WEB 3.0 플랫폼을 위한 *PoS* 기반 컨텐츠 검증 합의 알고리즘[1)]

홍진화°, 정진우, 인호
고려대학교 컴퓨터학과
january0507@korea.ac.kr, kuntdari@korea.ac.kr, hoh_in@korea.ac.kr

PCV : PoS for Content Validation in Web3.0 Platform

Jin Hwa Hong °, Jin Woo Jung, Hoh Peter in
Department of Computer Science and Engineering

요 약

WEB 2.0을 통해 정보의 생산과 활용, 공유와 소통이라는 인터넷 통합환경이 조성되면서 여러 형태의 가짜 컨텐츠도 우후죽순처럼 생겨났다. 진위 여부를 확인할 수 없는 정보가 무분별하게 수용 및 공유되는 문제들을 블록체인 기술로 해결하고자 한다. 본 연구는 Dapp 플랫폼 안에서 컨텐츠의 진위여부를 검증하면서 운영할 수 있도록 PCV(PoS for Content Validation)라는 알고리즘을 고안하였다. PCV는 PoS(Proof of Stake)기반 알고리즘이나, 지분이 많은 사람에 의해 합의되는 과정이 아니라 누구나 직접 컨텐츠의 진위 여부에 참여하여 결정할 수 있도록 하는 통합적 직접민주주의 시스템을 실현한 알고리즘이다.

ABSTRACT

WEB 2.0 brought the advent of environment of information production, utilization, sharing and communication. However, in spite of those advantages there are a lot of incorrect contents which are not validated on the web. Therefore we found the solution to use the consensus algorithm of blockchain in a different way from PoS(Proof of Stake). This study devised an algorithm called PCV(PoS for Content Validation) to be operated in a verifiable authenticity of contents in the Dapp platform by using vote from members as a direct democracy system.

1. 서론

사용자 참여 비즈니스는 여러 분야에서 이용되고 있다. 하지만 실질적 정보를 제공하는 주체인 사용자에게는 충분한 보상이 이루어지지 않고 있다. 컨텐츠에서 발생하는 이익은 대부분 플랫폼 측에서 가져간다. 이에 Web3.0에 맞는 새로운 형태의 플랫폼을 제안하고자 한다. Dapp단에서 사용자는 컨텐츠를 제공하면서 보상받고, 조회하면서 토큰을 사용한다. 검증되지 않은 컨텐츠가 사용자에게 노출될 경우, 사용자는 토큰을 사용하면서 잘못된 정보를 얻게 될 위험이 생긴다. 이는 사용자의 서비스 만족도를 크게 저하하므로 컨텐츠 검증 과정은 필수적이다.

본 연구는 이러한 컨텐츠 검증을 블록체인 합의 알고리즘을 활용해 해결하고자 한다. Web3.0의 특성을 이용한 합의 알고리즘을 통하여 사용자들의 투표방식으로 정보를 검증할 수 있다. 올바른 컨텐츠를 투표하는 경우에서 Nash equilibrium을 이룰 수 있도록 설계한다. 이러한 Nash equilibrium 형성을 위해서는 특정 집단의 사용자가 아닌 전체적인 사용자 집단의 의사가 포함되어야 한다. 그러나 기존의 PoS는 지분이 많은 사용자에 의해 합의가 이루어지는 방식이다. DPoS(Delegated Proof of Stake)도 지분이 많은 사용자 중 선출자에 의

해 합의가 진행되므로 두 합의 알고리즘 모두 소규모의 지분이 있는 사용자들은 합의에 참여하지 못한다. 본 논문에서는 지분의 많고 적음 없이 투표에 참여하고 싶은 회원들에 의해서 올바른 컨텐츠를 투표할 때 Nash equilibrium을 이룰 수 있음을 보이고, 직접민주주의를 합리적으로 실현할 수 있는 합의 방법인 PCV(PoS for Content Validation)를 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 PoS 합의 알고리즘의 방식을 다루고 있다. 3장에서 본 연구의 핵심인 PCV 합의 알고리즘과 유효성을 논한다. 4장에서는 향후 연구 방향에 대한 논의와 결론을 서술하고 본 논문을 마무리한다.

2. 관련연구

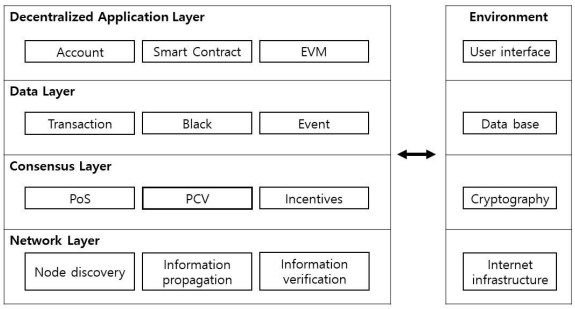

그림 *1. PCV* 합의 알고리즘이 적용된 블록체인 아키텍쳐

PoS(Proof- of- Stake) 합의 알고리즘

합의 알고리즘이란 블록체인에서 상호 연결점이 없는 분산된 노드들 사이의 트랜잭션과 블록의 유효성을 결정하여 신뢰성과 보안성과 무결성을 보장해주는 특정한 메커니즘으로써 전체 분산 네트워크 시스템을 원활하게 작동될 수 있게 해주는 것이다. 합의 알고리즘의 종류도 여러 가지가 있는데 이 논문에서 우리가 사용할 알고리즘은 PoS(Proof- of- Stake)라는 합의 메커니즘이다. 가지고 있는 지분에 따라 무작위로 선정된 블록 생성자(proposer)는 블록을 생성하고 검증자(validator)는 블록을 검증 및 승인하는 방식으로 해당 암호화폐(native token)를 보유하고 있는 지분에 비례해 블록을 생성할 확률이 달라진다. 이더리움에서 validator가 되려면 특정 양(32ETH) 이상의 코인을 예치하고 있는 validator만이 투표의 자격을 가지게 된다. 따라서 PoS는 직접민주주의라고 하지만 최소 32ETH(2022년 10월 기준 5만 달러)를 가지고 있는 지분 투자자들만이 투표하는 조건적 민주주의 방식이라고 할 수 있다. 이 논문에서 제시하는 그림1의 PCV(PoS for Content Validation) 알고리즘은 지분(자본)을 많이 가지고 있는 사용자가 아니더라도 자신의 토큰으로 투표에 참여해 합의를 이루어낸다. 사용자가 올바른 컨텐츠에 대한 명확한 결정을 내림으로 블록체인 네트워크가 운영되는 직접민주주의합의 알고리즘을 제시하였다.

Nash equilibrium

경쟁자의 대응에 따라 각자 제일 합리적인 선택을 할 때, 서로가 자신의 선택을 더는 바꿀 필요를 느끼지 않는 상태를 말한다.

전체 투표한 사람을 N명, 사람들이 올바른 컨텐츠를 택할 확률을 a라 하자. 과반수인 $\left[\frac{N}{2}\right]+1$명 이상이 올바른 컨텐츠를 택하면 된다. Nash equilibrium이 올바른 컨텐츠를 선택할 경우에 형성된다면, 아래의 확률이 a 값보다 더 커야 한다.

$$P(X \geq \left[\frac{N}{2}+1\right]) = \sum_{x=\left[\frac{N}{2}+1\right]}^{N} {}_{N}C_{x} \times a^{x} \times (1-a)^{N-x}$$

식 *1.* 집단 단위에서 올바른 컨텐츠가 선택될 확률 *P*

실제로 a가 0.8, N이 5일 때, 확률 $P(X \geq \left[\frac{N}{2}+1\right])$는 0.94208이다. 해당 식은 이항분포를 따르고, N이 커질수록 1에 수렴한다. N이 30 이상인 경우에는 정규분포로 근사할 수 있다. 정규분포로 근사해서 계산해보면, a가 0.6, N이 100일 때, 확률 $P(X \geq \left[\frac{N}{2}+1\right])$는 0.9729이다. 실제 개인이 올바른 컨텐츠를 선택할 확률보다 집단 단위가 되었을 때, 올바른 컨텐츠를 선택할 확률이 더 높아짐을 알 수 있다. 그리고 그 집단의 규

모N가 커질수록, 개별적으로 올바른 컨텐츠를 선택할 확률a이 0.5를 초과하면 최종적인 검증도 올바를 확률 $P(X \geq \left[\frac{N}{2}+1\right])$이 높다.

3. PCV(PoS for Content Validation) Algorithm

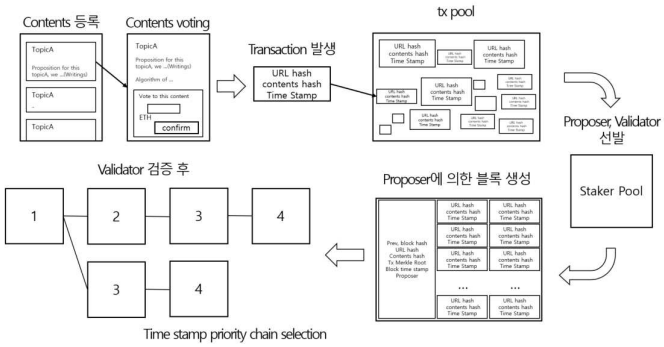

그림 *2. PCV(PoS for Content Validation)* 알고리즘

그림2는 PCV(PoS for Content Validation) 알고리즘을 순서대로 나타낸다. 이 논문에서 제안하는 방식은 컨텐츠의 진위를 Dapp단에서 사용자에게 올바른 컨텐츠에 투표하고 블록 생성자(proposer)와 검증자(validator)를 통해 블록을 생성하고 검증하여 판별한다. PoS 합의 알고리즘을 바탕으로 기존에 중앙화 되어 있던 플랫폼 비즈니스 방식을 다수 사용자가 보상받을 수 있는 public blockchain의 장점을 살려 구체적으로 적용해 보고자 했다. 기본적으로 PoS기반 분산 원장 합의 과정에 참여하기 위해 네이티브 토큰을 보유하고 있어야 하며, 기존 DPoS(Delegated Proof of Stake)방식과 다르게 Dapp에 등록된 모든 토큰 소유자가 합의에 참여할 수 있다. 그림 2는 PCV 알고리즘의 전체 흐름도이다. Dapp에 등록된 사용자들이 컨텐츠를 작성한 뒤 등록을 하게 된다. 네이티브 토큰을 보유한 모든 사용자 중 참여하고 싶은 사용자는 메타마스크를 이용해 컨텐츠에 본인의 토큰을 이용해 1cpu당 1vote의 투표를 시행한다. 이때 어떤 컨텐츠에 몇 표가 나왔는지는 사용자들은 알 수 없다. 투표가 끝난 컨텐츠들은 스마트 컨트랙트를 통해 Dapp system_deposit에 쌓인 총액, 투표수, 모든 투표자의 계정 주소와 투표한 금액, URL 주소 해시, 컨텐츠 해시, timestamp, 트랜잭션 해시값을 하나의 트랜잭션 형태로 하여 블록체인 네트워크 트랜잭션 풀(transaction pool)로 옮겨진다. 트랜잭션 풀에서 각 트랜잭션을 검증한 후, 비콘체인(beacon chain)에서 다수의 지분을 소유한 사용자 중에 랜덤으로 proposer와 validator를 선출한다. 이때 선출 랜덤함수는 VRF(Verifiable Random Function)를 사용한다. proposer는 트랜잭션 풀에 있는 검증이 끝난 컨텐츠들을 묶어서 블록을 생성한다. 생성된 블록은 validator가 블록 헤더 값(트랜잭션에 대한 머클루트 값, 컨텐츠와 컨텐츠의 URL에 대한 해시, 트랜잭션마다 투표된 합계, timestamp)을 검증한다. 검증이 끝난 블록은 블록체인 네트워크에 확정된다. 결국 높은 확률로 올바른 컨텐츠가 높은 투표수를 받고 블록체인 네트워크에 확정되는 방향으로 Nash equilibrium을 이루므로 진위가 판별된다.

여기서 포크(fork)가 일어날 경우, time priority selection으로 블록 안에 있는 정보에서 timestamp가 빠른 블록이 선택되어 올바른 chain이 계속 선택되도록 한다. 중복 보상 처리 방지와 악의적인 블록 생성에 대한 예방을 위해 검증된 현재 컨텐츠를 포함하여 과거 6개에 대한 블록이 confirm이 되었을 시(6 confirms) 컨텐츠를 Dapp에 올린 제공자와 토큰을 스테이킹하고 투표에 참여한 자, proposer, validator가 일정 보상을 받게 된다. 올바르지 않은 컨텐츠를 선택했던 회원은 투표 시에 걸었던 본인 소유의 토큰을 빼앗기게 되고, 빼앗긴 토큰은 앞서 설명한 보상으로 쓰인다. proposer가 잘못된 블록을 생성하거나 validator의 잘못된 검증이 이루어질 경우, 본인이 가지고 있는 토큰을 빼앗기게(flushing) 되는 페널티를 갖게 하여 잘못된 블록이 생성되는 것을 예방한다. 지분을 가지고 있는 사람들은 일정 시간 동안 암호화폐 지갑 (cryptocurrency wallet)의 코인을 담보로 시스템에 맡기는 것만으로도 보상받을 수 있다. 하지만 맡겨진 지분은 잠긴(Locking) 상태가 되므로 담보 기간에는 사용할 수 없다.

4. 향후 연구 및 결론

유튜브가 Web3.0 플랫폼이라고 하는 사람들이 있다. 하지만 유튜브는 참여자가 활동에 따른 보상을 받지만,

거버넌스(governance) 상에서 컨텐츠의 적합성과 기준과 같은 요소들이 중앙의 통제로부터 자유롭지 않다는 단점이 있다. PCV(PoS for Content Validation) 알고리즘은 기존 PoS의 합의 방식인 대의 민주주의 방식이 아닌 사용자가 직접 선정한 컨텐츠의 투표수에 의해서 합의가 이루지는 방식이다. 결국 투표자들이 자신의 손실을 최소화하는 선택을 할 때, 서로가 선택을 더는 바꿀 필요를 느끼지 않는 상태는 본인이 올바른 컨텐츠를 선택하고, 집단적으로도 올바른 컨텐츠가 선정될 경우라는 수학적 증명을 바탕으로 설계되었다.

PCV 알고리즘을 이용하여 컨텐츠의 범위를 넓히는 부분도 고려하고 있다. 본 연구에서는 객관적인 해답이 존재하는 컨텐츠로 범위를 제한했지만, 앞으로는 다수결에 의하여 주관적인 방향성이 있는 컨텐츠까지 범위를 넓혀가고자 한다. 또한 컨텐츠의 진위를 판별했지만, 세월이 흘러감에 따라 그 진위가 바뀌는 경우도 있는데, 이러한 경우 Dapp단에서 과거에 올바르게 컨텐츠에 투표했던 투표자에 대한 보상은 어떻게 해야 할지와 내부 블록체인 네트워크 시스템에서는 어떻게 처리해야 하는지에 대한 고찰이 필요하다.

5. 참고 문헌

[1] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[2] BACH, Leo Maxim; MIHALJEVIC, Branko; ZAGAR, Mario. Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Ieee, 2018. p. 1545-1550.

[2] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. (2019). IEEE Access, 7, 85727-85745.

[3] Nick Szabo, Smart contracts (1994,); Nick Szabo, Formalizing and securing relationships on public networks, 2 First Monday (No. 9, 1997).

[4] Madani, Kaveh. "Game theory and water resources." Journal of hydrology 381.3-4 (2010): 225-238.

[5] Aumann, Robert J. "What is game theory trying to accomplish?." Frontiers of Economics, edited by K. Arrow and S. Honkapohja. 1985.

[6] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." self-published paper, August 19.1 (2012).

1) 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신 기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00177, 스마트 컨트랙트의 개발-배포-실행의 전주기적 취약점 및 신뢰성 오류 개선 기술개발)