(AI / 빅데이터 / **블록체인**) 문제

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 윤성철,배민수, 김호영, 박수현 | | |
| 문제 1 | | | |
| 블록체인 컨센서스 알고리즘에서 PoW, PoS, DPoS 방식이 있다. 각각 방식이 무엇인지 쓰고 장단점을 설명하시오. | | | |
| 출제 키워드 | | CONSENSUS | |
| 참고 데이터  (사이트, 서적 등) | | <https://steemit.com/kr/@donekim/consensus-pow-pos-dpos> | |
| 해설 | | | |
| 블록체인 컨센서스 알고리즘은 Pow(Proof-of-work)라는 지분 증명방식과 PoS(Proof of Stake) 방식과 DPoS(Delegated Proof-of-Stake)방식이 존재한다.  PoW는 **작업증명** 으로 부르기도 하며 해시연산을 처리하는 하드웨어(GPU, ASIC채굴기) 등을 사용해서 증명하는 방식입니다. 간단하게 말해 하드웨어 장비를 사용해 코인을 채굴하는 것입니다.블록 생성 시간동안 가장 많은 해시파워를 제공한 노드가 블록을 생성할 수 있도록 설계가되어있습니다.  현재 높은 시장 가치를 형성하고 있는 주류 코인들이 채택하고있습니다.강력한 보안성을 제공하고 서비스 남용을 쉽게 방지할 수 있습니다.하지만, 높은 전력소모를 통해 자원을 낭비하며 지속적으로 해시파워를 유지해야합니다.또한 특정 마이닝 세력의 해시 독점으로 생태계 교란의 우려가 있다는 단점이 있습니다.  PoS는 **지분증명** 이라 부르기도 하며 채굴기 없이 본인이 소유한 코인의 지분으로 채굴되는 방식입니다. 위 PoW의 단점을 극복하기위해 등장하였습니다.  해시파워가 많이 필요하지 않아 경제적이며 친환경적입니다. 그리고 블록 생산자의 탈중앙화로 안정성 확보가 가능합니다. 또한, 블록을 생성하기 위해서는 지분을 담보로 잡아야 하기 때문에 덤핑 방지가 가능하다는 장점이있습니다. 하지만, 모두 이자를 받으려고 코인을 묶어놓기 때문에 시중 코인의 유통량 감소로 이어질 수 있다는 단점이있습니다. 또한 보안성에대해서도 검증이되지않앗습니다.  DPoS는 **위임지분증명** 이라 부르기도 하며 말그대로 위임된 POS입니다. PoS가 자산을 가진 사람들이 전부 참여할 수 있는 방식이라면 **DPoS는 특정 인원에게만 POS를 할 수 있도록 권한을 위임하는 것입니다.** 즉 특정인 몇 명만이 블록을 생성하여 증명할 수 있습니다.  Pos에비해 많은 트랙잭션을 빠르게 처리할 수 있고 PoW에 비해 비용이 낮습니다. 하지만 증인끼리 담합할 위험이 존재하며 공개된 소수의 증인에 대한 DDoS 공격 위험이 있습니다. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 윤성철,배민수, 김호영, 박수현 | | |
| 문제 2 | | | |
| 블록체인 P2P 기술의 장단점에대해 쓰시오. | | | |
| 출제 키워드 | | P2P | |
| 참고 데이터  (사이트, 서적 등) | | <https://needjarvis.tistory.com/237> | |
| 해설 | | | |
| 블록체인은 일명 CS구조라고 하는 Client-Server를 채택하지 않습니다. P2P 구조를 사용하고있습니다. CS구조보다 단점이 많을것 같지만 P2P는 CS에서 느낄 수 없는 자유스러움과 강력함이 있습니다. 비교하자면 검열이 강력한 iOS와 자유로운 안드로이드같은 느낌입니다. 안드로이드가 자유롭기 때문에 악성 프로그램도 많지만 iOS보다 더 많은 개발자가 참여하여 더욱 다양한 프로그램이 등장할 수 있는 것이 바로 그 사유입니다. 또 자유롭기 때문에 누구나 참여할 수 있는데 이 참여를 하는 사람들에게 보상을 주게 되면 CS보다 안정적인 서비스를 보여줄 수 있습니다.  클라이언트-서버 구조는 서버를 운영하는 사람이 존재한다면 언제 어디서든지 서비스를 이용할 수 있고 검증된 데이터를 사용할 수 있습니다. P2P같은 경우 서버의 역할을 해줄 사람이 없다면 서비스를 당연히 이용할 수 없습니다. 본인이 이용한 만큼 본인도 그 댓가를 지불하게 되는 원리기 때문에 댓가를 지불하기 싫은 사람이 많을수록 점점 서비스의 퀄리티가 죽을 수 있습니다. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 윤성철,배민수, 김호영, 박수현 | | |
| 문제 3 | | | |
| 공개키 방식을 설명하시오.(공개키로 암호화하는 경우와 개인키로 암호화하는 두가지 케이스에 대해 서술하시오.) | | | |
| 출제 키워드 | | Private Key | |
| 참고 데이터  (사이트, 서적 등) | | - <https://brunch.co.kr/@artiveloper/24>  - | |
| 해설 | | | |
| 1. 공개키로 암호화하는 경우   상대방의 공개키로 대데이터를 암호화하고 데이터를 전달하면, 데이터를 전달받은 사람은 자신의 개인키로 데이터를 복호화한다   1. 개인키로 암호화하는 경우   개인키 소유자: 캐인키로 데이터 암호화 -> 공개키와 함께 전달 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 윤성철,배민수, 김호영, 박수현 | | |
| 문제 4 | | | |
| 핫월렛과 콜드월렛의 차이를 설명하고, 비트코인 거래소 지갑과 블록체인 지갑의 차이를 서술하시오. | | | |
| 출제 키워드 | | wallet | |
| 참고 데이터  (사이트, 서적 등) | | <http://www.thebchain.co.kr/news/articleView.html?idxno=185> | |
| 해설 | | | |
| **1)핫월렛 vs 콜드월렛**  핫월렛  온라인에 연결돼 있어 바로 입출금, 송금이 가능한 암호화폐 지갑을 의미함. 언제나 연결되어있어 편리하고 빠르지만, 해킹에 취약 콜드월렛  오프라인에서 작동하는 지갑을 의미하고 콜드 월렛에는 하드웨어 지갑, USB보관, 종이 지갑 등이 있다. 콜드 월렛은 인터넷에 연결되어있지 않으므로, 해커가 그 지갑 자체를 소유하고 있지 않는 이상 해킹은 거의 불가능하다고 보면됨  다만 웰렛에 해당되는 개인 키를 잃어버렸을때에 끝이고, 복구할 방법 없음  **2) 거래소 지갑 vs 블록체인 지갑**  편 하고 심플한 서비스를 이용하고자 하는 사용자, 그리고 비트코인을 실제 돈으로 매수/매각하려는 사용자, 혹은 이를 이용해 비트코인 시세차익 투자(트레이딩)을 하려는 사용자의 경우 거래소의 지갑 서비스가 적합할 것이다. 따로 비밀키와 공개키를 적어둘 필요 없이 거래소에 일반적인 아이디와 비밀번호로 로그인하면 지갑을 이용하는 것이 가능하기 때문이다. 다만 사용자가 비밀키에 대한 권한이 없고, 각종 인증 절차와 회원가입으로 인해 비트코인 최대의 장점인 ‘익명성’이 보장되기 힘들며, 이 때문에 결국 거래소라는 제3자 집단(Third Party)이 거래 과정에 개입된다는 단점이 있다.  조 금 더 세심한 주의와 비트코인에 대한 지식을 요구하지만, 코인을 좀 더 안전하게 보관하며 최대의 익명성을 보장받고 싶은 사용자는 블록체인 지갑이 적합할 것이다. 여러가지 정보를 사용자가 책임을 지고 기록 및 관리해야 하며 한 번 잃어버린 비밀번호는 복구가 어렵다는(전적으로 불가능하진 않다) 단점이 있지만, 비트코인의 최대 장점인 익명성을 보장하며 더욱 높은 자유도와 유연성을 제공하는 서비스임에는 틀림없다. 사용자의 비밀번호조차 블록체인 서버에 저장되지 않으며 블록체인 인포 당사에서도 사용자 정보를 최소한으로 보관하는 것을 목표로 하기 때문이다. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 윤성철,배민수, 김호영, 박수현 | | |
| 문제 5 | | | |
| Solidity 의 간단한 설명과 특징을 서술하시오 | | | |
| 출제 키워드 | | Solidity | |
| 참고 데이터  (사이트, 서적 등) | | <https://krksap.tistory.com/1246> <http://wiki.hash.kr/index.php/%EC%86%94%EB%A6%AC%EB%94%94%ED%8B%B0> | |
| 해설 | | | |
| * - Solidity는 이더리움의 스마트 컨트랙트를 만들기 위한 언어이다. * - 특징   - 정적타입  - 상속, 라이브러리, 유저타입 지원  - 튜링완전 언어  - 반복문과 제어문 사용가능  - 응용 이진 인터페이스 기능 탑제  - 하나의 계약 내에서 다중 타입의 안전한 함수가 가능하게 함   * - 솔리디티 코드 문법   - 일부 함수는 숫자나, 참/거짓을 묻는 질문에 대한 값으로 값(Value)을 반환한다. 이 반환 값은 솔리디티의 자료형에 따라 결정  - 튜링완전 언어  - 어떤 프로그래밍 언어나 추상 머신이 튜링 머신과 동일한 계산 능력을 가짐을 의미  - 튜링완전언어는 프로세스를 충분히 분할할 있을 만큼 작은 단위를 사용할 수 있어야 하며 조건설정과 반복 명령어가 있어야 하는 조건이 있다..  - 스마트계약  - 계약 당사자가 사전에 협의한 내용을 미리 프로그래밍 하여 전자 계약서 문서 안에 넣어두고, 이 계약 조건이 모두 충족되면 자동으로 계약 내용이 실행되도록 하는 시스템 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 윤성철,배민수, 김호영, 박수현 | | |
| 문제 6 | | | |
| DDoS에 대해 간단히 설명하고 블록체인의 특징을 DDoS와 연관시키시오 | | | |
| 출제 키워드 | | DDoS | |
| 참고 데이터  (사이트, 서적 등) | | <https://terms.naver.com/entry.nhn?docId=3586111&cid=59277&categoryId=59283>  <https://www.blockchainhub.kr/bbs/board.php?bo_table=ryu&wr_id=603> | |
| 해설 | | | |
| - DDoS는 수십대에서 수백만대의 PC를 원격 조종하여 특정 웹사이트에 동시 접속키켜 단시간 내에 서버나 네트워크 대역이 감당할 수 없는 많은 양의 트래픽을 순간적으로 일으켜 서버를 마비시키는 크래킹 수법이다.   * - 블록 체인은 여러 노드가 있는 분산 시스템이기 때문에 DDoS의 공격자가 DNS를 성공적으로 다운시키기 위해서는 여러 노드를 동시에 액세스 해야하기 때문에 공격이 어려워지고, 시간, 비용이 소요된다. 또한 서버의 대역폭을 신속하게 보낼 수 있는 서버 네트워크를 통해 추가 대역폭을 사용해 초과 트래픽을 흡수하여 DDoS공격을 방어할 수 있다. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 배민수 | | |
| 문제 7 | | | |
| 1. 외부 소유 계정 : 스마트 컨트랙트를 갖지 않음  2. 컨트랙트 계정 : 스마트 컨트랙트를 소유하고 있는 계정  특정 기능을 수행하는 스마트 컨트랙트는 메시지 또는 트랜잭션을 통해 기능을 수행하게 됩니다.  이때 메시지와 트랜잭션의 차이점을 설명해주세요. | | | |
| 출제 키워드 | | Ethereum, Smart Contract | |
| 참고 데이터  (사이트, 서적 등) | | <https://github.com/ethereum> | |
| 해설 | | | |
| |  |  |  |  | | --- | --- | --- | --- | | **​** | **생성주체(발신자)​** | **거래내역저장여부​** | **수신자​** | | Transation​ | 외부소유계정​ | 저장​ | 컨트랙트​ | | Message​ | 컨트랙트​ | 저장안함​ | 컨트랙트​ |   메시지는 컨트랙트에서 컨트랙트를 호출하는 경우 , 컨트랙트에서 외부 소유 계정으로 이더를 전송할 때 사용되게 됩니다. 컨트랙트 수행도중 또 다른 이벤트를 처리하기 위해 사용되는 것으로 트랜잭션과는 달리 기록이 저장되지는 않습니다. 메시지는 이더리움 가상머신에서만 생성되어 이용되는 가상 객체입니다.  트랜잭션은 외부 소유 계정이 컨트랙트를 호출, 사용자간 이더리움 전송, 스마트 컨트랙트 배포와 같은 경우 사용됩니다. 외부 소유 계정이 특정 스마트 컨트랙트를 수행하기 위한 정보 및 가스, 이더와 같은 정보를 담아 컨트랙트를 수행하게 됩니다.  예를 들어 a라는 스마트 컨트랙트는 인자로 int b를 받는다고 하면 트랜잭션에는 스마트 컨트랙트의 주소, 발신자 서명, 이더양, 가스 허용치, 컨트랙트에 필요한 인자 등을 담게 됩니다.  트랜잭션    트랜잭션 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 5678조 |
| 조원 | 배민수 | | |
| 문제 8 | | | |
| 이더리움의 가스는 무분별한 evm 실행을 방지하기 위한 수수료입니다.  가스는 이더리움 화폐의 작은 단위를 나타냅니다.  같은 동작을 실행하더라도 더 많은 가스를 지불하는 사용자의 동작이 먼저  실행됩니다. 사용자는 Gas Limit라는 값을 통해 자신의 해당 동작에서 지불할  수 있는 최대값을 제안하게 됩니다. 수행 도중 가스가 모자라게 되면 지금까지  소모된 가스는 그대로 소모되고 동작은 모두 롤백 됩니다. 그렇다고 해서 남은  가스가 소멸되지는 않습니다. 남은 가스는 환불됩니다. 그런데 Gas Limit를  무작정 높게 잡는다고 해서 좋지 않습니다 이유가 무엇일까요오? | | | |
| 출제 키워드 | | Gas | |
| 참고 데이터  (사이트, 서적 등) | | <https://github.com/ethereum>  <https://simsimjae.tistory.com/229> | |
| 해설 | | | |
| 하나의 블록에는 여러 트랜잭션이 포함될 수 있습니다. 이 블록에는 트랜잭션을 담을 수 있는 한계가 있습니다. 한 블록의 Gas Limit는 670만 정도입니다. 따라서 트랜잭션의 Gas Limit가 너무 높아서 블록에 포함되지 못하게 되면 우선순위가 밀려 다음 블록에서 이를 수행해야 합니다.  만일 블록의 제한이 1000인데 자신의 트랜잭션의 제한이 900이라고 가정할 때 이미 다른 트랜잭션으로 블록 제한이 200이 잡혀있다면 이번 블록에서는 자신의 트랜잭션이 수행되지 않고 트랜잭션 pool에서 대기하며 다음 블록을 기다려야합니다.  만약 반대로 Gas Limit가 너무 낮다면 다른 트랜잭션들에게 우선순위가 밀려 채굴자(EVM을 실행시켜줄)들이 포함시키지 않게 됩니다. | | | |