블록체인 시험 박성준 교수 졸업시험

|  |
| --- |
| 1. 블록체인의 정의 |
| **블록체인**(block chain, blockchain)은 관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장되어 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 데이터 위 변조 방지 기술이다. |

|  |
| --- |
| 2.비트코인과 이더리움의 차이 |
| 튜링 완전성의 차이가 존재함  비트코인은 단순히 거래만 가능하지만 이더리움은 플랫폼으로서 스마트 컨트렉트 라는 프로그래밍을 통한 튜링 완전한 기능이 추가됨 |

|  |
| --- |
| 3.블록체인 분류 : 퍼블릭과 프라이빗 |
| 퍼블릭 : 블록생성 권한을 가지는 권한을 체인에 참여한 모든 노드가 가짐 대신 그만큼 느림  프라이빗 : 블록생성 권한을 가지는 노드를 선별하거나 제한을 둠 대신 그만큼 속도가 빠름 |

|  |
| --- |
| 4.대표적인 합의알고리즘 |
| 합의 알고리즘 : 블록체인 에서는 블록을 생성하는 문제에 관하여 합의가 필요함 왜냐하면 모든 노드가 기본적으로 자신에게 유리한 블록을 생성하려는 악의적 행동을 할 가능성 존재함 그렇기 때문에 블록체인 네트워크에 가장 바람직한 블록을 생성 하려는 모든 노드들 간의 합의 알고리즘이 필요하게 됨  POW : 가장 기본적인 알고리즘으로 퍼즐을 주어 그 퍼즐을 제일 빨리 해결하는 노드에게 블록 생성 권리을 주는 알고리즘  POS : 가지고 있는 코인의 지분에 따라 블록 생성 권리율을 조정하는 알고리즘  POI : 단순히 지분 뿐만 아니라 노드의 네트워크 참여도, 신뢰도 다양한 경우를 따져서 블록생성 권리율을 조정함 |

|  |
| --- |
| 5. 현 블록체인의 문제 및 해결 방안 |
| 확장성 문제의 존재  사람이 혼자서 어떤 일을 하는 결정하기는 쉽다. 그런데 2명 3명 합의를 해야 하는 사람이 늘면 꼭 문제가 터진다. 이유는 단순하다. 모두 생각이 다르기 때문이다. 대신 혼자 한일은 번복하기도 쉽지만 이렇게 힘들게 모두가 합의한 일은 번복하기 어렵다. 왜냐하면 당신이 번복하는순간 사람들이 당신을 절대 가만 두지 않을꺼다. ^&^ 그래서 많은 사람들이 참여한 일은 신뢰를 가진다고 한다.  (위의 말을 잘 순화해서 쓰세용 ^^)  블록체인은 이렇게 노드 수가 많아지면 합의하는데 속도가 느려지고 대신 신뢰성이 증가된다.  반대로 노드수가 줄면 속도는 빨라지고 신뢰성은 줄어든다.  어떻게 둘 다 잡을 수 있을까?  그럼 답은 간단하다.  1. 믿을 있는 사람을 선출하여 대신 일을 하게 하는 것 ( ex : 국회의원? ) (DPOS 방식)  2. 다수결을 적용하는 것 ( 만장일치 하지 말고 적당히 3분의 2만 넘으면 통과 ) (PBFT 사용)  3. 일을 나누는 방법 (플라즈마와 같은 하부 체인)  4. 외주사용 (라이트닝 네트워크)  와 같은 방식을 통해 해결 할 수 있다.  또 다른 문제들  보안 문제 ( 이거 박성준 교수님이 좋아하는 문제지만 확정성만 해도 충분하다. )  입력 데이터 문제 ( 오라클 문제지만 너무 어려운 문제이므로 넘어가자) |