블록체인 기반 모바일 엣지 컴퓨팅(Mobile Edge Computing): 이슈 및 해결 후보 기술

소빗 반다리 · 조홍평 · 김훈

인천대학교

5G 이동통신과 더불어 모바일 엣지 컴퓨팅(Mobile Edge Computing: MEC)의 도입이 시작되고, 그 응용 분야 또한 점차 확대되고 있는 상황이다. 블록체인은 비트코인(Bitcoin)과 같은 가상화폐의 근간이 되는 기술로 분산 데이터 관리 프레임워크 등을 시작으로 그 활용 가치가 점차 확대 고려되고 있으며, MEC 환경에서 블록체인(Blockchain)과의 연동을 다루는 연구에 대한 관심 또한 대두되고 있다.

블록체인은 금융, 의료, 물류 등 다양한 애플리케이션에서 채택되어 왔지만, 모바일 서비스에서의 애플리케이션은 여전히 제한적이다. 이는 모발일 블록체인 사용자가 새로운 데이터 즉, 블록을 블록체인에 추가하기 위해 미리 설정된 작업 증명 퍼즐을 해결해야 하는 과정이 요구되기 때문이다. 이 작업 증명을 해결하면 컴퓨팅 자원이 제한적인 모바일 장치에 CPU 시간 및 에너지 측면에서 상당한 자원 소비를 필요로 하여 현 수준의 단말로는 적합하지 않은 점이 있다.

본 기고에서는 이와 같은 블록체인의 MEC 환경에의 접목에서 발생하는 기술적 이슈를 검토하며, 이를 효과적으로 해소하는 연구를 소개한다. 이를 위해 먼저 모바일 블록체인 기술을 위한 MEC 시스템 구조를 소개한다. 이어 블록체인 기반 MEC 시스템 운용 시나리오를 살펴보고, 주요 기술 이슈와 함께 이를 효과적으로 해결하는 솔루션을 차례로 제시한다.

Ⅰ. 서 론

MEC는 ETSI 산업 표준 그룹(Industry Specification Group: ISG)에서 클라우드 컴퓨팅 기능을 무선접속네트워크(Radio Access Network: RAN)와 모바일 사용자에 가까이 위치한 네트워크의 종단에 IT 서비스 환경을 제공하고자 제안되었다.[1],[2] MEC는 클라우드 컴퓨팅, 그리드 컴퓨팅 그리고 IoT를 아우르는 융합 기술이다. 이는 클라우드와 사용자 단말기 사이에 층이 추가되고, 컴퓨팅 자원을 종단 사용자에 더욱 가까이에서 지원하려는 것이다. 이는 사용자 단말기 또는 시스템에서 컴퓨팅 자원이 필요해짐에 따라 이를 위한 지원이 클라우드를 대신하여 엣지 서버에서 분산적으로 처리됨을 의미한다. '엣지'는 기지국 자체와 무선네트워크에 가까이 위치한 데이터 센터를 지칭한다. 운용자는 RAN 엣지를 허가된 제3자에게 개방하여 모바일 가입자, 기업, 세부 응용 분야에 혁신적인 응용과 서비스가 유연하게 그리고 적기에 제공 가능하도록 한다. MEC는 이처럼 그 이득이 운영자뿐만 아니라, 제3자 기업과 OTT(Over-The-Top) 기업에게 제공되어 모바일 엣지, 모바일 가입자 가까이에서 기업 솔루션이 제공되는 기회를 얻는다. MEC는 또한 일반적인 통신 서비스 관점에서도 보다 향상된 서비스 경험을 사용자에게 제공할 수 있다.

엣지 컴퓨팅은 최종 사용자에게 데이터 계산, 저장 및 응용 프로그램 서비스를 제공할 수 있는 새로운 분산형 패러다임이며, 실시간 응답, 위치 인식 및 터미널 장치와의 근접성으로 인한 이동성과 같은 몇 가지 이점을 제공한다. 기존 연구에서 스마트 그리드, 스마트 트래픽 조명, 증강 현실 응용, 비디오 스트리밍 등과 같은 다양한 시나리오에 적합하다는 것을 보이고, MEC가 서비스의 효율성과 품질을 높일 수 있음을 제시한다[1]~[5].

엣지 컴퓨팅은 많은 이점을 가져다주지만 다양한 보안 및 개인 정보 위협에 직면해 있다. 한편, 엣지 컴퓨팅은 클라우드 컴퓨팅의 확장으로 간주되기 때문에 클라우드 컴퓨팅의 일부 보안 문제를 상속한다. 한편, 엣지 컴퓨팅은 지리적 분포, 이질성 및 낮은 대기 시간과 같은 고유한 기능으로 인해 보안 및 개인 정보 보호 문제에 직면한다. 보안 데이터

본 기고는 2019년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2019019904).

분석을 수행하려면 보안 메커니즘을 배포하는 것이 필수적이다. 불행하게도 엣지 장치의 제한된 자원 때문에, 클라우드 프레임 워크에서 제안된 전형적인 보안 메커니즘은 엣지 프레임 워크에 적합하지 않다. 따라서 IoT 애플리케이션 기반의 안정적이고 효율적인 엣지 컴퓨팅을 지원하기 위해 엣지 컴퓨팅에서 보안 솔루션을 개발하는 것이 중요하다.

유사하게 블록체인은 비트코인, 이더(Ether) 등과 같은 가상화폐시스템의 근간이 되는 기술이다. 이는 본질적으로 기록의 보관 방식이며, 기록 보관 또는 데이터베이스 관리의 일부 형식을 사용하는 거의 모든 제품에서 사용할 수 있다. 변경 불가능하고 파괴할 필요가 없는 모든 데이터를 보호하는 것에 이상적이다. 전통적으로 데이터는 타사에서 소유하고 운영하는 서버에 보관된다. 이러한 중앙 집중식 접근 방식에는 트랜잭션 처리 효율성이 낮고, 단일 지점 오류 및 공격, 중앙 당국의 도덕적 위험과 같은 몇 가지 단점이 있다. 이러한 방식으로 제3자가 귀하의 데이터에 액세스 할 수 있다면 데이터의 파괴 가능성이 커지고 누출 위험이 뒤따른다. 블록체인을 통해 데이터는 암호화된 다음 분산된 컴퓨터 네트워크를 통해 전파된다. 이러한 방식으로 데이터는 절대적인 누군가에 의해서만 소유되지 않으며, 데이터의 파괴나 변경 또한 어렵게 된다. 블록체인의 모든 사용자의 트랜잭션은 블록으로 기록되며, 블록체인에 추가된 트랜잭션 데이터 간의 논리적 관계를 나타내기 위해 연결된 목록 데이터 구조로 서로 연결된다. 데이터 블록은 중앙 집중식 시스템과 달리 전체 네트워크에서 복사되고 공유된다. 블록체인은 여러 분산 시스템 및 다중 액세스 네트워크 애플리케이션 시나리오, 예를 들어 컨텐츠 전달 네트워크, 인지 무선 및 스마트 그리드 시스템에 적용되어 왔다. 블록체인이 많이 언급되는 많은 다른 응용 프로그램이 있다.

블록체인의 모든 거래는 광부에 의해 확인되며, 광부 중 51 %만 승인할 경우에만 승인된다. 광부는 작업 증명이라고 하는 계산상 어려운 문제를 해결하여 거래를 검증할 책임이 있는 사람들이다. 광부들은 블록 채광에 대한 인센티브를 제공받는다. 작업 증명 퍼즐을 해결하는 것은 실질적으로 컴퓨팅 능력을 소모하기 때문에 자원 제약이 발생할 수 있는 모바일 시스템에서는 블록체인을 일반적으로 널리 채택하지 않는다. 블록체인의 배치는 예기치 않은 토폴로지 및 단순한 장치로 고도로 분산되는 IoT(Internet of Things) 네트워크 아키텍처에서 큰 문제에 직면하게 된다. 이 문제는 여러 블록체인 사용자가 광산업에서 승리하기 위해 경쟁하기 때문에 더 어려워질 것이다. 즉, 작업 증명 퍼즐을 완전히 풀어 결과를 블록체인 네트워크, 즉 광부 네트워크에 전파하고 블록체인 사용자는 사용한 컴퓨팅 파워와 성공적인 광산의 보상을 절충해야 한다.

MEC의 보안 문제는 블록체인 기술의 구현으로 해결할 수 있다. 마찬가지로 블록체인 기술에 필요한 컴퓨팅 성능은 엣지 자원을 활용하여 완화할 수 있다. 블록체인 사용자는 작업 증명 퍼즐을 해결하는 작업을 엣지 컴퓨팅 서비스로 오프로드하여 광업 및 블록체인에서 성공할 가능성을 높일 수 있다.

엣지 컴퓨팅 환경에서, 로컬 데이터 센터 및 서버는 이동 네트워크의 "엣지"에서 엣지 컴퓨팅 서비스 제공자, 예를 들어 무선 액세스 네트워크의 기지국 및 액세스 포인트에 의해 배치된다. 모바일 IoT 장치는 엣지 컴퓨팅 서버에 액세스하여 IoT 감지 데이터 분석 및 처리와 같은 모바일 작업의 컴퓨팅 성능을 향상시킬 수 있다. 원격 클라우드 및 데이터 센터를 통하지 않고 모바일 IoT 사용자의 컴퓨팅 작업을 로컬에서 엣지 컴퓨팅 서비스로 오프 로딩함으로써 대기 시간 및 백홀 대역폭 사용을 상당히 줄일 수 있다. 이 기능을 통해 엣지 컴퓨팅은 모바일 환경에서의 블록체인 애플리케이션의 유망한 패러다임이 될 수 있다. 블록체인 사용자는 작업 증명 퍼즐을 해결하는 작업을 엣지 컴퓨팅 서비스로 오프로드 하여 광업 및 블록체인의 성공 가능성을 높일 수 있다.

본 기고에서는 모바일 사용자인 IoT 장치가 분산 MEC 서비스 공급자로부터 블록체인 응용 프로그램을 지원하기 위해 전략적으로 데이터, 정보 및 컴퓨팅 성능에 액세스하여 자원를 활용할 수 있는 엣지 컴퓨팅을 지원하는 모바일 IoT 블록체인 네트워크에 관한 연구 동향을 소개한다.

먼저 2장에서 엣지 컴퓨팅과 블록체인 아키텍처의 시스템 모델을 제시하고 3장과 4장에서는 블록체인을 사용하는 엣지 컴퓨팅의 사용 사례와 기술적 문제를 제시한다. 다음으로 5장에서 가능한 솔루션 접근 방식들을 일부 소개하고 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 시스템 모델 및 구조

블록체인의 기본 개념은 체인 형태의 데이터 구조이다. 체인의 각 노드는 히스토리, 검증된 트랜잭션, 정보 및 제어 데이터를 포함하는 데이터 블록이다. 블록체인을 복제하고 블록체인 네트워크의 모든 참여자에게 보급하여 블록체인에 포함 된 데이터를 전역적으로 동기화 할 수 있다.

그림 1은 블로체인 기반 MEC 시스템 구조 구조를 보인다. 블록체인의 각 블록에는 일반적으로 트랜잭션 데이터와 해시 값의 두 부분이 있다. 트랜잭션 데이터는 블록체인 사용자 또는 시스템, 예를 들어, 모바일 IoT 장치에 의해 기록된다. 해시 값은 코딩된 정보나 보안된 정보를 저장하는 데 사용된다. 블록 내의 해쉬 값은 이전 블록의 정보에 기초하여 생성되며, 이는 현재 블록으로부터 그 블록 이전의 블록을 포인팅하는 링크와 유사하다. 블록체인의 첫 번째 블록은 초기 블록을 가리키는 해시 값이 없는 기성 블록이라고 한다. 또한 타임 스탬프와 해시 트리 같은 다른 데이터 구조가 블록에 포함되어 보안 및 트랜잭션 성능 요구 사항을 향상시킬 수 있다. 일반적으로 블록체인은 다음 단계로 작동한다.

i. 블록체인 사용자는 트랜잭션을 수행하고, 새 트랜잭션 레코드를 작성하며, 새로운 트랜잭션은 블록체인 네트워크에서 인접한 피어 사용자에게 전송된다.

ii. 각 이웃 피어 사용자는 특정 기간 동안 전송된 트랜잭션을 수집한다. 가짜 사용자 거래와 같은 거래 또는 직불 결제 계정의 마이너스 잔액은 삭제되고, 이 기간이 지나면 일련의 트랜잭션을 수집한 사용자가 트랜잭션을 블록으로 채우고 마이닝을 수행한다.

iii. 마이닝된 블록은 다른 블록체인 사용자에게 알리기 위해 네트워크로 전송된다. 마이닝된 블록을 수신한 다른 사용자는 이에 따라 보안 메커니즘의 유효성을 검사한다. 블록의 유효성이 입증되면 현재 블록체인의 끝에 추가된다. 이 경우, 사용자의 뷰, 즉 현재 블록체인의 내용 및 구조가 업데이트되었다. 2단계에서 생성된 블록의 트랜잭션은 일반적으로 블록체인 사용자가 수락한다. 이것은 합의로 불린다.

2-1 블록체인 동작 원리와 MEC 환경

2-1-1 분산 컨센서스

블록체인은 노드간 신뢰가 상호 보장되어 있지 않은 분산 네트워크에서 트랜잭션 및 데이터에 대한 암호화 이상의 기능을 제공할 수 있다. 악의적인 중개인에 의해 블록체인이 변경, 위조 또는 삭제되는 것을 방지하기 위해 암호화 기술이 광산업에 채택되는 동안, 블록체인은 많은 사용자들에 의해 인정받게 된다. 컨센서스는 네트워크의 신뢰를 보장하는 메커니즘으로, 네트워크의 사용자가 기존 블록체인에 추가된 블록의 동의에 도달하는 것을 의미한다. 사용자는 네트워크에서 확인된 블록체인을 얻고 확인하여 공격자가 삽입한 잘못된 트랜잭션을 발견할 수 있다. 따라서 대다수의 사용자는 잘못된 거래를 버리도록 거부할 수 있다. 컨센서스의 배포는 모바일 네트워크와 같은 독립 사용자가 있는 분산 컴퓨팅 시스템에 유용하다.

2-1-2 작업 증명 기반 마이닝

그러나 공격자가 가짜 블록체인 정보와 많은 익명의 사용자를 네트워크에서 생성하는 Sybil 공격과 같은 공격에 대해서는 여전히 합의가 이루어질 수 있다. 가짜 블록체인 정보와 익명의 사용자는 공격자가 생성한 잘못된 트랜잭션에 대한 합의로 이어질 수 있다. 이러한 공격에 대한 해결책은 공격자가 네트워크의 가짜 사용자를 지원할 수 있는 충분한 컴퓨팅 성능을 가질 수 없도록 광업의 복잡성을 높이는 것이다. PoW는 광업 복잡성을 증가시키는 데 사용되고 생산이 어렵지만, 쉽게 검증할 수 있는 작업 프로세스이다. PoW를 해결하면 헤더 해시 값을 주어진 "난이도 목표"보다 낮게 만드는 값을 계산해야 한다. 트랜잭션의 무결성과 유효성을 확인하고 확보하는 것은 일련의 광부에 의해 실행된다. 비트코인과 같은 많은 블록체인 시스템에서 블록을 성공적으로 채광하는 광부는 채굴된 블록이 블록체인에 성공적으로 추가될 때 채광 보상을 받는다. 합의는 블록체인 시스템의 보안과 신뢰성을 보장하고, 광업이 비용이 많이 드는 블록체인 네트워크에서 공격자는 블록체인을 조작하기 위해 원칙적으로 네트워크의 모든 컴퓨팅 성능의 51 % 이

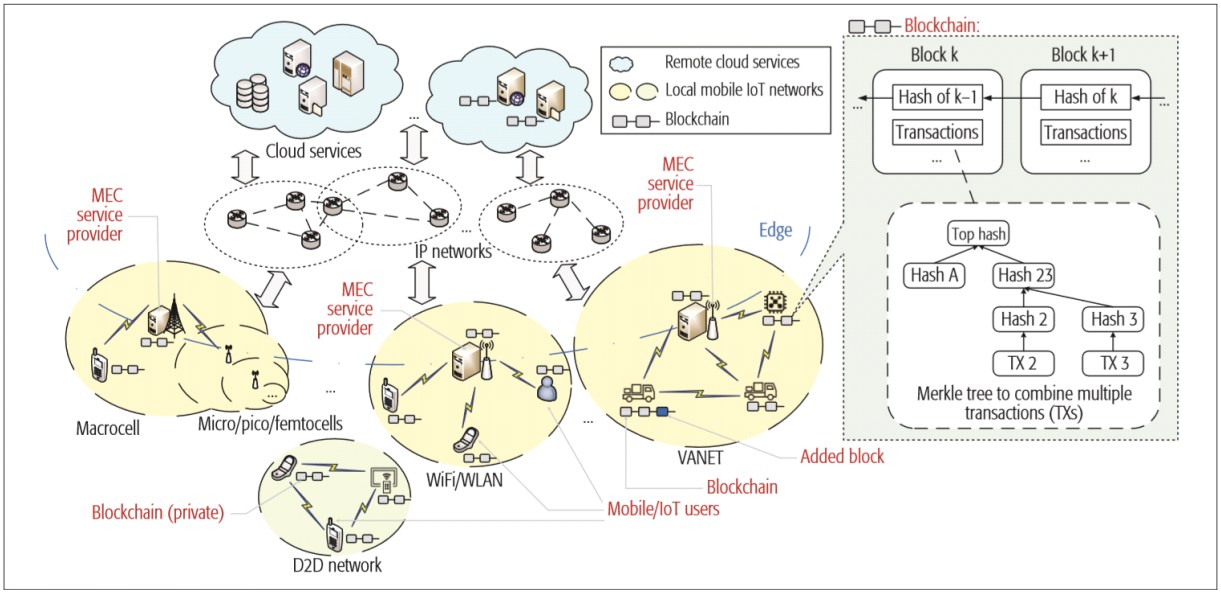
상을 제어해야 한다. 이것은 공격자에게 엄청난 비용이며, 실제로는 거의 실현될 수 없다.

이같은 분산 컨센서스와 작업 증명 기반 마이닝을 효과적으로 적용하기 위해서는 노드의 이동성과 분산적 네트워크 구조가 기반이 되는 모바일 네트워크 환경이 고려될 수 있다.

Ⅲ. 모바일 엣지 컴퓨팅: 사용 예와 서비스 시나리오

최근 블록체인은 다양한 네트워크 및 분산 시스템에서 많은 애플리케이션에 대한 가능성이 확인되고 있으며, 그 중 하나가 IoT이다. IoT 시스템은 모바일 네트워크의 대표적인 응용 환경이며, 모바일 장치, 센서 및 액추에이터와 같은 다양한 물리적 개체가 인터넷에 연결되는 구조이다.

IoT 장치는 스마트 교통, 물류, 의료 및 제조와 같은 특정 시스템 목표를 달성하기 위해 서로 정보를 감지, 교환 및 교환할 수 있다. 그러나 IoT 장치는 일반적으로 저전력, 지리적으로 분산되어 있으며, 이동 가능한 경우가 많다. 즉, 제한된 컴퓨팅 자원과 IoT 장치의 에너지 공급에서의 제한은 블록체인이 일반적인 IoT 시스템에 적용될 시에, 특히 마이닝 프로세스에 의해 주요 장벽이 될 수도 있다. 대신 MEC는 모바일 블록체인을 위한 컴퓨팅 및 통신 자원을 제공할 수 있다. 즉, MEC를 사용하면 서비스 제공 업체는 [그림 1]에서와 같이 모바일 인터넷의 '가장자리'에서 클라우드 컴퓨팅 서비스를 배포할 수 있다. 예를 들어 소규모 데이터 센터가 설치된 기지국 또는 무선 액세스 네트워크의 서버 세트는 오프로드 작업을 수용할 수 있고, 인접한 모바일 및 IoT 장치에서 로컬 컴퓨팅 성능을 제공함으로써 MEC은 PoW 퍼즐, 해싱, 암호화 알고리즘 및 가능한 합의를 해결할 수 있도록 IoT 네트워크에서 블록체인 배포를 지원한다. 엣지 컴퓨팅 서비스 공급자와 IoT 장치 또는 사용자 간의 상호작용은 IoT 사용자로부터 수익을 창출하는 데이터 및 컴퓨팅 파워와 같은 자원를 판매하는 시장 활동으로 모델링할 수 있다. 실제로는 클라우드와 블록체인을 통합하는 비슷한 개념이 실현된다. 예를 들어, Microsoft는 Azure 클라우드 플랫폼에서의 서비스 형태로 블록체인(BaaS)을 제공한다. 영국의 회사인 CloudHashing은 Bitcoin Mining as a Service(MaaS)를 제공하며, 사용자는 하드웨어 장비를 설치 및 배치하지 않고, 온라인 Bitcoins 소프트웨어 서비스만 구입할 수 있다. IBM은 IBM의 비즈니스 레벨 클라우드 서비스에 통합된 개인 블록체인 원장에서 IoT 데이터를 관리하기 위해 Watson IoT 플랫폼을 제공한다. 모든 클라우드 기반 블록체인 서비스에도 불구하고, 엣지 컴퓨팅 시스템에서 블록체인 트랜잭션을 위한 경제적 모델은 잘 연구되지가 않고 있다. 또한 엣



[그림 1] 블록체인 기반 MEC 시스템[6]

지 컴퓨팅 서비스는 안개 노드(fog node) 또는 광부에 가까운 엣지 장치(edge device)와 같이 클라우드 컴퓨팅보다 대기 시간이 훨씬 짧은 근거리 컴퓨팅 장치를 제공할 수 있고, 따라서 지연에 민감한 IoT 애플리케이션에 적합하다. 모바일 블록체인을 염두한 MEC 서비스는 다양한 애플리케이션 시나리오에 적용될 수 있으며, 아래와 같이 대표적인 사례가 도출된다.

3-1 안전한 스마트 홈

스마트 장치 제조업체나 소매 업체가 관리하는 중앙 집중식 데이터베이스에 다량의 가정 및 개인 데이터를 업로드하는 가전제품은 심각한 프라이버시 문제에 노출될 수 있다. 따라서 블록체인을 사용하는 IoT의 엣지 컴퓨팅은 스마트 홈에서 개인 데이터 관리를 위한 투명하고 안전한 대체 프레임 워크를 제공할 수 있다.

3-2 스마트 그리드

스마트 그리드 시스템은 이기종 센서(예: 스마트 미터)를 포함한다. 스마트 계량기의 경우 에너지 소비 데이터 및 에너지 거래가 기록되고, 엣지 컴퓨팅은 스마트 미터와 함께 통합되어 복잡한 작업을 자동으로 처리할 수 있다(예: 트랜잭션 준비, 스마트 전기 계약 실행 및 그리드로드 균형 조정). 비슷한 개념이 에너지 저장 공유를 지원하기 위해 플러그인 하이브리드 전기 자동차(PHEV)에 적용될 수 있다.

3-3 안전한 치료

MEC 기반의 IoT 치료 플랫폼은 장애인을 대상으로 분산된 방식으로 전신 공동동작 데이터 범위를 제공할 수 있다. MEC를 이 프레임워크에 활용하여 장애로 태어났거나, 사고, 전쟁으로 인한 부상 또는 노령으로 장애인이 된 인류의 상당 부분에 대한 치료 진단 및 분석 데이터를 제공할 수 있다. 보안을 위해 프레임 워크는 Blockchain-Tor 기반 분산 트랜잭션을 사용하여 치료 데이터 개인 정보, 소유권, 생성, 저장 및 공유 상태로 보존된다.

3-4 크라우드 소싱

IoT 시스템에서 크라우드 소싱은 미정의 IoT 장치 세트가 내용을 점진적으로 생성 및 수정하여 작업(예: 감지)을 완료하도록 허용한다. 모바일 엣지 컴퓨팅을 지원하는 블록체인은 데이터를 디지털화 된 자산으로 투명하고 안전하게 전송할 수 있다. 컴퓨팅 능력의 제약으로 인해 IoT 장치는 추후 처리를 위해 엣지 컴퓨팅 서버로 데이터를 오프로드 할 수 있다. 또한 IoT 장치에 대한 보상 및 지불을 위해 기록 추적 가능 레코드를 블록체인에서 사용할 수 있다.

Ⅳ. 연구 이슈

블록체인을 사용하여 IoT용 MEC에서 해결해야할 많은 문제가 여전히 있는데, 그 중 일부는 다음과 같다.

4-1 보안 문제

블록체인은 분산 데이터 처리 및 스토리지에 대한 매력적인 보안 기능을 제공하지만, 블록체인이 엣지 컴퓨팅을 지원하는 IoT 시스템, 특히 사설 블록체인에 맞게 조정되면 일부 보안 문제가 발생한다. 하나의 가능한 구현은 모든 네트워크 노드가 서로를 신뢰하는 소규모 '화이트리스트' IoT 네트워크일 수 있으며, PoW는 반드시 신뢰 메커니즘으로 요구되지는 않는다. 이 경우 모바일 IoT 장치에서 모바일 엣지 컴퓨팅 서버로 트랜잭션 데이터를 전송할 때 공격이 발생할 수 있다. 장치와 서버 사이의 안전하고 신뢰할 수 있는 네트워크가 필요하다. IoT 장치가 보호 수준이 낮기 때문에 모바일 IoT 네트워크에서 DDoS(Distributed Denial of Service) 공격을 쉽게 시작할 수 있는데, 마찬가지로 모바일 IoT 장치는 무선 전송에 의존하기 때문에 방해 전파(jamming) 공격은 블록체인 데이터 교환을 방해할 수 있다.

4-2 불균형한 컴퓨팅 성능

합의 방법이 잘 설계되어 있다면 블록체인 네트워크에는 신뢰가 필요하지 않지만, 침입자가 블록체인 네트워크의 51 % 이상의 컴퓨팅 성능을 제어할 수 있다면 침입자는 블록체인 레코드를 속이거나 속일 수 있다. 이로 인해 공격자는 네트워크에서 많은 수의 블록체인 광부와 협력해야 한다. 이는 실제로 달성하기 어려울 수 있으나, MEC 서비스를 사용하는 IoT 시스템에서는 모바일 IoT 네트워크의 컴퓨팅 성능이 낮기 때문에 이 문제가 중요시 되고 있다. 소수의 침입

자 또는 손상된 서버만이 '51 % 공격' 협력 상황을 쉽게 야기할 수 있다. 그러한 담합을 방지하기 위한 효과적인 메커니즘이 개발되어야 한다.

4-3 자원 활용 및 할당

앞서 서술한 바와 같이 모바일 IoT 장치는 블록체인의 작업 증명 퍼즐을 효율적으로 해결할 수 없다. MEC 서비스는 마이닝을 수행하도록 조정될 수 있다. 다음은 IoT 사용자 주변 네트워크 가장자리에 마이닝 작업을 오프로드하기 위한 새로운 패러다임을 제시함으로써 또한 MEC가 가능한 블록체인 네트워크의 시범 프로토타입을 구현하고, 자원 사용률을 분석하여 최적화된 자원 운용과 관리가 되도록 한다.

Ⅴ. 기술적 해결책

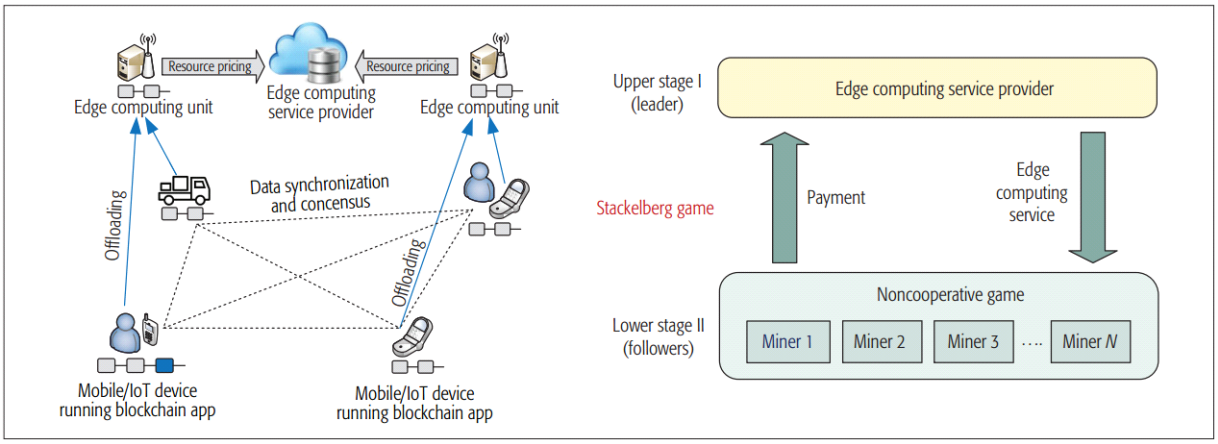
블록체인이 가능한 MEC 시스템의 기술적 문제를 해결하기 위한 다양한 솔루션 접근법이 제시된다.

5-1 엣지 컴퓨팅 자원 관리[2]

[그림 2]에서와 같이 Stackelberg 게임 기반 모델은 광부에 대한 보상과 서비스 제공자에게 지불할 가격을 결정함으로써 이익을 극대화할 것을 제안한다.

모바일 블록체인 네트워크는 광부로 활동하는 N명의 사용자로 구성되어 있다. 각 사용자는 모바일 블록체인 응용 프로그램을 실행하여 트랜잭션 데이터를 기록한다. MEC 서비스 제공 업체는 광부를 위해 엣지 컴퓨팅 서버를 배포한다. PoW 퍼즐은 MEC 서버로 오프로드 할 수 있으며, 광부는 공급자가 가격을 책정한다. 무선 액세스로 인한 통신 지연이 무시할 수 있는 상대적으로 작은 블록체인 네트워크가 고려되며, 오프로드 된 마이닝 프로세스는 데이터 마스킹이나 난독 화와 같은 보안 솔루션에 의해 보호되어 블록체인의 퍼즐 해결에 대한 세부 사항을 숨기고 제공자(판매자)는 엣지 컴퓨팅 서비스를 액세스하고 소비하는 광부(구매자)로부터 지불을 수신한다. MEC에 대한 통신 및 액세스는 광부의 에너지를 소비하지만, 그럼에도 불구하고 PoW를 해결하는 데 필요한 것보다 훨씬 적다. 따라서 사용자의 이동 장치는 통신 기능이 지원되며, 각 광부는 현재 블록체인 동작(예: 블록체인 데이터 동기화)에 따라 CPU 속도 또는 사용할 CPU 코어 수 등 서비스 요구 사항을 결정한다. 공급자는 수요를 수용하고, MEC 서버는 광부를 위해 오프로드 된 PoW를 처리한다. MEC 서비스 수요를 해당 광부의 컴퓨팅 용량으로 간주될 수 있다.

모바일 블록체인 네트워크에서 광부는 처음으로 PoW를 성공적으로 해결하기 위해 서로 경쟁한다. PoW를 성공적으로 해결한 광부는 솔루션을 모바일 블록체인 네트워크에 브로드캐스트하여 합의에 도달하고, 합의에 도달한 블록을 성공적으로 채굴한 최초의 광부는 채굴 보상을 얻는다. 보상은 유틸리티 기능으로 표현된 블록체인 응용 프로그램에서 가져온 것이다. MEC x_i 수요를 가진 i 번째 광부의 효용 함수는 다음 두 가지 면에서 구성된다.



[그림 2] MEC(Mobile Edge Computing) 2단계 Stackelberg 게임 모델[6]

i. 블록이 채굴되고 컨센서스에 도달했을 때 얻은 보상은 고정 부분과 가변 부분을 모두 포함할 수 있다.

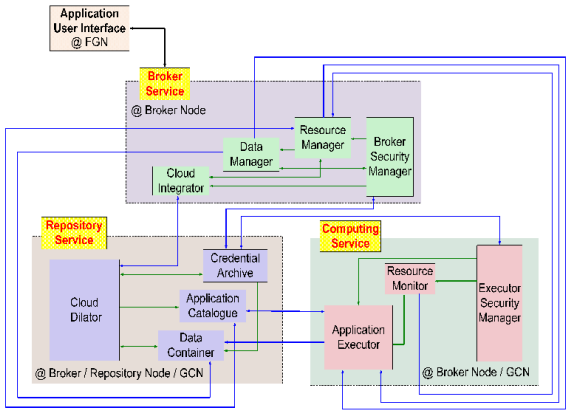
ii. PoW를 해결할 때 발생하는 비용(채굴 사업자가 MEC 서비스를 사용하기 위해 제공자에게 단가 pi를 지불).

5-2 포그 버스(FogBus)[3]

FogBus는 실행 및 상호 작용을 위해 IoT 응용 프로그램 및 컴퓨팅 인스턴스에 대한 플랫폼 독립적인 인터페이스를 제공한다. 개발자가 응용 프로그램을 만들 때 도움이 될 뿐만 아니라, 사용자가 한 번에 여러 응용 프로그램을 실행하고, 서비스 공급자가 자원을 관리하는 데 도움이 된다. 또한, FogBus는 중요한 데이터에 대한 작업을 보안하기 위해 블록체인, 인증 및 암호화 기술을 적용한다. 경량 및 교차 플랫폼 소프트웨어 시스템으로 인해 배포가 쉽고 확장 가능하며, 비용면에서 효율적이다.

FogBus는 IoT-Fog-Cloud 통합을 간소화하기 위해 상호 연관적이고 플랫폼 독립적인 다양한 소프트웨어 구성 요소를 제공한다. 이러한 구성 요소는 크게 세 가지 유형의 시스템 서비스로 분류된다. 브로커 서비스는 브로커 노드의 모든 기능을 관리하고, 필요에 따라 다른 소프트웨어 구성 요소를 시작하지만, 컴퓨팅 서비스는 일반 컴퓨팅 노드의 운영을 제어한다. 브로커 노드 자체가 백엔드 응용 프로그램의 실행을 시작하면 컴퓨팅 서비스가 실행된다. 반대로 저장소 서비스는 모든 포그 노드에서 실행되어 저장소 관련 작업을 관리할 수 있다. 다양한 FogBus 소프트웨어 구성 요소 간의 상호 작용이 [그림 3]에 제시되어 있다. FogBus 소프트웨어 구성 요소의 세부 사항은 다음과 같이 설명된다.

브로커 보안 관리자(Broker Security Manager): 브로커 보안 관리자는 특정 포그 게이트웨이 노드(FogNode)에서 사용자의 인증 자격 증명을 받은 후 리포지토리 서비스의 자격 증명 아카이브와 관련하여 이를 검증한다. 또한 Credential Archive는 원격 클라우드 통합에 필요한 보안 인증서와 함께 이 구성 요소를 지원한다. 브로커 보안 관리자 자체는 공개 키 및 비공개 키 - 값 쌍을 생성하여 포트 노킹, 권한 있는 포트 인증 및 해당 브로커 노드와 다른 포그 노드와의



[그림 3] FogBus 프레임워크 내 다른 소프트웨어 구성 요소의 상호 작용[15]

통신을 보호하기 위한 속성 기반 암호화를 용이하게 한다. 또한 이 구성 요소는 여러 구성 요소와 데이터를 교환하는 동안 무결성을 보장하기 위해 블록체인 인터페이스로 동작한다. 이 경우 Data Manager를 사용하여 수신된 데이터에서 새 블록을 만든다. 각 블록의 해시 값과 작업 증명은 다른 노드간에 분배하기 위해 Credential Archive로 보내지므로 여러 목적지에서 체인의 일관된 검증이 보장될 수 있다. 브로커 보안 관리자는 자격 정보 보관 및 실행자 보안 관리자 컴퓨팅 서비스와 함께 FogBus 내의 추가 보안 문제를 관리하며, 다른 구성 요소는 필요한 정보에 쉽게 액세스할 수 있다.

자원 관리자(Resource Manager): 이 구성 요소는 응용 프로그램을 실행하는 데 적합한 자원을 선택한다. 리포지토리 서비스의 응용 프로그램 카탈로그에서 여러 응용 프로그램의 요구 사항을 식별하고, 컴퓨팅 서비스의 자원 모니터를 통해 각 브로커 및 일반 컴퓨팅 노드의 자원 상태를 감지한다. Cloud Integrator는 가상 시스템 및 컨테이너와 같은 Cloud 기반 인스턴스의 상황 별 데이터로 Resource Manager를 지원한다. 자원 및 응용 프로그램에 관한 모든 정보를 얻은 후 Resource Manager는 FCN 및 클라우드에 필요한 자원을 응용 프로그램에 제공한다. 이 경우 Computing 서비스의 Application Executor와 FCNs 및 Cloud의 내부 소프트웨어 시스템이 자원 관리자를 지원한다. 또한 FogBus는 서비스 제공 업체가 Resource Manager에서 다양한 정책을 적용할 수 있게 해주며, 동시에 애플리케이션에 대한 자원을 제공한다. 또

한 배포된 응용 프로그램과 함께 FCN 및 Cloud 인스턴스의 주소를 추적하는 소스 구성 파일을 유지하므로 스트림의 후속 데이터가 처리를 위해 할당된 자원로 직접 전송될 수 있다. 이 파일은 Cloud와 공유되어 해당 노드의 장애 발생시 배치 정보를 복구한다.

데이터 관리자(Data Manager): 이 구성 요소는 IoT 장치에서 감지 및 사전 처리된 데이터를 수신한다. 또한 여러 소스의 데이터를 집계하고, 컨텍스트에 따라 데이터 수신 빈도를 조정할 수 있다. 그러나 이 데이터를 사용하면 브로커 보안 관리자와 관련하여 무결성을 유지하기 위한 블록과 체인이 만들어집니다. 나중에 데이터를 처리를 위해 Computing 서비스의 Application Executor로 전달하고, 추가 사용을 위해 Repository 서비스의 Data Container에 암호화 된 방식으로 저장한다. 할당된 자원에 응용 프로그램을 배포한 후 Resource Manager는 자원 구성 파일을 Data Manager에 공유하여 스트림의 후속 데이터를 처리 대상에 직접 보낼 수 있다.

클라우드 통합 업체(Cloud Integrator): FogBus 프레임 워크와 Cloud의 모든 상호 작용은 Cloud Integrator에서 처리한다. 클라우드 인스턴스의 컨텍스트를 프레임 워크에 알리고, 스토리지 및 자원 프로비저닝 명령을 클라우드로 전달한다. 이 구성 요소를 통해 FogBus는 사용자 정의된 클라우드 통합 스크립트 개발을 위해 공급 업체와 인터페이스 할 뿐만 아니라, 여러 클라우드 데이터 센터를 동시에 처리할 수 있도록 제3자 소프트웨어 시스템에 대한 액세스를 용이하게 한다.

자격증 명 기록 보관소(Credential Archive): 사용자 인증 자격 증명은 IoT 장치 구성 중에 설정되고 자격 증명 아카이브에 보존된다. 브로커 서비스에서 생성된 각 데이터 블록의 보안키 및 세부 정보를 다른 사람에게 배포한다. 이 구성 요소는 클라우드 통합을 위한 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security) 인증서도 제공한다. 또한 저장된 데이터를 암호화하고 해독하는 데이터 컨테이너를 지원한다. 저장소 서비스의 Cloud Dilator를 통해 클라우드의 이미지를 주기적으로 업데이트하여 해당 노드의 불확실한 오류 발생 후 보안 속성을 다른 노드 간에 쉽게 복구하고 배포할 수 있다.

응용 카탈로그(Application Catalogue): 이 구성 요소는 해당 운영, 실행 및 프로그래밍 모델을 비롯한 다양한 유형의 응용 프로그램에 대한 세부 정보를 유지 관리한다. 또한 응용 프로그램 및 구성원 작업의 자원 요구 사항 및 종속성을 지정한다. 응용 프로그램 카탈로그는 클라우드에서 Cloud Dilator를 통해 이 정보를 확장할 수 있다. Broker 서비스의 Resource Manager는 제공된 스펙을 기반으로 애플리케이션에 대한 자원을 제공한다. Resource Manager의 명령에 따라 컴퓨팅 서비스의 Application Executor와 관련하여 할당된 자원의 응용 프로그램도 동기화한다.

클라우드 확장기(Cloud Dilator): 이 구성 요소는 저장소 서비스의 다른 소프트웨어 구성 요소가 Cloud와 상호 작용하도록 한다. 이 경우 Broker 서비스의 Cloud Integrator는 애플리케이션 사양을 확장하고, 보안 속성을 전송하며, 데이터를 교환하는 데 필요한 명령을 사용하여 Cloud dilator를 지원한다.

Executor Security Manager: 컴퓨팅 연산을 수행하는 동안 안개 계산 노드(Fog Computational Nodes: FCN)와 다른 사람과의 완벽한 보안 상호 작용은 Executor Security Manager에 의해 관리된다. 이 경우, 저장소의 Credential Archive 서비스는 이 구성 요소가 필수 보안 속성으로 도움이 되도록 지원한다. Credential Archive 및 Broker Security Manager와 함께 이 구성 요소는 블록체인을 검증하는 데 중요한 역할을 한다.

자원 모니터(Resource Monitor): 컴퓨팅 자원의 사용 중 및 유휴 상태는 모두 Application Executor와 관련하여 이 구성 요소에 의해 모니터링된다. 이 정보는 자원 관리자가 다른 응용 프로그램에 대한 자원을 제공하는 데 도움이 된다. 또한 응용 프로그램의 런타임 QoS 요구사항과 이를 충족시키는 데 필요한 자원 성능을 추적한다. 할당된 자원이 예상보다 적게 수행되면 애플리케이션을 처리하거나 불확실한 오류가 발생하면 이 구성 요소는 자원 관리자에게 동적 자원 프로비저닝, 애플리케이션 실행 마이그레이션 및 중간 데이터 저장과 같은 필수 동작을 즉시 시작하도록 알린다.

응용 프로그램 실행자(Application Executor): 자원 관리자가 발행한 프로비저닝 지침에 따라 이 구성 요소는 해당 FCN에 있는 여러 응용 프로그램에 대한 자원을 할당한다. 또한 응용 프로그램 카탈로그의 응용 프로그램 실행 파일을 할당된 자원에 대한 배포로 확장한다. 응용 프로그램 배포가 수행되면 처리를 위해 데이터 관리자가 전달한 데이터를

받기 시작한다. 또한 이 구성 요소는 주기적으로 자원 상태를 자원 모니터에 알린다. 예외가 감지되거나 예측되면 이 구성 요소는 자원 관리자가 응용 프로그램 실행에서 중간 데이터를 추출하여 데이터 컨테이너에 저장하여 프레임 워크에 내결함성을 부여하도록 요청한다.

Ⅵ. 결 론

이 기사에서는 모바일 블록체인 응용 프로그램, 특히 IoT 블록체인 마이닝 작업을 사용 사례 및 기술적 문제로 인해 오프로드할 때 엣지 컴퓨팅을 도입했다. 그리고 모바일 블록체인을 위한 효율적인 엣지 자원 관리를 위해 Stackelberg 게임 모델과 FogBus 방법을 제시했다.

Stackelberg 게임 모델과 FogBus는 다양한 인프라에서 서비스 품질을 향상시킬 수 있지만, 인공 지능 기술을 사용하면 더 큰 범위에서 여전히 개선될 수 있다.

참 고 문 헌

[1] P. Mach, Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1628-1656, 2017.

[2] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450-465, Feb. 2018.

[3] N. Herbaut, N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains", *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70-76, Sep. 2017.

[4] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains", *IEEE Trans. Industrial Informatics*, vol. 13, no. 6, pp. 3154-3164, May 2017.

[5] Y. Zhang, L. Liu, Y. Gu, D. Niyato, M. Pan, and Z. Han "Offloading in software defined network at edge with information asymmetry: A contract theoretical approach", *J. Signal Processing Systems*, vol. 83, no. 2, May 2016, pp. 241-253.

[6] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing", *in IEEE Communications Magazine*, vol. 56, no. 8, pp. 33-39, Aug. 2018.

[7] E. M. Schooler, D. Zage, and J. Sedayao, "An architectural vision for a data-centric IoT: Rethinking things, trust and clouds", *Proc. 37th IEEE Int'l. Conf. Distributed Computing Systems, Atlanta, GA*, pp. 1717-1728, Jun. 2017.

[8] R. Pass, E. Shi, "FruitChains: A fair blockchain", *PODC '17 Proc. ACM Symp. Principles of Distributed Computing*, Washington, DC, pp. 315-324, Jul. 2017.

[9] K. Christidis, M. Devetsikiotis, "Blockchains and smart contracts for the internet of things", *IEEE Access*, vol. 4, pp. 2292-2303 May 2016.

[10] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie "Mobile edge computing: A survey", *IEEE Internet of Things J.*, vol. 5, no. 1, pp. 450-465, Feb. 2018.

[11] Y. Wu, J. Zheng, K. Guo, L. Ping Qian, X. Shen, and Y. Cai, "Joint traffic scheduling and resource allocations for traffic offloading with secrecy-provisioning", *IEEE Trans. Vehic. Tech.*, vol. 66, no. 9, pp. 8315-8332, Sep. 2017.

[12] Y. Wu, X. Tan, L. Qian, Danny H. K. Tsang, Wen-Zhan Song, and L. Yu, "Optimal pricing and energy scheduling for hybrid energy trading market in future smart grid", *IEEE Trans. Industrial Informatics*, vol. 11, no. 6, pp. 1585-1596, Apr. 2015.

[13] A. Thurai, "Cloud Computing Moves to the Edge in 2016", https://www.ibm.com/blogs/cloud-computing/2016/01/cloud-computing-move-to-the-edge-in-2016/, accessed 10 Apr. 2018.

[14] M. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani "Blockchain-based mobile edge computing framework for secure therapy applications", *IEEE Access*, vol. 6, pp. 72469-72478, 2018.

[15] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: A blockchain-based lightweight framework for edge and fog computing", *Journal of Systems and Software*, vol. 154, pp. 22-36, 2019.

≡ 필자소개 ≡

Sovit Bhandari

2016년 08월: Kathmandu University (공학사)
2018년 09월～현재: 인천대학교 전자공학과 석사과정
[주 관심분야] 5G 네트워크, 블록체인, 클라우드랜, 무선네트워크, IoT, 블록체인

조 홍 평

2016년 06월: Jilin Jianzhu University (공학사)
2018년 03월～현재: 인천대학교 전자공학과 석사과정
[주 관심분야] 5G 네트워크, 머신러닝, 빅데이터, IoT, 블록체인

김 훈

1998년 2월: 한국과학기술원 전기및전자공학과 (공학사)
1999년 8월: 한국과학기술원 정보통신공학과 (공학석사)
2004년 8월: 한국과학기술원 정보통신공학과 (공학박사)
1998년 3월～2001년 2월: 한국전자통신연구원 위촉연구원
2004년 9월～2005년 10월: 삼성전자 책임연구원
2005년 12월～2007년 8월: 정보통신부 사무관
2007년 9월～2008년 8월: 스탠포드대학교 방문연구원
2014년 9월～2015년 8월: 스탠포드대학교 방문교수
2008년 9월～현재: 인천대학교 전자공학과 교수
[주 관심분야] 통신망, 이동통신, 최적화기법, 빅데이터, 블록체인