WorldLand 합의메카니즘의 핵심 요소

이흥노*, 김영식, 만짓카르, 딜박 싱, 권효민, 이명은

*heungno@gist.ac.kr

Key Points on the WorldLand Consensus Mechanism

Heung-No Lee*, Youngsik Kim,
Manjit Kaur, Dilbag Sing, Myeongeun Lee, Hyomin Kwon

Youngsik Kim is with Chosun University. All other authors are with GIST.

요 약

This is an executive summary of the WorldLand presentation for KICS 2022 Summer Conference.

Ⅰ. Extended Summary

Blockchain technology is envisioned to transform the Internet from an information-sharing platform to a metaverse in which citizens worldwide can gather, dwell, and transact directly with each other. Transactions will not need to be arbitrated by a trusted third party thanks to the blockchain. Enriched will be person-to-person interactions among individuals and improved the lives of people throughout the world. For such a vision, it is crucial to continue innovation in the blockchain technology.

Consensus, virtual machines, and peer-to-peer networking are the three primary components of a blockchain. One of the most pressing demands at the moment is to 1) update the consensus mechanism that allows a new scalable, secure, and decentralized blockchain network, and 2) upgrade the cryptographic primitives used in consensus and virtual machines so that they are post quantum-computer (PQ) safe.

In this project, we aim to develop a novel consensus mechanism called WorldLand. WorldLand consensus is composed of two major parts, a verifiable (self-election) coin-toss function (VCT) and a novel proof-of-computation (PC) primitive. WorldLand will base its PC part on a newly published finding known as the error-correction code proof- of-work (ECCPoW). The main upgrades are to make the PC primitives PQ safer than ECCPoW and to address environmental concerns about energy expenditures. A critical component of the virtual machine will also be enhanced; particularly, the elliptic-curve cryptography and other parts built on it will be replaced with our PQ-safe cryptography.

Ethereum 2.0 is scheduled to migrate to a Proof-of-Stake (PoS) system with the Merge. It can benefit from the WorldLand consensus and virtual machine. To further contribute to the Ethereum foundation's efforts, we want to incorporate a PoS option into our WorldLand consensus. Using PoS embedding, one may regulate the barrier to entry into the pool of peer-to-peer nodes and strike a strategic balance among security, scalability, and energy consumption issues.

WorldLand protocol suite will be developed into an existing open-source version such as the Ethereum Instanbul. A proof-of-concept network will be created for validation and testing. All project outcomes will be made available to the global community through open-source code and paper publications.

ACKNOWLEDGMENT

This research was supported in part by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2021-0-01835) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation).

참 고 문 헌

[1] WorldLand NFT at Opensea.io. Type in TXID at https://opensea.io. TXID: 6359398087550852524659257829779235585141641411605797206666224231673676745932 9, Minted on May 18th, 2022.