JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 2, pp. 115-124, February 2022
https://doi.org/10.9708/jksci.2022.27.02.115

NextAuction: A DID-based Robust Auction Service for Digital Contents

Young-Eun Lee*, Hye-Won Kim*, Myung-Joon Lee**

*Student, Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan, Ulsan, Korea
*Student, Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan, Ulsan, Korea
**Professor, School of IT Convergence, University of Ulsan, Ulsan, Korea

[Abstract]

In this paper, we present an NFT auction service for the next generation, named NextAuction, which can reliably trade ownership of individual content using DID technology. Recently, as the types and sizes of tradable digital assets have expanded, the number of NFT transactions has also increased, and a significant number of marketplaces are being operated. But, the current user authentication methods of NFT marketplaces are done only through the associated blockchain wallets. It is desirable that ownership transfer through NFT transactions be transparently managed based on a more reliable identity authentication service. NextAuction increases the reliability of auction service participants by transparently and consistently providing identity authentication for users of auction services based on the DID technique using the Klaytn blockchain. In addition, in preparation for server failure that may occur during the auction of individual content, it provides users with a robust auction service using the BR2K technique that continuously provides consistent service through the replication of a target service. The NextAuction service is developed by extending BCON, a blockchain-based content management service.

▸ **Key words**: NFT, Blockchain Service, DID, Auction Service, BR2K

[요 약]

본 논문에서는 개인의 콘텐츠에 대한 소유권을 DID 기술을 사용하여 신뢰성 있게 거래할 수 있는 차세대 NFT 경매 서비스인 NextAuction을 제시한다. 최근 소유권이 거래될 수 있는 자산의 종류와 규모가 확대됨에 따라 NFT 거래의 규모도 커지면서 이와 함께 상당수의 거래소가 운영되고 있다. 그러나 현재 NFT 거래소들의 사용자 인증 방식은 연결된 블록체인 지갑을 통해서만 이루어진다. NFT 거래를 통한 소유권 이전은 더욱 신뢰할 수 있는 신원 검증 서비스를 기반으로 투명한 소유권 관리가 이루어지는 것이 바람직하다. NextAuction은 클레이튼 블록체인을 활용한 DID 기법을 기반으로 경매 서비스의 사용자들에 대한 신원 인증을 투명하고 일관성 있게 제공하여 경매 서비스 참여자에 대한 신뢰성을 높인다. 또한, 개별 콘텐츠의 경매 진행 중 발생 될 수 있는 서버의 실패상황에 대비하여, 서비스 복제를 통하여 일관성 있는 서비스를 끊임없이 제공하는 BR2K 기법을 활용한 견고한 경매 서비스를 사용자에게 제공한다. NextAuction 서비스는 블록체인 기반의 콘텐츠 관리 서비스인 BCON을 확장하여 개별 콘텐츠에 NFT를 발행하고, DID를 통한 안전하고 신뢰성 있는 NFT 경매를 제공하도록 개발되었으며 옥션 매니지먼트 컨트랙트, NFT 매니지먼트 컨트랙트 및 옥션 서버와 옥션 사용자 인터페이스로 구성된다.

▸ **주제어**: NFT, 블록체인 서비스, DID, 경매 서비스, BR2K

• First Author: Young-Eun Lee, Corresponding Author: Myung-Joon Lee
*Young-Eun Lee (lyoung828@cicweb.ulsan.ac.kr), Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan
*Hye-Won Kim (alsldjcjstk@cicweb.ulsan.ac.kr), Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan
**Myung-Joon Lee (mjlee@ulsan.ac.kr), School of IT Convergence, University of Ulsan
• Received: 2021. 12. 23, Revised: 2022. 01. 12, Accepted: 2022. 01. 13.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 NFT(Non-Fungible Token)[1] 시장이 세상의 많은 관심을 받고 있다. 소유권이 거래될 수 있는 자산의 종류와 규모가 급격히 확대됨에 따라 NFT 거래의 규모도 함께 커지고 있다. NFT는 디지털 콘텐츠에 대한 소유권과 거래 이력이 명시되어 있어 자신의 소유권을 증명할 수 있고, 이를 블록체인에 저장함으로써 블록체인 상에 NFT 출처와 발행시간, 소유자 내역 등의 정보가 공개되어 NFT 관련 정보의 추적이 용이하다. NFT 거래가 활발해짐에 따라 상당수의 거래소가 운영되고 있으며 이들 중 대표적으로 거론되는 OpenSea는[2] NFT를 포함한 디지털 자산의 거래를 지원하는 P2P방식의 거래소로서, 블록체인을 통하여 디지털 거래의 고질적인 문제점인 거래 쌍방의 불신임 관계 문제를 해결하고 있다. 국내의 가장 큰 NFT 거래소인 Klip Drops는[3] 디지털 아트 거래소로 카카오의 블록체인 개발 자회사 그라운드X가 운영한다. 뿐만 아니라 다양한 형태의 NFT 거래소들이 운영되고 있다. 그러나 현재 운영되고 있는 거래소들의 사용자 로그인 방식은 블록체인 지갑을 통해서만 이루어진다. NFT 거래는 해당 디지털 콘텐츠에 대한 비가역적인 소유권 이전이므로, 보다 객관적인 신원 검증 서비스를 기반으로 소유권의 이전 이후에 해당 콘텐츠와 변경된 소유권에 대한 관리가 철저하게 이루어지도록 콘텐츠 거래 서비스가 운영되는 것이 바람직하다.

DID(Decentralized Identifier)는[4] 기존 신원 제공자, 인증기관 등 제3의 중앙기관으로부터 독립되어 사용자 본인이 자신의 신원을 증명 가능한 분산 디지털 신원확인 기술로서 차세대 신원 인증 서비스로 주목받고 있다. BCON은[5] DID를 기반으로 개인 스스로가 자신의 신원을 인증하여 자신의 콘텐츠를 안전하게 보관하며, 콘텐츠에 대한 소유권을 신뢰성 있게 보장받을 수 있는 블록체인 서비스이다. 본 논문에서는 BCON 서비스를 확장하여, 개별 콘텐츠들에 카카오 블록체인 플랫폼 클레이튼의[6] 대체 불가 토큰 표준 KIP-17으로[7] NFT를 발행한다. 이를 기반으로 안전하고 신뢰성 있는 NFT 콘텐츠 경매를 제공하는 옥션 서비스인 차세대 경매 서비스 NextAuction을 소개한다. NextAuction은 사용자가 자신의 콘텐츠에 NFT를 발급받아 언제든지 경매에 참여할 수 있으며, 경매가 종료된 후 해당 콘텐츠에 대한 NFT와 소유권 증명서를 이용해 체계적인 소유권 이전을 제공한다. 또한, 기존의 NFT 거래소들과 달리 DID를 이용해 경매 서비스의 사용자들에 대한 신원 인증을 투명하고 일관성 있게 제공하여 경매 서비스 참여자에 대한 신뢰성을 높인다. 이와 더불어 NextAuction은 개별 NFT에 대한 경매 도중에서의 서버 실패상황에 대비해 서비스 복제를 기반으로 일관성 있는 서비스를 끊임없이 제공하는 BR2K(Blockchain application, Replication & Recovery technique using Kubernetes) 기법을[8-9] 사용하여 옥션 서비스를 복제 실행함으로써 서비스의 견고성을 사용자에게 제공한다. NextAuction은 클레이튼에서 동작하며 옥션 서비스와 NFT 매니지먼트 컨트랙트, 옥션 매니지먼트 컨트랙트 그리고 옥션 사용자 앱으로 구성되어있다. 또한, 이 구성요소들은 BCON 서비스의 구성요소들과 함께 동작한다.

본 논문의 구성은 다음과 같다. 1장 및 2장에서는 서론과 배경지식을 다룬다. 3장에서는 NextAuction의 시스템 구조를 제안하고, 4장에서는 NextAuction의 구현 기법 및 옥션 서비스의 견고성 실험에 관하여 기술한다. 마지막으로 5장에서는 본 논문의 결론에 관하여 서술한다.

II. Background Knowledge

1. NFT

NFT(Non-Fungible Token)는 고유하며 대체 불가능한 토큰을 의미한다. NFT를 통해 디지털 또는 물리적 자산에 대한 소유권을 나타내는 것이 가능하며, 개별적으로 구별 가능한 특성을 이용하여 자산의 디지털화를 실현한다. 모든 NFT에는 정보에 대한 메타데이터, 소유자의 ID 등과 같은 식별 정보가 포함되어 NFT를 고유하게 만들고 NFT마다 각자 다른 가치를 가지게 한다. 이러한 NFT는 배포된 스마트 컨트랙트를[10] 저장소로 삼아 새롭게 토큰을 생성하는 것이 가능하다. 클레이튼에선 독자적으로 자체 버전의 NFT인 KIP-17을 개발하였다. KIP-17은 이더리움의 NFT인 ERC-721에서 파생되었고, 제공되는 표준 인터페이스 API를 통해 쉽게 생성과 관리가 가능하다. 새 토큰을 발행하는 Minting, 발행된 토큰을 사용자 간 주고받는 Transfer, 토큰을 폐기하는 Burn과 같은 행위를 통해 NFT 활동을 추적한다. NFT가 지니는 대체 불가능한 특성으로 암호화 자산 시장인 OpenSea에선 블록체인 기반 디지털 항목의 판매와 구매가 가능하다.

2. BCON

BCON은 서비스 사용자 스스로 자신의 신원을 인증하여 개인 콘텐츠를 안전하게 보관하고, 콘텐츠에 대한 자신의 소유권을 신뢰성 있게 보장받을 수 있는 DID 기반의 콘텐츠 관리 서비스이다. BCON은 서비스를 위한 DID 기반의 신원 및 권한 인증 방식으로 기존의 DID Auth 과정을 간략화하여 개발한 BCON auth를 사용한다. BCON 사

용자는 BCON 서비스에 자신의 콘텐츠를 업로드 및 다운로드를 할 수 있다. 업로드와 다운로드 시 BCON auth 기반의 신원 인증이 일어나며, 액세스 토큰과 콘텐츠에 대한 자격증명서 및 소유증명서를 통해 체계적으로 콘텐츠에 대한 사용자의 접근 권한을 제어한다. 이로 인해 콘텐츠 소유자의 콘텐츠를 안전하고 신뢰성 있게 보관할 수 있으며 소유권 또한 확실하게 보장받을 수 있다.

3. BR2K scheme

BR2K는 자체적인 서비스 복제 방법과 서비스 실패에 대한 신속 재가동을 지원하는 복구 방법을 통해 블록체인 응용 서비스의 견고성을 지원하는 기법이다. BR2K는 ETCD[11] 분산 스토리지를 이용한 사용자 요청의 체계적인 처리 절차, 쿠버네티스를[12-13] 이용한 배포 등을 통해 블록체인 응용 서비스를 기민하게 복제하여 장애 상황에서도 서비스의 연속성을 지원한다. 또한, 이 기법은 이더리움의 스마트 컨트랙트로 개발된 서비스 레지스트리를 통해 사용자에게 서비스의 최신 접속 정보를 지속적으로 제공할 수 있으며 최악의 경우를 대비한 서비스 복구 정보의 관리를 지원할 수 있다. 그리고 BR2K 기법은 이 서비스 레지스트리에 백업된 복구 정보를 이용하여 블록체인 응용 서비스가 중지되는 상황에서 신속히 서비스를 복구할 수 있는 체계적인 절차도 지원한다.

III. Architecture and NextAuction

본 장에서는 DID를 이용해 안전하게 신원을 보장하며 BR2K를 통해 견고한 NFT 기반 콘텐츠 경매를 할 수 있는 옥션 서비스인 NextAuction의 서비스 시나리오와 구조를 설명한다.

1. Service Scenario of NextAuction

그림 1과 같이, NextAuction은 콘텐츠 판매자, 콘텐츠 구매자 및 신뢰할 수 있는 NFT 기반의 콘텐츠 거래 플랫폼 NextAuction 이렇게 세 가지 참여자가 있다.

Seller (콘텐츠 판매자): 자신의 콘텐츠 중에서 BCON 서비스에 등록되어있고 NFT를 발급받은 콘텐츠를 NextAuction 서비스를 통해 판매함과 동시에 소유권을 양도한다.

Buyer (콘텐츠 구매자): 콘텐츠가 필요한 개인 또는 조직이며, NextAuction 서비스를 통해 콘텐츠를 구매함과 동시에 콘텐츠에 대한 소유권을 양도받는다.

NextAuction 서비스: 신뢰할 수 있는 NFT 기반의 콘텐츠 거래 플랫폼으로 BCON 서비스와 경매 서비스로 구성되며 NFT 기반의 콘텐츠 경매 및 소유권 이전이 이루어진다.

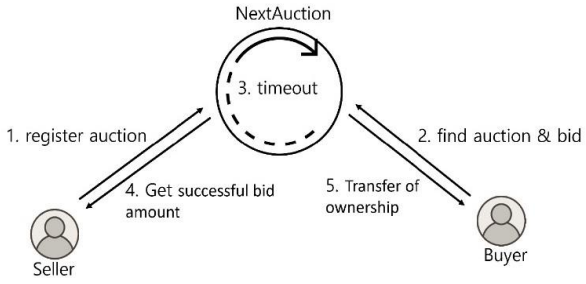

Fig. 1. Service Scenario of NextAuction

그림 1은 NextAution의 전체적인 진행 과정을 간략하게 나타낸 것이다. Seller는 NextAuction 서비스에 콘텐츠 옥션 등록을 요청하여 해당 콘텐츠가 경매 중 상태가 되면 다른 NextAuction 사용자인 Buyer들이 해당 콘텐츠에 대한 입찰을 시작한다. 이때 입찰가격은 가장 최근 입찰가 이하가 될 수 없으며, 입찰시 입찰금액은 NextAuction 서비스에 미리 보내고 경매 종료 시까지 입찰 취소가 불가능하다. 해당 콘텐츠의 경매가 종료되면 Seller는 최종 낙찰금액에서 서비스 수수료를 제외한 금액을 NextAuction 서비스로부터 전송받으며, 수수료는 옥션 서비스에 지급된다. Buyer는 콘텐츠에 대한 모든 소유권을 이전받으며 경매가 종료된다.

2. architecture of NextAuction

NextAuction은 BCON 서비스의 컴포넌트들과 옥션 서비스의 컴포넌트들로 구성되어있다.

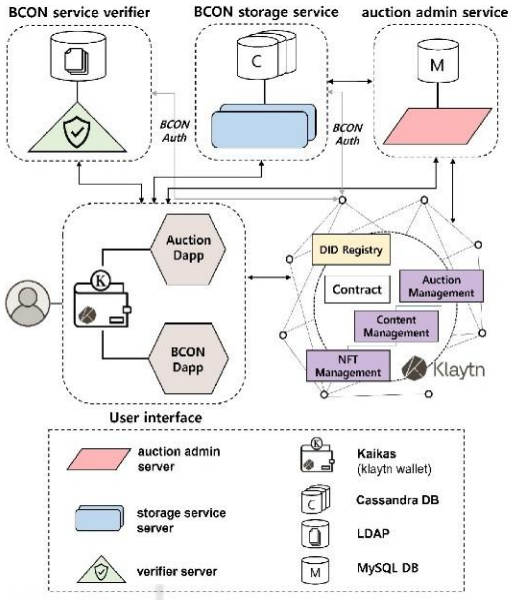

Fig. 2. Content Upload Process

우선 BCON은 카카오 블록체인 플랫폼인 클레이튼에서 동작하며 콘텐츠 서비스 검증자, 콘텐츠 보관 서비스, 콘텐츠 매니지먼트 컨트랙트, 콘텐츠 서비스 사용자 앱으로 구성된다. 콘텐츠 서비스 검증자는 DID를 기반으로 사용자의 신원 및 권한을 관리하는 서비스이다. 콘텐츠 보관 서비스는 사용자가 콘텐츠에 접근하는 권한과 콘텐츠를 유지 및 관리한다. 콘텐츠 매니지먼트 컨트랙트는 콘텐츠 관리에 필요한 정보를 클레이튼 블록체인에 저장함으로써 콘텐츠에 대한 신뢰성 있는 관리를 가능하게 한다. 콘텐츠 서비스 사용자 앱은 3개의 독립적인 서비스들과 상호작용하여 사용자가 BCON 서비스를 보다 편리하게 이용할 수 있게 개발된 클레이튼 분산 어플리케이션이다.

NextAuction의 옥션 관리 서비스는 경매 시작부터 종료 시까지 해당 콘텐츠에 대한 소유주의 권한을 위임받으며, 전반적인 경매 진행을 담당한다. 해당 서비스는 경매 진행에 대한 서비스를 제공하는 옥션 관리 서버와 경매 진행에 관한 정보들을 저장하기 위한 오픈소스 관계형 데이터베이스 관리 시스템 MySQL로[14] 구성된다. 경매 진행 시 일어나는 모든 이벤트는 해당 서비스에서 검증을 거친 후 실행됨으로 옥션 관리 서비스를 통해 좀 더 체계적인 경매 서비스를 제공한다. 신뢰성 있는 서비스를 위해 2개의 클레이튼 스마트 컨트랙트를 사용한다. 우선 옥션 매니지먼트 컨트랙트는 옥션 관리 서비스의 동작하에 경매 진행 및 경매에 사용되는 모든 정보를 관리한다. NFT 매니지먼트 컨트랙트는 BCON 서비스의 콘텐츠 매니지먼트 컨트랙트와 함께 동작하며 NFT 생성 및 소유주 관리를 한다. 옥션 사용자 앱은 각 독립적인 서비스들과 컨트랙트와 상호작용하여 사용자가 NextAuction을 보다 편리하게 이용할 수 있게 동작하는 클레이튼 분산 애플리케이션이다.

IV. Implementation and Test of NextAuction

본 장에서는 NextAuction의 구현 기법 및 옥션 Dapp의 실행에 관하여 기술한다. 구현 기법은 크게 3개의 절로 나눈다. 경매 시작에 앞서 경매 진행 동안 해당 콘텐츠의 소유주 권한을 옥션 관리 서비스에 임시로 위임하며 경매를 준비하는 단계를 **Preparing for the Auction** 단계로 표현한다. 그리고 해당 콘텐츠에 대한 경매를 생성하고 입찰하는 단계를 **In Progress Auction** 단계로 표현한다. 마지막으로 해당 경매가 종료되고 경매에 대한 낙찰금액 및 수수료 정산과 함께 콘텐츠에 대한 소유권 이전이 일어나는 단계를 **End of the Auction** 단계로 표현한다.

1. Preparing for the Auction

경매 시작에 앞서 원활한 경매 진행을 위해 판매자는 경매가 진행되는 동안 옥션 관리 서비스에 자신의 콘텐츠에 대한 모든 권한을 위임해야 한다. 이 절은 사용자와 옥션 서비스가 권한 위임을 위해 체계적이고 신뢰성 있게 합의하는 과정을 설명한다.

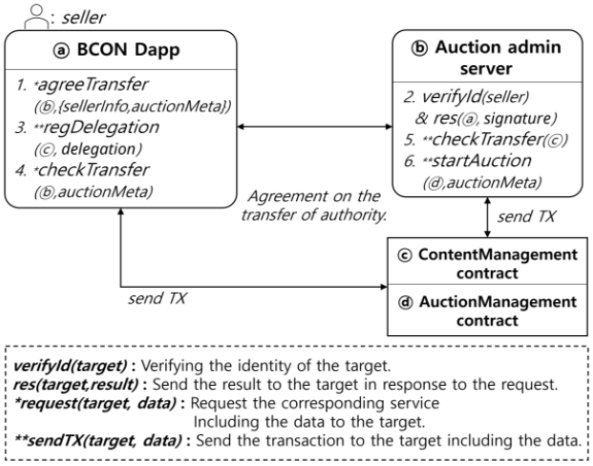

Fig. 3. Preparing for the Auction Process

[step1-3 in fig. 3] 사용자는 BCON 서비스 사용자 앱에 업로드된 자신의 콘텐츠 중 경매를 시작할 콘텐츠를 선택해 경매 시작을 위한 소유주 임시 권한 위임 요청을 옥션 관리 서비스에 보낸다. 요청을 받은 옥션 관리 서비스는 사용자의 신원을 BCON auth를 통해 확인하고, 확인이 완료되면 요청 시 받은 *auctionMeta*에(Table 2, AuctionMeta) 옥션 관리 서비스의 프라이빗 키로 사인한 시그니쳐 값으로 요청에 응답한다. 응답을 받은 BCON 서비스 사용자 앱은 시그니쳐 값을 포함하여 *delegation*을(Table 2, Delegation) 생성한 뒤 콘텐츠 매니지먼트 컨트랙트에 기록한다. 이때 *delegation*은 옥션 서비스가 해당 콘텐츠에 대한 사용자의 모든 권한을 경매 동안 위임받는 것을 수락하였으며 경매 시작에 앞서 해당 콘텐츠의 소유주가 경매 진행 동안 옥션 관리 서비스에 권한을 위임함을 합의하였음을 증명한다.

[step4-6 in fig. 3] 콘텐츠 매니지먼트 컨트랙트에 *delegation* 등록을 마친 후 사용자는 옥션 관리 서비스에 권한 위임 확인 요청을 경매 메타정보와 함께 보낸다. 요청을 받은 옥션 관리 서비스는 콘텐츠 매니지먼트 컨트랙트에 트랜잭션을 보내 *delegation*이 등록된 내용을 확인한다. 확인이 완료되면 요청 시 BCON 서비스 사용자 앱을 통해 받은 경매 메타정보를 옥션 매니지먼트 컨트랙트에 전달하여 해당 경매를 생성하면서 경매가 시작된다.

2. In Progress Auction

경매가 시작되면 해당 콘텐츠를 구매하고자 하는 구매자들의 입찰참여를 통해 해당 경매의 입찰가가 갱신된다. 이 절은 해당 경매의 입찰참여를 위한 일정한 조건 검사를 거쳐 입찰가가 갱신되는 과정을 설명한다.

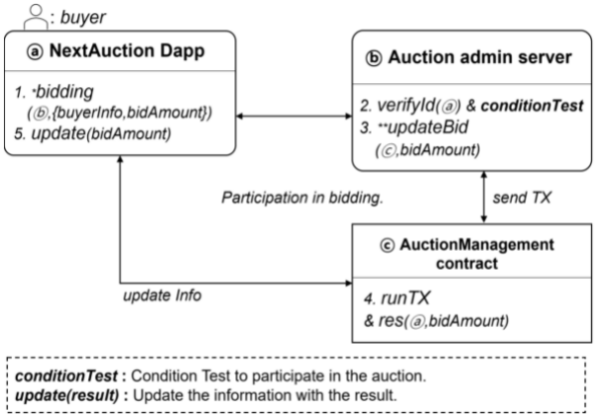

Fig. 4. In progress Auction Process

Table 1. Pseudo-code for [§fig. 4. condition Test]

Condition Test (auction.middleware in Auction admin server)	
1:	function **isEqualSeller**(auction, buyer) {
2:	return (buyer == auction.user_addr); }
3:	function **isBiggerthanLast**(auction, amount) {
4:	return (amount < auction.bid_amount); }
5:	async function **isNotExpired**(auction) {
6:	const res = await jwt.verifyJWT(auction.valid_time, auction.valid_key);
7:	return (amount < auction.amount); }

[step1-4 in fig. 4] 구매자는 옥션 사용자 앱을 통해 진행 중인 콘텐츠의 경매에 대해 최소 입찰금액 및 이전 입찰 기록들을 확인한 후 원하는 입찰금액을 입력한다. 입력이 완료되면, 옥션 사용자 앱은 구매자의 입찰참여 요청을 옥션 관리 서비스에 전달한다. 요청을 받은 옥션 관리 서비스에선 BCON auth를 통한 구매자의 신원확인과 입력된 입찰가가 경매의 입찰조건에 부합되는지 확인하는 조건 검사를 진행한다. 조건 검사는 해당 경매의 소유주가 아닌지(Table 1. line 1), 해당 경매의 기한 안에 진행되는 입찰인지(Table 1. line 3), 해당 경매의 최고 입찰가보다 큰 금액을 입찰했는지(Table 1. line 5) 확인한다. 확인이 완료되면 옥션 매니지먼트 컨트랙트로 입찰 트랜잭션을 보낸다. 요청한 입찰금액이 가장 최고 입찰가로 갱신되고 직전의 입찰가의 사용자에게 입찰금액을 돌려준다.

Table 2. Data Structure

AuctionMeta	
NFT	NFT of content.
name	name of content.
price	initial bid.
expire	Auction validity time.
desc	description of auction.
contentOwner	DID of the current owner of the content.
contentCreator	DID of the creator of the content.
Delegation	
contentOwner	owner of content
account	name of content.
price	initial bid.
signMeta	AuctionMeta
signature	value signed by auction admin service with a private key on the signMeta.
validTime	DID of the current owner of the content.
isActivate	DID of the creator of the content.
OwnerchipCert	
[ContentMeta]	
NFT	NFT of content.
created	time when the content was registered.
name	name of content.
fileType	file format of content.
size	size of content.
metahash	hash value of content.
contentType	type of content.
desc	description of content.
[OwnerInfo]	
userDID	DID of the current owner of the content
keyID	each ID of various public keys held by userDID.
history	owner list of content.
[StorageService]	
storageDID	DID of BCON storage service
signature	value signed with private key of BCON storage service throughout ownership certificate
downloadEndpoint	Endpoint of content download
accessLocation	Endpoint of BCON storage service database
reIssueEndpoint	Endpoint of reIssue ownership certificate

[step5 in fig. 4] 옥션 매니지먼트 컨트랙트에서 입찰함수가 실행되고 난 후 실행결과에 대한 receipt이 옥션 사용자 앱에 전송된다. 옥션 사용자 앱은 새로 갱신된 입찰정보를 토대로 화면을 업데이트하며 다른 구매자들 또한 실시간으로 갱신된 입찰가 및 경매정보를 확인할 수 있다.

3. End of the Auction

개별 콘텐츠에 대한 경매의 유효시간이 종료되면, 우선 해당 경매에 대한 정산이 이루어지고 해당 콘텐츠에 대한 두 가지 소유권 이전이 일어난다. 첫 번째는 해당 콘텐츠에 접근하여 콘텐츠를 다운로드할 수 있는 권한을 증명하는 소유권 증명서의 소유권 이전이며, 두 번째는 NFT 자체의 소유권 이전이다. 그림 5는 경매 종료 절차의 시퀀스 다이어그램이며, 각 번호는 해당 절차의 단계를 나타낸다. 또한, 표 3은 각 단계의 의사코드이며, 표 4는 단계 4와 7에 대한 컨트랙트 코드이다.

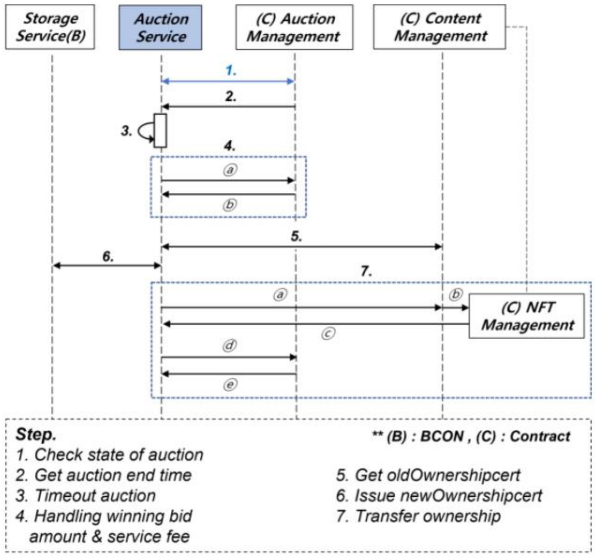

Fig. 5. End of the Auction Process

Table 3. Pseudo-code for [§fig. 5.]

Auction End Process(Auction server)
(C): smart contract of klaytn (B): BCON service *Request(target, data): Request the corresponding service including the data to the target
1: **REPEAT (1 minute)**
2: Get *auctionEndTime* from AuctionMangement(C)
3: **IF** *currentTime* > *autionEndTime*
4: **send Transaction** function sendLastBid in AuctionManagement(C)
5: Get *oldOwnershipcert* from ContentMangement(C)
6: *newOwnershipcert* = *NewOwnershipcert(stroage service(B), [buyerInfo, *oldOwnershipcert*])
7: **send Transaction** function changeOwnershipCert in ContentManagement(C)
8: **UNTIL** Auction end

Table 4. Contract Code for [§fig. 5. step 4,7]

Send last Bid to Seller & Transfer NFT Ownership process
_userDID: newly changed user DID _signature: newly changed signature data
Step 4. Send last Bid to Seller
1: Auction myAuction = auctions[_auctionID];
2: bidsLength = auctionBids[_auctionID].length;
3: Bid lastBid = auctionBids[_auctionID][bidsLength-1];
4: feeEx = (lastBid.amount*9)/10;
5: if(!myAuction.owner.transfer(feeEx)){
6: revert("cannot send");
Step 7. (1) Transfer OwnershipCert
7: ownershipCerts[_nft].ownerInfo.did = _userDID;
8: ownershipCerts[_nft].storageSvc.storageSignature = _storageSignature;
9: ownershipCerts[_nft].ownerInfo.history.push(_newOwnerAddress);
Step 7. (2) Transfer NFT
10: if(approveAndTransfer (prevOwnerAddress, _newOwnerAddress, _NFTManagermentAddr, _nft) {
11: // *approveAndTransfer()*
12: nftContract.approve(_newOwnerAddress, _nft);
13: nftContract.transferFrom(prevOwnerAddress, _newOwnerAddress, _nft);
14: delegations.isActivate = false; }

[step1-3 in fig. 5] 옥션 관리 서비스는 해당 경매의 진행 상태를 1초 간격으로 모니터링한다. 토큰 형태로 생성된 경매 유효시간을 지속적으로 검증한다.

[step4 in fig. 5] 경매 유효시간이 만료되면 옥션 관리 서비스는 경매가 종료되었다고 판단하여 옥션 매니지먼트 컨트랙트에 낙찰가 정산 트랜잭션을 보낸다. 트랜잭션을 받은 옥션 매니지먼트 컨트랙트는 판매자에게 해당 경매의 낙찰가를 전송하는데, 이때 서비스의 수수료인 낙찰가의 일부 금액을 제외한 최종 금액을 계산하여 판매자의 계좌로 전송하며 해당 경매에 대한 정산이 완료된다.

[step5-6 in fig. 5] 정산이 완료되면 해당 콘텐츠에 대한 소유권 이전 절차가 시작된다. 우선 소유증명서의 소유주 이전을 위해 옥션 관리 서비스는 콘텐츠 매니지먼트 컨트랙트에서 이전 소유주의 소유증명서를 가져온다. 이전 소유증명서와 해당 콘텐츠의 구매자 신원정보와 함께 BCON 콘텐츠 보관 서비스에 구매자의 새 소유증명서 발급을 요청한다. 요청을 받은 BCON 콘텐츠 보관 서비스는 BCON auth를 통해 구매자의 신원을 확인하고 이전 소유증명서가 변경되진 않았는지 검증한다. 모든 검증이 완료되면 새 소유증명서를 발급한다.

[step7 in fig. 5] 새 소유증명서를 발급받은 옥션 관리 서비스는 새 소유증명서와 함께 콘텐츠 매니지먼트 컨트랙트에 소유주 이전 트랜잭션을 보낸다. 콘텐츠 매니지먼트 컨트랙트는 새 소유증명서에서 구매자의 DID와 소유증명서 시그니쳐 값을 발췌해 이전 소유증명서에 해당 값을 변경하며 구매자로 소유증명서의 소유주를 이전한다. 마지막으로 콘텐츠 매니지먼트 컨트랙트는 NFT 매니지먼트 컨트랙트를 통해 NFT 소유주를 구매자 변경한다. 모든 절차가 완료되면 옥션 관리 서비스는 옥션 매니지먼트 컨트랙트에 경매 상태를 종료로 변경하며 최종적으로 경매가 종료된다.

4. Implementation

이 절에서는 NextAuction 서비스에서 경매가 진행되는 과정을 옥션 사용자 앱의 사용자 인터페이스 화면을 통해 설명한다.

(1) 경매 등록 및 생성

그림 6은 BCON 서비스에 업로드되어 있는 사용자의 콘텐츠 중에서 경매를 시작하기 원하는 콘텐츠를 클릭하면 나타나는 화면이다. 그림과 같이 입력 후 아래의 옥션 생성 버튼을 클릭하면 3장 1절의 Preparing for the Auction 과정이 일어난다.

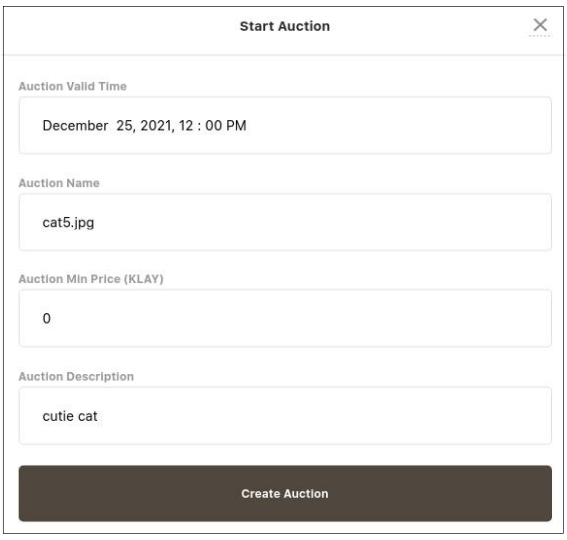

Fig. 6. Auction registration screen

그림 7은 옥션을 생성한 후 자신의 경매 페이지를 나타낸다. 해당 콘텐츠의 경매 상태가 Active로 변경된 것을 확인할 수 있다.

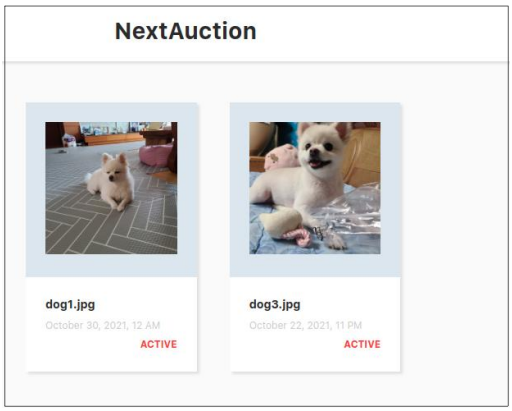

Fig. 7. User page in BCON Dapp after auction registration

(2) 경매 진행 및 입찰참여

그림 8은 콘텐츠 구매를 원하는 사용자가 옥션 사용자 앱에 접속했을 때 나타나는 메인 화면이다. 현재 경매가 진행 중인 콘텐츠들이 경매 생성시간 순으로 나열된다.

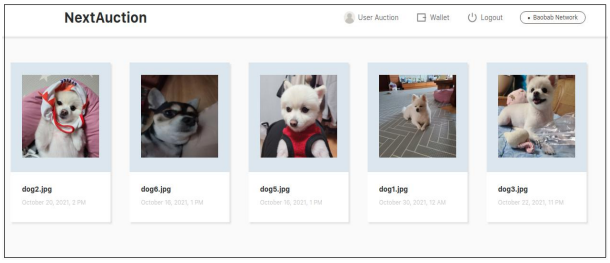

Fig. 8. Main page in Auction Dapp

그림 9는 그림 8의 화면에서 구매를 원하는 콘텐츠를 클릭한 뒤 나타나는 사용자 인터페이스를 나타낸다. 클릭한 콘텐츠에 대한 간단한 미리보기 이미지와 콘텐츠 이름 및 경매 생성시간, 최초 입찰금액, 경매 설명, 콘텐츠 제작자, 콘텐츠 현재 소유자 정보를 확인할 수 있다.

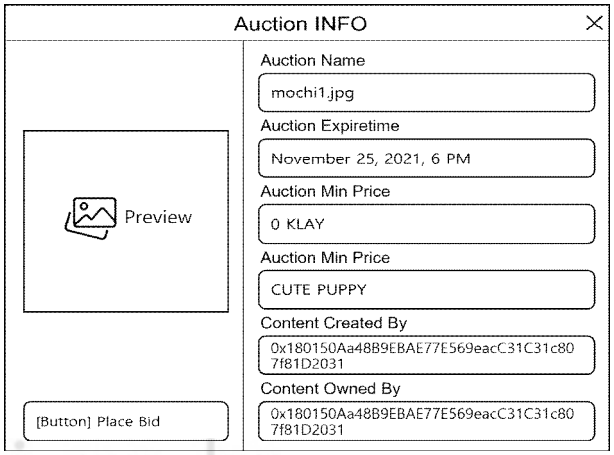

Fig. 9. UI of auction Information

그림 10은 그림 9에서 해당 경매에 입찰을 원하는 사용자가 좌측 하단의 입찰참여 버튼을 클릭하면 나오는 사용자 인터페이스이다. 좌측에는 해당 경매의 전체 입찰내역을 볼 수 있으며 우측에는 사용자가 원하는 입찰가를 입력하는 칸이 나타난다. 입력 후 입찰 버튼을 누르면 3장 2절의 In Progress Auction 과정이 일어난다.

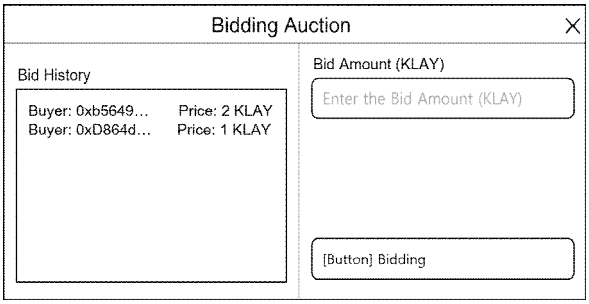

Fig. 10. UI of auction bidding

(3) 경매 종료

한 콘텐츠에 대한 경매의 유효시간이 끝나면 경매가 종료된다. 그림 11은 해당 콘텐츠를 판매한 사용자와 구매한 사용자가 자신의 경매 페이지에서 해당 콘텐츠를 클릭하면 나오는 사용자 인터페이스이다. 콘텐츠 이름과 설명, 최종 입찰자와 수수료를 제외한 경매 낙찰가 확인이 가능하다.

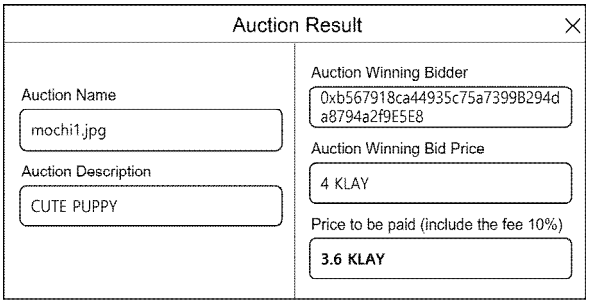

Fig. 11. UI of auction result

5. Test for Service Robustness

이 절에서는 NextAuction의 서비스 견고성을 검증하기 위하여 BR2K 기법을 사용하여 옥션 서비스를 복제 실행하고, Next Auction 테스트 서비스를 구축하고 그 실행결과를 제시한다. 테스트 서비스는 네트워크 장애 시에도 응용 서비스의 상태 복제의 정확성을 확인하기 위하여, 다음 작업을 10번 반복하여 수행한다. 그림 12는 테스트 환경을 보여주며 분산 환경을 구성하는 각각의 노드에 BR2K 기법을 적용한 하나의 옥션 서버를 실행한다.

(1) 판매자가 새로운 경매를 생성하면, 5명의 구매자가 해당 경매에 한 번씩 입찰하여, 총 5번의 입찰이 이루어진다.

(2) 입찰이 진행되는 중간에 리더 노드에 네트워크 장애를 발생시킨다.

(3) BR2K 프레임워크를 통해 자동으로 복구가 일어난다.

(4) 나머지 입찰이 끝나고, 경매의 유효시간이 종료될 때 리더 노드에 네트워크 장애를 발생시킨다.

(5) BR2K 프레임워크를 통해 자동으로 복구가 일어난다.

(6) 옥션 정보가 저장된 데이터베이스와 옥션 사용자 앱을 통해 경매가 정상적으로 종료되었는지 확인한다.

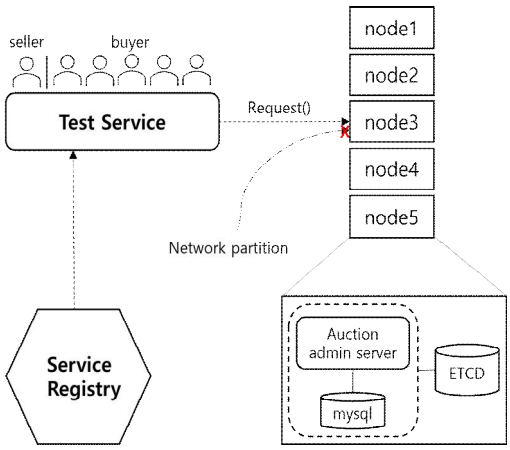

Fig. 12. Test environment

테스트를 위해 경매 서비스에 참여한 계정으로는 총 5명의 구매자와 1명의 판매자가 있다. 표 5는 각 참여자의 DID 계정을 나타낸다.

Table 5. DID Address of Users

User	DID Address
1-Buyer	did:kt:e9d8c44c1db4904d373de177df865699c233c456
2-Buyer	did:kt:a5e220216bcec60d5d4e6148b19411908183a3fe
3-Buyer	did:kt:dc8d6e9db113c475467b9bf472808397dd7f3bf8
4-Buyer	did:kt:dbbc4256e1234185c1610e34cb79fd5d9d106739
5-Buyer	did:kt:77ebc9d0e5ac26741756a956a55330175c886e0e
Seller	did:kt:180150aa48B9ebae77e569eacc31c807f81d2031

위 절차에 따라 10번의 테스트 중 5번의 결과를 아래의 표 6에서 나타낸다. 경매 서비스 중간에 네트워크 장애에도 BR2K 프레임워크를 통해 적절하게 서버 복구가 이루어졌으며, 모든 경매 서비스의 절차가 정상적으로 이루어졌다.

Table 6. Result of Test

NFT content type	Situation	Buyer	Time (sec)	Auction server ID	Result
Text	Bidding	1	4.23	4->2	success
	Done	3	6.34	2->1	
Image	Bidding	3	8.73	1->5	success
	Done	5	5.15	5->3	
Video	Bidding	3	3.63	3->2	success
	Done	1	10.15	2->4	
Music	Bidding	2	6.71	4->2	success
	Done	5	9.77	2->1	
Music	Bidding	1	7.33	1->3	success
	Done	2	4.79	3->4	
...					

**NFT content type* : *The types of contents subject to the auction.*
**Situation* : *The auction procedure where the network partition took place in the test.*
**Buyer* : *When a network partition occurs, the person who did the situations.*
**Auction Server ID* : *The server ID where the leader changed.*
**Time* : *Leader recovery time in case of network partition.*

V. Conclusions

본 논문에서는 DID 기술을 이용한 사용자들의 신원 인증을 통해 신뢰성 있게 개인의 콘텐츠에 대한 소유권을 거래할 수 있는 경매 서비스인 NextAuction의 개발에 대하여 기술하였다. NextAuction 서비스는 옥션 서비스와 NFT 매니지먼트 컨트랙트, 옥션 매니지먼트 컨트랙트 그리고 옥션 Dapp으로 구성되어있으며, 안전한 콘텐츠 관리를 보장하기 위하여 블록체인 기반의 콘텐츠 관리 서비스인 BCON을 확장하여 개발하였다.

NextAuction 서비스는 디지털 콘텐츠에 대해 NFT를 발급하여 블록체인을 통해 콘텐츠에 대한 소유권 증명을 지원하며, NFT에 명시된 소유권과 거래 이력을 통해 투명한 NFT 거래가 가능하다. NextAuction 서비스는 경매 전 과정을 통하여 DID를 이용해 사용자들에 대한 신원 인증을 투명하고 일관성 있게 제공하여 서비스 참여자에 대한 신뢰성을 높인다. 경매가 완료되면 낙찰자는 블록체인에 기록된 NFT 소유권 및 발급받은 소유증명서를 통해 콘텐츠에 대한 소유권 관리를 체계적으로 제어하고, 안전하고 신뢰성 있게 거래할 수 있다. 또한, BR2K 기법을 사용하여 옥션 서비스를 복제 실행함으로써 끊임없이 일관성 있는 서비스를 제공한다. 추후 정부 차원의 신원 증명 서비스와 본 논문의 DID 서비스를 연동하여 운영하는 방안을 모색하여 차세대의 NFT 경매 서비스의 상용화를 적극적으로 모색하고자 한다.

ACKNOWLEDGEMENT

This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(No. 2019R1I1A3A01052970)

REFERENCES

[1] Lennart Ante, “The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum,” BRL Working Paper Series No. 20, pp.1-9, June 2021. DOI: 10.2139/ssrn.3861106
[2] OpenSea, https://opensea.io/
[3] Klip Drops, https://klipdrops.com/
[4] D.S. Kwon, et al. "Digital Identity Trend for Digital Trust Society," Electronic communication trend analysis, Vol.34, No.3, pp.114-124, June 2019. DOI: 10.22648/ETRI.2019.J.340312
[5] HW Kim, et al. “BCON : Blockchain-based Content Management Service Using DID,” Journal of The Korea Society of Computer and Information, Vol.26, No.6, pp. 97-105, June 2021. DOI: 10.9708/jksci.2021.26.06.097
[6] Ground X, https://www.klaytn.com
[7] KIP-7, https://ko.docs.klaytn.com/smart-contract/token-standard
[8] MH Kwon, and MJ Lee. “BR2K : A Replication and Recovery Technique Using Kubernetes for Blockchain Services,” Journal of The Korea Society of Computer and Information, Vol.25, No.10, pp. 77-86, Oct 2020. DOI: 10.9708/jksci.2020.25.10.077
[9] MH Kwon, and MJ Lee. “Replication of blockchain application services using kubernetes and blockchain service registry,” Proceedings of the Korean Society of Computer Information Conference, pp. 363-364, July 2020.
[10] M. Wohrer, and U. Zdun, “Smart contracts: security patterns in the ethereum ecosystem and solidity,” Blockchain Oriented Software Engineering (IWBOSE) 2018 International Workshop on, pp.2-8, Mar 2018. DOI: 10.1109/iwbose.2018.8327565
[11] Truffle framework, https://etcd.io/
[12] Kubernetes, https://kubernetes.io/
[13] J. Shah, and D. Dubaria, “Building Modern Clouds: Using Docker, Kubernetes & Google Cloud Platform,” 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Mar 2019, pp.184-189, DOI: 10.1109/CCWC.2019.8666479
[14] MySQL, https://www.mysql.com/

Authors

Young-Eun Lee received the B.S degrees in IT convergence from University of Ulsan, Korea, in 2021. She is currently an M.S student in Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan. She is interested in blockchain technology, distributed computing, and Artificial Intelligence technology.

Hye-Won Kim received the B.S degrees in IT convergence from University of Ulsan, Korea, in 2021. She is currently an M.S student in Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan. She is interested in blockchain technology, distributed computing, and Artificial Intelligence technology.

Myung-Joon Lee received the B.S. degree in Mathematics from Seoul National University in 1980, and the M.S. and Ph.D. degrees in Computer Science from KAIST in 1982 and 1991, respectively.

Dr. Lee joined the faculty of the Department of Computer Science at University of Ulsan, Ulsan, Korea, in 1982. He is currently a Professor in the School of IT Convergence, University of Ulsan. He is interested in blockchain technology, distributed computing, and mobile/cloud service.