
1995년 2월 : 포항공과대학교 공학석사
1999년 2월 : 포항공과대학교 공학박사
2004년: Ruhr University Bochum, Post Doctorial
1998년~2008년 : 한국전자통신연구원 팀장
2008년~현재 : 부산대학교 전기컴퓨터공학부 교수
<관심분야> 블록체인, 보안, 사물인터넷