Article

A Traceable Firearm Management System Based on Blockchain and IoT Technology

Chin-Ling Chen ^{1,2,3} , Mao-Lun Chiang ^{4,*}, Yong-Yuan Deng ^{3,*}, Wei Weng ^{1,*}, Kunhao Wang ^{5,6,*} and Ching-Cheng Liu ⁴

¹ School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361005, China; clc@mail.cyut.edu.tw

² School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China

³ Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 413, Taiwan

⁴ Department of Information and Communication Engineering, Chaoyang University of Technology, Taichung 413, Taiwan; s10730615@cyut.edu.tw

⁵ Computer College, Jilin Normal University, Siping 136000, China

⁶ College of Information Engineering, Changchun University of Finance and Economics, Changchun 130122, China

* Correspondence: mlchiang@cyut.edu.tw (M.-L.C.); allendeng@cyut.edu.tw (Y.-Y.D.); wweng@xmut.edu.cn (W.W.); wkhyoyo@jlnu.edu.cn (K.W.)

Citation: Chen, C.-L.; Chiang, M.-L.; Deng, Y.-Y.; Weng, W.; Wang, K.; Liu, C.-C. A Traceable Firearm Management System Based on Blockchain and IoT Technology. *Symmetry* **2021**, *13*, 439. <https://doi.org/10.3390/sym13030439>

Academic Editor: Stuart Harvey Rubin

Received: 9 February 2021

Accepted: 1 March 2021

Published: 8 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: In some liberal democracies, governments allow people to legally own guns to protect their lives and property. However, gun crime has been increasing in recent years. Taking the United States, for example, a report pointed out that Americans are 10 times more likely to be shot than citizens of other countries. Murder using guns in the United States is 25 times more than that in the other 22 high-income countries. Most of these guns came from other cities. These illegally circulating guns are directly linked to deadly street violence. This means that effective firearm management can reduce deadly violence. In the past few years, Radio Frequency IDentification (RFID) technology was often used to track the supply chain. However, in the traditional supply chain, only the participants of the supply chain can query information. Furthermore, only the participants can verify the correctness of the data. This result causes information to be not transparent. On the other hand, blockchain technology, with a unique combination of features such as distributed notes, decentralized structure, consensus algorithm, storage mechanism, asymmetric encryption, and smart contract, ensures network visibility, transparency, and security. Therefore, we combine blockchain and RFID technology to propose a traceable firearm management system based on blockchain and Internet of Things (IoT) technology. The proposed method achieves several goals. First of all, the characteristic data through the blockchain can be publicly verified and the information will not be modified. The traceability of the data and the application of RFID can effectively manage the production chain. In addition, we used Burrows–Abadi–Needham logic (BAN logic) logic to prove mutual authentication, and the nonrepudiation and integrity method can also be achieved in our proposed scheme.

Keywords: firearm management; blockchain; smart contract; traceable; IoT; BAN logic

1. Introduction

In recent years, gun crime has been increasing. In the past, some researchers [1] also collected research on trends in gun violence in the United States. According to the statistics [2], the proliferation of firearms (there were about 310 million firearms in the United States in 2009, excluding military use) led to most firearm crimes occurring in the United States. The report [3] pointed out that Americans are 10 times more likely to be shot than citizens of other countries. Murder using guns in the United States is 25 times more than that in the other 22 high-income countries. On the other hand, according to the

statistics from the Gun Violence Archive organization, the number of gun deaths in the United States in 2019 was approximately 39,447. The number of deaths excluding suicide was approximately 15,357 [4]. In [5], it was mentioned that death due to American guns has reached the highest level in nearly 40 years. The proportion of gun crimes in Chicago is quite high in the United States. One report [6] mentioned that Chicago has recovered around 7000 “crime guns” each year since 2013. These “crime guns” refer to firearms that were recovered from the Chicago Police Department (CPD). In 2017, CPD recovered far more guns than the previous year. Moreover, most of these guns came from other cities. These illegally circulating guns are directly linked to deadly street violence. This means that effective firearm management can reduce deadly violence.

In the current supply chain, only the participants of the supply chain can query information, and only the participants can verify the correctness of the data. This result causes information to be not transparent. Therefore, opaque and unverifiable information exists in the traditional supply chain. Since such a management method cannot grasp and track the flow of criminal tools, it naturally cannot deter the occurrence of criminal acts. Effective management and traceable technology are the only effective way to prevent crime from happening.

In the past few years, Ans. Radio Frequency IDentification (RFID) technology was often used to track the supply chain [7,8]. In particular, RFID was also used for weapon tracking due to the reason that it can automatically associate issued weapons with personnel, verify the qualifications of the individual to receive the issued weapon, and locate specific weapons and identify assets that require upkeep or re-certification. Furthermore, paperless check-in and check-out and track usage history have been implemented to accelerate and improve the accuracy of cycle counts [9,10].

On the other hand, blockchain technology, with a unique combination of features such as distributed nodes, decentralized structure, consensus algorithm, storage mechanism, asymmetric encryption, and smart contract, ensures network visibility, transparency, and security. Blockchain has immense potential to transform supply chain (SC) functions, from SC provenance to business process reengineering and security enhancement [11]. It is better to involve the management of the firearm supply chain. For these reasons, we combine blockchain and RFID technology to propose a firearm tracking system such that the information cannot be modified and tampered with once the data are uploaded to the blockchain center. This information is transparent and traceable for people to verify.

The remainder of this article is organized as follows: We briefly introduce preliminary and security requirements in Section 2. Section 3 shows the proposed scheme. Then, Section 4 describes the security analysis and discusses the performance analysis of the proposed scheme. Lastly, Section 5 provides the conclusions.

2. Preliminary and Security Requirements

2.1. Elliptic Curve Digital Signature Algorithm (ECDSA)

In cryptography, the Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA), which uses elliptic curve cryptography [12]. As with elliptic curve cryptography in general, the bit size of the public key believed to be needed for ECDSA is about twice the size of the security level, in bits. For example, at a security level of 80 bits (meaning an attacker requires a maximum of about 2^{80} operations to find the private key), the size of an ECDSA public key would be 160 bits, whereas the size of a DSA public key is at least 1024 bits. On the other hand, the signature size is the same for both DSA and ECDSA: approximately $4t$ bits, where t is the security level measured in bits; that is, about 320 bits for a security level of 80 bits.

2.2. Burrows–Abadi–Needham logic (BAN logic) Logic

BAN logic was created to assist in the validation of authentication protocols [13]. It has been used to prove the correctness of a scheme. It is a set of rules for defining and analyzing information exchange protocols. BAN logic helps its users determine whether

information is secured against eavesdropping and/or whether exchanged information is trustworthy. BAN logic starts with the assumption that all information exchanges happen on media vulnerable to tampering and public monitoring. We use BAN logic to prove the correctness of authentication and key establishment.

2.3. Security Requirements

In addition to involving RFID technology [14] to facilitate firearm logistics management, we also use blockchain technology to fulfill decentralization, transparency, public verification, trustless, non-tamperproof, and irreversibility characteristics. Secondly, it is worth mentioning that a smart contract is a special agreement used through a contract in the blockchain, which is mainly used to provide verification and execution of conditions set within the smart contract [15]. Firearm transactions should be traceable, difficult to tamper with, and irreversible. Therefore, smart contracts can conduct secure transactions without a third party. All messages related to the terms of the contract in the transaction are automatically executed under the operations set in the contract to reduce the need for trusted arbitrations, intermediaries, fraud losses, and enforcement costs, as well as reduce accidental exceptions and malicious acts, in our scheme. Therefore, to implement a secure communication environment in a traceable firearm system based on blockchain, the proposed scheme needs to satisfy the following security requirements:

(1) Mutual Authentication [13,16,17]

In the transmission process, identity authentication is a basic requirement. It is important to ensure the legitimacy of the sender and receiver during the communication.

(2) Verifiability [14,18]

The authorized on-chain information of the firearm manufacturer can be disclosed, and the identity of the firearm owner can be verified through the verification of the social security number.

(3) Resistance to Forgery [17–19]

The new decentralized model of blockchain combined with timestamp technology makes it impossible to arbitrarily change the data on the chain, thus effectively solving the trust problem.

(4) Traceability [14,19,20]

By achieving traceability in the production chain, people can track the products from the source. Moreover, the user can know which goods have been handled throughout the supply chain. This allows fast traceability analysis in critical situations.

(5) Integrity [14,16,21,22]

In an insecure transmission environment, the transmitted data are vulnerable to tampering. They are vulnerable to incorrect influence when users receive the wrong information. Thus, the integrity of the information is an important issue.

(6) Decentralization/Distribution [23,24]

The authorization information of the system is transparent. As a function of the open transparency of information on the chain, it can obtain trust between nodes at a low cost and realize the sharing of authentication information.

(7) Nonrepudiation [14,16,25]

The attacker can easily perform an impersonation attack and send a false message if the identity is not authenticated. The nonrepudiation mechanism can effectively prevent impersonation attacks. The common strategy to achieve a nonrepudiation issue is to use a digital signature.

3. The Proposed Scheme

3.1. System Architecture

The system consists of the following five parties: blockchain center, firearm authority, manufacturer, retailer, and customer. All parties must pass the firearm authority's authentication when they want to access the information of the blockchain center. Section 3.1 is the overall architecture description, the details of which are described later. The system framework is shown in Figure 1.

Figure 1. System framework of the proposed scheme.

1. Blockchain center (BCC): An Ethereum platform to produce a public key and private key for participating parties.
2. Firearm authority (FA): This is the firearm management department that belongs to the government organization. This is a trusted institution. The firearm management must authenticate and certify a user when any party wants to purchase the firearm.
3. Manufacturer (MA): They produce the firearm and sell the firearm to the retailer. Moreover, they can also produce the genesis blockchain after obtaining the license.
4. Firearm store (FS): They sell the firearm to the customer. In addition, they can join a transaction to the blockchain after obtaining the license.
5. Firearm owner (FO): They can proceed with the transaction to buy a firearm, and they are allowed to add this transaction to the blockchain.

In this paper, the access party (AP) is one of the firearm authority (FA), manufacturer (MA), firearm store (FS), or firearm owner (FO).

Step 1. All parties want to register with the BCC. All parties get public/private keys from the BCC.

Step 2. When the MA produces the firearm, the MA must embed an RFID tag in the firearm. Then, the MA hands out to the FA to upload the firearm data to the genesis blockchain. After uploading, the firearm is sent back to the MA.

Step 3. The MA uses the blockchain to initiate a transaction to the FS and deliver the firearm to the FS. After the FS receives the firearm, the firearm transaction is recorded to the blockchain center.

Step 4. If the FO wants to buy the firearm, the FS initiates a transaction in the blockchain and delivers the firearm to the FO.

3.2. Registration Phase

The FA, MA, FS, and FO should register with the blockchain center and obtain a relative public/private key pair. The access party (AP) can represent the FA, MA, FS, and FO. Figure 2 shows the flowchart of the registration phase.

Figure 2. The flowchart of the registration phase.

Step 1: Access party AP generates a name ID_{AP} and sends it to the blockchain center.

Step 2: The blockchain center generates an ECDSA private key d_{AP} according to the role of the AP, calculated as $Q_{AP} = d_{AP}G$. If the identity of the registered role is verified, the smart contract is triggered, the content of which is the Algorithm 1 as follows:

Algorithm 1. Smart contract apins of the proposed scheme.

```

function insert ap smart contract apins (          ap[count].id = id;
string ap_id, string ap_detail) {                  }
count ++;                                         string ap_keypairs;
ap[count].id = id;
  
```

Then, the blockchain center transmits $ID_{AP}, (d_{AP}, Q_{AP}), PK_{AP}, SK_{AP}$ to the role of the AP.

Step 3: The role of the AP stores $(d_{AP}, Q_{AP}, PK_{AP}, SK_{AP})$.

3.3. Smart Contract Initialization

Blockchain technology was applied in the proposed architecture. Some key information is saved and verified through the blockchain, during the authentication and authorization process. The key information in the blockchain is defined in the smart contract. The following Algorithm 2 is the blockchain smart contract structure for the proposed scheme:

Algorithm 2. Smart contract mafainf/famainf/mafsinf/fsmainf of the proposed scheme.

<pre> struct smart contract mafainf/famainf/mafsinf/ fsmainf { string mafa/fama/mafs/fsma id; string mafa/fama/mafs/fsma detail; string mafa/fama/mafs/fsma cert; string mafa/fama/mafs/fsma tsp; } </pre>	<pre> struct smart contract mafainf/famainf/mafsinf/ string fofs/fsfo id; string fofs/fsfo detail; string fofs/fsfo ssn; string fofs/fsfo tsp; } string keypairs; string count; </pre>
--	--

We developed key information that is stored in the blockchain in the proposed smart contract. In the structure of the mafa/fama/mafs/fsma smart contract, we developed the fields of id (identification), transaction detail, certificate, and timestamp. In the structure of

the fofs/fsfo smart contract, we developed the fields of id, transaction detail, ssn (social security number), and timestamp. The blockchain center also issues the public and private key pairs for all roles in the initialization phase.

3.4. Authorized Production Phase

Before the MA can produce guns, it must first apply to the FA. If the FA agrees to the production, it sends the approval document back to the MA and send the relevant information to the BCC. We present the flowchart of the authorized production phase in Figure 3.

Figure 3. Authorized production phase.

Step 1: The MA generates a random value k_{MA-FA} , calculates $z_{MA-FA} = h(ID_{MA}, M_{MA-FA}, Cert_{MA}, TS_{MA-FA})$, $(x_{MA-FA}, y_{MA-FA}) = k_{MA-FA}G$, $r_{MA-FA} = x_{MA-FA} \bmod n$,

$s_{MA-FA} = k_{MA-FA}^{-1}(z_{MA-FA} + r_{MA-FA}d_{MA}) \bmod n$, $C_{MA-FA} = E_{PK_{FA}}(ID_{MA}, M_{MA-FA}, Cert_{MA}, TS_{MA-FA})$, and sends $ID_{MA}, C_{MA-FA}, (r_{MA-FA}, s_{MA-FA})$ to the FA.

Step 2: The FA first calculates $(ID_{MA}, M_{MA-FA}, Cert_{MA}, TS_{MA-FA}) = D_{SK_{FA}}(C_{MA-FA})$, uses $TS_{NOW} - TS_{MA-FA} \leq \Delta T$ to confirm whether the timestamp is valid, and then verifies the correctness of the ECDSA signature, by calculating $z_{MA-FA}' = h(ID_{MA}, M_{MA-FA}, Cert_{MA}, TS_{MA-FA})$, $u_{MA-FA1} = z_{MA-FA}'s_{MA-FA}^{-1} \bmod n$, $u_{MA-FA2} = r_{MA-FA}s_{MA-FA}^{-1} \bmod n$, $(x_{MA-FA}', y_{MA-FA}') = u_{MA-FA1}G + u_{MA-FA2}Q_{MA}$, $x_{MA-FA}' \stackrel{?}{=} r_{MA-FA} \bmod n$. If the verification is passed, the FA gets the relevant production request information and trigger the smart contracts mafains and mafachk. The content is the Algorithm 3 as follows:

Algorithm 3. Smart contract mafains of the proposed scheme.

<pre>function insert smart contract mafains(string mafa_id, string mafa_detail, string mafa_cert, string mafa_tsp) { count ++; mafa[count].id = id; mafa[count].detail = detail; mafa[count].cert = cert; mafa[count].tsp = tsp; } sign string ma_key (mafa_id, mafa_detail, mafa_cert, mafa_tsp);</pre>	<pre>verify string ma_key (mafa_id, mafa_detail, mafa_cert, mafa_tsp); function check smart contract mafachk(string mafa_id, string mafa_detail, string mafa_cert, string mafa_tsp) { return mafa_id.exist; return mafa_detail.exist; return mafa_cert.exist; return mafa_tsp.exist; }</pre>
---	---

The FA that calculates $BC_{MA-FA} = h(r_{MA-FA}, s_{MA-FA})$, (ID_{BC}, BC_{MA-FA}) is also uploaded to the blockchain center. Then, the FA generates a random value k_{FA-MA} , calculates $z_{FA-MA} = h(ID_{FA}, M_{FA-MA}, Cert_{GUN}, TS_{FA-MA}, ID_{BC})$, $(x_{FA-MA}, y_{FA-MA}) = k_{FA-MA}G$, $r_{FA-MA} = x_{FA-MA} \bmod n$, $s_{FA-MA} = k_{FA-MA}^{-1}(z_{FA-MA} + r_{FA-MA}d_{FA}) \bmod n$, $C_{FA-MA} = E_{PK_{MA}}(ID_{FA}, M_{FA-MA}, Cert_{GUN}, TS_{FA-MA}, ID_{BC})$, and sends $ID_{FA}, C_{FA-MA}, (r_{FA-MA}, s_{FA-MA})$ to the MA.

Step 3. The MA first calculates $(ID_{FA}, M_{FA-MA}, Cert_{GUN}, TS_{FA-MA}, ID_{BC}) = D_{SK_{MA}}(C_{FA-MA})$, uses $TS_{NOW} - TS_{FA-MA} \leq \Delta T$ to confirm whether the timestamp is valid, and then verifies the correctness of the ECDSA signature, calculates $z_{FA-MA}' = h(ID_{FA}, M_{FA-MA}, Cert_{GUN}, TS_{FA-MA}, ID_{BC})$, $u_{FA-MA1} = z_{FA-MA}'s_{FA-MA}^{-1} \bmod n$, $u_{FA-MA2} = r_{FA-MA}s_{FA-MA}^{-1} \bmod n$, $(x_{FA-MA}', y_{FA-MA}') = u_{FA-MA1}G + u_{FA-MA2}Q_{FA}$, $x_{FA-MA}' \stackrel{?}{=} r_{FA-MA} \bmod n$. If the verification is passed, the production request information is confirmed by MA, and the smart contracts famains and famachk are sent. The content is the Algorithm 4 as follows:

Algorithm 4. Smart contract famains of the proposed scheme.

<pre>function insert smart contract famains(string fama_id, string fama_detail, string fama_cert, string fama_tsp) { count ++; fama[count].id = id; fama[count].detail = detail; fama[count].cert = cert; fama[count].tsp = tsp; } sign string fa_key (fama_id, fama_detail, fama_cert, fama_tsp);</pre>	<pre>verify string fa_key (fama_id, fama_detail, fama_cert, fama_tsp); function check smart contract famachk(string fama_id, string fama_detail, string fama_cert, string fama_tsp) { return fama_id.exist; return fama_detail.exist; return fama_cert.exist; return fama_tsp.exist; }</pre>
---	---

The MA that calculates $BC_{FA-MA} = h(r_{FA-MA}, s_{FA-MA})$, (ID_{BC}, BC_{FA-MA}) is also uploaded to the blockchain center. The MA produces firearms and $(Info_{GUN}, ID_{BC})$ is written to the RFID tag.

3.5. Firearm Selling Phase

After MA produces the gun, it is sent to FS for sale. The Global Positioning System (GPS) coordinates of the gun production location are also uploaded to the BCC. We present the flowchart of the firearm selling phase in Figure 4.

Figure 4. Firearm selling phase.

- Step 1: The MA generates a random value k_{MA-FS} , calculates $z_{MA-FS} = h(ID_{MA}, M_{MA-FA}, Cert_{MA}, Info_{GUN}, TS_{MA-FS}, ID_{BC})$, $(x_{MA-FS}, y_{MA-FS}) = k_{MA-FS}G$, $r_{MA-FS} = x_{MA-FS} \bmod n$, $s_{MA-FS} = k_{MA-FS}^{-1}(z_{MA-FS} + r_{MA-FS}d_{MA}) \bmod n$, $C_{MA-FS} = E_{PK_{FS}}(ID_{MA}, M_{MA-FS}, Cert_{MA}, Info_{GUN}, TS_{MA-FS}, ID_{BC})$, and sends $ID_{MA}, C_{MA-FS}, (r_{MA-FS}, s_{MA-FS})$ to the FS.
- Step 2: The FS first calculates $(ID_{MA}, M_{MA-FA}, Cert_{MA}, Info_{GUN}, TS_{MA-FS}, ID_{BC}) = D_{SK_{FS}}(C_{MA-FS})$, uses $TS_{NOW} - TS_{MA-FS} \leq \Delta T$ to confirm whether the timestamp is valid, verifies the correctness of the ECDSA signature, and then calculates $z_{MA-FS}' = h(ID_{MA}, M_{MA-FA}, Cert_{MA}, Info_{GUN}, TS_{MA-FS}, ID_{BC})$, $u_{MA-FS1} = z_{MA-FS}' s_{MA-FS}^{-1} \bmod n$, $u_{MA-FS2} = r_{MA-FS} s_{MA-FS}^{-1} \bmod n$, $(x_{MA-FS}', y_{MA-FS}') = u_{MA-FS1}G + u_{MA-FS2}Q_{MA}$, $x_{MA-FS}' \stackrel{?}{=} r_{MA-FS} \bmod n$. If the verification is passed, the FS gets the relevant firearm production information and trigger the smart contracts mafsins and mafschk. The content is the Algorithm 5 as follows:

Algorithm 5. Smart contract mafsins of the proposed scheme.

<pre>function insert smart contract mafsins(string mafs_id, string mafs_detail, string mafs_cert, string mafs_tsp) { count ++; mafs[count].id = id; mafs[count].detail = detail; mafs[count].cert = cert; mafs[count].tsp = tsp; } sign string ma_key (mafs_id, mafs_detail, mafs_cert, mafs_tsp);</pre>	<pre>verify string ma_key (mafs_id, mafs_detail, mafs_cert, mafs_tsp); function check smart contract mafschk(mafs_id, string mafs_detail, string mafs_cert, string mafs_tsp) { return mafs_id.exist; return mafs_detail.exist; return mafs_cert.exist; return mafs_tsp.exist; }</pre>
---	--

The FS that calculates $BC_{MA-FS} = h(r_{MA-FS}, s_{MA-FS})$, (ID_{BC}, BC_{MA-FS}) is also uploaded to the blockchain center. Then, the FS generates a random value k_{FS-MA} , calculates $z_{FS-MA} = h(ID_{FS}, M_{FS-MA}, Cert_{FS}, Info_{GUN}, TS_{FS-MA}, ID_{BC})$, $(x_{FS-MA}, y_{FS-MA}) = k_{FS-MA}G$, $r_{FS-MA} = x_{FS-MA} \bmod n$, $s_{FS-MA} = k_{FS-MA}^{-1}(z_{FS-MA} + r_{FS-MA}d_{FS}) \bmod n$, $C_{FS-MA} = E_{PK_{MA}}(ID_{FS}, M_{FS-MA}, Cert_{FS}, Info_{GUN}, TS_{FS-MA}, ID_{BC})$, and updates $(Info_{GUN}, ID_{BC})$ to the RFID tag. The FS then sends $ID_{FS}, C_{FS-MA}, (r_{FS-MA}, s_{FS-MA})$ to the MA.

- Step 3: The MA first calculates $(ID_{FS}, M_{FS-MA}, Cert_{FS}, Info_{GUN}, TS_{FS-MA}, ID_{BC}) = D_{SK_{MA}}(C_{FS-MA})$, uses $TS_{NOW} - TS_{FS-MA} \leq \Delta T$ to confirm whether the timestamp is valid, verifies the correctness of the ECDSA signature, and calculates $z_{FS-MA}' = h(ID_{FS}, M_{FS-MA}, Cert_{FS}, Info_{GUN}, TS_{FS-MA}, ID_{BC})$, $u_{FS-MA1} = z_{FS-MA}' s_{FS-MA}^{-1} \bmod n$, $u_{FS-MA2} = r_{FS-MA} s_{FS-MA}^{-1} \bmod n$, $(x_{FS-MA}', y_{FS-MA}') = u_{FS-MA1}G + u_{FS-MA2}Q_{FS}$, $x_{FS-MA}' \stackrel{?}{=} r_{FS-MA} \bmod n$. If the verification is passed, the firearm selling information is confirmed by MA, and the smart contracts fsmains and fsmachk are sent. The content is the Algorithm 6 as follows:

Algorithm 6. Smart contract fsmains of the proposed scheme.

<pre>function insert smart contract fsmains(string fsma_id, string fsma_detail, string fsma_cert, string fsma_tsp) { count ++; fsma[count].id = id; fsma[count].detail = detail; fsma[count].cert = cert; fsma[count].tsp = tsp; } sign string fs_key (fsma_id, fsma_detail, fsma_cert, fsma_tsp);</pre>	<pre>verify string fs_key (fsma_id, fsma_detail, fsma_cert, fsma_tsp); function check smart contract fsmachk(string fsma_id, string fsma_detail, string fsma_cert, string fsma_tsp) { return fsma_id.exist; return fsma_detail.exist; return fsma_cert.exist; return fsma_tsp.exist; }</pre>
---	---

The MA that calculates $BC_{FS-MA} = h(r_{FS-MA}, s_{FS-MA})$, (ID_{BC}, BC_{FS-MA}) is also uploaded to the blockchain center.

3.6. Owner Holding Phase

When FO goes to FS to buy a gun, the FS checks the SSN of the FO. If it passes the check, FS writes the FO's SSN to the RFID tag. The information is also uploaded to the BCC. We present the flowchart of the owner holding phase in Figure 5.

Figure 5. Owner holding phase.

Step 1: The FO generates a random value k_{FO-FS} , calculates $z_{FO-FS} = h(ID_{FO}, M_{FO-FA}, SSN_{FO}, TS_{FO-FS})$, $(x_{FO-FS}, y_{FO-FS}) = k_{FO-FS}G$, $r_{FO-FS} = x_{FO-FS} \bmod n$, $s_{FO-FS} =$

$k_{FO-FS}^{-1}(z_{FO-FS} + r_{FO-FS}d_{FO})\bmod n$, $C_{FO-FS} = E_{PK_{FS}}(ID_{FO}, M_{FO-FA}, SSN_{FO}, TS_{FO-FS})$, and sends $ID_{FO}, C_{FO-FS}, (r_{FO-FS}, s_{FO-FS})$ to the FS.

Step 2: The FS first calculates $(ID_{FO}, M_{FO-FA}, SSN_{FO}, TS_{FO-FS}) = D_{SK_{FS}}(C_{FO-FS})$, uses $TS_{NOW} - TS_{FO-FS} \leq \Delta T$ to confirm whether the timestamp is valid, verifies the correctness of the ECDSA signature, and calculates $z_{FO-FS}' = h(ID_{FO}, M_{FO-FS}, SSN_{FO}, TS_{FO-FS})$, $u_{FO-FS1} = z_{FO-FS}'s_{FO-FS}^{-1} \bmod n$, $u_{FO-FS2} = r_{FO-FS}s_{FO-FS}^{-1} \bmod n$, $(x_{FO-FS}', y_{FO-FS}') = u_{FO-FS1}G + u_{FO-FS2}Q_{FO}$, $x_{FO-FS}' \stackrel{?}{=} r_{FO-FS} \bmod n$. If the verification is passed, the FS gets the relevant firearm request information and triggers the smart contracts fofsins and fofschk. The content is the Algorithm 7 as follows:

Algorithm 7. Smart contract fofsins of the proposed scheme.

<pre>function insert smart contract fofsins(string fofs_id, string fofs_detail, string fofs_ssn, string fofs_tsp) { count ++; fofs[count].id = id; fofs[count].detail = detail; fofs[count].ssn = ssn; fofs[count].tsp = tsp; } sign string fo_key (fofs_id, fofs_detail, fofs_ssn, fofs_tsp);</pre>	<pre>verify string fo_key (fofs_id, fofs_detail, fofs_ssn, fofs_tsp); function check smart contract fofschk(string fofs_id, string fofs_detail, string fofs_ssn, string fofs_tsp) { return fofs_id.exist; return fofs_detail.exist; return fofs_ssn.exist; return fofs_tsp.exist; }</pre>
---	--

The FS that calculates $BC_{FO-FS} = h(r_{FO-FS}, s_{FO-FS})$, (ID_{BC}, BC_{FO-FS}) is also uploaded to the blockchain center. Then, the FS generates a random value k_{FS-FO} , calculates $z_{FS-FO} = h(ID_{FS}, M_{FS-FO}, Cert_{FS}, Info_{GUN}, SSN_{FO}, TS_{FS-FO}, ID_{BC})$, $(x_{FS-FO}, y_{FS-FO}) = k_{FS-FO}G$, $r_{FS-FO} = x_{FS-FO} \bmod n$, $s_{FS-FO} = k_{FS-FO}^{-1}(z_{FS-FO} + r_{FS-FO}d_{FS}) \bmod n$, $C_{FS-FO} = E_{PK_{FO}}(ID_{FS}, M_{FS-FO}, Cert_{FS}, Info_{GUN}, SSN_{FO}, TS_{FS-FO}, ID_{BC})$, and updates $(Info_{GUN}, SSN_{FO}, ID_{BC})$ to the RFID tag. The FS then sends $ID_{FS}, C_{FS-FO}, (r_{FS-FO}, s_{FS-FO})$ to the FO.

Step 3: The FO first calculates $(ID_{FS}, M_{FS-FO}, Cert_{FS}, Info_{GUN}, SSN_{FO}, TS_{FS-FO}, ID_{BC}) = D_{SK_{FO}}(C_{FS-FO})$, uses $TS_{NOW} - TS_{FS-FO} \leq \Delta T$ to confirm whether the timestamp is valid, verifies the correctness of the ECDSA signature, and calculates $z_{FS-FO}' = h(ID_{FS}, M_{FS-FO}, Cert_{FS}, Info_{GUN}, SSN_{FO}, TS_{FS-FO}, ID_{BC})$, $u_{FS-FO1} = z_{FS-FO}'s_{FS-FO}^{-1} \bmod n$, $u_{FS-FO2} = r_{FS-FO}s_{FS-FO}^{-1} \bmod n$, $(x_{FS-FO}', y_{FS-FO}') = u_{FS-FO1}G + u_{FS-FO2}Q_{FS}$, $x_{FS-FO}' \stackrel{?}{=} r_{FS-FO} \bmod n$. If the verification is passed, the firearm-related information is confirmed by FO, and the smart contracts fsfoins and fsfochk are sent. The content is the Algorithm 8 as follows:

Algorithm 8. Smart contract fsfoins of the proposed scheme.

<pre>function insert smart contract fsfoins(string fsfo_id, string fsfo_detail, string fsfo_ssn, string fsfo_tsp) { count ++; fsfo[count].id = id; fsfo[count].detail = detail; fsfo[count].ssn = ssn; fsfo[count].tsp = tsp; } sign string fs_key (fsfo_id, fsfo_detail, fsfo_ssn, fsfo_tsp);</pre>	<pre>verify string fs_key (fsfo_id, fsfo_detail, fsfo_ssn, fsfo_tsp); function check smart contract fsfochk(string fsfo_id, string fsfo_detail, string fsfo_ssn, string fsfo_tsp) { return fsfo_id.exist; return fsfo_detail.exist; return fsfo_ssn.exist; return fsfo_tsp.exist; }</pre>
---	--

The FO that calculates $BC_{FS-FO} = h(r_{FS-FO}, s_{FS-FO})$, (ID_{BC}, BC_{FS-FO}) is also uploaded to the blockchain center.

4. Security Analysis and Discussion

4.1. Mutual Authentication

The BAN logic proof model is applied to prove that mutual authentication is achieved between different parties in each phase of the proposed scheme.

In the authorized production phase of the proposed scheme, the main goal of the scheme is to authenticate the private key of the manufacturer MA and the firearm authority FA .

- G1: $MA \mid \equiv MA \stackrel{x_{FA-MA}}{\leftrightarrow} FA$.
 G2: $MA \mid \equiv FA \mid \equiv MA \stackrel{x_{FA-MA}}{\leftrightarrow} FA$.
 G3: $FA \mid \equiv MA \stackrel{x_{MA-FA}}{\leftrightarrow} FA$.
 G4: $FA \mid \equiv MA \mid \equiv MA \stackrel{x_{MA-FA}}{\leftrightarrow} FA$.
 G5: $MA \mid \equiv ID_{FA}$.
 G6: $MA \mid \equiv FA \mid \equiv ID_{FA}$.
 G7: $FA \mid \equiv ID_{MA}$.
 G8: $FA \mid \equiv MA \mid \equiv ID_{MA}$.

According to the authorized production phase, BAN logic is applied to produce an idealized form as follows:

- M1: $(\langle ID_{MA}, k_{MA-FA}, TS_{MA-FA} \rangle_{PK_{FA}}, \langle H(ID_{MA}, k_{MA-FA}, TS_{MA-FA}) \rangle_{x_{MA-FA}})$,
 M2: $(\langle ID_{FA}, k_{FA-MA}, TS_{FA-MA} \rangle_{PK_{MA}}, \langle H(ID_{FA}, k_{FA-MA}, TS_{FA-MA}) \rangle_{x_{FA-MA}})$.

To analyze the proposed scheme, the following assumptions are made:

- A1: $MA \mid \equiv \#(k_{MA-FA})$,
 A2: $FA \mid \equiv \#(k_{MA-FA})$,
 A3: $MA \mid \equiv \#(k_{FA-MA})$,
 A4: $FA \mid \equiv \#(k_{FA-MA})$,
 A5: $MA \mid \equiv FA \mid \Rightarrow MA \stackrel{x_{FA-MA}}{\leftrightarrow} FA$,
 A6: $FA \mid \equiv MA \mid \Rightarrow MA \stackrel{x_{MA-FA}}{\leftrightarrow} FA$,
 A7: $MA \mid \equiv FA \mid \Rightarrow ID_{FA}$,
 A8: $FA \mid \equiv MA \mid \Rightarrow ID_{MA}$.

According to these assumptions and rules of BAN logic, the main proof of the authorized production phase is as follows:

- a. The firearm authority FA authenticates the manufacturer MA .

Through M1 and the *seeing rule*, we originate the following statement:

$$FA \triangleleft (\langle ID_{MA}, k_{MA-FA}, TS_{MA-FA} \rangle_{PK_{FA}}, \langle H(ID_{MA}, k_{MA-FA}, TS_{MA-FA}) \rangle_{x_{MA-FA}}). \quad (1)$$

Through A2 and the *freshness rule*, we originate the following statement:

$$FA \mid \equiv \#(\langle ID_{MA}, k_{MA-FA}, TS_{MA-FA} \rangle_{PK_{FA}}, \langle H(ID_{MA}, k_{MA-FA}, TS_{MA-FA}) \rangle_{x_{MA-FA}}). \quad (2)$$

Through Equation (1), A4, and the *message meaning rule*, we originate the following statement:

$$FA \mid \equiv MA \mid \sim (\langle ID_{MA}, k_{MA-FA}, TS_{MA-FA} \rangle_{PK_{FA}}, \langle H(ID_{MA}, k_{MA-FA}, TS_{MA-FA}) \rangle_{x_{MA-FA}}). \quad (3)$$

Through Equations (2) and (3), and the *nonce verification rule*, we originate the following statement:

$$FA \mid \equiv MA \mid \equiv (\langle ID_{MA}, k_{MA-FA}, TS_{MA-FA} \rangle_{PK_{FA}}, \langle H(ID_{MA}, k_{MA-FA}, TS_{MA-FA}) \rangle_{x_{MA-FA}}). \quad (4)$$

Through Equation (4), and the *belief rule*, we originate the following statement:

$$FA \mid \equiv MA \mid \equiv MA \stackrel{x_{MA-FA}}{\leftrightarrow} FA. \quad (5)$$

Through Equation (5), A6, and the *jurisdiction rule*, we originate the following statement:

$$FA| \equiv MA \stackrel{x_{MA \rightarrow FA}}{\leftrightarrow} FA. \quad (6)$$

Through Equation (6), and the *belief rule*, we originate the following statement:

$$FA| \equiv MA| \equiv ID_{MA}. \quad (7)$$

Through Equation (7), A8, and the *jurisdiction rule*, we originate the following statement:

$$FA| \equiv ID_{MA}. \quad (8)$$

b. The manufacturer MA authenticates the firearm authority FA.

Through M2 and the *seeing rule*, we originate the following statement:

$$MA \triangleleft (\langle ID_{FA}, k_{FA-MA}, TS_{FA-MA} \rangle_{PK_{MA}}, \langle H(ID_{FA}, k_{FA-MA}, TS_{FA-MA}) \rangle_{x_{FA-MA}}). \quad (9)$$

Through A1 and the *freshness rule*, we originate the following statement:

$$MA| \equiv \#(\langle ID_{FA}, k_{FA-MA}, TS_{FA-MA} \rangle_{PK_{MA}}, \langle H(ID_{FA}, k_{FA-MA}, TS_{FA-MA}) \rangle_{x_{FA-MA}}). \quad (10)$$

Through Equation (9), A3, and the *message meaning rule*, we originate the following statement:

$$MA| \equiv FA| \sim (\langle ID_{FA}, k_{FA-MA}, TS_{FA-MA} \rangle_{PK_{MA}}, \langle H(ID_{FA}, k_{FA-MA}, TS_{FA-MA}) \rangle_{x_{FA-MA}}). \quad (11)$$

Through Equations (10) and (11), and the *nonce verification rule*, we originate the following statement:

$$MA| \equiv FA| \equiv (\langle ID_{FA}, k_{FA-MA}, TS_{FA-MA} \rangle_{PK_{MA}}, \langle H(ID_{FA}, k_{FA-MA}, TS_{FA-MA}) \rangle_{x_{FA-MA}}). \quad (12)$$

Through Equation (12), and the *belief rule*, we originate the following statement:

$$MA| \equiv FA| \equiv MA \stackrel{x_{FA \rightarrow MA}}{\leftrightarrow} FA. \quad (13)$$

Through Equation (13), A5, and the *jurisdiction rule*, we originate the following statement:

$$MA| \equiv MA \stackrel{x_{FA \rightarrow MA}}{\leftrightarrow} FA. \quad (14)$$

Through Equation (14), and the *belief rule*, we originate the following statement:

$$MA| \equiv FA| \equiv ID_{FA}. \quad (15)$$

Through Equation (15), A7, and the *jurisdiction rule*, we originate the following statement:

$$MA| \equiv ID_{FA}. \quad (16)$$

Through Equations (6), (8), (14) and (16), it can be proven that, in the proposed scheme, the manufacturer MA and the firearm authority FA authenticate each other. Moreover, it can also be proven that the proposed scheme can authenticate the private key of the manufacturer MA and the firearm authority FA.

In the proposed scheme, the firearm authority authenticates the manufacturer by

$$x_{MA-FA}' \stackrel{?}{=} r_{MA-FA} \bmod n.$$

If it passes the verification, the firearm authority authenticates the legality of the manufacturer. The manufacturer authenticates the firearm authority by

$$x_{FA-MA}' \stackrel{?}{=} r_{FA-MA} \bmod n.$$

If it passes the verification, the manufacturer authenticates the legality of the firearm authority. The authorized production phase of the proposed scheme, thus, guarantees mutual authentication between the firearm authority and the manufacturer.

In the firearm selling phase of the proposed scheme, the main goal of the scheme is to authenticate the private key of the manufacturer MA and the firearm store FS.

$$\begin{aligned}
 G9: MA| &\equiv MA \stackrel{x_{FS-MA}}{\longleftrightarrow} FS. \\
 G10: MA| &\equiv FS| \equiv MA \stackrel{x_{FS-MA}}{\longleftrightarrow} FS. \\
 G11: FS| &\equiv MA \stackrel{x_{MA-FS}}{\longleftrightarrow} FS. \\
 G12: FS| &\equiv MA| \equiv MA \stackrel{x_{MA-FS}}{\longleftrightarrow} FS. \\
 G13: MA| &\equiv ID_{FS}. \\
 G14: MA| &\equiv FS| \equiv ID_{FS}. \\
 G15: FS| &\equiv ID_{MA}. \\
 G16: FS| &\equiv MA| \equiv ID_{MA}.
 \end{aligned}$$

According to the firearm selling phase, BAN logic is applied to produce an idealized form as follows:

$$\begin{aligned}
 M3: (< ID_{MA}, k_{MA-FS}, TS_{MA-FS} >_{PK_{FS}}, < H(ID_{MA}, k_{MA-FS}, TS_{MA-FS}) >_{x_{MA-FS}}), \\
 M4: (< ID_{FS}, k_{FS-MA}, TS_{FS-MA} >_{PK_{MA}}, < H(ID_{FS}, k_{FS-MA}, TS_{FS-MA}) >_{x_{FS-MA}}).
 \end{aligned}$$

To analyze the proposed scheme, the following assumptions are made:

$$\begin{aligned}
 A9: MA| &\equiv \#(k_{MA-FS}), \\
 A10: FS| &\equiv \#(k_{MA-FS}), \\
 A11: MA| &\equiv \#(k_{FS-MA}), \\
 A12: FS| &\equiv \#(k_{FS-MA}), \\
 A13: MA| &\equiv FS| \Rightarrow MA \stackrel{x_{FS-MA}}{\longleftrightarrow} FS, \\
 A14: FS| &\equiv MA| \Rightarrow MA \stackrel{x_{MA-FS}}{\longleftrightarrow} FS, \\
 A15: MA| &\equiv FS| \Rightarrow ID_{FS}, \\
 A16: FS| &\equiv MA| \Rightarrow ID_{MA}.
 \end{aligned}$$

According to these assumptions and rules of BAN logic, the main proof of the firearm selling phase is as follows:

c. The firearm store FS authenticates the manufacturer MA.

Through M3 and the *seeing rule*, we originate the following statement:

$$FS \triangleleft (< ID_{MA}, k_{MA-FS}, TS_{MA-FS} >_{PK_{FS}}, < H(ID_{MA}, k_{MA-FS}, TS_{MA-FS}) >_{x_{MA-FS}}). \quad (17)$$

Through A10 and the *freshness rule*, we originate the following statement:

$$FS| \equiv \#(< ID_{MA}, k_{MA-FS}, TS_{MA-FS} >_{PK_{FS}}, < H(ID_{MA}, k_{MA-FS}, TS_{MA-FS}) >_{x_{MA-FS}}). \quad (18)$$

Through Equation (17), A12, and the *message meaning rule*, we originate the following statement:

$$FS| \equiv MA| \sim (< ID_{MA}, k_{MA-FS}, TS_{MA-FS} >_{PK_{FS}}, < H(ID_{MA}, k_{MA-FS}, TS_{MA-FS}) >_{x_{MA-FS}}). \quad (19)$$

Through Equations (18) and (19), and the *nonce verification rule*, we originate the following statement:

$$FS| \equiv MA| \equiv (< ID_{MA}, k_{MA-FS}, TS_{MA-FS} >_{PK_{FS}}, < H(ID_{MA}, k_{MA-FS}, TS_{MA-FS}) >_{x_{MA-FS}}). \quad (20)$$

Through Equation (20), and the *belief rule*, we originate the following statement:

$$FS| \equiv MA| \equiv MA \stackrel{x_{MA-FS}}{\longleftrightarrow} FS. \quad (21)$$

Through Equation (21), A14, and the *jurisdiction rule*, we originate the following statement:

$$FS| \equiv MA \stackrel{x_{MA-FS}}{\longleftrightarrow} FS. \quad (22)$$

Through Equation (22), and the *belief rule*, we originate the following statement:

$$FS| \equiv MA| \equiv ID_{MA}. \quad (23)$$

Through Equation (23), *A16*, and the *jurisdiction rule*, we originate the following statement:

$$FS| \equiv ID_{MA}. \quad (24)$$

d. The manufacturer *MA* authenticates the firearm store *FS*.

Through *M4* and the *seeing rule*, we originate the following statement:

$$MA \triangleleft (\langle ID_{FS}, k_{FS-MA}, TS_{FS-MA} \rangle_{PK_{MA}}, \langle H(ID_{FS}, k_{FS-MA}, TS_{FS-MA}) \rangle_{x_{FS-MA}}). \quad (25)$$

Through *A9* and the *freshness rule*, we originate the following statement:

$$MA| \equiv \#(\langle ID_{FS}, k_{FS-MA}, TS_{FS-MA} \rangle_{PK_{MA}}, \langle H(ID_{FS}, k_{FS-MA}, TS_{FS-MA}) \rangle_{x_{FS-MA}}). \quad (26)$$

Through Equation (25), *A11*, and the *message meaning rule*, we originate the following statement:

$$MA| \equiv FS| \sim (\langle ID_{FS}, k_{FS-MA}, TS_{FS-MA} \rangle_{PK_{MA}}, \langle H(ID_{FS}, k_{FS-MA}, TS_{FS-MA}) \rangle_{x_{FS-MA}}). \quad (27)$$

Through Equations (26) and (27), and the *nonce verification rule*, we originate the following statement:

$$MA| \equiv FS| \equiv (\langle ID_{FS}, k_{FS-MA}, TS_{FS-MA} \rangle_{PK_{MA}}, \langle H(ID_{FS}, k_{FS-MA}, TS_{FS-MA}) \rangle_{x_{FS-MA}}). \quad (28)$$

Through Equation (28), and the *belief rule*, we originate the following statement:

$$MA| \equiv FS| \equiv MA \stackrel{x_{FS-MA}}{\longleftrightarrow} FS. \quad (29)$$

Through Equation (29), *A13*, and the *jurisdiction rule*, we originate the following statement:

$$MA| \equiv MA \stackrel{x_{FS-MA}}{\longleftrightarrow} FS. \quad (30)$$

Through Equation (30), and the *belief rule*, we originate the following statement:

$$MA| \equiv FS| \equiv ID_{FS}. \quad (31)$$

Through Equation (31), *A15*, and the *jurisdiction rule*, we originate the following statement:

$$MA| \equiv ID_{FS}. \quad (32)$$

Through Equations (22), (24), (30) and (32), it can be proven that, in the proposed scheme, the manufacturer *MA* and the firearm store *FS* authenticate each other. Moreover, it can also be proven that the proposed scheme can authenticate the private key of the manufacturer *MA* and the firearm store *FS*.

In the proposed scheme, the firearm store authenticates the manufacturer by

$$x_{MA-FS}' \stackrel{?}{=} r_{MA-FS} \bmod n.$$

If it passes the verification, the firearm store authenticates the legality of the manufacturer. The manufacturer authenticates the firearm store by

$$x_{FS-MA}' \stackrel{?}{=} r_{FS-MA} \bmod n.$$

If it passes the verification, the manufacturer authenticates the legality of the firearm store. The firearm selling phase of the proposed scheme, thus, guarantees mutual authentication between the firearm store and the manufacturer.

In the owner holding phase of the proposed scheme, the main goal of the scheme is to authenticate the private key of the firearm owner *FO* and the firearm store *FS*.

$$\begin{aligned}
G17: FO| &\equiv FO \stackrel{x_{FS-FO}}{\leftrightarrow} FS. \\
G18: FO| &\equiv FS| \equiv FO \stackrel{x_{FS-FO}}{\leftrightarrow} FS. \\
G19: FS| &\equiv FO \stackrel{x_{FO-FS}}{\leftrightarrow} FS. \\
G20: FS| &\equiv FO| \equiv FO \stackrel{x_{FO-FS}}{\leftrightarrow} FS. \\
G21: FO| &\equiv ID_{FS}. \\
G22: FO| &\equiv FS| \equiv ID_{FS}. \\
G23: FS| &\equiv ID_{FO}. \\
G24: FS| &\equiv FO| \equiv ID_{FO}.
\end{aligned}$$

According to the owner holding phase, BAN logic is applied to produce an idealized form as follows:

$$\begin{aligned}
M5: (< ID_{FO}, k_{FO-FS}, TS_{FO-FS} >_{PK_{FS}}, < H(ID_{FO}, k_{FO-FS}, TS_{FO-FS}) >_{x_{FO-FS}}), \\
M6: (< ID_{FS}, k_{FS-FO}, TS_{FS-FO} >_{PK_{FO}}, < H(ID_{FS}, k_{FS-FO}, TS_{FS-FO}) >_{x_{FS-FO}}).
\end{aligned}$$

To analyze the proposed scheme, the following assumptions are made:

$$\begin{aligned}
A17: FO| &\equiv \#(k_{FO-FS}), \\
A18: FS| &\equiv \#(k_{FO-FS}), \\
A19: FO| &\equiv \#(k_{FS-FO}), \\
A20: FS| &\equiv \#(k_{FS-FO}), \\
A21: FO| &\equiv FS| \Rightarrow FO \stackrel{x_{FS-FO}}{\leftrightarrow} FS, \\
A22: FS| &\equiv FO| \Rightarrow FO \stackrel{x_{FO-FS}}{\leftrightarrow} FS, \\
A23: FO| &\equiv FS| \Rightarrow ID_{FS}, \\
A24: FS| &\equiv FO| \Rightarrow ID_{FO}.
\end{aligned}$$

According to these assumptions and rules of BAN logic, the main proof of the owner holding phase is as follows:

- e. The firearm store FS authenticates the firearm owner FO.

Through *M5* and the *seeing rule*, we originate the following statement:

$$FS \triangleleft (< ID_{FO}, k_{FO-FS}, TS_{FO-FS} >_{PK_{FS}}, < H(ID_{FO}, k_{FO-FS}, TS_{FO-FS}) >_{x_{FO-FS}}). \quad (33)$$

Through *A18* and the *freshness rule*, we originate the following statement:

$$FS| \equiv \#(< ID_{FO}, k_{FO-FS}, TS_{FO-FS} >_{PK_{FS}}, < H(ID_{FO}, k_{FO-FS}, TS_{FO-FS}) >_{x_{FO-FS}}). \quad (34)$$

Through Equation (33), *A20*, and the *message meaning rule*, we originate the following statement:

$$FS| \equiv FO| \sim (< ID_{FO}, k_{FO-FS}, TS_{FO-FS} >_{PK_{FS}}, < H(ID_{FO}, k_{FO-FS}, TS_{FO-FS}) >_{x_{FO-FS}}). \quad (35)$$

Through Equations (34) and (35), and the *nonce verification rule*, we originate the following statement:

$$FS| \equiv FO| \equiv (< ID_{FO}, k_{FO-FS}, TS_{FO-FS} >_{PK_{FS}}, < H(ID_{FO}, k_{FO-FS}, TS_{FO-FS}) >_{x_{FO-FS}}). \quad (36)$$

Through Equation (36), and the *belief rule*, we originate the following statement:

$$FS| \equiv FO| \equiv FO \stackrel{x_{FO-FS}}{\leftrightarrow} FS. \quad (37)$$

Through Equation (37), *A22*, and the *jurisdiction rule*, we originate the following statement:

$$FS| \equiv FO \stackrel{x_{FO-FS}}{\leftrightarrow} FS. \quad (38)$$

Through Equation (38), and the *belief rule*, we originate the following statement:

$$FS| \equiv FO| \equiv ID_{FO}. \quad (39)$$

Through Equation (39), A24, and the *jurisdiction rule*, we originate the following statement:

$$FS| \equiv ID_{FO}. \quad (40)$$

f. The firearm owner *FO* authenticates the firearm store *FS*.

Through M6 and the *seeing rule*, we originate the following statement:

$$FO \triangleleft (< ID_{FS}, k_{FS-FO}, TS_{FS-FO} >_{PK_{FO}}, < H(ID_{FS}, k_{FS-FO}, TS_{FS-FO}) >_{x_{FS-FO}}). \quad (41)$$

Through A17 and the *freshness rule*, we originate the following statement:

$$FO| \equiv \#(< ID_{FS}, k_{FS-FO}, TS_{FS-FO} >_{PK_{FO}}, < H(ID_{FS}, k_{FS-FO}, TS_{FS-FO}) >_{x_{FS-FO}}). \quad (42)$$

Through Equation (41), A19, and the *message meaning rule*, we originate the following statement:

$$FO| \equiv FS| \sim (< ID_{FS}, k_{FS-FO}, TS_{FS-FO} >_{PK_{FO}}, < H(ID_{FS}, k_{FS-FO}, TS_{FS-FO}) >_{x_{FS-FO}}). \quad (43)$$

Through Equations (42) and (43), and the *nonce verification rule*, we originate the following statement:

$$FO| \equiv FS| \equiv (< ID_{FS}, k_{FS-FO}, TS_{FS-FO} >_{PK_{FO}}, < H(ID_{FS}, k_{FS-FO}, TS_{FS-FO}) >_{x_{FS-FO}}). \quad (44)$$

Through Equation (44), and the *belief rule*, we originate the following statement:

$$FO| \equiv FS| \equiv FO \stackrel{x_{FS-FO}}{\leftrightarrow} FS. \quad (45)$$

Through Equation (45), A21, and the *jurisdiction rule*, we originate the following statement:

$$FO| \equiv FO \stackrel{x_{FS-FO}}{\leftrightarrow} FS. \quad (46)$$

Through Equation (46), and the *belief rule*, we originate the following statement:

$$FO| \equiv FS| \equiv ID_{FS}. \quad (47)$$

Through Equation (47), A23, and the *jurisdiction rule*, we originate the following statement:

$$FO| \equiv ID_{FS}. \quad (48)$$

Through Equations (38), (40), (46) and (48), it can be proven that, in the proposed scheme, the firearm owner *FO* and the firearm store *FS* authenticate each other. Moreover, it can also be proven that the proposed scheme can authenticate the private key of the firearm owner *FO* and the firearm store *FS*.

In the proposed scheme, the firearm store authenticates the firearm owner by

$$x_{FO-FS}' \stackrel{?}{=} r_{FO-FS} \bmod n.$$

If it passes the verification, the firearm store authenticates the legality of the firearm owner. The firearm owner authenticates the firearm store by

$$x_{FS-FO}' \stackrel{?}{=} r_{FS-FO} \bmod n.$$

If it passes the verification, the firearm owner authenticates the legality of the firearm store. The owner holding phase of the proposed scheme, thus, guarantees mutual authentication between the firearm store and the firearm owner.

4.2. Verifiability

Using digital certificate verification can publicly verify the identity of the manufacturer and the authorization information that was published. Due to the openness and

transparency of the information on the chain, we can truly realize high efficiency and specialization in the field of firearm management.

Let us take the message transmitted by MA and FA as an example. When FA sends a message signed by ECDSA to the MA, the MA first verifies the correctness of the time stamp and signature, generates blockchain data $BC_{FA-MA} = h(r_{FA-MA}, s_{FA-MA})$, and uses ID_{BC} as an index to upload the blockchain data to the Blockchain Center (BCC). That is to say, after verifying the correctness of the time stamp and signature for each role that receives the message, it also verifies the correctness of the blockchain data generated by the previous role. Therefore, our proposed solution achieves the characteristics of public verification through blockchain technology and the ECDSA digital signature.

Threat scenario: FO wants to confirm whether the firearm purchased is a qualified firearm authorized by FA.

Response analysis: Through the blockchain message $BC_{FA-MA} = h(r_{FA-MA}, s_{FA-MA})$, the MA can confirm that the firearm is authorized by FA. Through the blockchain message $BC_{MA-FS} = h(r_{MA-FS}, s_{MA-FS})$, the FS can confirm that the firearm is manufactured by a legal MA. Lastly, through the blockchain message $BC_{FS-FO} = h(r_{FS-FO}, s_{FS-FO})$, the FO can confirm that the firearm is sold by a qualified FS.

4.3. Resistance to Forgery

The timestamp and signature mechanism can be used to irreversibly generate a string composed of random numbers and letters for the data placed in each block. This original text cannot be inferred from the string, thus effectively solving the trust problem. After the hash function operation, the messages are described as follows:

$$\begin{aligned} z_{MA-FA} &= h(ID_{MA}, M_{MA-FA}, Cert_{MA}, TS_{MA-FA}) \\ z_{FA-MA} &= h(ID_{FA}, M_{FA-MA}, Cert_{GUN}, TS_{FA-MA}, ID_{BC}) \\ z_{MA-FS} &= h(ID_{MA}, M_{MA-FS}, Cert_{MA}, Info_{GUN}, TS_{MA-FS}, ID_{BC}) \\ z_{FS-MA} &= h(ID_{FS}, M_{FS-MA}, Cert_{FS}, Info_{GUN}, TS_{FS-MA}, ID_{BC}) \\ z_{FO-FS} &= h(ID_{FO}, M_{FO-FS}, SSN_{FO}, TS_{FO-FS}) \\ z_{FS-FO} &= h(ID_{FS}, M_{FS-FO}, Cert_{FS}, Info_{GUN}, SSN_{FO}, TS_{FS-FO}, ID_{BC}) \end{aligned}$$

The hash value cannot be reversed back to the original content; thus, this agreement achieves the characteristic that the message cannot be tampered with.

Threat scenario: FO wants to use the firearm they own to commit a crime, subsequently trying to falsify the personal information provided at the time of purchase.

Response analysis: The FO will not be able to modify the purchase information, because the social security number used to purchase the firearm is recorded in the blockchain $z_{FO-FS} = h(ID_{FO}, M_{FO-FS}, SSN_{FO}, TS_{FO-FS})$ and $z_{FS-FO} = h(ID_{FS}, M_{FS-FO}, Cert_{FS}, Info_{GUN}, SSN_{FO}, TS_{FS-FO}, ID_{BC})$, and it can no longer be modified.

4.4. Traceability

After the firearm information is on the chain, the data block containing the social security number information is permanently stored on the blockchain and cannot be tampered with. All production and transaction traces can be traced throughout the entire process, which can be used for firearm management. For example, when we want to verify and trace whether the blockchain data between MA and FA is legal, we can compare and verify $BC_{MA-FA} \stackrel{?}{=} h(r_{MA-FA}, s_{MA-FA})$ and $BC_{FA-MA} \stackrel{?}{=} h(r_{FA-MA}, s_{FA-MA})$. When we want to verify and trace whether the blockchain data between MA and FS is legal, we can compare and verify $BC_{MA-FS} \stackrel{?}{=} h(r_{MA-FS}, s_{MA-FS})$ and $BC_{FS-MA} \stackrel{?}{=} h(r_{FS-MA}, s_{FS-MA})$. When we want to verify and trace whether the blockchain data between FO and FS is legal, we can compare and verify $BC_{FO-FS} \stackrel{?}{=} h(r_{FO-FS}, s_{FO-FS})$ and $BC_{FS-FO} \stackrel{?}{=} h(r_{FS-FO}, s_{FS-FO})$.

Threat scenario: When the MA finds that some firearms have production defects, they need to be recycled, but they may have been sold to a FO.

Response analysis: MA can use the blockchain messages $BC_{MA-FS} \stackrel{?}{=} h(r_{MA-FS}, s_{MA-FS})$ and $BC_{FS-MA} \stackrel{?}{=} h(r_{FS-MA}, s_{FS-MA})$ to know which FS the firearms were dis-

tributed to, and the FS can also use the blockchain messages $BC_{FO-FS} \stackrel{?}{=} h(r_{FO-FS}, s_{FO-FS})$ and $BC_{FS-FO} \stackrel{?}{=} h(r_{FS-FO}, s_{FS-FO})$ to confirm which FO these firearms were sold to, before carrying out a full recovery.

4.5. Integrity

To achieve the integrity of the data in this paper, we used digital signatures and public-key technology. When a malicious person alters the data, the receiver can verify whether the data were altered by verifying the signature. The user can further use the public key to encrypt data for transmission. Malicious people will not be able to obtain encrypted data because they do not have a correct private key, and they are unable to tamper with data because malicious people cannot access it.

Threat scenario: The attacker intercepts the message from the firearm authority to the accessing party and tampers with the message before sending it to the accessing party.

Response analysis: The attacker will fail because our proposed method uses public keys to encrypt data. Malicious people will not be able to obtain encrypted data because they do not have a correct private key. Even if the attacker intercepts the message, the attacker cannot decrypt the message and tamper with the message. In summary, the attacker cannot modify the message and send it to the accessing party.

4.6. Decentralization/Distribution

In the proposed scheme, the information handled by each role is signed by the role with a private key, and the circulation of all information is open and transparent. A node cannot deceive other nodes. In this way, the trust relationship between nodes is realized, making it possible to obtain trust between nodes at a low cost. Thus, the proposed scheme achieves decentralization and distribution.

4.7. Nonrepudiation

The content of the message sent by each role is signed by the sender with its ECDSA private key. After receiving the message, the receiver verifies the message with the sender's public key. If the message is successfully verified, the sender will not deny the content of the message transmitted. Table 1 proposes the description of each role in this program.

Table 1. Nonrepudiation of the proposed scheme.

Phase \ Item	Signature	Sender	Receiver	Signature Verification
Authorized production phase	(r_{MA-FA}, s_{MA-FA})	MA	FA	$x_{MA-FA}' \stackrel{?}{=} r_{MA-FA} \bmod n$
	(r_{FA-MA}, s_{FA-MA})	FA	MA	$x_{FA-MA}' \stackrel{?}{=} r_{FA-MA} \bmod n$
Firearm selling phase	(r_{MA-FS}, s_{MA-FS})	MA	FS	$x_{MA-FS}' \stackrel{?}{=} r_{MA-FS} \bmod n$
	(r_{FS-MA}, s_{FS-MA})	FS	MA	$x_{FS-MA}' \stackrel{?}{=} r_{FS-MA} \bmod n$
Owner holding phase	(r_{FO-FS}, s_{FO-FS})	FO	FS	$x_{FO-FS}' \stackrel{?}{=} r_{FO-FS} \bmod n$
	(r_{FS-FO}, s_{FS-FO})	FS	FO	$x_{FS-FO}' \stackrel{?}{=} r_{FS-FO} \bmod n$

4.8. Computation Cost

Table 2 presents the computation cost analysis of this scheme.

Table 2 shows the computation cost analysis of all stages and roles in this scheme. We analyzed the highest cost of the authorized production phase as an example. The MA requires seven multiplication operations, three hash function operations, two comparison operations, and two encryption operations. The FA requires seven multiplication operations, three hash function operations, two comparison operations, and two encryption operations. The proposed scheme has a good computational cost.

Table 2. Computation cost analysis of this scheme. BCC, blockchain center; MA, manufacturer; FA, firearm authority; FS, firearm store; FO, firearm owner; N/A, not applicable.

Phase \ Role	BCC	MA	FA	FS	FO
Access party registration phase	$1T_{Mul}$	N/A	N/A	N/A	N/A
Authorized production phase	N/A	$7T_{Mul} + 3T_H + 2T_{Cmp} + 2T_{Enc}$	$7T_{Mul} + 3T_H + 2T_{Cmp} + 2T_{Enc}$	N/A	N/A
Firearm selling phase	N/A	$7T_{Mul} + 3T_H + 2T_{Cmp} + 2T_{Enc}$	N/A	$7T_{Mul} + 3T_H + 2T_{Cmp} + 2T_{Enc}$	N/A
Owner holding phase	N/A	N/A	N/A	$7T_{Mul} + 3T_H + 2T_{Cmp} + 2T_{Enc}$	$7T_{Mul} + 3T_H + 2T_{Cmp} + 2T_{Enc}$

T_{Mul} : multiplication operation. T_H : hash function operation. T_{Cmp} : comparison operation. T_{Enc} : encryption operation.

4.9. Communication Cost

Table 3 analyzes the communication cost of this scheme.

Table 3. Communication cost analysis of our scheme.

Phase \ Item	Message Length	Rounds	3.5G (14 Mbps)	4G (100 Mbps)	5G (20 Gbps)
Access party registration phase	2528 bits	2	0.181 ms	0.025 ms	0.126 us
Authorized production phase	2528 bits	2	0.181 ms	0.025 ms	0.126 us
Firearm selling phase	2528 bits	2	0.181 ms	0.025 ms	0.126 us
Owner holding phase	2528 bits	2	0.181 ms	0.025 ms	0.126 us

The communication cost analysis of each phase in this scheme is shown in Table 3. We assume that the ECDSA key and signature are 160 bits, the asymmetric message is 1024 bits, and the rest of the message length such as the ID is 80 bits. We analyzed the authorized production phase as an example. The message sent by the MA to the FA includes two ECDSA keys and signatures, one asymmetric message, and one other message. The message includes two ECDSA keys and signatures, one asymmetric message, and one other message. The total communication cost in the authorized production phase is 2528 bits, which takes 0.181 ms under the 3.5G (14 Mbps) communication environment, 0.025 ms under the The fourth generation of mobile phone mobile communication technology standards, (4G, 100 Mbps) communication environment, and 0.126 us under the 5G (20 Mbps) communication environment [26]. The proposed scheme has excellent performance.

5. Conclusions

The availability of firearms has led to a surge in the number of firearms. The number of guns usually affects gun crime. Therefore, an effective management mechanism can reduce the rate of gun crime. Therefore, how to manage the gun supply chain is an important

issue. In this article, we propose a blockchain-based tracking firearm framework with RFID technology. The blockchain allows all participants to verify the chained data. It can ensure that the message will not be tampered with. In addition, we also combined the application of RFID to effectively track the supply chain.

As mentioned above, this study proposes a secure firearm supply chain architecture based on blockchain. The proposed method achieves several goals. First of all, the characteristic data through the blockchain can be publicly verified and the information will not be modified. The traceability of the data and the application of RFID can effectively manage the production chain. Moreover, we used BAN logic to prove mutual authentication. Our proposed method also achieves verifiability, resistance to forgery, traceability, integrity, and nonrepudiation.

Author Contributions: Conceptualization, C.-L.C., C.-C.L., and Y.-Y.D.; methodology, C.-L.C., C.-C.L., and Y.-Y.D.; validation, W.W., K.W., and C.-C.L.; investigation, C.-C.L. and Y.-Y.D.; data analysis, C.-L.C., Y.-Y.D. and C.-C.L.; writing—original draft preparation, C.-L.C., C.-C.L., and Y.-Y.D.; writing—review and editing, M.-L.C., W.W., and K.W.; supervision, M.-L.C. and C.-L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Natural Science Foundation of Fujian Province of China (2018J01572).

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

Abbreviations

q	A k -bit prime number
$GF(q)$	Finite group q
E	The elliptic curve defined on finite group q
G	A generating point based on the elliptic curve E
ID_x	A name representing identity x
k_x	A random value on the elliptic curve
(r_x, s_x)	Elliptic curve signature value of x
(x_x, y_x)	An ECDSA signature message of x
M_{x-y}	A message from x to y
ID_{BC}	An index value of blockchain message
BC_x	Blockchain message of x
TS_x	Timestamp message of x
C_x	Encrypted message using the asymmetric key of x
SSN_x	The social security number of x
$Info_x$	The manufacturing information of the firearm
$Cert_x$	A digital certificate of x conforming to the X.509 standard
$h(.)$	Hash function
$A \stackrel{?}{=} B$	Verification of whether A is equal to B

References

1. Alcorn, T. Trends in research publications about gun violence in the United States, 1960 to 2014. *JAMA Intern. Med.* **2017**, *177*, 124–126. [CrossRef] [PubMed]
2. Gun Control Offers No Cure-All in America. Available online: http://nbcpolitics.nbcnews.com/_news/2012/12/18/15977143-gun-control-offers-no-cure-all-in-america (accessed on 30 December 2020).
3. How, U.S. Gun Deaths Compare to Other Countries. Available online: <https://www.cbsnews.com/news/how-u-s-gun-deaths-compare-to-other-countries/> (accessed on 30 December 2020).
4. Gun Violence Archive. Available online: <https://www.gunviolencearchive.org/past-tolls> (accessed on 30 December 2020).
5. Gun Deaths in U.S. Reach Highest Level in Nearly 40 Years, CDC Data Reveal. Available online: <https://edition.cnn.com/2018/12/13/health/gun-deaths-highest-40-years-cdc/index.html> (accessed on 30 December 2020).
6. Gun Trace Report—City of Chicago. Available online: <https://www.chicago.gov/content/dam/city/depts/mayor/Press%20Room/Press%20Releases/2017/October/GTR2017.pdf> (accessed on 30 December 2020).
7. Angeles, R. RFID technologies: Supply-chain applications and implementation issues. *Inf. Syst. Manag.* **2005**, *22*, 51–65. [CrossRef]
8. Sarac, A.; Absi, N.; Dauzère-Pérès, S. A literature review on the impact of RFID technologies on supply chain management. *Int. J. Prod. Econ.* **2010**, *128*, 77–95. [CrossRef]

9. Weapon Tracking System. Available online: <http://www.bartronics.com/weapon-tracking.html> (accessed on 18 March 2020).
10. RFID for Weapons Tracking. Available online: <https://www.vizinexrfid.com/industry-applications/weapons-tracking/> (accessed on 18 March 2020).
11. Dutta, P.; Choi, T.M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067. [CrossRef] [PubMed]
12. Miller, V.S. Use of Elliptic Curves in Cryptography. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Linköping, Sweden, 20–22 May 1986; Springer: Berlin/Heidelberg, Germany, 1985; pp. 417–426.
13. Burrows, M.; Abadi, M.; Needham, R.M. A logic of authentication. *Proc. R. Soc. Lond. Math. Phys. Sci.* **1989**, *426*, 233–271.
14. Chen, C.L.; Li, Y.T.; Deng, Y.Y.; Weng, W.; Zhou, M.; Sun, H. A blockchain based intelligent anti-switch package in tracing logistics system. *J. Supercomput.* **2021**, 1–42. [CrossRef]
15. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 1–36.
16. Chen, C.L.; Chen, Y.X.; Lee, C.F.; Deng, Y.Y.; Chen, C.H. An efficient and secure key agreement protocol for sharing emergency events in VANET systems. *IEEE Access* **2019**, *7*, 148472–148484. [CrossRef]
17. Chen, C.L.; Li, Y.T.; Deng, Y.Y.; Li, C.T. Robot identification and authentication in a robot cloud service system. *IEEE Access* **2018**, *6*, 56488–56503. [CrossRef]
18. Chen, C.L.; Deng, Y.Y.; Li, C.T.; Zhu, S.; Chiu, Y.J.; Chen, P.Z. An IoT-based traceable drug anti-counterfeiting management system. *IEEE Access* **2020**, *8*, 224532–224548. [CrossRef]
19. Szabo, N. Smart contracts: Building blocks for digital markets. *EXTROPY J. Transhumanist Thought* **1996**, *18*, 16.
20. Szabo, N. The Idea of Smart Contracts. 1997. Available online: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html (accessed on 26 November 2020).
21. Han, W.; Zhu, Z. An ID-based mutual authentication with key agreement protocol for multiserver environment on elliptic curve cryptosystem. *Int. J. Commun. Syst.* **2014**, *27*, 1173–1185. [CrossRef]
22. Boneh, D.; Lynn, B.; Shacham, H. Short Signatures from the Weil Pairing. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, 2001, Innsbruck, Austria, 6–10 May 2001; Ans. Springer: Berlin/Heidelberg, Germany, 2001; pp. 514–532.
23. Chen, C.-L.; Yang, T.-T.; Chiang, M.-L.; Shih, T.-F. A privacy authentication scheme based on cloud for medical environment. *J. Med. Syst.* **2014**, *38*, 143. [CrossRef] [PubMed]
24. Chen, C.-L.; Yang, T.-T.; Shih, T.-F. A secure medical data exchange protocol based on cloud environment. *J. Med. Syst.* **2014**, *38*, 112. [CrossRef] [PubMed]
25. Blaze, M.; Bleumer, G.; Strauss, M. Divertible Protocols and Atomic Proxy Cryptography. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Espoo, Finland, 31 May–4 June 1998; Springer: Berlin/Heidelberg, Germany, 1998; pp. 127–144.
26. Marcus, M.J. 5G and IMT for 2020 and beyond. *IEEE Wirel. Commun.* **2015**, *22*, 2–3. [CrossRef]