scientific reports

Check for updates

OPEN

Blockchain enabled traceability in the jewel supply chain

Aman Patel[1,3], Siva Sai[2,3], Ankit Daiya[1], Harshal Akolekar[1]✉ & Vinay Chamola[2]

This article examines the potential of blockchain technology to revolutionize the jewelry supply chain by enhancing trust, transparency, and efficiency. Utilizing Ethereum, we developed a blockchain network tailored to the industry's needs. Blockchain operates as a secure, immutable ledger, ensuring data integrity and transparency while preventing fraud and tampering due to its decentralized nature. Ethereum's key features, including nodes, addresses, and smart contracts, make it an ideal platform for this application. The system incorporates robust security measures, addressing vulnerabilities such as reentrancy attacks and unauthorized access. Performance tests on networks demonstrated the solution's viability, with Layer 2 optimizations reducing transaction costs. The system also uses IPFS (InterPlanetary File System) to store certificate templates in order to improve scalability and data accessibility. Six primary participants in the supply chain, from miners to customers, engage with the blockchain, ensuring full traceability and transparency. Certificates are dynamically generated by retrieving transaction hashes from the blockchain. The certificate template is stored on the InterPlanetary File System (IPFS), and when needed, the relevant data is populated into the template in real-time to produce the certificate. While challenges remain in terms of industry-wide adoption and regulatory compliance, the solution's potential to enhance transparency and efficiency positions it as a significant advancement for the jewelry supply chain within the Industry 4.0 framework.

Keywords Blockchain, Supply chain, Traceability, Ethereum, Jewels, Smart contract

The jewelry supply chain is a complex network, spanning the globe from raw material extraction to the hands of consumers. It involves numerous steps, from mining precious metals and gemstones to crafting exquisite jewelry. Intermediaries like wholesalers and retailers play roles in distributing these products. The industry's complexities arise from the unique properties of gemstones and metals, complex designs, and the involvement of various craftsmen[1]. Global operations introduce geographical challenges, requiring extensive supply networks and adherence to diverse laws and ethical standards. Since customers demand more transparency and ethical jewelry options, the origin and ethical sourcing of materials becomes crucial[2]. This complex process demands precision at every level to meet modern customer expectations for authenticity, quality, and ethical sourcing. Addressing challenges like fraud, transparency, and counterfeiting is crucial, emphasizing the need for a robust system in the jewelry supply chain[3].

This work is motivated by the challenges faced by the jewelry industry and rise of Industry 4.0. The introduction of blockchain technology becomes imperative as it serves as a cornerstone for the transformation towards a more connected and technologically advanced industry. As an innovative solution, blockchain promises to revolutionize the jewelry sector by establishing a secure and transparent digital ledger. This not only verifies the authenticity of jewelry and traces the origin of materials but also aligns with the principles of Industry 4.0 by promoting data-driven decision-making and supply chain transparency[4]. By embracing blockchain, the jewelry industry can enhance consumer confidence, offering clear and verifiable information about the jewelry's journey from production to sale. The decentralized nature of blockchain minimizes the risk of fraud, ensuring the reliability and tamper-proof nature of information- a crucial step towards realizing the vision of Industry 4.0 within the jewelry supply chain. In essence, integrating blockchain aligns the industry with the values of Industry 4.0, creating a more transparent, trustworthy, and efficient system that meets the expectations of both businesses and consumers in this digital transformation[5].

Several researchers have explored the use of blockchain technology, to create a secure and distributed ledger that enhances data transparency and security. Abeyratne et al.[6] proposed a blockchain system concept to improve manufacturing supply chain transparency, traceability, and process integrity. The potential advantages of blockchain in addressing trust and transparency concerns, lowering operational expenses, and facilitating effective collaboration among supply chain partners have been discussed. However this system has certain

[1]Department of Mechanical Engineering, Indian Institute of Technology, Jodhpur 342304, India. [2]Department of Electrical and Electronics Engineering, Birla Institute of Technology and Science, Pilani 333031, India. [3]Aman Patel and Siva Sai contributed equally to this work. ✉email: harshal.akolekar@iitj.ac.in

limitations in terms of the extent to which they enhance the visibility of supply chains, the level of detail in the data they capture, the level of engagement they facilitate with stakeholders, and their ability to integrate with existing processes and systems. Caro et al.[7] presents a blockchain-based traceability system that utilizes Internet of Things (IoT) sensors to gather data from fields. The system is specifically designed to assist in the management of the agri-food sector. Ethereum (a public blockchain) and Hyperledger Sawtooth (a private blockchain), two distinct blockchain technologies, are compared in their study to assess their respective benefits and drawbacks in depth. However, their analysis does not include the complete supply chain, from production to sale. Lu et al.[8] describe a traceability system built on blockchain and smart contracts called OriginChain. In addition to guaranteeing data availability and providing transparent, tamper-proof provenance data, this system automatically verifies data to address regulatory compliance. OriginChain takes into account the perspectives of suppliers and retailers about traceability. Retailers place more emphasis on product origin and quality, while suppliers concentrate on demonstrating product origin, quality, and regulatory compliance. As a traceability provider, OriginChain accepts applications from interested parties. OriginChain's design uses private blockchain technology to support geographically dispersed nodes spread over three distinct locations. The blockchain's data storage system keeps track of several off-chain data sources while storing their hash addresses on the chain. However, this solution is only applicable to service providers, as traceability services are given per terms made in contracts for the rendered service.

Wu et al.[9] developed a hybrid blockchain architecture for real-time shipment tracking in shipping logistics. It uses confidential ledgers for partner-exclusive shipment exchanges and a public ledger for secure online shipment status. This framework addresses limitations of existing systems, such as restricted access, carrier-only data, and reliance on single data sources. Kittipanya-In et al.[10] explored the effects of digital transformation on food supply chains. They found enhanced connectivity, efficiency, and responsiveness but noted challenges in transitioning from traditional to digital supply chains, requiring specialized resource allocation.

Toyoda et al.[11] examined the difficulties presented by conventional RFID (Radio Frequency IDentification) technology in guaranteeing the genuineness of products, particularly in the post-supply chain stage. Their study presented the Product Ownership Management System (POMS), an innovative method that combines blockchain technology to enhance the security and traceability of products using RFID tags. POMS utilizes the decentralized structure of blockchain to guarantee that only authentic products with verifiable ownership may be sold to final consumers. The real implementation of this system on the Ethereum platform proved its viability and cost-effectiveness. While the solution provided by Toyoda et al.[11] is a strong method for ensuring the validity of products after they have passed through the supply chain, our suggested system offers improved scalability, which addresses a wider range of difficulties in the supply chain management. Fernandez et al.[12] have developed blockchain-based solutions that utilize drones and blockchain technology for industrial applications. One method utilizes drones for gathering inventory data, while smart contracts are employed through the use of blockchain technology. This system utilises drones as blockchain clients to provide a product traceability system for Industry 4.0. This drone-powered blockchain system has demonstrated a substantial increase in speed compared to the traditional method of inventory collection and administration performed by human operators in a supply chain warehouse. The drone generates new blocks on the blockchain, which are subsequently saved offline on the local warehouse server. Wang et al.[13] conducted a two-year design science research study on a smart contract initiative in the UK's construction sector, exploring how a group of supply chain actors collectively designed and piloted a blockchain solution to address supply chain transparency and provenance problems. Their research reaffirmed that the business model serves as a valid system-level theoretical framework and generative mechanism, enabling actors to coordinate and bundle activities to create value from emerging technologies like blockchain. The researchers developed a blockchain-enabled supply chain system and smart contracts to improve traceability, shareability, and collaboration in the construction supply chain through information sharing and automation. They presented a set of design principles that can be applied and tested in different supply chain contexts. Additionally, the authors provided in-depth insights on how blockchain can be implemented in a multi-tier complex supply network based on their longitudinal empirical case study in the construction industry. They also explored the adoption of information systems theories and the use of surveys to investigate the theoretical constructs that could influence blockchain adoption in the supply chain. Yiu et al.[2] have proposed a distributed NFC (Near Field Communication) anti-counterfeiting system that leverages blockchain technology to decentralize anti-counterfeiting efforts across the supply chain industry. This system aims to strengthen product traceability and enhance the credibility of supply chain records. The key features of this blockchain-based anti-counterfeiting framework include the decentralisation of the anti-counterfeiting system across the supply chain, rather than relying on a centralized authority, integration of NFC technology to enable trustworthy data provenance retrieval, verification, and management for products. Improved traceability and credibility of supply chain records have been obtained through the use of blockchain technology.

However, most of the blockchain implementations mentioned above simply represent theoretical concepts that propose how blockchain technology could enhance provenance, traceability, and process integrity. Only a few have been executed with comprehensive evaluations of the prototypes and strategies for their implementation and integration into the supply chain sector. By contrast, this study introduces a fully operational blockchain-powered system for the jewelry supply chain. It offers a thorough execution and assessment of the suggested solution and user engagements.

The supply chain in the jewelry industry has several challenging issues about false jewelry, a lack of transparency, concerns about the origins of materials, and the intricate network of firms that deal with jewelry[14]. These issues are significant because they highlight the need for a technology like blockchain to improve the transparency and honesty of the supply chains for jewelry. Counterfeiting is a significant issue in the jewelry sector, involving the sale of fake stones or replica jewelry as genuine. This practice, combining natural and artificial gemstones, not only misleads customers but also undermines confidence in the supply chain. Fraudulent

material mixing compromises the quality and authenticity of jewelry, posing a threat to the reputation of the entire supply chain[15]. The lack of transparency is a significant issue in the jewelry supply chain. The opaque journey of jewelry products from production to sale makes it challenging for customers to verify authenticity and provenance. This lack of visibility allows untrustworthy participants to exploit the situation for their benefit[16]. Consumer concerns about the origin and reliability of metals gemstones in jewelry have recently grown. Lack of specific information on procuring these resources can weaken consumer confidence. Protecting the authenticity of gemstones is crucial for the jewelry supply chain in order to maintain customer trust[17]. The complex network of the jewelry supply chain poses a key challenge due to the involvement of numerous intermediaries, each with distinct duties. This complexity makes it challenging to trace the history of a piece of jewelry, hindering efforts to track factors like provenance, ethical sourcing, and quality control. Providing customers with precise and reliable information about the jewelry's origins becomes challenging in this complex network where information may be lost or confused[18].

This study proposes a blockchain-based solution to improve transparency, traceability, and authenticity in the jewelry supply chain. Leveraging Ethereum's blockchain and smart contracts, the system tracks the entire product journey, from mining to retail, with secure records stored on a decentralized ledger. Certificate templates are stored off-chain and dynamically filled with data fetched from the blockchain at the time of retrieval. The system's decentralized nature prevents fraud, while the user-friendly interface enables easy verification of product authenticity by all stakeholders. Designed to align with Industry 4.0 principles, the solution addresses challenges in traditional supply chains. Key contributions include a fully operational system offering practical traceability solutions and cryptographic hash-based certification, which replaces large file storage with lightweight, scalable, and cost-efficient solutions. This approach demonstrates the value of focusing on data integrity while dynamically generating visual representations when needed. Tailored for the jewelry sector, it showcases blockchain's potential for high-value industries, providing a roadmap for future applications across sectors. These innovations emphasize interoperability and practical implementation, enhancing blockchain adoption in supply chain management.

Table 1 compares the proposed blockchain-based solution for the jewelry supply chain with traditional supply chains and other blockchain-based systems like OriginChain, Everledger, and IBM Food Trust. The comparison is made across various criteria, including user authentication, data integrity, traceability, scalability, authenticity, secure storage, trustworthy operation, setup difficulty, and the degree of decentralization. One of the key advantages of the proposed solution is its decentralized nature, which sets it apart from traditional centralized systems and some other blockchain-based solutions. Decentralization eliminates the need for a central authority or intermediary, distributing control and trust across a network of participants. This design principle aligns with the core tenets of blockchain technology, fostering transparency, security, and resilience against single points of failure. However, the proposed solution also excels in other aspects, such as user authentication and data integrity. By leveraging the inherent security features of blockchain technology, such as cryptographic hashing and consensus mechanisms, the system ensures robust user authentication and maintains the integrity of data throughout the supply chain. This addresses the vulnerabilities commonly found in traditional supply chains, where user authentication and data integrity can be compromised. Moreover, the proposed solution offers enhanced traceability and authenticity compared to traditional supply chains. By recording every step of the supply chain process on an immutable blockchain ledger, the system enables complete traceability of products, from raw material sourcing to final retail. Additionally, the use of digital certificates and cryptographic signatures ensures the authenticity of the products, preventing counterfeiting and fraud. Regarding scalability, the integration of the IPFS in the proposed solution addresses the potential scalability limitations of blockchain technology. Furthermore, the proposed solution ensures secure storage of data by leveraging the decentralized and immutable nature of the blockchain. Unlike traditional centralized systems, where data can be compromised or lost due to a single point of failure, the distributed architecture of the blockchain provides redundancy and fault tolerance, enhancing data security and availability. While the setup difficulty of decentralized systems may initially be higher compared to centralized or private blockchain solutions, the proposed solution mitigates this challenge by leveraging the Ethereum platform and its well-established ecosystem. The use of Ethereum's smart contracts and the availability of development tools and resources facilitate the setup and deployment process, reducing the overall complexity.

Application architecture

In this digital transformation era, blockchain technology has transformed the way we handle data and transactions. It is essentially a decentralized ledger, a chain of blocks, where each block contains a bundle of transactions. What sets blockchain apart is its core attributes: transparency, security, and immutability. The

	Integrity	Traceability	Scalable	Authenticity	Secure storage	Trustworthy	Setup difficulty	Degree of decentralization
Traditional supply chain[16]	✗	✗	✓	✗	✗	✗	High	Centralized
OriginChain[8]	✓	✓	✓	✓	✓	✓	High	Centralized
Everledger[19]	✓	✗	✓	✗	✓	✓	Low	Centralized
IBM food trust[20]	✓	✓	✓	✓	✓	✗	High	Centralized
Malik et. al.[21]	✓	✓	✗	✓	✓	✗	High	Centralized
Our solution	✓	✓	✓	✓	✓	✓	Low	Decentralized

Table 1. Comparison of the current solution with other systems.

whole point of using a blockchain is to let people who do not trust one another share valuable data in a secure, tamperproof way. The heart of blockchain lies in its decentralized and distributed nature[22]. It operates across a network of computers or nodes, where transactions are verified and recorded. Once a block is filled with data, it is linked to the previous one, forming an unchangeable chain. This interconnected structure ensures that data, once recorded, cannot be altered without the consensus of the network. The information stored on a blockchain is secure and resistant to fraud or tampering, making it an ideal solution for recording valuable data and digital transactions[23].

Blockchains

Beyond cryptocurrencies like Bitcoin, blockchain technology is finding its place in several industries. Supply chain management, healthcare, finance, and many others are exploring its potential. It promises a future where trust and transparency are at the forefront of digital interactions, reshaping how we exchange and secure information across the globe. Blockchain's versatility and innovation have made it a critical force in our increasingly interconnected world. A few terms are subsequently explained in the context of blockchains.

- Ethereum: Ethereum is a prominent blockchain platform that goes beyond basic cryptocurrency transactions. It allows the creation of decentralized applications and smart contracts, making it a versatile and widely adopted blockchain[24].
- Nodes: Nodes are individual computers that participate in the blockchain network. They maintain a copy of the entire blockchain and validate transactions, contributing to the decentralized nature of the network[24].
- Ethereum address: An Ethereum address serves as a unique identifier on the Ethereum network. Similar to an account number, it is used for sending and receiving transactions within the blockchain[24].
- Smart contracts: Smart contracts, which are self-executing codes on the blockchain, can automate various supply chain procedures. These contracts automatically execute actions when predefined conditions are met. They play a crucial role in automating processes and ensuring trust within the blockchain network[24].
- Cryptographic hash functions: Cryptographic hash functions are algorithms that secure data by converting it into a fixed-size string of characters (hash). This ensures data integrity and authenticity within the blockchain[25].
- IPFS: IPFS plays a crucial role in enhancing the efficiency and scalability of the proposed blockchain-based system for the jewelry supply chain. While blockchain technology excels at providing an immutable and transparent ledger for recording transactions, it faces limitations when dealing with large files or data. Storing substantial amounts of data directly on the blockchain can lead to congestion, slowing down the network and increasing operational costs[26]. IPFS addresses this challenge by acting as a decentralized data storage and retrieval system, complementing the blockchain's capabilities. Instead of storing large files directly on the blockchain, IPFS allows these files to be stored off-chain, while only the cryptographic hash of the data is recorded on the blockchain itself. This approach ensures data integrity and authenticity while minimizing the strain on the blockchain network. The InterPlanetary File System (IPFS) is employed to store templates, which are dynamically populated to generate certificates associated with specific assets. The working of an IPFS is shown in Fig. 1.

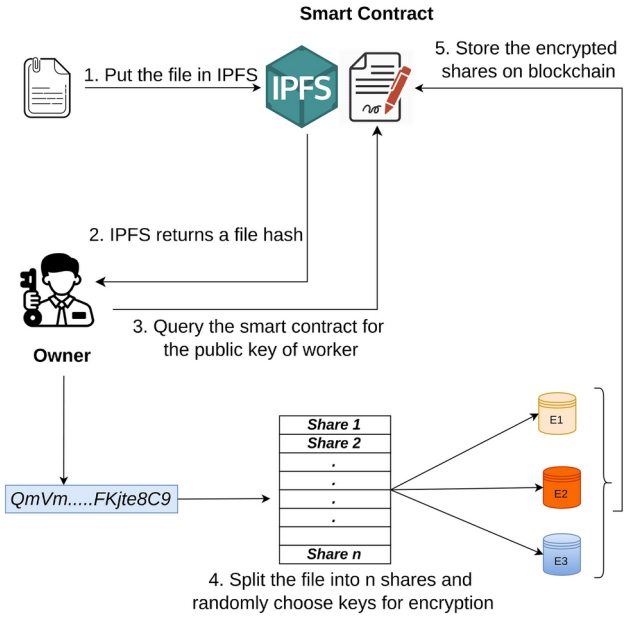

Figure 1. IPFS in a blockchain.

Data management: on-chain vs. off-chain storage

Our blockchain-based system for the jewelry supply chain employs a hybrid approach to data storage, utilizing both on-chain and off-chain solutions. This strategy optimizes the system's efficiency, scalability, and cost-effectiveness while maintaining data integrity and accessibility. A few terms are explained in the context of data management.

- On-chain storage: The data that is essential for the core functionality of the blockchain, and requires frequent access are stored on on-chain storage. In the proposed framework, the on-chain data include transaction metadata, cryptographic hashes, smart contract logic, product identifiers, and critical supply chain events.
- Off-chain storage: IPFS is used for off-chain storage of certificate templates.The hybrid approach offers several advantages:
-
- Scalability: By storing only essential data on-chain, we prevent the blockchain from becoming overburdened, ensuring faster transaction processing and reduced network congestion.
- Cost-effectiveness: On-chain storage is typically more expensive due to the need for every node to replicate the data. Off-chain storage reduces these costs significantly.
- Data integrity: While data is stored off-chain, its integrity is ensured by storing cryptographic hashes on-chain. This approach ensures data integrity and authenticity while minimizing the strain on the blockchain network.
- Accessibility: IPFS's distributed nature ensures that off-chain data remains accessible and retrievable, even if some nodes become unavailable.
- Flexibility: Allows for the storage of diverse data types and sizes without compromising the blockchain's performance.

Stakeholders

In this system, when stakeholders such as miners, refiners, manufacturers, or retailers need to upload a certificate, the process begins by computing the cryptographic hash of the certificate file, creating a unique fingerprint that ensures its integrity.

This hash is recorded on the Ethereum blockchain, establishing an immutable record of the certificate's association with specific products or materials. Templates for generating certificates will be stored on the IPFS system to reduce the overload. This integration of IPFS not only boosts the scalability and efficiency of the system but also aligns with blockchain principles of decentralization and data integrity. The jewelry supply chain architecture is designed for transparency and authenticity verification, utilizing smart contracts written in Solidity, a React.js user interface, and Metamask wallet for user authentication. The network accommodates six participant types, each with defined actions. The process is shown in Fig. 2 and the stakeholders are described below.

- Admin: Adds new Miners, Refiners/Polishers, Manufacturers, and Retailers.
- Miners: Record details of mining, including location, date, and materials mined
- Refiners/polishers: Record refining process details, such as refining date, location, and quality checks. Issue relevant certificates for the material.
- Manufacturer: Records jewelry manufacturing details, such as design, production date, and quality checks.
- Retailer: Records sales of jewelry to customers.
- Customer: Access detailed information about the jewelry, including its components, origin, and quality.

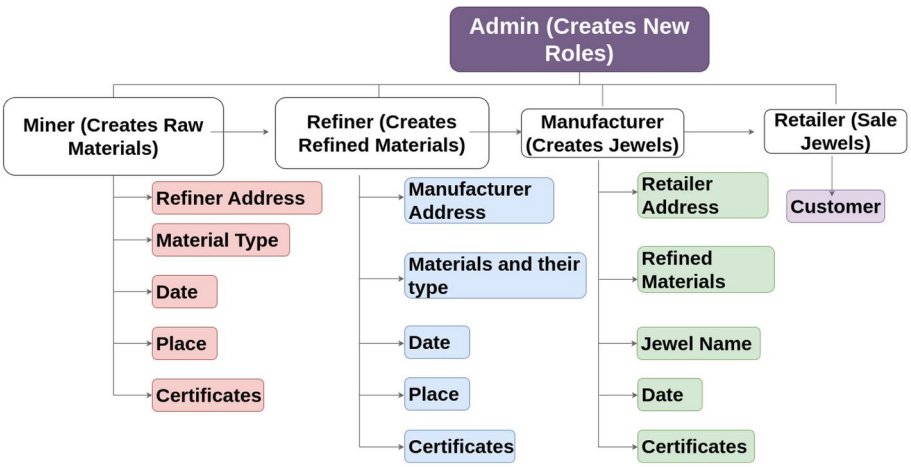

Figure 2. Schematic of the jewel supply chain.

Architecture

Using a public blockchain is crucial for transparency, allowing everyone involved, from miners to consumers, to access and verify information easily. This transparency builds trust by independently confirming the authenticity of materials and products. Additionally, the decentralized nature of public blockchains enhances security, minimizing the risk of tampering. The persistence of recorded data ensures an unchangeable journey record from the mine to the customer, which is essential for traceability and maintaining supply chain integrity. The architecture for the proposed methodology is presented in Fig. 3. The step-by-step working of the designed supply chain is explained below.

1. It begins with miners, responsible for extracting raw materials and sending information about the mined resources to this server using their dedicated blockchain accounts. This information includes details such as the date of mining and the source of the materials.
2. Before sending the transaction to the smart contract in subsequent steps, it is first verified off-chain whether the materials exist and whether they belong to the same account that is making the request.
3. Subsequently, refiners become part of the process, adding information regarding the refining procedures.
4. Manufacturers play a pivotal role by creating unique jewelry items and adding their specifications to the blockchain.
5. Once the jewelry items are ready, they are distributed to retailers, who act as the final gatekeepers of product authenticity, able to conveniently verify the genuineness of these items by accessing the blockchain.
6. Once customers receive their products, they are afforded the capability to verify their purchased jewelry items easily. This is achieved by scanning QR codes or alternative mechanisms(unique IDs in our case), allowing customers to authenticate their purchases confidently. he relevant details, including certificates and product information, will be fetched and displayed according to the IPFS layout, ensuring transparency and easy access to verification data.

Algorithm

The following algorithms represent pseudocode implementations of key smart contract functionalities used in the proposed blockchain-based solution for the jewelry supply chain. These algorithms detail the core operations that govern interactions within the system, ensuring transparency, traceability, and authenticity across all stages of the supply chain.

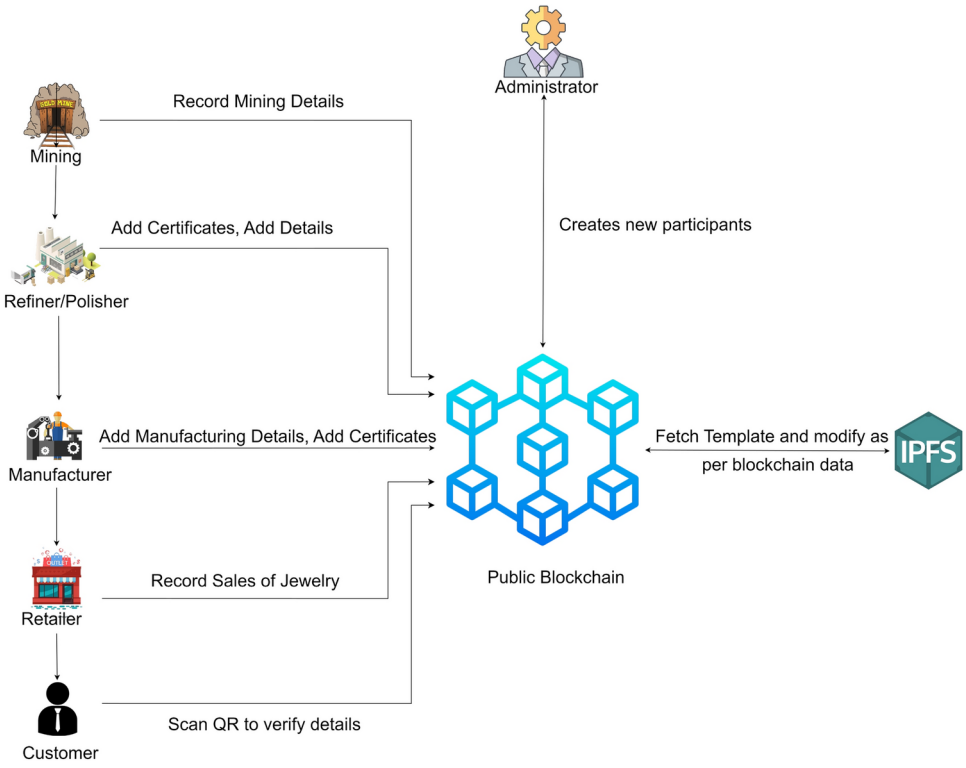

Figure 3. Architecture of the jewel supply chain (made in app.diagrams.net).

Input: *_retailer*: address, *_refinedMats*: bytes32[], *_name*: string, *_date*: uint, *_certificates*: string[]
Output: *id*: bytes32
Function `createJewel(_retailer, _refinedMats, _name, _date, _certificates)`:

```
// Check if the caller has manufacturer permissions
require userHasRole(msg.sender, Roles.Manufacturer), "Only manufacturer can create new jewels"
    // Create the jewel with the provided data
newJewel ← Jewel({
    manufacturer : msg.sender,
    retailer : _retailer,
    refinedMaterials : _refinedMats,
    name : _name,
    date : _date,
    certificates : _certificates
    })
    // Generate a unique identifier for the jewel using Keccak256
id ← keccak256(abi.encode(newJewel.manufacturer,
    newJewel.retailer,newJewel.refinedMaterials,
    newJewel.name,newJewel.date,newJewel.certificates))
    // Store the jewel in the mapping for quick retrieval
JewelById[id] = newJewel

return id
```

End Function

Algorithm 1. Create jewel function.

Algorithm 1 outlines the process by which a manufacturer creates a new jewelry item by combining refined materials, associating it with certificates, and generating a unique identifier. The createJewel function takes the following input parameters. *retailer*: the address of the retailer for the new jewel. *refinedMats*: an array of bytes32 representing the refined materials used in the jewel. *name*: the name of the new jewel. *date*: the date of creation for the new jewel. *certificates*: an array of strings representing the certificates associated with the new jewel. The function performs the following steps. It requires that the caller of the function has the "Manufacturer" role using the *userHasRole* function. After that, it creates a new Jewel structure (struct) with the provided input parameters and generates an ID for the new jewel by taking the *keccak256* hash of the encoded Jewel struct. The new Jewel struct is stored in the *JewelById* mapping using the generated ID as the key. The function returns the generated ID which can be used to verify the jewelry and access related certificates. In our solution, this hashID is converted into a QR code for ease of access.

Algorithm 2 describes the process of creating a unique hash for raw materials, ensuring secure tracking and provenance. The above function takes the following as input parameters. *miner*: the name of the miner. *refiner*: the name of the refiner. *materialType*: the type of material. *date*: the date of the material. *place*: the place of origin for the material. *certificates*: a list of certificates associated with the material. The function performs the following steps: It creates a new *RawMaterial* struct with the input parameters. It encodes the raw material data using the *abi.encode* function. It generates a hash ID using the *keccak256* function by hashing the encoded raw material data. And returns the generated hash. The hashing algorithm is using the default keccak-256 function of solidity. The generated hash represents the certificate data. This hash is stored on the blockchain, eliminating the need for storing large files like PDFs or images. The hash ensures immutability, while static templates off-chain are dynamically populated during certificate retrieval.

Require: *miner*, *refiner*, *materialType*, *date*, *place*, *certificates*
Ensure: *hash_id*

```
function GETHASH(miner, refiner, materialType, date, place, certificates)
    newRawMaterial ← RawMaterial({
        miner: miner,
        refiner: refiner,
        materialType: materialType,
        date: date,
        place: place,
        certificates: certificates
     })
    rawMaterialData ← abi.encode(miner, refiner, materialType, date, place, certificates)
    id ← keccak256(rawMaterialData)
    return id
end function
```

Algorithm 2. Algorithm for generating hash.

Results and discussions

The proposed blockchain-based solution for the jewelry supply chain was implemented using a combination of cutting-edge technologies. Ethereum, a prominent decentralized blockchain platform, was employed to create the blockchain network, leveraging its capabilities for developing secure and transparent decentralized applications and smart contracts. The smart contracts were developed using Solidity, Ethereum's native programming language, and tested locally on Ganache, a personal Ethereum blockchain environment. The user interface was built using React, a powerful JavaScript library for constructing dynamic web applications, along with Node.js for the backend server. The development and deployment was carried out on an Ubuntu 22.04 LTS environment, a reliable and secure Linux distribution. Truffle, a comprehensive development framework for Ethereum, facilitated the compilation, deployment, and testing of smart contracts. Furthermore, MetaMask, a widely adopted cryptocurrency wallet and browser extension, was integrated to enable secure user authentication and interaction with the Ethereum blockchain network.

Blockchain and supply chain solution

The following is a demonstration of the blockchain solution. Only the owner, identified by their unique Ethereum address, has the privilege to register new participants. Each participant is assigned a distinct Ethereum address, enabling them to undertake specific actions within the supply chain. Additionally, participants' roles can be verified using their addresses, ensuring the legitimacy of their presence in the network. This process is shown in Fig. 4. Here the accounts of participants can be stored in a hash table which will contain a unique ID for every participant and other necessary information like the role of the participant, Ethereum address, location, etc. Additionally for adding a new participant in the existing system, multisig[27] (short for multi-signature) can be used, which is similar to the method of Cao et al.[28]. Multisig is a digital signature scheme that requires multiple parties to authorize a transaction or contract deployment. In the context of the proposed system, the owner role, responsible for adding new participants, can be a decentralized entity consisting of a group. This group can collectively control the owner account through a multisig setup, where a predefined number of signatures (e.g., a majority) from the group members is required to execute sensitive operations like registering new participants. This approach enhances security and prevents any single entity from having sole control over the system, aligning with the principles of decentralization inherent to blockchain technology.

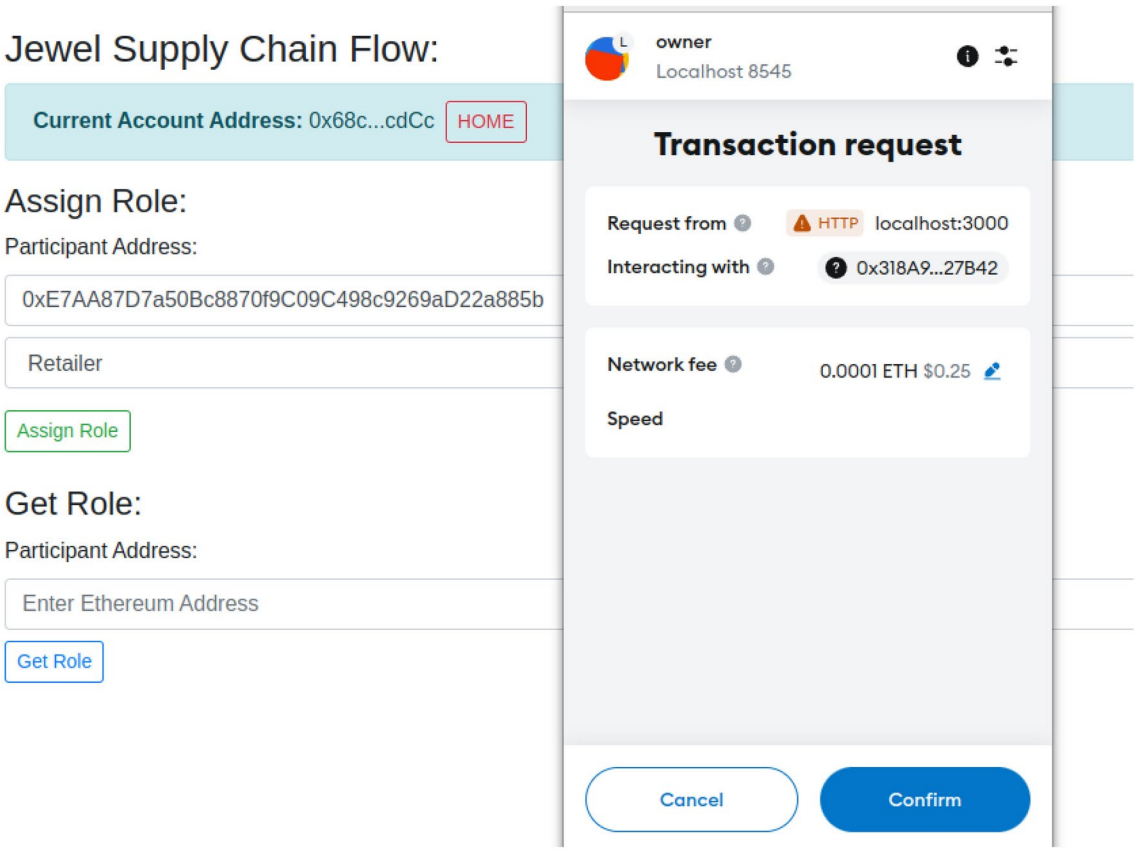

Figure 4. Creation of roles.

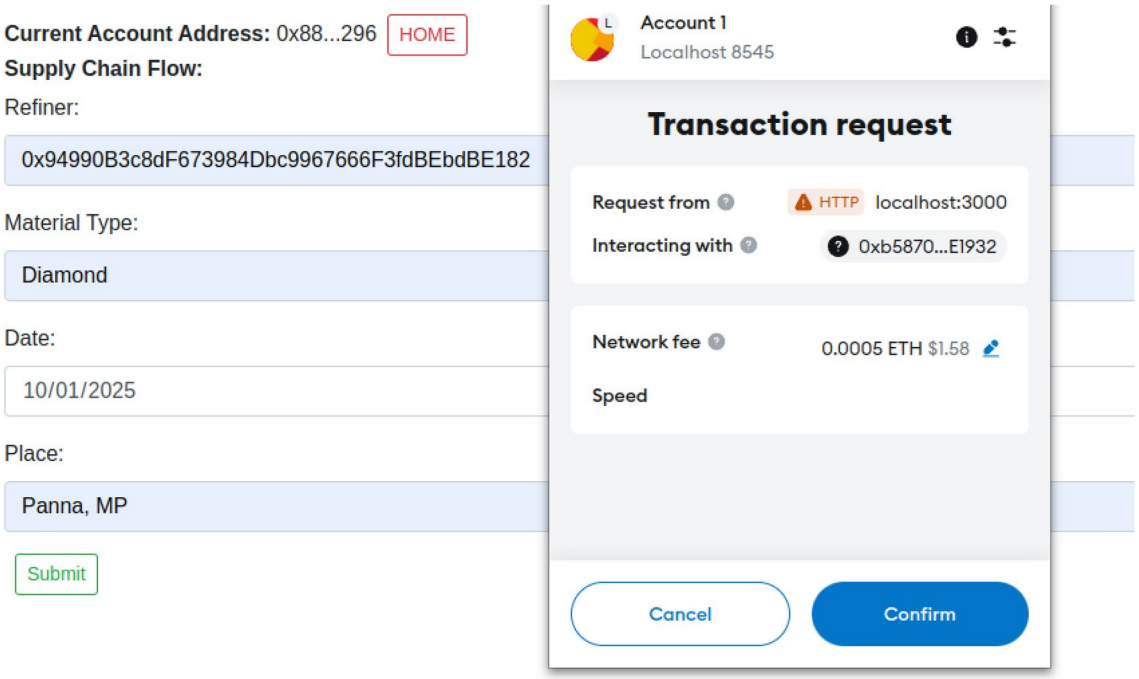

Figure 5. Creation of raw materials.

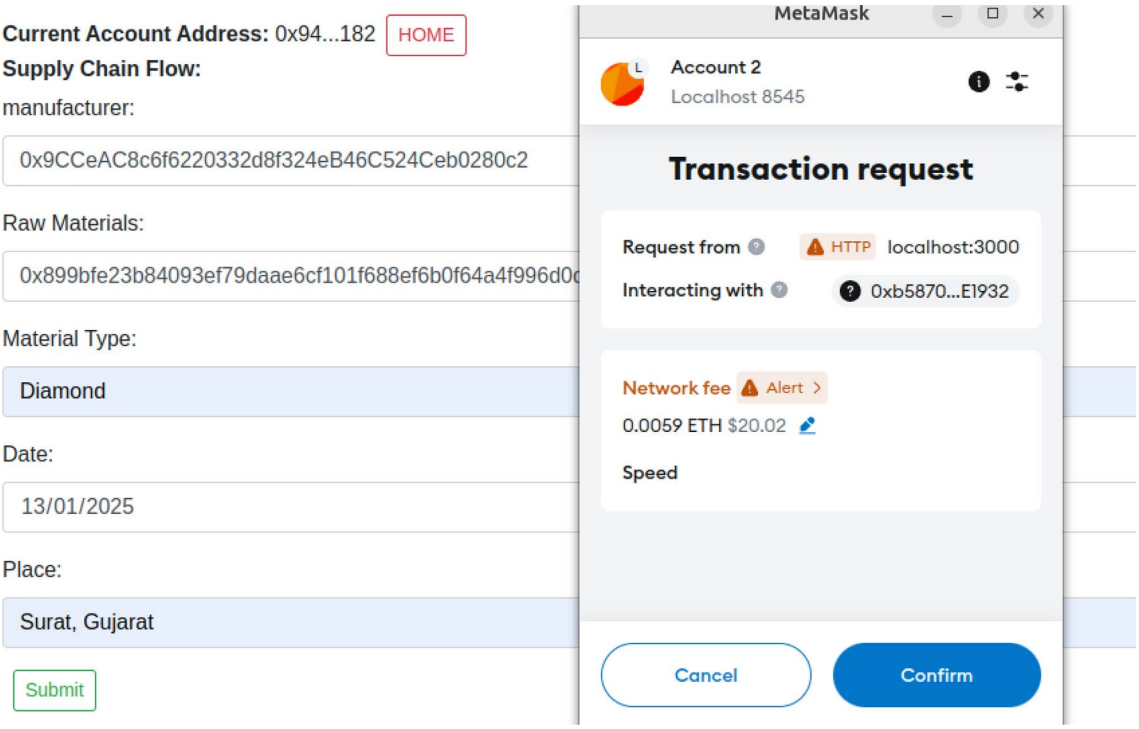

Figure 6. Creation of refined materials.

After submission, a QR code with a unique ID for the raw material is generated. This QR code serves two important purposes: it acts as a reference for updating information in later stages of the product's journey, and it serves as a means to verify the authenticity of the product. This step is shown in Fig. 5.

As the product is processed from the mining stage, refiners come into play. Using the QR code generated after the mining stage, they will create a unique ID of raw materials processed by miners. Using this ID they can update the status of the product in the supply chain. Static templates are populated dynamically for authenticity

and verification. A QR code will be generated after this stage which comprises the ID of the refined materials. This process is shown in Fig. 6.

After processing materials from refiners or polishers, the manufacturer uses them to craft jewels, dispatching the finished products to retailers. A single jewel may incorporate multiple materials sourced from various refiners and polishers. For streamlined record-keeping, the manufacturer can effortlessly scan QR codes received from different polishers and refiners, including the data into the jewel's information for traceability. Figure 7 illustrates a typical transaction from the manufacturer to the retailer. Once the jewel is added to the blockchain, the manufacturer can affix the generated QR code, which will serve both as a means to verify the jewel's authenticity and to facilitate traceability.

Figure 8 demonstrates the traceability and authenticity verification capabilities of the proposed blockchain-based system for the jewelry supply chain. The interface allows users to enter a unique 'Jewel ID' or optionally scan the QR code this sends a request to smart contract and retrieves relevant information and presents it on the website. As we can observe from Fig. 8 it displays different stages of material processing, such as refining, and lists the involved participants. Additionally, the interface provides other crucial details like dates and locations, which aid in verifying originality and authenticity with ease. By presenting this comprehensive and interconnected information, the system enables complete traceability of the jewelry piece, right from the initial mining of raw materials to the final retail stage. Users, including customers, can verify the authenticity of the jewel by cross-checking the details at each stage, such as the locations and dates. The use of Ethereum addresses for miners, refiners, manufacturers, and retailers ensures secure and transparent identification of the parties involved. Moreover.

Figure 9 illustrates the contract deployment transaction on the Sepolia Test Network, demonstrating the successful implementation of the proposed system on the Ethereum blockchain. This deployment verifies the operational integrity of the smart contracts and highlights the transparency and reliability of interactions within the blockchain environment. The visual representation of the transaction provides evidence of the system's functionality and ensures reproducibility within a decentralized framework.

The user interface of the proposed system is designed to cater to the diverse needs of participants across the jewelry supply chain, ensuring ease of use and accessibility. Each type of user - miners, refiners, manufacturers, retailers, and consumers - is presented with a role-specific interface that streamlines their interactions with the blockchain. For instance, miners have access to intuitive forms for logging new raw materials, while retailers can easily verify product authenticity and access provenance information. All interfaces are responsive, allowing for seamless use across desktop and mobile devices (web3 browsers), which is particularly crucial for on-the-go verification by retailers and consumers. User authentication is managed securely through integration with MetaMask, leveraging Ethereum addresses and digital signatures for login and transaction signing. This approach ensures robust security while maintaining a straightforward user experience. The system also incorporates QR code functionality, allowing for quick and easy product tracking and verification. For example, a consumer can simply scan a QR code on a piece of jewelry to access its entire history on the blockchain, presented in an easily digestible format including timelines and maps.

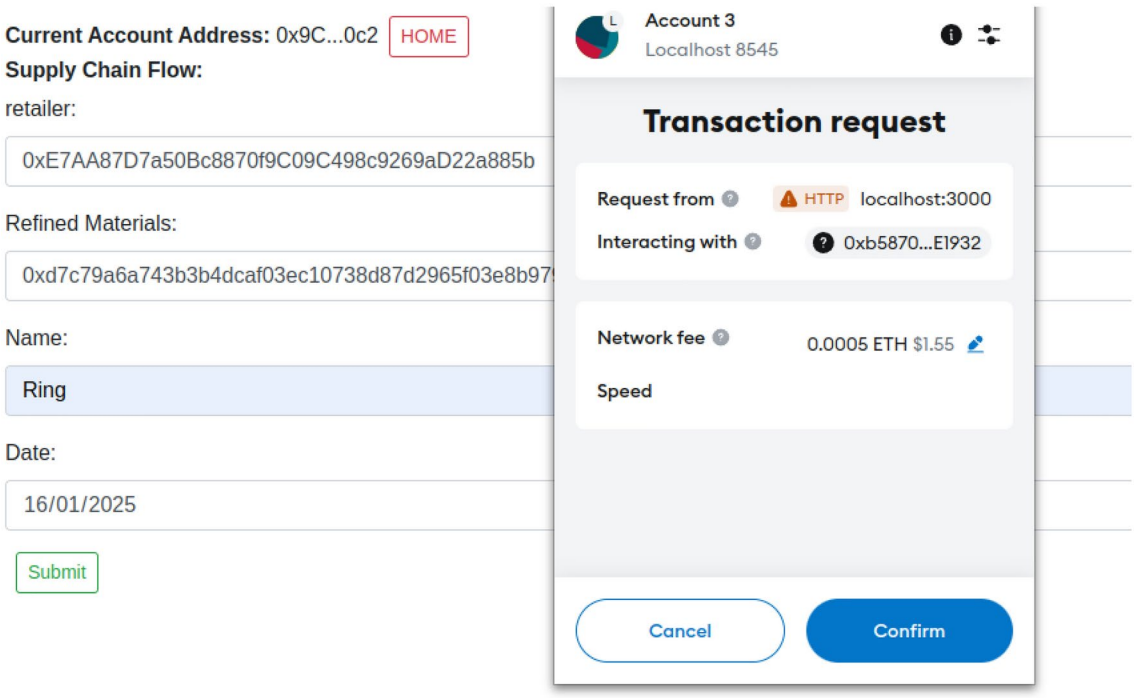

Figure 7. Creation of new jewels.

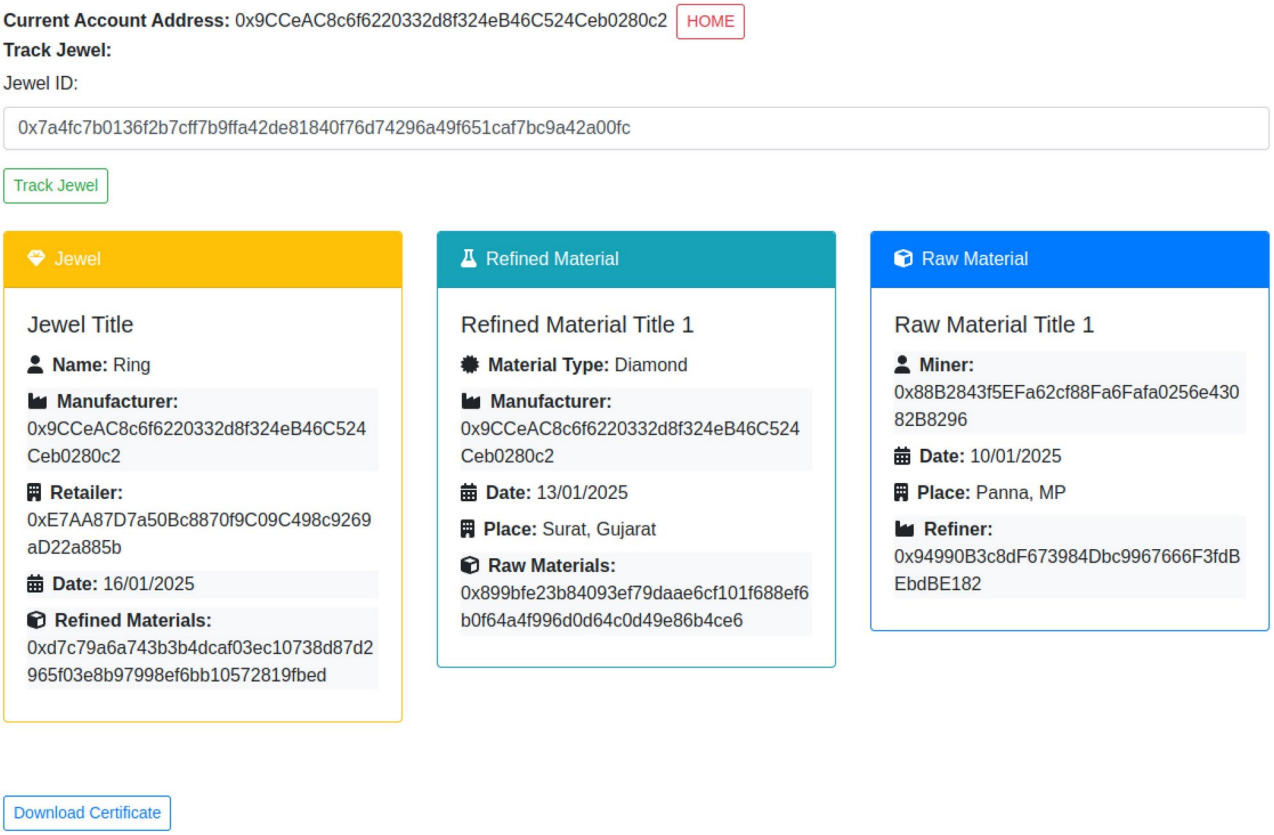

Figure 8. Tracking of a product.

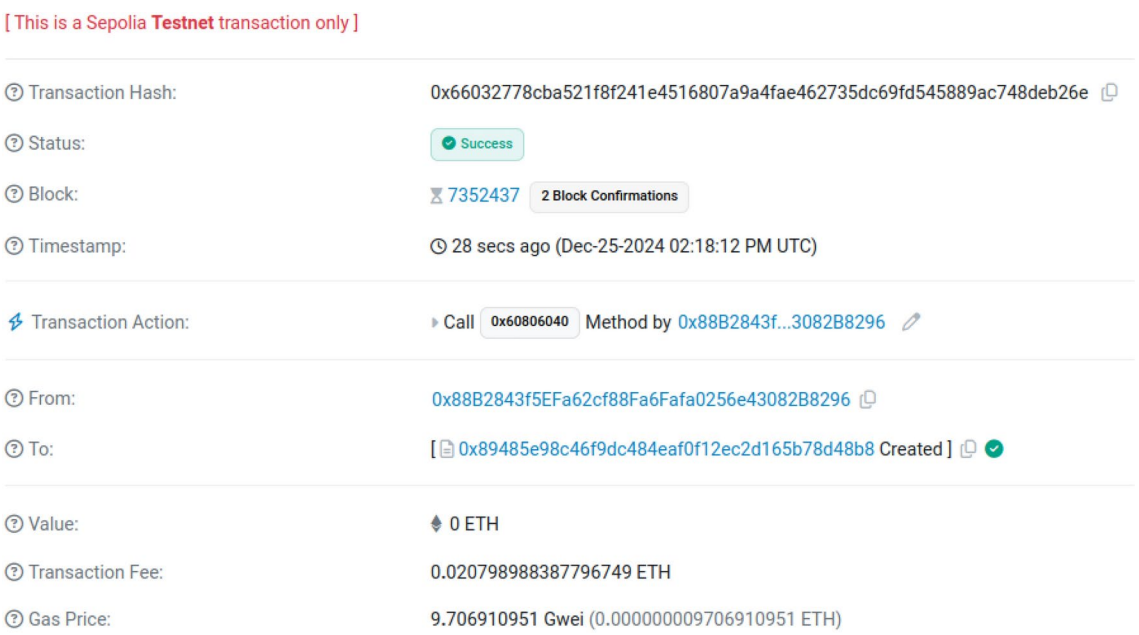

Figure 9. Smart contract deployment on Sepolia testnet.

Method	Called by	Data size (bytes)	Avg. execution time (ms) (Sepolia)	Avg. execution time (ms) (Ganache)	Transaction fees (Sepolia)
createRole	Owner	21 bytes	15219.49	0.84	1.25-05
getRole	Requestor	32 bytes	0.86	0.23	–
createRawMaterial	Miner	148 bytes	18624.62	0.94	1.4E-05
getRawMaterial	Requestor	32 bytes	1.43	0.43	–
createRefinedMaterial	Refiner	180 bytes	18090.99	0.92	2.73E-05
getRefinedMaterial	Requester	32 bytes	0.88	0.38	–
createJewel	Manufacturer	148 bytes	17053.48	0.94	2.24E-05
getJewel	Requester	32 bytes	1.64	1.06	–

Table 2. Average execution time and transaction fees of the smart contract methods on Ganache and test network.

Security analysis

In designing the smart contracts for the blockchain-based jewelry supply chain, we considered several security vulnerabilities, focusing on reentrancy attacks, gas limit issues, and access control.

1. Reentrancy attacks: Reentrancy attacks are a significant threat in Ethereum smart contracts, allowing an external contract to repeatedly call a function before its previous execution finishes, which can drain funds or disrupt the contract state. To counter this, we adopted the checks-effects-interactions pattern, placing all external calls at the end of each function while updating the contract state first. Additionally, we used non-Reentrant modifiers in functions interacting with external contracts to prevent recursive calls and ensure a single entry point for execution.
2. Gas limit concerns: Complex functions within smart contracts can incur high gas costs, potentially reaching Ethereum's gas limit and causing failed transactions. Functions that handle multiple operations, such as batch updates or large data processing tasks, are particularly susceptible. To address gas limit concerns, our contracts are designed with modular and efficient functions. By breaking down complex operations into smaller, discrete functions, we can reduce the gas cost per function call. Additionally, data-heavy operations, such as updating traceability records or adding certificates, are managed off-chain via IPFS, with only critical hashes stored on-chain. This approach minimizes on-chain data storage and keeps transaction costs manageable for all participants.
3. Access control and authorization: Unauthorized access to sensitive functions can compromise the integrity of the jewelry supply chain. Without proper access control, users could manipulate contract data or perform actions outside their designated role (e.g., miners impersonating retailers). Role-based access control (RBAC) is enforced through require statements that check each user's role before executing functions. The system leverages Ethereum addresses to authenticate users and assign roles, ensuring that only authorized users can access specific contract functions. Additionally, role verification checks are embedded within each function, allowing only designated roles, such as miners or retailers, to update records or add data.
4. Integer overflow and underflow: Integer overflow or underflow occurs when arithmetic operations exceed the storage limits of the data type, potentially leading to unexpected values and security vulnerabilities. Solidity's SafeMath library is employed for all arithmetic operations within the smart contracts, which automatically checks for overflow and underflow conditions. This library ensures that arithmetic operations are secure, maintaining data integrity and preventing potential exploits from integer manipulation.
5. Denial of service (DoS) attacks: DoS attacks can be initiated by repeatedly calling contract functions, either to exhaust gas limits or to disrupt service for other users. This risk is particularly relevant in public blockchain environments where anyone can interact with the contract. To guard against DoS attacks, we have implemented rate-limiting mechanisms in certain functions, restricting excessive calls within a specified timeframe. Additionally, critical functions include safeguards, such as circuit breakers, that can halt execution under abnormal conditions, preserving contract integrity during a potential DoS attack.

Performance assessment

Table 2 provides a comprehensive analysis of the performance and cost of the smart contract methods used in the proposed blockchain-based jewelry supply chain system. It highlights execution times across two key environments: the Sepolia test network, representing real-world conditions, and the local Ganache network, which serves as a controlled testing environment. This comparison allows for understanding the performance characteristics of the methods in a live, public test network (Sepolia) as well as in a local development environment (Ganache), enabling optimizations and performance tuning. In addition to performance metrics, the table categorizes methods based on their data size in bytes, illustrating the storage and processing impact of different operations. Finally, the methods are organized by participant roles - owner, miner, refiner, manufacturer, and requestor mapping each operation to the stakeholders responsible for its execution.

Challenges in implementation

While our blockchain-based solution offers significant potential benefits for the jewelry supply chain, several practical challenges must be addressed for successful real-world implementation. Many stakeholders, particularly small-scale jewelers, may distrust new technologies due to past experiences with costly or ineffective solutions.

They may perceive blockchain as yet another complicated system, especially if they have limited experience with digital solutions. For instance, smaller retailers may worry that they lack the resources to adopt and maintain blockchain systems or may fear that the transparency blockchain provides could disrupt traditional business practices where secrecy in sourcing is sometimes valued. Extensive education and training efforts may be necessary to communicate how blockchain can enhance supply chain transparency and consumer trust, and industry groups could play a role in helping explain these benefits. The jewelry industry spans multiple countries, each with its own regulations on sourcing, environmental impact, and ethical practices. Blockchain, by nature, provides transparency but may also expose areas where certain regulations are not strictly followed. Companies may need to navigate legal complexities related to data privacy laws, as blockchain's immutability could conflict with regulations requiring the ability to delete data upon request. To tackle these challenges one should develop a phased rollout strategy, starting with industry leaders willing to pilot the technology. Collaborate with industry associations like the World Jewellery Confederation to promote awareness and benefits. Provide comprehensive training and support to ease the transition. Overcoming these challenges will require ongoing collaboration between technology providers, industry stakeholders, and regulatory bodies. However, the potential benefits in terms of increased transparency, efficiency, and consumer trust make this a worthwhile endeavor for the future of the jewelry supply chain.

Conclusions & future work

This work presented the application of blockchain technology in the jewelry supply chain. The supply chain plays a very crucial role in the mechanical industry. This study dives into the world of jewelry supply chains, aiming to make them more trustworthy and efficient. The jewelry industry faced challenges like fake jewelry and a lack of clear information about where materials come from. Blockchain technology is an efficient way to address these challenges. Blockchain brings transparency, making it easy for everyone involved, from miners to customers, to trust and verify information. It is a super-secure and unchangeable record book that ensures the real deal in jewelry. Our journey explored Ethereum as the best tool for this transformation as it ensures data security and permanence. Using React.js, we designed a user-friendly platform to trace the entire journey of a product in the jewelry industry while prioritizing transparency. In the mechanical world of jewelry-making, a solid supply chain is key. Our blockchain-powered system isn't just about fixing problems but about improving the whole process. We are offering transparency, security, and a traceable journey for every piece of jewelry, from the mine to the customer. Imagine a world where everyone in the jewelry game, including you, can trust and verify information easily. That is the world this study aims to build - a world where the jewelry you adore is as genuine as it gets. It is not just about Industry 4.0; it's about making jewelry better!

Blockchain technology in this study can enhance transparency, traceability, and efficiency in the jewelry supply chain. Future prospects include IoT integration for real-time data capture during transport and storage, using systems like IOTA's Tangle or Ethereum's Swarm for secure data transfer. Blockchain's transparency provides rich historical data for machine learning analysis to forecast demand, optimize inventory, and address inefficiencies through techniques like time-series forecasting. Smart contracts can facilitate secure financial transactions via tokenization using Ethereum's ERC-20 or Hyperledger's Fabric, enabling automated invoicing and payments. Oracles, like Chainlink, can connect blockchains with external data for better decision-making. Zero-knowledge proofs (ZKP) can ensure privacy while maintaining transparency and regulatory compliance.

Data availibility

The datasets used and/or analysed during the current study are available from the corresponding author upon reasonable request.

Received: 3 August 2024; Accepted: 28 January 2025
Published online: 30 January 2025

References

1. Somboonwiwat, T. & Atthirawong, W. Re-engineering of business processes in the integrated supply chain of fine gemstones and jewelry industries in Thailand (2009).
2. Yiu, N. C. Decentralizing supply chain anti-counterfeiting and traceability systems using blockchain technology. *Future Internet* **13**, 84 (2021).
3. Queiroz, M. M., Telles, R. & Bonilla, S. H. Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain Manag. Int. J.* **25**, 241–254 (2020).
4. Chang, S. E. & Chen, Y. When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access* **8**, 62478–62494 (2020).
5. Li, X., Jiang, P., Chen, T., Luo, X. & Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **107**, 841–853 (2020).
6. Abeyratne, S. A. & Monfared, R. P. Blockchain ready manufacturing supply chain using distributed ledger. *Int. J. Res. Eng. Technol.* **5**, 1–10 (2016).
7. Caro, M. P., Ali, M. S., Vecchio, M. & Giaffreda, R. Blockchain-based traceability in agri-food supply chain management: A practical implementation. In *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*. 1–4 (IEEE, 2018).
8. Lu, Q. & Xu, X. Adaptable blockchain-based systems: A case study for product traceability. *IEEE Softw.* **34**, 21–27 (2017).
9. Wu, H. et al. A distributed ledger for supply chain physical distribution visibility. *Information* **8**, 137 (2017).
10. Kittipanya-Ngam, P. & Tan, K. H. A framework for food supply chain digitalization: Lessons from Thailand. *Product. Plan. Control* **31**, 158–172 (2020).
11. Toyoda, K., Mathiopoulos, P. T., Sasase, I. & Ohtsuki, T. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access* **5**, 17465–17477 (2017).
12. Fernández-Caramés, T. M., Blanco-Novoa, O., Suárez-Albela, M. & Fraga-Lamas, P. A UAV and blockchain-based system for industry 4.0 inventory and traceability applications. *Multidiscip. Digit. Publish. Inst. Proc.* **4**, 26 (2018).
13. Wang, Y., Chen, C. H. & Zghari-Sales, A. Designing a blockchain enabled supply chain. *Int. J. Product. Res.* **59**, 1450–1475 (2021).

14. Alladi, T., Chamola, V., Parizi, R. M. & Choo, K.-K. R. Blockchain applications for industry 4.0 and industrial IOT: A review. *IEEE Access* **7**, 176935–176951 (2019).
15. Molakatala, N. et al. Fraudulent practice detection in bullion trade in selling of gold jewelry through AI methods. In *International Conference on Intelligent Human Computer Interaction*. 380–393 (Springer, 2023).
16. Hawlitschek, F., Notheisen, B. & Teubner, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electron. Commerce Res. Appl.* **29**, 50–63 (2018).
17. Eisend, M. & Schuchert-Güler, P. Explaining counterfeit purchases: A review and preview. *Acad. Market. Sci. Rev.* **2006**, 1 (2006).
18. Kannabiran, G. & Bhaumik, S. Corporate turnaround through effective supply chain management: The case of a leading jewellery manufacturer in india. *Supply Chain Manag. Int. J.* **10**, 340–348 (2005).
19. Main Home - Everledger. https://everledger.io/. Accessed 29 May 2024.
20. IBM Supply Chain Intelligence Suite - Food Trust. https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust. Accessed 29 May 2024.
21. Malik, S., Kanhere, S. S. & Jurdak, R. Productchain: Scalable blockchain framework to support provenance in supply chains. In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*. 1–10 (IEEE, 2018).
22. Francisco, K. & Swanson, D. The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics* **2**, 2 (2018).
23. Abbasi, M., Prieto, J., Shahraki, A. & Corchado, J. M. Industrial data monetization: A blockchain-based industrial IOT data trading system. *Internet Things* **24**, 100959 (2023).
24. Buterin, V. et al. A next-generation smart contract and decentralized application platform. *White Paper* **3**, 2–1 (2014).
25. Sobti, R. & Geetha, G. Cryptographic hash functions: A review. *Int. J. Comput. Sci. Issues (IJCSI)* **9**, 461 (2012).
26. Zheng, X., Lu, J., Sun, S. & Kiritsis, D. Decentralized industrial IOT data management based on blockchain and IPFS. In *IFIP International Conference on Advances in Production Management Systems*. 222–229 (Springer, 2020).
27. Di Angelo, M. & Salzer, G. Characteristics of wallet contracts on ethereum. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. 232–239 (IEEE, 2020).
28. Cao, S., Foth, M., Powell, W., Miller, T. & Li, M. A blockchain-based multisignature approach for supply chain governance: A use case from the Australian beef industry. *Blockchain Res. Appl.* **3**, 100091 (2022).

Author contributions

A.P. and S.S equally contributed to initial idea generation, formulation of pseudo-codes, methodology, analysis, and original draft writing. A.D. contributed to the formulation of pseudo-codes, methodology and analysis. H.A. and V.C. contributed to initial idea generation, analysis, draft review, and supervision.

Declarations

Compeing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.