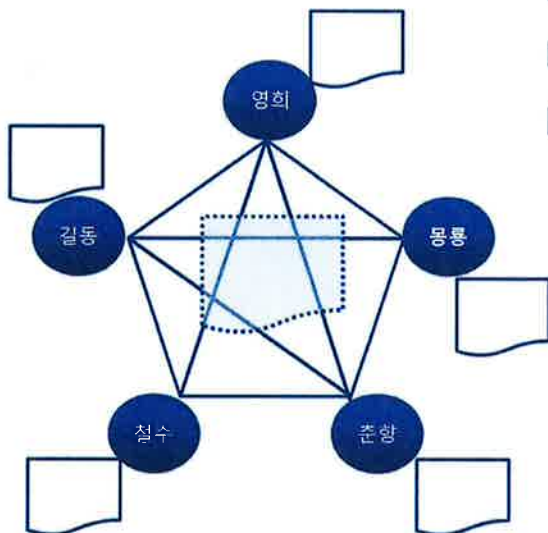


기록관리연구세미나 토론문

2019. 07. 24

오 경 희
khoh@tcaservices.kr

분산원장

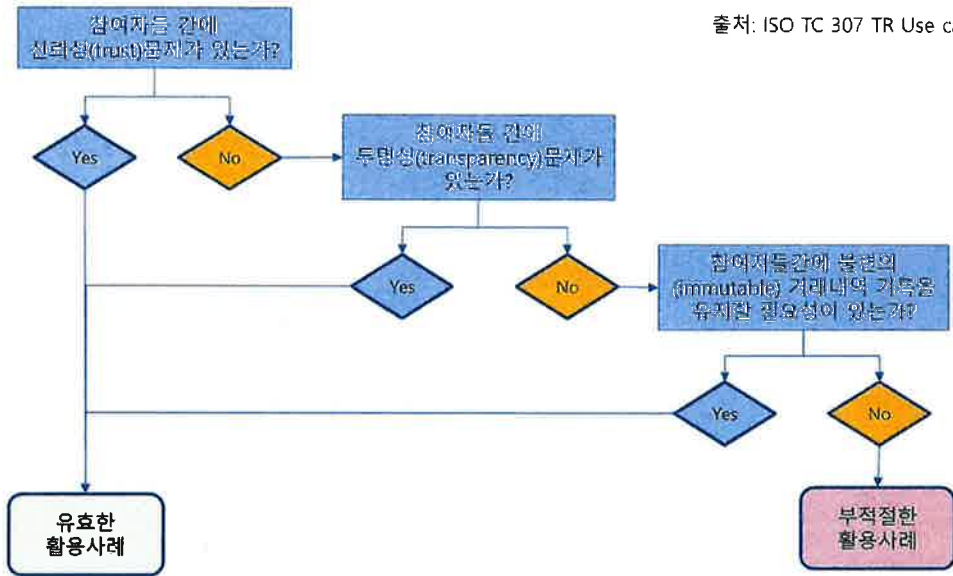


- 각자의-공통의 원장
- 복제 및 공동 생성
- 원장 대한 신뢰
 - 암호 알고리즘에 의한 보호
 - 분산 검증

“Trustless”

활용사례 평가 기준

■ 블록체인 구축 비용을 투자할 가치가 있는가?



기록의 무결성과 아카이브의 신뢰성

- 분산원장에 포함된 기록은 포함된 이후 변경되지 않는다고 믿어진다 – 그러나 포함되는 시점에서?
- 블록체인에 기록을 포함시키는 사람을 얼마나 믿을 것인가? – “아카이브의 명성과 권위”
 - 아카이브에 저장된 기록이 변경되지 않았다는 것을 믿기 위해 아카이브의 명성과 권위에 의존하는가?
 - 또는 저장된 기록의 가치에 대해 아카이브의 명성과 권위에 의존하는가?
- “비트코인과 달리 참여기관의 신뢰가 중요한 선정 이유”

블록체인 기록과 포맷 변환

- 파일 포맷이 변하면 파일 해쉬도 변한다
 - 복사본의 동일성/ 복제본의 진본성
- 블록체인에 저장되는 트랜잭션은 어떤 정보를 포함할 것인가?
 - 문서의 해시, 문서 메타데이터
 - 문서 원본 파일? (노드 간 공유?)
- 각 노드는 트랜잭션의 어떤 정보를 검증할 것인가?
 - 전자서명과 소유자 권한
 - 문서의 진본성???
 - 합의 알고리즘?

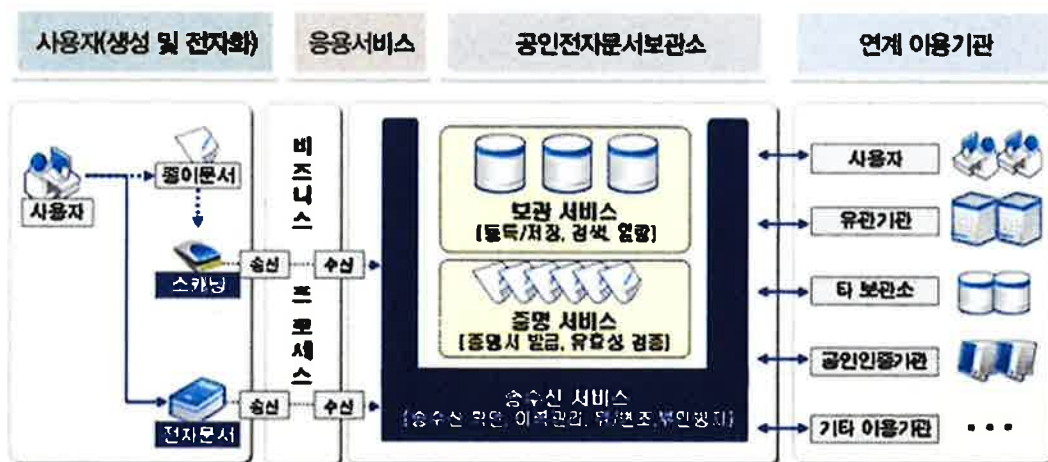
가능성은 보장되지 않는다

- 인증서 만료 문제
- 인증서는 블록체인에 보관되지만 부동산과 그림은 블록체인에 보관되지 않음
 - 부동산의 소유권 이전 기록은 확인 가능
 - 최초의 소유권 등록에는 신뢰할 수 있는 검증자가 필요
 - 이후의 소유권 이전은 제3자 개입 없이 전자서명으로 가능
 - 문서에 기록된 부동산과 현실 세계의 부동산의 일치성?
 - 인증서는 변조되지 않았지만 (디지털 파일이 아닌) 그림은 변조될 수 있음
- 진본 인증서의 블록체인 유지로 기록변경 확인
 - 사용자가 블록체인에 물어보아야만 함
 - 현재의 인터넷 발급 민원서류 역시 동일한 문제 보유

국가기록원 목표 시스템

- 4개 노드
 - 국가기록원, 행정안전부, 경남기록원, 경상남도
- 이들 간에 신뢰 이슈가 있는가?
 - 국가기록원과 행정안전부 간에 기록의 불일치 이슈
- 이들 간에 공통의 기록에 대한 요구가 있는가?
 - 경남기록원과 경상남도가 동일한 기록을 보유해야 할 필요성
- 위험관리 원칙:
 - 위험 = 사고 발생 시 손실 X 사고 발생가능성
 - 해시로 연결된 로그 파일을 4개의 사본으로 타 기관에 분산보관하면?

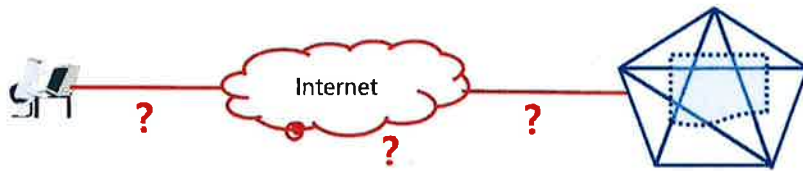
블록체인 vs. 공인전자문서보관소



- 블록체인
 - 다수의 노드가 중복 저장
 - 트랜잭션의 블록을 해시 값으로 사슬 모양으로 연결

블록체인과 전자 서명

- 블록체인은 전자서명에 의존한다
 - 서명되지 않는 것은 아무것도 없다. (트랜잭션, 블록)
 - 모든 사용자는 자신이 사용하는 개인키를 보관한다 (전자지갑)
- 블록체인이 암호학적으로 안전하다
 - ≠ *블록체인 시스템과 연결되어 사용자에게 제공되는 인터페이스와 프로그램이 안전하다*



그 외...

- 블록체인이 개인정보보호를 개선?
- 블록체인 기록과 트랜잭션 데이터의 차이?
- 제안 데이터
 - 철, 건, 컴포넌트(해시)
 - 입력자가 잘못된 정보를 입력하면 검증 가능한가?
- 진본검증 요청 화면
 - 필수입력 항목 : 본문 파일, TXID ???
- 현황 조회!!!
 - 원장은 데이터베이스가 아니며 현황 정보는 복사본
- 대상기관 확대?
 - 노드의 수와 합의된 기록의 신뢰성 연관성은?

결론

- 공공기관의 블록체인 도입 확대에 의한 기록생산 환경의 변화?
- 블록체인에 저장되는 해시, 트랜잭션 데이터 등의 기록관리 방안?
- 현행 전자서명 기반의 무결성 보장방식의 블록체인 대체?
- 블록체인 적용 공공기록 환경의 기록관리 업무 방식의 변화가능성?
- 권위 기반의 중앙집중식 기록관리 체계의 기술적 대안과 분산?

감사합니다