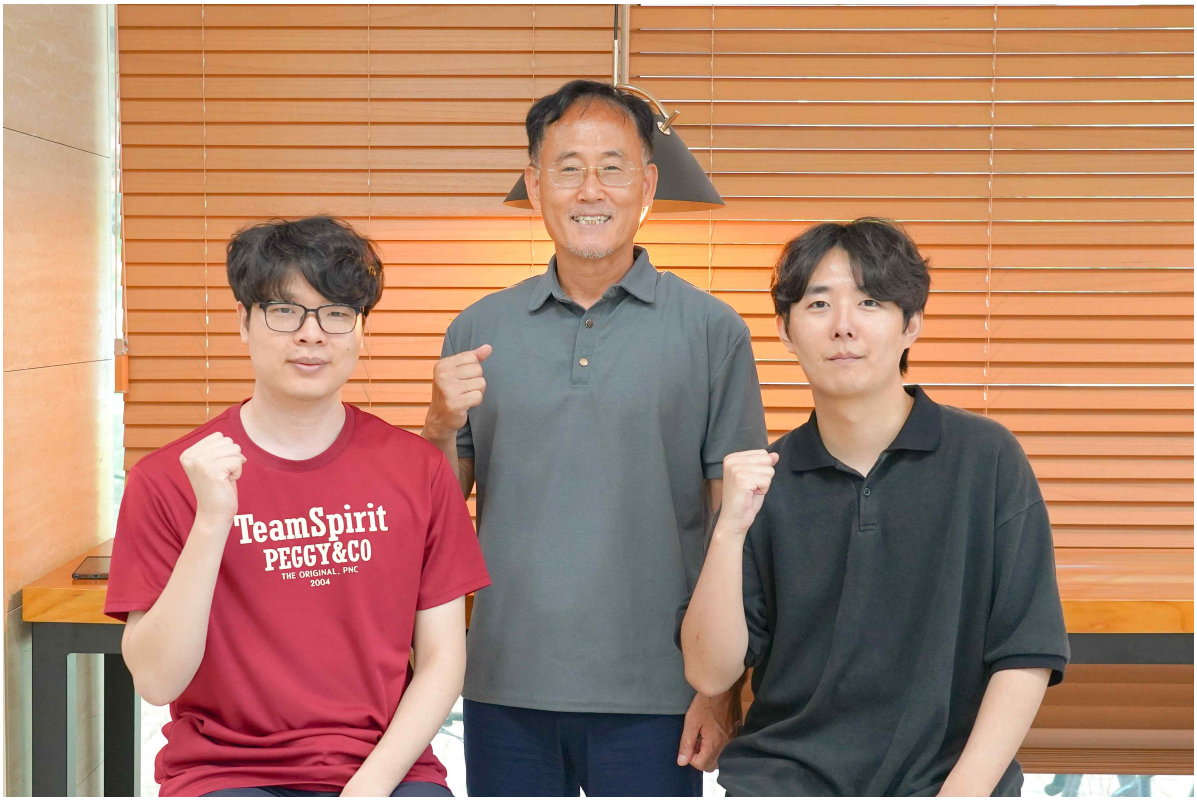
GIST, 탈중앙성과 에너지 효율 동시에 달성한 신개념 블록체인 합의 알고리즘 'ECCVCC' 개발

- 전기전자컴퓨터공학과 이흥노 교수팀, 복잡한 통신 없는 PoW의 장점은 살리면서 ASIC에 의한 채굴 독점과 PoS의 참여 제한 문제는 해결한 합의 알고리즘 설계
- 검증 기반 구조로 보안성·탈중앙성·에너지 효율 동시 확보... 차세대 메인넷 표준 기술로 주목
- 국제학술지《IEEE Transactions on Information Forensics and Security》게재



▲ (왼쪽부터) 전기전자컴퓨터공학과 최해웅 학생, 이흥노 교수, 김승민 학생

광주과학기술원(GIST, 총장 임기철)은 전기전자컴퓨터공학과 이흥노 교수 연구팀이 **블록체인의 탈중앙성을 강화하면서도 에너지 효율을 높이는 새로운 합의 알고리즘*** **'ECCVCC(Error Correction Code Verifiable Computation Consensus, 오류정정부호 기반 검증가능 연산 합의 알고리즘)'를 개발**했다고 밝혔다.

이번 연구는 **기존 작업증명(PoW)* 기반 블록체인의 장점은 유지하면서, 에너지 낭비와 채굴의 중앙화 문제를 동시에 해결**할 수 있는 기술로 주목받고 있다. 특히 **PoW와 지분증명(PoS)* 방식이 각각 갖고 있던 한계를 보완**하며, 새로운 대안으로서 **차세대 블록체인 생태계의 기반 기술로 부상**할 것으로 기대된다.

* **합의 알고리즘:** 블록체인과 같은 분산 네트워크에서 모든 참여자가 동일하고 신뢰할 수 있는 데이터 상태(블록 내용)에 도달하도록 만드는 핵심 메커니즘이다.

* **주문형 반도체(ASIC, Application-Specific Integrated Circuit):** 특정 계산 작업만을 수행하도록 설계된 고성능 반도체. 일반적인 컴퓨터나 그래픽카드(GPU)와 달리, 하나의 알고리즘이나 작업에 최적화되어 있어 해당 작업을 매우 빠르고 에너지 효율적으로 연산할 수 있다.

* **작업증명(PoW, Proof of Work):** 블록체인에서 블록 생성 권한을 얻기 위해 참여자들이 복잡한 암호 퍼즐을 경쟁적으로 푸는 방식의 합의 알고리즘. 핵심은 노드들이 합의하는데 대화를 하지 않는 점이다. 각자 퍼즐을 풀면 합의에 도달한다. 퍼즐 문제 풀이에 소비된 연산 에너지가 블록 내용을 보호한다. 구조가 단순하고 많은 노드가 참여할 수 있어 탈중앙성에 유리하지만, 연산에 많은 에너지를 소비하며, 고성능 장비를 보유한 소수에 의한 채굴 독점 문제가 발생할 수 있다.

* **지분증명(PoS, Proof of Stake):** 암호화폐를 네트워크에 예치(스테이킹)한 사용자 중 블록 생성자가 선정되는 합의 알고리즘이다. 생성된 블록에 문제가 발견될 시 블록 생성자의 예치금을 징수하도록 하여 블록 내용을 보호한다. 에너지 소모가 적지만 예치금으로 인한 진입장벽이 있다. 나아가, 비잔틴장군 문제를 푼 80년대에 고안된 Byzantine Fault Tolerance(BFT)라는 대화형 합의를 POS와 병용한다. 합의알고리즘의 구조적 복잡성 문제와 MEV 취약성 등이 문제로 지적되고 있다.

블록체인 기술은 **중앙 관리자가 없어도 참여자 간 데이터의 신뢰성과 무결성을 유지할 수 있는 분산형 시스템으로, 그 핵심은 '합의 알고리즘'**이다.

가장 널리 알려진 **PoW 방식은** 참여자들이 복잡한 암호 퍼즐을 경쟁적으로 푸는 구조로, 대화 없이 합의가 이루어지는 **'비대화형' 시스템이라는 점에서 단순하고 안정적이며, 수많은 노드*가 참여할 수 있어 높은 탈중앙성**을 가진다.

* **노드(node):** 블록체인 네트워크를 구성하는 개별 컴퓨터나 서버로, 거래 정보를 저장하고 다른 노드와 데이터를 주고받으며, 블록 생성·검증·전파 등 네트워크 유지에 핵심적인 역할을 수행하는 단위이다. 일부 노드는 전체 블록체인 데이터를 보관하는 전체 노드(full node) 역할을 하며, 다른 노드는 거래 검증이나 채굴 등 특정 기능만 수행할 수도 있다.

그러나 **ASIC 장비의 등장으로 이러한 구조에 한계**가 드러났다. 특정 연산에 특화된 고성능 장비를 가진 소수 채굴자들이 블록 생성 권한을 독점하게 되면서 **PoW는 오히려 중앙화에 취약해졌고, 막대한 전력 소모 문제**도 지적됐다. 실제로 비트코인 네트워크의 연간 전력 소비량은 폴란드 전체 수준에 근접한다는 분석도 있다.

이런 이유로 '이더리움'을 비롯한 신생 블록체인들은 PoS 방식으로 전환하거나 이를 채택하고 있으나, **PoS 역시 암호화폐를 많이 보유한 소수에게 블록 생성 권한이 집중되고, 복잡한 통신 기반의 '대화형 합의' 구조로 인해 탈중앙성과 확장성에서 한계**를 보이고 있다.

특히 PoS 기반 네트워크에서는 **소수 검증자가 거래 순서를 임의로 조작해 부당 이익을 챙기는 MEV(최대 추출 가능 가치)* 문제가 더욱 심화**되고 있다.

* **MEV(Maximal Extractable Value, 최대 추출 가능 가치)**: MEV는 블록 생성자가 거래 순서를 조작해 부당한 이익을 얻는 행위를 뜻한다. 예를 들어, 수수료가 높은 거래를 먼저 넣거나 자신의 거래를 유리하게 배치하는 방식이다. 특히 PoS 기반 블록체인에서는 소수 검증자에 권한이 집중되어 MEV 발생 가능성이 더 크다.

연구팀이 개발한 ECCVCC는 이러한 문제를 해결하기 위해 고안된 차세대 합의 알고리즘이다.

이 방식은 **무선 통신에서 사용되는 오류정정부호(ECC) 기술을 블록체인 퍼즐 구조에 접목**한 새로운 형태의 PoW로, **ASIC으로도 사전 최적화가 어려운 퍼즐을 매번 새롭게 생성**한다.

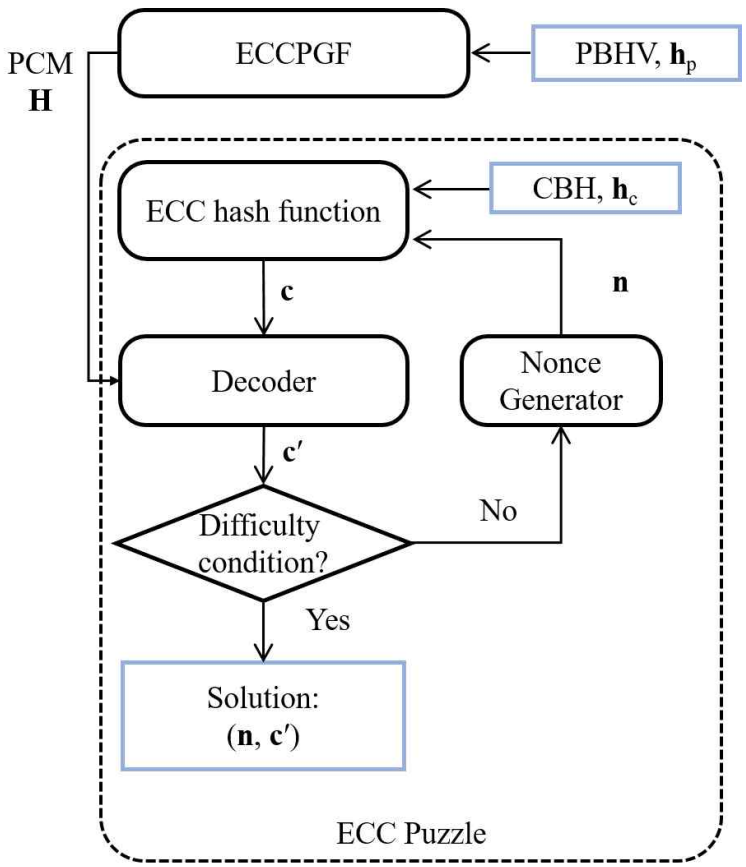
각 블록마다 **이전 블록의 해시값을 활용해 무작위성이 높은 '패리티체크 행렬'*을 생성하고, 이를 기반으로 퍼즐을 구성**한다. 이 퍼즐은 매번 구조와 정답 조건이 달라져 ASIC 장비의 일괄 적용이 불가능하다.

동시에 PoW의 비대화형 특성은 유지해 **네트워크 구조를 단순하게 유지하면서도 탈중앙성과 확장성을 확보**할 수 있다.

연구팀은 시뮬레이션을 통해 **ECCVCC가 기존 비트코인 방식보다 탈중앙성이 높고, 최근 제안된 여러 ASIC 저항형 PoW보다 약 19배 높은 저항성**을 보였다는 사실을 입증했다.

또한 ECCVCC에 **'검증가능한 동전 던지기 함수*'를 결합해 블록마다 퍼즐에 참여하는 노드 수를 자동으로 조절할 수 있도록 설계**함으로써, 불필요한 에너지 소비를 줄이고 효율성을 극대화할 수 있도록 했다.

* **검증가능한 동전 던지기 함수(Verifiable Coin Toss Function)**: 블록체인 네트워크에서 참여 노드들이 각자 채굴(합의)에 참여할지를 무작위로 결정하는 방법이다. 마치 동전을 던져 앞면이 나오면 채굴에 참여하는 것처럼, 이 함수는 네트워크가 자동으로 참여자 수를 조절해 불필요한 에너지 소비를 줄이고 효율성을 높이는 역할을 한다. 참여자가 많아지면 앞면이 나올 확률을 낮춰 경쟁 노드 수를 제한하는 방식으로 설계된다. 다만, 이 함수는 검증 함수와 쌍을 이룬다. 즉, 각 노드는 앞면이 나온 증명을 제출해야 하고, 타 노드는 검증 함수로 제출된 증명을 검증하여 참(True)이 나온 경우에만 수용하게 된다.



▲ **제안된 ECCVCC 알고리즘 개요.** 퍼즐생성함수(ECCPGF)가 이전 블록의 해쉬값 (PBHV)에 기반하여 PCM(parity-check marix)를 생성한다. ECCVCC의 암호 퍼즐은 이 PCM을 기반으로 한 오류정정부호의 디코딩 과정을 포함한다.

이 알고리즘은 **이흥노 교수의 실험실 창업기업인 리버밴스㈜가 개발·운영하는 메인넷 '월드랜드(WorldLand) My AI Network'에 실제 적용돼 기술의 실용성과 안정성을 입증**했다.

이흥노 교수는 "이번 연구는 **PoW의 단순성과 탈중앙성이라는 장점을 살리면서도 ASIC 독점 문제와 에너지 낭비를 해결할 수 있는 새로운 해법을 제시**한 것"이라며, "ECCVCC 기반 블록체인은 **'블록체인 기반 사용자 소유형 AI 에이전트 서비스(My AI Network)' 등 다양한 미래 기술 서비스의 기반 인프라**가 될 것"이라고 말했다.

이번 연구는 GIST 전기전자컴퓨터공학과 이흥노 교수가 지도하고 최해웅·김승민 박사과정생이 수행했으며, 정보통신기획평가원(IITP) 대학ICT연구센터(ITRC) 사업의 지원을 받았다. 연구 성과는 국제학술지 《IEEE Transactions on Information Forensics and Security》에 2025년 6월 24일 온라인 게재됐다.

논문의 주요 정보

1. 논문명, 저자정보

- 저널명 : IEEE Transactions on Information Forensics and Security (IF: 8.0, 2024년 기준)
- 논문명 : Error-Correction Code Verifiable Computation Consensus
- 저자 정보 : 최해웅(제1저자, EECS), 김승민(제2저자, EECS), 이흥노(교신저자, EECS)