**소프트웨어융합프로젝트**

중간고사

1 - J

차민재

2021. 04. 20.

**A. 제안 단계**

**1. 프로젝트 제안**

본 프로젝트는 CCTV의 스냅샷을 촬영해 블록 체인에 저장하여 데이터 유실 및 위조와 변조를 막을 수 있는 프로세스를 제안한다.

**2. 프로젝트 개요**

범죄 발생 시 수사에 사용되는 CCTV나 일반적인 방범용으로 제작된 CCTV는 데이터 저장 한계가 정해져 있고, 중앙화 된 저장소에 저장되기 때문에 데이터 유실 문제에 취약점이 노출되어 있다. 따라서 이러한 취약점을 보완하기 위해 새로운 유형의 CCTV 데이터 저장 방식이 필요하다.

**3. 프로젝트 목적**

현재 중앙 집중화 된 저장 방식을 탈피해 CCTV 스냅샷 저장 방식을 분산 저장하여 데이터의 유출 및 위,변조를 막고 무결성과 신뢰성을 확보한다.

**4. 프로젝트 기능**

블록 체인 내에 현재 실시간으로 촬영 중인 CCTV의 스냅샷을 주기적으로 저장하고, 텔레그램을 통해 사용자의 명령어 입력 시 기간 별, 개수 별로 블록 내에 저장되어 있는 이미지를 전송한다.

**5. 프로젝트 기대효과**

중앙화 되어 있지 않은 블록에 데이터를 저장하여 위조, 변조, 해킹과 같은 데이터의 무결성을 해칠 수 있는 위협에서 벗어날 수 있고, 이로 하여금 사용자에게 신뢰성을 얻을 수 있다.

**B. 분석 단계**

**1. 데이터 분석**

체인 내에 저장되는 데이터는 스트리밍 중인 연속된 데이터가 아닌 실시간으로 녹화 중인 CCTV의 화면을 캡쳐 한 정적 데이터이다.

**2. 기능 정의**

**1) 데이터 저장**

데이터베이스를 통한 스냅샷 저장이 아닌, 블록 체인 내의 트랜잭션에 캡쳐 된 이미지를 저장한다.

**2) 명령어**

소셜 미디어인 ‘텔레그램’과 블록 체인을 연결하여, 텔레그램 내의 봇(Bot)에 사용자가 명령어를 입력 시 기간, 개수 별로 블록에 저장된 이미지를 반환한다.

**3. AS-IS 정의**

CCTV 영상 데이터의 저장 방식과 활용은 모두 중앙 집중형으로 설계 된 데이터베이스를 통해 이루어진다. 따라서 데이터의 신뢰성과 무결성을 결정짓는 것은 데이터가 저장되어 있는 저장소의 성능에 맡겨진다. 이런 중앙 집중화 형태의 저장소의 문제점은 외부에서의 침입으로부터 매우 취약하다는 것이다.

만약 데이터베이스가 해킹을 당하거나 물리적인 충격을 받게 된다면 저장되어 있는 데이터는 손실될 가능성이 매우 크다.

**C. 설계 단계**

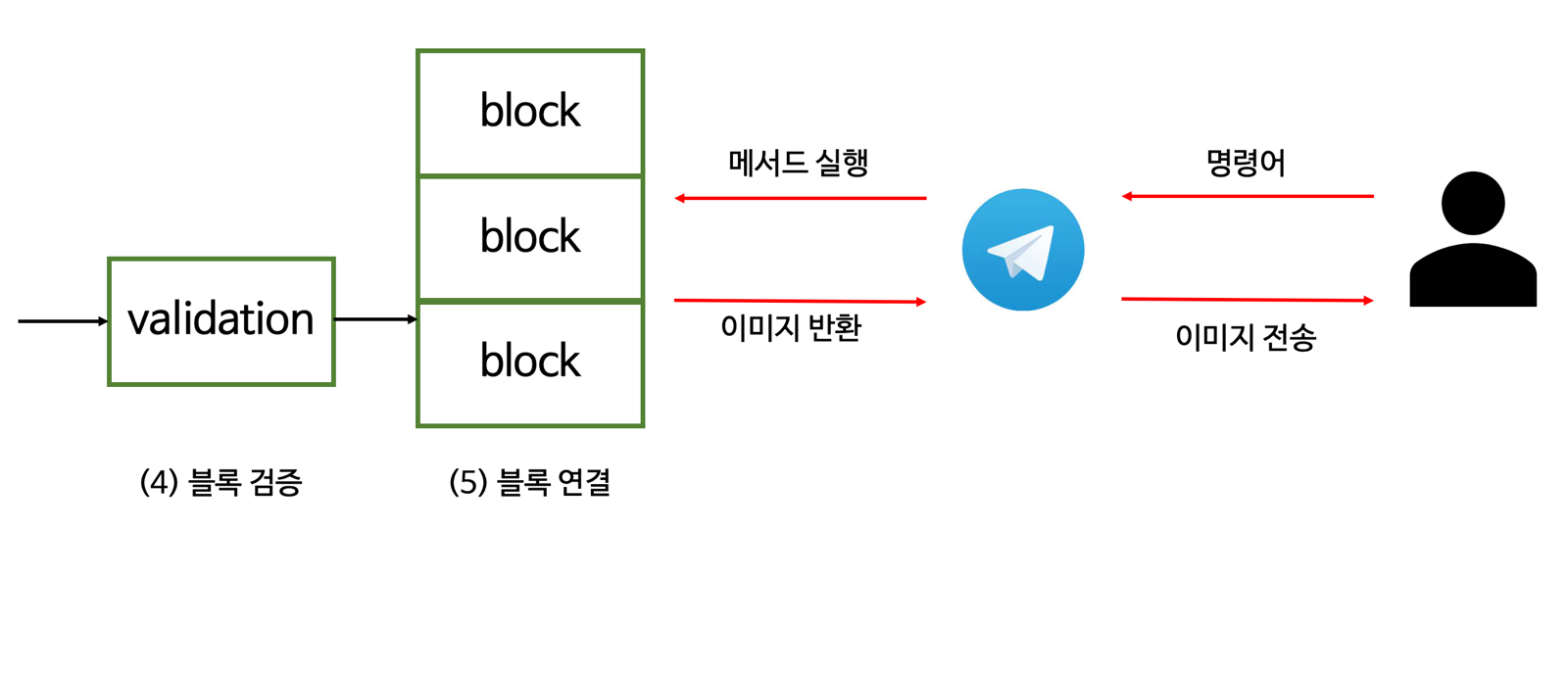
**1. 화면 설계**

텍스트, 전자기기, 스크린샷, 디스플레이이(가) 표시된 사진

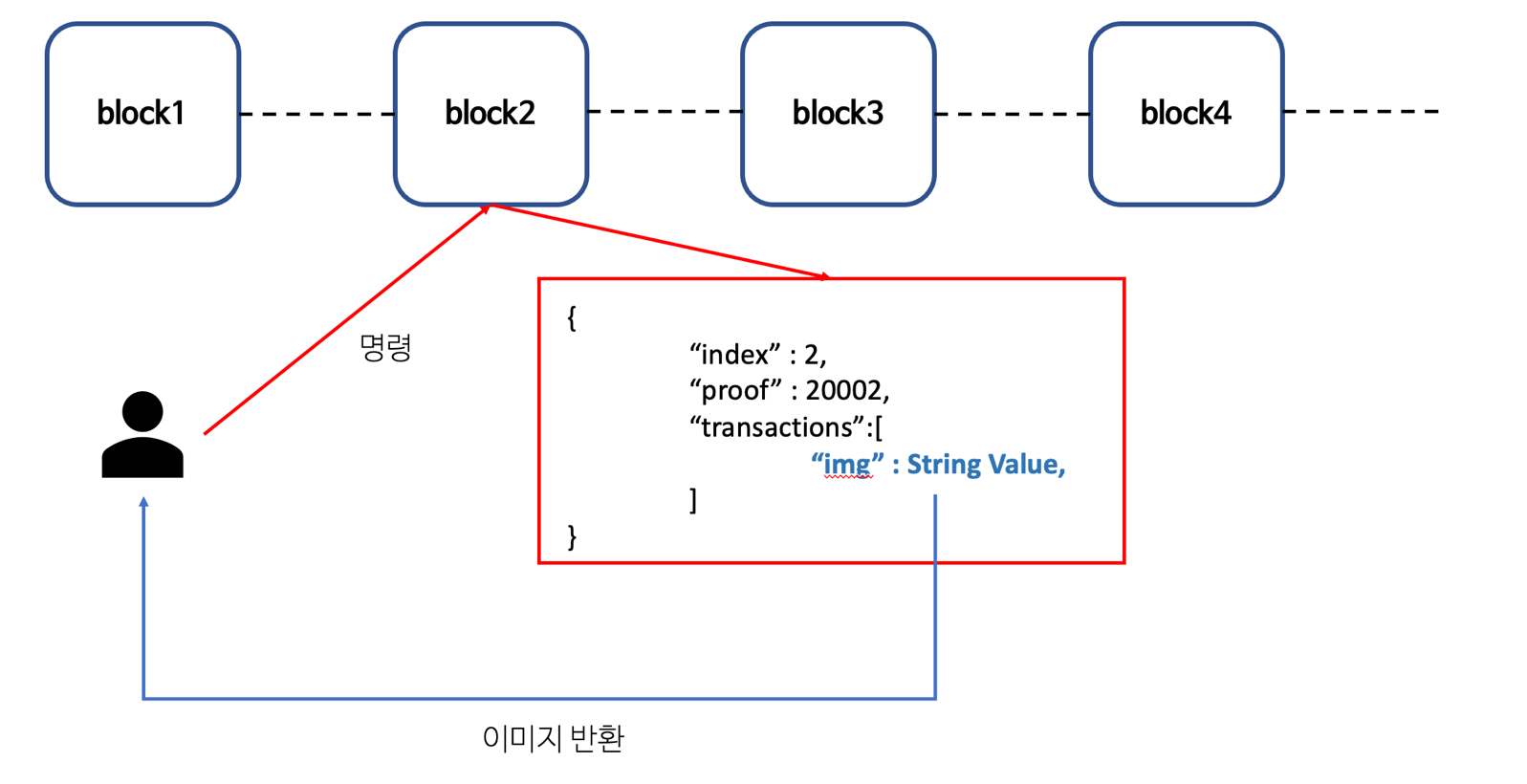
자동 생성된 설명

좌측에는 블록 체인의 상태를 보여주는 커맨드와, 우측에는 사용자가 명령어를 입력할 수 있는 텔레그램을 배치한다.

**2. Diagram**



1) 블록 체인에서 이미지를 요청



2) 블록에 접근하여 이미지 파일을 반환 받기

**3. To-Be 프로세스**

CCTV 스냅샷을 블록 체인 기반의 탈 중앙화 된 저장소에 저장하여 노드 간 합의를 통해 데이터의 무결성을 유지한다.

만약 어느 한 노드가 해킹이 되어도 블록 체인 내에 설정 된 검증 방식을 통해 해시 값을 비교하여 변조 된 데이터는 파기된다. 따라서 CCTV의 스냅샷을 반환 받는 사용자로 하여금 신뢰성을 가질 수 있게 할 수 있다.