GIST develops 'ECCVCC', a new concept blockchain consensus algorithm that simultaneously achieves decentralization and energy efficiency

- Professor Heung-No Lee's team from the Department of Electrical Engineering and Computer Science designed a consensus algorithm that solves the problems of ASIC mining monopoly and PoS participation restrictions while maintaining the advantages of PoW without complex communication

- Securing security, decentralization, and energy efficiency at the same time with a verification-based structure... Attention as a next-generation mainnet standard technology

- Published in the international academic journal 《IEEE Transactions on Information Forensics and Security》

▲ (From left) Department of Electrical Engineering and Computer Science student Haeung Choi, Professor Heung-No Lee, and student Seungmin Kim

The Gwangju Institute of Science and Technology (GIST, President Kichul Lim) announced that the research team of Professor Heung-No Lee of the Department of Electrical Engineering and Computer Science has developed a new consensus algorithm*, 'ECCVCC (Error Correction Code Verifiable Computation Consensus)', that enhances the decentralization of blockchain while increasing energy efficiency.

This research is attracting attention as a technology that can simultaneously solve the problems of energy waste and centralization of mining while maintaining the advantages of existing proof-of-work (PoW)*-

based blockchains. In particular, it is expected to emerge as a new alternative as a foundation technology for the next-generation blockchain ecosystem by complementing the limitations of PoW and proof-of-stake (PoS)* methods.

* consensus algorithm: A key mechanism that ensures that all participants in a distributed network such as blockchain reach the same and reliable data state (block contents).

* application-specific integrated circuit (ASIC): A high-performance semiconductor designed to perform only specific computational tasks. Unlike general computers or graphics cards (GPUs), it is optimized for a single algorithm or task, so it can compute that task very quickly and energy-efficiently.

* proof of work (PoW): A consensus algorithm in which participants competitively solve complex cryptographic puzzles to gain the right to create blocks in a blockchain. The key is that nodes do not communicate when reaching an agreement. Each person solves a puzzle to reach an agreement. The computational energy consumed in solving the puzzle problem protects the contents of the block. It is simple in structure and allows many nodes to participate, which is advantageous for decentralization, but it consumes a lot of energy in computation and can cause a mining monopoly problem by a small number of high-performance equipment.

* proof of stake (PoS): A consensus algorithm in which a block creator is selected from among users who have deposited (staked) cryptocurrency in the network. When a problem is found in the created block, the block creator's deposit is collected to protect the contents of the block. It consumes little energy, but there is an entry barrier due to the deposit. Furthermore, it uses an interactive consensus called Byzantine Fault Tolerance (BFT), which was designed in the 1980s to solve the Byzantine Generals' Problem, in conjunction with POS. The structural complexity of the consensus algorithm and MEV vulnerability are being pointed out as problems.

Blockchain technology is a distributed system that can maintain the reliability and integrity of data between participants without a central administrator, and its core is the ‘consensus algorithm’.

The most widely known PoW method is a structure in which participants competitively solve complex cryptographic puzzles, and it is simple and stable in that it is a ‘non-interactive’ system in which agreement is reached without conversation, and it has high decentralization because numerous nodes* can participate.

* node: An individual computer or server that constitutes a blockchain network, it is a unit that stores transaction information, exchanges data with other nodes, and plays a key role in maintaining the network, such as block generation, verification, and propagation. Some nodes serve as full nodes that store the entire blockchain data, while other nodes may only perform specific functions, such as transaction verification or mining.

However, the emergence of ASIC equipment revealed the limitations of this structure. As a small number of miners with high-performance equipment specialized for specific operations monopolized the authority to create blocks, PoW became vulnerable to centralization, and the problem of massive power consumption was also pointed out. In fact, there is an analysis that the annual power consumption of the Bitcoin network is close to the entire Polish level.

For this reason, new blockchains including ‘Ethereum’ are switching to or adopting the PoS method, but PoS also has limitations in decentralization and scalability due to the concentration of block creation authority in the hands of a small number of people who hold a lot of cryptocurrency and the complex communication-based ‘interactive consensus’ structure.

In particular, in PoS-based networks, the MEV (Maximum Extractable Value)* problem, in which a small number of validators arbitrarily manipulate the transaction order to gain unfair profits, is becoming more severe.

* maximal extractable value (MEV): MEV refers to an act in which a block generator manipulates the transaction order to gain unfair profits. For example, it is a method of putting high-fee transactions first or arranging one’s own transactions to their advantage. In particular, in PoS-based blockchains, the possibility of MEV occurrence is greater because power is concentrated in a small number of validators.

ECCVCC, developed by the research team, is a next-generation consensus algorithm designed to solve these problems.

This method is a new form of PoW that grafts the error correction code (ECC) technology used in wireless communication onto the blockchain puzzle structure, and generates a new puzzle every time that is difficult to pre-optimize even with ASIC.

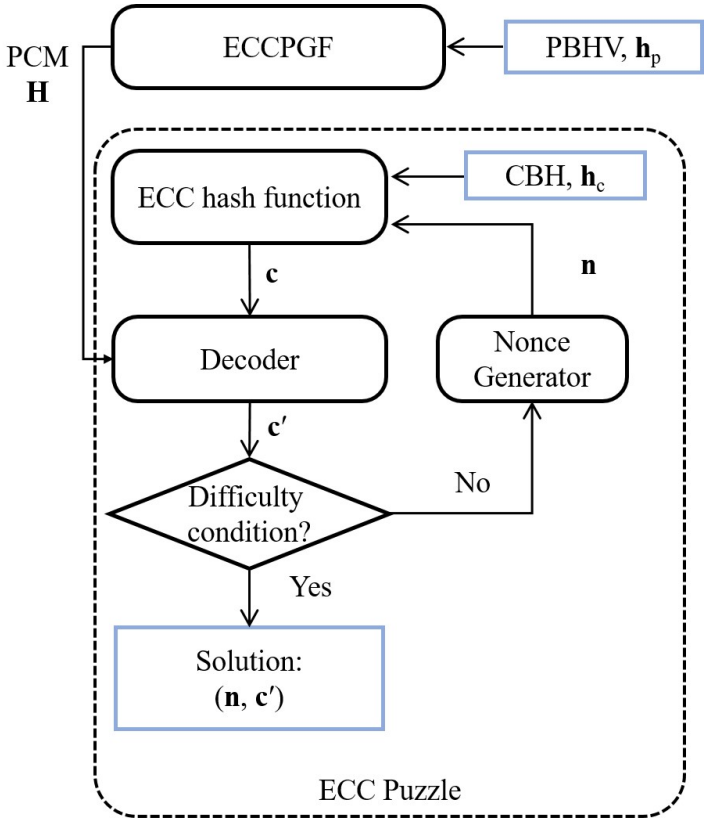
For each block, a highly random 'parity check matrix'* is generated using the hash value of the previous block, and the puzzle is constructed based on this. Since the structure and correct conditions of this puzzle are different each time, it is impossible to apply ASIC equipment in bulk.

At the same time, the non-interactive nature of PoW is maintained, so that the network structure can be kept simple while securing decentralization and scalability.

Through simulation, the research team proved that ECCVCC has higher decentralization than the existing Bitcoin method and has about 19 times higher resistance than several ASIC-resistant PoWs recently proposed.

In addition, by combining a 'verifiable coin tossing function*' with ECCVCC and designing it to automatically adjust the number of nodes participating in the puzzle for each block, unnecessary energy consumption can be reduced and efficiency can be maximized.

* verifiable coin toss function: This is a method in which participating nodes in a blockchain network randomly decide whether to participate in mining (consensus). Just as if a coin is tossed and mining occurs if the head comes up, this function allows the network to automatically adjust the number of participants to reduce unnecessary energy consumption and increase efficiency. It is designed to limit the number of competing nodes by lowering the probability of heads coming up as the number of participants increases. However, this function is paired with a verification function. That is, each node must submit a proof that the head comes up, and other nodes verify the proof submitted to the verification function and accept it only if it comes up true.



▲ Overview of the proposed ECCVCC algorithm. The puzzle generation function (ECCPGF) generates a PCM (parity-check marix) based on the hash value (PBHV) of the previous block. The cryptographic puzzle of ECCVCC includes the decoding process of the error correction code based on this PCM.

This algorithm was actually applied to the main net ‘WorldLand My AI Network’ developed and operated by Professor Heung-No Lee’s laboratory startup company, LiberVance, to prove the practicality and stability of the technology.

Professor Heung-No Lee said, “This study presents a new solution that can solve the ASIC monopoly problem and energy waste while taking advantage of the simplicity and decentralization of PoW,” and “ECCVCC-based blockchain will become the basic infrastructure for various future technology services such as ‘Blockchain-based user-owned AI agent service (My AI Network)’.”

This study was supervised by Professor Heung-No Lee of the Department of Electrical Engineering and Computer Science at GIST and conducted by Ph.D students Haeung Choi and Seungmin Kim, and was supported by the University ICT Research Center (ITRC) project of the Institute of Information and Communications Technology Planning and Evaluation (IITP). The research results were published online in the international journal 《IEEE Transactions on Information Forensics and Security》 on June 24, 2025.

GIST
Since 1993