Article

Not peer-reviewed version

Research on Decentralized Digital Inheritance Management System Empowered by Blockchain and Smart Contracts: With a Discussion on the Inheritance and Destruction of Digital Assets

Rui Deng *

Posted Date: 4 June 2025

doi: 10.20944/preprints202506.0292.v1

Keywords: Digital Inheritance; Blockchain; Smart Contracts; Decentralized Application (DApp); Digital Asset Inheritance; Digital Asset Destruction; Artificial Intelligence Agent (AI Agent); Privacy Protection

 doi:10.20944/preprints202506.0292.v1

Article

Research on Decentralized Digital Inheritance Management System Empowered by Blockchain and Smart Contracts: With a Discussion on the Inheritance and Destruction of Digital Assets

Rui Deng

Independent Researcher; ruideng31@gmail.com

Abstract: With the rapid development of the digital economy, the types and value of digital assets are increasing daily, making their inheritance and destruction an urgent legal and technical problem to be solved. The lag of traditional legal frameworks in this field has led to a "digital inheritance vacuum." This paper deeply explores the application potential of blockchain and smart contract technology in constructing a decentralized digital inheritance management system. Firstly, it analyzes the practical needs and research significance of digital asset inheritance and destruction, and reviews the current status and challenges of relevant legal frameworks domestically and internationally. Secondly, it elaborates on the inherent advantages of blockchain technology in the implementation of digital wills and evaluates the applicability of different blockchain platforms. The core functional design of smart contracts in digital wills is a key research focus, including liveness detection, multi-signature, conditional execution, and innovative asset classification processing and destruction strategies, with a special discussion on the feasibility and research direction of introducing Artificial Intelligence Agents (AI Agents) to assist in complex destruction tasks. Furthermore, a decentralized digital inheritance management DApp architecture is proposed, including a blockchain underlying layer, a middleware layer (containing oracles, encryption and key management, DID systems), and an application layer. The paper analyzes the key technical challenges faced by this system, such as private key management, data privacy, oracle problems, cross-chain interoperability, and legal regulatory conflicts, and proposes corresponding solutions. Finally, it discusses ways to ensure the legal validity of blockchain-based digital wills, provides suggestions for China's implementation path in this field by combining international practical cases, and looks forward to future development trends. This research aims to provide a theoretical basis and practical reference for building a secure, transparent, efficient, and automated digital inheritance management system.

Keywords: digital inheritance; blockchain; smart contracts; decentralized application (DApp); digital asset inheritance; digital asset destruction; artificial intelligence agent (AI Agent); privacy protection

I. Research Background and Significance

With the vigorous development of the global digital economy, the scale of personal digital assets is expanding at an unprecedented rate, and their types are also becoming increasingly diversified. Such assets cover a wide range, including but not limited to traditional categories such as social media accounts, emails, cloud storage data, as well as emerging fields like cryptocurrencies, Non-Fungible Tokens (NFTs), virtual items in games, copyrights for digital content creation, and even virtual land and digital identities in the metaverse. These digital assets not only carry individual emotions, memories, and reputations but also embody considerable economic value. However, in stark contrast to the rapid growth of digital assets, existing legal frameworks generally lag in regulating the inheritance and disposal of digital assets, leading to an increasingly prominent "digital inheritance vacuum" phenomenon. Statistical data show that over 50% of adults worldwide already own digital

 doi:10.20944/preprints202506.0292.v1

assets with substantial economic or emotional value, yet it is noteworthy that only about 12% of individuals have made explicit arrangements for the future inheritance of such assets. [If there is a specific source for this data, please add a citation here.] This lag not only can lead to the loss, inaccessibility, or misuse of digital assets, thereby causing economic losses and emotional distress to heirs, but may also trigger complex legal disputes.

In addition to inheritance, the "destruction" demand for digital assets is also growing and holds critical significance. Individuals may wish to permanently destroy certain digital assets under specific conditions (e.g., after death or the occurrence of a specific event) based on considerations such as privacy protection, data security, preventing sensitive information leakage, or preventing specific digital footprints from being tracked. Typical examples include personal health data, confidential business documents, personal creations not intended for public disclosure, or social media content. Traditional centralized service providers often lack transparent, trustworthy, and automated destruction mechanisms, making it difficult for users to truly control the "lifecycle" of their digital assets.

Driven by the wave of Web3.0 and the metaverse, the boundaries of digital assets are further blurring, and their value and complexity will grow exponentially. The emergence of new types of digital assets such as Decentralized Identities (DIDs), on-chain reputation, and rare items in virtual worlds [7] means that digital inheritance management is no longer limited to "inheritance" in the traditional sense, but also covers the continuation or termination of digital identity and digital footprint. In view of this, constructing a transparent, secure, efficient, automated, and privacy-preserving decentralized digital inheritance management system to effectively address the inheritance and destruction of digital assets has become a major issue urgently needing resolution in the current digital age. This research aims to delve into the application potential of blockchain and smart contract technology in this field and proposes a system architecture design based on a "Decentralized Application (DApp)," hoping to provide a theoretical basis and practical reference for future legislative improvements, technological practices, and user popularization.

Declaration on the Use of Artificial Intelligence: The authors confirm that Artificial Intelligence (AI) and AI-assisted technologies, including large language models (LLMs) such as ChatGPT, were utilized during the preparation of this manuscript for purposes including translation, linguistic refinement, and structural suggestions. The authors have reviewed and edited the content as needed and take full responsibility for the accuracy and integrity of the work. It is confirmed that AI tools do not meet the authorship criteria and have not been listed as authors.

II. Legal Status of Digital Asset Inheritance Domestically and Internationally

A. Chinese Legal Framework

China is in a phase of gradual exploration and improvement regarding the legal protection of digital assets. Article 127 of the Civil Code of the People's Republic of China, which came into effect on January 1, 2021, clearly stipulates: "Where the law has provisions on the protection of data and network virtual property, those provisions shall apply." This clause lays the foundation for the legal status of digital assets; however, its phrasing "those provisions shall apply" also reflects the absence of specific implementation rules. As of now, China has not yet promulgated specific laws and regulations for digital inheritance.

However, legislative practice in related fields is continuously advancing. The "Provisions on the Management of Internet Information Service Algorithmic Recommendations," effective January 1, 2022, first mentioned the user's right to dispose of their personal data. This provision provides a legal basis for users to arrange their digital assets during their lifetime but still does not directly address inheritance issues. Furthermore, laws and regulations such as the "Cybersecurity Law of the People's Republic of China," the "Data Security Law of the People's Republic of China," and the "Personal Information Protection Law of the People's Republic of China," although primarily focused on data security and personal information protection, their definition and protection principles for data rights

 doi:10.20944/preprints202506.0292.v1

will undoubtedly have an indirect impact on the disposal of digital inheritance. In recent years, there have been several inheritance cases involving digital assets such as game accounts and cryptocurrencies in Chinese judicial practice [3,10]. Courts usually analyze individual cases based on the general principles of inheritance in the Civil Code, combined with the nature of digital assets, but a unified adjudication standard is still lacking.

B. International Legal Framework

The international community's legislative exploration of digital inheritance presents a diversified trend:

- **United States**: The legislative process varies by state, but the Uniform Fiduciary Access to Digital Assets Act (RUFADAA) [1] has been widely adopted. This act explicitly authorizes executors or trustees, with a will or court order, to access, manage, or dispose of a deceased user's digital assets, but usually does not include the content itself, only directory information of the account. However, for new types of digital assets like crypto assets, states still need to further clarify their legal status and inheritance methods.
- **European Union**: Although the General Data Protection Regulation (GDPR) establishes the "Right to Erasure," allowing individuals to request the deletion of their personal data, it does not explicitly stipulate the right to inherit digital inheritance [2]. In practice, this may lead to conflicts between the "Right to Erasure" and the right of heirs to access the data of deceased relatives. To address this issue, EU member states such as Germany and France have begun to formulate or revise special laws on digital inheritance [1]. For example, the German Federal Supreme Court ruled in 2018 that social media accounts can be inherited as part of an estate, providing an important precedent for the judicial practice of digital inheritance.
- **Japan**: The "Digital Inheritance Act" promulgated in 2019 clearly stipulates that digital assets can be part of an estate [1] and provides detailed regulations on the scope of digital inheritance, inheritance methods, and the validity of wills. It is one of the earliest countries in the world to issue specialized digital inheritance laws.
- **United Kingdom**: The UK does not yet have specific digital inheritance legislation and mainly relies on existing inheritance and wills laws. However, the UK Law Commission has issued consultation papers on digital asset inheritance, exploring how to update existing laws to adapt to the needs of the digital age, including the legal validity of electronic wills.
- **Canada and Australia**: These countries also face similar challenges. Some provinces or states have begun to formulate relevant bills with reference to RUFADAA or handle digital inheritance disputes through judicial practice.
- **Cross-border Digital Inheritance Issues**: With the global flow of digital assets, cross-border digital inheritance issues are becoming increasingly prominent. Differences in legal definitions of digital assets, inheritance rules, and tax policies among different countries and regions may lead to complex legal conflicts and jurisdictional disputes. This requires

 doi:10.20944/preprints202506.0292.v1

strengthening international cooperation in the future to explore a unified legal framework or international agreements.

III. Technical Basis for Digital Will Implementation

A. Applicability Analysis of Blockchain Technology

Blockchain, as a decentralized, distributed, and immutable ledger technology, provides inherent advantages and a technical basis for the implementation of digital wills [4,5]:

- **Immutability and Security**: Data recorded on the blockchain is difficult to tamper with. This feature ensures the authenticity, integrity, and finality of digital will content, effectively preventing wills from being forged or maliciously modified, and greatly enhancing the credibility of wills.
- **Timestamp Function**: Each block on the blockchain contains a timestamp, which provides precise and undeniable time proof for the creation, modification, and execution of wills, helping to resolve common date disputes in traditional wills.
- **Decentralization and Censorship Resistance**: Digital wills stored on a decentralized blockchain network are not controlled by a single central institution, effectively avoiding risks such as centralized server failures, data loss, or censorship, thereby improving the availability and attack resistance of wills.
- **Smart Contract Support**: Smart contracts are programmable protocols running on the blockchain that can automatically execute based on preset conditions. This enables digital wills to achieve complex, multi-conditional automated execution logic, such as liveness detection, multi-party verification, and proportional asset allocation, without third-party intermediary intervention.
- **Traceability and Transparency**: All transactions and state changes on the blockchain can be publicly queried (provided privacy requirements are met), which provides high transparency for the execution process of wills. All relevant parties can verify whether the will is executed according to established rules.
- **Challenges and Solutions for Privacy Protection**: Although blockchain has the characteristic of public transparency, will content usually involves personal privacy. This requires combining cryptographic technologies such as Zero-Knowledge Proofs (ZKP) [8] and Secure Multi-Party Computation (MPC) to verify the existence and integrity of the will or perform secure computation of key fragments without leaking the specific content of the will.

B. Evaluation of Blockchain Platforms Suitable for Digital Wills

Choosing a suitable blockchain platform is crucial for the performance, cost, security, and scalability of a digital will DApp. The following table evaluates several mainstream platforms:

 doi:10.20944/preprints202506.0292.v1

Platform	Advantages	Limitations	Applicable Scenarios	Community Activity & Developer Support	Scalability Solutions	Security Audit History
Ethereum	Mature smart contracts, well-developed ecosystem, high security, high degree of decentralization	High Gas fee volatility, relatively slow processing speed (Layer 1)	High-value assets, complex conditions, scenarios with extremely high demands on decentralization and security	Very High	Layer 2 (Arbitrum, Optimism, zkSync)	Good (but smart contract vulnerability risk still exists)
BSC	Low transaction fees, high efficiency, EVM compatibility, low development threshold	Relatively high degree of centralization, security depends on a few validators	Small and medium-sized asset packages, scenarios sensitive to transaction costs	High	-	Average
Solana	High throughput, low latency, extremely low transaction costs	Network stability issues (occasional interruptions), relatively high degree of centralization	Large amounts of small assets, high-frequency interactive digital assets (e.g., metaverse assets)	High	-	Average
Cardano	Formal verification, high security, academic rigor, sustainable development	Relatively limited development ecosystem, smart contract functions still developing	Scenarios with extremely high security requirements, long-term stable digital inheritance planning	Medium	Hydra (Layer 2)	Good
Hyperledger Fabric	Privacy protection, permissioned, enterprise-level applications, controllable performance	Steep learning curve, lower degree of decentralization, ecosystem not as rich as public chains	Enterprise-level or institutional solutions, consortium chain scenarios	Medium	-	Good
Polygon	EVM compatible, low Gas fees, high throughput, Layer 2 solutions	Relies on Ethereum mainnet security, centralization risk (specific solutions)	Suitable for Ethereum ecosystem expansion, small and medium-sized assets	High	PoS, zkEVM	Good
Avalanche	High throughput, low latency, customizable	Ecosystem developing, some	Scenarios requiring high performance and	Medium	Subnets	Average

 doi:10.20944/preprints202506.0292.v1

	subnets, EVM compatibility	centralization risks	customizable blockchains

Comprehensive evaluation suggests that for a decentralized digital inheritance management DApp, Ethereum and its Layer 2 solutions (such as Arbitrum, Optimism) are currently the most robust choices, balancing smart contract maturity, ecosystem support, and security. For application scenarios with higher requirements for cost and speed, Polygon or Solana can be considered, but their decentralization and security risks need to be carefully weighed.

IV. Application Design of Smart Contracts in Digital Wills

Smart contracts form the core logic layer of a digital will DApp, encoding the terms and execution rules of the will into automatically executable code.

A. Core Functional Design of Smart Contracts

A robust digital will smart contract should include the following core functions:

1. **Liveness Detection Mechanism**:
    - **Periodic Check-in**: Requires the asset owner to perform an on-chain check-in (calling a smart contract function) via the DApp periodically (e.g., every 180 days) to prove their living status.
    - **Web3.0 Wallet Activity Monitoring**: Combines Decentralized Identity (DID) and on-chain analysis tools to monitor the on-chain activity of the user's bound DID (e.g., transactions, NFT minting, DApp interactions). If the user does not generate any on-chain activity within a preset period, further liveness detection confirmation procedures may be triggered.
    - **Multiple Non-Response Trigger**: If there are consecutive failures to check-in or no on-chain activity (e.g., 3 times), the warning phase of the inheritance process is triggered.
    - **Grace Period**: A cooling-off period (e.g., 90 days) is set after the warning phase. During this period, if the owner resumes check-in or is confirmed alive by a legal representative, the inheritance process is terminated.
2. **Multi-Signature Verification**:
    - **Executor Multi-Sig**: The smart contract can be configured as a multi-signature wallet, requiring multiple parties (e.g., owner, designated lawyer, notary, or trusted family member) to jointly sign to modify the will or trigger core execution.
    - **MPC Integration**: Introduce Secure Multi-Party Computation (MPC) technology to split the private key into multiple shares held by different participants. Only when a specific number of participants (e.g., k out of n) jointly compute can the private key be reconstructed or a valid signature generated, thus achieving more secure key management and transaction authorization.
3. **Time Lock & Conditional Execution**:
    - **Cooling-off Period**: As mentioned earlier, used to prevent accidental triggering or

 doi:10.20944/preprints202506.0292.v1

malicious execution when the owner is not fully conscious.

- **Specific Event Trigger**: Inheritance or destruction can be triggered based on specific events, such as:
  - **Oracle Verification**: An oracle confirms the owner's death certificate (connecting to government death registration systems).
  - **Court Judgment Certification**: A legal representative or court submits and verifies a court judgment on-chain through a specific interface, forcibly triggering will execution.
  - **Specific Date/Time**: Set to automatically execute at a specific date or time point.
  - **Combined Conditions**: For example, execution only occurs after "the owner has not checked in for 6 consecutive months" AND "the oracle confirms death" AND "legal representatives confirm via multi-sig."

4. **Asset Classification & Destruction Strategy**:
   - **Refine Asset Types**: Set differentiated processing strategies based on the nature of digital assets (cryptocurrency, NFT, game accounts, cloud data, social media accounts, etc.).
   - **Encrypt Access Information**: The smart contract does not directly store sensitive access credentials (e.g., passwords, mnemonic phrases) but stores their encrypted hash values or IPFS/Arweave addresses. Actual decryption and access occur off-chain, provided after key management module and heir identity verification.
   - **Parallel Inheritance and Destruction**:
     - **Inheritance**: For inheritable assets (e.g., cryptocurrencies, NFTs), the smart contract can directly trigger on-chain transfers; for account-based assets, the encrypted access information is securely transmitted to the heir through an off-chain notification mechanism.
     - **Destruction**: For sensitive data designated for destruction or assets unclaimed under specific conditions, the smart contract can trigger the following destruction logic. Furthermore, the introduction of Artificial Intelligence Agents (AI Agents) to execute complex destruction tasks can be researched:
       - **AI Agent-Assisted Destruction**: Deploy AI Agents activated by the smart contract when preset conditions are met. These AI Agents can be programmed to:
         - **Autonomous Interaction**: Interact with various platforms (including APIs of centralized service providers, social media backends, cloud storage interfaces, etc.) to execute multi-step destruction protocols, such as requesting

 doi:10.20944/preprints202506.0292.v1

account deactivation, deleting data, revoking access permissions, etc.

- **Deep Cleaning**: AI Agents can perform more thorough digital footprint cleaning, such as tracking and requesting the deletion of associated data copies or mentions scattered across multiple platforms.
- **Verification and Reporting**: After performing destruction operations, AI Agents can return proof of execution status (e.g., API responses, operation log hashes) to the smart contract, ensuring the effectiveness and auditability of the destruction.
- **Adaptive Execution**: When facing platform interface changes or unexpected errors, AI Agents can possess a certain degree of adaptive adjustment capability, trying alternative destruction paths or notifying human intervention.

- **Cryptocurrency**: Send tokens to a "black hole address" (0x0...0), making them permanently unusable.
- **Off-Chain Data**: Notify decentralized storage services (e.g., IPFS) to delete relevant indexes, or destroy the private keys used to encrypt the data, making the data undecryptable and inaccessible. AI Agents can also assist in verifying the completion of such operations.
- **Centralized Accounts**: **AI Agents can replace or enhance the functionality of oracles,** directly sending and tracking destruction requests to centralized service providers via API (if the platform supports it), handling more complex interaction processes, such as multi-factor authentication or CAPTCHA challenges (within their capabilities).
- Introducing AI Agents for digital asset destruction requires focusing research on their security, behavioral controllability, decision transparency, and ethical boundaries, ensuring their actions fully comply with the deceased's wishes and legal regulations.

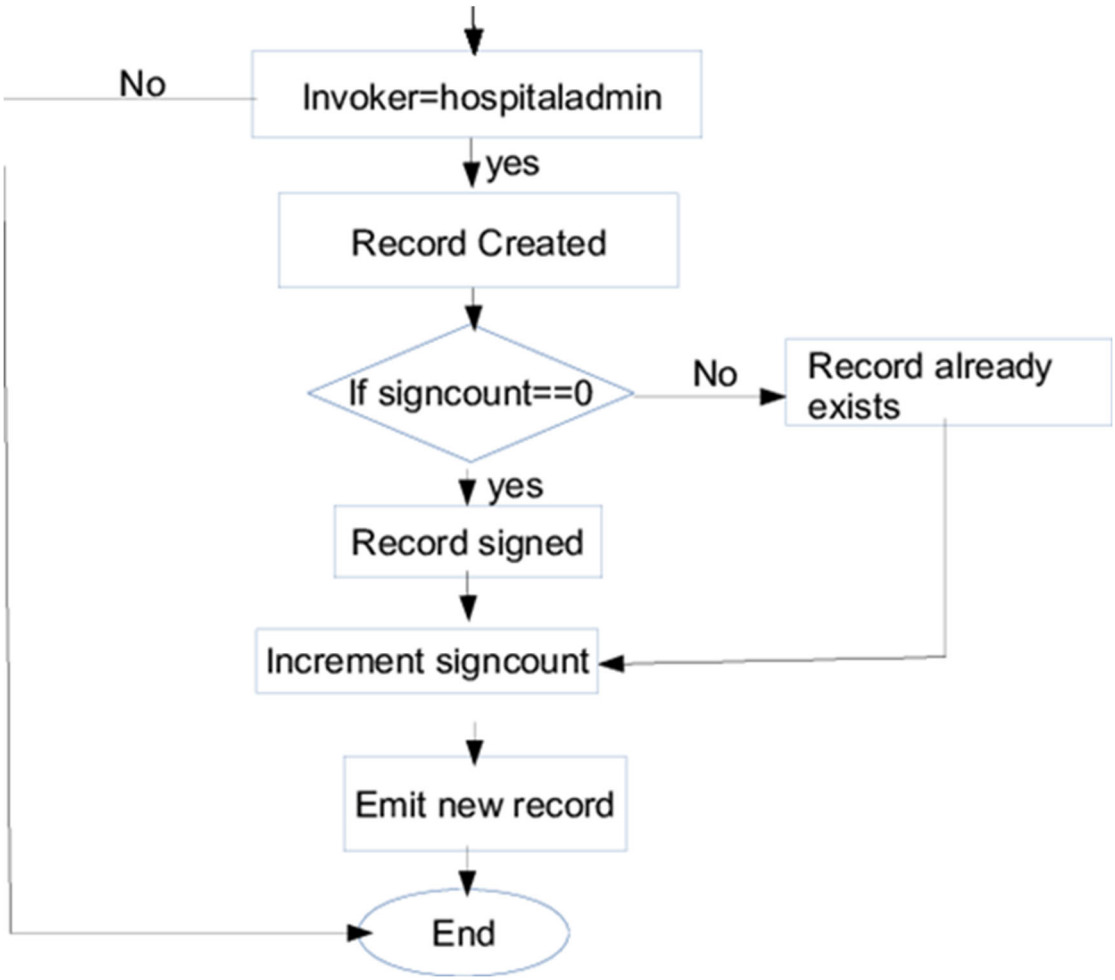
- **Asset Status Management**: Record the current status of each asset (unprocessed, inherited, destroyed) to avoid duplicate operations.

B. Schematic Diagram of Smart Contract Code Implementation

 doi:10.20944/preprints202506.0292.v1

The implementation of smart contracts involves writing and deploying Solidity language. Its core logic defines data types (such as Heir, Asset) through structs, and implements will creation, liveness detection, asset addition, and triggering will execution and asset processing (including transfer and destruction) under specific conditions through functions. Events are used for off-chain applications to listen for contract state changes. Modifiers are used to control function access permissions and execution conditions.

The schematic diagram is as follows:



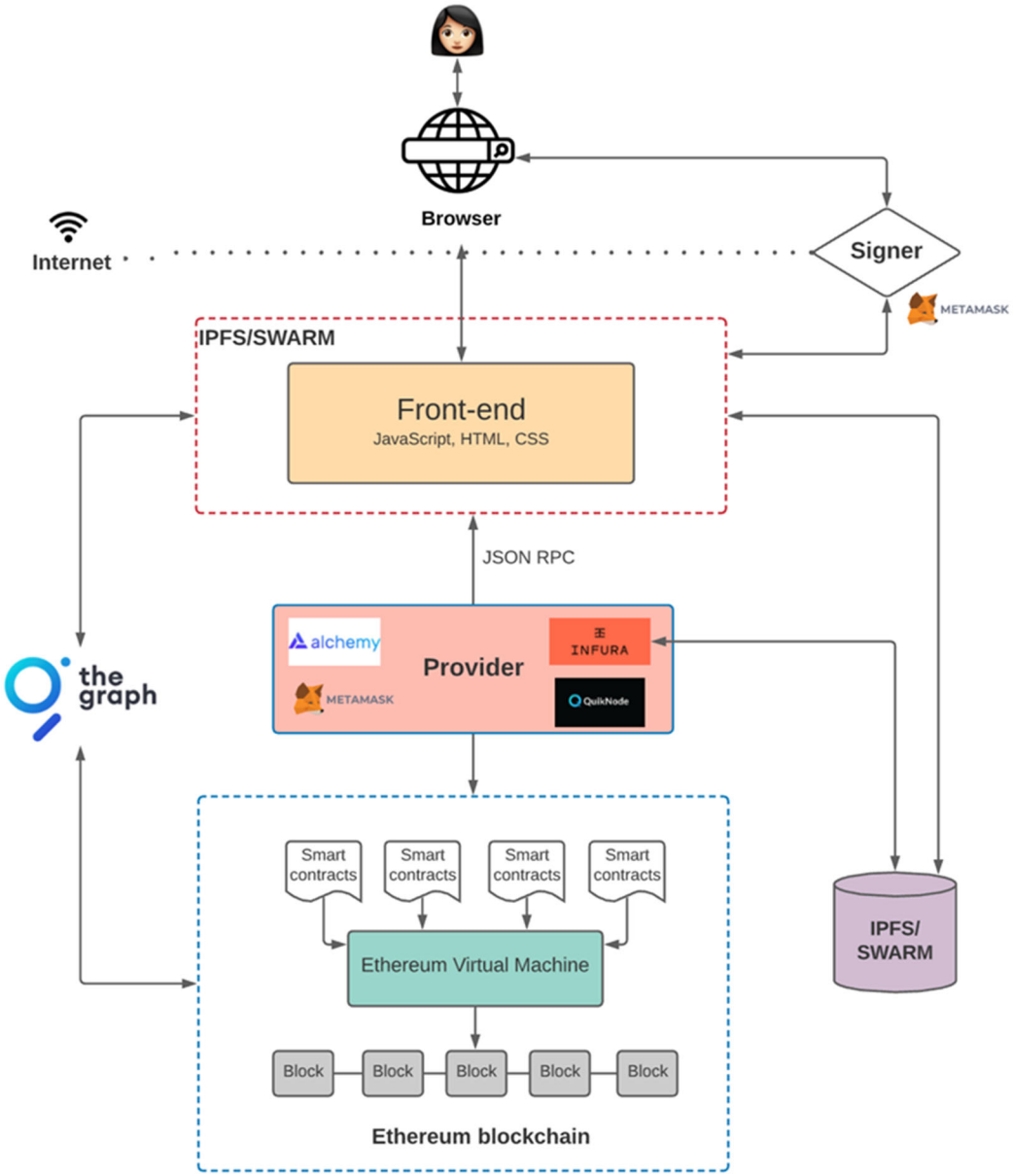
This diagram shows the main components of the smart contract and their interaction, rather than specific code details.

V. Decentralized Digital Inheritance Management DAPP Architecture Design

The blockchain-based digital will system will be presented as a Decentralized Application (DApp), employing a multi-layer architecture aimed at achieving a functionally complete, secure, reliable, and user-friendly experience.

 doi:10.20944/preprints202506.0292.v1

A. Overall Architecture



1. **Blockchain Layer**:
    - **Core Trust Layer**: Hosts smart contracts (e.g., the DigitalWill contract mentioned above) and all critical transaction records. This layer serves as the trust foundation for the entire system, ensuring the immutability and automated execution of will logic.
    - **Data Storage**: Stores core metadata of the will, asset identifiers, heir addresses, encrypted information hashes, timestamps, and event logs. Sensitive plaintext information is not stored on this layer.
    - **Smart Contracts**: Contain core business logic such as liveness detection, asset registration, heir management, will execution, asset destruction, and legal intervention.

 doi:10.20944/preprints202506.0292.v1

- **Decentralized Ledger**: All operations are publicly transparent and verifiable by any entity.

2. **Middleware Layer**:
   - **Oracle Services**:
     - **External Data Integration**: Connects to off-chain real-world data sources, such as government death registration system APIs, news media (for auxiliary judgment), and medical institution data (requires strict authorization and privacy protection).
     - **Decentralized Oracle Network**: Adopts decentralized oracle networks like Chainlink, ensuring the accuracy and attack resistance of death facts or other trigger conditions through multi-node, multi-data source verification mechanisms, thus avoiding single points of failure.
     - **Trusted Execution Environment (TEE)**: In certain sensitive data processing or complex logic verification scenarios, TEE (e.g., Intel SGX) can be used as the data processing layer for oracles, providing a hardware-level trusted computing environment.
   - **Cryptography & Key Management**:
     - **Threshold Signature**: Adopts algorithms like Shamir's Secret Sharing to split the owner's master private key or the key used to encrypt sensitive asset access information into n shares, distributed to multiple trusted parties (e.g., lawyers, notaries, designated guardians). Only when at least k shares are collected can the key be reconstructed or a signature generated, thus achieving multi-party joint control and preventing single points of failure.
     - **Secure Multi-Party Computation (MPC)**: Further enhances key security, allowing multiple parties to collaboratively compute sensitive information (e.g., decrypting key fragments), ensuring that no single party can obtain the complete secret.
     - **Decentralized Storage Integration**: Stores encrypted sensitive access information (e.g., mnemonic phrase fragments, API credentials) on decentralized storage networks like IPFS or Arweave. Only their content hashes are stored on-chain to ensure data censorship resistance and persistence.
     - **Programmable Privacy**: Combines Zero-Knowledge Proof (ZKP) technology [8], allowing users to prove the existence, integrity, or certain specific conditions (e.g., "I have checked in") without revealing the specific content of the will.
   - **Decentralized Identity (DID) System**:

 doi:10.20944/preprints202506.0292.v1

- **Identity Verification**: Provides a decentralized identity verification mechanism for will owners, heirs, legal representatives, and other participants, ensuring the correlation and trustworthiness between their on-chain identity and off-chain real identity.
- **Credential Management**: Users can manage their digital credentials (e.g., death certificates, lawyer licenses) through DID and present them to the smart contract or DApp for on-chain verification when needed.
- **On-Chain Activity Association**: DID can be associated with the user's Web3.0 wallet address, facilitating DApp monitoring of the user's on-chain activity.

3. **Application Layer**:
    - **User Interface (UI)**:
        - **Will Creation Wizard**: Provides an intuitive, step-by-step wizard to guide users in creating digital wills, including adding digital assets (type, platform, encrypted access information hash), specifying heirs (wallet address, contact information hash, whether they are legal representatives), setting liveness detection cycles, destruction strategies, etc.
        - **Liveness Detection Reminders and Check-in**: Periodically reminds users to perform on-chain check-ins and provides a one-click check-in function.
        - **Asset List and Status**: Clearly displays the list of registered digital assets and their current processing status (unprocessed, pending execution, inherited, destroyed).
        - **Notifications and Alerts**: Sends notifications of will status changes, check-in reminders, execution notices, etc., to users, heirs, and legal representatives via Web3.0 messaging protocols or traditional push services.
    - **Heir/Executor Interface**:
        - Provides an interface for viewing the status of the deceased owner's will, requesting access to asset information, and triggering will execution (when conditions are met).
        - May need to integrate off-chain identity verification (e.g., KYC) to ensure legitimacy.
    - **Legal Professional Interface**:
        - Provides specific permissions for lawyers and notaries to view will content (under authorization), verify off-chain legal documents (e.g., death certificates, court judgments), and trigger legal intervention functions in the smart contract.
        - Provides evidence chain generation and export functions for legal evidence

 doi:10.20944/preprints202506.0292.v1

collection.

- **Optional Centralized Backend Services**: Although a DApp, to enhance user experience and handle complex off-chain logic, some centralized backend services may still be needed, such as:
  - **Notification Push Service**: Sends traditional notifications like emails and SMS.
  - **Off-Chain Data Encryption/Decryption Service**: Assists users in securely encrypting/decrypting sensitive data.
  - **External API Integration**: Interacts with APIs of centralized platforms (e.g., social media, cloud storage) to trigger account destruction or information transfer (requires strict control over permissions and security).
  - **Data Indexing Service**: Optimizes the query and display speed of on-chain data.

B. Key Technical Challenges and Solutions

1. **Private Key Management and Recovery**
   - **Challenge**: Loss or inaccessibility of the digital will owner's private key is a core risk. Traditional private key management methods (e.g., mnemonic phrases) are not user-friendly for non-technical users and have single points of failure.
   - **Solution**:
     - **Threshold Signature Wallets**: Threshold signature wallets built with MPC technology split the private key into multiple shares, managed separately by the user, trusted family members, lawyers, or notary institutions. Will execution requires multi-party joint signatures to unlock or execute, effectively reducing the risk of single points of failure.
     - **Social Recovery Wallets**: Allow users to designate a group of "Guardians." If the user loses their private key, wallet access can be restored through the approval of a majority of guardians. This mechanism is highly consistent with the concept of digital wills.
     - **Hardware Wallet Integration**: Encourage users to store their master private keys in hardware wallets and seamlessly integrate them through the DApp, providing the highest level of physical security.
     - **Decentralized Key Management System (DKMS)**: Explore blockchain-based DKMS to achieve decentralized generation, storage, and recovery of keys.
2. **Balancing Data Privacy and Publicity**
   - **Challenge**: There is a contradiction between the public transparency of the blockchain and the privacy of will content (e.g., asset details, heir contact

 doi:10.20944/preprints202506.0292.v1

information, sensitive access credentials).

- **Solution**:
  - **Off-Chain Encrypted Storage and On-Chain Hash**: Sensitive will content and access credentials are not stored directly on-chain. They should be encrypted and stored on decentralized storage networks like IPFS or Arweave, or encrypted and distributed to trusted third parties. The on-chain smart contract only stores the hash values of this encrypted content and access control logic.
  - **Zero-Knowledge Proofs (ZKP)**: Allow proving the authenticity of certain facts without revealing the specific content of the will. For example, proving "the will owner has checked in" or "a certain heir possesses a legitimate credential" without disclosing the specific time of check-in or credential content [8].
  - **Secure Multi-Party Computation (MPC)**: Used for multi-party collaborative computation of sensitive information (e.g., decrypting key fragments), ensuring that no single party can obtain the complete secret.
  - **Homomorphic Encryption**: Although currently computationally expensive, it may allow direct computation on encrypted data in the future, further enhancing privacy.

3. **Oracle Problem**
   - **Challenge**: Smart contracts cannot directly access off-chain data, such as death certificates or court judgments, requiring trusted oracles to bring off-chain information on-chain. Centralization of oracles or untrustworthy data sources can lead to single points of failure or data poisoning.
   - **Solution**:
     - **Decentralized Oracle Network**: Adopt decentralized oracle networks like Chainlink, which obtain information from multiple authoritative data sources (e.g., government APIs, notary institutions) through multiple independent nodes and verify data authenticity through consensus mechanisms, reducing single-point risks.
     - **Multi-Source Verification Mode**: Require multiple oracles from different sources to provide the same information and set a threshold, triggering the smart contract only when a majority consensus is reached.
     - **Trusted Execution Environment (TEE)**: Utilize TEE technology to ensure that oracle nodes execute data acquisition and verification logic in a secure, isolated environment, preventing data tampering during transmission and processing.
     - **Off-Chain Computation and On-Chain Verification**: For complex off-

 doi:10.20944/preprints202506.0292.v1

chain logic (e.g., comprehensive judgment of death fact), off-chain computation solutions (e.g., Truebit) can be adopted to perform computations off-chain and generate proofs verifiable by on-chain smart contracts.

4. **Cross-Chain Interoperability Problem**
    - **Challenge**: Users' digital assets may be distributed across different blockchain networks (e.g., ERC-20 tokens on Ethereum, NFTs on Solana, DeFi positions on BSC). A digital will on a single chain cannot manage all assets.
    - **Solution**:
        - **Cross-Chain Bridges**: Allow asset transfer between different blockchains but come with security risks.
        - **Cross-Chain Communication Protocols**: Adopt protocols like IBC (Inter-Blockchain Communication Protocol) or LayerZero to enable direct communication between smart contracts on different blockchains, allowing a digital will contract on one chain to trigger asset transfer or destruction operations on other chains [9].
        - **Multi-Chain Deployment**: Deploy compatible digital will smart contracts on multiple mainstream blockchains and manage them through a unified DApp front-end.
5. **Legal and Technical Conflicts and Regulatory Challenges**
    - **Challenge**: There are coordination issues between the automated execution of smart contracts and the complex procedures, manual reviews, and court judgments in traditional legal systems. Cross-border issues and tax issues related to digital inheritance also require attention.
    - **Solution**:
        - **Legal Framework Integration**: Embed legal templates into smart contract design and reserve interfaces for legal professionals to intervene, ensuring compatibility between technical implementation and legal requirements [1,6].
        - **Human-Computer Interaction Interface**: Smart contracts should be designed to allow legal representatives or courts to intervene or provide final confirmation through specific interfaces before critical execution steps (e.g., final asset distribution) to comply with judicial procedures.
        - **Regulatory Sandbox Pilot**: Test digital will DApps in a controlled regulatory sandbox environment and cooperate with regulatory agencies to gradually explore compliance paths.
        - **International Cooperation and Legislative Coordination**: Promote international cooperation and coordination in digital asset inheritance laws

 doi:10.20944/preprints202506.0292.v1

to address cross-border issues.

VI. Ensuring the Legal Validity of Digital Wills

To ensure that blockchain-based digital wills have legal effect and can be recognized in judicial practice, the deep integration of technology and law is crucial.

A. Legal Framework Integration

- **Embedding Legal Templates and Clauses**:
  - The DApp should provide pre-set will templates based on the legal requirements of different jurisdictions (e.g., China, US, EU). When creating a will, users can select their applicable legal system, and the smart contract will automatically load necessary clauses and declarations compliant with local regulations [1–3,6].
  - Such templates should include clear definitions of digital assets, heir qualifications, execution conditions, dispute resolution mechanisms, and other legal elements.
- **Participation Mechanism for Legal Professionals**:
  - **Lawyer/Notary Nodes**: Design specific roles and permissions in the smart contract to allow certified lawyers, notaries, or will executors to participate as multi-signature parties or privileged nodes in the creation, modification, and execution of wills.
  - **Off-Chain Identity Verification**: After legal professionals undergo KYC (Know Your Customer) and professional qualification verification off-chain, their on-chain identity (DID) is bound to their real identity to ensure the legality of their operations.
  - **Legal Opinion and Confirmation**: At critical stages of will execution (e.g., confirmation of death, estate distribution), on-chain signature confirmation from legal professionals can be required to give it legal effect.
- **Evidence Preservation Mechanism**:
  - **Immutable Blockchain Records**: Utilize the immutability of the blockchain [4] to form a complete and traceable evidence chain of all on-chain operations related to the will, such as creation, modification, check-ins, and execution. Each operation is timestamped and signed by participants, providing strong support for judicial review.
  - **On-Chain and Off-Chain Association**: Associate on-chain transaction hashes, block heights, etc., with off-chain legal documents (e.g., death certificates, court orders) and notarize them to form a mutually corroborating evidence system.
  - **Data Audit and Export**: The DApp should provide convenient data audit and export functions for courts, lawyers, etc., to collect and review evidence.

B. Judicial Practice Paths

 doi:10.20944/preprints202506.0292.v1

- **Path to Judicial Recognition**:
    - **Promote Legislation and Judicial Interpretation**: Actively promote the promulgation of specialized national laws, regulations, or judicial interpretations on digital inheritance, clarifying the legal validity of electronic wills, the legality of blockchain as evidence, and the legal binding force of smart contracts [3].
    - **Case Accumulation and Guidance**: Encourage courts to refer to the technical characteristics of blockchain and smart contracts when hearing digital inheritance cases, gradually forming unified adjudication rules and guiding cases.
    - **Applicability of Electronic Signature Law**: Explore applying the principles of electronic signature law and electronic evidence law to digital signatures and transaction records on the blockchain to provide a basis for their legal validity.
- **Notarization Integration Model**:
    - **Participation of Digital Notary Institutions**: Introduce digital notary institutions as privileged nodes or oracles for smart contracts, responsible for verifying off-chain legal facts (e.g., death certificates, identity information) and putting them on-chain, providing a legal basis for the execution of smart contracts.
    - **Blockchain Evidence Preservation**: Notary institutions can use blockchain for electronic data preservation, ensuring the authenticity and integrity of documents related to digital wills.
- **Arbitration Clauses and Decentralized Dispute Resolution**:
    - **Built-in Arbitration Clauses**: Preset arbitration clauses in the digital will smart contract, designating specific arbitration institutions or decentralized arbitration platforms (e.g., Kleros, Aragon Court) as dispute resolution mechanisms.
    - **On-Chain Arbitration**: Explore blockchain-based decentralized arbitration mechanisms, where community jurors or professional arbitrators adjudicate on-chain disputes, and the arbitration results are fed back into the smart contract for execution.

VII. Case Analysis and Implementation Path

A. International Practical Cases

Globally, some projects and companies are exploring the application of blockchain and smart contracts in digital inheritance management:

- **Ethereum Trust Alliance**: A decentralized autonomous organization (DAO) based on Ethereum, aiming to provide digital inheritance planning tools and standards. It utilizes smart contracts to manage the inheritance of crypto assets and explores integration with Decentralized Identity (DID).
- **Safe Haven (SHA)**: A blockchain solution focused on crypto asset inheritance. Its product, SafeKey, uses multi-signature and time-lock mechanisms, allowing users to designate heirs

 doi:10.20944/preprints202506.0292.v1

and unlock crypto assets under specific conditions. The project emphasizes the secure storage and distribution of private key fragments.

- **Digipulse**: Provides digital asset transfer services triggered by user activity. If a user does not log into their platform within a certain period, the system triggers notifications and eventually transfers preset digital asset information to designated recipients. Its model leans towards a combination of centralized services and blockchain technology.
- **Willbox**: A hybrid solution combining traditional notarization with blockchain. Users can create digital wills through a notary office and store their hash values on the blockchain to ensure the immutability of the will. When the will is executed, the notary office will handle it according to on-chain records and off-chain legal procedures.
- **Dorg (DAO for Digital Legacy)**: Some DAO projects have begun to explore how to manage collectively owned digital assets or NFTs through DAO governance mechanisms and provide digital inheritance planning options for DAO members.

These cases have different focuses in technical implementation but generally face challenges in how to securely manage private keys, reliably obtain off-chain death facts, and effectively integrate with traditional legal systems [1,6].

B. Suggested Implementation Path for China

Given China's leading position in the digital economy and blockchain technology, the following is a suggested implementation path for digital will DApps in China:

- **Regulatory Sandbox Pilot**:
  - It is recommended to carry out pilot projects for blockchain-based digital will DApps within fintech regulatory sandboxes or specific free trade zones.
  - Pilot content can include: filing and compliance review of smart contracts, testing the docking of oracles with government death registration systems (while ensuring data security and privacy), verifying the effectiveness of multi-signature mechanisms in legal practice, and exploring the compliance of digital asset destruction mechanisms.
  - Through pilots, collect actual operational data, assess risks, and provide a basis for subsequent large-scale promotion and legislation.
- **Industry Standard Construction**:
  - Jointly formulate technical standards for digital will smart contracts (e.g., interface specifications, data formats), security audit standards, and operational procedure specifications by blockchain technology and application alliances, legal associations, notary associations, and relevant technology enterprises.
  - Develop industry guidelines for the classification, valuation, and disposal of digital assets to provide a unified reference for DApp development and user use.
- **Legislative Suggestions and Policy Promotion**:
  - Promote the promulgation of relevant implementation rules for the Civil Code: Clarify the legal status of digital assets as inheritance, the valid forms of digital

 doi:10.20944/preprints202506.0292.v1

wills, the legal binding force of smart contracts, and the legal basis and procedures for digital asset destruction [3].

- Improve relevant laws and regulations: In conjunction with the Cybersecurity Law, Personal Information Protection Law, Data Security Law, etc., clarify the principles for handling personal information in digital inheritance, cross-border transfer rules, and legal responsibilities for destruction.
- Encourage the participation of notary institutions: Promote the combination of notary institutions and blockchain technology, explore the "digital notarization" model, and provide stronger legal credibility for digital wills.

- **Strengthen Public Education and Popularization**:
  - Through multiple channels such as government, media, and industry associations, popularize the importance of digital inheritance planning, the application advantages of blockchain technology therein, and how to securely use digital will DApps.
  - Provide easy-to-understand user guides and legal consultation services to lower the user threshold.

VIII. Conclusions and Outlook

Blockchain and smart contract technology offer unprecedented technical feasibility and innovative paths for solving the challenges of personal digital asset inheritance and destruction [5,6]. By constructing decentralized, automated, and immutable digital will systems, the lag of existing legal frameworks can be effectively compensated, ensuring the orderly inheritance and reasonable disposal of digital assets.

However, this emerging field still faces numerous challenges: including the lag in legal recognition, security vulnerability risks of smart contracts, data credibility of oracles, complexity of cross-chain interoperability, user private key management difficulties, and insufficient public awareness of new technologies.

Looking ahead, digital inheritance management will be an indispensable infrastructure in the era of the metaverse and Web3.0. With the popularization of Decentralized Identity (DID) [7], the maturation of programmable privacy technologies [8], and the application of AI in on-chain data analysis and decision support, digital will systems will become more intelligent, secure, and personalized. We anticipate:

- **Participation of Decentralized Autonomous Organizations (DAOs)**: DAOs may play a role in the inheritance and management of collective digital assets, for example, how the digital identities and assets of DAO members are disposed of after their demise.
- **AI-Empowered Smart Wills**: AI can assist users in generating will drafts that better reflect their intentions, analyze the risks of digital assets, and even assist in the judgment of liveness detection algorithms under strict authorization.
- **Deep Integration of DID and Programmable Privacy**: Users will be able to control the access permissions and privacy disclosure conditions of their digital assets more finely through DID, achieving true "data sovereignty."
- **Seamless Realization of Cross-Chain Interoperability**: A unified multi-chain digital

 doi:10.20944/preprints202506.0292.v1

inheritance management platform will be able to manage all digital assets distributed across different blockchains, achieving one-stop service [9].

- **Improvement of Digital Asset Valuation and Taxation Systems**: As the value of digital assets becomes increasingly prominent, their valuation methods and tax policies upon inheritance will become urgent legal and economic issues to be resolved.

Ultimately, the construction of a digital inheritance management system requires the concerted efforts of multiple parties, including governments, technology enterprises, the legal community, academia, and the general public. Only in this way can a digital will ecosystem that meets both technological logic and legal requirements, and balances privacy protection with asset inheritance, be jointly built to safeguard personal digital assets in the digital age.

References

1. A. G. Alzahrani, "Blockchain-based Digital Asset Inheritance: Legal and Technical Challenges," Journal of Law, Technology & Policy, vol. 37, no. 2, pp. 112–129, 2023.
2. European Commission, "Report on Digital Assets and Inheritance in the EU Digital Single Market," European Commission, 2022.
3. W. Li and X. Zhang, "中国数字遗产法律问题研究 (Research on Legal Issues of Digital Inheritance in China)," 法学研究 (Legal Research), vol. 45, no. 3, pp. 78–92, 2023.
4. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Whitepaper, 2008. Available: https://bitcoin.org/bitcoin.pdf. Accessed on May 29, 2025.
5. H. Wang et al., "Smart Contract-based Digital Will: System Design and Implementation," IEEE Transactions on Engineering Management, vol. 69, no. 4, pp. 1214–1227, 2022.
6. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Designing a Legal Framework for Digital Assets Inheritance Using Blockchain Technology," Computer Law & Security Review, vol. 48, p. 105706, 2023.
7. Y. Zhu and J. Chen, "Decentralized Identity (DID) and its Application in Digital Asset Inheritance," Journal of Blockchain Research, vol. 15, no. 1, pp. 45–60, 2024.
8. A. Smith and B. Jones, "The Role of Zero-Knowledge Proofs in Privacy-Preserving Digital Wills," International Journal of Cryptography and Security, vol. 10, no. 2, pp. 88–102, 2024.
9. C. Brown, "Cross-Chain Interoperability for Multi-Asset Digital Legacy Management," Blockchain Systems Review, vol. 7, no. 1, pp. 1–15, 2025.
10. P. Liu and Q. Wu, "中国数字遗产司法实践的新发展与挑战 (New Developments and Challenges in China's Judicial Practice of Digital Inheritance)," 法律科学 (Legal Science), vol. 29, no. 4, pp. 112–125, 2024.