

# 자율운항선박의 블록체인 기반 사용자 인증 시스템 연구

홍승표\* · 이훈재\*\* · † 이영실

\*동서대학교 일반대학원 컴퓨터공학과, \*\*동서대학교 정보보안학과, † 동서대학교 International College

**요 약** : 자율운항선박의 시대 도입을 위해 보안체계의 중요성은 더욱 커져가고 있다. 국내 및 국외 학계에서는 해양선박 보안에 관한 연구가 활발히 이루어지고 있는데 자율운항선박은 자율운행자동차와 마찬가지로 주위 환경에 대한 자동식별장치가 필요하다. 선박자동식별장치(Automatic Identification System, AIS)는 선박의 종류와 위치 관련 데이터와 인증서를 포함한 정보를 인근의 항로표지로 전달한다. 인간이 개입하지 않는 자율운항 개발 단계에서는 사용자 인증이 더욱더 중요하며, 본 논문에서는 기존 사용자 인증방식에 대한 취약점을 보완할 블록체인을 기반한 사용자 인증 시스템을 연구하였다.

**핵심용어** : 자율운항선박, AIS, 블록체인, 하이퍼레저 패브릭

**DSU** Dongseo University

2022KINPR 한국해양과학기술협의회 춘계공동학술대회

## 자율운항선박의 블록체인 기반 사용자 인증 시스템 연구

동서대학교  
홍승표

1

**DSU** Dongseo University

### 1. Introduction

▶ 연구 배경

1. 자율운항선박의 시대 도입을 위해 보안체계의 중요성은 더욱 커져가고 있음.
2. 국내 및 국외 학계에서는 해양선박 보안에 관한 연구가 활발히 이루어지고 있다.
3. 자율운항선박은 자율운행자동차와 마찬가지로 주위 환경에 대한 자동식별장치가 필요하다.
4. 선박자동식별장치(Automatic Identification System, AIS)는 선박의 종류와 위치 관련 데이터와 인증서를 포함한 정보를 인근의 항로표지로 전달한다.
5. 인간이 개입하지 않는 자율운항 개발단계에서는 사용자 인증이 더욱더 중요함.

▶ 최근 대표적인 국내 해양선박 보안관련 연구현황

2022 해양선박 보안&보안 GRC 워크숍 - CPS 보안연구회, 해양사이버보안연구회, 정보보안GRC연구회

2

**DSU** Dongseo University

### 2. BlockChain

▶ 퍼블릭 블록체인 - Public

개방형 혹은 무허가형 블록체인이라고 불리는 퍼블릭 블록체인은 조직의 승인없이 누구나 참여가 가능한 블록체인 네트워크를 뜻한다.

1. 가장 중요한 핵심은 '탈 중앙화', 가상화폐를 시작으로 에너지 산업분야, 콘텐츠 직거래 플랫폼, 사물인터넷 등 다양한 분야에서 사용이 되고 있음.
2. 모든 사람들이 거래에 참여하기 때문에 투명성이 강화되어, 의사소통이 원활함.
3. 하지만, 모든 사람들에 의해 합의가 진행되고, 연결되어 있는 모든 네트워크에 전파하여 동기화가 필요하기 때문에 속도가 느리다는 단점이 있음.

3

**DSU** Dongseo University

### 2. BlockChain

▶ 허가형 블록체인 - Private

프라이빗 혹은 폐쇄형으로 불리는 허가형 블록체인은 기업을 대상으로 만들어진 방식이며, 이름의 뜻 그대로 허가된 사용자(노드)만 네트워크에 접속할 수 있다.

1. 퍼블릭과 동일하게 가상화폐 또는 금융거래의 목적은 있으나 그 외에 다른 기관에서 데이터의 보안성 유지를 위해 사용함.
2. 퍼블릭과 다른 점은 '탈 중앙화'형식과 다르게 사용자 인증을 하는 중앙 기관이 존재하기 때문에 기존의 블록체인 네트워크 성격과 상이한 점이 존재.
3. 허가된 사용자 측, 소수의 인원을 구성한 네트워크의 형태를 띄고 있어 속도 측면에서 뛰어나.
4. 신뢰된 관계로 구성되어 있어 기술적인 보안성이 낮음.

4

† 교신저자: lys0113@dongseo.ac.kr  
\* alfkdlthd@gmail.com, \*\* hjlee@dongseo.ac.kr

## 2. BlockChain

### ▶ 하이퍼레저 패브릭 - Hyperledger Fabric

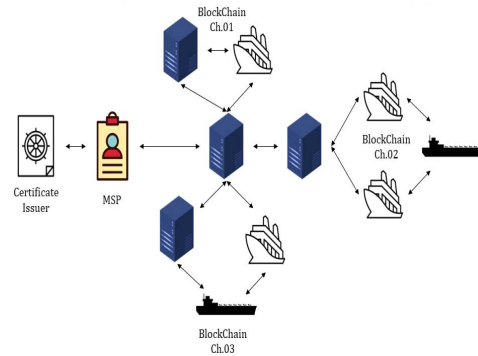
하이퍼레저 패브릭은 디지털 기반의 원장, 스마트 계약, 참여자들에게 의해 관리할 수 있는 시스템. 블록체인 참가자들의 신원을 인증하는 체계를 갖추고 있다.

1. 공개키 기반 암호화 기술인 PKI(Public Key Infrastructure)를 활용하고 있고, CA(Certificates Authority)는 참여자의 인증서를 발급 및 서명에 필요한 공개키와 비밀키를 부여 받게 됨.
2. MSP(Membership Service Provider)를 통해 거래 제안을 할 경우 자신이 서명한 문서임을 알리기 위해 개인키로 서명하여 거래 상대방 문서의 인증에 필요한 공개키를 제공한다.
3. 거래를 승인하는 노드 Endorsing Peer, 승인된 계약들을 모아 블록을 만드는 역할만을 수행하는 노드 Orderer, 거래 내역의 유효성을 검증하는 노드
4. 각 역할별로 구분되어 있는 노드에 의해 거래 처리 효율성과 처리 속도를 유지할 수 있는 장점을 제공.

5

## 3. Model

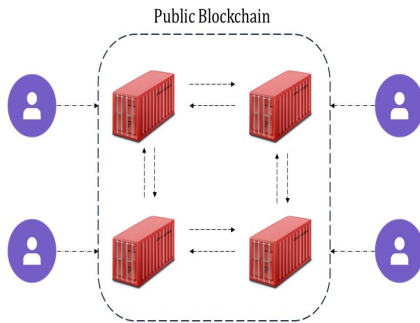
### Autonomous Surface Ship Blockchain-based User Authentication Model [2]



6

## 3. Model

### Cargo Container Blockchain-based Authentication Model



7

## 3. Model

### ▶ Autonomous Surface Ship Blockchain-based User Authentication Model [2]

Qing Hu (2021)은 선박 신원 인증을 위하여 블록체인 기술을 이용하여 하이퍼레저 패브릭을 기반한 분산 원장을 제안하였다.

- 소유권 및 최종 통제 권한을 선주에게 할당하고, 선박 인증서에 대한 통제 권한은 해양국에 할당하여 안정성 있는 통제를 할 수 있다.

### ▶ Cargo Container Blockchain-based Authentication Model

- 또한, 해양 선박 내 컨테이너 화물 관리에 블록체인 적용 모델은 용도에 맞게 하이퍼레저 패브릭 플랫폼과 호환이 가능한 퍼블릭 블록체인 형태 제안.
- 모든 사람들이 화물에 대한 정보(이동경로, 위치, 온도 등)를 실시간 확인할 수 있으며 무결성, 실시간성, 신뢰성이 기본으로 보장.

8

## 4. Conclusion

### ▶ (Public Blockchain <-> Private Blockchain)

선박간 통신은 서로 다른 기관 혹은 사용자의 신뢰 관계가 중요. 따라서, 블록체인을 기반으로 한 선박 사용자 인증 및 화물 컨테이너 인증 모델을 제안.

1. 제안된 모델은 선박의 소유권 및 최종 권한은 사용자에게 할당
2. 선박 인증서 정보에 대한 권한은 해양국에 할당하여 데이터에 액세스할 수 있는 사람과 추적 데이터가 기록 및 활용되는 방식을 안전하게 통제가 가능.
3. 시스템은 Hyperledger Fabric을 기반으로 설계하여 네트워크에 대한 안정성, 투명성 및 효율성을 제공.

9

## REFERENCE

- [1] Jinsu Kim, Namje Park. (2021).Blockchain Technology and Major Domestic Applied Industry Trends.Korea Institute of Information Technology Magazine,19(1),19-24.
- [2] Qing Hu, Wenshuo Han, and Hao Zhang. 2021. Ship identity authentication security model based on Blockchain. In 2021 4th International Conference on Data Science and Information Technology (DSIT 2021). Association for Computing Machinery, New York, NY, USA, 135-142.
- [3] Four Considerations for the Security of Marine Ships in 2022, Security News, Available : <https://www.boannews.com/media/view.asp?idx=105264>
- [4] Hanool Choi.(2021).A Study on Application of Blockchain Platform to Trade Process based on Hyperledger Fabric.International Commerce and Information Review,23(2),3-20.

10

## Acknowledgment

이 논문은 2022년 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임 (해양 디지털 항로표지 정보협력시스템 개발(2/5) (20210650))