9-23-2022

NFT Certificates and Proof of Delivery for Fine Jewelry and Gemstones

Noura Alnuaimi
Khalifa University of Science and Technology

Alanoud Almemari
Khalifa University of Science and Technology

Mohammad Madine
Khalifa University of Science and Technology

Khaled Salah
Khalifa University of Science and Technology

Hamda Al Breiki
Zayed University

See next page for additional authors

Author First name, Last name, Institution
Noura Alnuaimi, Alanoud Almemari, Mohammad Madine, Khaled Salah, Hamda Al Breiki, and Raja Jayaraman

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

NFT Certificates and Proof of Delivery for Fine Jewelry and Gemstones

NOURA ALNUAIMI[1], ALANOUD ALMEMARI[1], MOHAMMAD MADINE[2], KHALED SALAH[1], (SENIOR MEMBER, IEEE), HAMDA AL BREIKI[3], RAJA JAYARAMAN[2]

[1]Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi, UAE.
[2]Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi, UAE.
[3]College of Technological Innovation, Zayed University of Science Technology, Abu Dhabi, UAE.

Corresponding author: Raja Jayaraman (e-mail: raja.jayaraman@ku.ac.ae)

ABSTRACT Fine jewelry is a unique class of ornaments composed of precious metals and gemstones. Premium-grade metals such as gold, platinum, and sliver, and gemstones such as pearls, diamonds, rubies, and emeralds are used use to make fine jewelry. Paper-based certificates are typically issued by retailers and producers for fine jewelry and gemstones as a proof of origin, sale, ownership, history, and quality. However, paper certificates are subject to counterfeiting, loss, or theft. In this paper, we show how non-fungible tokens (NFTs) and Ethereum blockchain can be used for digital certification, proof of ownership, sale history, and quality, as well as proof of delivery for fine jewelry and gemstones. We present the proposed system design and architecture with sequence diagrams covering key interactions for jewelry production, purchase, and sale, along with algorithms related to NFT minting, auctioning, ownership management, and physical delivery. We demonstrate that our proposed NFT and blockchain-based solution can provide superior alternative in terms of verifiability, traceability, immutability, and security when compared with paper-based certification and traditional auctioning, delivery and ownership management. We make our developed smart contracts and testing scripts publicly available on GitHub.

INDEX TERMS Blockchain, NFTs, Ethereum, Fine Jewelry, Gemstone, Proof of Delivery, Digital Certificates

I. INTRODUCTION

Precious gemstones and metals are the most valuable materials for making fine jewelry and other ornaments. The precious stones are obtained from minerals, rocks, living organisms, and metal alloys [1]. The characteristics of such materials, like rarity, durability, size, color, clarity, and shape, influence their value. For example, diamonds are one of the most rigid and durable minerals, and their rarity comes from their slow formation in the Earth's crust for over three billion years, making them extremely expensive [2, 3]. Natural pearls, on the other hand, grow accidentally in a living organism, such as oysters, without human intervention. As a result, a natural pearl formation takes six to four years [4].

Gemstones go on a long journey from mining to polishing before being used in fine jewelry. The current diamond or pearl industry lacks adequate transparency, and traceability of the gemstone used for a specific piece of jewelry [5, 6]. Customers have the right to know the mining source of a purchased diamond, as they are becoming less compromising on ensuring their fine jewelry is sourced ethically [7]. An issue called *Blood Diamonds* in Africa has introduced concerns regarding the non-ethical approach to mining diamonds. Rebel organizations are mining diamonds in war zones, indirectly resulting in customers supporting the conflicts through their purchase [8].

Natural pearls face a different issue these days. The value of a natural pearl depends on its quality and scarcity. In the late 1800s, Kokichi Mikimoto changed the pearl industry by introducing the first cultured pearl [4]. Cultured pearls grow with the help of human intervention. Farms intentionally insert foreign materials into an oyster and mollusk to produce up to thirty pearls per oyster. On the other hand, a natural pearl forms when a foreign object enters the oyster, triggering its defensive mechanism that produces the pearl. By creating pearl farms, workers can drastically increase the number of pearls harvested, thus decreasing the scarcity aspect of pearls. In addition, cultured pearls are known to have lower quality and variety when compared to natural ones.

Traditional methods of verifying the quality and value of a gemstone use paper certificates, which add a trusted-third

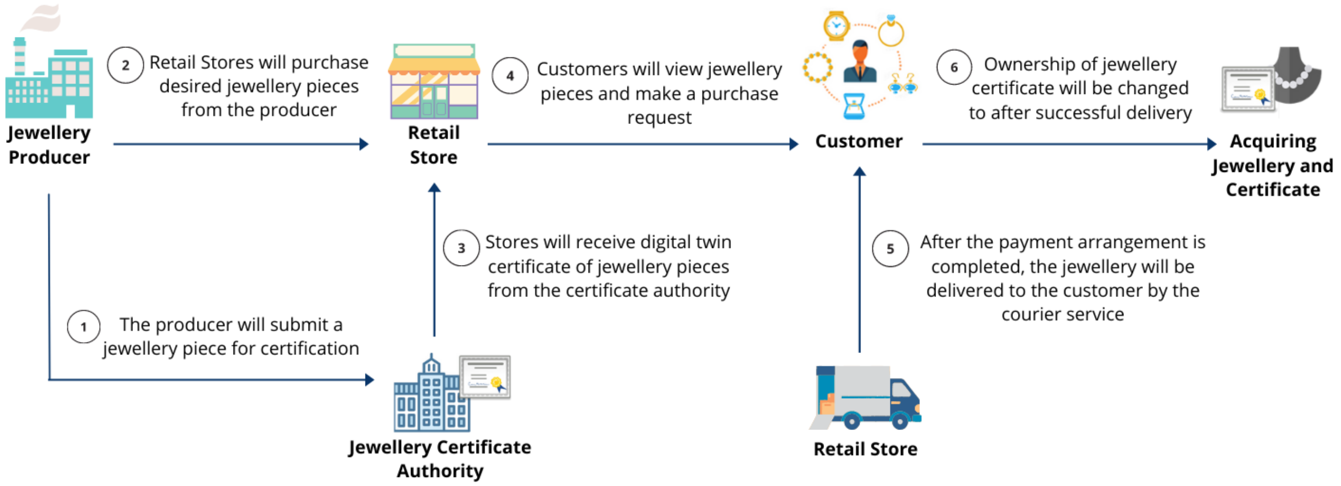

Jewellery Producer
2 Retail Stores will purchase desired jewellery pieces from the producer
Retail Store
4 Customers will view jewellery pieces and make a purchase request
Customer
6 Ownership of jewellery certificate will be changed to after successful delivery
Acquiring Jewellery and Certificate
3 Stores will receive digital twin certificate of jewellery pieces from the certificate authority
5 After the payment arrangement is completed, the jewellery will be delivered to the customer by the courier service
1 The producer will submit a jewellery piece for certification
Jewellery Certificate Authority
Retail Store

FIGURE 1. A typical purchasing process flow for fine jewelry from producer to customer

party issue. Those certificates include limited information that explicitly describes the gemstone features, such as the weight, type, and color [9]. A customer must trust the centralized system that issues the value certificate to the gemstone. A centralized system lacks traceability and transparency of the gemstone from mining to purchasing. For fine jewelry that has a high value, customers and buyers look for their assurance of being of high quality and the authenticity of their history, and whether these goods originated from a natural source. However, maintaining transparency in the trading process of such high-value precious items as diamonds and natural pearls is difficult. Thus, trust plays a critical role in trading gemstones, making the idea of open trading of gems extremely challenging [10].

Using a blockchain-based ledger can overcome the traditional methods that lack transparency. Blockchain works by keeping a list of transactions in a block [11]. A block contains a header and a body. The header includes the previous block's hash, thus linking the blocks together and creating a chain. This method provides an immutability feature where it is difficult to tamper with the data stored in the blockchain. In addition, blockchain is decentralized since it does not have a central trusted authority, nor a trusted-third party is required to verify the transactions. A way to customize transactions in a blockchain is by implementing smart contracts [12]. Smart contracts are self-executing codes that monitor and manage transactions. Blockchain has proved to be a secure way to store and share data. For example, several fields implement it as the basis of their applications, such as managing autonomous vehicles, healthcare applications, supply chain management, and waste processing management [13–18]. The immutable feature of the blockchain ledger helps keep unchanged traces of the entire process flow in the fine jewelry industry and limits fraudulent activities. With blockchain, customers and entities can know every stage and process when purchasing jewelry, thus creating a more traceable record and encouraging ethical sourcing of its gemstones and metals [19, 20].

On top of the blockchain implementation to facilitate the gemstone supply chain, non-fungible tokens (NFTs) can be employed to create digital assets and certificates that correspond to the physical gemstone [21]. NFTs are *non-fungible*, meaning each token is unique and cannot be exchanged for another [22]. Each NFT has a single owner and is backed by the blockchain, which adds value and traceability to the ownership of the digital asset [23]. Today, the NFTs market is estimated to be worth USD 1.2 billion [24]. One of the prominent areas that leverage NFTs is creative work. For example, the fashion industry uses NFTs by providing digital assets of their physical counterparts that can be used in the virtual world [24]. Similarly, NFTs can be useful to encode the features of precious stones and metals, provide identification and quality assurance, and help customers avoid purchasing fine jewelry from fraud organizations, thus ensuring a the purchase of a legitimate piece.

In addition to blockchain and NFTs, further work must be done to ensure the safe delivery of the jewelry pieces to the consumers before transferring the NFT ownerships. Various technologies being developed under the web3 umbrella can help guarantee the delivery of physical assets. Such technologies include decentralized storage and dispute resolution protocols [25].

Figure 1 illustrates the purchasing process flow of a purchase from *Jewelry Producer* to *Customer*. The figure has been created by adapting process flows in the diamond industry and generalizing it to suit a process flow of purchasing jewelry pieces [9, 10]. Integrating blockchain, NFTs, and proof of delivery can establish a trustworthy network for managing valuable assets. This paper proposes a decentralized solution to issue digital certificates for fine jewelry and gemstones, and guarantee their delivery throughout the supply chain. Our proposed approach utilizes Ethereum blockchain network, in which our developed smart contracts operate to manage proof of ownership and proof of delivery for valuable assets. The primary contributions of our work can be summarized as follows:

- We present a system that leverages NFTs and blockchain to provide digital certification, proof of ownership, and proof of delivery for fine jewelry and gemstones.
- We incorporate ERC-721 and marketplace smart contracts to trace and manage ownership of jewelry and allow fully decentralized bidding and sale of fine jewelry and gemstones, with proof of delivery and secure transfer of NFTs.
- We demonstrate our proposed approach by defining the system stakeholders, presenting the system architecture overview, and illustrating the interactions among stakeholders in three use case scenarios with sequence diagrams.
- We lay out and explain algorithms to manage issuing ERC-721 NFTs for fine jewelry, conduct auctions, and establish and approve a physical delivery of the assets. Further, we implement the algorithms into Ethereum-based smart contracts and deploy them for extensive testing. We make our code publicly available on GitHub [1].
- We evaluate our solution and assess its feasibility by executing cost and security analysis for minting and bidding jewelry NFTs and explore generalization potential beyond the industry of physical valuable assets. Finally, we show how our solution is a superior alternative compared to prior studies, in terms of verifiability, trust, and reliability.

The remaining of this paper is organized as follows: Section II presents related work, followed by our proposed NFTs solution in Section III. Then, Section IV describes our implementation details, which we assess and discuss in Section V and Section VI. Finally, Section VII concludes and summarizes this paper.

II. RELATED WORK

This section covers related work where blockchain and NFTs were used to build or assess the supply chain of fine jewelry and gemstones. However, to our best knowledge, no proposed implementation uses NFTs to trace the ownership of valuable assets.

A. BLOCKCHAIN-BASED APPLICATIONS FOR JEWELRY

A work done by Cartier et al. focuses on tracing diamonds by implementing a generalized traceability blockchain [5]. Firstly, stone information is added to the blockchain, such as mining location, photo, and weight. Next, a block is produced within the blockchain, and the stone is assigned a unique ID number. Then, the rough stone is purchased by a gemstone cutter, and the blockchain is updated with new information about the new cut and polished stone. After that, the cut stone is purchased and mounted in a ring for retail sale by a jeweler. In the production stage, the blockchain is updated with the new information about the ring. Finally, the ring is purchased by a customer. The consumer may be given documentation about the precious item that may include a unique ID to visualize specific aspects of the history on a specialized platform. If requested, the consumer identity can also be stored on the blockchain as proof of ownership. This approach provides transparent tracking and traceability for consumers, auditors, or companies. However, the paper leaves room for further details to be investigated, considering various factors that may affect security, diamond certification, and delivery. This approach was studied by Dasaklis et al. [26], among other supply chain traceability implementations, in which the authors discovered a general lack of implementation and deployment details in the studies, in addition to calling for newly developed solutions to perform tests in real-life environments.

When actors and processes increase, a blockchain-based system gets complicated to manage and design. A compelling work by Kanak et al. introduces a Diamond Accountability Model (DAM) that provides information on designing blockchain-based solutions [27]. The researchers propose a solution comprising three main layers: user level, operational level cyber-physical systems (CPSs), and authorized coordination level. Most importantly, data exchange and manipulation techniques are implemented in CPS. The DAM system comprises many partnering organizations, each with its own CPS that generates data. Therefore, blockchain is used to store data and prevent manipulation. Meanwhile, an authorized coordinator begins receiving data and storing it in a secure database. However, when data verification is required during the functioning of CPSs, the coordinator verifies if the partner is authenticated before sending the data. Next, each partner hashes the corresponding data and confirms the validity of the smart contract operations. Generally, the proposed approach can be applied for various applications with a flexible range of partners and CPSs. However, this approach requires further enhancements to the privacy and security aspects.

B. PROOF OF DELIVERY FOR JEWELRY

The supply chain system based on blockchain consists of a trade chain and an information chain platform [28]. The critical functionality of the trade chain platform is to regulate the trading process between supply chain companies, during which a trade smart contract verifies the authenticity and completion of a transaction. Additionally, when a transaction is completed, the trade chain platform logs the start time, parties involved, completion status, and other details and makes them available to supply chain companies. However, Information management is responsible for the information chain platform. The supply chain platform stores relevant data about the products in the supply chain. Also, the whole life cycle of a product can be traced using recorded product information. Based on the results obtained, the system meets essential supply chain criteria but must improve throughput and security and ensure the physical delivery to customers.

Authors in [29] provided a proof of delivery system that

[1] https://github.com/AnonGitter20220902/nft-for-jewels

creates a trusted, secure, decentralized, and accountable permissionless Ethereum blockchain. The system uses Ethereum smart contracts to prove the delivery of a sent item between a seller and a buyer, regardless of how many intermediate carriers are required. The use of double deposit collateral incentivizes all participating companies to perform honestly. Automated Ether payment is a critical component of their solution that ensures that each entity receives its intended portion of Ether upon successful delivery. An arbitration mechanism is also included if a dispute emerges throughout the shipping process.

Proof of digital assets delivery system in [30] provides a decentralized system using the Ethereum blockchain. The system uses fundamental aspects of blockchain and Ethereum smart contracts to provide immutable and tamper-proof logs, accountability, and traceability. Ethereum smart contracts coordinate and manage all interactions and transactions, including automatic payments in Ether cryptocurrency among customers, digital content providers, and the file server storing the digital material. This system includes a mechanism for resolving disagreements among participants. A secure off-chain download phase involving the file server and customers is part of the solution. Furthermore, the solution uses the advantages of the InterPlanetary File System (IPFS) to store the terms and conditions that the smart contract actors have agreed to.

III. OUR PROPOSED SOLUTION

In this section, we present our proposed solution that utilizes the Ethereum blockchain, NFTs, IPFS, and smart contracts to trace, perform transactions, and create digital certificates for fine jewelry and gemstones. We embrace the Ethereum blockchain to utilize its programmable nature and target the jewelry production, bidding, and delivery industry with smart contracts. Moreover, our system eliminates all trusted centralized authority requirements and provides security, high integrity, reliability, traceability, and transparency.

Unlike traditional solutions, the change of fine jewelry ownership is done in an automated and secure way without the need for any visits to shops or certificate authorities. Moreover, the physical delivery of the assets is done through courier services, which are an integral element of the on-chain system and play a role in the suggested solution, which improves the trust and security and the accuracy with which conflicts are resolved.

A. GENERAL SYSTEM OVERVIEW

The smart contracts built on Ethereum help keep a secure, traceable record of fine jewelry ownership. Our proposed framework focuses on creating smart contracts available for the general public to call functions that support the standard NFTs operations. Once deployed, smart contracts are considered immutable since they are shared with all mining nodes of the blockchain network. A mining node is considered a machine that captures all the network transactions to execute and validate them. The mining nodes then solve a consensus algorithm like the proof-of-work to mine a new block to the chain. Each mining node has an identical copy of the entire list of blocks. Actors in the system can use the front-end Decentralized Applications (DApps) to call the smart contract functions. Application programming interfaces such as Infura help connect the DApps with the Ethereum network containing the smart contracts. Generally, each entity interacting with the smart contracts requires a customized DApp for its specified use case. Events in smart contracts help notify all the participating actors in the system of alerts from function processes.

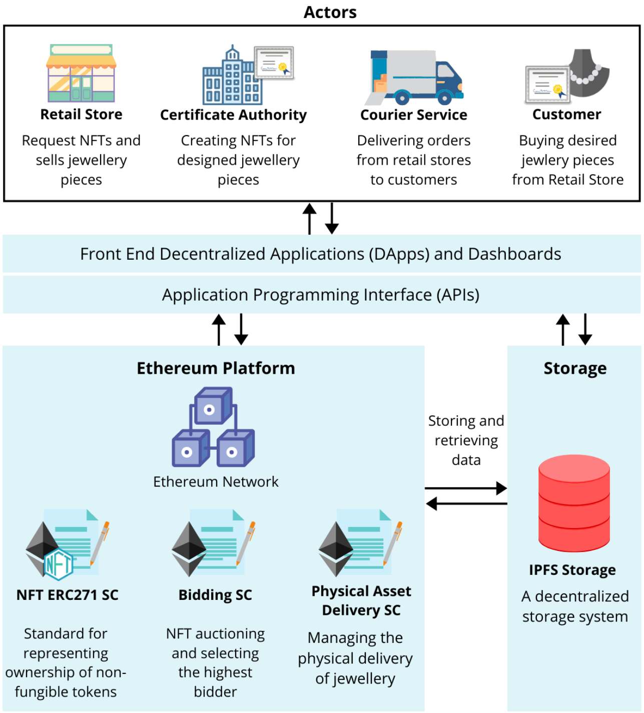

Actors
Retail Store
Request NFTs and sells jewellery pieces
Certificate Authority
Creating NFTs for designed jewellery pieces
Courier Service
Delivering orders from retail stores to customers
Customer
Buying desired jewlery pieces from Retail Store
Front End Decentralized Applications (DApps) and Dashboards
Application Programming Interface (APIs)
Ethereum Platform
Ethereum Network
NFT ERC271 SC
Standard for representing ownership of non-fungible tokens
Bidding SC
NFT auctioning and selecting the highest bidder
Physical Asset Delivery SC
Managing the physical delivery of jewellery
Storing and retrieving data
Storage
IPFS Storage
A decentralized storage system

FIGURE 2. A general system overview of the proposed NFT-based system architecture for fine jewelry management

Our proposed system aims to transfer and trace fine jewelry NFT ownership. Figure 2 illustrates the system architecture and gives a general overview of our work. The participating actors are shown in the figure. They include the *Certificate Authority*, Jewelry *Retail Store*, *Courier Service*, and *Customer*. The actors use the DApps to communicate with the Ethereum Virtual Network. Each participating entity has a unique Ethereum Address (EA) used to call the functions of the smart contracts. An Ethereum Address is created by hashing the public key of the actor. Each Ethereum account contains a public-private key pair used to sign and verify transactions digitally. Building the framework on Ethereum helps provide anonymity, transparency, and integrity to all transactions.

The proposed framework consists of three smart contracts (SCs). The first smart contract is the ERC-721 NFT SC, which contains predefined functions from the ERC-721 library that help mint and manage NFTs. The second SC, the

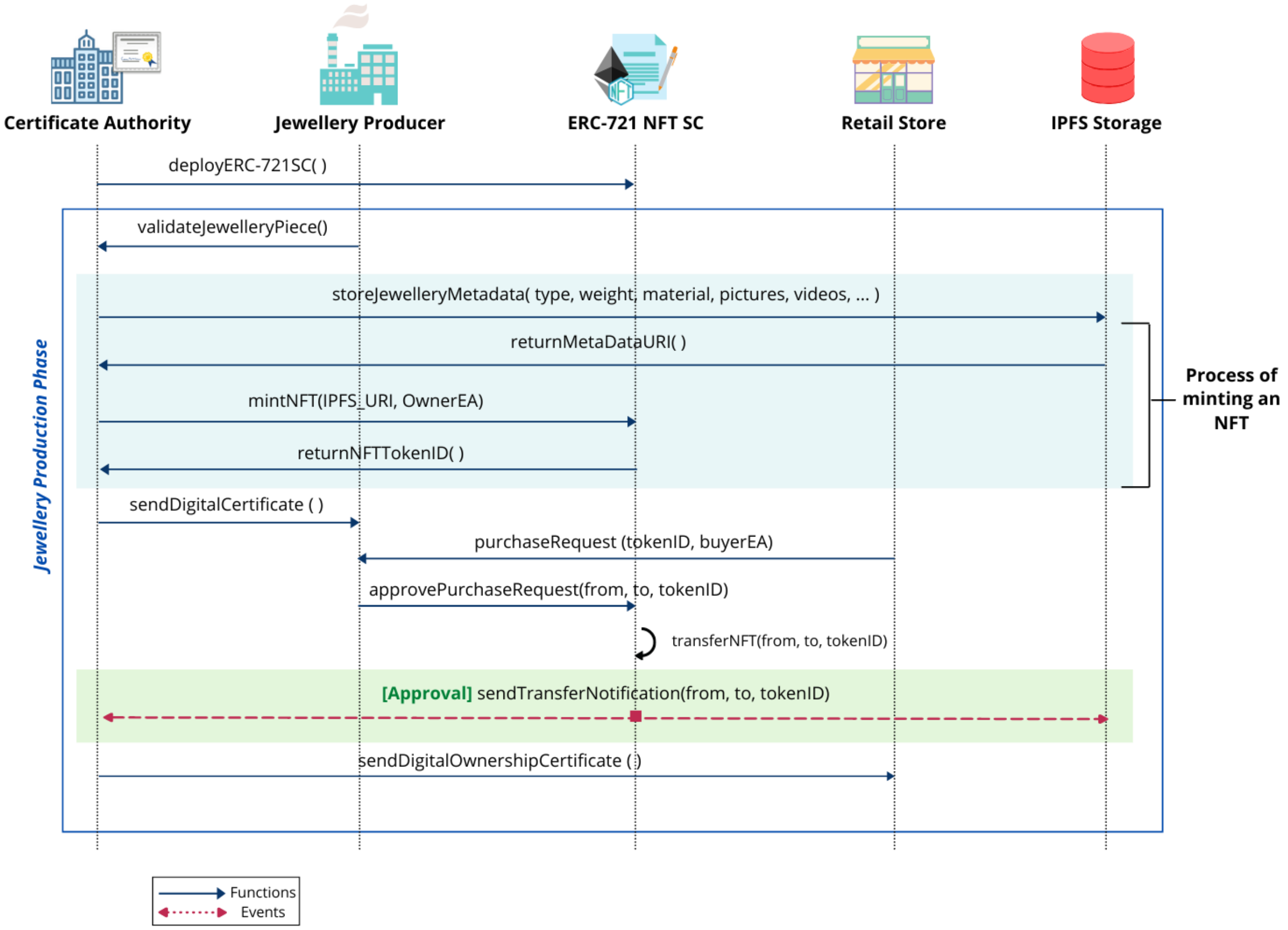

Certificate Authority
Jewellery Producer
ERC-721 NFT SC
Retail Store
IPFS Storage
deployERC-721SC( )
Jewellery Production Phase
validateJewelleryPiece()
storeJewelleryMetadata(type, weight, material, pictures, videos, ...)
returnMetaDataURI( )
mintNFT(IPFS_URI, OwnerEA)
returnNFTTokenID( )
Process of minting an NFT
sendDigitalCertificate ( )
purchaseRequest (tokenID, buyerEA)
approvePurchaseRequest(from, to, tokenID)
transferNFT(from, to, tokenID)
[Approval] sendTransferNotification(from, to, tokenID)
sendDigitalOwnershipCertificate ( )
Functions
Events

FIGURE 3. Sequence diagram showing the interactions of actors during the fine jewelry production phase

Bidding SC, consists of rules defined to create a jewelry auction. Through it, *Retail Stores* create an auction by displaying an item that *Customers* can view. Once the auction begins, *Customers* call the bidding function to set a desired bidding amount for the jewelry piece. Later, the SC finds the highest bidder and announces the winner. Physical Delivery SC is the last SC in our design. Functions from this smart contract are influenced by the work done in [29, 30]. This smart contract manages the delivery services to ensure a safe and secure package delivery. Lastly, our design leverages decentralized storage to establish a framework possessing completely decentralized properties. All fine jewelry and gemstones data are stored as NFT metadata in the decentralized storage.

B. SEQUENCE DIAGRAMS

Actors in the system communicate with the smart contracts by calling functions and sharing their EAs. The sequence diagrams describe the flow of processes in purchasing and owning a jewelry piece. Figure 3 displays the sequence diagram illustrating the interactions in the first phase of the system. The *Certificate Authority* needs to deploy the ERC-721 SC as a first step. Then, *Jewelry Producers* submit their jewelry pieces for checking and validation to generate a digital certificate. Next, the *Certificate Authority* extracts the metadata related to the jewelry piece and stores it in the IPFS storage. Attributes such as the jewelry identification number, IPFS reference, and the owner EA get shared with the SC to mint the NFT. The *Retail Store* then purchases jewelry pieces from the *Jewelry Producer* and receives the digital ownership of the jewelry NFT. Finally, an event gets triggered to announce that the NFT ownership has been changed.

Figure 4 presents the sequence diagram of the interactions during the jewelry bidding phase. First, the *Retail Store* deploys the Bidding SC and initiates a new jewelry auction. This action triggers an event to notify all the *Customers* that an auction for the specified jewelry piece has begun. Interested *Customers* view the event and send bidding requests to the Bidding SC. The SC calculates the highest bidder, stores the value sent by the *Customer*, and sends an event to notify the actors of the winning bidder. The *Retail Store* then approves the *Customer* and launches an event that a delivery service is required to deliver the jewelry piece. Figure 5 displays both the physical delivery phase and the NFT ownership transfer phase. A *Courier Service*

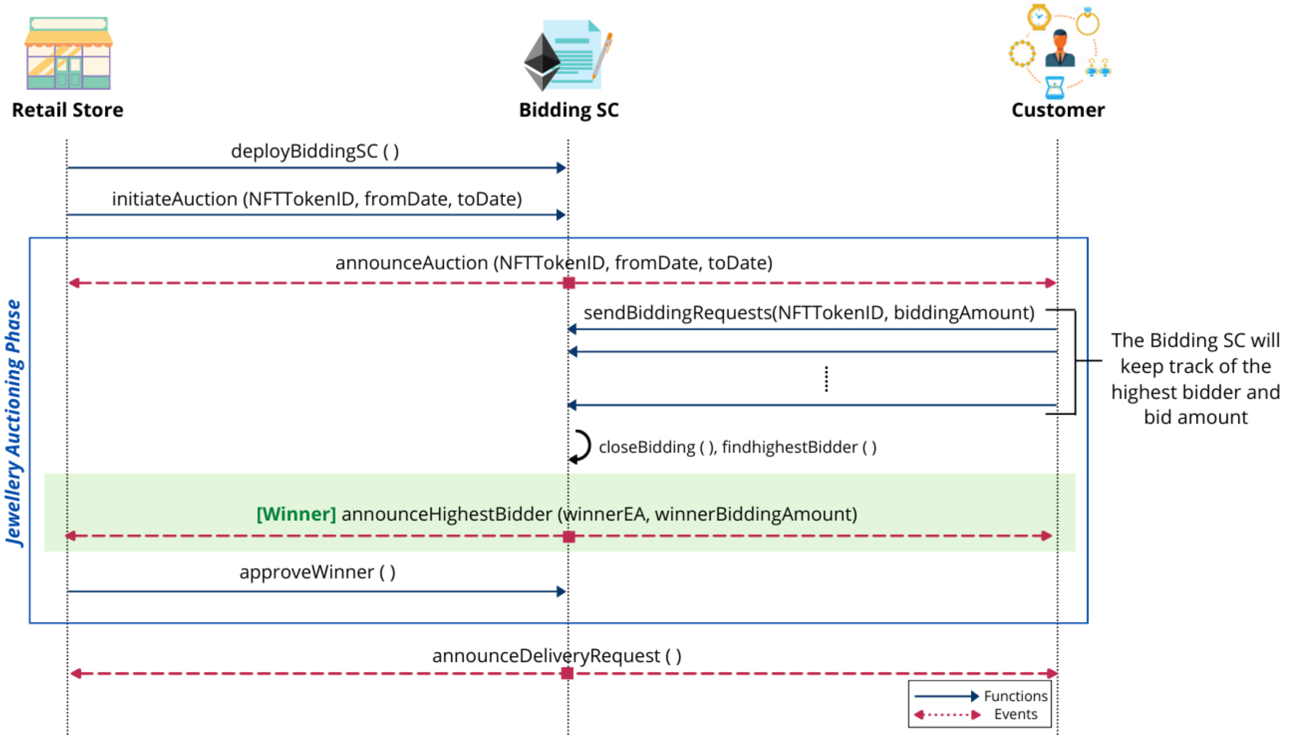

Retail Store
Bidding SC
Customer
deployBiddingSC ( )
initiateAuction (NFTTokenID, fromDate, toDate)
Jewellery Auctioning Phase
announceAuction (NFTTokenID, fromDate, toDate)
sendBiddingRequests(NFTTokenID, biddingAmount)
The Bidding SC will keep track of the highest bidder and bid amount
closeBidding ( ), findhighestBidder ( )
[Winner] announceHighestBidder (winnerEA, winnerBiddingAmount)
approveWinner ( )
announceDeliveryRequest ( )
Functions
Events

FIGURE 4. Sequence diagram showing the interactions of actors during the bidding phase

views the delivery request event, notifies the *Retail Store* by communicating with the Physical Asset Delivery SC, and sends the security deposit fee required to start the delivery process (the *Customer* also needs to send a security deposit). The beginning of the delivery process is broadcasted as an event, and the *Courier Service* physically starts to deliver the package. Upon successful delivery, the *Customer* needs to approve that the package has been delivered successfully by contacting the Physical Assets Delivery SC. The security deposits are returned to the *Courier Service* and the *Customer* upon successful delivery. Also, the bidding amount sent by the *Customer* gets transferred to the *Retail Store*. The NFT token transfer is completed once the requirements have been met, and the new owner of the fine jewelry NFT becomes the *Customer* who won the auction.

C. SYSTEM DESIGN

As shown in Figure 2 previously, there are a total of four main participating actors plus *Jewelry Producers*. Each participating actor has a specified role in the system and in interacting with the smart contracts. The roles of the actors are summarized below:

Jewelry Producer: The *Jewelry Producer* customizes and manufactures jewelry pieces, such as necklaces, rings, earrings, and bracelets. Each jewelry piece has its own attributes, including the type of gemstones and metals used. Then, the *Jewelry Producer* submits the jewelry piece to the *Certificate Authority* to assess it and generate a digital twin certificate using an NFT.

Certificate Authority: The *Certificate Authority* creates digital certificates by building a digital twin of the jewelry piece using NFTs. The NFT contains metadata that is stored on IPFS.

Retail Store: The *Retail Store* purchases jewelry pieces from the *Jewelry Producer*, the NFT gets transferred from the *Jewelry Producer* to the *Retail Store*, and the *Retail Store* receives the digital ownership of the fine jewelry NFT.

Courier Service: *Courier Services* are called by the *Retail Store* to deliver the jewelry piece to the *Customer* who purchased it. The delivery is based on the geographical location of the buyer.

Customer: A *Customer* views the jewelry pieces auctions of the *Retail Store* and bids for items to purchase. Upon a successful purchase, the *Customer* is the new owner of the jeweler NFT.

All contributing actors communicate through smart contracts in the Ethereum network. There is a total of three smart contracts in the proposed system. The *Jewelry Producer* first designs and manufactures a jewelry piece. The jewelry has its metadata which includes: jewelry type, metals used, gemstones used, and manufacturing date. The metadata gets uploaded to the IPFS decentralized storage. In addition, information such as a video capturing all angles of a jewelry piece can be added to the IPFS storage. The *Jewelry Producer* then submits the jewelry piece to the *Certificate Authority* to generate a digital certificate for the jewelry by using NTFs. The jewelry NFTs include the address of their

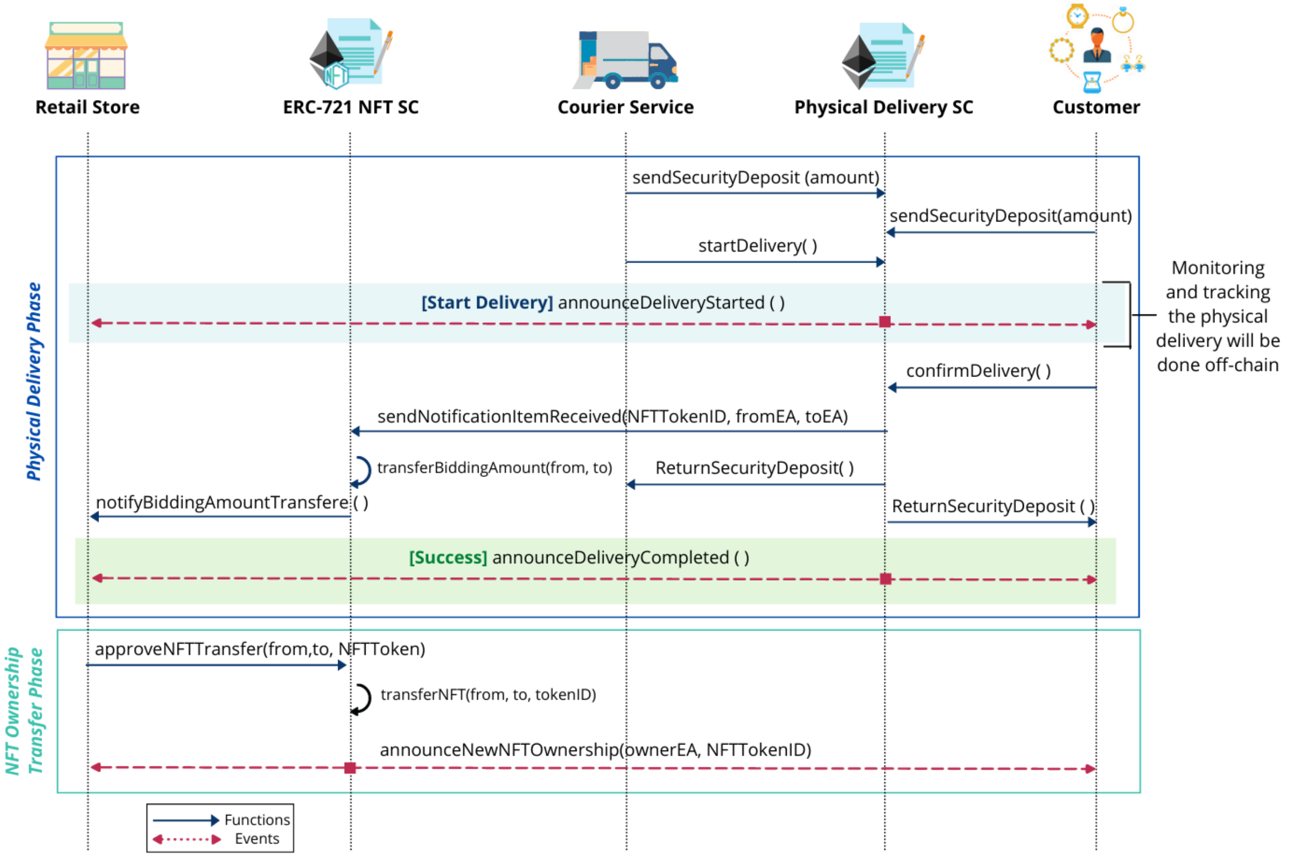

Retail Store
ERC-721 NFT SC
Courier Service
Physical Delivery SC
Customer
Physical Delivery Phase
sendSecurityDeposit (amount)
sendSecurityDeposit(amount)
startDelivery( )
[Start Delivery] announceDeliveryStarted ( )
Monitoring and tracking the physical delivery will be done off-chain
confirmDelivery( )
sendNotificationItemReceived(NFTTokenID, fromEA, toEA)
transferBiddingAmount(from, to)
ReturnSecurityDeposit( )
notifyBiddingAmountTransfere ( )
ReturnSecurityDeposit ( )
[Success] announceDeliveryCompleted ( )
NFT Ownership Transfer Phase
approveNFTTransfer(from,to, NFTToken)
transferNFT(from, to, tokenID)
announceNewNFTOwnership(ownerEA, NFTTokenID)
Functions
Events

FIGURE 5. Sequence diagram showing the interactions of actors during the physical delivery phase and the transfer of NFT ownership

Jewelry Producer and the metadata of the jewelry. Once the NFT is minted, the jewelry piece can be sold physically with its NFT digital twin to a *Retail Store*. A *Customer* views *Retail Store* auctions on jewelry pieces and bids on the desired piece to buy. When the auction ends, and the winning bidder is announced, the *Courier Service* gets notified of a delivery process. Information about the *Customer* and the delivery location get shared with the *Courier Service* to ensure safe delivery from the *Retail Store* to the *Customer*. Security deposits by the *Customer* and the *Courier Service* are made to ensure policy compliance and that the actors are not committing violations. Once delivery is completed, the security deposits are returned to both the *Customer* and *Courier Service*. When the *Retail Store* receives the purchase amount, the NFT ownership of the jewelry piece purchased gets transferred to the *Customer*.

D. NFT TOKEN CREATION

Tokenization is the process of creating digital assets, and in Ethereum, there are two mainstream standards to tokenize assets: ERC-20 and ERC-721. ERC-721 allows the freedom of creating unique token IDs, a feature not found in ERC-20. NFTs are popular in gaming and digital art. However, in our implementation we use NFTs to create digital certificates for jewelry and gemstones. As described before, *Jewelry Producers* submit jewelry pieces to *Certificate Authorities*, where the jewelry metadata gets generated based on the assessment performed by the *Certificate Authority*. The metadata of the jewelry piece includes description details such as the jewelry type, material used, weight, and dimensions. Other metadata may include pictures and videos taken of the jewelry piece. Storing large files of the jewelry metadata is costly on the ledger. Thus IPFS storage system is utilized. A URL link is obtained from the IPFS storage and used as a reference to the NFT metadata. The *Certificate Authority* generates the jewelry NFT and provides ownership to the *Jewelry Producer*. The jewelry NFT ownership is then transferred based on the ERC-721 standards once a *Retail Store* or a *Customer* purchases a physical twin of the NFT.

IV. IMPLEMENTATION DETAILS

In this section, we describe the functions and algorithms used to perform the requirements of our proposed NFT-based solution. The blockchain ledger is built on the Ethereum platform during implementation, and smart contracts are written using Solidity language. First, Algorithm 1 describes the process of minting a new NFT, a feature exclusive to the *Certificate Authority*. The algorithm takes in the EA of the NFT owner, which is initially set to the *Jewelry Producer*. Additional input information includes the fine jewelry serial number and

Algorithm 1: ERC-721 and NFT management

```
Input: ItemSN, URI, NFTOwnerEA
NFTOwnerEA: Ethereum address of the owner
ItemSN: Serial number of the jewelry piece
URI: IPFS of the jewelry metadata
Modifier: onlyCertificateAuthority
Generate TokenID
Call mint(NFTOwnerEA, TokenID)
Call setTokenURI(TokenID, URI)
Map ItemSN $\rightarrow$ TokenID
Emit an event to announce the creation of a new
  jewelry NFT
Return: TokenID
```

Algorithm 2: Creating a jewelry auction

```
Input: BiddingTime, CustomerEA, CustomerBid
BiddingTime: Total time allowed for bidding
CustomerEA: Address of the bidding customer
CustomerBid: Bidding amount provided by the
  customer
AuctionClose $\leftarrow$ CurrentTime + BiddingTime
Call StartAuction()
if $CustomerBid > TopBid$ then
    TopBid $\leftarrow$ CustomerBid
    TopBidder $\leftarrow$ CustomerEA
end
Emit an event to announce the highest bidder once the
  bidding time is over
```

Algorithm 3: Establish physical delivery of jewelry

```
Input: BuyerEA, ItemSN, CourierEA
BuyerEA: Ethereum address of the customer
CourierEA: Ethereum address of the courier
Call approve(BuyerEA)
if Buyer pays deposit and Courier pays deposit then
    Emit an event to announce the creation of a new
      delivery request
end
```

Algorithm 4: Approve delivery and transfer NFT ownership

```
Input: BuyerEA, CourierEA, RetailEA, TokenID,
  Approved
Retail: Ethereum address of the retail store
Approved: Decision of the customer based on the
  delivery
if Approved then
    Transfer securityDeposit to Buyer and Courier
    Transfer biddingAmount to Retail
    Call transfer(Retail, Buyer, TokenID)
    Transfer biddingAmount to Retail
    Emit events to announce successful delivery and
      transfer of jewelry NFT
else
    Emit an event to notify a failed delivery
end
```

the IPFS link that includes the jewelry metadata. Eventually, predefined functions from the ERC-721 library are called to formally mint the NFT, after which an event is triggered at the end to notify the entities in the network that a new jewelry piece with its digital twin NFT has been added.

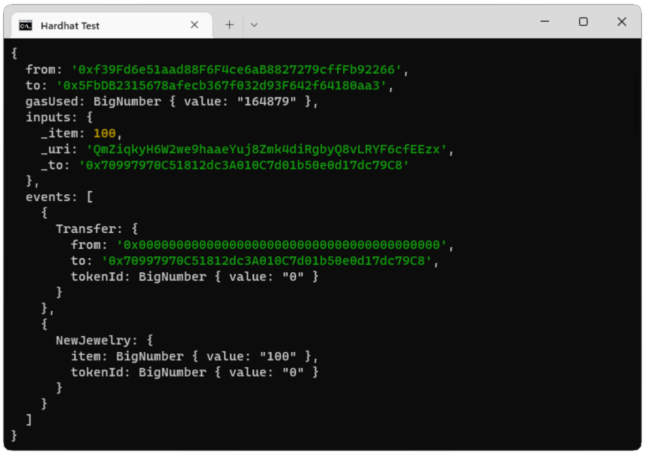
After the winner is announced, the *Retail Store* approves the *Customer* as a purchaser of the jewelry piece. Algorithm 3 describes the process of establishing a delivery request. First, an event is triggered to notify *Courier Services* that a new delivery request has been created. The *Courier Service* needs to pay a security deposit amount of 1 Ether to take in the request. Next, the *Customer* needs to pay a security deposit of 1 Ether to establish the delivery process. The security deposits are saved in the smart contract until the delivery is completed. A final event gets sent to notify that the physical delivery has started.

The Bidding SC includes methods that create rules for the fine jewelry auctions. Algorithm 2 presents the bidding algorithm used. The *Retail Store* establishes a jewelry auction by providing the bidding time. During the bidding time, bidders participate by calling the `bid` method and sharing the desired bidding value in Ether. A *Customer* can only request a bid by providing a bidding value higher than the current top bid. Once the auction is completed, the *Retail Store* ends the auction and triggers an event that announces the winner and the top bid. The bidding amount remains stored in the smart contract until the physical item is delivered successfully. The amount then gets transferred to the *Retail Store*.

Algorithm 4 describes the process of approving a successful delivery. After the physical delivery off-chain is completed, the *Customer* must confirm receiving the physical asset. If the *Customer* approves the delivery, the security deposits get transferred back to the *Customer* and the *Courier Services*. Additionally, the bidding amount saved in the bidding smart contract gets transferred to the *Retail Store*. If the *Customer* does not approve the delivery, the security deposit remains in the smart contract, and the *Retail Store* investigates the issue off the chain. The *Retail Store* controls transferring the security deposits based on the entered amount. On a successful delivery, the *Retail Store* confirms the transfer of the jewelry NFT, and the new owner becomes the *Customer* who purchased the physical jewelry piece.

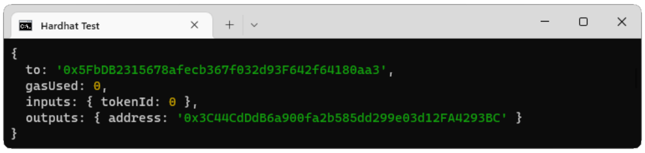
V. TESTING AND VALIDATION

This section includes the testing and validation procedure of the smart contracts. Testing of smart contracts is done on Ethereum by using Hardhat environment. Hardhat provides various tools to compile, deploy, run, and test Solidity code. For our tests, we compile the code using solc version 0.8.9,



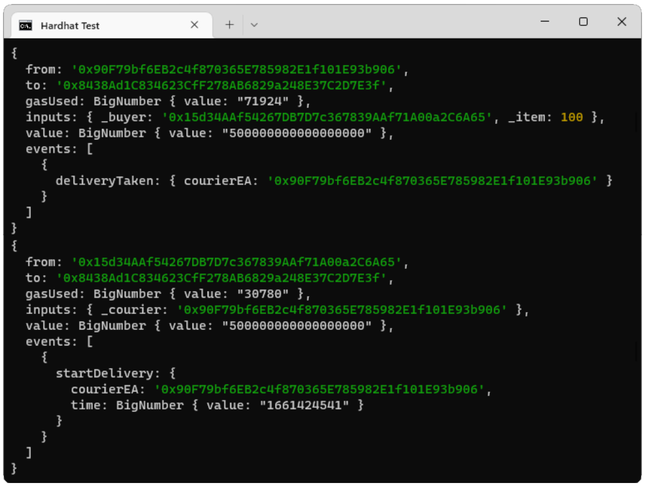
```
{
  from: '0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266',
  to: '0x5FbDB2315678afecb367f032d93F642f64180aa3',
  gasUsed: BigNumber { value: "164879" },
  inputs: {
    _item: 100,
    _uri: 'QmZiqkyH6W2we9haaeYuj8Zmk4diRgbyQ8vLRYF6cfEEzx',
    _to: '0x70997970C51812dc3A010C7d01b50e0d17dc79C8'
  },
  events: [
    {
      Transfer: {
        from: '0x0000000000000000000000000000000000000000',
        to: '0x70997970C51812dc3A010C7d01b50e0d17dc79C8',
        tokenId: BigNumber { value: "0" }
      }
    },
    {
      NewJewelry: {
        item: BigNumber { value: "100" },
        tokenId: BigNumber { value: "0" }
      }
    }
  ]
}
```

FIGURE 6. Transaction details and events of calling the Jewelry mint function



```
{
  to: '0x5FbDB2315678afecb367f032d93F642f64180aa3',
  gasUsed: 0,
  inputs: { tokenId: 0 },
  outputs: { address: '0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC' }
}
```

FIGURE 7. Inquiry of ERC-721 ownerOf function showing the owner of the jewelry is RS



```
{
  from: '0x90F79bf6EB2c4f870365E785982E1f101E93b906',
  to: '0x8438Ad1C834623CfF278AB6829a248E37C2D7E3f',
  gasUsed: BigNumber { value: "71924" },
  inputs: { _buyer: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65', _item: 100 },
  value: BigNumber { value: "500000000000000000" },
  events: [
    {
      deliveryTaken: { courierEA: '0x90F79bf6EB2c4f870365E785982E1f101E93b906' }
    }
  ]
}
{
  from: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65',
  to: '0x8438Ad1C834623CfF278AB6829a248E37C2D7E3f',
  gasUsed: BigNumber { value: "30780" },
  inputs: { _courier: '0x90F79bf6EB2c4f870365E785982E1f101E93b906' },
  value: BigNumber { value: "500000000000000000" },
  events: [
    {
      startDelivery: {
        courierEA: '0x90F79bf6EB2c4f870365E785982E1f101E93b906',
        time: BigNumber { value: "1661424541" }
      }
    }
  ]
}
```

FIGURE 8. Transaction details and events of CS and C_1 paying security deposits

TABLE 1. List of Ethereum addresses used in smart contract testing

Actor	Ethereum Address
Certificate Authority	0xf39Fd6e51aad8...827279cffFb92266
Jewelry Producer	0x70997970C5181...01b50e0d17dc79C8
Retail Store	0x3C44CdDdB6a90...99e03d12FA4293BC
Courier Service	0x90F79bf6EB2c4...982E1f101E93b906
Customer 1	0x15d34AAf54267...9AAf71A00a2C6A65
Customer 2	0x9965507D1a55b...16FB37d819B0A4dc
Customer 3	0x976EA74026E72...54763abd0C3a0aa9
Customer 4	0x14dC79964da2C...3cc7Ca32193d9955
Jewelry SC	0x5FbDB2315678a...d93F642f64180aa3
Auction SC	0x663F3ad617193...334eE4Ed07016602
Delivery SC	0x8438Ad1C83462...29a248E37C2D7E3f

with optimizations enabled at 1000 runs. We utilize Hardhat's local node to deploy the compiled smart contracts to an Ethereum testnet, enabling us to call any public function and retrieve actual statistics on costs and blocktime latency. Furthermore, we take advantage of Hardhat's tools to automate the test cases, generate coverage reports, and track the gas costs of functions. In Ethereum, the gas cost of a function represents how complex it is, and it is the metric used by mining nodes to take rewards upon executing the code. This section describes the test path we ran to validate our proof-of-concept implementation of the smart contracts.

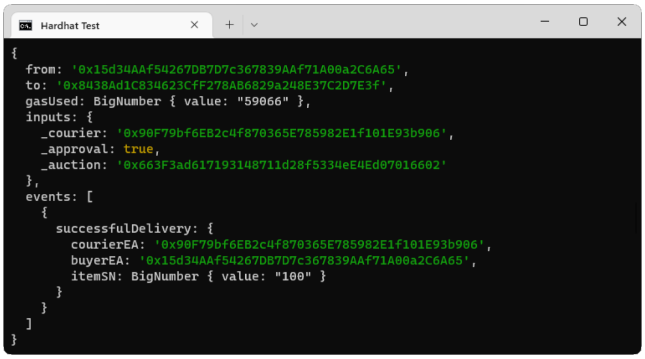
In our testing we use a total of eight Ethereum accounts, the first four are the *Certificate Authority* (CA), *Jewelry Producer* (JP), *Retail Store* (RS), and *Courier Service* (CS). The remaining four accounts are of different *Customers*, denoted as C_i where $i \in \{1, 2, 3, 4\}$ is the index. The addresses of the accounts and deployed smart contracts are shown in Table 1.

The testing begins with CA deploying the ERC-721 NFT SC on the network and minting a new fine jewelry NFT on behalf of JP, which is what Figure 6 shows. The **mint** function call takes the owner JP address, the jewelry item identifier (100), and the jewelry metadata URL on IPFS as a 59-character UTF-8 string. The next step is the RS to acquire the fine jewelry by calling the **approveTransfer** function, which takes the new owner address (RS) and the NFT identifier (0). At this point, the owner of the jewelry is RS, as depicted by Figure 7.

To sell the jewelry piece, RS deploys an Auction SC and assigns two parameters: NFT identifier (0) and auction duration in seconds (7200 for two hours). The customers are allowed for the duration of the auction to place their bids by calling the **bid** function accompanied by a payment. In our test C_1 starts the biddings with 0.5 ETH, followed by C_2 with 0.6 ETH, then C_3 and C_4 with bids 0.7 ETH and 0.8 ETH, respectively. Finally, C_1 increases the bid amount to 0.9 ETH, at which point the auction period ends, and RS closes the auction. Since $C_{2,3,4}$ are no longer top bidders, they can call **withdraw** to return their payment from the Auction SC.

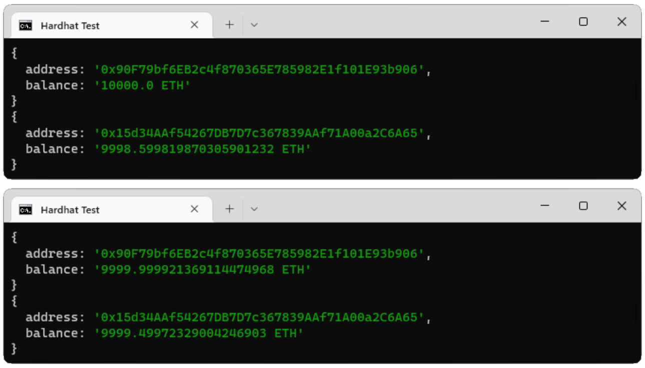
For the delivery phase, RS deploys a Delivery SC, calls **changeDeposit** function to set the required deposit amount to 0.5 ETH and confirms the winner of the auction on item 100 as C_1 by calling **approveBuyer** with the address and item number as inputs. Then, each of the CS and C_1 pay a security deposit of 0.5 ETH to establish the delivery, by calling **courierDeposit** and **buyerDeposit** respectively. Figure 8 displays a value amount represented in Wei successfully submitted by both actors. An event is then triggered to notify that a physical delivery has started off the chain.

After receiving the delivery, C_1 calls **buyerApproval** to confirm that the delivery was successfully completed, which emits an event as seen in Figure 9, and returns the security



```
{
  from: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65',
  to: '0x8438Ad1C834623CfF278AB6829a248E37C2D7E3f',
  gasUsed: BigNumber { value: "59066" },
  inputs: {
    _courier: '0x90F79bf6EB2c4f870365E785982E1f101E93b906',
    _approval: true,
    _auction: '0x663F3ad617193148711d28f5334eE4Ed07016602'
  },
  events: [
    {
      successfulDelivery: {
        courierEA: '0x90F79bf6EB2c4f870365E785982E1f101E93b906',
        buyerEA: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65',
        itemSN: BigNumber { value: "100" }
      }
    }
  ]
}
```

FIGURE 9. Transaction details and events of C_1 confirming a successful delivery



```
{
  address: '0x90F79bf6EB2c4f870365E785982E1f101E93b906',
  balance: '10000.0 ETH'
}
{
  address: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65',
  balance: '9998.599819870305901232 ETH'
}
```

```
{
  address: '0x90F79bf6EB2c4f870365E785982E1f101E93b906',
  balance: '9999.999921369114474968 ETH'
}
{
  address: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65',
  balance: '9999.499723290042469O3 ETH'
}
```

FIGURE 10. Ethereum balance of CS and C_1 before (upper) and after (lower) the delivery process

deposits back to the CS and C_1. Figure 10 shows the ETH balance of the two entities.

The last step in the testing is for RS to call **approveTransfer** and provide C_1 as the address and (0) as the NFT identifier, upon which the NFT gets transferred to C_1, as confirmed by Figure 11 and Figure 12.

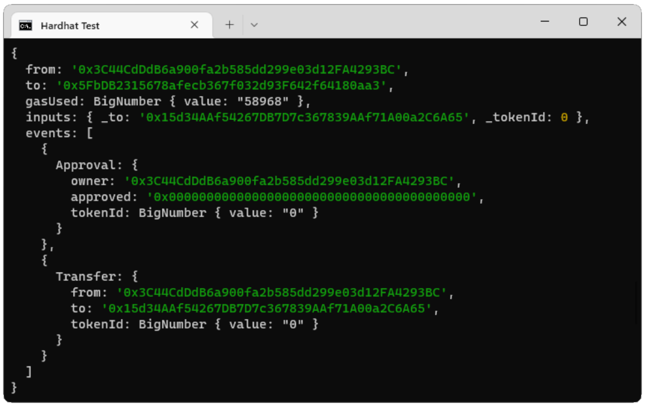
All the executed tests in this validation path succeeded and returned the expected results. The tests cover over 92.98% of the developed code statements, and 93.1% of the lines of code, according to Hardhat's coverage report.

VI. DISCUSSION

In this section, we present cost and security analyses of our proposed solution and implementation to demonstrate its financial viability and robustness against well-known security threats and weaknesses. Moreover, we analyze the latency and throughput of our developed architecture and compare our proposal to prior solutions.

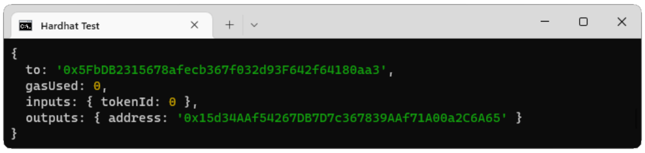
A. SECURITY ANALYSIS

Our proposed solution addresses essential security and privacy concerns commonly found in the assets traceability field. These concerns range from data security aspects, such as the integrity and confidentiality of the data, to service-related aspects, such as availability, accountability, and non-repudiation. Our security discussion qualitatively evaluates these aspects of the proposed architecture and quantitatively analyzes the security of the developed smart contracts using dedicated tools.



```
{
  from: '0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC',
  to: '0x5FbDB2315678afecb367f032d93F642f64180aa3',
  gasUsed: BigNumber { value: "58968" },
  inputs: { _to: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65', _tokenId: 0 },
  events: [
    {
      Approval: {
        owner: '0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC',
        approved: '0x0000000000000000000000000000000000000000',
        tokenId: BigNumber { value: "0" }
      }
    },
    {
      Transfer: {
        from: '0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC',
        to: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65',
        tokenId: BigNumber { value: "0" }
      }
    }
  ]
}
```

FIGURE 11. Transaction details and events of RS transferring the jewelry NFT to C_1



```
{
  to: '0x5FbDB2315678afecb367f032d93F642f64180aa3',
  gasUsed: 0,
  inputs: { tokenId: 0 },
  outputs: { address: '0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65' }
}
```

FIGURE 12. Inquiry of ERC-721 ownerOf function showing the owner of the jewelry is C_1

Data Integrity: Blockchain, in essence, ensures the integrity of all data that is passed to it as inputs, state variables, and outputs. Our solution ensures that all data flows through the Ethereum network. Data of small sizes, such as the fine jewelry pricing, bidding amounts, and the owner of the jewelry, are stored directly on the ledger. In contrast, large data, such as the jewelry metadata, are linked to the chain via their hash.

As for data processing, our solution solely uses blockchain for all code execution, eliminating any possibility of a malicious entity manipulating the data. However, considering Ethereum continues to use proof of work, there is a chance of a 51% attack, where more than half the participating Ethereum nodes collude to sway the mining decisions.

Data Confidentiality: Although blockchain does not offer confidentiality to data stored on the ledger by default, this aspect is not a barrier to adopting the solutions due to two reasons: First, Ethereum entities are pseudonyms, meaning even if the data is public, it cannot be easily associated with an individual. Second, the solution is compatible with encrypting the jewelry metadata files before publishing them on IPFS.

Availability: Due to its decentralization structure, blockchain is very resilient to attacks that prevent the availability of resources to legitimate users. Even during attacks, such as denial of service, all functions like minting jewel NFTs, bidding in the marketplace, delivering goods,

TABLE 2. Vulnerability risk-confidence matrix

		Impact			
		High	Medium	Low	Total
Confidence	**High**	0	0	3	3
	Medium	0	1	6	7

and transferring ownership continue to work.

Accountability: In our proposed system, tracking the actions of participants is crucial to maintaining a trustworthy environment. Inquiries such as knowing the initiator and miner of transactions are stored with timestamps as part of the tamper-proof ledger. Therefore, our approach allows us to track and trace all activities. Furthermore, our adoption of the ERC-721 standard ensures our solution provides a robust mechanism against allowing unwanted entities from managing and maliciously transferring the jewelry NFTs.

Non-repudiation: Stakeholders in our solution cannot falsely claim calling a function with given parameters because all transactions are recorded in an immutable and public manner. However, considering that the highest bidding *Customer* must pay the fees beforehand, the *Retail Store* and *Courier Service* can reject delivering the jewelry piece or transferring the NFT.

Vulnerability Analysis: We performed quantitative vulnerability analysis on the developed Solidity code using Slither analyzer tool. The analysis results are detailed in Table 2, showing the lack of high-impact vulnerability in our prototype smart contracts. Moreover, it is evident from the risk matrix that most of the vulnerabilities are concentrated at the low-impact medium-confidence spot, further indicating the minimal risk associated with our Solidity code. In a deeper analysis of the detected vulnerabilities, we noticed they are related to the possibility of Ether being locked in a smart contract, which can be solved by adding guarded transfer functions to retrieve any locked amounts.

B. COST ANALYSIS

This section discusses the cost analysis of the SC transactions. Each transaction execution requires a specific amount of gas. *Gas* is defined as the unit to measure the transaction cost required for execution. On Ethereum, gas fees are paid by Ether. Since the gas fees are usually small, they are represented by Giga-wei (Gwei) instead of Ether, where 1 Ether is equivalent to 1,000,000,000 Gwei. Since miners prefer to capture transactions with higher gas prices, offering a high gas amount is recommended to mint transactions quickly.

Transaction cost depends on the complexity of the smart contract function. Functions that perform more extensive calculations and call other functions are bound to have higher transaction costs. View functions, which only read and process information, are performed with lower transaction costs. Table 3 presents a summary of the transaction costs required to run the functions defined in our proposed NFT-based approach. The gas costs are reported by Hardhat's gas reporting tool, and the USD conversions are calculated considering 22 Gwei gas price and 1600 USD Ether price [2].

TABLE 3. Cost analysis and throughput (in transactions per second)

Contract	Function	Cost (Gas)	Cost (USD)	Throughput
Jewelry	Deployment	1,466,204	51.61	1.57
	`mint`	119,971	4.22	19.24
	`approveTransfer`	58,962	2.08	39.14
Auction	Deployment	380,421	13.39	6.07
	`bid`	59,681	2.10	38.67
	`auctionClosed`	51,203	1.80	45.07
	`withdraw`	28,514	1.00	80.93
Delivery	Deployment	673,553	23.71	3.43
	`changeDeposit`	28,673	1.01	80.48
	`approveBuyer`	69,846	2.46	33.04
	`courierDeposit`	71,924	2.53	32.09
	`buyerDeposit`	30,780	1.08	74.97
	`buyerApproval`	59,066	2.08	39.07

Besides the contract deployments, which ordinarily consume the most amounts of gas, the function `mint` is shown to be the function with the highest transaction cost. This function is used by the *Certificate Authority* to generate new NFTs. The transaction cost is high due to the strict minting procedure dictated by the ERC-721 standard. Inheritance in Ethereum and calling functions from different smart contracts heavily increase the gas cost of a transaction. On the contrary, the other functions display much lower transaction costs. Overall, the displayed transaction costs present a feasible implementation of integrating blockchain and NFTs in purchasing valuable assets. However, it needs to be noted that Ether prices are not stable and keep fluctuating, so this fluctuation introduces a tradeoff between cost and requirement.

C. OVERHEAD, LATENCY, AND THROUGHPUT

Considering our solutions adopts the Ethereum blockchain, there can be a heavy overhead toward a fully decentralized connection to the network. Traditionally, end users must have an updated Ethereum node running on their devices to be able to initiate and respond to transactions and events. However, more recently, solutions such as Infura and Alchemy simplify the connection procedure and minimize the overhead of using blockchain solutions.

On the other hand, latency is a character of the Ethereum network, which is defined to stay in the range of 10 to 15 seconds, averaging around 13 seconds for most blocks. However, in cases where the end-user requests a transaction with a low gas price offer, the mining nodes will neglect the request for long durations. As for throughput, it differs based on the function called, which is why we include the maximum theoretical throughput (transactions per second) in Table 3.

[2] Prices as of August 28th, 2022. https://etherscan.io/charts.

TABLE 4. Comparison of our proposed solution against prior ones

	[10]	[32]	[33]	[28]	[34]	[29] [30]	[31]	Our Solution
Proof of ownership	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Proof of phys. delivery	No	No	No	Yes	No	Yes	No	Yes
Off-chain decen. storage	No	No	No	No	Yes	Yes	Yes	Yes
Non-fungible tokens	No	No	No	No	No	No	Yes	Yes
Decentralized payments	No	Yes	No	No	Yes	Yes	No	Yes
Implemented	Yes	No	Yes	Yes	No	Yes	Yes	Yes
Deployed and tested	No	No	Yes	Yes	Yes	Yes	Yes	Yes

D. COMPARISON TO PREVIOUS SOLUTIONS

To gain a further understanding of how our proposed approach achieves the goal of providing proof of ownership and proof of delivery for fine jewelry and gemstones, we compare our solution against previous ones. For the comparison, we chose all studies that propose a blockchain-based technical solution.

As evident in Table 4, we are the only implemented and deployed solution to offer scalable NFT-based proof of ownership, proof of delivery, and a fully decentralized payment mechanism. Notable studies such as Westerkamp et al. [31] lacks the delivery aspect and does not consider the payments, and Hasan and Salah [29, 30] lack the ownership aspect and are not oriented around NFTs.

E. GENERALIZATION

To address the traceability, transparency, and security criteria of issuing digital certificates and physical delivery of valuable assets utilizing NFTs, our suggested system is designed, tested, and validated on a public Ethereum platform. Our proposed technique provides a secure way for business stakeholders to record their transactions because blockchain systems encrypt the desired data effectively. Furthermore, any company dealing with physical and valuable assets like watches, gold, diamond, or known brands can customize the proposed smart contracts to meet their needs.

The suggested system effectively traces and tracks the activities and aspects of the proposed certificate issuing, ensuring physical delivery and transferring ownership to a new owner if the process is completed successfully. In addition, the suggested system effectively tracks entities, roles, and actions in the certification and delivery processes. As a result, this research applies to the certification and delivery of valuable assets in various businesses. Owners of valuable watches, for example, can take advantage of our system to sell their products and monitor and manage the certification process, buyers, delivery, and ownership changes. As a result, the watch owner can manage the entire process with more precision, accuracy, and minimal damage. Additionally, the buyer will have more confidence in purchasing an original item that a reputable source has verified.

Our system includes all aspects of issuing digital certification via NFT and physical delivery. As a result, it can be easily adapted for use by different industries. In addition, our system implements three smart contracts that can be applied to different aspects of selling and buying jewelry. Thus, our solution improves existing business processes beyond the precious assets industry.

VII. CONCLUSION

In this paper, we have presented a solution that leverages NFTs and blockchain to provide secure and trusted digital ownership certificates, physical delivery, and provenance of data associated with producing and selling valuable items like fine jewelry, pearls, and gemstones. Our solution is based on the public Ethereum blockchain and ERC-721 NFT smart contracts. Specifically, we created three smart contracts that govern the interactions and rules for generating and managing NFTs, bidding for fine jewelry, transferring funds, proof of delivery, and changing ownership. We demonstrated that our solution is cost-effective and secure against cyberattacks and vulnerabilities by presenting cost and security analysis. Furthermore, we compared our approach against prior ones, where we confirmed providing a comprehensive solution in terms of reliability, security, traceability, and verifiability. We also discussed that our solution could be used by additional industries where physical assets are essential to trace and deliver. As future work, we plan to develop front-end user DApps and deploy our smart contracts on the Ethereum main network.

VIII. ACKNOWLEDGEMENT

This publication is based upon work supported by the Khalifa University of Science and Technology under Award No. CIRA-2019-001.

REFERENCES

[1] M. C. Laowattanakul, “The Study of Thai Millennials’ Internal Characteristics and External Factors Impacting Purchasing of Fine Jewelry,” Ph.D. dissertation, Thammasat University, 2020. [Online]. Available: https://doi.org/10.14457/TU.the.2020.343

[2] M. I. Pshenichnyi, “Gemstones and technologies of their treatment,” Russian Journal of General Chemistry, vol. 81, no. 6, pp. 1375–1380, Jun 2011. [Online]. Available: https://doi.org/10.1134/S1070363211060429

[3] I. Baker, Diamond. Springer, 2019, p. 55–58. [Online]. Available: https://doi.org/10.1007/978-3-319-78766-4

[4] P. C. Southgate and J. S. Lucas, “The Pearl Oyster,” in The Pearl Oyster. London: Elsevier, 2008, p. xi. [Online]. Available: https://doi.org/10.1016/B978-0-444-52976-3

[5] L. Cartier, S. Ali, and M. Krzemnicki, “Blockchain, Chain of Custody and Trace Elements: An Overview of Tracking and Traceability Opportunities in the Gem Industry,” The Journal of Gemmology, vol. 36, pp. 212–227, 01 2018. [Online]. Available: https://doi.org/10.15506/JoG.2018.36.3.212

[6] L. E. Cartier, “Gemstones and sustainable development: Perspectives and trends in mining, processing and trade of precious stones,” The Extractive Industries and Society, vol. 6, no. 4, pp. 1013–1016, 2019. [Online]. Available: https://doi.org/10.1016/j.exis.2019.09.005

[7] T. Serdari and J. Levy, “A Framework That Describes the Challenges of the High Jewelry Market in the US,” Luxury, vol. 5, no. 3, pp. 245–263, 2018. [Online]. Available: https://doi.org/10.1080/20511817.2020.1746091

[8] B. S. Cankurtaran, "This Is Africa": The Melian Dialogue in Blood Diamond. Cham, ZG, Switzerland: Springer International Publishing, 2019, pp. 217–234. [Online]. Available: https://doi.org/10.1007/978-3-319-90731-4_14

[9] K. Scarratt, “Environmental issues challenge pearl industry, but create opportunities as well,” 2019.

[10] U. Thakker, R. Patel, S. Tanwar, N. Kumar, and H. Song, “Blockchain for Diamond Industry: Opportunities and Challenges,” IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8747–8773, June 2021. [Online]. Available: https://doi.org/10.1109/JIOT.2020.3047550

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in 2017 IEEE International Congress on Big Data (BigData Congress), June 2017, pp. 557–564. [Online]. Available: https://doi.org/10.1109/BigDataCongress.2017.85

[12] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, “Untangling Blockchain: A Data Processing View of Blockchain Systems,” IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366–1385, July 2018. [Online]. Available: https://doi.org/10.1109/TKDE.2017.2781227

[13] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “BlockChain: A Distributed Solution to Automotive Security and Privacy,” IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, Dec 2017. [Online]. Available: https://doi.org/10.1109/MCOM.2017.1700879

[14] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, “A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain,” IEEE Access, vol. 9, pp. 9728–9743, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3049920

[15] I. A. Omar, R. Jayaraman, K. Salah, M. Debe, and M. Omar, “Enhancing Vendor Managed Inventory Supply Chain Operations Using Blockchain Smart Contracts,” IEEE Access, vol. 8, pp. 182 704–182 719, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3028031

[16] D. Lamken, T. Wagner, T. Hoiss, K. Seidenfad, A. Hermann, M. Kus, and U. Lechner, “Design patterns and framework for blockchain integration in supply chains,” in 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), May 2021, pp. 1–3. [Online]. Available: https://doi.org/10.1109/ICBC51069.2021.9461062

[17] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, “Blockchain for Waste Management in Smart Cities: A Survey,” IEEE Access, vol. 9, pp. 131 520–131 541, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3113380

[18] G. Mugurusi and E. Ahishakiye, “Blockchain technology needs for sustainable mineral supply chains: A framework for responsible sourcing of Cobalt.” Procedia Computer Science, vol. 200, pp. 638–647, 2022, 3rd International Conference on Industry 4.0 and Smart Manufacturing. [Online]. Available: https://doi.org/10.1016/j.procs.2022.01.262

[19] N. B. Al Barghuthi, H. J. Mohamed, and H. E. Said, “Blockchain in Supply Chain Trading,” in 2018 Fifth HCT Information Technology Trends (ITT), Nov 2018, pp. 336–341. [Online]. Available: https://doi.org/10.1109/CTIT.2018.8649523

[20] N. Kshetri, “Blockchain systems and ethical sourcing in the mineral and metal industry: a multiple case study,” The International Journal of Logistics Management, vol. 33, no. 1, pp. 1–27, Jan 2022. [Online]. Available: https://doi.org/10.1108/IJLM-02-2021-0108

[21] V. Babich and G. Hilary, Tutorial on Blockchain Applications in Supply Chains. Cham: Springer International Publishing, 2022, pp. 51–72. [Online]. Available: https://doi.org/10.1007/978-3-030-81945-3_3

[22] D. Ross, E. Cretu, and V. Lemieux, “NFTs: Tulip Mania or Digital Renaissance?” in 2021 IEEE International Conference on Big Data (Big Data), Dec 2021, pp. 2262–2272. [Online]. Available: https://doi.org/10.1109/BigData52589.2021.9671707

[23] H. Treiblmaier, “Beyond blockchain: How tokens trigger the internet of value and what marketing researchers need to know about them,” Journal of Marketing Communications, vol. 0, no. 0, pp. 1–13, 2021. [Online]. Available: https://doi.org/10.1080/13527266.2021.2011375

[24] W. Rehman, H. e. Zainab, J. Imran, and N. Z. Bawany, “NFTs: Applications and Challenges,” in 2021 22nd International Arab Conference on Information Technology (ACIT), Dec 2021, pp. 1–7. [Online]. Available: https://doi.org/10.1109/ACIT53391.2021.9677260

[25] G. Korpal and D. Scott, “Decentralization and web3 technologies,” 5 2022. [Online]. Available: https://doi.org/10.36227/techrxiv.19727734.v1

[26] T. K. Dasaklis, T. G. Voutsinas, G. T. Tsoulfas, and F. Casino, “A Systematic Literature Review of Blockchain-Enabled Supply Chain Traceability Implementations,” Sustainability, vol. 14, no. 4, 2022. [Online]. Available: https://doi.org/10.3390/su14042439

[27] A. Kanak, N. Ugur, and S. Ergun, “Diamond Accountability Model for Blockchain-enabled Cyber-

Physical Systems," in 2020 IEEE International Conference on Human-Machine Systems (ICHMS), Sep. 2020, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICHMS49158.2020.9209518

[28] J. Li and Y. Song, "Design of Supply Chain System Based on Blockchain Technology," Applied Sciences, vol. 11, no. 20, 2021. [Online]. Available: https://doi.org/10.3390/app11209744

[29] H. R. Hasan and K. Salah, "Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters," IEEE Access, vol. 6, pp. 46 781–46 793, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2866512

[30] H. R. Hasan and K. Salah, "Proof of Delivery of Digital Assets Using Blockchain and Smart Contracts," IEEE Access, vol. 6, pp. 65 439–65 448, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2876971

[31] M. Westerkamp, F. Victor, and A. Küpper, "Tracing manufacturing processes using blockchain-based token compositions," Digital Communications and Networks, vol. 6, no. 2, pp. 167–176, 2020. [Online]. Available: https://doi.org/10.1016/j.dcan.2019.01.007

[32] Z. Xu, T. Jiao, Q. Wang, C. B. Van, S. Wen, and Y. Xiang, "An Efficient Supply Chain Architecture Based on Blockchain for High-Value Commodities," in Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, ser. BSCI '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 81–88. [Online]. Available: https://doi.org/10.1145/3327960.3332384

[33] J. Sunny, N. Undralla, and V. Madhusudanan Pillai, "Supply chain transparency through blockchain-based traceability: An overview with demonstration," Computers & Industrial Engineering, vol. 150, p. 106895, 2020. [Online]. Available: https://doi.org/10.1016/j.cie.2020.106895

[34] H. Hamledari and M. Fischer, "The application of blockchain-based crypto assets for integrating the physical and financial supply chains in the construction & engineering industry," Automation in Construction, vol. 127, p. 103711, 2021. [Online]. Available: https://doi.org/10.1016/j.autcon.2021.103711

AUTHOR BIOS

NOURA ALNUAIMI is a graduate student in the Department of Electrical Engineering and Computer Science at Khalifa University, Abu Dhabi, United Arab Emirates. Her research interests include Cloud computing, blockchain applications and NFTs.

ALANOUD ALMEMARI is a graduate student in the Department of Electrical Engineering and Computer Science at Khalifa University, Abu Dhabi, United Arab Emirates. Her research interests include blockchain technology and Internet of Things (IoT) applications.

MOHAMMAD MADINE received the B.Sc. and M.Sc. degree in computer engineering from Khalifa University, Abu Dhabi, United Arab Emirates, in 2019 and 2021. He is currently a Research Associate at Khalifa University. His research interests include Blockchain solutions in healthcare, personal health records, and edge computing.

KHALED SALAH is a full professor at the Department of Electrical and Computer Engineering, Khalifa University, UAE. He received the B.S. degree in Computer Engineering with a minor in Computer Science from Iowa State University, USA, in 1990, the M.S. degree in Computer Systems Engineering from Illinois Institute of Technology, USA, in 1994, and the Ph.D. degree in Computer Science from the same institution in 2000. He joined Khalifa University in August 2010, and is teaching graduate and undergraduate courses in the areas of cloud computing, computer and network security, computer networks, operating systems, and performance modeling and analysis. Prior to joining Khalifa University, Khaled worked for ten years at the department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), KSA. Khaled has over 190 publications and 3 patents, has been giving a number of international keynote speeches, invited talks, tutorials, and research seminars on the subjects of Blockchain, IoT, Fog and Cloud Computing, and Cybersecurity. Khaled was the recipient of Khalifa University Outstanding Research Award 2014/2015, KFUPM University Excellence in Research Award of 2008/09, and KFUPM Best Research Project Award of 2009/10, and also the recipient of the departmental awards for Distinguished Research and Teaching in prior years. Khaled is a senior member of IEEE, and serves on the Editorial Boards of many WOS-listed journals including IET Communications, IET Networks, Elsevier's JNCA, Wiley's SCN, Wiley's IJNM, J.UCS, and AJSE. Khaled is the Track Chair of IEEE Globecom 2018 on Cloud Computing. He is an Associate Editor of IEEE Blockchain Newsletter and a member of IEEE Blockchain Education Committee.

HAMDA AL BREIKI holds a Ph.D. in Interdisciplinary Engineering from Khalifa University. Her thesis was about defining a trust requirements model for Blockchain systems. She co-founded a start-up company in systems development (Afkar for Systems and Programming), where she worked as a primary developer in several projects. She has worked in localizing Scratch applications and a website (a programming tool for kids) in cooperation with MIT and UAE University. She worked as an IT faculty member at Higher Colleges of Technology from 2012 to 2015.

RAJA JAYARAMAN is an Associate Professor at the Department of Industrial & Systems Engineering at Khalifa University, Abu Dhabi, UAE. He received his Ph.D. in Industrial Engineering from Texas Tech University, a Master of Science degree in Industrial Engineering from New Mexico State University, Masters and Bachelor's degree in Mathematics from India. Raja's research interests includes application of blockchain technology, systems engineering and process optimization techniques to characterize, model and analyze complex systems with applications to supply chains, maintenance planning, and healthcare delivery. His post doctorial research was on technology adoption and implementation of innovative practices in the healthcare supply chains and service delivery. He has led several successful research projects and pilot implementations of supply chain data standards in the US healthcare system.