(블록체인) 문제

|  |  |  |  |
| --- | --- | --- | --- |
| 지역 | 대전 | 조 | 9조 해피해킹 |
| 조원 | 김예랑, 윤현규, 윤영우, 조성원, 박신종 | | |

|  |  |
| --- | --- |
| 문제 1 | |
| 비대칭키 암호화 구조란? | |
| 출제 키워드 | PrivateKey |
| 참고 데이터  (사이트, 서적 등) | 사진 출처 : <https://preamtree.tistory.com/38> |
| 해설 | |
| 일단 디지털 서명을 설명하기 위해선 암호화 구조를 이해해야 한다.  암호화구조는 대칭키 암호화/비대칭키 암호화로 구분되는데, 디지털 서명은 비대칭키 암호화 구조로 구분된다.  먼저, 대칭키 암호화 구조는 원본 데이터를 하나의 키로 암호화 시키고, 같은 키로 복호화 시킨다는 개념이다.  ëì¹­í¤ ìí¸íì ëí ì´ë¯¸ì§ ê²ìê²°ê³¼  대칭키 암호화 구조는 비교적 간편하지만, 대칭키를 전달하는 과정에서 해킹의 위험에 노출될 수 있다.  비대칭키 구조는 대칭이 아닌 구조, 즉 하나의 키가 아닌 서로다른 두개의 키(개인키/공개키)로 암호화/복호화를 하겠다. 개인키는 개인이 혼자만 알고있는 키, 공개키는 모두가 알고있는 키다.  비대칭키 암호화 방법은 두가지가 있다.  하나는 개인키로 암호화 시키는 방법, 다른 하나는 공개키로 암호화 하는 방법이다.  디지털 서명이 전자에 해당하여, 송신자가 개인키로 암호화를 함으로써 부인방지 효과를 낼수있다..  https://t1.daumcdn.net/cfile/tistory/242B243B587B395323 | |
|  | |

|  |  |
| --- | --- |
| 문제 2 | |
| HyperLedger Fabric 의 구조를 그려보시오.. | |
| 출제 키워드 | HyperLedger Fabric |
| 참고 데이터  (사이트, 서적 등) | <https://cyberx.tistory.com/187> |
| 해설 | |
| HyperLedger Fabric 이란 ?  Hyperledger 프로젝트의 창립 멤버 중 한 명인 IBM이 44,000 줄의 블록체인 코드를 Hyperledger Fabric에 기부하게 되면서 프로젝트화가 진행되게 되었습니다. Fabric은 Hyperledger 프로젝트의 핵심 프로젝트로 블록체인의 런타임을 구현하는 프로젝트로 블록체인을 이용한 기반 기술에 대한 내용이 포함되어 있습니다.  Hyperledger Fabric은 모듈형 아키텍처 기반의 블록체인 애플리케이션 또는 솔루션 개발을 위한 근간으로 고안된 비즈니스 블록체인 프레임워크로서 리눅스 재단이 주도하고 있습니다. Hyperledger Fabric은 합의, 멤버십 서비스 등 구성요소의 플러그 앤 플레이를 지원합니다.  Fabric의 특징    HyperLedger 구조  https://t1.daumcdn.net/cfile/tistory/993AAB355AFBD2AB0A  **Membership(MSP : Membership Service Provider)**  Fabric은 참여 권한이 있는 유저들만이 사용 참여 할 수 있는 폐쇄형 구조입니다. 그래서 유저들이Fabric 즉 원장(Ledger)에 데이터를 기록, 수정, 삭제 등의 처리를 하기 위해서 인증서가 필요로 하며 인증서를 발급 받기 위한 기능이 필요합니다. 이 인증서를 등록 및 발급 관리 해주는 작업을 하는 것이Membership 입니다. 이렇게 생성된 인증서를 통해 트랜잭션을 인정하고 Peer는 이 인증서를 사용하여 트랜잭션의 결과를 인증합니다.  **Blockchain**  Blockchain은 프라이빗 블록체인의 기본 구성요소로 블록체인에 저장하기 위한 데이터를 관리하는 분산원장 데이터베이스며, 이를 관리 및 처리하기 위한 기능으로 구성되어 있습니다. 블록체인 서비스는HTTP/2 표준을 기반으로 P2P 프로토콜을 통해서 분산원장을 관리합니다. 데이터 구조는 해시 알고리즘을 통해 World state를 복제하는 등 관리 하는데 가장 효율적으로 관리할 수 있도록 최적화되어 있습니다. 필요에 따라 다른 합의 알고리즘 플러그인(PBFT, Raft, PoW, PoS)을 연결하고 구성 할 수 있습니다.  **Transaction**  프라이빗 블록체인에서 서비스나 처리에서 생성되는 트랜잭션을 관리하는 기능입니다. 거래에서는 트랜잭션을 처리하는 부분을 기초로 구성되어 있습니다. 보증 피어 기능이라는 'Endorsement Validation'과 트랜잭션을 배치 처리하고 블록을 생성해 프라이빗 블록체인망에 참여하고 있는 모든 노드들에 분기 및 정렬 역할을 하는 오더링(Ordering) 서비스가 있습니다.  **Chaincode**  Chaincode는 Fabric에서 말하는 스마트 컨트랙트를 말하는 것으로 프라이빗 블록체인에서 중요한 기능입니다. Chaincode는 기업 및 컨소시엄으로 구성된 서비스에 맞게 블록체인을 활용할 수 있도록 로직을 구현, 변경 할 수 있으며 로직을 개발할 수 있도록 'Go', 'Node.js', 자바와 같은 언어로 개발을 할 수 있도록 지원하고 있습니다. Chaincode는 수신 된 트랜잭션에 대한 응답으로 메소드가 호출 되는 방식으로 되어있습니다. 즉 트랜잭션이 생성되어 전송될 때 마다 Chaincode 내에 정의되어있는 메소드가 실행되는 구조로 되어있습니다.  Fabric v1.0 구조  https://t1.daumcdn.net/cfile/tistory/994925335AFBD52014  위의 그림은 Fabric의 구조를 간략하게 나타낸 것입니다. 위의 구조에 대해 간략하게 설명하면 다음과 같습니다.  1.     MSP(Membership Service Provider)에 해당 Application이 Fabric을 사용할 수 있도록 인증서 등록을 하는 작업을 진행합니다. (0번)  2.     Fabric을 이용 시 Application이 블록체인에 트랜잭션 수행을 위한 Proposal을 합니다. (1번)  3.     Proposal은 Peer에서 수행됩니다. Endorser들은 Poroposal을 받은 뒤 내부 처리를 통해 서명을 한 뒤 Proposal response를 Application에게 보냅니다.  4.     서명된 proposal response를 받은 Application은 트랜잭션을 수행합니다. (2번)  5.     Peer에 있는 체인코드를 통해 필요한 처리를 진행합니다.  6.     처리를 진행 후 트랜잭션은 모든 채널에 대해서 Orderer가 받아서 트랜잭션의 순서대로 정렬을 합니다. (3번)  7.     이렇게 정렬 및 처리가 된 내용을 다시 Peer들에게 일괄적으로 전송을 하게 됩니다.    위의 흐름에서 Endorser는 보증된 트랜잭션을 처리하도록 하는 역할을 하게 되며, 오더링 서비스는 합의 알고리즘을 수행합니다.  추가적으로 Fabric에서는 채널이라는 것이 있는데 채널은 실제 Chaincode가 디플로이되고 트랜잭션이 실행되는 구간을 말합니다. 즉 아래와 같이 두개의 채널(파란선, 붉은선) 각각 다른 비즈니스 로직을 담고 있는 Chaincode가 실행되며, 채널이 생성될 때 해당하는 Peer를 지정할 수 있습니다. 예를 들어 아래의 붉은선을 보게 되면 모든 Peer에 사용되는 것이 아닌 지정된 Peer(1, 2, 3, 6, 8, 11)에만 실행이 되는 것을 볼 수 있습니다. 이처럼 채널이라는 개념을 통해 비즈니스적인 확장성을 제공해 줄 수 있으리라고 판단됩니다. | |

|  |  |
| --- | --- |
| 문제 3 | |
| 기또리의 비트코인 보유량은 0BTC 입니다. 잘생긴조성원이 기또리에게 5BTC을 입금하고 구현짱이 기또리에게 3BTC을 입금하였습니다. 그 후 기또리는 구현짱에게 3BTC을 입금하였습니다. 현재 기또리의 UTXO 총합을 구하세요. | |
| 출제 키워드 | UTXO |
| 참고 데이터  (사이트, 서적 등) | <https://steemit.com/kr/@yahweh87/16-utxo-5-5> |
| 해설 | |
| UTXO === Unspent Transaction Output (소비되지 않은 거래 출력 값)  잘생긴조성원이 기또리에게 5BTC을 입금 > 기또리 : 새 UTXO(5BTC)생성  구현짱이 기또리에게 3BTC을 입금 > 기또리 : 새 UTXO(3BTC)생성  현재 기또리의 UTXO 총합 : 8BTC  기또리가 구현짱에게 3BTC을 입금  > 구현짱이 기또리에게 3BTC을 보낸 입금 기록이 소비됨 > 기또리 : UTXO(3BTC)소멸  > 기또리가 구현짱에게 3BTC을 입금 > 구현짱 : 새 UTXO(3BTC)생성  > 기또리가 기또리에게 5BTC을 입금 > 기또리 : 새 UTXO(5BTC)생성  현재 기또리의 UTXO 총합 : 5BTC | |

|  |  |
| --- | --- |
| 문제 4 | |
| Oracle 종류 다섯가지와 각각의 의미를 설명하세요. | |
| 출제 키워드 | Oracle Problem |
| 참고 데이터  (사이트, 서적 등) | <https://medium.com/theblocksmith/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-oracle-problem-47ef60718d2f> |
| 해설 | |
| Oracle 종류  [Software Oracle] 온라인에서 사용 가능한 데이터를 가지고 오는 것. (온도, 상품 및 물품 가격, 비행 또는 기차 지연 등)  [Hardware Oracle] 물리적 센서를 통한 데이터를 가지고 오는 것. (‘냉장고가 비어있다.’, ‘누군가 내 문앞에 서있다.’ 등)  [Inbound Oracle] 외부세계에서 블록체인 상에 데이터를 전송하는 것 (현재 환율은 1,100원 이다. 물건을 구매 한다.)  [Outbound Oracle] 블록체인 상의 데이터를 외부 세계에 전송하는 것. (송금이 되었다! 물건을 넘겨라.)  [Consensus Based Oracle] Augur와 Gnosis와 같은 미래 예측 시장 플랫폼 블록체인에서 데이터를 받아오는 것 | |

|  |  |
| --- | --- |
| 문제 5 | |
| DDos 공격은 공격 대상인 OSI 모델의 계층에 따라 분리 되는데  DDos 공격이 가장 많은 계층 3, 4, 6, 7의 계층이름을 작성하시오. | |
| 출제 키워드 | DDos |
| 참고 데이터  (사이트, 서적 등) | <https://aws.amazon.com/ko/shield/ddos-attack-protection/> |
| 해설 | |
| 3네트워크, 4전송, 6프레젠테이션, 7애플리케이션 | |

|  |  |
| --- | --- |
| 문제 6 | |
| P2P 의 풀 네임을 적고, P2P의 특징을 적으시오. | |
| 출제 키워드 | P2P |
| 참고 데이터  (사이트, 서적 등) | 위키 |
| 해설 | |
| P2P는 Peer to Peer 의 줄임말로 컴퓨터의 쌍방향 파일 전송 시스템을 가리킨다.  중앙서버 없이 컴퓨터와 컴퓨터를 연결해 주며, 프로그램 엔진만 만들면 되기 때문에 매우 간편하게 파일을 전송 할 수 있는 장점이 있다.  P2P의 가장 큰 특징은 사용자 컴퓨터의 자원을 어느 정도 나눠서 쓰기 때문에  서버 성능의 한계를 극복할 수 있다. 대단히 유용한 기술이다. | |

|  |  |
| --- | --- |
| 문제 7 | |
| ‘확장성’ 은 블록체인 응용 프로그램의 실현에 큰 문제가 되고 있다. 기존 네트워크 구조는 더 많은 서버를 추가하거나 서버의 CPU나 메모리를 교체함에 따라 이러한 문제를 해결할 수 있으나 블록체인은 그렇지 못하다. 그 이유는 무엇인가? | |
| 출제 키워드 | scale |
| 참고 데이터  (사이트, 서적 등) | <https://brunch.co.kr/@curg/3>  [http://wiki.hash.kr/index.php/%ED%99%95%EC%9E%A5%EC%84%B1#cite\_note-1](http://wiki.hash.kr/index.php/%25ED%2599%2595%25EC%259E%25A5%25EC%2584%25B1#cite_note-1)  [https://medium.com/decipher-media/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%ED%99%95%EC%9E%A5%EC%84%B1-%EC%86%94%EB%A3%A8%EC%85%98-%EC%8B%9C%EB%A6%AC%EC%A6%88-3-2-relayer-1efdef52b16b](https://medium.com/decipher-media/%25EB%25B8%2594%25EB%25A1%259D%25EC%25B2%25B4%25EC%259D%25B8-%25ED%2599%2595%25EC%259E%25A5%25EC%2584%25B1-%25EC%2586%2594%25EB%25A3%25A8%25EC%2585%2598-%25EC%258B%259C%25EB%25A6%25AC%25EC%25A6%2588-3-2-relayer-1efdef52b16b) |
| 해설 | |
| 블록체인은 분산 원장 기술을 이용해서 모든 노드가 똑같은 정보를 처리하고 저장하기 때문에 네트워크에 노드 수를 늘린다고 해서 네트워크 처리 성능이 올라가지 않는다. 오히려 노드 수가 증가하면 트랜잭션이 발생할 확률이 더 커지기 때문에 네트워크 속도가 더 느려질 수 있다. 왜냐하면, 네트워크에 참여하는 노드들은 네트워크를 유지하는 보상으로 디지털 자산인 코인을 받으므로 이것을 다른 곳으로 이동시키는 트랜잭션을 발생시킬 확률이 발생하기 때문이다. 즉, 블록체인에서는 전통적인 서버 아키텍처 방식의 최적화 기법을 그대로 적용하기 어렵다. | |

|  |  |
| --- | --- |
| 문제 9 | |
| Consensus의 각 설명을 보고 해당하는 종류를 쓰시오.   1. 가장 먼저 나온 Consensus 알고리즘이며 블록 생성 시간동안 가장 많은 해시파워를 제공한 노드가 블록을 생성할 수 있도록 설계된 알고리즘 2. 코인을 보유한 지분율에 따라 새롭게 생성하는 코인을 분배받는 방식의 Consensus 알고리즘. 일정 수 이상의 코인을 보관하고 있는 지급을 블록체인 네트워크에 연결하면 보상을 받을 수 있다. 3. 네트워크의 모든 노드의 투표 결과로 선출한 상위 노드에게 권한을 위임하여 합의 하도록 하는 알고리즘. 일정 수의 증인들은 모든 권한을 위임 받아 블록 생성을 담당한다. | |
| 출제 키워드 | Consensus |
| 참고 데이터  (사이트, 서적 등) | <https://steemit.com/kr/@donekim/consensus-pow-pos-dpos> |
| 해설 | |
| Consensus 란?  블록체인의 데이터는 전 세계에 흩어져 있는 수많은 노드에 보관이 되고 각각의 노드들은 블록에 기록하는 데이터가 위변조되지 않은 것이라는 상호간 합의가 필요합니다. 이에 악의적인 상황이 발생하더라도 네트워크를 올바른 방향으로 이끌고자하는 다수의 노드들이 상호 검증을 거쳐 올바른 블록생성을 이끌어내는 프로세스와 알고리즘을 바로 Consensus(합의) 라고 합니다.   1. **Pow(Proof-of-Work) 작업증명**   최초의 블록체인인 비트코인을 창시한 사토시 나카모토가 제안한 Consensus입니다. 작업증명 방식으로도 불리고 블록 생성 시간동안 가장 많은 해시파워를 제공한 노드가 블록을 생성할 수 있도록 설계가 되어있습니다. 컴퓨팅 파워를 통해 블록체인 네트워크에 전송된 암호화된 거래정보를 푼 뒤, 새로운 블록을 체인에 연결하는 작업을 하는 것을 의미합니다.   1. **PoS(Proof-of-Stake) 지분증명**   PoS는 코인을 보유한 지분율에 따라 새롭게 생성하는 코인을 분배받는 방식의 컨센서스 알고리즘입니다. 영문 뜻 그대로 **"지분증명"**방식으로 불립니다. PoW와는 다르게 **일정 수 이상의 코인을 보관하고 있는 지갑을 블록체인 네트워크에 연결시켜 놓기만 하면 보상**을 받을 수 있습니다. 보상의 경우, PoW와 마찬가지로 블록이 생성될 때 보상이 지급되는데 차이점은 **이자와 같은 방식으로 코인이 지급된다는 것이 차이점**입니다.   1. **DPoS(Delegated Proof-of-Stake) 위임된 지분증명**   DPoS는 PoS 컨센서스 알고리즘을 변형한 형태로 위임된 지분증명 방식을 말합니다. 모든 노드의 자격을 가진 주주들이 블록생성에 참여하는 방식(PoS방식) 대신에 네트워크의 모든 노드의 투표 결과로 선출한 상위 노드(이를 증인\* 또는 Witness라고 일컫습니다.)에게 권한을 위임하여 합의하도록 하는 방식입니다. 일정 수의 증인들은 모든 권한을 위임 받아 블록 생성을 담당합니다. PoS방식이 직접민주주의 방식이라면, DPoS는 간접민주주의 방식이라고 할 수 있습니다. | |

|  |  |
| --- | --- |
| 문제 10 | |
| 1. Solidity가 돌아가는 가상 머신은? 2. Solidity에서 계약 선언을 하는 키워드는? 3. 트랜젝션 생성 과정에서 각각의 트랜젝션는 일정한 양의 OOO를 소모. | |
| 출제 키워드 | Solidity |
| 참고 데이터  (사이트, 서적 등) | <https://ggs134.gitbooks.io/solidityguide/content/chapter1.html> |
| 해설 | |
| 1) EVM(Ethereum Virtual Machine)  2) contract  3) GAS  <https://ggs134.gitbooks.io/solidityguide/content/chapter1.html> 참고.. | |