Proof of Stake versus Proof of Work (White paper)

BitFury Group, 2015

이부형 (boohyung@pel.smuc.ac.kr)

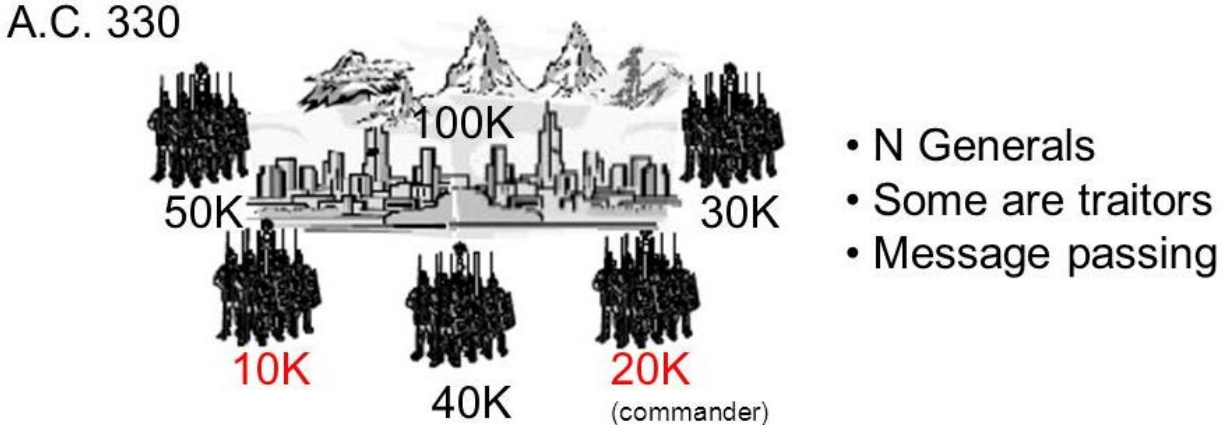
상명대학교 프로토콜공학연구실

Contents

- Theory
- Implementations
- Attacks and Problems

Theory (1/5)

- Consensus Algorithm
  - P2P 네트워크 내 서로 신뢰할 수 없는 노드들 간의 의사 결정 문제를 해결하기 위한 수단
    - “Byzantine Generals Problem”



  - 블록체인 플랫폼에서 사용하는 대표적인 합의 알고리즘: PoW, PoS, DPoS
    - 다수가 참여하고 일정 시간이 걸리는 연산작업을 통해 누가 블록 생성할 것인지 결정

Theory (2/5)

- Proof of Work (PoW)
  - 거래 사실을 선의의 노드들이 자신의 노동 (연산작업)으로 증명하고 검증하는 절차를 의미
    - 컴퓨팅 파워가 높은 노드일 수록 빠른 연산을 수행하여 증명 작업을 빨리할 수 있음
    - 블록 생성을 위한 작업을 “마이닝 (Mining)”이라고 칭함
  - 동작 과정
    - 거래가 생기면 네트워크 내 모든 노드들에게 브로드캐스트
    - 임의의 노드들 (마이너)은 생성된 블록을 검증하기 위해 연산 작업을 수행
      - $h(h(n-1\ th\ block\ header)||nonce) \geq x$
        - nonce = 0부터 시작하여 조건을 만족하는 x를 찾을 때까지 1씩 증가하는 값
    - 연산 작업을 완료한 마이너는 10분 단위로 발생한 거래들을 모두 모아 블록을 생성

Theory (3/5)

- Proof of Stake (PoS)
  - PoW의 대안으로 제안되어 사용된 합의 알고리즘
    - Peercoin, 2012
    - 블록 생성을 위한 작업을 “마인팅 (Minting)”이라고 칭함
  - 컴퓨팅 파워가 아닌 지분의 보유량에 따라 랜덤하게 노드의 합의 결정권이 달라짐
  - 블록을 생성하기 위해 노드 A는 아래의 조건을 만족해야 함
    - $h(h(n-1\ th\ block\ header)||A||t) \leq bal(A) * \frac{1}{d}$
      - t를 계속 1씩 증가시키면서 대입, 조건에 부합하면 다음 블록 생성
        - A = 노드 A의 주소
        - $bal(A)$ = 노드 A가 가진 지분의 양
        - t = 시간; 현재 시각 - 이전 블록 생성 시각
        - d = bits (난이도)

Theory (4/5)

- Proof of Stake (PoS)
  - PoW와 비교했을 때의 장점
    - 노드가 보유한 자산을 이용하기 때문에 블록 생성권이 집중되지 않음
      - PoW를 사용할 경우 높은 컴퓨팅 파워를 가진 마이닝 풀이 생기고, 블록 생성에 대한 권리를 독점할 가능성이 있음
    - 블록 생성 속도가 매우 빠름
      - PoW를 사용할 때는 평균 10분, PoS를 사용하면 평균 1분 이내
    - 51% Attack에 강인함
      - 공격자는 전체 네트워크가 소유한 자산 중 절반 이상을 차지하고 있어야 네트워크를 통제할 수 있음

Theory (5/5)

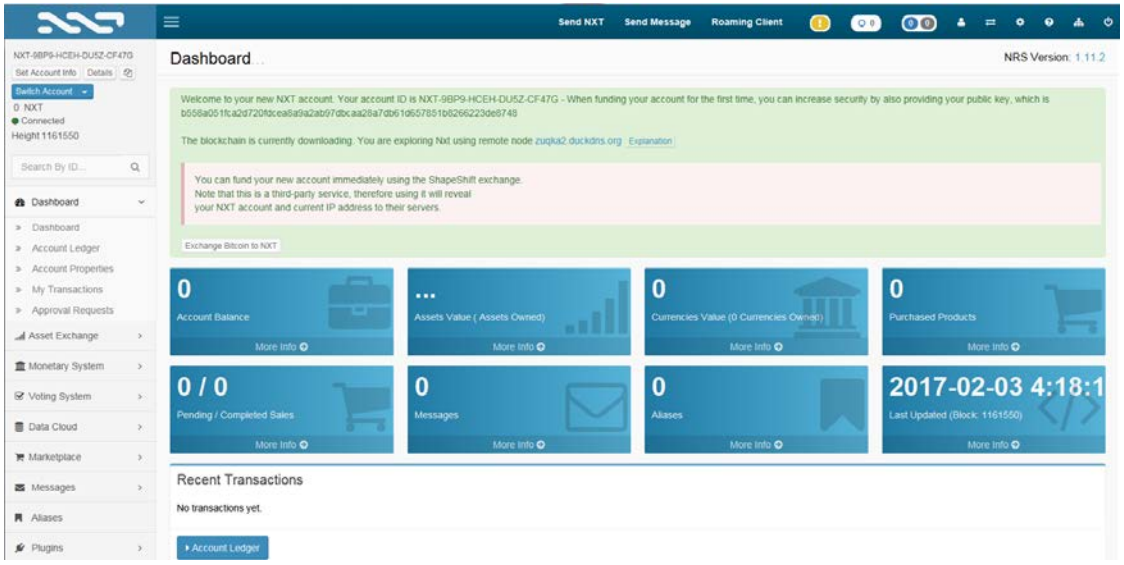
- Delegated Proof of Stake (DPoS)
  - 네트워크를 구성하는 모든 노드들간의 투표 결과로 대표자 노드들을 선정, 대표자 간의 합의로 블록 생성
    - 대표자의 권한
      - 블록을 생성하여 블록체인에 추가
      - 대표자 간의 투표를 통해 악의의 노드를 추방 가능
      - 블록 내 발신자, 수신자, 잔고 등의 정보는 임의로 변경할 수 없음
    - 단위 시간 당 생성되는 블록 개수가 상대적으로 적고, 비용이 적게 소요됨
      - 합의 절차에 참여하는 노드의 수가 적기 때문
  - 2013년부터 Bitshares에서 합의 알고리즘으로 사용

Implementations (1/4)

- Peercoin (PPCoin)
  - P2P 분산 네트워크 기반 암호화폐
    - 2012년, Sunny King이라는 익명의 개발자가 제안
  - 합의 알고리즘으로 PoW와 PoS를 함께 사용
    - PoW: Bitcoin과 동일
    - PoS: “Coin age”가 가장 많은 지갑을 가진 노드가 블록을 생성
      - Coin age = 화폐의 양 * 보유한 일수
      - 화폐를 보유한 일수는 타임스탬프를 통해 계산
      - 화폐를 소비한 경우 Coin age는 줄어듬

Implementations (2/4)

- Nxt
  - 블록체인 어플리케이션 플랫폼
    - P2P 분산 네트워크 위에서 누구든 다양한 응용 프로그램을 개발하고 서비스할 수 있도록 지원
  - PoS를 합의 알고리즘으로 사용
    - 블록 생성 시간: 평균 60초
  - Nxt Client를 통해 현재 화폐 거래, 자산 교환, 메신저, 전자 투표 등의 기능을 제공



Implementations (3/4)

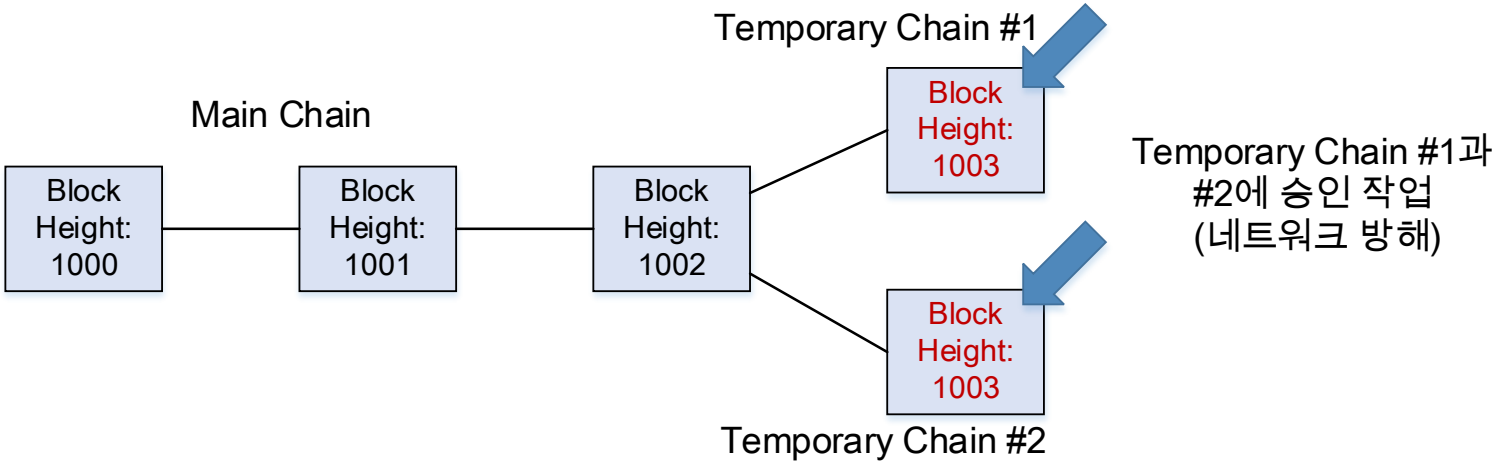
- Bitshares
  - Decentralized Autonomous Company, DAC
    - 블록체인을 이용한 서비스 제공을 통해 수수료로 수익을 창출하는 일종의 기업
    - 가상 자산의 판매자와 구매자들을 연결해주는 중개자 역할
  - 합의 알고리즘으로 DPoS를 사용
    - 대표자 수 = 101명
    - 101명의 대표자가 순번을 정하여 차례대로 블록을 생성
  - 제공하는 서비스
    - 금융 관련 서비스: 송금 및 저축
    - 거래소 서비스: 비트코인을 포함한 자산거래
    - 음원 등 디지털컨텐츠를 제공하는 서비스
    - 도메인 거래 서비스

Implementations (4/4)

- Tendermint
  - 블록체인 어플리케이션 플랫폼
    - Go언어 기반 고성능 API 구현
  - 블록 생성: 채굴 작업을 하지 않고, 노드 간 동의를 사용
  - 블록 승인
    - 승인에 참여하는 노드들은 보증금을 걸고 승인에 참여
    - 정상적으로 승인 작업이 완료되면 보증금을 돌려받음
    - 악의적인 사용자는 보증금을 회수할 수 없음
  - Ethereum에서 개발 중인 Casper와 유사
    - Ethereum이 합의 알고리즘을 PoW에서 PoS로 변경하면서 Casper를 개발

Attacks and Problems (1/5)

- PoS를 사용할 경우 발생할 수 있는 공격이나 문제점
  - Nothing at Stake Problem
    - 블록체인이 fork된 경우, 공격자가 고의로 두 체인의 마지막 블록에 승인을 위한 작업을 할 수 있음
    - 메인 체인을 빨리 식별하지 못하게 네트워크를 방해
      - PoS 합의 알고리즘의 가장 큰 문제
    - 방어: DPoS를 이용하면 대표자들이 블록을 생성하기 때문에 이러한 문제점을 해결할 수 있음



Attacks and Problems (2/5)

- PoS를 사용할 경우 발생할 수 있는 공격이나 문제점
  - Bribe Attack
    - 가정: 6-Confirmation이 완료되야 거래가 확정됨
    - 공격 시나리오
      - 거래1 생성: “선의의 노드 A -> 100만원, 선의의 노드 B”
      - 거래1이 확정되기 전에 거래2(“선의의 노드 A -> 100만원, 악의의 노드 C”)를 생성
      - 다수의 노드들 (선의의 노드이지만 소유한 자산이 적어서 블록 생성이 힘든 노드들)에게 뇌물 명목으로 인센티브를 제공
      - 다수의 노드들로 인해 거래 1보다 거래 2가 먼저 확정처리됨
    - 거래가 확정되면 선의의 노드 B가 아니라 악의의 노드 C에게 소유권이 생김
      - 노드C가 제공한 인센티브의 합 < 100만원
    - 방어: 합의 알고리즘으로 DPoS를 사용

Attacks and Problems (3/5)

- PoS를 사용할 경우 발생할 수 있는 공격이나 문제점
  - Coin Age Accumulation Attack
    - 공격자가 자신의 Coin age를 정당한 노드들보다 월등히 높게 축적시켜놓고 그를 이용하여 네트워크를 방해하는 행위
      - 예. 전체 자산이 10,000, 공격자가 500을 가지고 있으며 시간이 지나도 자산의 양 변화 없음
        - 공격자는 시간이 지날 수록 자신의 Coin age를 늘릴 수 있음; 2년만 지나도 전체 자신의 10% (이중 지불 유도 가능), 10년이 지나면 절반 이상을 차지하여 네트워크를 지배할 수 있음
    - 원인: Peercoin PoS v1에서 Coin age의 한도를 제한하지 않고 사용함
    - 해결: Peercoin PoS v2에서 Coin age를 90으로 제한
      - Blackcoin이나 Novacoin에서도 이를 차용하여 사용

Attacks and Problems (4/5)

- PoS를 사용할 경우 발생할 수 있는 공격이나 문제점
  - Denial of Service
    - 정상적인 네트워크 동작을 방해하는 것이 목적
    - 예. 하나의 공격자가 매우 많은 수의 low-value transaction을 일으키는 행위
      - 불필요한 블록 발행 및 거래 서명/검증 작업이 요구됨
      - 실제로 2015년 7월에 비트코인을 공격한 사례가 있었음
  - Sybil Attack
    - 원활한 네트워크 동작의 방해를 목적으로 공격자가 가짜 노드를 만들어서 불필요한 거래를 만드는 행위

Attacks and Problems (5/5)

- 공격 방법에 따른 합의 알고리즘 별 공격 가능 여부 비교

공격 방법	PoW	PoS	DPoS
bribe attack	X	O	X
Coin age accumulation attack	X	PoS의 구현에 따라 다름	X
Denial of Service	O	O	O
Sybil Attack	O	O	O

감사합니다!

이부형 (boohyung@pel.smuc.ac.kr)