# NFT 기반 비대면 계약 서비스

권용준, 김남석, 이종훈, 임수민, 고석주
경북대학교 컴퓨터학부

# NFT-based untact contract service

Yong-Jun Kwon, Nam-Seok Kim, Jong-Hoon Lee, Soo-Min Im, Seok-Ju Ko
Dept. of Computer Science, Kyungpook National University

요 약

2020년 전자서명법 개정으로 공인인증서가 폐지됨에 따라 자체 인증 기술의 도입이 필요한 실정이다. 특히나 COVID-19로 인한 비대면 상황이 지속됨에 따라 기존 아날로그 방식을 통해 대면으로 계약서를 작성하고 수립하는데 많은 비효율적 문제가 대두되었다. 디지털 전환 가속화와 비대면 거래 확대로 인한 전자 신원확인 중요성이 점차 커지고 있음에 따라 전자 서명 및 전자 봉투 방식으로 계약할 수 있는 안전한 시스템 개발을 진행하고자 한다. 이를 위해 계약 시스템의 보안 요구 사항을 도출하였으며 최종적으로 NFT 연동을 통해 안전한 계약을 진행할 수 있도록 프로세스를 설계하였다. 시스템의 동작 방식을 표현하기 위하여 DFD 등을 포함한 Diagram 형태로 나타내었으며 실제 프로토타입을 제작 후 블록체인 네트워크에 연결한 뒤 테스트를 진행하여 시스템 검증을 수행하였다. 추후 이 시스템을 통해 B2B, B2C 모델 등의 모델 기반 다양한 거래와 계약이 가능하도록 구성할 예정이며 추가적인 연구를 진행하여 사용자 측면에서 더 간편하고 안전한 환경이 될 수 있도록 고도화 시키는 것을 목표로 한다.

## I. 서론

4차 산업 혁명을 통해 IT 기술이 발전함에 따라 보안의 중요성 또한 점점 커져가는 추세이다. 특히나 정보 보안의 기본 3요소인 기밀성, 무결성, 가용성의 중요성이 점점 커지고 있는데, 블록체인 기술의 등장과 성장에 따라 정보 보안 분야에 대한 엄청난 발전이 있었다.

[1]블록체인 기술은 분산 형태의 데이터베이스를 뜻하며 블록체인 기술이 비트코인, 기록 추적, 콘텐츠 관리 등 다양한 곳에서 활용되고 있다. 이는 COVID-19로 인한 비대면 환경에 적합한 기술로써 급부상하였으며 예술, 인사 및 회계 등 분야를 가릴 것 없이 다양한 곳에서 쓰일 수 있기 때문이다. 특히나 기존 네트워크에 비해 투명한 아키텍처를 제공하는데, 위/변조 방지가 매우 어렵기 때문에 무결성을 기반으로 한 신뢰성을 제공한다. 전망과 기술 예측에 대한 연구가 활발히 이루어지고 있는 반면, 블록체인 기술을 활용하여 수행하는 서비스에 대해서는 다양한 이유로 인하여 범용적으로 공개가 되어있지 않은 경우가 대부분이다.

본 논문은 이에 주목하여 Non Fungible Token(이하 NFT) 기술을 기반으로 한 비대면 계약 시스템을 설계하였으며 전자 문서를 암복호화 하는데 공개키 알고리즘을 사용하였고 검증을 위해 해시 알고리즘을 사용하여 Data Flow Diagram 형태로 나타내었다. 각각의 데이터 전송 포맷을 하나의 프로토콜 형태로 설계한 뒤 안전한 송수신을 목적으로 전자 봉투를 구현하고 이를 Sequence Diagram 형태로 나타냈다. 이후 계약 프로세스가 끝나고 계약에 관한 검증 및 증명을 위해 블록체인 기술을 활용하여 저장하였고 구현을 통해 실제 환경에서 동작하는 트랜잭션과 블록 정보를 확인하였다.

본 논문의 구성은 Ⅰ. 서론, Ⅱ. 비대면 계약 서비스 설계 및 구성, Ⅲ. 제안 시스템 타당성 분석 및 검증, Ⅳ. 결론으로 되어있다. 2장에서는 시스템 아키텍처를 포함한 전체 구성도를 확인할 수 있고 3장에서는 서비스 보안 요구 사항을 기준으로 기존 시스템과의 비교를 통한 타당성을 확인할 수 있다.

## II. 비대면 계약 서비스 설계 및 구성

본 논문에서는 부동산, 물품 등과 같은 상호 간의 거래를 진행하는 자유 형태의 비대면 계약 시스템을 제시한다. [1]NFT란 Non Fungible Token으로써 블록체인에 저장된 데이터 단위로, 고유하면서 상호 교환할 수 없는 토큰을 뜻한다. 이러한 기술을 활용한 전자 서명을 통해 보다 안전한 시스템을 구축하는 것을 목표로 한다.

### 1. 서비스 보안 요구사항

비대면 환경에서의 계약 진행을 위해 핵심 기술인 전자 서명 측면에서의 [2]에 따라 보안 요구 사항들을 도출하여 제시하였고 각각의 내용은 아래 표 1에서 확인할 수 있다.

<표 1> 전자 서명 보안 요구사항

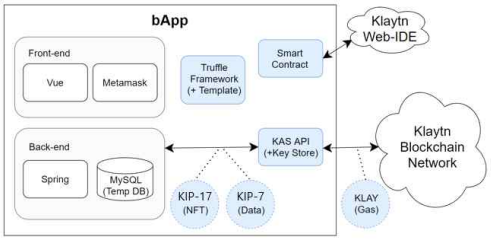
| Requirement | Contents |
|---|---|
| Unforgeable | 타 사용자 위조 불가 |
| User Athentication | 서명자 인증 및 검증 |
| Non-repudiation | 서명자의 서명 사실 부인 방지 |
| Unalterable | 생성키 소유자 외 서명 예정 문서 내용 변경 불가 |
| Not Reusable | 타 문서 서명 재사용 불가 |
| Judge | 제3자 통한 정당성 검증 가능 |

### 2. 제안 시스템 구성

비대면 계약 서비스 진행을 위해 앞서 언급한 보안 요구 사항을 지킨 시스템 구성을 설계하였고 시스템 처리 단계에 따라 세 가지 주요 프로세스를 나타내었다.

### 2.1 시스템 개요

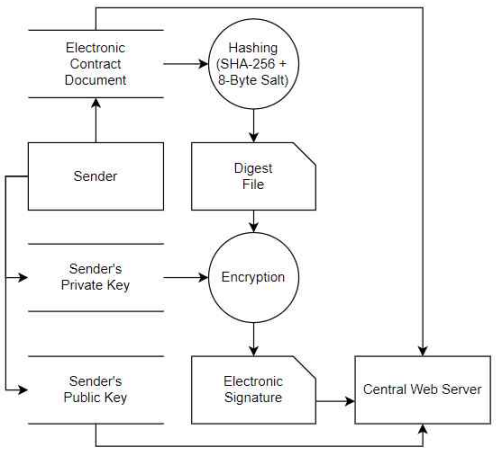
서비스 측면에서의 블록체인 장점 활용[3] 극대화를 위해 bApp 기반의 시스템을 설계하였으며 먼저 공개키 및 대칭키 기반의 계약 서비스를 위해 각각의 아키텍처를 나타내었다. 이후 해당 데이터들을 교환하기 위해 KAS API를 통해 bApp의 표준 토큰 데이터 형태를 활용하였으며 각각의 정보들이 최종적으로 클레이튼 네트워크에 저장되는 구조이다. 그림 1은 [4]의 dApp을 참고하여 블록체인 기술을 포함한 bApp 형태의 전체 시스템 개요도를 간단하게 나타내었다.




<그림 1> Simplified System Architecture

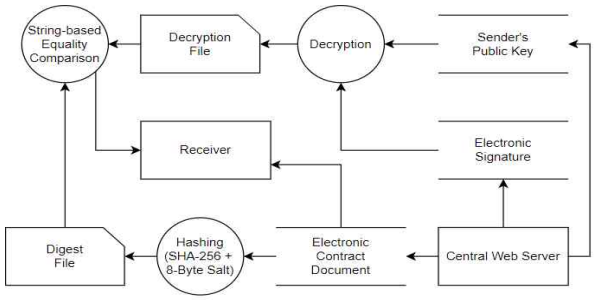
### 2.2 비대면 계약 프로세스

송신자 측에서는 계약을 위한 전자 문서와 송신자의 공개키, 그리고 해당 문서의 Hash 값을 개인키로 암호화한 전자서명 총 세 가지 데이터를 프로토콜로써 수신자에게 전달한다. 공개키 및 개인키 기반의 암/복호화 방식으로 RSA 알고리즘을 채택하여 사용하였으며 해시값을 얻는 방식으로 SHA-256 알고리즘에 8-Byte의 Salt 값을 더하였다. 그림 2는 해당 과정을 Data Flow Diagram 형태로 나타내었다.



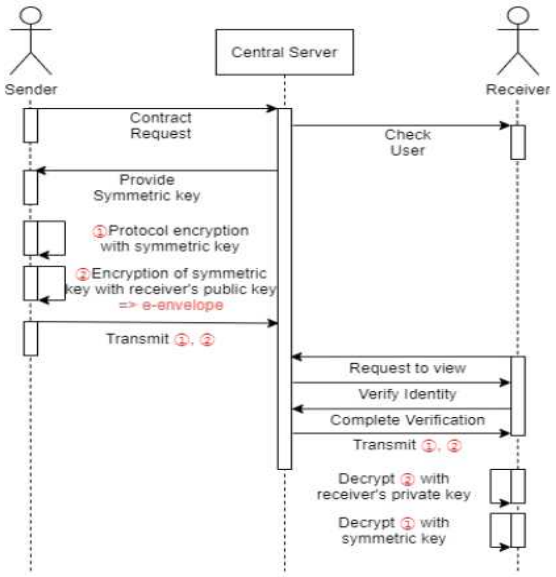

<그림 2> Transmission Process DFD

수신자 측에서는 전달받은 전자 문서의 해시 값을 구하고 송신자의 공개키를 기반으로 전달받은 전자서명을 복호화 하여 두 값이 동일한지 검증하는 과정을 진행한다. 만약 해당 값이 다르다면 정상적인 전송이 이루어지지 않았다고 판단하여 해당 Task를 즉시 종료한다. 그림 3은 해당 과정을 Data Flow Diagram 형태로 나타낸 것이다.




<그림 3> Reception Process DFD

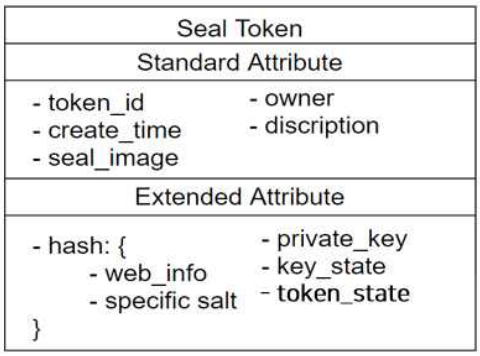
중앙 서버에서 주고받는 데이터를 AES 알고리즘 기반의 대칭키로 암호화시키고 해당 키와 함께 전자 봉투에 넣어서 전달한다. 아래 그림 4는 Sequence Diagram을 기반으로 전자 봉투 제작 및 전달 프로세스를 나타낸 것이다.




<그림 4> E-envelope Delivery Process

## 2.3 NFT 서명 프로세스 (KIP-17)

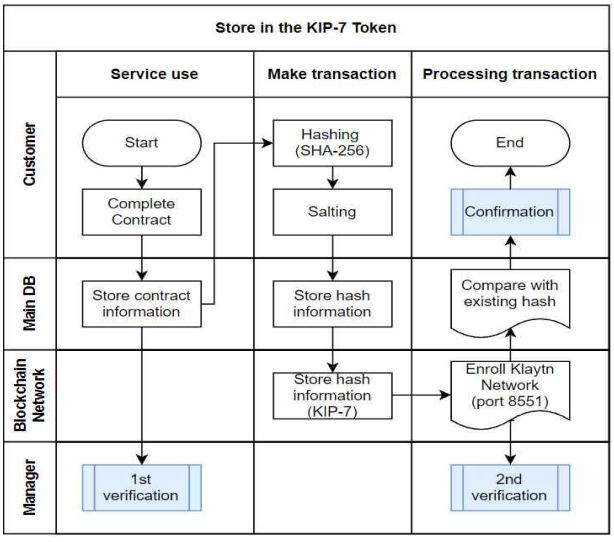
계약을 수립하는 과정에서 서명을 진행할 때 NFT 기반의 전자 서명으로 대체하는 과정이다. 사회 공학 기법이나 스푸핑 등을 방지하기 위하여 인증 과정을 통해 자신의 NFT 서명을 중앙 서버에서 불러올 수 있도록 [5]를 참고하여 설계하였다. 표준은 KIP-17을 사용하였으며 이더리움 토큰의 표준인 ERC-721에서 파생되었다. 아래 그림 5는 이용자의 서명 파일을 NFT 화 시킬 때 해당 토큰 안에 저장되는 정보들을 나타낸 것이다.




<그림 5> NFT(KIP-17) Token Data Structure

## 2.4 블록체인 저장 프로세스 (KIP-7)

모든 계약 프로세스가 종료되면 해당 계약을 증명하기 위하여 계약서 관련 해시값을 블록체인 네트워크에 저장하는 단계가 필요하다. 이후 관리자 또는 사용자는 해당 계약서 정보가 변조되지 않았음을 확인하기 위하여 블록체인 네트워크에 저장된 해시값과 계약서의 해시값을 비교 및 검증 할 수 있다. 표준은 KIP-7을 사용하였으며 이는 이더리움 토큰의 표준인 ERC-20에서 파생되었다. 아래 그림 6은 블록체인 네트워크에 저장되는 과정을 표현하기 [6]을 Customize하여 설계한 Cross Functional Flowchart의 일부이다.




<그림 6> Blockchain Cross Functional Flowchart

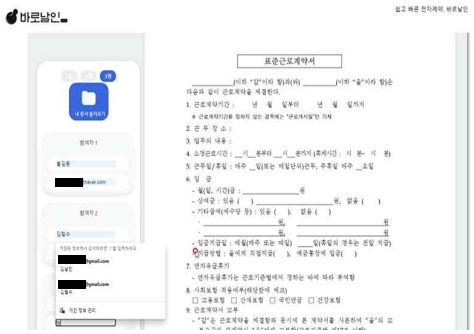
## III. 제안 시스템 타당성 분석 및 검증

제안 시스템의 타당성 분석을 위해 앞서 언급한 전자 서명 보안 요구 사항에 따라 시스템 평가를 진행하였다. 제안 시스템은 DB에 저장된 로그의 유효성 문제가 있는 기존 전자 계약 시스템의 단점을 블록체인으로 개선하였다.

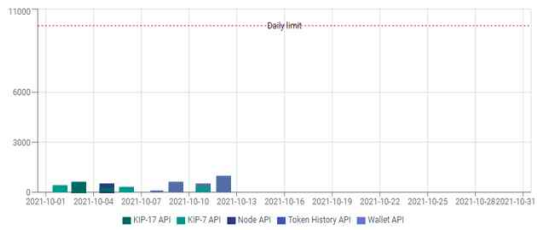
<표 2> 기존 시스템과 제안 시스템의 비교

| Requirement | 수기 계약 | 기존 계약 시스템 | 제안 시스템 |
|---|---|---|---|
| Unforgeable | Δ | Δ | O |
| User Athentication | O | O | O |
| Non-repudiation | Δ(녹음) | Δ | O |
| Unalterable | X | Δ | O |
| Not Reusable | X | O | O |
| Judge | Δ(사본) | Δ | O |

프로토타입 제작 후 실제 적용성 문제를 해결하기 위하여 다양한 지표를 활용할 예정이다. 일간/주간 웹 사이트 트래픽 발생량 및 컨트랙트 트랜잭션 API 호출 빈도, 유저 피드백 등의 지표를 종합하여 시스템 고도화를 진행할 계획이다. 아래의 그림 7은 완성된 웹 프로토타입의 계약 진행 단계이고 그림 8은 핵심 지표 모니터링을 위한 대시보드이다.



<그림 7> 프로토타입의 계약서 작성 과정




<그림 8> Klaytn API Dashboard

## IV. 결론

본 논문에서는 전자 서명 측면에서의 보안 요구 사항을 반영하여 비대면 상황에서 사용할 수 있고 안전하게 계약할 수 있는 시스템을 제시하였다. PKI 기술을 기반으로 비대면 계약 업무에 대한 전반적인 프로세스를 제작하였으며 전자 봉투 인증, 블록체인을 통한 검증과 확인까지 각각의 단계에 걸친 시스템을 설계하였다. 향후 다양한 사업 모델과 서비스 모델에 사용할 수 있도록 실무적으로 접근할 예정이며 계약 관련 추가적인 기능 구현을 통해 프로토타입을 추가 개발하여 테스트를 진행하고 문제점을 보완할 계획이다. 이를 통해 비대면 환경에서의 거래, 계약 및 전자 서명과 블록체인 기술 연구에 중요 지표로 작용할 것으로 기대한다.

## ACKNOWLEDGEMENT

"본 연구는 2021년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음" (2021-0-01082)

## 참고문헌

[1]. 민경식, 김관영, 박진상, "NFT 기술의 이해와 활용, 한계점 분석, 한국인터넷진흥원(KISA), 2020.12.

[2]. 정태규, "전자 인증 이용을 위한 보안 요구사항 분석 및 가이드라인", 석사학위논문, 충북대학교, 2017.02.

[3]. 서상민, 권동환 외 10명, "클레이튼 블록체인 플랫폼의 고성능 합의 알고리즘", 한국통신학회지, 2020.02.

[4]. 이현경, 이지현 외 2명, "블록체인 이더리움 기반 저작권 거래 서비스 DApp", 한국정보과학회, 2020.12.

[5]. 황제영, 홍상원 외 2명, "NFT를 활용한 메신저 서비스 보안 지원 기법", 한국정보과학회, 2020.06.

[6]. Qin Wang, Rujia Li 외 2명, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges", arXiv, 2021.05.