The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 2, pp.1-11, Apr. 30, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.2.1
JIIBC 2020-2-1

블록체인 기반 스마트 미터 집계 보안 시스템 구축

Implementation of Secure System for Blockchain-based Smart Meter Aggregation

김용길*, 문경일**

Yong-Gil Kim*, Kyung-Il Moon**

요 약 스마트 그리드 환경의 중요한 기본 구성 요소라 할 수 있는 스마트 미터기는 유틸리티 기관에게 실시간 전력 소비 정보를 제공한다. 그렇지만, 스마트 미터기에 의한 전력 소비 데이터 집계 과정에서 정보 보안 및 사생활 보호를 보장하는 작업은 쉽지 않다. 최근 몇 년 동안 특정 소비자의 전력 소비 정보 추출을 방지하는 정보 보안 데이터 집계 프로세스에 관해 많은 연구가 있었으나 대부분 내부 공격자로부터 안전하지 않거나 데이터 무결성을 제공하지 못하고 있다. 게다가, bilinear pairing 또는 hash-to-point 작업이 스마트 미터기에서 수행되기 때문에 계산 비용이 만족스럽지 않은 상황이다. 현재 에너지 공급 회사, 신생 기업, 기술 개발자, 금융 기관, 국가 정부 및 학계에서 큰 관심을 끌고 있는 기술로 블록체인 또는 분산 원장 기술이 활발히 연구되고 있다. 특히, 전력 소비 네트워크와 관련하여 블록체인은 상당한 이점과 혁신을 가져올 것으로 소개되고 있다. 이에 본 연구에서는 블록체인 기술을 사용한 분산된 전력 소비 정보 보호 및 보안 미터 데이터 집계 시스템을 제안하고, 손쉽게 구현할 수 있는 자바 프로그램을 나타낸다. 여기에서 스마트 미터 데이터는 계층적 Merkle 트리에 의해 집계 및 검증되며, 비잔틴 결함 허용 프로토콜에 의한 합의 방식이 지원된다.

Abstract As an important basic building block of the smart grid environment, smart meter provides real-time electricity consumption information to the utility. However, ensuring information security and privacy in the smart meter data aggregation process is a non-trivial task. Even though the secure data aggregation for the smart meter has been a lot of attention from both academic and industry researchers in recent years, most of these studies are not secure against internal attackers or cannot provide data integrity. Besides, their computation costs are not satisfactory because the bilinear pairing operation or the hash-to-point operation is performed at the smart meter system. Recently, blockchains or distributed ledgers are an emerging technology that has drawn considerable interest from energy supply firms, startups, technology developers, financial institutions, national governments and the academic community. In particular, blockchains are identified as having the potential to bring significant benefits and innovation for the electricity consumption network. This study suggests a distributed, privacy-preserving, and simple secure smart meter data aggregation system, backed up by Blockchain technology. Smart meter data are aggregated and verified by a hierarchical Merkle tree, in which the consensus protocol is supported by the practical Byzantine fault tolerance algorithm

Key Words : Aggregate block structure, Blockchain, Data aggregation, Peer-to-peer energy network, Smart meter

*정회원, 조선이공대학교 컴퓨터보안과
**정회원, 호남대학교 컴퓨터공학과(교신저자)
접수일자 2020년 3월 1일, 수정완료 2020년 4월 1일
게재확정일자 2020년 4월 3일

Received: 1 March, 2020 / Revised: 1 April, 2020 /
Accepted: 3 April, 2020
*Corresponding Author: kimoon@honam.ac.kr
Department of computer engineering, Honam university. korea.

Ⅰ. 서 론

스마트 그리드는 양방향 통신 기술을 사용하여 주기적으로 소비 데이터를 데이터 집중기 게이트웨이에 보낸 다음 유틸리티 회사에 전송하게 되는데, 양방향 통신은 많은 잠재적인 보안 및 개인 정보 위협을 유발한다. 소비 데이터가 동적 가격 책정 및 청구 목적과 함께 에너지 피드백을 위한 건전한 목적보다는 해커에게 잘못된 데이터를 주입하는 기회를 제공함으로써 로드 관리와 동적 가격 시스템의 균형을 맞출 수 없게 된다. 구체적으로 전력망에서 여러 가지 허위의 스마트 그리드나 다른 잘못된 데이터 주입 프로그램을 통해 조작된 미터의 판독 값을 보낼 수 있으며, 이러한 잘못된 판독 값은 수요 반응과 같은 로드 관리 프로그램이 불균형을 유발하도록 한다. 이는 전력망의 원활한 기능을 방해하고 더 높은 에너지 생성 비용을 가져오며 때로는 지역의 에너지 정전을 초래할 수도 있다. 대금 청구 관점에서 잘못된 의도를 가진 고객은 자신의 에너지 소비에 대한 잘못된 보고서를 홈 영역 네트워크에서 유틸리티 회사로 보낼 수 있다. 잘못된 보고는 에너지 시장의 혼란을 일으킬 수 있으므로 스마트 미터의 데이터 보안이 스마트 그리드에서 가장 중요하다. 소비자의 사생활 보호 관점에서 소비 데이터는 개인의 일상 활동의 패턴을 공개하기 때문에 가격, 청구 및 에너지 피드백 목적으로 사용되는 스마트 미터 데이터는 스마트 그리드에서 안전하고 개인 정보 보호 방식으로 전송 및 기록되어야 한다. 스마트 미터 데이터에 관한 보호 방식으로 소비 사용량을 수집하기 위한 보안 데이터 집계 등의 여러 가지 방법이 제안되고 있지만, 대부분의 접근 방식이 데이터 집계에 계산 복잡성을 도입하거나, 악의적인 데이터 집중 장치에 대한 개인 정보 보호를 지원하지는 못하고 있다. 2016년 브루클린에서 최초의 블록체인 기반 마이크로 그리드가 출시된 이래 블록체인 기술은 (분산 및 변조 방지 데이터베이스의 원칙에 따라 작동) 많은 스마트 그리드 시연자에게 상당 부분 견인력을 주고 있다. 특히, 소비 네트워크와 관련하여 블록체인은 분산 전력 생산을 관리하기 위한 잠정적인 기술로 자리매김하고 있다. 블록체인은 중앙 관리 서버가 없어도 시스템의 모든 구성원 간에 공유되는 분산 데이터베이스를 구성한다. 따라서 이론적으로 모든 구성원이 인식하지 않고는 수정할 수 없다. 그것은 암호 화폐뿐만 아니라 추적해야 할 상업 거래, 교환 및 계약 관리에 완벽하게 적합하다[3]. 스마트 그리드 시스템과 관련하여 안전한 P2P 에너지 거래 환경 조성이 무엇보다도 중요한데, 현재 대체 에너지 공급원 사용자가 서로 구매, 판매 및 거래하는 움직임이 점점 더 커지고 있다. 핵심은 이러한 거래가 합법적이고 영구적으로 기록되도록 보안을 유지하는 것인데, 블록체인은 이를 가능하게 한다. 블록체인 기술은 에너지 산업에서 상당한 잠재력을 보여주며, 인증, 인증 및 데이터 교환을 위한 새로운 변조 방지 메커니즘을 제공한다. 그렇지만, 현재 에너지 업계에서 인정되는 블록체인 정의는 없으며 다양한 연구에서 좁고 넓은 의미에서 블록체인을 정의하고 있다.

본 연구에서는 블록체인의 Merkle 해시 트리 기술을 사용하여 스마트 미터 집계 시스템을 보호하는 인증체계와 자바 구현을 나타낸다. 제안되는 블록체인 기반 스마트 미터 집계 시스템은 소비량 집계 관련 보안 및 개인 정보 보호를 크게 높일 수 있다. Merkle 해시 트리 구조는 분산 합의 알고리즘을 통해 효율적인 자료수집 및 저장을 원활하게 하는 분산 데이터 저장 시스템의 역할을 한다. 제안된 블록체인 네트워크는 모든 시스템 노드에서 공유 원장의 사본을 저장하고 동기화함으로써 단일 지점 실패 및 신뢰성 문제를 효과적으로 방지한다. 특히, 블록체인이 분산성을 갖기 때문에 네트워크 전반에 걸친 블록체인 갱신과 관련하여, 블록을 채굴한 노드가 추가 사항을 전역적인 블록체인에 중계하여, 다른 블록 노드가 볼 수 있도록 HTTP 서버로 보내는 방식으로 새 블록체인을 중계한다.

Ⅱ. 기술적 배경

스마트 미터 집계 보안 및 개인 정보 보호를 위한 접근 방식은 현재 크게 두 가지로 구분할 수 있는데, 하나는 전통 암호화 체계에 의한 것과 블록체인의 Merkle 해시 트리 접근으로 나눌 수 있다.

1. 스마트 미터 정보 보호 집계

내 결함 성 개인 정보 보호 데이터 집계 체계는 Chen 등을 참조할 수 있는데[4], 이 방식에서 스마트 미터는 Paillier 암호화 방식으로 암호화 측정 데이터를 데이터 집중기 게이트웨이로 보낸다. 여기에서 암호화된 데이터를 집계한 후 정보는 여러 작업 서버로 구성된 제어 센터로 전송된다. 각 서버는 Paillier 암호 해독 알고리즘을 사용하여 집계된 데이터를 암호 해독할 수 있다. 제안 방식은 악의적인 데이터 집중기 게이트웨이 또는 제어 센터로부터 고객의 개인 정보 보호가 가능하다. Wang이

제안한 신원 기반 데이터 집계 프로토콜로 주요 개념은 서명과 함께 식별자 기반 암호화 체계를 사용하는 것이다[5]. 체계 실행과 관련하여 스마트 미터는 계량 데이터에서 암호문을 계산하고 소비 데이터에서 서명을 계산한다. 마지막으로 보고서를 집계기로 보낸다. 스마트 미터기로부터 자료를 수집할 때 집계기는 배치 검증을 수행하여 미터기로부터 수신된 모든 서명을 확인한다. 집계 프로토콜은 Man-in-the-Middle, 집계기 및 유틸리티 기업에 대한 내외부 공격에 대해 안전한 것은 사실이지만, 배치 프로세싱의 계산 비용이 집계기에서 만족스럽지 못한 단점을 가지고 있으며, 많은 미터기 배치와 관련해서 프로토콜이 효율적이지 못하다. Badra와 Zeadally는 스마트 미터 데이터를 개인 정보 보호 방식으로 집계하기 위해 대칭 동형 암호화 및 Elliptic Curve Diffie Hellman 키 교환 방법을 사용하는 효율적이고 가벼운 개인 정보 보호 집계 방법을 제안했다[6]. 이 방법의 가장 큰 단점은 내부 공격을 방어할 수 없다는 점이다. 유사하게, Asmaa와 Xuemin은 소비자 네트워크를 위한 간단한 보안 및 개인 정보 보호 체계를 제안했다. 시스템 체계는 격자 기반 암호화의 개념을 활용하는 것으로 거의 직교성을 갖는 짧은 벡터를 찾는 것이지만, 시간 복잡도가 만족스럽지 않다[7]. Debiao 등은 내부 공격에 대한 간단한 데이터 집계를 제안했는데, 이 방식은 타원 곡선 암호화를 활용하여 효율성을 달성했지만, 청구를 지원하지 못하는 단점을 가지고 있다[8]. Vahedi 등은 소비 사용량 데이터에 대한 개인 정보 보호를 제공하는 ECC 기반 데이터 집계 체계를 제안했다[9]. 이 체계에서 스마트 미터기는 가정 내 에너지 소비 사용량 데이터를 측정하고 이를 암호화 후에 암호화 텍스트인 에너지 소비 데이터에 서명하고 집계기로 전송한다. 메시지를 수신하면 집계기는 메시지의 무결성을 확인하고 수집한다. 그런 다음에 집계기는 집계 메시지에 서명하고 안전한 방식으로 주 운영 센터에 메시지를 전달한다. 소비자 사용 데이터는 주 운영 센터에서 검증되는 방식이다. 위에 언급된 최근 기술 체계의 대부분은 데이터 집계에서 보안 및 개인 정보 보호를 제공하지만, 데이터 집중기 게이트웨이가 집계된 소비 데이터를 도출할 수 있으므로 청구 시스템의 개인 정보 문제를 해결하지는 못한다. 보안 데이터 집계를 포함한 프라이버시 보호 청구 처리를 위해 최근 몇 가지 체계가 제안되었는데, Shaohua 등은 스마트 그리드 네트워크에서 프라이버시 보호 다중 부분 집합 데이터 집계 체계를 제안했다[10]. 이 체계에서 스마트 미터기는 주거 지역의 일정 시점 동안 전력 소비에 따라 다중 하위 집합으로 구분된다. 제어 센터는 집계기를 통해 안전한 개인 정보 보호 방식으로 각 부분 집합에 대한 전력 사용량 데이터의 합계를 얻을 수 있다. 개인 정보 보호를 위해 동형 암호 시스템을 사용하여 전력 소비 데이터를 집계한다. 이 체계의 단점은 자원이 제한된 스마트 계량기에 대해 계산 비용이 만족스럽지 못하고, 스마트 미터기가 손상되는 문제가 있다.

Fábio 등은 네트워크 내에서 계량 데이터를 집계하기 위한 개인 정보 보호 강화 체계를 제안했다[11]. 스마트 미터 데이터 집계를 위해 동형 암호화 체계로 동형 계약을 활용했지만, 주요 단점은 개념 증명 및 시뮬레이션 결과가 없어 실현 가능성과 보안에 대해 논의하기가 어렵다. Jianbing 등은 오작동하는 데이터 수집기에 대해 안전한 데이터 집계 및 청구 체계를 제안했다[12]. 새로운 공격 모델로 정직한 공격자와 악의적인 공격자를 구축했는데, 이 체계는 데이터 집중기 게이트웨이의 오작동을 결정할 수 있다. 악의적인 자료 수집기에 대한 보안을 위해 프록시 재 암호화 체계와 동형 인증을 사용했지만, 이러한 메커니즘은 계산 집약적인 쌍 선형 페어링 작업을 사용하므로 통신 및 계산 비용이 만족스럽지 않고, 자료수집 과정에서 공격에 취약한 문제점이 있다. Kazuma 등은 스마트 그리드 네트워크에서 개인 정보 보호 청구 및 에너지 관리 체계를 제안했는데, 보안 및 개인 정보 보호 목표를 달성하기 위해 동형 암호화, 표준 디지털 서명과 같이 계산 비용이 많이 드는 메커니즘을 사용했지만, 집중기 게이트웨이에 관한 보호가 없다[13]. Gope와 Sikdar는 스마트 그리드 보안 관련 친화적 동적 가격 결정 및 수요 응답 관리를 위한 효율적인 데이터 집계 체계를 제안했다[14]. 대칭 키 암호화 및 해싱 작업을 활용하고 자원이 제한된 스마트 미터에서 낮은 계산 비용이 장점이다. 이 체계에서, 스마트 미터의 익명 작업은 스마트 미터에 여러 개의 임시 식별자를 발행함으로써 달성된다. 제안된 방식은 현실적인 상황에서 문제가 될 수 있는데, 임시 식별자 재발급에 반드시 사용자 참여가 요구되며, 더 나아가서, 악의적인 집계기에서는 작동하지 않을 수 있다. 지금까지 소개된 스마트 미터 보안 시스템 개발과 관련해서 대부분 자원이 제한된 스마트 미터기에 대해 계산 비용이 만족스럽지 않거나 악의적인 공격에 취약할 수 있다. 앞으로 10년 이내에 어느 정도 규모의 양자 컴퓨터가 구체화 될 것으로 추측되는데, 이러한 양자 컴퓨터의 등장은 인터넷의 가장 보편적인 암호 체계 보안이 양자 알고리즘에 의해 안전하지 않을 가능성이 크다는 점이다. 단적으로 양자 컴퓨터는 불연속 로그 연산을 빠르게 처

리할 수 있다는 점에서 일반 디지털 서명 체계를 무력화 시킬 수 있다. 이러한 맥락에서 Merkle 트리로 불리는 블록체인 암호화 시스템은 양자 컴퓨팅 공격으로부터 안전한 디지털 서명 체계를 유지할 수 있는 바탕이 될 수 있다.

2. 블록체인 기반 스마트 미터 시스템

블록체인의 Merkle 트리에 의한 디지털 보안이 양자 컴퓨팅에 의한 공격에 대해 안전할 것으로 여겨지는 이유는 Merkle 트리 보안이 가변적인 간단한 가정을 바탕으로 하고 있다는 점이다. 특히, Merkle 트리 가정은 무작위 접근에 대한 강한 저항성을 가지는데, 구체적으로 SHA 변형이라 할 수 있는 해시 함수로 구성된다. 현재 양자 컴퓨팅과 관련하여 효율적인 해시 함수의 충돌 방식은 소개되고 있지 않다. 단적으로 Merkle 트리 가정은 양자 컴퓨터 이후 상황에서의 보안 접근 방식이 될 수 있다. 분산 컴퓨팅 패러다임에 속하는 블록체인은 암호화, 합의 프로토콜 및 스마트 계약을 통해 신뢰할 수 있는 공유 원장을 설정한다[15]. 블록체인 네트워크에서 소비자는 분산 노드 역할을 하며, 신뢰할 수 있는 당사자에 의존하지 않고 거래 또는 디지털 이벤트의 공유 레코드를 공동으로 보호하고 유지한다. 모든 노드는 블록체인 네트워크에서 생성된 데이터 거래를 공유, 패킹, 검증 및 저장해야 한다. 블록체인은 단일 기술이 아니라 여러 기술 구성 요소의 통합이다. 기본 요소에는 비대칭 암호화, 해시 함수, 타임 스탬프, Merkle 해시 트리, 합의 메커니즘 및 스마트 계약이 포함된다. 분산 블록체인 시스템에서 비대칭 암호화는 올바른 수신자가 올바른 메시지를 읽을 수 있도록 하고 데이터 전송 프로세스 중에 데이터가 변경되는 것을 방지한다. 해시 함수는 일반 텍스트를 메시지 다이제스트로 인코딩하는 단방향 알고리즘이다. 메시지 다이제스트는 일반 텍스트의 지문으로, 특정 길이의 숫자와 문자로 구성된다. 각 블록의 타임 스탬프 및 해싱 값은 블록체인 네트워크에서 블록 추적을 가능하게 한다. Merkle 해시 트리는 블록의 모든 트랜잭션을 하나의 메시지 다이제스트로 인코딩하여 블록 유효성 검사를 효율적으로 수행한다. 특정 응용 프로그램의 경우에 관련된 비즈니스 규칙에 따라 블록체인 시스템의 실행을 지원하도록 서로 다른 사용자 정의, 합의 메커니즘 및 블록 구조를 설계할 수 있다. Merkle 서명 체계는 RSA, DSA, ECDSA와 같이 잘 확립된 서명 체계에 대한 흥미로운 대안이라 할 수 있는데, 서명 체계의 보안은 암호로 안전한 해시 함수들이 존재하는 경우로만 국한되지만, 양자 컴퓨터에 의한 공격에 강한 저항력을 갖는다[1]. 그렇지만, 비밀키의 크기, 키 쌍의 생성 시간과 서명 생성 시간이 만족스럽지 않다. Merkle 트리는 완전 이진 트리로 각 마디가 그것이 갖는 자식 마디 해시들의 연결 해시에 해당하는 값을 갖는다. 트리의 잎은 특정 확인 키의 해시를 갖는데, 그 값은 별도의 일회용 서명 방식으로 사용된다. 서명 방식의 공개키는 트리의 루트에 있는 해시값이다. 메시지에 서명할 때까지 트리의 나머지 부분은 비밀로 유지된다. 메시지에 서명할 때 트리 잎에 해당하는 서명 키를 선택하고, 해당 키를 사용하여 일회성 서명 방식으로 서명을 한 후에 검증자에게 제출한다. 제출 방식은 검증자가 이러한 마디들을 사용하여 선택된 잎에서 루트에 이르는 경로상에서 해시들을 계산할 수 있도록 마디들로부터 해시값 집합을 트리의 각 레벨에서 하나씩 제공한다. 검증자는 먼저 1회 서명 방식에 따른 메시지 검증을 하고, 트리 루트에 이르는 경로를 따진 후에 계산된 해시값이 공용 키의 해시값에 부합되는지 검토한다. 잎마다 하나의 메시지 서명이 주어지기 때문에, 서명하려는 메시지들이 어느 정도인지에 따라 매개 변수화 방식이 진행된다. 잎 개수의 함수로 트리에 적지 않은 노드들이 존재하기 때문에, 물론 여기에 절충 방식이 사용될 수 있다. 모든 해시를 저장은 비효율적이므로, 필요한 해시 마디를 찾아 트리를 효율적으로 탐색하기 위한 방식들이 사용되고 있다.

합의 프로토콜은 신뢰할 수 있는 블록을 생성하는 데 중요한 역할을 하는데, 최첨단 합의 프로토콜에는 작업 증명, 스테이크 증명 및 실용적인 비잔틴 내 결함 성이 포함된다[16]. 작업 증명과 스테이크 증명은 대부분 비트코인 및 이더리움과 같은 통화 기반 블록체인 시스템에 적용된다[17]. 이 두 알고리즘은 마이닝에 따른 보상 및 경쟁 방식으로 인해 많은 계산 성능을 소비하기 때문에, 미터 데이터 집계 애플리케이션에는 바람직하지 않고, 복잡성과 효율성이 낮은 비잔틴 내 결함 성 합의 방식이 적절하다. 비잔틴 합의 방식은 분산된 투표 메커니즘이라 할 수 있는데, F개의 동시 장애 노드를 갖는 N개 노드의 네트워크에서 합의는 $N \geq 3F+1$을 만족해야 한다는 것이다.

Ⅲ. 스마트 미터 집계 시스템 구성

1. 스마트 미터 시스템 모델

스마트 미터 관련 전반적인 시스템 운영 및 관련 개체 구성은 그림 1과 같다. 먼저 시스템의 운영 관련 개체로

서 운영 센터는 전력 소비에 대한 실시간 유지 보수, 전력 품질 분석 및 동적 가격 결정을 담당한다. 스마트 미터 모델에서 운영 센터는 시스템 매개 변수를 생성하고 공개하는 신뢰할 수 있는 개체로서 모든 참여 개체를 등록한다[2]. 스마트 미터 보안 관점에서 운영 센터는 개별 사용자의 전력 소비를 도출해서는 안 된다. 대신에 운영 센터는 수신된 집계 소비 데이터의 무결성을 확인하고 동적 가격이 올바른 방식으로 적용되도록 한다. 데이터 집중기 게이트웨이 개체는 특정 스마트 미터 개체가 보낸 정보의 수집 및 집계를 담당한. 디지털 보안 관점에서 이 개체는 특정 기간 또는 전체 기간의 실제 사용자 소비 사용량 데이터를 도출할 수 없으며, 전송 메시지의 무결성을 검증할 수 있다. 추후 수신된 동적 가격에 기초하여 암호화 데이터를 계산하여 운영 센터와 소비자만이 실제 가격을 도출 할 수 있다. 집중기는 자원이 풍부한 장치로서 스마트 미터와 비밀 및 공유 키를 저장하기에 충분한 변조 방지 저장 장치를 갖추고 있어야 한다.

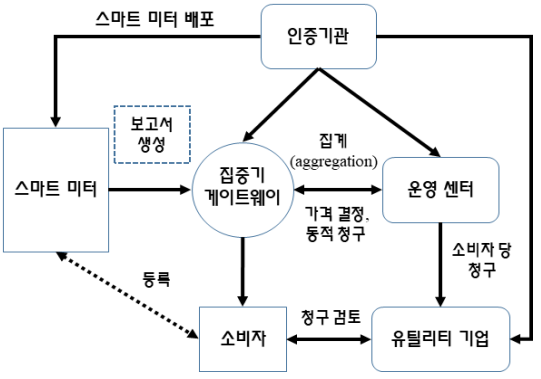

그림 1. 미터 시스템 운영 및 관련 개체
Fig. 1. Meter system operation and related objects

스마트 미터 개체는 실시간으로 측정되는 전력 소비 관련 고정 기간의 암호화 정보를 집중기에 전송한다. 이 개체는 보편적으로 제한된 자원을 가진다. 스마트 미터와 집중기 간에 통신은 로라 네트워크와 같은 저전력 또는 전력선 통신을 통해 구축할 수 있다. 유틸리티 개체는 운영 센터가 받은 데이터를 바탕으로 청구서를 생성한다. 인증 기관 개체는 적법한 스마트 미터 배포 관리와 공개 키를 계산할 수 있는 인증서 생성을 담당한다. 각 스마트 미터기에는 두 개의 사전 저장된 키가 설치되어 있는데, 하나는 집중기와 공유하고 다른 하나는 운영 센터와 공유한다. 소비자는 USB 등을 통해 자체 보안 관련된 것들을 스마트 미터 상에 통합한다. 운영 센터의 게시된 동적 가격 및 집중기에 저장된 데이터를 바탕으로 유틸리티 개체에서 생성한 자체 청구서의 유효성을 확인할 수 있다.

시스템 운영은 시스템 초기화, 스마트 미터 배포, 소비자 등록, 집계 보고서 생성, 가격 결정, 동적 청구, 고객 확인 단계 순서로 진행된다. 운영 센터는 시스템 매개 변수 설정과 필요한 키를 처리하며, 배포 단계에서 스마트 미터 개체는 핵심 데이터를 받는다. 고객 등록 단계에서 고객은 자체 비밀키를 설치하여 스마트 미터에 연결된다. 암호화된 스마트 미터 측정의 전송은 보고서 생성 단계에서 수행되는데, 데이터 집중기 게이트웨이는 여러 시점에 걸친 보고서 생성을 통해 보고서 생성 단계에서 수행되는 집계 보고서를 작성할 수 있다. 집중기 게이트웨이로부터 집계 보고서를 받은 후 운영 센터는 먼저 각 스마트 미터에 대해 집계된 소비 데이터를 도출하기 위해 보고서를 해독해야 하는데, 이러한 작업은 서로 다른 시점의 변동 가격을 참조하기 때문에 가격 결정 단계에서 진행된다. 유동성 가격을 집중기 게이트웨이로 보내면, 집중기는 새로운 통합 보고서를 작성하며, 이 보고서는 운영 센터에서 최종 가격을 도출하기 위해 사용된다. 이러한 활동은 동적 청구 단계에서 실행된다. 마지막으로, 집중기로부터 다른 가격이 수령되면 고객은 고객 검증 단계에서 운영 센터의 청구를 확인할 수 있다.

2. 스마트 미터 데이터 집계 아키텍처

블록체인 기반 스마트 미터 집계 아키텍처는 그림 2와 같이 나타낼 수 있다. 인증 기관은 초기 시스템 작동과 관련하여 예비 명령을 통해 프로그램을 로딩할 수 있도록 한다. 시스템 초기화 관련하여 키 생성, 데이터의 수집, 신원 인증, 마이닝 노드 선정, 새로운 블록 설정, 블록 검증, 청구 단계를 진행한다. 키 생성과 관련해서는 두 개의 큰 소수 p, q를 선택하여 $n = p*q$를 계산한 후에, $1 < e < E_n$인 정수 e를 선택한다. 여기서 E_n은 오일러 함수로 e와 E_n의 최대 공약수는 1이다. 다음으로, $d*e$를 n으로 나눈 나머지가 1인 정수 d를 찾는다. 여기서, e는 개인 키이고, d는 공개 키에 해당한다. 각 소비자는 등록을 위해 자신의 ID를 인증 기관에 보내 공개 및 비밀키를 얻는다. 각 소비자는 여러 쌍의 공개 및 개인 키를 획득할 수 있으며, 공개키는 익명을 사용한다. 전력 소비자는 소비 유형에 따라 여러 그룹으로 나눌 수 있는데, 각 그룹에 대한 큐를 사용할 수 있다. 먼저, w개의 비트를 갖는 배열을 설정한 후에, k개의 해시 함수들을 사용하여 같은 그룹에 있는 모든 익명에 대해 해시 처리를 한다. 해시 처리된 값을 w로 나눈 나머지가 인덱스의 값과 같

다면 1로 처리한다. 이는 소비자 익명의 타당성 검토를 위한 것으로 대응 값이 0이 아니면 익명은 합법적이다.

데이터의 수집과 관련하여 같은 그룹의 다른 사용자로부터 신원을 숨기려면 익명을 사용하여 사용자의 실제 신원을 대체하고 각 사용자는 전력 소비 데이터를 여러 익명으로 묶어서 더욱 난해하게 만들 수 있다. 각 소비자의 전력 소비 데이터를 각 시간대로 무작위 분할하고 소비량, 소인, 익명 등으로 구성된 순서쌍을 공개한다. 사용자 익명의 타당성 검토와 관련하여 소비자가 다른 소비자가 보낸 순서 쌍으로 구성된 전력 소비 데이터를 수신하면 발신자의 익명을 사용하여 서명을 확인한다. 신원 인증 후 모든 사용자는 마이닝 노드를 결정하여 전력 소비 데이터를 집계하고 이러한 데이터를 블록체인에 기록한다. 먼저, 각 사용자는 수신된 모든 데이터를 기반으로 평균 전력 소비 데이터를 계산하고, 다음으로 데이터가 평균에 가장 가까운 것이 채굴 노드로 선택된다. 전력 소비 데이터가 평균에 근접한 여러 익명이 있을 수 있는데, 이는 모두 특정 시간대의 채굴 노드가 됨을 의미한다. 이러한 특정 경우는 채굴 노드에서 생성되는 새 블록 생성에 영향을 미치지 않는다. 모든 사용자로부터 자료를 수집하기 전에는 평균을 알 수 없으므로, 악의적인 사용자가 채굴 노드로 선택될 확률은 낮다.

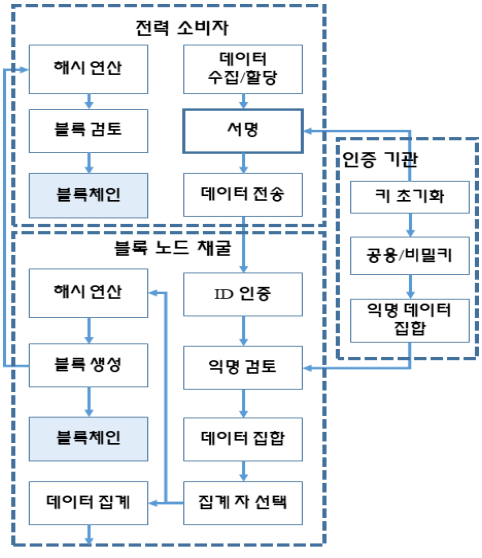

그림 2. 블록체인 기반 스마트 미터 집계
Fig. 2. Blockchain-based Smart Meter Aggregation

새로운 블록 생성과 관련하여 블록의 구조는 그림 3과 같이 나타낼 수 있다. 여기서 m은 전력 소비 데이터이고, Pk는 같은 그룹 내에 익명들을 나타낸다. 채굴 노드를 선택하면 전력 소비 데이터가 블록체인에 기록되고 메시지 인증을 위해 모든 소비자에게 게시된다. 전력 소비 데이터는 Merkle 트리의 채굴 노드에 의해 해싱 처리된다. 이어서 채굴 노드는 루트 해시, 소인, 이전 블록의 해시, 익명 및 평균을 블록 헤더에 기록되고, 새 블록은 메시지 인증을 위해 다른 소비자에게 게시된다. 블록 검증과 관련하여, 새로운 블록을 수신한 후에 각 소비자는 기록의 타당성을 검토한다. 새 블록의 순서쌍이 올바른 경우에 소비자는 이 블록을 자신의 데이터 집합에 저장된 블록체인에 연결한다. 새 블록의 레코드에 대해 아무도 없으면 채굴 노드는 전력 소비 데이터의 집계를 운영 센터로 보낸다. 각 사용자는 자신의 데이터와 관련된 레코드만 확인하면 되며 오프라인으로 확인할 수 있으므로 분산 방식으로 블록체인을 갖는 거의 실시간 데이터를 집계할 수 있다. 각 그룹으로부터 전력 소비 데이터의 집계를 수신한 후에 운영 센터는 전력 소비 프로파일을 작성하고 동적 가격 책정을 제공하여 사용자가 전력 소비 패턴을 조정하도록 할 수 있다. 각 결제 주기에서 각 그룹의 개인 블록체인은 유틸리티 회사로 전송된다. 블록체인이 데이터 무결성을 보장할 수 있으므로 정확한 청구가 가능하다.

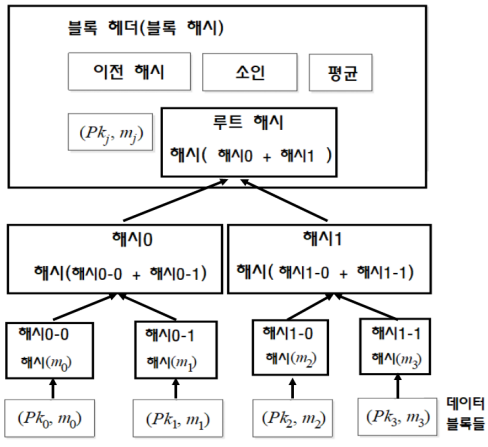

그림 3. 집계 블록 구조
Fig. 3. Aggregate block structure

블록체인 보안 해싱과 관련하여 MD5, SHA256, SHA512, PBKDF2, BCrypt, SCrypt 등이 사용된다. MD5는 가장 널리 사용되는 해싱 알고리즘으로 안전하지 않지만, 빠르고 구현하기 쉽다. SHA 시리즈는 암호화 해시 함수 집합에 속하는데, MD5보다 강력한 해시를 생

성한다는 점을 제외하면 MD5와 매우 유사하다. 그렇지만, 이러한 해시는 항상 유일하지는 않으며 두 개의 다른 입력에 대해 충돌이 발생할 수 있지만, 이러한 충돌은 매우 드물다. 보안 해시를 작성하고 임의로 생성된 텍스트(salt)를 통해 안전한 보안 대책을 세울 수 있지만, 현재 하드웨어가 너무 빨라 사전과 레인보우 테이블을 사용하는 무차별 대입 공격이 발생하여 암호가 몇 시간 안에 붕괴될 수 있다. 이러한 문제에 관한 대책으로 무차별 대입 공격을 느리게 하여 피해를 최소화하는 PBKDF2, Bcrypt 또는 Scrypt와 같은 일부 CPU 집약적 알고리즘이 사용된다. 이들 알고리즘은 보안 요소 또는 반복 횟수를 매개변수로 사용하는데, 이 값은 해시 함수의 속도를 결정한다.

Ⅳ. 자바 구현

블록체인은 정보를 포함하는 긴 블록들의 연결 리스트로 블록체인의 주요 특징은 보안, 블록 마이닝, 합의 및 분산에 있다. 블록은 단순히 사람들 간에 거래로 그것의 구조는 체인 내에 ID를 나타내는 인덱스, 블록 생성 시점, 데이터 필드, 이전 블록의 해시 포인터 및 현재 블록의 해시로 구성된다. 먼저, 블록 클래스는 다음과 같이 작성할 수 있다.

```
public class Block{
 /* 블록 속성 */
 private int index;
 private long timestamp;
 private Data data;
 private String prevHash;
 private String selfHash;
 // 생성자: 변수로 전달되는 블록 구축에 이어
 // 현재 블록에 대한 해시 생성 */
 public Block(int index, long timestamp, Data data,
    String prevHash){
    /* 로컬 속성 설정 */
    this.index = index;
    this.timestamp = timestamp;
    this.data = data;
    this.prevHash = prevHash;
    /* 현재 블록에 대한 해시 생성 */
    this.selfHash = hashBlock();
 }
 ...
}
```

생성자 하단에 현재 해시를 만들기 위한 hashBlock()이 사용되는데, 이것은 블록체인의 보안 프로토콜의 일부이다. 각 블록은 블록체인이라는 연결 리스트의 노드에 해당한다. 블록의 data 필드는 작업 증명 및 거래를 포함하기 때문에 블록의 핵심 부분에 해당한다. 작업 증명에 관한 사항은 블록 마이닝에서 나타내기로 한다. 데이터 클래스는 다음과 같이 작성될 수 있다.

```
public class Data {
    private List<Transaction> transactions;
    private int id;
    ...
}
```

각 블록은 블록체인으로 불리는 연결 리스트의 노드를 나타내기 때문에 다음과 같은 클래스 Blockchain로 작성할 수 있다. 클래스는 단순히 Block 객체들의 배열 리스트를 포함한다. 생성자에서는 블록체인의 초기화 관련 Block에 관한 매개 변수들이 사용된다. 초기화에서 첫 번째 블록이 생성된다. 이러한 초기 블록은 데이터를 보유하지 않고 블록체인의 시작을 위한 헤더 노드의 역할을 한다. 이상이 자바 클래스로 나타낸 블록체인의 기본 구현으로 블록체인의 우수함은 여기에서 체인을 처리하는 보안 알고리즘과 그것의 구현에 달려있다.

```
public class Blockchain {
 private List<Block> blockchain;
 /** 생성자: 블록체인 시작을 위해 생성된
 블록 데이터를 취함 */
 public Blockchain(int index, long timestamp,
    Data data, String prevHash){
    // 블록체인 초기화 및 생성 블록 추가
    blockchain = new ArrayList<Block>();
    blockchain.add(new Block(index, timestamp,
      data, prevHash));
    ...
    }
    ...
}
```

블록체인의 가장 큰 특징은 해커로부터 보호되고 안전하다는 것이다. 해커가 블록체인의 정보를 변경하려면 블록체인 일부를 검증하기 위해 51%의 마이닝 능력이 요구되는데, 사실상 거의 불가능하다. 즉, 해커의 처리 능력이 블록체인 마이닝 풀에서 전체 처리 능력의 51%를 차지해야 가능하다. 더 나아가서, 블록체인은 암호화를 사용하여 정보를 보호하고 체인을 주기적으로 검증하기 때문에 해킹은 더욱 불가능하다. Block 클래스의 hashBlock()

은 해시 포인터를 사용하여 블록을 연결하며, 또한 블록 정보를 해시 함수에 정리하여 각 블록에 고유한 해시를 만든다. SHA-256 해싱을 사용하는 경우에 hashBlock()은 다음과 같이 작성할 수 있다.

```
// 블록 정보를 해시 함수로 채우는 방식으로
// 각 블록에 대한 유일한 해시 생성
// 정보는 인덱스, 소인, 거래, 이전 해시, 집계
private String hashBlock(){
  /* 해시 처리될 문자열 구축 */
  String hash = Integer.toString(this.index) +
    Long.toString(this.timestamp)
    + hashTransactions() + this.prevHash;
  /* 해시 함수에 보내기 */
  hash = hashFcn(hash);
  return hash;
}
/** SHA-256 해시 함수는 문자열을 받아
    256-비트 해시로 출력함 */
private String hashFcn(String toHash){
  String hashed =
    Hashing.sha256().hashString(toHash,
    Charsets.UTF_8).toString();
  return hashed;
}
```

hashBlock()에 의한 출력은 비가역적인 256-바이트 해시로 블록에 대한 신뢰성이 보장된다. 문제는 전체 블록체인에 대한 보안인데, 앞서 논의한 바와 같이 공격자가 블록의 단일 비트 정보만 변경하려고 하면 전체 해시가 완전히 새로운 256-바이트 값으로 변경되기 때문에 문제가 되지 않는다. 전체 블록체인 검증 코드는 다음과 같이 작성할 수 있다.

```
public boolean checkChain(){
  // 체인을 통한 순회 및 해시 포인터 검토
  // false 출력은 블록이 변경되었음을 의미함.
  for(int i=0; i<blockchain.size()-1; i++){
  // 현재 해시와 다음 블록의 이전 해시 비교
    String currHash =
      blockchain.get(i).getselfHash();
    String nextHash =
      blockchain.get(i+1).getprevHash();
    if(!(currHash.equals(nextHash))) return false;
  }
  return true;
}
```

공격자가 블록의 정보를 변경하면 다음 블록의 prevHash 및 현재 블록의 selfHash의 정보가 일치하지 않아 체인이 무효 처리된다. 따라서, 블록체인에 대한 공격자의 단일 체인은 전체 체인이 유효하지 않은 것으로 등록하고 노드는 타당한 블록체인을 취하기 위해 다른 마디로 이동하게 된다. 위와 같이, 블록체인 보안은 거의 도달 불가능한 51% 마이닝 능력과 암호화 매칭으로 구성된다. 대부분 공격자는 전체 블록체인 풀 처리를 위한 능력 또는 인프라가 없을 확률이 높아서, 블록 조작 중심으로 공격이 이루어질 것으로 예상된다. 그렇지만, 해싱 처리는 블록에 대한 어떠한 변경에 대해 체인을 무효화시키고 검증된 새 체인을 찾기 위한 마디를 채굴하게 된다. 그림 4는 거래, 블록 생성 및 채굴 과정과 결과 화면으로 블록체인의 핵심적인 사항이다. 전력 소비자 A와 B가 그룹 내에 집계 책임자 D에게 소비량을 전송한 경우의 출력이다. 이러한 거래는 모든 노드가 블록을 검색하고 채굴할 수 있도록 서버로 중계된다.

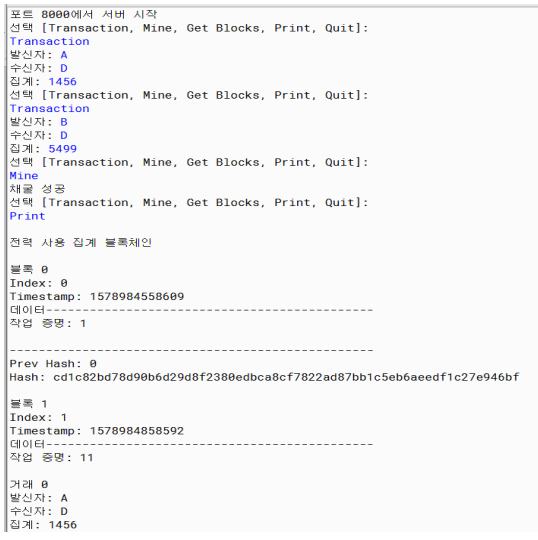

그림 4. 거래, 블록 생성 및 채굴 결과
Fig. 4. Transaction, block generation and mining results

블록은 채굴 이후에 체인에 추가된다. 즉, 블록이 검증되고 작업 증명 알고리즘이 구현된 이후에 추가된다. 본 구현에서는 익명 검토 대신에 가장 최근 거래를 하는 노드 선택 관련 startMine()을 통해 작업 증명을 거친 후에 블록을 체인에 추가하도록 한다. 작업 증명은 단순히 블록 마이닝 과정 중에 일부 연산이 진행되었음을 증명하는 방식으로 진행한다. 여기에서는 단순히 특정 소수와 마지막 블록으로 나눌 수 있는 숫자를 찾는 연산을 적용하기로 한다. 채굴 시작 방식은 초기 블록과 임의의 집계

로 시작한 후에 작업 증명 알고리즘을 통해 진행한다. 이러한 작업이 일단 종료되면, 새로운 거래가 마이너에 대한 보상으로 가짜 화폐를 한 단위를 주는 방식으로 생성되도록 한다. 이는 실제 블록체인이 거대 채굴 데이터를 유지할 수 있도록 하기 위한 것이다.

```
/* 거래 마이닝 및 체인에 추가할 블록 생성 */
public boolean startMine(Transaction
  transactionHistory){
  // 블록 타당성 검토
  if(transactionHistory.getAmount().equals("0") ||

transactionHistory.getAmount().equals("none")) {
    System.out.println("Mine Unsuccesful");
    return false;
  }
  // 작업 증명
  int proof = checkWork();
  // 원래 거래 및 블록 채굴에 대한 응답
  Transaction newTrans = new
    Transaction("NETWORK", "MINER", "1");
  List<Transaction> transactions = new
    ArrayList<Transaction>();
  transactions.add(transactionHistory);
  transactions.add(newTrans);
  // 새 블록을 위한 데이터 생성
  Data newDataBlock = new Data(proof,
    transactions);
  // 새 블록 생성
  Block prospectiveBlock =
    makeProspectiveBlock(blockchain.get(
    blockchain.size()-1), newDataBlock);
  /*블록체인에 추가*/
  blockchain.add(prospectiveBlock);
  return true;
}

/** 단순 작업 증명 (블록 마이닝에 있어서 cpu 사용이 있었음을 나타냄) */
public int checkWork(){
    int lastProof =
    blockchain.get(blockchain.size()-1).getData()
    .getProofId();
    int incrementor = lastProof + 1;
    int divisor = 11;
    while (!(incrementor % lastProof == 0 &&
      incrementor % divisor == 0)){
      incrementor++;
    }
    return incrementor;
}
```

블록체인이 분산성을 갖기 때문에 네트워크의 각 노드가 다른 모든 노드와 같은 체인을 갖도록 하기 위해서는 합의가 요구된다. 개별 노드 만이 블록을 채굴하기 때문에 노드 간에 불일치가 일어나기 쉽다. 이러한 문제는 모든 프로토콜이 다른 모든 노드와 같은 블록체인을 갖도록 하는 합의 프로토콜을 통해 해결된다. 노드가 블록을 채굴하는 경우에, 해당 블록이 노드의 로컬 블록체인에 추가되지만, 이 블록은 다른 노드의 블록체인에 추가되지 않는다. 네트워크 전반에 걸쳐 블록체인을 갱신하려면 블록을 채굴한 노드가 추가 사항을 전역적인 블록체인에 중계해야 한다. 여기에서는 다른 블록 노드가 볼 수 있도록 HTTP 서버로 보내는 방식으로 새 블록체인을 중계한다.

```
/* 서버에서 가장 최근 블록체인 취하기 */
Blockchain latestChain =
HTTPServer.getServerBlockchain("http://localhost
:8000/blockchain");
// 블록체인이 크다면, 자체 로컬 체인으로 대체
if(latestChain.getBlockchain().size() >
blockchain.getBlockchain().size()){
  blockchain = latestChain;
}
```

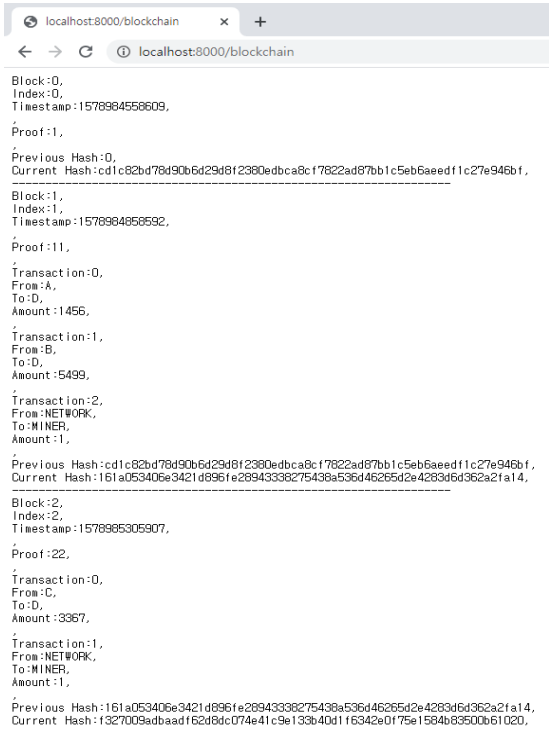

그림 5. 서버상의 최근 블록체인
Fig. 5. Recent blockchain on server

그림 5는 그림 4의 상태에서 소비자 C가 D에게 사용량을 전송한 이후의 간단한 거래에 따른 서버상에 최근 블록체인으로 두 번째 블록은 모든 거래 데이터 및 최근 거래의 부기 정보를 갖는 형태이다. 이제 네트워크상의 모든 다른 노드는 이러한 블록체인을 볼 수 있다. 여기서 블록체인의 중요한 점은 완전히 분산되어 있다는 것인데, 즉, 네트워크의 모든 노드에는 그림과 같은 자체 버전의 블록체인을 갖는다. 이것은 모든 노드가 참조하는 중앙 집중식 블록체인을 갖는 것과 다르다. 또한, 합의 프로토콜과 관련해서 각 노드는 최근 블록체인을 얻기 위해 서버에서 이를 검색하고 서버 블록체인과 자체 블록체인의 길이를 비교하는데, 암호 화폐의 프로토콜에 따라 더 긴 블록체인이 채택된다. 즉, 로컬 블록체인이 더 길면 노드가 이를 유지하지만, 서버에 게시된 최신 블록체인이 더 길면 노드는 서버 블록체인을 자체 블록체인으로 채택한다. 본 연구의 구현에서 블록체인은 단순성을 위해 블록당 하나의 거래만을 수행하는 형태이다. 블록당 더 많은 거래를 추가하면 체인 크기가 줄어들고 한 블록에 더 많은 데이터를 넣을 수 있다. 블록당 더 많은 거래를 추가하는 것은 Merkle 트리로 해싱 처리 때문에 큰 문제가 되지 않는다.

V. 결 론

본 연구에서는 스마트 미터 데이터 섭동 및 집계와 관련하여 블록체인 접근 방식을 나타내고, 손쉽게 구현할 수 있는 자바 코드를 작성하였다. 제안된 블록체인 기반 전력 소비 데이터 집계 체계는 효율적이고 가벼운 방식으로 섭동 기술의 강력함과 암호화 시스템을 결합하여 스마트 미터기와 같은 제한된 하드웨어 장치에 쉽게 적용할 수 있음을 확인하였다. 블록체인의 주요 목적은 중개자의 필요성을 제거하고 거래를 확인하고 원장의 무결성을 보호하기 위해 분산된 디지털 사용자 네트워크로 대체하는 것이다. 그렇지만, 에너지 관련 기관들이 블록체인 기술의 채택에 앞서 해결할 몇 가지 문제들이 있는데, 무엇보다도 중요한 점은 체계적이고 기술적인 정보화를 위해서 분산 원장의 기본 원칙, 에너지 블록체인 시스템의 중요한 기술적 특성을 결정하는 시스템 아키텍처 및 합의 알고리즘에 대한 고찰이 우선이고, 다음으로 에너지 부문에 대한 최적화된 블록체인 시스템 구축을 위한 여러 가지 사례와 비즈니스 기회를 검토할 필요가 있다.

References

[1] Y. Wang, F. Luo, Z. Dong, Z. Tong, Y. Qiao. Distributed meter data aggregation framework based on Blockchain and homomorphic encryption. IET Cyber Physical Systems. Vol.4 No.1, pp.30-37, 2019.
DOI: https://doi.org/10.1049/iet-cps.2018.5054

[2] Y. G. Kim, K. I. Moon. Noisy Weighted Data Aggregation for Smart Meter Privacy System. The Journal of the Institute of Internet, Broadcasting and Communication, Vol.18, No.3, pp.49-59, 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.3.49

[3] M. B. Mollah, J. Zhao, D. Niyato, K. Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, L. Yang. Blockchain for Future Smart Grid: A Comprehensive Survey. arXiv: 1911.03298v1 [cs.CR] 8 Nov 2019.

[4] L. Chen, R. Lu, Z. P. Cao. A privacy preserving data aggregation scheme with fault tolerance for smart grid communications. Peer-to-Peer Netw. Appl. 6, pp.1122-1132, 2015.
DOI: https://doi.org/10.1007/s12083-014-0255-5

[5] Z. Wang. An Identity-Based Data Aggregation Protocol for the Smart Grid. IEEE Trans. Ind. Inform. 13, pp.2428-2435, 2017.
DOI: https://doi.org/10.1109/TII.2017.2705218

[6] M. Badra, S. Zeadally. Light weight an defficient privacy-preserving dataaggregation approach for the Smart Grid. Ad Hoc Netw. 64, pp.32-40,2017.
DOI: https://doi.org/10.1016/j.adhoc.2017.05.011

[7] A. Asmaa, S. Xuemin. Lightweight security and privacy preserving scheme for smart grid customer-side networks. IEEE Trans. Smart Grid, 8, pp.1064-1074, 2017.
DOI: https://doi.org/10.1109/TSG.2015.2463742

[8] H. Debiao, Z. Sherali, W. Huaqun, L. Qin. Light weight Data Aggregation Scheme against Internal Attackers in Smart Grid Using Elliptic Curve Cryptography. Wirel. Commun. Mob. Comput. 194845, 2017.
DOI: https://doi.org/10.1155/2017/3194845

[9] E. Vahedi, M. Bayat, M. R. Pakravan, M. R. Aref. A secure ECC-based privacy preserving data aggregation scheme for smart grids. Comput. Netw. 129, pp.28-36, 2017.
DOI: https://doi.org/10.1016/j.comnet.2017.08.025

[10] L. Shaohua, X. Kaiping, Y. Qingyou, H. Peilin. PPMA: Privacy-Preserving Multi-Subset Aggregation in Smart Grid. IEEE Trans. Ind. Inform. 14, pp.462-471, 2018.
DOI: https://doi.org/10.1109/TII.2017.2721542

[11] B. Fábio, D. Denise, B. Leon, B. Johannes, M. Max. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In Proceedings of the IEEE Symposium on Computers and Communication, Funchal, Portugal, pp.1-6, 23-26 2014.
DOI: https://doi.org/10.1109/ISCC.2014.6912612

[12] N. Jianbing, Z. Kuan, L. Xiaodong, S. Xuemin. Balancing security and efficiency for smart metering against misbehaving collectors. IEEE Trans. Smart Grid 2017.
DOI: https://doi.org/10.1109/TSG.2017.2761804

[13] O. Kazuma, S. Yusuke, Y. Fumiaki, I. Mitsugu, O. Kazuo. Privacy-preserving smart metering with verifi ability for both billing and energy management. In Proceedings of the 2nd ACM Workshop on ASIA Public-Key Cryptography, Kyoto, Japan, 3, pp.23-32, 2014.
DOI: https://doi.org/10.1145/2600694.2600700

[14] P. Gope, B. Sikdar. An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-based Billing and Demand-Response Management in Smart Grids. IEEE Internet Things J. 2018,
DOI: https://doi.org/10.1109/JIOT.2018.2833863.

[15] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, pp.79-94, 2016.
DOI:https://doi.org/10.1007/978-3-662-53357-4_6

[16] J. Li, Z. Zhou, J. Wu, S. Mumtaz, X. Lin, H. Gacanin. Decentralized On-Demand Energy Supply for Blockchain in Internet of Things: A Microgrids Approach. IEEE Trans. Comput. Soc. Syst. 2019.
DOI: https://doi.org/ 10.1109/TCSS.2019.2917335

[17] S. Nakamoto. Bitcoin: A Peer-To-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 31 May 2019).

저 자 소 개

김 용 길(정회원)

- 1990년 호남대학교 전산통계학과 졸업(이학사)
- 1992년 광주대학교 대학원 컴퓨터학과 졸업(공학석사)
- 2014년 ~ 현재 : 조선이공대학교 컴퓨터보안과 부교수

• 관심분야 : 네트워크보안, 통신시스템, 정보보호

문 경 일(정회원)

- 1982년 서울대학교 계산통계학과 졸업(이학사)
- 1980년 서울대학교 대학원 계산통계학과 졸업(이학석사)
- 1991년 서울대학교 대학원 계산통계학과 졸업(이학박사)
- 1987년 ~ 현재 : 호남대학교 컴퓨터공학과 교수

• 관심분야 : 지능 시스템, 복잡성 과학

※ 이 논문은 2019년도 조선이공대학교 연구비의 지원을 받아 연구되었음