**2018-1 캡스톤 디자인**

**<프로젝트 제안서>**



**Professor: 권영빈 교수님**

**Team Name: Bourgeois**

**20155303 김준희**

**20151773 이민수**

**20154983 장건희**

1. **About team**Team Name: Bourgeois

Members : 김준희(20155303), 이민수(20151773), 장건희(20154983)

1. **Project subject**블록체인을 이용한 다이아몬드 데이터 관리
2. **Project Introduction**
   1. **개발 배경**

현재 다이아몬드는 보석 감정서에 의존하여 거래되므로 다이아몬드가 가지는 가치에 비해 그 거래의 신뢰도는 굉장히 낮다. 주로 보석 감정서에는 4C라고 불리는 중량, 커팅, 컬러, 투명도에 대한 정보가 들어간다. 게다가 소비자들이 일반적으로 사용하는 감정서 이외에 감정사가 감정한 내용에는 40여가지가 넘는 정보가 포함된다. 이 많은 정보를 종이에 모두 기록할 수 없을 뿐더러, 보증서에는 분실, 변조 등의 위험이 도사리고 있다. 또한, 단순히 감정만으로 해당 다이아의 도난 여부 등을 판단하기 불가능하다. 초고가를 자랑하는 다이아몬드 거래의 신뢰성을 높이기 위해 블록체인 기술을 적용하여 다이아에 대한 정보를 안전한 디지털 데이터로 보관하고 관리하는 시스템을 개발하고자 한다.

* 1. **프로젝트 소개**

거래시 다이아몬드 제품의 신뢰성을 보장해주기 위해 인증된 여러 기관에서의 감정서와 현재 소유권자, 도난여부 등을 데이터로 한 블록체인을 만든다. ~~각 다이아몬드를 가리키는 고유값은 해당 다이아의 감정서를 기반으로 한 해쉬코드를 이용하도록 한다.~~ 블록체인은 데이터를 한 곳에 집중하지 않고 분산저장한다. 블록들이 모든 참여자에게 공유되는 특성상 위조가 불가능하며, 실시간으로 도난여부를 파악할 수 있기 때문에 신뢰성이 보장된 거래를 진행할 수 있다. ~~감정원 등 인증된 기관은 다이아의 감정과 거래를 주관한다.~~ 감정원은 다이아몬드의 감정과 거래를 주관한다. 블록체인 네트워크에서 트랙잭션을 생성하고 블록을 만드는 역할을 한다. 판매소는 오직 다이아모든의 거래만을 주관하는 곳으로, 블록체인 네트워크에서 트랜잭션 생성만 가능하다. 소비자는 이 기관을 통해 다이아몬드의 감정서를 조회할 수 있다. 또, 거래가 이루어지기 전에 블록에 저장된 데이터를 조회하여 거래하고자 하는 다이아몬드가 도난당한 것인지 확인할 수도 있다.

1. **Project Goals** 블록체인 기술을 이용하여 저장된 정보들은 다이아몬드 거래 시 정보의 열람이 가능하다. 구매자의 경우 블록체인 기술로 신뢰성이 보장된 거래를 할 수 있다는 장점을 지닌다. 따라서, 이 프로젝트의 최종 목표는 다이아몬드에 대한 모든 정보를 블록체인 기술로 구현하여 데이터의 위조, 변조를 방지할 수 있는 시스템을 만드는 것이다. 다이아몬드에 대한 감정 정보는 지속적으로 업데이트 될 수 있으며, 누적된 감정 정보들은 조회가 가능하다. 또한 다이아에 대한 소유권 정보도 블록에 포함되기 때문에, 해당 제품의 귀속 여부도 쉽게 확인이 가능하고 이 또한 업데이트가 가능하다. 감정원은 감정 내역을 표준화하여 관리할 수 있고 판매소는 거래 신뢰성을 높일 수 있다.
2. **Project Outline**
   1. **~~Server~~**

~~- MySQL Database Server~~

~~- Google Cloud Platform~~

* 1. **BlockChain System**

- GoLand

- Hyperledger Fabric 1.1 (Open Source)

* 1. **Client Application**

- JAVA SDK

- Intelli J IDEA

* 1. **Sharing Tool**

- Slack

- Github

* 1. **Development Process**

- Pair Programming : Blockchain 구현에 있어 Pair Programming을 적용하여 처음 학습하여 개발하는 Blockchain의 결함을 감소시키고자 한다.

1. **Program Scenario**

**1) 소비자 입장**

- ~~소비자끼리의~~ 판매소에서 거래 : 매물을 가지고 다이아를 취급하는 ~~상점~~판매소에서 다이아몬드에 대한 정보를 확인 후 소비자 간의 거래가 진행된다. 이 때, 소유권이 바뀌었다는 트랜잭션이 추가된다.

- ~~상점에서의 구매~~ 감정원에서 거래 : 블록을 통해 다이아에 대한 정보를 열람할 수 있으며, 비교 대조하여 상품을 구매한 후 소유권을 등록할 수 있다.

**2) 상점 입장**

- 소비자 구매시 : 소비자가 구매 시 소유권 변경 정보를 트랜잭션에 추가한다.

- 도난 다이아 확인 : 소비자가 현물 거래하거나 매물을 팔러 왔을 때 블록과 감정서를 비교함으로써 도난 상태인지 소유권이 일치하는지 확인할 수 있다.

**3) 서비스 제공자 입장**

- 엄격하고 공증되어 있는 기관들을 통해 감정 후 새로운 다이아를 등록할 수 있다.

**4) 블록체인 시스템 입장**

- 거래가 발생하면 현재 리더 노드에게 트랜잭션을 전송한다. 리더 노드는 모든 노드에게 트랜잭션을 브로드 캐스트하고, 이것을 받은 노드는 트랜잭션의 유효성을 검증한다. 검증이 완료되면 리더 노드에게 수신 완료 메시지를 전송한다. 과반수의 노드가 메시지를 보내면 리더 노드는 블록에 트랜잭션을 추가한다.

1. **Team Roles**

|  |  |
| --- | --- |
| **Name** | **Part** |
| 김준희 | ~~Blockchain (structure, node)~~  Blockchain (structure, transaction) |
| 이민수 | ~~Blockchain (structure), Database~~  Blockchain (structure, PBFT algorithm) |
| 장건희 | ~~Server, Client Application~~  Client Application |

1. **Schedule**

|  |  |
| --- | --- |
| **Week** | **To Do** |
| 1 | 프로젝트 주제 선정 |
| 2 | 프로젝트 제안 및 설계 |
| 3 | 프로젝트 설계 및 개발 환경 세팅, Blockchain 공부 |
| 4 | 프로그램 구조 디자인, Blockchain 공부 |
| 5 | ~~김준희 & 이민수: Blockchain 구조체 정의~~ ~~장건희: 서버 세팅~~  김준희: Hyperledger Fabric Data & Transaction 분석  이민수: Hyperledger Fabric System 분석, 개발 환경 추가 세팅  장건희: Hyperledger Fabric Network 분석 |
| 6 | ~~김준희 & 이민수: Block 생성, Transaction 생성 장건희: JSON I/O Setting~~  김준희: Chaincode 분석 및 Sample Demo 구현  이민수: Chaincode 분석 및 Sample Demo 시각화  장건희: Client Application 개발 (1) |
| 7 | ~~김준희 & 이민수: Block 생성, Transaction 생성 장건희: Blockchain 버그 리포팅~~  김준희: Transaction & Block 생성 구현 (1)  이민수: Transaction & Block 생성 구현 (1)  장건희: Client Application 개발 (2) |
| 8 | 중간고사 |
| 9 | ~~김준희 & 이민수: Node 생성 및 구현 장건희: Blockchain 서버 연결~~  김준희: Transaction & Block 생성 구현 (2)  이민수: Transaction & Block 생성 구현 (2)  장건희: Rest API 연동 |
| 10 | ~~김준희 & 이민수: Node 생성 및 구현 장건희: Blockchain 서버 연결~~  김준희: Blockchain Network 연결  이민수: 트랜잭션 & 블럭 유효성 검사  장건희: Transaction List 인터페이스 구현 |
| 11 | ~~김준희: Node 생성 및 구현~~  ~~이민수: 다이아몬드 정보 수집 및 Database 입력~~  ~~장건희: 클라이언트 프로그램 구현~~  김준희: PBFT 알고리즘 구현 (1)  이민수: PBFT 알고리즘 구현 (1)  장건희: 다이아몬드 정보 수집 및 Database 입력 |
| 12 | ~~김준희: Blockchain 버그 리포팅~~  ~~이민수: Blockchain Database 연결 장건희: 클라이언트 프로그램 구현~~  김준희: PBFT 알고리즘 구현 (2)  이민수: PBFT 알고리즘 구현 (2)  장건희: System과 Application 연결 및 점검 |
| 13 | 프로그램 테스트 및 피드백, 오류 수정 |
| 14 | 데모 시나리오 준비 및 보고서/메뉴얼 작성 |
| 15 | 최종 데모 |
| 16 | 기말고사 |