블록체인을 적용한 성적인증 시스템

1871227
IT공과대학
임세진

현재 시스템의 문제점

성적 전산조작 사건 터진 부산외대 보안강화 뒷북 대책

대학교 해킹해 성적 조작…'F'에서 'A'로

[뉴스탐색] "우리 학교도 성적조작…" 학사비리 의혹에 경찰수사 나선다

기사입력 2018-11-30 09:01

가 가

경찰, 제자와 성관계맺고 성적 조작해준 교사 소환

이 사건은 대학 당국이 특정 학생의 성적을 임의로 올렸다는 점에서 '정유라 사건'과 흡사하다.

中 대학생 해커, 대학 전산 시스템 해킹해 성적조작

현재 시스템의 문제점

- 고등학교와 대학교) 확정된 성적을 일정기간이 지난 뒤 개인적인 목적으로 조작한 사례 有
- 대학의 경우, 학생들이 각 평가요소에서 자신이 받은 점수를 제때에 확인하지 못하고 마지막에 학점으로만 확인하게 되는 경우가 많음 => 정보의 비대칭성
- 학번으로 평가요소별 성적을 공개하는 등의 방법이 있지만 익명성이 떨어짐
- 각 평가요소마다 본인의 상대적인 성적이 어느 정도인지를 정확히 알 수가 없어 만족스럽지 못한 성적이 나와도 선뜻 이의제기를 할 수 없음

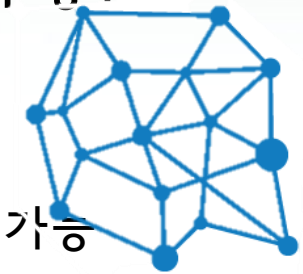
왜 블록체인을 이용?

블록체인 : 참여하는 모든 사용자들이 데이터를 서로 분산, 저장하여 데이터가 조작되는 것을 막는 기술

- **탈중앙화 :** 분산화 된 서버들에 블록이 보관되고 이 기록은 누구나 확인 가능
- **보안성 :** 해킹을 하려면 모든 노드들의 거래 데이터를 공격해야 하므로 불가능
- **투명성 :** 기록의 참,거짓 여부를 과반수의 합의를 얻어야 하며, 누구나 기록 열람 가능

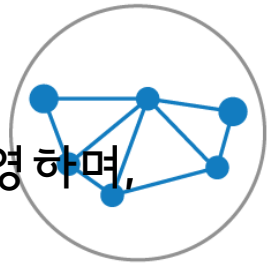
왜 블록체인을 이용?

노드 권한에 따른 블록체인의 종류



- 퍼블릭(Public) 블록체인

: 누구나 장부의 관리에 참여가능



- 프라이빗 (private) 블록체인

: 하나의 기관이나 기업이 독자적으로 운영하며,
사전허가를 받은 사람만이 참여가능

- 컨소시엄 블록체인(Consortium blockchain)

: 네트워크에 허가된 여러 참여자가 블록을 생성가능
즉, 기업 연합형 블록체인

왜 블록체인을 이용?

퍼블릭(Public) 블록체인

- 어느 누구나 열람이 가능한 공개형태의 블록체인
- 컴퓨팅 파워를 이용한 채굴(Proof-of-Work)과정을 통해 거래의 정당성 인증
- 개인 또는 중앙기관의 영향을 받지 않는 탈중앙화, 분권화된 시스템

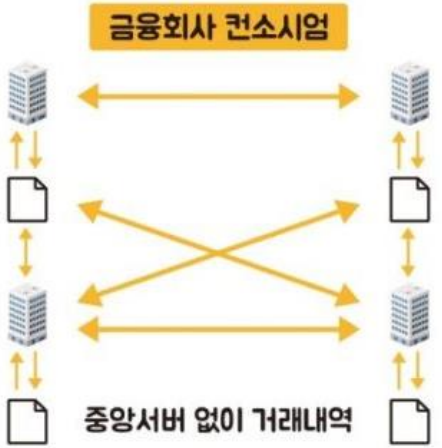
- 많은 인원이 참여할 시 네트워크 처리속도가 더뎌질 수 있고,
  인증이 안된, 악의적인 목적을 가진 해커의 접근이 가능
- 모든 노드가 같은 권한을 가져 규제가 필요한 영역 적용에 한계

왜 블록체인을 이용?

프라이빗 (private) 블록체인

- 폐쇄형 블록체인 => 한 집단의 독자적인 블록체인
- 완전히 개인화된 블록체인으로서, 한 중앙기관이 모든 권한을 가지며 네트워크에 참여하기 위해선 그 중앙기관의 허락이 필요함 => 기밀성과 보안성
- 하나의 주체와 블록체인의 참여자가 분명함
- 허가된 참여자 외에게는 거래내역이 공유되지 않음
- 네트워크 처리속도 신속
- 블록체인의 중요가치인 탈중앙성을 잃게 됨

왜 블록체인을 이용?



컨소시엄 블록체인(Consortium blockchain)

- 퍼블릭과 프라이빗 블록체인의 중간형태
- 같은 목적을 가지고 있는 여러 기관이 하나의 컨소시엄을 구성하여 공정성과 확장성을 보완한 반 중앙형 블록체인
- N개의 기관이 노드를 한 개씩 운영하고 각 기관의 노드 간 동의가 일어나야 거래생성가능
- 블록체인의 기록 열람 권리를 대중에게 부여할 수도 있고(퍼블릭), 참여자에게만 제공하거나 API를 통해 특정 인원에게만 공개할 수도 있음

프로그램 간 커뮤니케이션을 담당하는 기능

왜 블록체인을 이용?

퍼블릭 블록체인 (Public blockchain)	컨소시엄 블록체인 (Consortium blockchain)
거래증명자가 익명이기 때문에 무법적 요소가 강함. 51% 공격이나 이중송금(double spending)의 위험성이 존재	거래 증명자가 인증을 거쳐 알려진 상태(known)이기 때문에 51% 공격이나 이중송금(double spending)과 같은 문제가 없음
한번 정해진 법칙을 바꾸기 굉장히 어려움	블록체인 소유자에게 알맞게 법칙을 바꿀 수 있음
네트워크 유지(채굴)하는데 드는 비용이 큼	네트워크 유지비용이 거의 없음
네트워크 확장이 어렵고 거래속도가 느림	네트워크 확장이 쉽고 거래속도가 빠름

왜 블록체인을 이용?

	퍼블릭 블록체인	컨소시엄 블록체인	프라이빗 블록체인
신뢰성	높음	중간	낮음
안정성	낮음	중간	높음
익명성	높음	중간	낮음

구현해보기(앱)

컨소시엄 블록체인 적용

참여노드 : 각 수업의 교수님들
열람 권리를 가진 사람 : 참여노드, 해당 수업의 학생들

노드 : 앱에서 교수인증을 통해 노드 허가를 받음 -> 각 평가(시험이나 과제물)마다 정정기간을 거친 뒤, 확정된 점수를 입력한 블록 생성

열람권리 : 앱에서 학생인증을 통해 해시ID생성 -> 열람권리를 받음

구현해보기(앱)

블록에 들어가는 내용

헤더 : Prev_Hash + Time + 해당 교수의 수업명

출력 : 해당 평가이름(ex. 중간평가) + 학생들 석차(이름 부분은 해시ID로) + 학생들 점수

기대효과

- 학생들이 해당 점수의 분포와 자신의 상대적 위치를 보고 학점예상이나 다음 시험 때 더욱 열심히 준비한다든지 등의 방향을 잡을 수 있음

- 석차가 상위권이었음에도 불구하고 납득할 수 없는 학점을 받은 경우, 이의제기를 하기에 용이함 (실수로 학점이 잘못 나가는 경우 방지 가능)

- 추후에 개인적 이익을 위한 성적조작을 방지할 수 있음

한계점

- 수정이 불가능 (양날의 검)

  블록을 수정하는 순간 해당 블록의 해시가 변경되고

  블록 헤더에 이전 해시(Prev_hash)가 들어있는데 블록 해시가 변경되면

  다음 블록 헤더에 있는 이전 해시와는 다른 해시 값이 되어 연결이 끊어지며 사용할 수 없게 됨

  => 정정기간을 다 거친 뒤, 확정된 평가요소별 성적을 블록으로 만들어야 함

- 성적 입력하여 블록 생성할 때 조작을 하는 경우는 막을 수 없음

  또한 수정이 어렵기 때문에 조작된 성적을 원래대로 복구하는 일도 어려움

Thank you