symmetry

Article

A Traceable Online Will System Based on Blockchain and Smart Contract Technology

Chin-Ling Chen [1,2,3], Ching-Ying Lin [4], Mao-Lun Chiang [4,*], Yong-Yuan Deng [3,*], Peizhi Chen [1,*] and Yi-Jui Chiu [5]

[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; s10430013@gm.cyut.edu.tw
[5] School of Mechanical and Automotive Engineering, Xiamen University of Technology, Xiamen 361024, China; chiuyijui@xmut.edu.cn
* Correspondence: mlchiang@cyut.edu.tw or s10830604@gm.cyut.edu.tw (M.-L.C.); allendeng@cyut.edu.tw (Y.-Y.D.); pzc@xmut.edu.cn (P.C.)

Abstract: In recent years, with the rapid levels of economic development, there have been more and more problems in property inheritance and distribution. In today's society, people still have many taboos when writing a will. Writing a will not only involves various laws and regulations but also costs a lot of money and time, which can be daunting. However, with the development of the Internet, blockchain technology has gradually been applied to many applications. Blockchain technology uses consensus algorithms to ensure consistency and records transaction information in blocks to ensure the effectiveness of transactions. In this paper, we use the cryptography mechanism to propose an online will system based on blockchain and smart contract technology. The architecture considers effectiveness and cost reduction. By combining this with blockchain technology, will assets are saved in blocks, which provides comprehensive will security and non-tamperable security protection. In addition, combined with a smart contract, it realizes the method of automatic property distribution. At the same time, this mechanism also proposes an arbitration solution when there are disputes over wills, and ensures the integrity of data, public verifiability, unforgeability, nonrepudiation, irreversibility of information, and the ability to resist counterfeiting attacks.

Keywords: e-will; blockchain; smart contract; data privacy; secrecy

check for updates

Citation: Chen, C.-L.; Lin, C.-Y.; Chiang, M.-L.; Deng, Y.-Y.; Chen, P.; Chiu, Y.-J. A Traceable Online Will System Based on Blockchain and Smart Contract Technology. *Symmetry* **2021**, *13*, 466. https://doi.org/10.3390/sym13030466

Academic Editor: Basil Papadopoulos

Received: 12 February 2021
Accepted: 9 March 2021
Published: 12 March 2021

1. Introduction

Family quarrels on inheritance issues are nothing new, but in recent years they have become the main content of the news. Most people do not adopt the habit of writing a will, mainly because they have scruples about death. This has led to many families fighting for inheritance rights, causing family members to hate each other and damaging the harmony of society. Succession struggles often occur. For example, after the parents hand over a property to their children, the children begin to rebel against the parents, or the siblings fight over the property with each other.

A starker example is Hendrix's USD 80 million real estate dispute [1]. Hendrix's brother, Leon, announced that he was also entitled to inherit the estate and started a real estate lawsuit with Al's adopted daughter. Other notable examples include pop singer Michael Jackson's USD 100 billion asset allocation event [2], and the occasion where Macau gambled king Stanley Ho's USD 100 billion assets [3]. Generally speaking, there are two types of will: the traditional form and the online electronic form. The traditional form of will usually requires a lawyer to write a will. In addition to paying high legal fees, it also takes time to process. Alternatively, you can write a will orally, but a will involves many laws and regulations, so people are usually afraid of orally writing a will. Even if you write a will yourself, you do not know whether it is complete and valid. Nowadays, with the rapid development of the Internet, the processing and control of documents and data have become easier, and there is an increasing number of online electronic wills. Electronic wills can also effectively reduce costs and make writing wills more feasible and easier.

With the continuous development of the Internet, there have been many related studies on electronic wills in recent years [4–7]. Chien and Lin [4] presented their first paper in 2009, studying the feasibility of an electronic will system on the Internet and designing a secure electronic will protocol. Then, Lee et al. [5] found that Chien and Lin's scheme has the following problems. First, the trust agency knows or can easily calculate the user's private key. Therefore, it cannot provide non-repudiation and does not comply with the relevant provisions of the "Digital Signature Law" and the "Civil Law of the Republic of China". Second, their scheme does not provide any effective method to verify the digital signature. Therefore, it may not be possible to check the validity of the will after death. To solve these problems, Li et al. [5] proposed a new electronic will system based on government public keys. Then, in 2012, Chen et al. [6] proposed an online will preservation system based on a secret sharing mechanism, which combines a public key and symmetric key system to prevent family disputes caused by inheritance and distribution. Through online hosting, you can reduce costs and increase efficiency; privacy is protected by powerful security mechanisms that can resist various types of attacks, improve paper defects, and meet various security requirements and other advantages. In 2017, Sreehari et al. [7] proposed the concept of saving wills in the blockchain through smart contracts. Using blockchain technology to draft a will can be tamper-proof, safe, and transparent. Additionally, it improves the speed of the probate and solves many annoying issues in the current will system. However, the scheme proposed by Sreehari et al. is only in the drafting stage, the real detailed protocol does not appear in this article.

Traditional wills have the following problems: how to verify the authenticity of the will; trust issues between individuals; complicated execution procedures, etc. An electronic will is a new type of will supported by the Internet. The Internet itself has complex functions. Although the Internet safe deposit box [8] provides users with a more private space, it will require corresponding security measures. However, this does not mean that the electronic wills stored in a secure deposit box are completely safe and reliable; on the other hand, whether the testator can test a will is not easy to accurately identify in the complex environment of the Internet. Generally, it is difficult to effectively guarantee and verify the authenticity of the content of an electronic will. This also greatly hinders the legal effect of electronic wills. Only by ensuring the authenticity of the contents of the will can it have legal effect.

Blockchain is the basic technology for creating bitcoin, the most popular cryptocurrency. Satoshi Nakamoto proposed the concept of "Blockchain" in 2008 [9], through the concept of a decentralized ledger to create a new accounting method, skipping the intermediary bank, and letting all participants' computers bookkeep together in order to achieve a decentralized transaction system. Traders' transactions need to be encrypted by miners and confirmed by most verifiers before they can be uploaded to the block. Therefore, this system also has the characteristics of non-tampering and traceability. The Ethereum blockchain platform was launched in 2014 [10]. It is a blockchain embedded with Turing's complete programming language, emphasizing that smart contracts are a feature of its platform. Programs stored in the blockchain through smart contracts can perform various tasks automatically, similarly to automatic programs. The deployment of any smart contract is carried out through blockchain transactions. Once the smart contract is deployed, it cannot be modified. Therefore, it also has the characteristics of consistency, non-tampering, and automation. In short, the core technology of blockchain solves the problem of distrust through timestamps, hash algorithms, smart contracts, and consensus mechanisms, that is, transactions can be conducted without establishing any trust relationship between all nodes in the system. The operation of the entire system and the chain structure of the database is open and transparent. Within the corresponding rules formulated by the system and within a specific time range, nodes cannot be tampered with or deceived.

In this research, we propose a traceable online will system based on blockchain and smart contract technology to solve the current issues of validity, privacy, and security protection that arise when producing a will. We deploy our smart contracts through the Ethereum blockchain and develop and test smart contracts through Web3.js, Solidity, and Ganache. In this research, as far as the integrity of the electronic will is concerned, we use the Elliptic Curve Digital Signature Algorithm (ECDSA) to sign the information transmitted by the parties. By combining blockchain technology, we use the three main characteristics of blockchain decentralization, non-modification, and publicly verifiable chains, allowing data to be decentralized without relying on other regulatory agencies and hardware facilities, with data being stored in a message block. These message blocks are linked together in a similar "chain" manner, which has the characteristics of preventing tampering and being publicly verifiable, thus, ensuring the integrity of the will. Regarding the trust of the electronic will, all messages must be verified before linking, and the user must have the correct encryption key to read or write the message to the block. This research also combines smart contracts to make the process automation lengthy and complicated. The process information is open and transparent, and will not be subject to human intervention or tampering. This not only reduces the process cost but also solves the trust problem.

Therefore, the general requirements for electronic will production can be summarized as follows:

(1) The integrity of data [4,6,11,12]: In the process of transmitting and storing information or data, methods such as digital signatures and hash functions are used to ensure data integrity.
(2) Public verifiability [6,7]: The data or the data source can be publicly verified.
(3) Unforgeability [4–6]: The information is released from the source that owns the private key.
(4) Non-repudiation [5,6,11,12]: The data source cannot arbitrarily reject the behavior and content of the message.
(5) Message irreversibility [13–18]: The corresponding plaintext cannot be traced back from the encrypted message.
(6) Resist counterfeiting attacks [14–19]: By verifying the public and private keys, the correctness of the message source can be ensured.
(7) Tamperproof [14–18]: Once the data in the will are confirmed, they are permanently written to the block, and once written into the blockchain, each datum cannot be changed.
(8) System decentralization [14–18]: Allow all nodes to verify the authenticity of transactions.
(9) Fair arbitration [20,21]: Legal arbitration institutions assist in the arbitration process.

The remaining sections of this paper are organized as follows: Section 2 introduces the preliminary research, the third section introduces our system architecture and algorithm in detail, the fourth and fifth sections, respectively, discuss the security analysis and performance. Finally, we conclude this article in Section 6.

2. Preliminary

2.1. Elliptic Curve Digital Signature Algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is an asymmetric key encryption technology used by Bitcoin and Ethereum blockchains. ECDSA [22] is a combination of ECC(Elliptic-Curve Cryptography) [23] and DSA(Digital Signature Algorithm) [24]. Compared with the general elliptic curve encryption algorithm, the required public key bit size is about twice the security level. For the ECDSA algorithm, the signing and verification process is as follows: Suppose Alice wants to send a message to Bob. First, both parties must choose the elliptic curve and the origin G on the curve. Then, Alice must generate a random number d_A as Alice's private key in the interval [*1, n-1*], and generate a public key $Q_A = d_AG$. If Alice wants to send a message m, Alice needs to generate a random number k in the interval [1, n−1], calculate $z = h(m)$, $(x_1, y_1) = kG$, $r = x_1 \text{mod}\ n$, $s = k^{-1}(z + rd_A)$ mod n, and then send the message m and the ECDSA signature (r, s) to Bob, and Bob receives it. The correctness of the ECDSA signature will be verified. First, Bob will calculate $z' = h(m)$, $u_1 = z's^{-1} \text{mod}\ n$, $u_2 = rs^{-1} \text{mod}\ n$, $(x_1', y_1') = u_1G + u_2Q_A$ $r = x_1' \text{mod}\ n$. If the verification passes, Bob confirms that the signature and message (m) sent by Alice are correct.

2.2. Smart Contract

Interdisciplinary legal scholar Nick Szabo proposed the concept of smart contracts in 1995 [25]. The following is a definition of a smart contract: A set of commitments (including contract participants) defined in digital form through smart contracts can achieve collaboration and trust between multiple entities in the blockchain through smart contracts, thereby expanding the scope of mutual cooperation and depth. The execution of smart contracts can be divided into three steps as follows [26]. (1) Develop smart contracts: Contract participants use programming languages to formulate the terms of the agreement, and use private keys to sign them. (2) Connect with the blockchain system: Each node of the blockchain will receive the contract, verify it and reach a consensus mechanism. (3) Execution of smart contracts: After most nodes are verified, the contract agreement will be successfully executed and contract participants will be notified. Figure 1 below shows the operation flow chart of the smart contract.

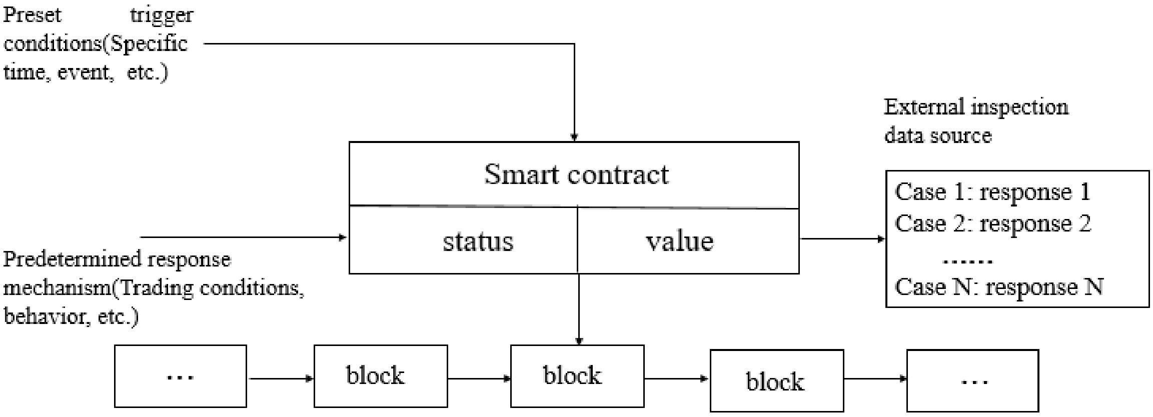

Preset trigger conditions(Specific time, event, etc.)
External inspection data source
Smart contract
status
value
Case 1: response 1
Case 2: response 2
......
Case N: response N
Predetermined response mechanism(Trading conditions, behavior, etc.)
...
block
block
block
...

Figure 1. Smart contract operation mechanism.

The blockchain combined with smart contract technology can realize the verifiability of data, files, and contract records. By calling the smart contract, the user can use the wallet address (owner account) of the deployed contract, or according to the written smart contract conditions, other wallet addresses can also call the smart contract.

2.3. ERC-20

ERC(Ethereum Request for Comments)-20 was written by Fabian Vogelsteller and Buterin in 2015 [27]. It is a protocol standard for smart contracts on the Ethereum blockchain. It is written in Ethereum's solidity language and is currently the most widely used Ethereum token in the mainstream. Specifications and standards include virtual currencies in the blockchain, such as Maker, OmiseGO, and Basic Attention tokens.

3. Method

3.1. System Architecture

This research uses blockchain technology to build a new online will system, by building a private Ethereum chain and writing smart contracts through solidity to achieve a privacy-protected and unmodifiable online will system. Figure 2 shows the structure of the will system, which is mainly used for the validity of the will proposed by the applicant and how the testator will execute the will after his death. The will certificate can be verified at any time through the validity of the blockchain to realize the anti-counterfeiting effect of the will certificate. The participating roles of the system include the Blockchain Center (BCC), Applicant (A), Family (F), Court (C), and Hospital (H).

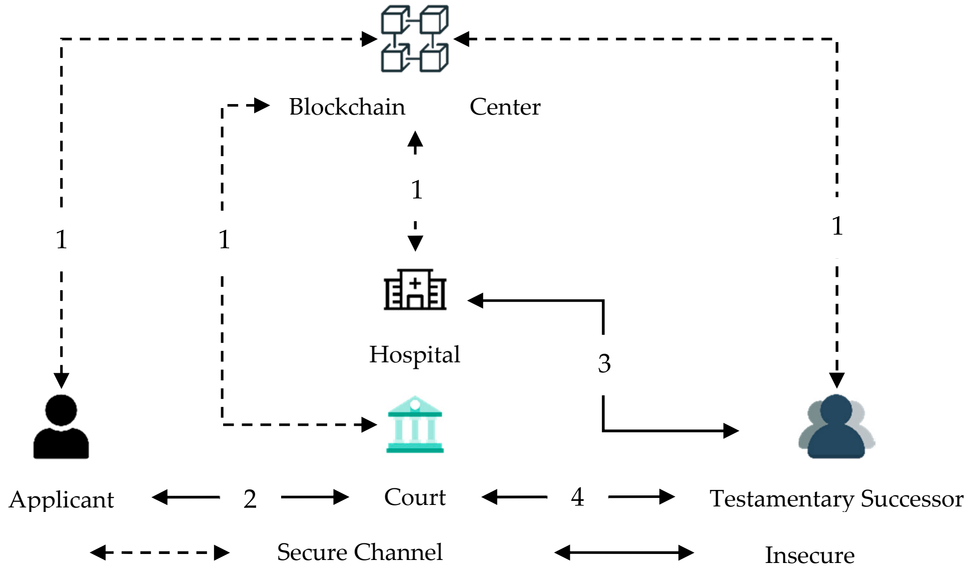


Figure 2. The structure of the will system.

The system architecture includes five main roles, namely:

1. Applicant (A): Pre-written testator.
2. Court (C): Accepts the registration of applicants for wills and applications for wills arbitration. This represents the review and arbitration department for will applications.
3. Hospital (H): The hospital that issued the death certificate when the person who made the will dies.
4. Testamentary Successor (TS): This is the owner of the inheritance will after the testator dies, for example, the testator's family.
5. Blockchain Center (BCC): According to the instructions of the will, a smart contract is issued and executed.

Step1. Each role in the system needs to register with the blockchain center before using the system and fill in relevant information on the registration webpage as needed, such as personal data, passwords, and Ethereum accounts. When making a will, the system will also verify whether the user's information is correct. If the format is incorrect, the front platform will return a corresponding error message. Finally, when each role transmits sensitive data to the blockchain center, it will use the Transport Layer Security (TLS) protocol to encrypt the data in transmission. After successful registration, the applicant will obtain the public and private signature key pair for the ECDSA.

Step2. Before the applicant makes a will, he/she will first download the will template for the court to fill out. The will template contains the applicant's sensitive personal information and the inheritance and distribution of the property. After the applicant fills in the contents of the will, the will content will be sent to the court for review. After the court receives the applicant's will information, it commences the stage of uploading the will. The court will review the contents of the applicant's will. After the review is passed, the private key of the court will be used to sign the content of the will with the ECDSA and it will be uploaded to the blockchain center.

Step3. When the applicant of a will dies, the testamentary heir should provide the hospital with relevant information about the applicant before applying for a death certificate.

When the hospital receives information from the testamentary heir, it will begin to review whether the information provided is correct. If it is correct, the content of the death certificate will be published and uploaded to the blockchain center. At this time, procedures related to the content of the will will be executed accordingly and the process will enter the stage of property distribution of the will.

Step4. The testamentary heir brings the death certificate to the court to apply for the contents of the will. When the court receives an application from the family of the testamentary heir, the court will judge whether the information provided by the family of the testamentary heir is correct. If it is correct, the will content will be downloaded from the blockchain center, so the will has a legal effect. If the testamentary successor has questions about the distribution of the property, he/she can also apply to the court for arbitration. The court will review the content of the testamentary heir's application. If the content of the application is correct, the result of the arbitration shall be determined.

3.2. Notations

Table 1 shows the definition of symbols used in this study as follows:

Table 1. Notations.

Symbol	**Description**
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	*X's* identity
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(Elliptic Curve Digital Signature Algorithm) signature message of *X*
ID_{BCi}	The index value of blockchain message
BC_X	Blockchain message of *X*
M_{will}	The plain text of the will
M_{Arg}	Arbitration dispute message content
M_{ArgID}	Identity information of an applicant for arbitration
M_{Argpay}	The message of the arbitrator's estate distribution
TS_X	Timestamp message of *X*
$h(.)$	Hash function
C_X	The ciphertext of role *X*
$E_{pukX}(M)$	Use X's public key Puk_X to encrypt message *M*
$D_{prkX}(M)$	Use X's private key Prk_X to decrypt message *M*
$A \overset{?}{=} B$	Verify whether A is equal to B

3.3. Initialization Phase

In the proposed scheme of the initial phase, this research study uses Ethereum blockchain technology. During the transaction, some key messages will be stored and verified through the blockchain center. The key information of these blockchains will be defined in smart contracts. Algorithm 1 and Algorithm 2 are the blockchain smart contract structure for the proposed scheme. The following key information will be stored in the blockchain:

Algorithm 1. Smart contract WillContent of the proposed scheme.

```
struct smart contract WillContent {
  string ap_name;
  address ap_account;
  Gender ap_gender;
  string ap_idNumber;
  string ap_createDate;
  Successor[] successor;
}

struct smart contract Successor {
  string ts_address;
  string ts_pay;
  string remarks;
}
```

Algorithm 2. Smart contract Death of the proposed scheme.

```
struct Death {
    address doctor_account;
    string hospital_name;
    string doctor_name;
    DeathType death_type;
    string de_name;
    string de_idNumber;
    Gender de_gender;
    string de_datetime;
    string de_remarks;
}
```

(1) In the structure of the will message, sensitive information about the identity of the testator, a list of heirs and distributions, and other types of information are recorded.

(2) In the structure of the death certificate, sensitive information about the identity of the deceased, the department that issued the death certificate, the date of death, and the attributes of the death are recorded.

3.4. Registration Phase

At this stage, when the system is used for the first time, all participants (such as the blockchain center, applicants, family members, courts, and hospitals) must be registered in the blockchain center. The roles of all parties on the registration page of the Blockchain Center are specified and the registration information is filled in in the correct format. After completing the registration information, the registration information filled in by the role to the Blockchain Center (BCC) is sent in order to apply for registration through Transport Layer Security (TLS) and the public and private keys of the elliptic curve digital signature algorithm (ECDSA) are obtained. Figure 3 below is a flowchart of the communication protocol during the registration phase.

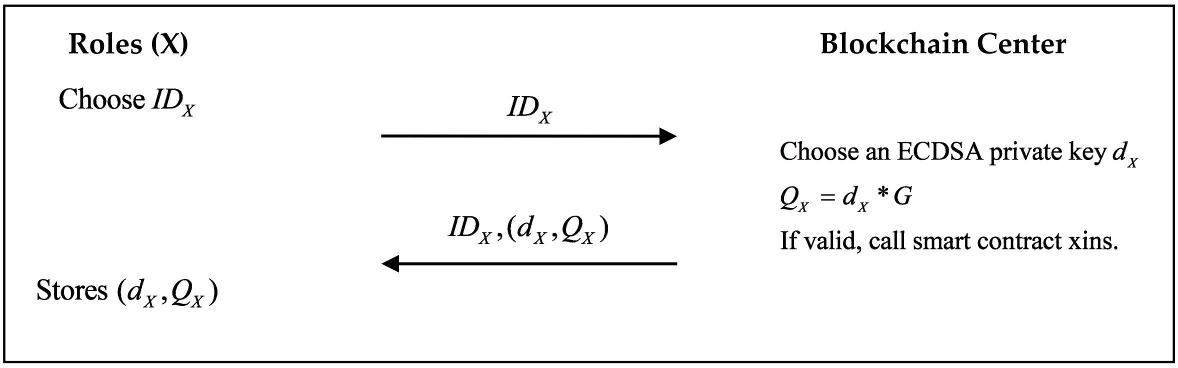


Figure 3. Flow chart of the registration phase.

Step1. Role X generates an identity ID_X, and sends it to the blockchain center.

Step2. The blockchain center generates an ECDSA private key dx based on the role X, calculates Q_X=d_X*G. If the identity of the registered role is verified as being correct, the smart contract xIns will be triggered, the content of which is the Algorithm 3 as follows:

Algorithm 3. Smart contract xIns of the proposed scheme.

```
function insert x smart contract xIns (
string x id, string x detail) {
      count ++;
x id.count = id;
x detail.count = detail;
}
string x keypairs;
```

Then the blockchain center will transmit ID_X, (d_X, Q_X) to role X.

Step3. The role X will store the key (d_X, Q_X).

3.5. Will Editing Phase

In the will editing phase, the applicant must visit the court's website and download the will template to edit the will. After the applicant has filled in the template, the will content will be sent to the court for review. Since personal wills are sensitive information, the will content will be encrypted before being sent to the court. After the court receives the will, it will first verify the identity to ensure that the source of the will is correct. If it is correct, it will review the contents of the will and upload the applicant's will to the blockchain center. Figure 4 below is a flow chart of the editing will phase.

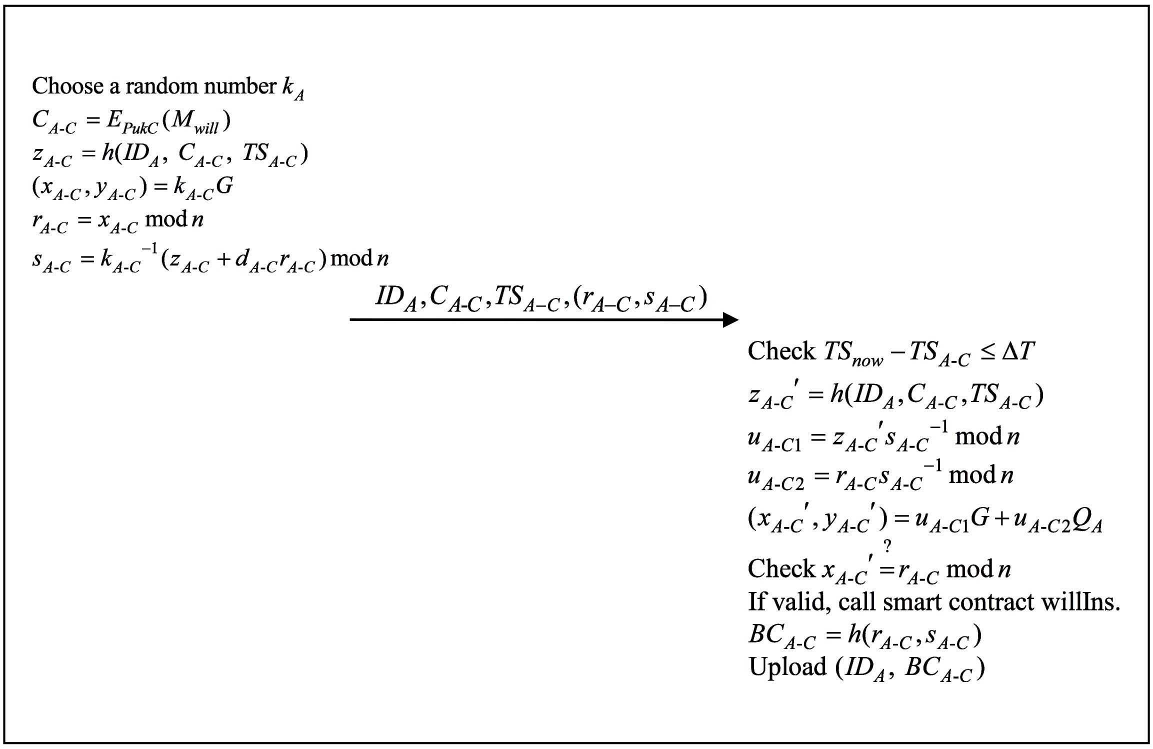

Choose a random number k_A
$C_{A\text{-}C} = E_{PukC}(M_{will})$
$z_{A\text{-}C} = h(ID_A,\ C_{A\text{-}C},\ TS_{A\text{-}C})$
$(x_{A\text{-}C}, y_{A\text{-}C}) = k_{A\text{-}C}G$
$r_{A\text{-}C} = x_{A\text{-}C} \bmod n$
$s_{A\text{-}C} = k_{A\text{-}C}^{-1}(z_{A\text{-}C} + d_{A\text{-}C}r_{A\text{-}C}) \bmod n$
$ID_A, C_{A\text{-}C}, TS_{A\text{-}C}, (r_{A-C}, s_{A-C})$
Check $TS_{now} - TS_{A\text{-}C} \le \Delta T$
$z_{A\text{-}C}' = h(ID_A, C_{A\text{-}C}, TS_{A\text{-}C})$
$u_{A\text{-}C1} = z_{A\text{-}C}' s_{A\text{-}C}^{-1} \bmod n$
$u_{A\text{-}C2} = r_{A\text{-}C}s_{A\text{-}C}^{-1} \bmod n$
$(x_{A\text{-}C}', y_{A\text{-}C}') = u_{A\text{-}C1}G + u_{A\text{-}C2}Q_A$
Check $x_{A\text{-}C}' \overset{?}{=} r_{A\text{-}C} \bmod n$
If valid, call smart contract willIns.
$BC_{A\text{-}C} = h(r_{A\text{-}C}, s_{A\text{-}C})$
Upload $(ID_A,\ BC_{A\text{-}C})$

Figure 4. Communication flow chart of the editing will phase.

Step1. The applicant first downloads the will from the court website and then fills in the contents of the will. After the applicant fills in the content of the will, the applicant will generate a random value k_{A-C} and use the court's public key Puk_C to encrypt the content of the will. The signature will be calculated $C_{A-C} = E_{PukC}(M_{will})$, $z_{A-C} = h(ID_A,\ C_{A-C},\ TS_{A-C})$, $(x_{A-C}, y_{A-C}) = k_{A-C}G$, $r_{A-C} = x_{A-C}\text{mod}n$, $s_{A-C} = k_{A-C}{}^{-1}(z_{A-C} + d_{A-C}r_{A-C})\text{mod}n$, and then $ID_A, C_{A-C}, TS_{A-C}, (r_{A-C}, s_{A-C})$ is sent to the court.

Step2. The court first uses $TS_{now} - TS_{A-C} \le \Delta T$ to check whether the timestamp is valid. Then, the correctness of the ECDSA signature is verified and the following is calculated: $z_{A-C}{}' = h(ID_A, C_{A-C}, TS_{A-C})$, $u_{A-C1} = z_{A-C}{}' s_{A-C}{}^{-1}\text{mod}n$, $u_{A-C2} = r_{A-C}s_{A-C}{}^{-1}\text{mod}n$, $(x_{A-C}{}', y_{A-C}{}') = u_{A-C1}G + u_{A-C2}Q_A$, $x_{A-C}{}' \overset{?}{=} r_{A-C}\text{mod}n$. If the verification is recognized, and the signature obtained by the representative is correct, the court will obtain information related to the will and trigger the smart contract will. the content of which is the Algorithm 4 as follows:

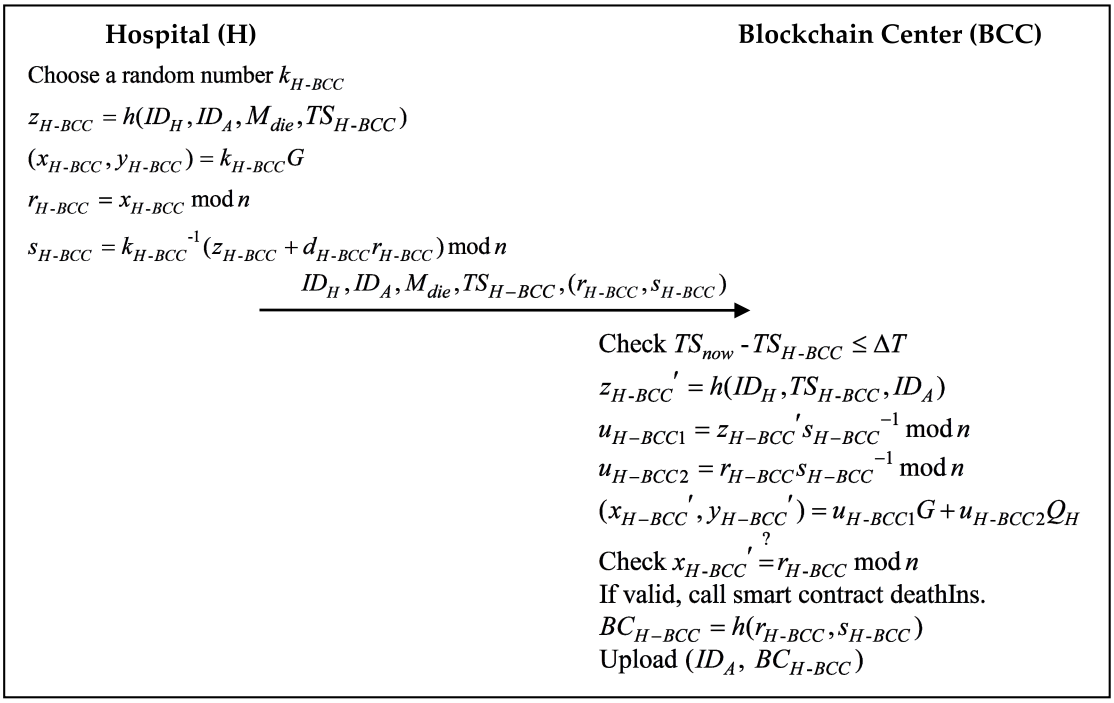
Algorithm 4. Smart contract willIns of the proposed scheme.

```
function insert smart contract willIns (
string ap_name, address ap_account, Gender
ap_gender, string ap_idNumber, string
ap_createDate, Successor[] successor;
) {
    WillContent.ap_name = ap_name;
    WillContent.ap_account = ap_account;
    WillContent.ap_gender = ap_gender;
    WillContent.ap_idNumber = ap_idNumber;
    WillContent.ap_createDate = ap_createDate;
    WillContent.successor = successor;
}
```

The court calculates $BC_{A-C} = h(r_{A-C}, s_{A-C})$ and uploads $(ID_A,\ BC_{A-C})$ to the blockchain center.

3.6. Death Certificate Issuing Phase

During the death certificate issuing phase, the testamentary successor applies to the hospital for the death certificate, and the testamentary successor provides the hospital with relevant information about the applicant. After the hospital receives the application message and confirms that the relevant information is correct, the hospital will issue a death certificate based on the application information provided by the probate successor. Since the death certificate contains sensitive information, personally sensitive information will be encrypted and sent to the blockchain center. Figure 5 shows a flowchart of the death certificate issuing phase.



Hospital (H)
Blockchain Center (BCC)
Choose a random number $k_{H\text{-}BCC}$
$z_{H\text{-}BCC} = h(ID_H, ID_A, M_{die}, TS_{H\text{-}BCC})$
$(x_{H\text{-}BCC}, y_{H\text{-}BCC}) = k_{H\text{-}BCC}G$
$r_{H\text{-}BCC} = x_{H\text{-}BCC} \bmod n$
$s_{H\text{-}BCC} = k_{H\text{-}BCC}^{-1}(z_{H\text{-}BCC} + d_{H\text{-}BCC}r_{H\text{-}BCC}) \bmod n$
$ID_H, ID_A, M_{die}, TS_{H-BCC}, (r_{H\text{-}BCC}, s_{H\text{-}BCC})$
Check $TS_{now} - TS_{H\text{-}BCC} \le \Delta T$
$z_{H\text{-}BCC}' = h(ID_H, TS_{H\text{-}BCC}, ID_A)$
$u_{H-BCC1} = z_{H-BCC}' s_{H-BCC}^{-1} \bmod n$
$u_{H-BCC2} = r_{H-BCC} s_{H-BCC}^{-1} \bmod n$
$(x_{H-BCC}', y_{H-BCC}') = u_{H\text{-}BCC1}G + u_{H\text{-}BCC2}Q_H$
Check $x_{H\text{-}BCC}' \overset{?}{=} r_{H\text{-}BCC} \bmod n$
If valid, call smart contract deathIns.
$BC_{H-BCC} = h(r_{H\text{-}BCC}, s_{H\text{-}BCC})$
Upload $(ID_A,\ BC_{H\text{-}BCC})$

Figure 5. Flow chart of the death certificate issuing phase.

Step1. The testamentary heir submits an application for a death certificate to the hospital. When the hospital receives the testamentary heir's application, the hospital generates a random value $k_{H\text{-}BCC}$, executes the signature calculation $z_{H-BCC} = h(ID_H, ID_A, M_{die}, TS_{H-BCC})$, $(x_{H-BCC}, y_{H-BCC}) = k_{H-BCC}G$, $r_{H-BCC} = x_{H-BCC}$ mod$n$, $s_{H-BCC} = k_{H-BCC}^{-1}(z_{H-BCC} + d_{H-BCC}r_{H-BCC})modn$, and then sends $ID_H, ID_A, M_{die}, TS_{H-BCC}, (r_{H-BCC}, s_{H-BCC})$ to the blockchain center.

Step2. The blockchain center (BCC) first uses $TS_{now} - TS_{H-BCC} \le \Delta T$ to check whether the timestamp is valid, then it verifies the correctness of the ECDSA signature, and calculates $z_{H-BCC}' = h(ID_H, TS_{H-BCC}, ID_A)$, $u_{H-BCC1} = z_{H-BCC}' s_{H-BCC}^{-1}modn$, $u_{H-BCC2} = r_{H-BCC}s_{H-BCC}^{-1}modn$, $(x_{H-BCC}', y_{H-BCC}') = u_{H-BCC1}G + u_{H-BCC2}$ Q_H, $x_{H-BCC}' \overset{?}{=} r_{H-BCC}$, and if it passes the verification, it means that the obtained signature is correct and triggers the smart contract deaths. the content of which is the Algorithm 5 as follows:

Algorithm 5. Smart contract willIns of the proposed scheme.

```
function insert smart contract deathIns(
address doctor_account, string hospital_name, string
doctor_name, DeathType death_type, string
de_name, string de_idNumber, Gender de_gender,
string de_datetime, string de_remarks) {
        Death.doctor_account = doctor_account;
        Death.hospital_name = hospital_name;
        Death.doctor_name = doctor_name;
        Death.death_type = death_type;
        Death.de_name = de_name;
        Death.de_idNumber = de_idNumber;
        Death.de_gender = de_gender;
        Death.de_datetime = de_datetime;
        Death.de_remarks = de_remarks;
}
```

The blockchain center calculates and uploads $BC_{H-BCC} = h(r_{H-BCC}, s_{H-BCC})$ to the blockchain, and uploads $(ID_A,\ BC_{H-BCC})$ to the blockchain center.

3.7. Will Assets Distributing Phase

In the will assets distributing phase, after the hospital issues the death certificate, the smart contract will be triggered at this time, and the will assets distribution action will be executed according to the content of the testator's will. Figure 6 demonstrates a flowchart of the will assets distributing phase.

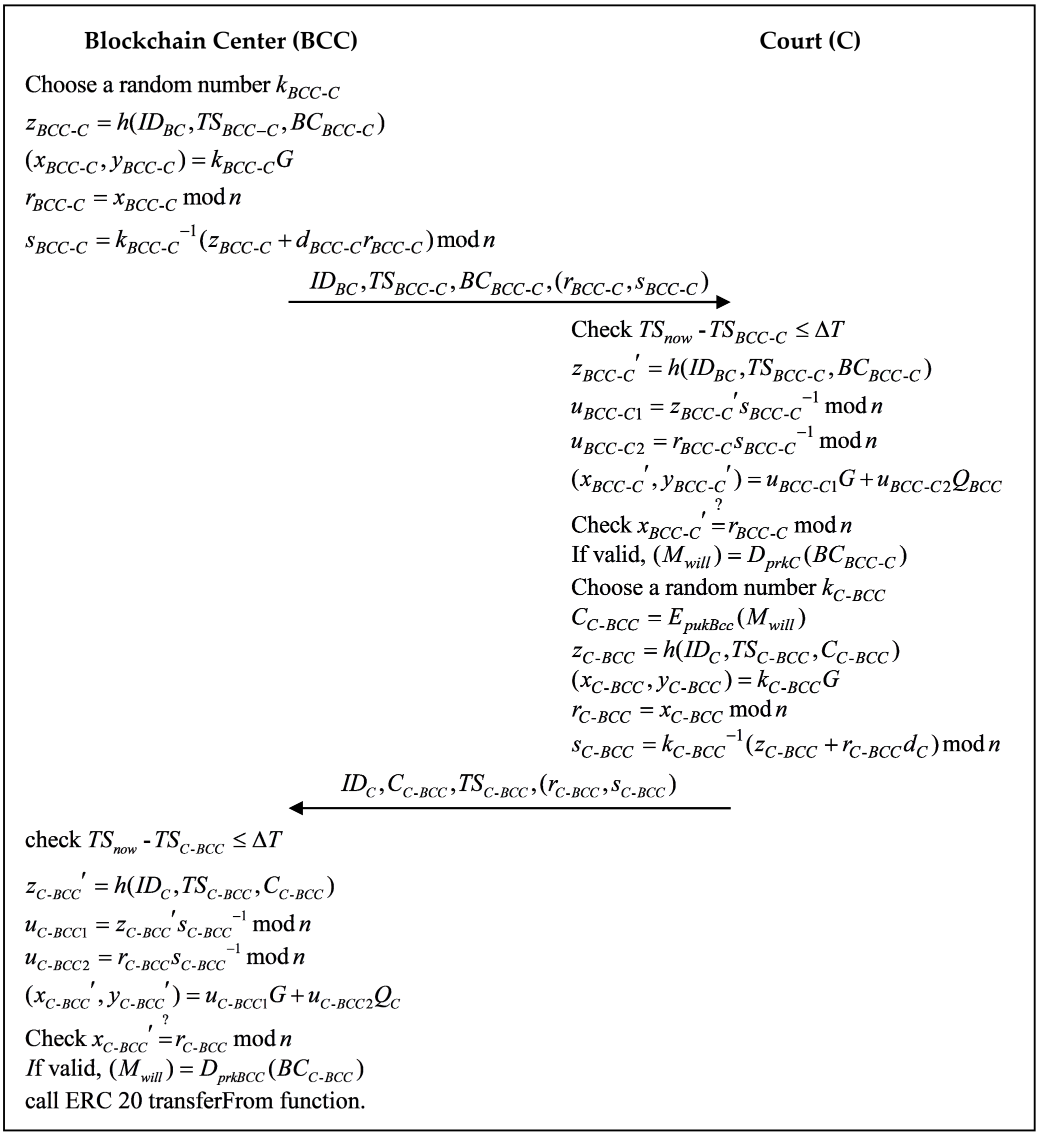

Blockchain Center (BCC)
Court (C)
Choose a random number $k_{BCC\text{-}C}$
$z_{BCC\text{-}C} = h(ID_{BC}, TS_{BCC-C}, BC_{BCC\text{-}C})$
$(x_{BCC\text{-}C}, y_{BCC\text{-}C}) = k_{BCC\text{-}C}G$
$r_{BCC\text{-}C} = x_{BCC\text{-}C} \bmod n$
$s_{BCC\text{-}C} = k_{BCC\text{-}C}^{-1}(z_{BCC\text{-}C} + d_{BCC\text{-}C}r_{BCC\text{-}C}) \bmod n$
$ID_{BC}, TS_{BCC\text{-}C}, BC_{BCC\text{-}C}, (r_{BCC\text{-}C}, s_{BCC\text{-}C})$
Check $TS_{now} - TS_{BCC\text{-}C} \le \Delta T$
$z_{BCC\text{-}C}' = h(ID_{BC}, TS_{BCC\text{-}C}, BC_{BCC\text{-}C})$
$u_{BCC\text{-}C1} = z_{BCC\text{-}C}' s_{BCC\text{-}C}^{-1} \bmod n$
$u_{BCC\text{-}C2} = r_{BCC\text{-}C} s_{BCC\text{-}C}^{-1} \bmod n$
$(x_{BCC\text{-}C}', y_{BCC\text{-}C}') = u_{BCC\text{-}C1}G + u_{BCC\text{-}C2}Q_{BCC}$
Check $x_{BCC\text{-}C}' \overset{?}{=} r_{BCC\text{-}C} \bmod n$
If valid, $(M_{will}) = D_{prkC}(BC_{BCC\text{-}C})$
Choose a random number $k_{C\text{-}BCC}$
$C_{C\text{-}BCC} = E_{pukBcc}(M_{will})$
$z_{C\text{-}BCC} = h(ID_C, TS_{C\text{-}BCC}, C_{C\text{-}BCC})$
$(x_{C\text{-}BCC}, y_{C\text{-}BCC}) = k_{C\text{-}BCC}G$
$r_{C\text{-}BCC} = x_{C\text{-}BCC} \bmod n$
$s_{C\text{-}BCC} = k_{C\text{-}BCC}^{-1}(z_{C\text{-}BCC} + r_{C\text{-}BCC}d_C) \bmod n$
$ID_C, C_{C\text{-}BCC}, TS_{C\text{-}BCC}, (r_{C\text{-}BCC}, s_{C\text{-}BCC})$
check $TS_{now} - TS_{C\text{-}BCC} \le \Delta T$
$z_{C\text{-}BCC}' = h(ID_C, TS_{C\text{-}BCC}, C_{C\text{-}BCC})$
$u_{C\text{-}BCC1} = z_{C\text{-}BCC}' s_{C\text{-}BCC}^{-1} \bmod n$
$u_{C\text{-}BCC2} = r_{C\text{-}BCC} s_{C\text{-}BCC}^{-1} \bmod n$
$(x_{C\text{-}BCC}', y_{C\text{-}BCC}') = u_{C\text{-}BCC1}G + u_{C\text{-}BCC2}Q_C$
Check $x_{C\text{-}BCC}' \overset{?}{=} r_{C\text{-}BCC} \bmod n$
If valid, $(M_{will}) = D_{prkBCC}(BC_{C\text{-}BCC})$
call ERC 20 transferFrom function.

Figure 6. Flowchart of the will assets distributing phase.

Step1. After the hospital issues the death certificate and uploads it to the blockchain center, it enters the testamentary property distribution process, then, the blockchain center generates a random value $k_{BCC\text{-}C}$, executes the signature to calculate $z_{BCC-C} = h(ID_{BC}, TS_{BCC-C}, BC_{BCC-C})$, $(x_{BCC-C}, y_{BCC-C}) = k_{BCC-C}G$, $r_{BCC-C} = x_{BCC-C}$ mod$n$, $s_{BCC-C} = k_{BCC-C}{}^{-1}(z_{BCC-C} + d_{BCC-C}r_{BCC-C})modn$, and then sends ID_{BC}, $TS_{BCC-C}, BC_{BCC-C}, (r_{BCC-C}, s_{BCC-C})$ to the court.

Step2. After the court receives the message from the blockchain center, it will first use $TS_{now} - TS_{BCC-C} \leq \Delta T$ to check whether the timestamp is valid, then verify the correctness of the ECDSA signature, and calculate $z_{BCC-C}{}' = h(ID_{BC}, TS_{BCC-C}, BC_{BCC-C})$, $u_{BCC-C1} = z_{BCC-C}{}'s_{BCC-C}{}^{-1}modn$, $u_{BCC-C2} = r_{BCC-C}s_{BCC-C}{}^{-1}modn$, $(x_{BCC-C}{}', y_{BCC-C}{}') = u_{BCC-C1}G + u_{BCC-C2}Q_{BCC}$. If the verification is recognized, and the signature is correct, the court will use $Dprk_C$ to decrypt the contents of the will. The court generates a random value $k_{C\text{-}BCC}$, executes the signature calculation $C_{C-BCC} = E_{pukBcc}(M_{will})$, $z_{C-BCC} = h(ID_C, TS_{C-BCC}, C_{C-BCC})$, $(x_{C-BCC}, y_{C-BCC}) = k_{C-BCC}G$, $r_{C-BCC} = x_{C-BCC}$mod$n$, $s_{C-BCC} = k_{C-BCC}{}^{-1}(z_{C-BCC} + r_{C-BCC}d_C)modn$, and then transmits $ID_C, C_{C-BCC}, TS_{C-BCC}, (r_{C-BCC}, s_{C-BCC})$ to the blockchain center.

Step3. When the blockchain center receives a message from the court, it will first use $TS_{now} - TS_{C-BCC} \leq \Delta T$ to check whether the timestamp is valid, then verify the correctness of the ECDSA signature and calculate $z_{C-BCC}{}' = h(ID_C, TS_{C-BCC}, C_{C-BCC})$, $u_{C-BCC1} = z_{C-BCC}{}'s_{C-BCC}{}^{-1}modn$, $u_{C-BCC2} = r_{C-BCC}s_{C-BCC}{}^{-1}modn$, $(x_{C-BCC}{}', y_{C-BCC}{}') = u_{C-BCC1}G + u_{C-BCC2}Q_C$. If the verification is recognized, it is confirmed that the signature is correct. Then, the blockchain center will use the private key to decrypt the encrypted content $(M_{will}) = D_{prkBCC}(BC_{C-BCC})$, read the successor list in the will, refer to the contract content proposed in the initialization phase, find the ts_address and ts_pay data from the contract, and then use the Ethereum ERC20 protocol [23], and Call the transferFrom function to execute the asset transfer process. The Algorithm 6 is the content of transferFrom.

Algorithm 6. Smart contract transferFrom of the ERC20 protocol.

```
function transferFrom(address _from, address _to,
uint256 _amount) returns (bool success) {
if (balances[_from] >= _amount &&
allowed[_from][msg.sender] >= _amount &&
_amount > 0 && balances[_to] + _amount >
balances[_to]
) {
        balances[_from] -= _amount;
         balances[_to] += _amount;
         Transfer(_from, _to, _amount);
          return true;
       } else {
          return false;
        }
    }
```

This function will first check whether the sender's balance is greater than or equal to the specified amount, and then check that the specified transfer amount does not exceed the previously set transfer limit. If all the conditions are met, the corresponding amount will be transferred from the applicant's wallet. The property amount is transferred to the designated account, and finally, the transaction message will be published and recorded on the block.

3.8. Arbitration Phase

During the arbitration phase, when the testamentary heirs object to the distribution of the testamentary property, the testamentary heirs will provide the court with $ID_{TS}, ID_A, ID_{BCwill}, ID_{BCdie}, M_{Arg}$ information. The court will use the application information provided by the testamentary heir and compare the blockchain data to confirm the validity of the will, the identity of the testamentary heir, death certificate, and property distribution. The flow of the arbitration phase is shown in Figure 7.

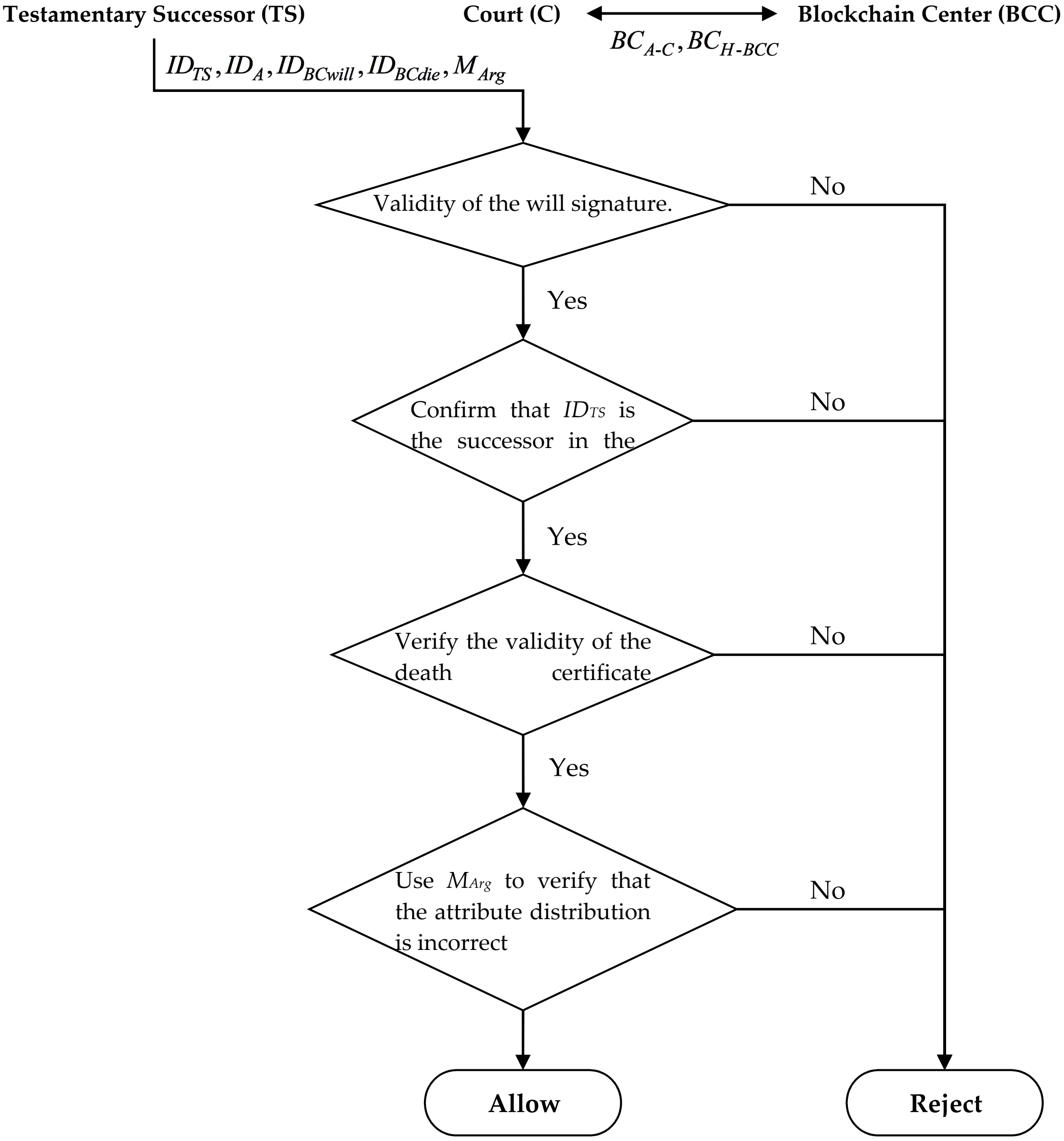

Testamentary Successor (TS)
Court (C)
Blockchain Center (BCC)
$BC_{A\text{-}C}, BC_{H\text{-}BCC}$
$ID_{TS}, ID_A, ID_{BCwill}, ID_{BCdie}, M_{Arg}$
Validity of the will signature.
No
Yes
Confirm that ID_{TS} is the successor in the
No
Yes
Verify the validity of the death certificate
No
Yes
Use M_{Arg} to verify that the attribute distribution is incorrect
No
Allow
Reject

Figure 7. Flow chart of the arbitration phase.

Step1. The testamentary heir applies to the court for arbitration and sends a message $ID_{TS}, ID_A, ID_{BCwill}, ID_{BCdie}, M_{Arg}$ to the court. After the court receives it, it enters the arbitration procedure. The court uses ID_A to obtain the testator's signature (r_{A-C}, s_{A-C}) and uses ID_{BCwill} to retrieve the blockchain data BC_{A-C} of the testator's will and verify the blockchain data $BC_{A-C} \overset{?}{=} h(r_{A-C}, s_{A-C})$. If the verification fails, the court will reject the arbitration application.

Step2. After the court verifies the validity of the will signature, the court checks the content BC_{A-C} of the will blockchain data and compares ID_{TS} with the ts_address data in the testament succession list to confirm if the identity of the testamentary heir is inherited by the testator $ID_{TS} \overset{?}{=} ts\_address$. If the verification fails, the court will reject the arbitration application.

Step3. After the court verifies the validity of the testamentary successor, the court uses ID_A to obtain the testator's signature (r_{A-C}, s_{A-C}) and uses ID_{BCwill} to retrieve the death certificate blockchain data BB, and verify the death certificate blockchain signature data $BC_{H-BCC} \overset{?}{=} h(r_{H-BCC}, s_{H-BCC})$. If it fails, the court will reject the arbitration application.

Step4. If the court verifies the validity of the death certificate, the court will use the will blockchain data BC_{A-C} obtained in the second step, and then compare M_{Arg} these with the information in the inheritance list in the will. The M_{Arg} message contains the address M_{ArgID} of the testamentary heir and property M_{Argpay} currently allocated to the testamentary heir. The court will then check the successor list from the BC_{A-C}. The heir list will refer to the contract content proposed in the initialization phase, and merge the ts_pay and M_{Arg} into the heir list. It will compare the amount of property currently allocated by the probate heir to check whether the property allocation is incorrect $M_{Argpay} \overset{?}{=} ts\_pay$. If the verification fails, the court will reject the arbitration application. If the verification is successful, it means that the blockchain data have been fully verified and the arbitration application of the testamentary heir has also been established.

Step5. When the testamentary heir receives the messages that the arbitration has been established, the testamentary heir can retain the results of the arbitration to execute legal procedures and redistribute the property through administrative procedures.

4. Security Analysis

4.1. Integrity

In our research, the elliptic curve digital signature algorithm (ECDSA) was used to sign the transmitted message and ensure data integrity. In the will editing phase, when the applicant sends a message to the court, the applicant will generate the ECDSA signature $(x_{A-C}, y_{A-C}) = k_{A-C}G$. After receiving the message, the court will verify the validity of the applicant's timestamp $TS_{now} - TS_{A-C} \le \Delta T$ and ECDSA signature $x_{A-C}' \overset{?}{=} r_{A-C} \text{mod} n$. Then, it enters the death certificate issuing phase. When the hospital wants to send a message to the blockchain center, the hospital will generate the ECDSA signature $(x_{H-BCC}, y_{H-BCC}) = k_{H-BCC}G$. The blockchain center will verify the hospital's timestamp $TS_{now} - TS_{H-BCC} \le \Delta T$ and the correctness of the ECDSA signature $x_{H-BCC}' \overset{?}{=} r_{H-BCC} \text{mod} n$. Finally, in the assets distributing phase, both the blockchain center and the court will generate its ECDSA signature $(x_{BCC-C}, y_{BCC-C}) = k_{BCC-C}G$, $(x_{C-BCC}, y_{C-BCC}) = k_{C-BCC}G$. After receiving the ECDSA signature, the hospital will verify the blockchain center's timestamp $TS_{now} - TS_{BCC-C} \le \Delta T$, $TS_{now} - TS_{C-BCC} \le \Delta T$, and the correctness of the signature $x_{BCC-C}' \overset{?}{=} r_{BCC-C} \text{mod} n$, $x_{C-BCC}' \overset{?}{=} r_{C-BCC} \text{mod} n$. Since the attacker does not know the private keys of the applicant, the court, and the hospital, even if the transmission content is tampered with, the correct ECDSA signature (x_{A-C}, y_{A-C}), (x_{H-BCC}, y_{H-BCC}), (x_{BCC-C}, y_{BCC-C}) and (x_{C-BCC}, y_{C-BCC}) will not be generated.

From the above descriptions, this study uses ECDSA signature technology to ensure the integrity of the transmitted message. If the attacker intercepts the message sent to the court and pretends to be a legitimate applicant who sent an incorrect testament message to the court. The attacker will not be able to successfully attack, because even if the attacker modifies the content of the applicant's will content sent to the court, the attacker cannot use the applicant's private key to sign the ECDSA. After receiving the messages, the court will immediately check the integrity of the received data. The court will find that the message content does not match the signature, and the attacker's attack will fail.

4.2. Public Verifiability

This research uses the ECDSA digital signature mechanism, combined with blockchain technology to design an electronic will system with smart contracts based on the blockchain mechanism, which has the characteristics of public verification. All messages must be verified before uploading, and the correctness of the messages will be verified during the process of sending and receiving messages. Next, take the message sent by the applicant and the court as an example. When the applicant sends a message signed with ECDSA to the court, the court will first verify the legality of the time stamp $TS_{now} - TS_{A-C} \leq \Delta T$ and the ECDSA signature $x_{A-C}' \overset{?}{=} r_{A-C}\text{mod}n$. Then, the court will generate blockchain data $BC_{A-C} = h(r_{A-C}, s_{A-C})$, and upload the blockchain data to the blockchain center using ID_A as an index. In other words, after verifying the correctness of the timestamp and signature for each role that receives the message, it will also verify the correctness of the ECDSA signature generated by the previous role. Therefore, our proposed solution achieves publicly verifiable features by applying blockchain technology and ECDSA digital signatures.

4.3. Unforgeability

This study uses blockchain technology, which has the characteristics of being decentralized, open, anonymous, and tamperproof, and can retain the integrity of the will content. Therefore, when the applicant, heirs, and family members of the applicant have questions about the will, they can verify and compare the signature information of the will at any time to confirm the legality of the information. Since the signature is signed by the applicant using his private key, neither the court nor illegal people can use the applicant's private key to sign the ECDSA. Therefore, when the verifier checks if the signature of the will matches the actual signature of the will, if it does not match, then it can be known that the will has been forged.

4.4. Non-Repudiation

In this study, when all roles send the content message, each role uses its private key to sign and transmit the message with ECDSA, and each role has its own private key. Take the applicant and the court as examples, when sending a message signed with ECDSA to the court, the court will use the applicant's public key to verify the message. If the message is successfully verified, the court will not reject the content of the sent message. Therefore, this mechanism has undeniable characteristics. After the receiver receives the message, it will use the sender's public key to verify the message. If the message is successfully verified, the sender cannot reject the content of the sent message. Table 2 is a description of the non-repudiation of each role in this scheme.

Table 2. The non-repudiation description.

Item Phase	Signature	Sender	Receiver	Signature Verification
Will editing phase	(r_{A-C}, s_{A-C})	Applicant (A)	Court (C)	$x_{A-C}' \overset{?}{=} r_{A-C}\text{mod}n$
Death certificate issuing phase	$(r_{H-BCC},\ s_{H-BCC})$	Hospital (H)	Blockchain Center (BCC)	$x_{H-BCC}' \overset{?}{=} r_{H-BCC}\text{mod}n$
Will assets distributing phase	(r_{BCC-C}, s_{BCC-C})	Blockchain Center (BCC)	Court (C)	$x_{BCC-C}' \overset{?}{=} r_{BCC-C}\text{mod}n$
	(r_{C-BCC}, s_{C-BCC})	Court (C)	Blockchain Center (BCC)	$x_{C-BCC}' \overset{?}{=} r_{C-BCC}\text{mod}n$

4.5. Message Irreversibility

In the proposed scheme, the key message content transmitted between each role is first passed through the hash function calculation and the time stamp mechanism before being chained to achieve the characteristic of message irreversibility. The information after the hash function operation is as follows:

$$
\begin{gathered}
z_{A-C} = h(ID_A,\ C_{A-C},\ TS_{A-C}) \\
z_{H-BCC} = h(ID_H, ID_A, M_{die}, TS_{H-BCC}) \\
z_{BCC-C} = h(ID_{BC}, TS_{BCC-C}, BC_{BCC-C}) \\
z_{C-BCC} = h(ID_C, TS_{C-BCC}, C_{C-BCC})
\end{gathered}
$$

Because the attacker cannot reverse the content of the original message, the message is irreversible.

4.6. Resist Counterfeiting Attacks

Attackers can fake the contents of a will by impersonating a legitimate applicant. To prevent such attacks, the proposed solution in this research uses ECDSA and hash functions to protect sensitive messages. Next, take the editing phase of a will as an example. When the applicant sends a message with an ECDSA signature to the court, the court will first verify the legality of the timestamp $TS_{now} - TS_{A-C} \leq \Delta T$ and the correctness of the ECDSA signature $x_{A-C}{}' \overset{?}{=} r_{A-C} \text{mod} n$. The ECDSA signature is signed by the applicant using his/her private key. Neither other legal roles nor illegal personnel can use the applicant's private key to sign on the ECDSA. When the court checks the ECDSA signature of the will does not match the actual signature of the will, the court will know that the will is forged. Therefore, this solution can safely prevent counterfeiting attacks.

4.7. Tamperproof

This research uses blockchain technology, which is a chain formed by linear connections of blocks. The transaction records of all parties on our system will be stored in the corresponding blockchain. For example, after confirming the correctness of the time stamp $TS_{now} - TS_{A-C} \leq \Delta T$, $TS_{now} - TS_{H-BCC} \leq \Delta T$ and the ECDSA signature $x_{A-C}{}' \overset{?}{=} r_{A-C}$, $TS_{now} - TS_{H-BCC} \leq \Delta T$, the contents of the will and death certificate will be written into this block. Due to the immutability of blockchain technology, once a block record is generated and uploaded to the chain, it cannot be tampered with, because other blockchain verifiers will not recognize the modified information, as long as the block data have been modified, the block hash value will fail to verify. Therefore, the proposed scheme realizes that the will cannot be tampered with.

4.8. System Decentralization

Since traditional applications and network platforms have servers and databases dedicated to processing and storing data and defining how the code should be executed, all data records are subjected to the official server and database constraints. However, if the official server is closed due to abnormalities or if a hacker invades and tampers with the data, then the data will be damaged. Therefore, this research adopts blockchain technology with decentralized characteristics. It is a decentralized data storage space on the blockchain. Therefore, no one has the opportunity to tamper with the data in the block. It will avoid stopping operations due to unexpected failures.

4.9. Fair Arbitration

As demonstrated in the arbitration process shown in Figure 7, this study designed a set of arbitration mechanisms. If there is a dispute over the distribution of property, the testamentary heirs can apply to the court for arbitration and provide the court with information, such as $ID_{TS}, ID_{A}, ID_{BCwill}, ID_{BCdie}, M_{Arg}$. The court will use the arbitration information provided by the probate heir to obtain block information from the blockchain center for review. After the review, the testamentary heirs will be notified of the result of the arbitration, and the testamentary heirs can initiate legal proceedings based on the result of the arbitration to redistribute the property. Therefore, the proposed scheme can ensure that the testamentary heirs will not suffer unfair arbitration.

5. Discussion

5.1. Calculation Cost Analysis

Table 3 shows the calculation cost analysis and function of each stage in our proposed plan.

Table 3. Analysis of the computational cost.

Role / Phase	BCC	A	C	H	TS
Registration phase	$1T_{Mui}$	N/A	N/A	N/A	N/A
Will editing phase	N/A	$3T_{Mui}+1T_H$ $+1T_{Cmp}+1T_{Sig}$	$4T_{Mui}+2T_H$ $+1T_{Cmp}+1T_{Sig}$	N/A	N/A
Death certificate issuing phase	$4T_{Mui}+2T_H$ $+1T_{Cmp}+1T_{Sig}$	N/A	N/A	$3T_{Mui}+1T_H$ $+1T_{Cmp}+1T_{Sig}$	N/A
Will assets distribution phase	$7T_{Mui}+2T_H$ $+1T_{Cmp}+2T_{Sig}$	N/A	$7T_{Mui}+2T_H$ $+1T_{Cmp}+2T_{Sig}$	N/A	N/A

T_{Mui}: Multiplication operation, T_{Cmp}: Comparison of operation, T_H: Hash function operation, T_{Sig}: Signature operation.

In Table 3, we analyzed the computational cost of the proposed scheme in each stage of the blockchain center, applicant, court, hospital, and testamentary successor. We found the highest computation cost in the will assets distribution phase; for example, the Blockchain Center needs seven multiplication operations, two hash function operations, one comparison operation, and two signature operations. The Court needs seven multiplication operations, two hash function operations, one comparison operation, and two signature operations. Thus, the computation cost is acceptable in our proposed system.

5.2. Total Communication Cost Analysis

Table 4 shows the communication cost analysis of the proposed scheme. In the current 3G environment, the maximum transmission speed is 14 Mbps. In a 4G environment, the maximum transmission speed is 100 Mbps. In a 5G environment, the maximum transmission speed is 20 Gbps [28]. We assume that the ECDSA key and signature are 160 bits, the hash function calculated value is 160 bits, and the remaining message length (such as ID and timestamp) is 80 bits. The cost of communication cost analysis at each phase is shown in Table 4 below:

Table 4. Communication cost analysis.

Item / Phase	Message Length	Rounds	3.5G (14 Mbps)	4G (100 Mbps)	5G (20 Gbps)
Registration phase	480 bits	2	0.034 ms	0.005 ms	0.024 us
Will editing phase	720 bits	1	0.051 ms	0.072 ms	0.036 us
Death certificate issing phase	640 bits	1	0.046 ms	0.064 ms	0.032 us
Will assets distributing phase	1280 bits	2	0.091 ms	0.128 ms	0.021 us

Take the analysis of the highest communication cost in the will assets distributing phase as an example, the effectiveness of this mechanism is higher than that of other phases, and its total communication cost is 1280 bits. It takes 0.091 ms in a 3.5G (14 Mbps) communication environment, 0.128 ms in a 4G (100 Mbps) communication environment, and 0.021 microseconds in a 5G (20 Gbps) communication environment. From the above analysis, we know that these communication costs are very low, so the proposed solution has better communication performance.

5.3. Function Comparison

Table 5 below shows a functional comparison of the proposed solutions. It can be seen from the table that although some documents using blockchain technology in the past, there are still some shortcomings.

Table 5. Functional comparison of proposed schemes.

Scheme / Feature	Chien and Lin [4]	Lee et al. [5]	Chen et al. [6]	Sreehari et al. [7]	Our Proposed Scheme
Integrity	Y	N	Y	N	Y
Public verifiability	N	N	Y	Y	Y
Unforgeability	Y	Y	Y	N	Y
Non-repudiation	N	Y	Y	N	Y
Message irreversibility	N	N	N	N	Y
Resist counterfeiting attacks	N	N	N	N	Y
Tamperproof	N	N	N	N	Y
System decentralization	N	N	N	N	Y
Fair arbitration	N	N	N	N	Y
Blockchain issues	N	N	N	Y	Y
Propose an architecture or framework	Y	Y	Y	Y	Y
Implementation of the legacy distribution mechanism	N	N	N	N	Y
Smart contract mechanism	N	N	N	N	Y

In Table 5, we can see that in the solutions proposed by Chien and Lin [4], Lee et al. [5], and Chen et al. [6], they all use a cryptographic system to encrypt the content of the electronic will, but none of these three references provide this function in terms of security, such as making the message irreversible, resistant to counterfeiting attacks, and tamperproof. In the proposed scheme by Sreehari et al. [7], although people are concerned about the blockchain issue and the concept of storing wills in the blockchain through smart contracts, the content of the document is only in the draft stage. The detailed protocol does not appear in this article. Therefore, all of our proposed schemes overcome the above shortcomings and implement a legacy distribution mechanism.

5.4. Limitations

In the proposed scheme, before using the system, all roles need to be registered with the blockchain center and have their respective data filled in. An Ethereum account and other relevant information are also required during the registration process. After successful registration, they need to obtain the public key and private key pair of the elliptic curve signature before they can use this system. Additionally, the legal effect of online wills will depend on the amendment of relevant digital signature legal provisions in various countries.

6. Conclusions

With the rapid development of the social economy, our society is gradually aging. There is an increasing number of family disputes about inheritance. A will allows the testator to decide how property will be distributed after their death in accordance with his/her wishes. It can also avoid ongoing disputes between children for the distribution of property and even avoid court appeals. Currently, traditional methods are used to produce a will, but privacy and security protection are relatively insecure. Electronic will production has a higher level of privacy and convenience. Users have their accounts and passwords, which can not only reduce costs but also improve efficiency. Through blockchain technology, the shortcomings of the existing architecture and environment can be solved.

In this research, we propose a traceable online will system based on blockchain and smart contract technology. The applicant first goes to the court to download the will document to fill in the content of the will, and then obtains the review of the court. All information about the pre-will process will be uploaded to the blockchain, and the relevant information will be signed by each role. Therefore, attackers cannot tamper with it. The legality of the data can be verified by a third party to achieve the purpose of anti-counterfeiting and to ensure the security of the will content.

The proposed scheme can meet the requirements of information security, including ensuring data integrity, and that information is irreversible, non-reproducible, and tamperproof. Through blockchain technology, not only anti-counterfeiting of the will is achieved, but also the cost is reduced and the efficiency is improved. It also incorporates smart contracts. The deployment of smart contracts needs to be done through blockchain transactions. After the deployment is completed, it cannot be changed. Therefore, the trust problem that cannot be solved by traditional wills has been completely resolved. This research also proposes an achievable arbitration mechanism solution to ensure that testamentary successors will not suffer unfair arbitration.

Author Contributions: Conceptualization, C.-L.C., C.-Y.L. and Y.-Y.D.; validation, M.-L.C., P.C. and Y.-J.C.; writing—original draft preparation, Ching-Ying, Lin, Y.-Y.D.; writing—review and editing, P.C. and Y.-J.C.; supervision, C.-L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (No.61801 413), Natural Science Foundation of Fujian Province (No.2017J05110), Young and Middle-aged Teachers Educational Scientific Research Project of Fujian Province (No. JAT160345, No.JT180437).

Institutional Review Board Statement: This study is based entirely on theoretical basic research. It does not involve humans.

Informed Consent Statement: This study is based entirely on theoretical basic research. It does not involve humans.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

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

References

1. Peter, A. Jimi Hendrix Ongoing Estate Litigation. Available online: https://medium.com/@injudiciouslex/jimi-hendrix-ongoing-estate-litigation-c16c39f81692 (accessed on 1 February 2021).
2. O'Malley Greenburg, Z. The Scandalously Boring Truth About Michael Jackson's Will. Available online: https://www.forbes.com/sites/zackomalleygreenburg/2012/08/17/the-scandalously-boring-truth-about-michael-jacksons-will/?sh=16cebb6348ed (accessed on 1 February 2021).
3. He, H.S. Family Property Distribution Disputes, Wikipedia Contributors. Available online: https://zh.wikipedia.org/w/index.php?title=%E4%BD%95%E9%B4%BB%E7%87%8A%E5%AE%B6%E6%97%8F%E5%88%86%E7%94%A2%E7%B3%BE%E7%B4%9B%E4%BA%8B%E4%BB%B6&oldid=59972272 (accessed on 1 February 2021).
4. Chien, H.Y.; Lin, R.Y. The Study of Secure E-Will System on the Internet. *J. Inf. Sci. Eng.* **2009**, *25*, 877–893.
5. Lee, K.; Won, D.; Kim, S. A practical approach to a secure e-will system in the ROC. In Proceedings of the 2010 IEEE 5th International Conference on Ubiquitous Information Technologies and Applications, Sanya, China, 16–18 December 2010; pp. 1–6.
6. Chen, C.L.; Lee, C.C.; Tseng, Y.M.; Chou, T.T. A private online system for executing wills based on a secret sharing mechanism. *Secur. Commun. Netw.* **2012**, *5*, 725–737. [CrossRef]
7. Sreehari, P.; Nandakishore, M.; Krishna, G.; Jacob, J.; Shibu, V.S. Smart will converting the legal testament into a smart contract. In Proceedings of the 2017 IEEE International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvanthapuram, India, 20–22 July 2017; pp. 203–207.
8. Ettoday, Launched the First Will App in Taiwan. Lawyer Liu Weide Spent Millions of NT Dollars to Develop and Provide Free Download. 2019. Available online: https://www.ettoday.net/news/20190403/1414747.htm (accessed on 1 February 2021).
9. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2019. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 1 February 2021).
10. Buterin, V. A next-generation smart contract and decentralized application platform. *White Paper* **2014**, *3*, 1–36.
11. Shih, T.F.; Chen, C.L.; Syu, B.Y.; Deng, Y.Y. A Cloud-Based Crime Reporting System with Identity Protection. *Symmetry* **2019**, *11*, 255. [CrossRef]
12. 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. [CrossRef]
13. HASH Coron, J.S.; Dodis, Y.; Malinaud, C.; Puniya, P. Merkle-Damgård revisited: How to construct a hash function. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 430–448.
14. Chen, C.L.; Deng, Y.Y.; Weng, W.; Zho, M.; Sun, H. A Blockchain Based Intelligent Anti-switch Package in Tracing Logistics System. *J. Supercomp.* **2021**. [CrossRef]
15. 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]

16. Li, C.T.; Shih, D.H.; Wang, C.C.; Chen, C.L.; Lee, C.C. A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System. *IEEE Access* **2020**, *8*, 173904–173917. [CrossRef]
17. Chen, C.L.; Deng, Y.Y.; Weng, W.; Sun, H.; Zho, M. A Blockchain-Based Secure Inter-Hospital EMR Sharing System. *Appl. Sci.* **2020**, *10*, 4958. [CrossRef]
18. Wang, Y.C.; Chen, C.L.; Deng, Y.Y. Authorization mechanism based on blockchain technology for protecting museum digital property rights. *Appl. Sci.* **2021**, *11*, 1085. [CrossRef]
19. Lin, C.C.; Chang, C.C.; Zheng, Y.Z. A Ring Signature Based Anonymity Authentication Scheme for Group Medical Consultation. *Symmetry* **2020**, *12*, 2009. [CrossRef]
20. Chen, C.L.; Shih, T.F.; Wang, K.H.; Chen, C.H.; Tsaur, W.J. An Investigator Unearths Illegal Behavior via a Subliminal Channel. *J. Internet Technol.* **2018**, *19*, 573–580.
21. Chen, C.L.; Liao, J.J. A fair online payment system for digital content via subliminal channel. *Electron. Commer. Res. Appl.* **2011**, *10*, 279–287. [CrossRef]
22. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
23. Kang, B.; Shao, D.; Wang, J. A fair electronic payment system for digital content using elliptic curve cryptography. *J. Algorithms Comput. Technol.* **2018**, *12*, 13–19. [CrossRef]
24. Pornin, T. Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA). *Internet Eng. Task Force RFC* **2013**, *6979*, 1–79.
25. 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 1 February 2021).
26. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transact. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
27. Vogelsteller, F.; Buterin, V. EIP-20: ERC-20 Token Standard. 2015. Available online: https://eips.ethereum.org/EIPS/eip-20 (accessed on 1 February 2021).
28. 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]