electronics

MDPI

Article

Asset Ownership Transfer and Inventory Using RFID UHF TAGS and Ethereum Blockchain NFTs

Cesar Munoz-Ausecha [1,*], Jorge Eliecer Gómez Gómez [2], Juan Ruiz-Rosero [3] and Gustavo Ramirez-Gonzalez [1]

[1] Departamento de Telemática, Universidad del Cauca, Popayán 190002, Colombia
[2] Department of Systems Engineering and Telecommunications, Faculty of Engineering, Universidad Córdoba, Montería 230002, Colombia
[3] Technology Innovation Institute (TII), Abu Dhabi P.O. Box 9639, United Arab Emirates
* Correspondence: munozausecha@unicauca.edu.co

Abstract: In the present, many organizations grow on a daily basis, using many assets to perform their activities and generate profit. In large organizations, all of these assets must be managed, occasionally leading to challenges depending on the organization's size. For this reason, the role of asset custodian is needed. This role entails assigning the fixed assets to one person for their care, maintenance, and safekeeping. In this process, it is necessary to update information in the central system, leading to further administrative processes, which, in the majority of cases, are carried out through traditional methods. This involves time to obtain wet signatures, a great deal of paperwork, and time for the person or people in charge to update the information. Due to these reasons, the process can be updated partially or entirely to use digital means in order to solve the mentioned inconveniences. This paper presents a proof-of-concept system to offer a modernized and practical solution to this problem using the advantages of blockchain technology, and speeding up the process by using assets identified with UHF RFID technology to permit the reading of many tags that can be embedded and hidden with no need for line-of-sight, allowing fast ownership transfer, using smart contracts in the Ethereum private blockchain.

Keywords: inventory; RFID UHF; ownership transfer; blockchain; NFT; Ethereum; DAPP; smart contract

Citation: Munoz-Ausecha, C.; Gómez, J.E.G.; Ruiz-Rosero, J.; Ramirez-Gonzalez, G. Asset Ownership Transfer and Inventory Using RFID UHF TAGS and Ethereum Blockchain NFTs. *Electronics* **2023**, *12*, 1497. https://doi.org/10.3390/electronics12061497

Academic Editor: Asma Khatoon

Received: 26 December 2022
Revised: 17 January 2023
Accepted: 19 January 2023
Published: 22 March 2023

1. Introduction

Asset management is not new. People and organizations have been managing assets for a very long time; however, it was not until the 1980s that the term "asset management" started to be used in the private and public sectors. To manage assets properly, an entire system is required, including the organization's structure, roles, and responsibilities, planning, operation, etc. All of these considerations are included in the international standard ISO 55000 for asset management [1]. For this reason, commonly in the case of large organizations such as universities, the role of asset custodian is needed; by using this role, the fixed assets are assigned to one person. Generally, this person is the main user of the element. In some cases, this person needs to be part of the organization in a full-time position, as the person responsible for the care, maintenance, and safe-keeping of the asset, for assurance that the element is used only for official business, and for verifying the accuracy of the information contained in the organizational information systems related to the elements in their charge, including history, value, and relevant characteristics [2]. Frequently, all information related to assets is stored in database servers, allowing more speed and flexibility in the information query process, and in some cases, the assets are identified using a visual bi-dimensional form of identification, such as bar-codes or QR codes [2]. This kind of identification requires a direct line of sight between the reader and the code. Methods such as this save time. However, systems used to manage these registers become more complex over time. For the identification of assets, new technologies emerge and evolve to

become more useful and faster; for example, far-field RFID technology permits the reading of many tags that can be embedded and hidden with no need for line-of-sight. They can be read through different materials, such as wood, plastic, cardboard, and almost any non-metallic material. There are many types of harsh environments, such as outdoors, chemically exposed environments, moist environments, and environments of unusual temperatures. This technology permits read distances in the range of 16 m away from the reader for passive tags and 100 m away for active tags [3]. For example, these are applied to manage numerous objects in supply chain environments [4–7].

Independently from an organization's activities, they possess different elements which play a role or have a function in the execution of a process. Furthermore, the relevant characteristics of these assets include a monetary value in the company balance sheet, being listed in a central record, deterioration by use, and depreciation over time [8]. Between these assets are those used by staff in their daily activities, including computational resources, machines, buildings, etc. The elements with these characteristics are classified as fixed assets. Additionally, to maintain control and traceability of the history and current value of the fixed assets, organizations keep registers that include all relevant information for each fixed asset in their life cycle. As a result, many aspects need to be managed and administered with the support of the responsible person.

The management of the information generated in the process of asset control in the present is controlled using centralized systems to organize and implement the data and management procedures [9]. This type of system can lead to inconveniences over time; for example, imprecise Building Information Modelling definitions, isolated software development, data interoperability, intellectual property, virtual property rights, skills and training requirements [10], and in the case of some organizations, many paper forms and wet signatures. These inconveniences lead to high time consumption for tasks such as the transfer of responsibilities over assets.

Consequently, in this paper, we address these inconveniences and demonstrate a solution to transfer the responsibility for assets using the RFID UHF technology for agile asset identification, which is steadily becoming more popular in the IoT environment [11]. Additionally, we demonstrate a method to use all the advantages offered by the blockchain by managing assets using non-fungible tokens (NFTs) with high encryption security and functional flexibility through the use of smart contracts, and to inherit properties such as integrity, auditability, and transparency. Finally, to exploit all of these advantages, we deploy a proof-of-concept scenario integrating these technologies in a distributed application (DAPP) to obtain feedback on the viability of the solution. In the remainder of this paper, we explore the main aspects of the DAPP, the details of the proposed solution, including the relevant characteristics and architecture details in the way the technologies communicate with each other, and demonstrate the results obtained in the deployment of the proof-of-concept solution, followed by the discussion and conclusion sections.

Related Works

In ref. [12], the authors propose an Ethereum-blockchain-based solution that captures the key interactions between supply chain trading partners using an Ethereum smart contract and a decentralized storage system. They present and discuss the main smart contract code and its algorithms that define the underlying principles of the proposed blockchain approach, validating and testing various scenarios of the overall system functionalities of the proposed solution.

In ref. [13], the authors work toward applications of a sharing economy, addressing the common problems of these platforms, the need for a Trusted Third Party, the lack of privacy when using them, and the repetitive individual sign-up for each platform. They propose a solution using Ethereum-based smart contracts to replace the intermediaries, demonstrating a web app for the sharing of objects based on a smart contract running on the Ethereum network and allowing anyone in the network to participate in the app without

signing up or disclosing their personal financial information. The objects are identified by scanning a QR code that references a key in the smart contract.

In ref. [14], the authors describe an approach to addressing limitations such as asset storage demands and non-standard user interfaces, proposing permitted blockchain usage that uses off-chain storage of the data assets, accessed through a standard browser and mobile app, and shows an implementation in the Hyperledger framework to manage patient-centered health data. In [15], the authors focus their attention on the pharmaceutical industry, presenting the concepts and architectural elements necessary to support a non-fungible token solution and presenting a prototypical application.

In ref. [16], the authors discuss the design and development of a distributed application for managing medical certificates, using a Logistic Map Encryption (LME) cipher to encrypt the existing medical certificates before passing them over a blockchain to manage the emission of medical certificates such as birth, death, and sickness (HCC) for special situations such as birth, death, and some health-related issues for employees to claim leave in their working environment. This assists fraud avoidance in the generation of medical certificates from healthcare centers.

In this research paper, in terms of the research gaps noted above, we focus on the common gap of the ownership transfer of the assets. All of the articles presented above focus on using smart contracts and NFTs for managing inventories, assets, information, and supply chains. Additionally, they use technologies such as centralized databases, encryption mechanisms, and bi-dimensional visual codes as identification mediums. It is important to note that the information in these applications is bounded to one person or entity from the first registration process and does not change over time. This research paper will present a novel design to manage the inventory of assets, allowing ownership transfer in order to transfer the responsibilities inherited from the custody of assets, using the agile identification and operation of RFID-UHF identified assets with the advantages inherent to the blockchain, including security, integrity, auditability, and transparency. This results in an agile process that removes the necessity of the intervention of third parties in the administrative process, allowing administrative personnel to focus on other tasks.

2. Approach

2.1. Scenario

Consider the following scenario presented in Figure 1. An employee of the organization, Thomas, needs to transfer the ownership of his printer to Mary. To accomplish this task, he and Mary need to fill and sign out an internal form. Additionally, it is necessary to obtain validation from Jim, the manager, in some cases. Then, this form needs to be delivered to the inventory division of the organization to validate the information and update the inventory register; to accomplish this, they need to contact the database administrator, Paul, to complete the process. Finally, Paul tells Thomas to hand the printer to Mary physically, concluding the process. Nevertheless, in organizational environments, ownership transfer is always a centralized process and requires many agents for a successful and authorized assignment. Additionally, reaching all the people involved creates an unsafe environment for the information concerned, where it can be lost or altered at any of these stages. Finally, the total control of the information is delegated to Paul, the database administrator. Under these circumstances, the process can generate a high consumption of time and an unsafe environment for information, focusing the responsibility for the process on selected people who act as mediums to make the process possible.

As mentioned in the introduction, this proof-of-concept solution is deployed in an organizational context; for its first iteration, the application is intended to be used in the area of inventory, where all the knowledge about the management and administration of assets are located, including accountability, maintenance, life cycle, and administrative procedures. We select this area because it helps to identify the requirements for the ownership transfer automation process and because the workers in this area can act as custodians and be in charge of the computers, printers, furniture, and other assets used for their daily

activities. Additionally, participation in this area contributes important feedback for the process, received directly from personnel experience and expertise.

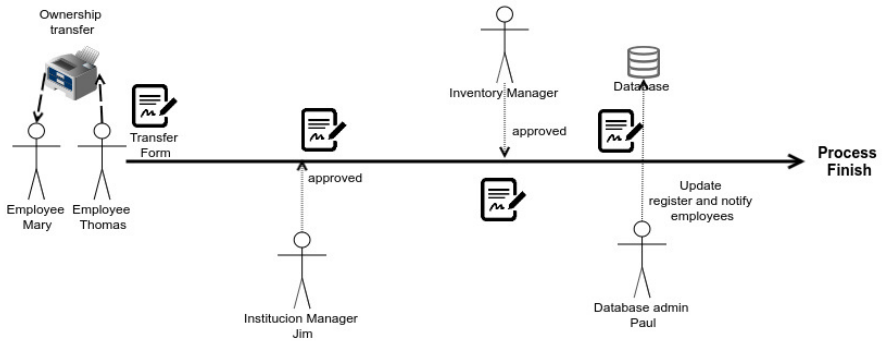

Figure 1. Problem of ownership transfer.

Initially, the prototype focuses on the basic requirements for inventory and ownership transfer processes, including the following aspects:

2.1.1. Auditability

An audit consists of the revision of documents, inventories, and other physical and documented evidence to ensure that the audited entity is following the defined procedures implemented by the organization [17]. In this particular case, we need to apply internal auditing, as this activity is defined as an independent, objective assurance and consulting activity designed to add value and improve the organization's operations [18]; in this case, we want to store all the records to complete this task.

This process can be performed using new disruptive technologies; these systems keep records of ownership and transaction timestamps, eliminating the possibility of digital copying and, thus, double-spending [19]. Additionally, the usage of smart contracts can evolve business practices by enhancing efficiency and transparency in the value chain. The fusion of these innovations is also likely to transform auditing by automating workflows, but, more importantly, by enhancing audit effectiveness and reporting [20]. Blockchain technology is designed to store information about transactions to be immutable over time, storing the information using hash technologies, and increasing the accuracy and trustworthiness of records [19]. Although blockchain technology is new, it will require auditors to develop and employ new approaches to assessing this new technology using well-established professional standards to ensure adequate assurances [21]. Blockchain technology, thanks to its characteristics (transparency, traceability, and integration of rules and procedures in the technology itself) [19] is becoming an essential tool used in government, such as in Canada, where many state dependencies are already involved. An example is the Toronto-based Blockchain Research Institute (blockchainresearchinstitute.org).

The use of this technology has some consequential, unanticipated effects on the auditor professions, requiring auditors to become more IT- rather than accounting-oriented, and creating a change in the auditor's profile in this new disruptive system [19].

2.1.2. Ease of Use

Although the blockchain is a relatively newly adopted technology, we can see significant advances in making it more accessible and available for the end user. With the development and release of new tools and mechanisms to verify and analyze data stored in blockchains using web dashboards [22], blockchains can be applied to the authentication and verification of identity to replace the usage of classic passwords [23], or alternatively to the development of new frameworks to test and develop fine-tuned blockchain applications [24]. Additionally, blockchains have been used to create electronic wallets to be used in daily devices, such as laptops and cellphones, such as the library MetaMask

(https://metamask.io/, accessed on 5 September 2022), which can be installed as an extension in the browser (Chrome, Firefox, Edge, Brave) to use cryptocurrencies and run compatible DAPPS (distributed applications) using deployed smart contracts.

2.1.3. Integrity

Integrity is one of the basic inherent characteristics of blockchain technology. In the blockchain system, the information is defined as a linked list of immutable tamper-proof blocks stored in each participating node. Each block records a set of transactions and the associated metadata. Blockchain transactions act on the identical ledger data stored in each node. [25] The blockchain was initially concieved by Satoshi Nakamoto [26]. For this reason, blockchains are used to mainly store and register all movements in the electronic currency known as Bitcoin, reaching values per unit far beyond any official currency from any country in the world. This shows a high level of trust that can be used as a reference for the level of integrity the technology manages.

The critical element of any blockchain system is the existence of an immutable tamper-proof block. In its simplest form, a block is an encrypted aggregation of a set of transactions. The existence of a block acts as a guarantee that the transactions have been executed and verified [25]. Some examples of the integrity offered by blockchains are: cloud data integrity protection [27], data integrity verification for large-scale IoT data [28], and the integration of any data to be hashed and verified any time using the tampering protection offered by blockchain technology [29].

The auditability and integrity are essential inherent characteristics of blockchain technology. In contrast, ease of use needs to be explored more deeply to implement a usable interface for the user that makes the ownership transfer of RFID UHF identified assets possible. After the booth parts agree on the transfer, the current custodian and the new receiver, in some cases, may require a supervisor's approbation to carry out the transfer of the asset and be added securely to the blockchain, using secure personal accounts in the blockchain. This will be reviewed in more detail in the following sections.

2.2. Proposed Solution

In this study, we used Ethereum Solidity smart contracts to manage user information and provide a means for users to access the data contained in the blockchain using a web interface based on libraries such as WEB3.js and META MASK wallet, and a gateway to blockchain apps, viable to be used in Chrome and other web browsers and Android or iOS mobile applications.

The contracts in Ethereum can be expressed as computer programs with well-defined semantics, using Solidity language that allows a well-defined design and flexible functionality. On the other hand, Bitcoin contracts work in a different way using a limited script structure and cryptographic protocols, where participants send/receive messages, verify signatures,and put/search transactions on the blockchain [25]; for this reason, Ethereum was selected as a base blockchain server to implement the smart contracts to manipulate and register all the changes to be handled by the distributed application, including the register of user accounts, the register of the active assets that the organization uses for its missions, and the necessary relations to have the role of custodian of one asset using non-fungible tokens (NFTs) to hold and reference every asset registered by the DAPP. This token is a non-interchangeable unit of data stored on a blockchain, a form of digital ledger, that can be sold and traded. [30] This NFT is part of the blockchain technology and, due to its nature, can be used by the smart contracts to expand its functionality; in this case, to be used as a unique ID of every asset, and allowing it to be traded, following the rules defined and programed in the smart contract developed in Solidity.

Deployment in this scenario uses a private blockchain with two predefined users to control the register process of the assets and the repeatability delegation, but it is possible to deploy the same smart contracts using the Ethereum public networks. However, in the main public networks, we cannot control the data chain and the users that have access, and

the costs of running the DAPP in the blockchain in exchange for the costs of infrastructure can be left aside.

The server and miner can be wrapped as Docker containers, allowing the creation of new nodes to spread and grow the network while decreasing the complexity through version control in medium and small deployments; for reference, we include the parameters used to run Geth for the initial node in Table 1, and the parameters to run a miner instance in Table 2. The fields with N/A do not receive parameters.

Table 1. Ethereum main node configuration parameters.

Parameter	Description	Value
datadir	Data directory for the databases and keystore (default: " /.ethereum")	./datadir
nat	NAT port mapping mechanism (any/none/upnp/pmp/extip:(IP)) (default: "any")	extip:hostname -i
netrestrict	Restricts network communication to the given IP networks (CIDR masks)	172.17.0.0/16
syncmode	Blockchain sync mode ("snap", "full" or "light") (default: snap)	'full'
rpc	Starts the rpc interface	N/A
rpcaddr	Sets the address of the rpc interface	'0.0.0.0'
rpcapi	Limits access via rpc to certain apis	'personal,eth,net, web3,txpool,miner'
unlock	Comma-separated list of accounts to unlock	"0xEb2D..."
password	Password file to use for non-interactive password input	pass.txt
allow-insecure-unlock	Allow insecure account unlocking when account-related RPCs are exposed by http	N/A
mine	Enable mining	
console	Start an interactive JavaScript environment	N/A

Table 2. Ethereum miner configuration parameters.

Parameter	Description	Value
datadir	Data directory for the databases and keystore (default: " /.ethereum")	./datadir
bootnodes	Comma separated enode URLs for P2P discovery bootstrap	N/A
netrestrict	Restricts network communication to the given IP networks (CIDR masks)	172.17.0.0/16
unlock	Comma-separated list of accounts to unlock	"0x77a8..."
password	Password file to use for non-interactive password input	pass2.txt
mine	Enable mining	N/A
miner.threads	Number of CPU threads to use for mining (default: 0)	1
miner.etherbase	Public address for block mining rewards (default = first account) (default: "0")	"0x00"

After the blockchain is deployed, it is necessary to provide a user interface to the users interested in our DAPP; for this, we use frameworks such as nodeJs for smart-contract generation and ReactJs for the user interface. Additionally, we use libraries such as Ethers

to interact with the smart-contract functions and truffle to translate the contracts written in Solidity language(.sol) to JSON format and be imported and used using Ethers. Finally, we use the openzeppelin library to implement the interaction and implementation of the standard for managing assets using non-fungible tokens (NFTs) normalized by the standard ERC-721. All the tokens generated have a globally unique 256 bit variable called tokenId; this value is often used in DAPPs to generate visual outputs, such as obtaining a unique variant of an image of a cat, alien, or abilities in a game. All of this is an aleatory result and provides fun in some games, and it cannot be considered to have real worth, despite attempts to argue otherwise in mediums such as media galleries and games. In contrast, the correct usage may be the identification and proof of ownership for objects from the real world.

All the web implementation runs in a server and exposes a web application to be available via HTTPS protocol over the Internet, allowing interaction with the blockchain smart contract through the web browser plugin MetaMask and allowing DAPP interoperability through JavaScript libraries; this can be observed in Figure 2.

It is important to keep in mind the codification of the tags; in this case, we implemented the RFID application to use the Fast-ID functionality. With this configuration, the reader uses the Electronic Product Code (EPC) programmed by the user, and the Tag Identification (TID), a read-only code programmed in the factory, to identify every produced TAG. This results in a unique code to prevent and reduce counterfeit, duplicity, and false-positive identifications.

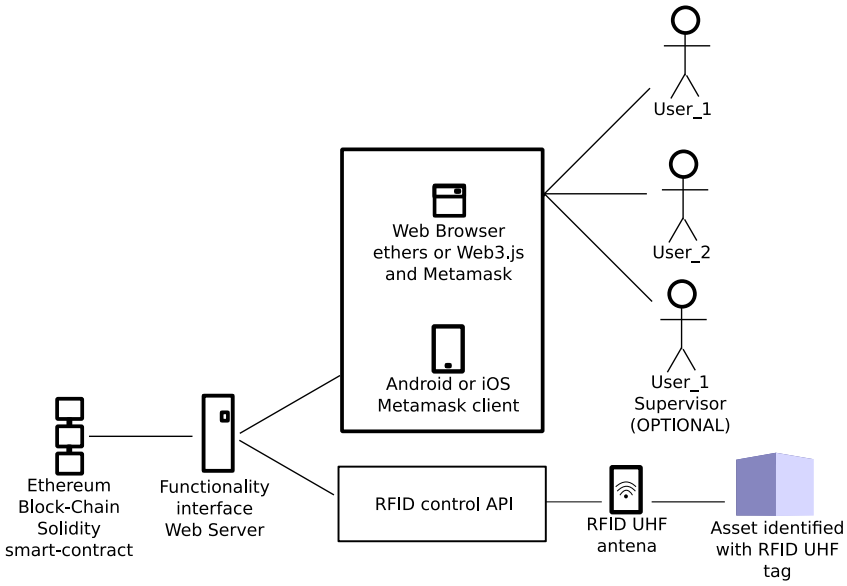

Figure 2. Solution architecture.

2.3. Architecture

Figure 2 illustrates the parts included in the system to allow the users to interact with the blockchain, using their personal account in the blockchain through the Metamask Ethereum wallet and making use of all the advantages that the blockchain system has to offer.

2.3.1. Ethereum

On the server side, Ethereum is a open-software platform based on blockchain technology, described as follows: "Ethereum is open access to digital money and data-friendly services for everyone no matter your background or location. It is a community-built technology behind the cryptocurrency ether (ETH) and thousands of applications you can use today" [31]. In the public blockchain, Ethereum can be used to send cryptocurrency to anyone for a small fee. It also powers applications that everyone can use and which no one can take down. Additionally, Ethereum is described as the world's most programmable

blockchain, enabling anyone to build and deploy decentralized applications called DAPPs to manage different digital assets, even bitcoin [31]. This flexibility in programmability is the main feature used in the proposed solution, because in Ethereum, contracts can be expressed as computer programs with well-defined semantics using Solidity programming language. On the other hand, Bitcoin contracts work differently; they are defined using cryptographic protocols, where participants send/receive messages, verify signatures, and put/search transactions on the blockchain [32].

2.3.2. Functionality Interface Web Server

On the server side, we used a web server running a React application, based on Ethers—an Ethereum Javascript API—to interact with the Ethereum blockchain [33] using a web interface. Additionally, the contracts were exported to be used by the web application using NodeJS and the truffle library.

2.3.3. Web Browser or Mobile APP + MetaMask

On the user side, it is necessary to use a web browser. Additionally, this browser must be compatible with MetaMask, the connection manager to the Ethereum blockchain, as MetaMask uses JSON RPC API to communicate and interact with the blockchain [34]. At the present moment, MetaMask is compatible with Firefox and Chrome, both popular web browsers, allowing users to manage accounts and their keys in a variety of ways, including hardware wallets, while isolating them from the site context. As a result, users can use this combination to access the distributed app (DAPP) web interface and interact with the data stored in the blockchain using their Ethereum account, configured in the MetaMask add-on in the browser.

2.4. RFID Ownership Transfer

The RFID UHF ownership-transfer method is used to define if the alteration of the tag information is necessary (optional data field usage for additional security information). The ownership of the fixed assets needs to be transferred securely to a new owner, as previously studied. For example, ownership transfer may resist cloning attacks and side-channel attacks [35], or focus on secure communications [36], digital fingerprint result of the physical attributes [37], temporal ownership transfer [38], or include people in the process using assistant tags [39]. Even so, in organizational environments, ownership transfer needs to be carried out from one person to another in different scenarios, such as the transference of the owner to a new division in the organization, renewal of the assets to modern versions, or extreme causes such as the death of the original owner.

User cases include direct transfer without a supervisor, supervised transfer with optional third-party authorization, and administrative transfer due to permanent inability of the current custodian in charge.

RFID ownership can be transferred by changing the passwords of the tag and storing the information only to be used by the current user that has the privileges of ownership over the asset. Every time the assets change their ownership this must be carried out, as it is necessary to have somebody able to perform the process if any of the participants cannot participate in the process due to external factors.

2.4.1. DAPP Login

As we can observe in Figure 3, to start the ownership transfer process, the user needs to be logged in using a valid account in the blockchain; in this case, the connection to the distributed network was made using a DAPP designed to work using the browser. To make this possible, it is necessary to use MetaMask, a browser complement that manages account funds and additionally allows interaction with smart contracts deployed in the Ethereum network using the functions developed as smart contracts, through the Ethers library in React to process and manipulate the information stored in the blockchain.

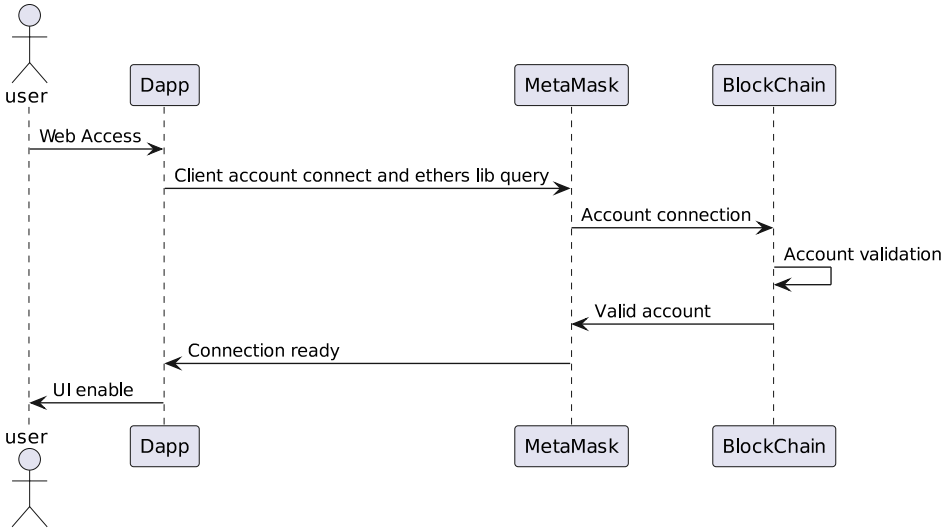

Figure 3. DAPP login process.

2.4.2. Asset Register

The smart contract deployed in the blockchain allows the registration of the assets in the system; the active assets need to be registered by one allowed user in the inventory or financial division. In this area, they manage all the new assets purchases. Once the asset is registered in the blockchain, it generates a new (NFT) unique code for that asset, including the RFID identifier, RFID security information, a first user with authority over the asset and a detailed description to avoid the counterfeiting of the identified asset in the future. If there is additional information, it can be stored in a traditional server when it is necessary to append extensive descriptions and media, such as photos, videos, and documents related to the new asset. This process can be observed in detail in the Figure 4.

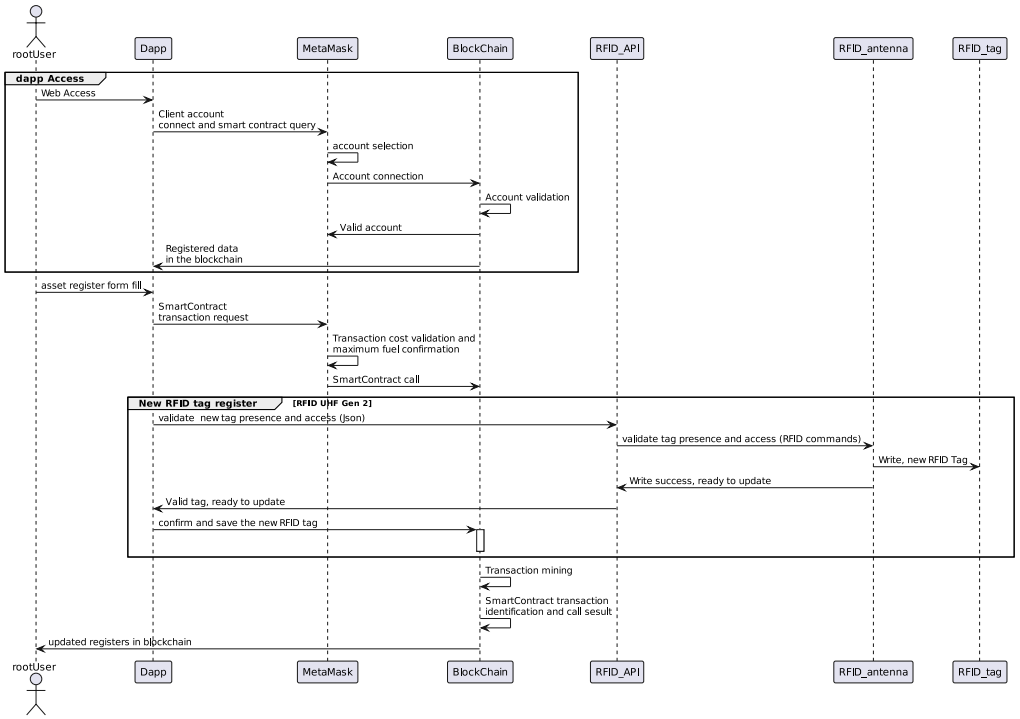

Figure 4. Asset register.

2.4.3. Direct RFID Ownership Transfer Query and Accept

With the assets registered in the distributed information system in the blockchain, the person in charge of the assets can perform the first transfers of ownership of the assets in their charge, with one difference compared to funds and regular NFTs. In this case, we are not receiving money or valuable goods that we can expend freely. For this application, we are receiving the ownership of one asset and its inherited responsibilities, including knowing the asset's state and location, and performing the respective maintenance.

For this reason, the new owner does not receive the asset directly; they receive a request to be the person assigned to be in charge of the asset and carry out all the tasks involved with the obligations and responsibilities dictated by the inventory division.

Internally, the asset identified by a unique NFT in the blockchain and by a unique RFID Electronic Product Code (EPC) in the real world using an RFID tag UHF generation II needs to complete two processes to complete the transference completely and successfully. First, if the user accepts the transference, they need to possess the asset and have a device equipped with RFID capabilities to request the information about the codes and passwords saved in the RFID Tag (Figure 5 in the section "RFID ownership transfer"), Once the information is read and decrypted from the blockchain it can be used to change and rewrite the access information to the tag, using a translator to run the commands in the RFID tags using a compatible antenna (Figure 5 in the section "RFID command process"). If the tag is found and can be accessed and updated, the process concludes by appending the information about the new user and the new parameters for the RFID Tag in the blockchain.

The following process must be completed to achieve an ownership transfer for one asset. First, user 1, the current owner of the asset, needs to make a request to user 2 to accept the transfer of asset ownership using the DAPP; the user logs into the application and queries the assets in their charge, and makes a transfer query of the asset. Internally, the request is queued, and left as pending for user 2 to respond if they accept the transfer. This process can be seen in Figure 6 in the section "Asset transfer request query".

In the second step, the second user (user 2) must log in to the DAPP using their account, along with the assets in their charge, to receive the transfer request. At this point, user 2 can review the information of the asset requested to be in their charge and accept the ownership transfer if they recognize the asset and the person that placed the request. This process can be seen in Figure 6 in the section "Asset transfer request accept".

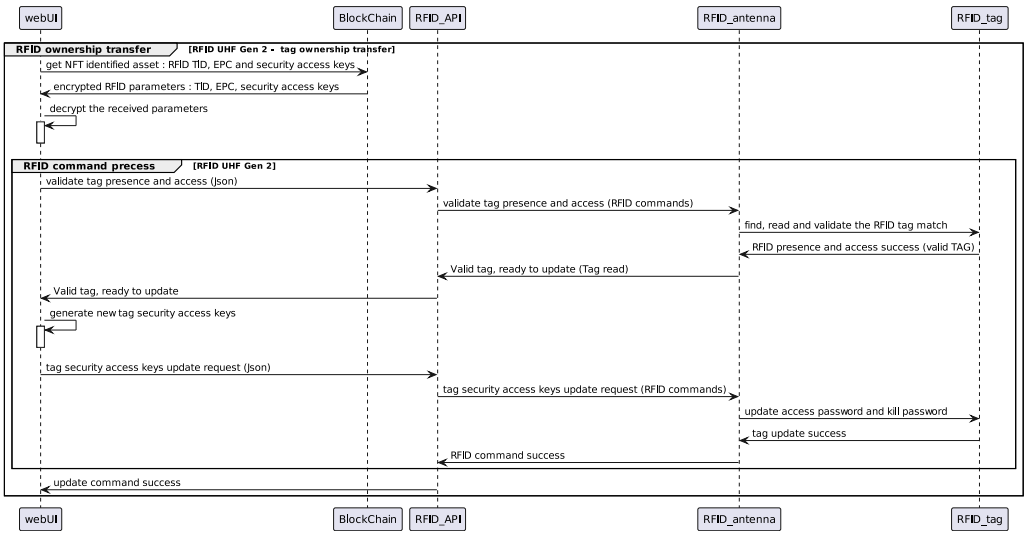

Figure 5. RFID ownership transfer process.

Finally, the next time that user 1 logs into the application, the requested asset for transfer is removed from the queue and from their owned assets list, such as if "the funds were transferred to the new account".

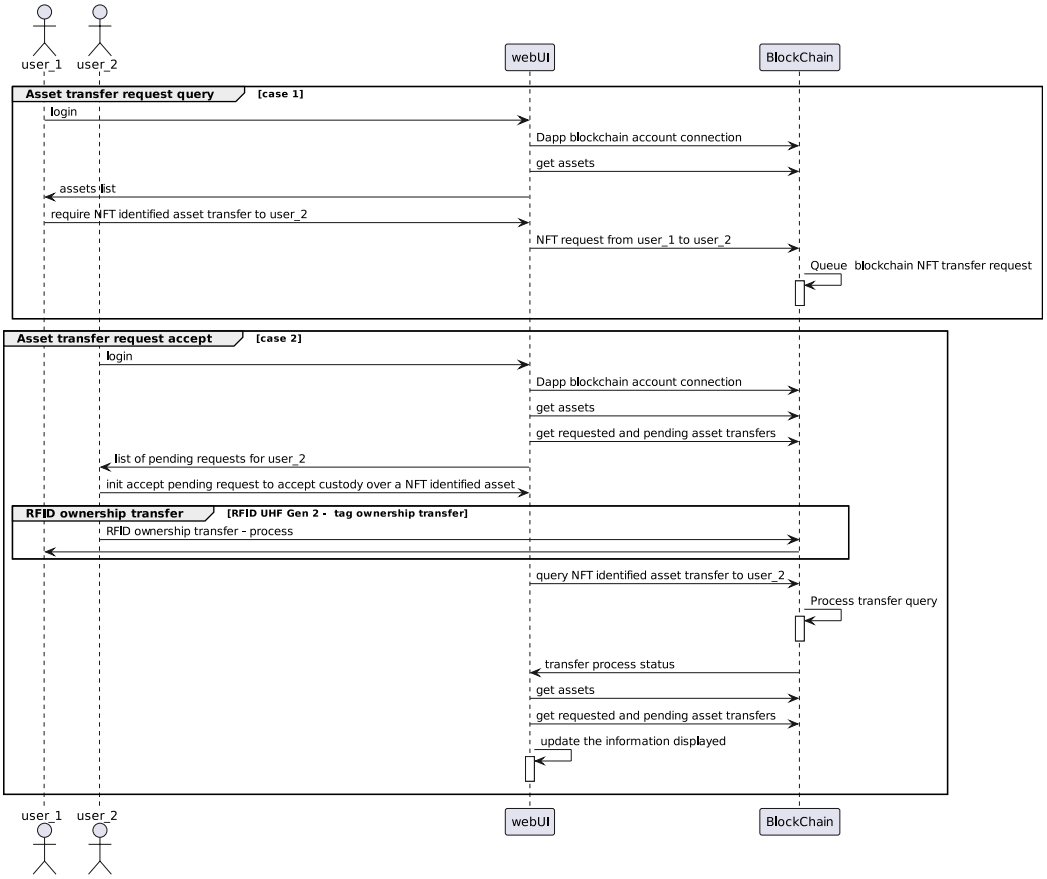

Figure 6. Ownership transfer query and accept process.

2.4.4. Supervised Ownership Transfer

In addition to the direct transfer option between two users, in some cases, the division supervisor must be informed and approve the transfer of the asset to a new person for reasons related to the usage or availability of the asset in the division. In this case, it is necessary to obtain the validation of the supervisor. To carry out this process, user 1 starts the ownership transfer process normally, but in this case, asset A in their registration process has been defined with a supervisor; this means that any ownership transfer needs to be approved before any further step, as shown in Figure 7 in the section "Supervisor validation process". This validation needs to be carried out before any request is placed to be reviewed by user 2, allowing control of special assets with specific characteristics and avoiding the movement of critical resources.

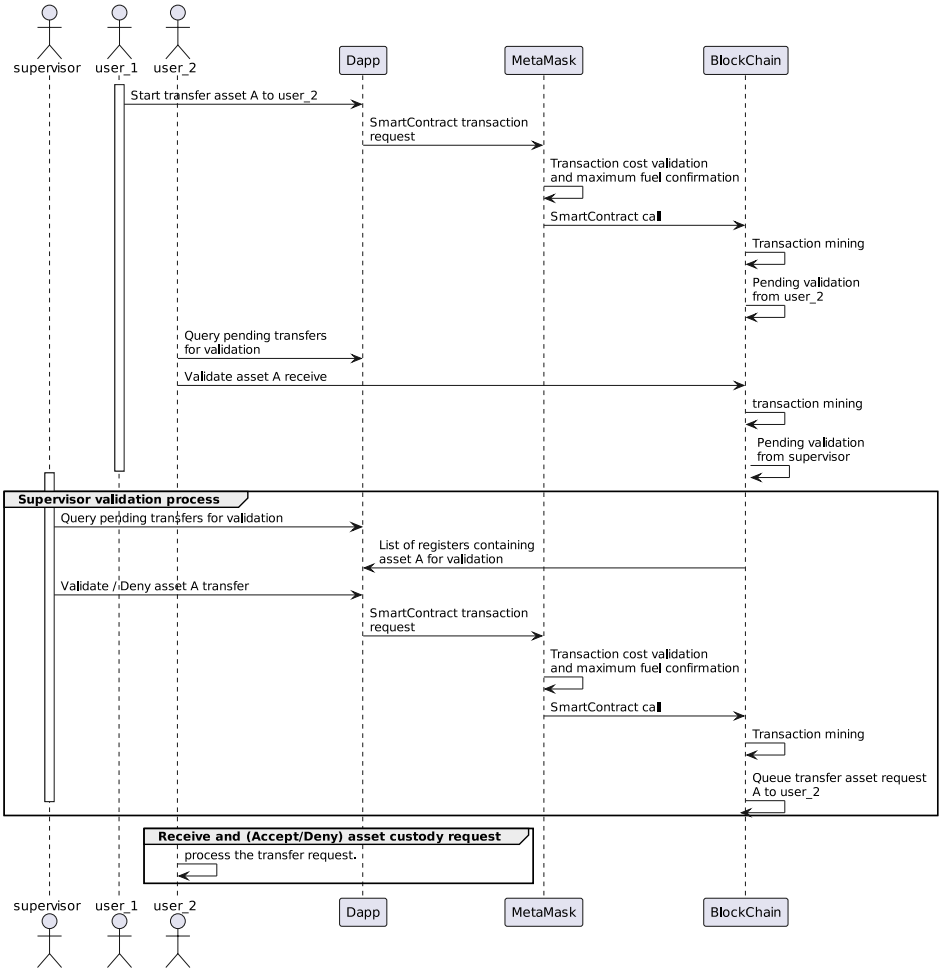

Figure 7. Supervised ownership transfer.

3. Results and Analysis

The DAPP was deployed in the inventory division of the University of Cauca in Colombia, and the applications were deployed using the local speaker's language. Additionally, we used a private blockchain configuring Ethereum as mentioned in Tables 1 and 2, configured to work using the RPC communication. Moreover, this system requires the browser extension MetaMask to interact with and carry out operations over a blockchain network. Additionally, as a development and testing environment, the Remix project was used to write smart contracts using Solidity language to implement the functions required by the system. Furthermore, we deployed the proposed system using a decentralized application designed using Web, with React and Ethers as mentioned in the Proposed solutionsection, and React Native for the mobile clients in the Chainway devices.

For DAPPS, the main difference is that Ethereum must be paid to run or operate any function of the DAPP in the blockchain network, as shown in Figures 8 and 9. MetaMask shows the block-chain requests to review and confirm the operations and costs. In this case, we are registering a new asset with an estimated cost of GAS 0.00028597. Generally, the estimated cost is very accurate, as we can observe in the confirmation received in the transaction log on MetaMask in Figure 10.

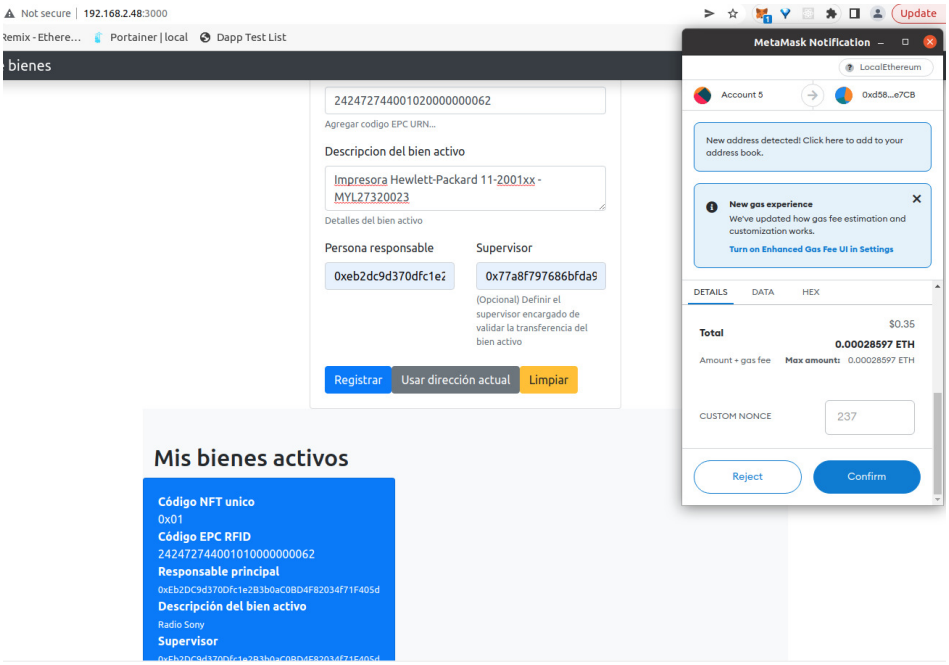

Figure 8. DAPP new asset registration form in Spanish, waiting for confirmation to operate using MetaMask, with a cost of ETH 0.00028597.

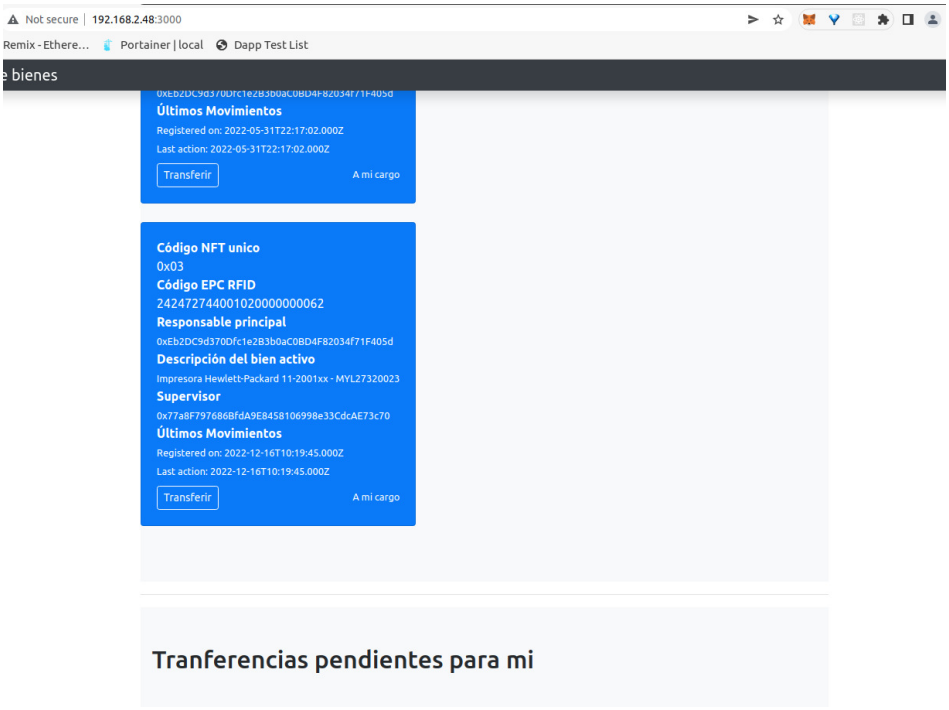

Figure 9. DAPP new register entry in the list of owned assets for the current active account in MetaMask, displayed in Spanish language.

To manage the RFID identification of the assets, we used UHF generation-II-compliant tags and a reader, as shown in Figure 11. The Tag shown in the left panel (a) is a rigid tag used for metallic assets, and the Tag displayed on the right is a soft adhesive tag used to identify plastic, wood, and cardboard assets, and finally in the center is the Chaninway C72 Reader used to access the smart contracts and the information stored in the DAPP in Figure 12. Using these elements and the personal user accounts, we transferred the ownership from one person to another in the organization.

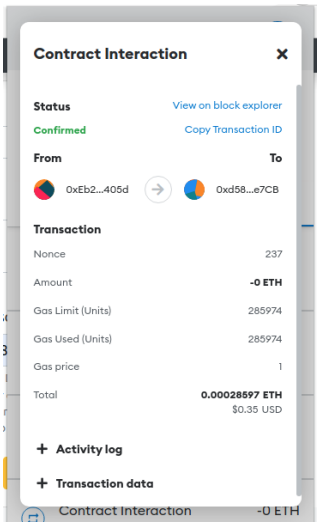

Figure 10. Screen capture of DAPP asset register transaction log entry in MetaMask showing the final cost of registering a new asset.

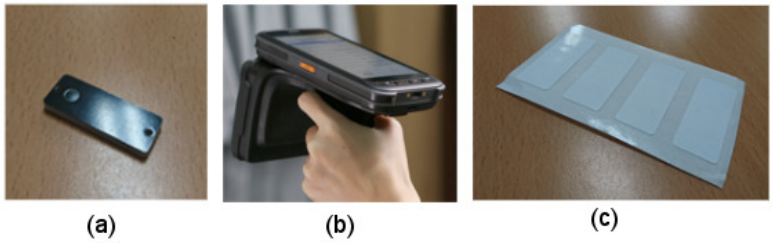

Figure 11. Used RFID UHF used elements used to identify the assets: (**a**) RFID UHF GEN II rigid solid TAG for metallic assets. (**b**) Android-based RFID UHF GEN II portable reader hand-held model Chainway C72. (**c**) RFID UHF GEN II adhesive plastic TAG for plastic, wood, and cardboard assets.

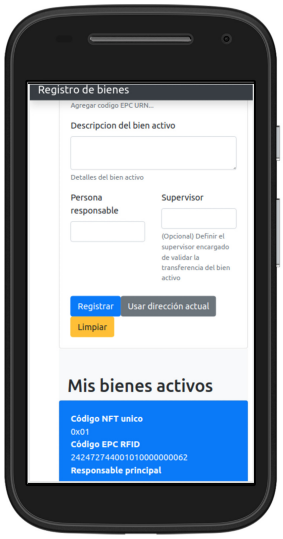

Figure 12. Chainway C72 RFID UHF GEN II portable reader, mobile DAPP showing the form to register new assets and the list of assets currently assigned in Spanish language.

In the migration of data from samples collected from the regular existent information system, we found asset registers with detailed description characteristics in text format. This information has between approximately 100 and 1100 characters. For this reason, the transaction cost can be a decisive factor in deploying the smart contract in a public

blockchain. For this reason, we measured the cost for character strings to be registered in the application in Figure 13 for small strings and descriptions, and Figure 14 for longer strings, to have a reference of the costs by transaction, to conserve the pure decentralized nature of the information offered by DAPPS, and to avoid the requirement for any centralized database or information system.

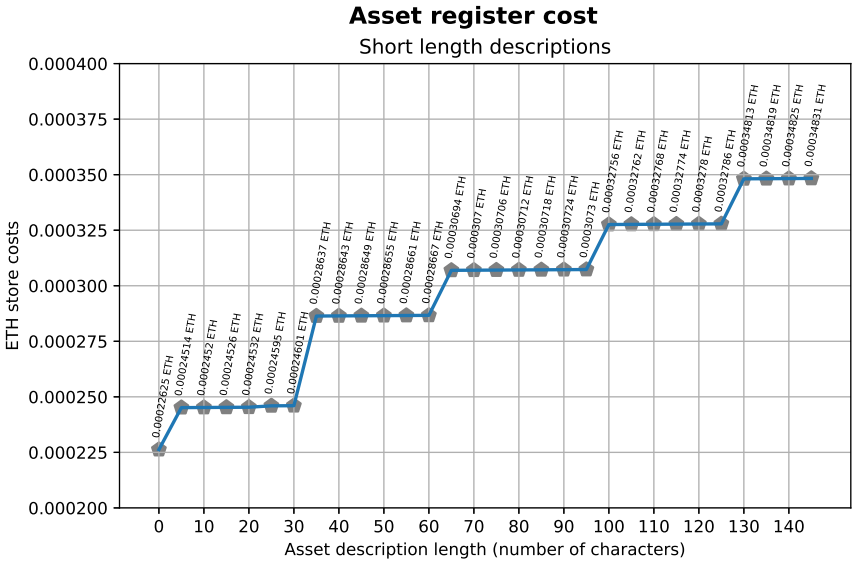

Figure 13. Ethereum cost to save a short length string description for the assets in blockchain by the DAPP. In total, 0 characters cost ETH 0.00022625, and 145 characters cost ETH 0.00034831.

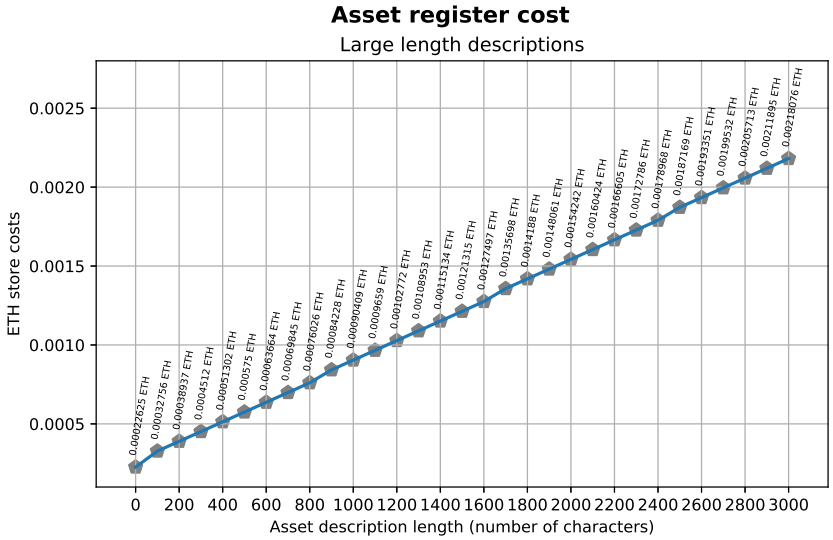

Figure 14. Ethereum cost to save a long-length string description for the assets in the blockchain. In total, 100 characters cost ETH 0.00032756, and 3000 characters cost ETH 0.00218076.

In our test case, the blockchain deployed and used was private, we controlled the funds, and the information was stored between the allowed nodes deployed, making it possible to avoid the mining process costs to append information to a public blockchain. However, in contrast, the organization has to use its computational infrastructure or pay to use services in the cloud. For example, in our case, the deployment was made using Microsoft Azure services to deploy multiple virtual machines using the Standard_B1s template instances with one vCPU and 1 GB of RAM. For our test, we used four nodes. The first one was used for RPC access to attend clients, two were used as miners and replication backups to complete the requested transactions, and one instance to serve

the Web Front-End developed using React for the users. The application's behavior and resource consumption can be seen in Figure 15 for the RPC server and Figure 16 for one of the replication instances.

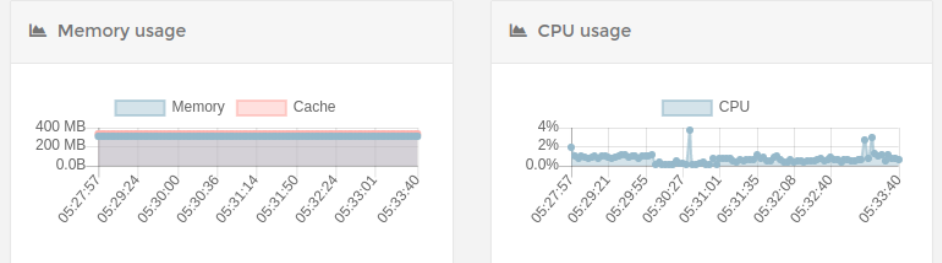

Figure 15. Docker CPU and memory utilization for the instance serving RPC and transactions for the clients during the test.

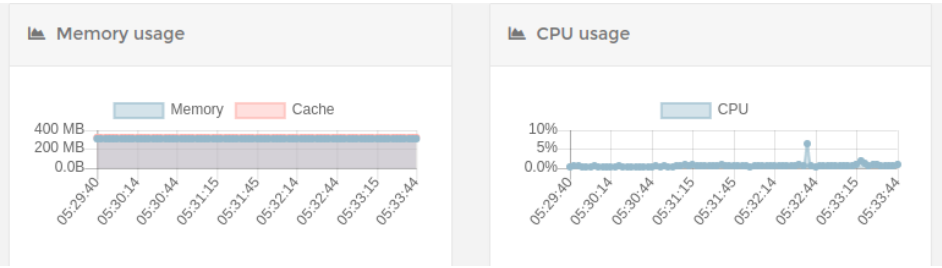

Figure 16. Docker CPU and memory utilization for one instance of mining and replicating the transactions requested during the test.

4. Discussion

In the process of this study, we found different challenges and questions, such as private blockchain usage. This model is becoming popular for private businesses and personal applications [40–44]. Nevertheless, the usage of public blockchain networks cannot be denied. This is reflected in the value of some currencies, such as Bitcoin or Ethereum, reflecting high levels of trust in the users as if it were a bank [45]. Another option could be the implementation of a consortium model using the National Research and Education Networks (NREN) infrastructure, keeping the data anonymous between users using libraries such as SEPIA [46], or for government environments where different organizations have IT infrastructure to deploy distributed solutions [47,48]. However, this requires articulating organizations connected to the NREN network or government order and regulation, which is currently in progress in some countries, including Colombia [49–54], but this took a considerable amount of time.

In the process of deploying the proof-of-concept scenario, we perceived a barrier in the blockchain technology usage. In some cases, people had not heard of it. This represents a challenge to be addressed in future works because it is necessary for the integration of more intuitive wallets [55–57] and may cause trouble for the RFID ownership transfer process. Hence, investigations are searching for secure ways to identify the users for DAPPS, such as that identified in this paper through the usage of biometrics, lowering the complexity of approving transactions in the blockchain [58]. The resolution of this inconvenience can lead to or result in new paths to WEB 4.0 available to anyone [59].

Blockchain is indeed a secure technology, as can be appreciated in the number of transactions and its currency value (ETH 1 equals about to USD 1583 in January 2023). Nevertheless, it is not one hundred percent secure for various reasons, such as possible human errors in the code of smart contracts, Solidity language limitations as listed on the Common Weakness Enumeration (CWE) list; for example, Self-Destruct, CWE-284; Improper Access Control, and Mishandled Exceptions, CWE-252; Unchecked Return Value, and Re-Entrancy, CWE-841; and Improper Enforcement of Behavioral Workflow. As a result, rigorous testing, security analysis, and the support of automated tools to identify

common vulnerabilities are necessary. For these instances, we have Oyente, ContractWard, NPChecker, and ContractFuzzer, among others [60].

RFID technology represents a large advantage in determining asset presence to carry out ownership transfer in ideal conditions. However, it is necessary to add additional security measures, keeping in mind the possible attack vectors [11], such as using clipped tags or watermarks [61–64] in a way to detect tamper attempts for a good level of trust [65], to avoid counterfeits and tag swaps in the assets. Nevertheless, RFID owner transfer using mobile devices is not new [36]; the expansion of the uses and scenarios involving RFID and blockchain advances to the final user has created new requirements and scenarios, such as that in this paper, to use the register of previous owners [66] differing from some industrial environments where untraceability is desired [67]. In general, we can see advances and flexibility in the technology and techniques to cover all these emerging scenarios.

The usage of blockchain and RFID UHF technology opens a wide range of possibilities and challenges. At the present moment, we have numerous tools and resources at hand to use. Additionally, we appreciate the expansion and optimization of both technologies to make them more lightweight and fast in the case of blockchains [68,69] and secure in the case of RFID [70–72], resulting in a more reliable and secure environment to generate new solutions.

5. Conclusions

As a result of this study, we found that the solution proposed can be beneficial for organizations with many assets in their inventory. However, in Colombia, there still exists a custom or preference for the use of paper and wet signatures, mainly in the public or government environments where these practices are regulated. Additionally, depending on the division, leaders are pessimistic about new technologies due to the time that specific systems have been working or have been part of regulated processes. This is why the new systems and applications need to be in harmony and deeply integrated with the standards and patterns established; for example, with mobile devices. In contrast, some participants with an affinity for technology show considerable interest in this solution, interested mainly in more flexible ways to perform these transactions in a secure and trustworthy manner. Additionally, they state special interest in third-person validation, to have the approval of the persons in charge to additionally act as a witness of the process and avoid misunderstanding and human error because it is required that the two persons and the asset identified using RFID need to be in mutual accordance. Therefore, the usage of blockchain technology, including smart contracts and NFTs with a connection to the real world through RFID UHF, is a very symbiotic relationship. Moreover, in the deployment of the proof-of-concept DAPP, we found that it was possible to exert secure control and ownership transfer of assets between the users registered in the platform. More research efforts are needed to formalize aspects such as full-security analysis from the DAPP to the physical RFID tag in the real world being necessary new techniques. Another future extension of this work is studying the implementation and usage of blockchain and standard IPv6 or EPC identifiers through RFID UHF tags.

The usage of blockchain technology allows the production of very flexible and complex solutions for different environments, presenting one attractive alternative to centralized Software Architecture Patterns for applications where transparency, immutability, and security are critical; even more important than the value to pay for the service. Moreover, Ethereum especially has an advantage over other distributed systems thanks to the number of frameworks and open-source libraries available. Additionally, the powerful code definition language using Solidity offers a higher level of complexity in the possible operations and its deep integration with the Web technology using Remote Procedure Call (RPC) interfaces that allow a wide range of client devices.

Author Contributions: Conceptualization, C.M.-A. and J.E.G.G.; methodology, C.M.-A. and J.R.-R.; software, C.M.-A.; validation, C.M.-A. and J.E.G.G.; writing—original draft preparation, C.M.-A. and J.E.G.G.; writing—review and editing, J.R.-R. and G.R.-G.; supervision, G.R.-G.; project administra-

tion, G.R.-G.; funding acquisition, G.R.-G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was conducted as part of the MSc program in Telematic Engineering at the Universidad del Cauca, Popayán, Colombia, and by the Universidad del Cauca (501100005682).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Institute of Asset Management. *Asset Management—An Anatomy*; Institute of Asset Management: Bristol, UK, 2011.
2. Peterson, R.H. *Accounting for Fixed Assets*; John Wiley & Sons: Hoboken, NJ, USA, 2002.
3. Kaur, M.; Sandhu, M.; Mohan, N.; Sandhu, P.S. RFID technology principles, advantages, limitations & its applications. *Int. J. Comput. Electr. Eng.* **2011**, *3*, 151.
4. Gaukler, G.M.; Seifert, R.W.; Hausman, W.H. Item-level RFID in the retail supply chain. *Prod. Oper. Manag.* **2007**, *16*, 65–76 . [CrossRef]
5. Helo, P.; Szekely, B. Logistics information systems—An analysis of software solutions for supply chain co-ordination. *Ind. Manag. Data Syst.* **2005**, *105*, 5–18 . [CrossRef]
6. Prater, E.; Frazier, G. Future impacts of RFID on e-supply chains in grocery retailing. *Supply Chain Manag. Int. J.* **2005**, *10*, 134–142. . [CrossRef]
7. Melski, A.; Thoroe, L.; Schumann, M. Managing RFID data in supply chains. *Int. J. Internet Protoc. Technol.* **2007**, *2*, 176–189. [CrossRef]
8. Davis, R. An introduction to asset management. *Retrieved Novemb.* **2016**, *20*, 2016.
9. Gharaibeh, N.G.; Darter, M.I.; Uzarski, D.R. Development of prototype highway asset management system. *J. Infrastruct. Syst.* **1999**, *5*, 61–68. [CrossRef]
10. Roberts, C.J.; Pärn, E.A.; Edwards, D.J.; Aigbavboa, C. Digitalising asset management: Concomitant benefits and persistent challenges. *Int. J. Build. Pathol. Adapt.* **2018** , *36*, 152–173. [CrossRef]
11. Munoz-Ausecha, C.; Ruiz-Rosero, J.; Ramirez-Gonzalez, G. RFID Applications and Security Review. *Computation* **2021**, *9*, 69. [CrossRef]
12. Omar, I.A.; Jayaraman, R.; Salah, K.; Debe, M.; Omar, M. Enhancing vendor managed inventory supply chain operations using blockchain smart contracts. *IEEE Access* **2020**, *8*, 182704–182719. [CrossRef]
13. Bogner, A.; Chanson, M.; Meeuw, A. A decentralised sharing app running a smart contract on the ethereum blockchain. In Proceedings of the 6th International Conference on the Internet of Things, Stuttgart, Germany, 7–9 November 2016; pp. 177–178.
14. Rouhani, S.; Butterworth, L.; Simmons, A.D.; Humphery, D.G.; Deters, R. MediChain^{TM}: A secure decentralized medical data asset management system. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1533–1538.
15. Chiacchio, F.; D'Urso, D.; Oliveri, L.M.; Spitaleri, A.; Spampinato, C.; Giordano, D. A Non-Fungible Token Solution for the Track and Trace of Pharmaceutical Supply Chain. *Appl. Sci.* **2022**, *12*, 4019. [CrossRef]
16. Rupa, C.; Midhunchakkaravarthy, D.; Hasan, M.K.; Alhumyani, H.; Saeed, R.A. Industry 5.0: Ethereum blockchain technology based DApp smart contract. *Math. Biosci. Eng.* **2021**, *18*, 7010–7027. [CrossRef] [PubMed]
17. Times, T.E. *What is Audit? Definition of Audit, Audit Meaning*; Times Publishing Company: Nueva Delhi, India 2022.
18. Institute of Internal Auditors; Research Foundation. *International Professional Practices Framework (IPPF)*; Institute of Internal Auditors: Lake Mary, FL, USA, 2009.
19. Brender, N.; Gauthier, M.; Morin, J.H.; Salihi, A. The Potential Impact of Blockchain Technology on Audit Practice. *J. Strateg. Innov. Sustain.* **2019**, *14*, 2. [CrossRef]
20. Rozario, A.M.; Thomas, C. Reengineering the audit with blockchain and smart contracts. *J. Emerg. Technol. Account.* **2019**, *16*, 21–35. [CrossRef]
21. Rooney, H.; Aiken, B.; Rooney, M. Q. Is internal audit ready for blockchain? *Technol. Innov. Manag. Rev.* **2017**, *7*, 41–44. [CrossRef]
22. Dillenberger, D.N.; Novotny, P.; Zhang, Q.; Jayachandran, P.; Gupta, H.; Hans, S.; Verma, D.; Chakraborty, S.; Thomas, J.; Walli, M.; et al. Blockchain analytics and artificial intelligence. *IBM J. Res. Dev.* **2019**, *63*, 5:1–5:14. [CrossRef]
23. Cresitello-Dittmar, B. *Application of the Blockchain for Authentication and Verification of Identity*; Independent Paper. 2016. Available online: https://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf (accessed on 20 December 2022).
24. Shbair, W.; Steichen, M.; François, J. Blockchain orchestration and experimentation framework: A case study of KYC. In Proceedings of the IEEE/IFIP Man2Block 2018-IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 27 April 2018.
25. Gupta, S.; Sadoghi, M. Blockchain transaction processing. *arXiv* **2021**, arXiv:2107.11592.
26. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008** , *1*, 21260.
27. Wei, P.; Wang, D.; Zhao, Y.; Tyagi, S.K.S.; Kumar, N. Blockchain data-based cloud data integrity protection mechanism. *Future Gener. Comput. Syst.* **2020**, *102*, 902–911. [CrossRef]

28. Wang, H.; Zhang, J. Blockchain based data integrity verification for large-scale IoT data. *IEEE Access* **2019**, *7*, 164996–165006. [CrossRef]
29. Kalis, R.; Belloum, A. Validating data integrity with blockchain. In Proceedings of the 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia, Cyprus, 10–13 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 272–277.
30. Wang, Q.; Li, R.; Wang, Q.; Chen, S. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv* **2021**, arXiv:2105.07447.
31. Buterin, V. What is Ethereum? Ethereum Official Webpage. 2016. Available online: Http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html (accessed on 5 February 2022).
32. Lande, S.; Zunino, R. SoK: Unraveling Bitcoin smart contracts. *Princ. Secur. Trust LNCS* **2018**, *10804*, 217.
33. Panda, S.K.; Satapathy, S.C. An Investigation into Smart Contract Deployment on Ethereum Platform Using Web3. js and Solidity Using Blockchain. In *Data Engineering and Intelligent Computing*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 549–561.
34. Lee, W.M. Using the metamask chrome extension. In *Beginning Ethereum Smart Contracts Programming*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 93–126.
35. Li, Q.S.; Xu, X.L.; Chen, Z. PUF-based RFID ownership transfer protocol in an open environment. In Proceedings of the 2014 15th International Conference on Parallel and Distributed Computing, Applications and Technologies, Hong Kong, China, 9–11 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 131–137.
36. Chen, C.L.; Chien, C.F. An ownership transfer scheme using mobile RFIDs. *Wirel. Pers. Commun.* **2013**, *68*, 1093–1119. [CrossRef]
37. Periaswamy, S.C.G.; Thompson, D.R.; Di, J. Ownership Transfer of RFID Tags based on Electronic Fingerprint. In Proceedings of the Security and Management, Las Vegas, NV, USA, 14–17 July 2008; pp. 64–67.
38. Li, T.L.; Jin, Z.G.; Si, X.K. Temporary Ownership Sharing in RFID Systems. *J. Internet Technol.* **2013**, *14*, 341–349. (In Chinese)
39. Li, T.; Jin, Z.; Pang, C. Secured ownership transfer scheme for low-cost RFID tags. In Proceedings of the 2010 Third International Conference on Intelligent Networks and Intelligent Systems, Shenyang, China, 1–3 November 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 584–587.
40. Xue, J.; Xu, C.; Zhang, Y. Private blockchain-based secure access control for smart home systems. *KSII Trans. Internet Inf. Syst. (TIIS)* **2018**, *12*, 6057–6078.
41. Wazid, M.; Bera, B.; Mitra, A.; Das, A.K.; Ali, R. Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; pp. 37–42.
42. Bera, B.; Das, A.K.; Sutrala, A.K. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Comput. Commun.* **2021**, *166*, 91–109. [CrossRef]
43. Cao, B.; Wang, X.; Zhang, W.; Song, H.; Lv, Z. A many-objective optimization model of industrial internet of things based on private blockchain. *IEEE Netw.* **2020**, *34*, 78–83. [CrossRef]
44. Jo, M.; Hu, K.; Yu, R.; Sun, L.; Conti, M.; Du, Q. Private blockchain in industrial IoT. *IEEE Netw.* **2020**, *34*, 76–77. [CrossRef]
45. Future of Money Research Collaborative; Nelms, T.C.; Maurer, B.; Swartz, L.; Mainwaring, S. Social payments: Innovation, trust, Bitcoin, and the sharing economy. *Theory Cult. Soc.* **2018**, *35*, 13–33.
46. Burkhart, M.; Dimitropoulos, X. How to Protect Data Privacy in Collaborative Network Security. *Cybercrime* **2012** , *90*, 38.
47. Hou, H. The application of blockchain technology in E-government in China. In Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–4.
48. Lykidis, I.; Drosatos, G.; Rantos, K. The Use of Blockchain Technology in e-Government Services. *Computers* **2021**, *10*, 168. [CrossRef]
49. Páez, R.; Pérez, M.; Ramírez, G.; Montes, J.; Bouvarel, L. An architecture for biometric electronic identification document system based on blockchain. *Future Internet* **2020**, *12*, 10. [CrossRef]
50. Vásquez, A.; Bernal, J.F.; Tarazona, G.M. Cryptocurrency and its digital panorama in the Colombian government. In Proceedings of the International Conference on Knowledge Management in Organizations, Zamora, Spain, 15–18 July 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 225–234.
51. Sánchez Muñoz, C. Blockchain y cultura tributaria en Colombia (Blockchain and Tax Culture in Colombia). *Rev. Derecho Fisc.* **2022**, *20*, 57–61.
52. Solarte-Rivera, J.; Vidal-Zemanate, A.; Cobos, C.; Chamorro-Lopez, J.A.; Velasco, T. Document management system based on a private blockchain for the support of the judicial embargoes process in colombia. In Proceedings of the International Conference on Advanced Information Systems Engineering, Tallinn, Estonia, 11–15 June 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 126–137.
53. Riveros Lancheros, D.F. *Diseño e Implementación de Tecnologías Blockchain para el Sector Salud en Colombia*; Universidad de los Andes: Bogota, Colombia, 2019.
54. Álvarez Zambrano, Ó.J. Blockchain, una Oportunidad para el Desarrollo de las Asociaciones Público-Privadas en Infraestructura en Colombia. Ph.D. Thesis, Universidad EAFIT, Medellin, Colombia, 2022.

55. Moniruzzaman, M.; Chowdhury, F.; Ferdous, M.S. Examining usability issues in blockchain-based cryptocurrency wallets. In Proceedings of the International Conference on Cyber Security and Computer Science, Dhaka, Bangladesh, 15–16 February 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 631–643.
56. Ghesmati, S.; Fdhila, W.; Weippl, E. Usability of Cryptocurrency Wallets Providing CoinJoin Transactions. *Cryptol. Eprint Arch.* **2022** , *2002*, 285.
57. Jang, H.; Han, S.H.; Kim, J.H.; Kwon, K. Usability Evaluation for Cryptocurrency Exchange. In Proceedings of the Joint Conference of the Asian Council on Ergonomics and Design and the Southeast Asian Network of Ergonomics Societies, Bohol, Philippines, 2–4 December 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 192–196.
58. Mun, H.J. Biometric information and OTP based on Authentication Mechanism using Blockchain. *J. Converg. Inf. Technol.* **2018**, *8*, 85–90.
59. Nath, K.; Iswary, R. What comes after Web 3.0? Web 4.0 and the Future. In Proceedings of the International Conference and Communication System (I3CS'15), Shillong, India, 16–18 March 2015; Volume 337, p. 341.
60. Zhou, H.; Milani Fard, A.; Makanju, A. The State of Ethereum Smart Contracts Security: Vulnerabilities, Countermeasures, and Tool Support. *J. Cybersecur. Priv.* **2022**, *2*, 358–378. [CrossRef]
61. Karjoth, G.; Moskowitz, P.A. Disabling RFID tags with visible confirmation: Clipped tags are silenced. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7 November 2005; pp. 27–30.
62. Yamamoto, A.; Suzuki, S.; Hada, H.; Mitsugi, J.; Teraoka, F.; Nakamura, O. A tamper detection method for RFID tag data. In Proceedings of the 2008 IEEE International Conference on RFID, Las Vegas, NV, USA, 16–17 April 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 51–57.
63. Potdar, V.; Chang, E. Tamper detection in RFID tags using fragile watermarking. In Proceedings of the 2006 IEEE International Conference on Industrial Technology, Mumbai, India, 15–17 December 2006; IEEE: Piscataway, NJ, USA, 2006; pp. 2846–2852.
64. Fan, M.Q.; Wang, H.X. Tamper Discrimination in RFID Tags Using Chaotic Fragile Watermark. In Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 25–26 April 2009; IEEE: Piscataway, NJ, USA, 2009; Volume 2, pp. 147–150.
65. Lehtonen, M.O.; Michahelles, F.; Fleisch, E. Trust and security in RFID-based product authentication systems. *IEEE Syst. J.* **2007**, *1*, 129–144. [CrossRef]
66. Zhou, X.; Wang, A.; Xi, T. A new optional ownership transfer mode of RFID tags. *J. Inf. Comput. Sci.* **2013**, *10*, 2471–2479. [CrossRef]
67. Wang, H.; Yang, X.; Huang, Q.; Long, K. A novel authentication protocol enabling RFID tags ownership transfer. In Proceedings of the 2012 IEEE 14th International Conference on Communication Technology, Chengdu, China, 9–11 November 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 855–860.
68. Jayabalasamy, G.; Koppu, S. High-performance Edwards curve aggregate signature (HECAS) for nonrepudiation in IoT-based applications built on the blockchain ecosystem. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 9677–9687. [CrossRef]
69. Guruprakash, J.; Koppu, S. EC-ElGamal and Genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain. *IEEE Access* **2020**, *8*, 141269–141281. [CrossRef]
70. Qian, Y.; Ye, F.; Chen, H.H. RFID Security. In *Security in Wireless Communication Networks*; Wiley-IEEE Press: Hoboken, NJ, USA, 2022.
71. Su, Y.; Chesser, M.; Gao, Y.; Sample, A.; Ranasinghe, D. Wisecr: Secure simultaneous code dissemination to many batteryless computational RFID devices. *IEEE Trans. Dependable Secur. Comput.* **2022**, *early access* . [CrossRef]
72. Khadka, G.; Ray, B.; Karmakar, N.C.; Choi, J. Physical Layer Detection and Security of Printed Chipless RFID Tag for Internet of Things Applications. *IEEE Internet Things J.* **2022**, *9*, 15714–15724. [CrossRef]