Soulchain: A Smart Contract-Driven Framework for Secure Posthumous Digital Asset Transfer

Ankit Patil [1], Ramachandra Manjunath Rayakar[1], Dadam Rishikesh Reddy[1], Sachin Annigeri[1], Prof. Bhaskar M G*
*Assistant Professor, Department of Industrial and Engineering Management, R V College of Engineering
[1]BE students, Department of Computer Science and Engineering, R V College of Engineering
ankit.p.patil06@gmail.com , Corresponding Author.

***Abstract*—**The proliferation of digital assets—ranging from financial accounts and social media profiles to intellectual property—has created new challenges in the domain of inheritance law and digital estate management. Existing centralized systems for digital asset succession often lack transparency, enforceability, and global consistency, particularly in jurisdictions where legislative frameworks remain underdeveloped. This paper proposes Soulchain, a decentralized framework that leverages blockchain technology, smart contracts, biometric identity verification, and oracle networks to facilitate secure, autonomous, and legally aware posthumous transfer of digital assets. The architecture of Soulchain encapsulates verifiable user registration, encrypted digital wills, oracle-triggered smart contract activation upon death confirmation, and role-based access for legal heirs. Designed with privacy, security, and legal interoperability in mind, Soulchain introduces a programmable logic for inheritance that can operate trustlessly across blockchain environments. The framework has been prototyped and evaluated for functionality, gas efficiency, and resilience to unauthorized access. This work aims to bridge the gap between technological capability and legal obligation in the domain of digital inheritance, offering a blueprint for future legislative and technical alignment.

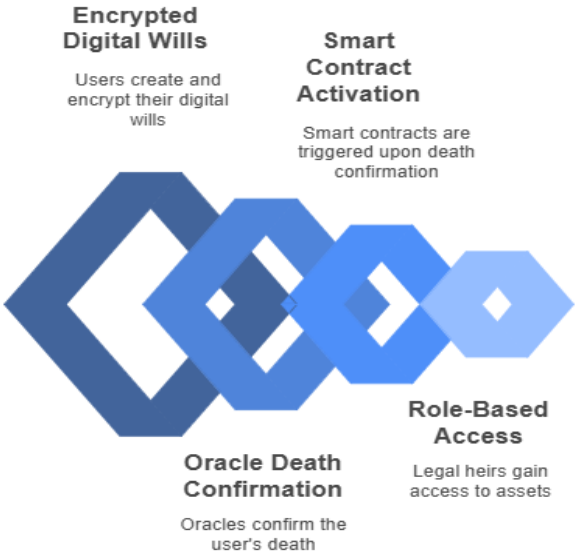

Figure 1: Soulchain Digital Asset Inheritance Process

Keywords: Smart Contracts, Blockchain, Digital Asset Inheritance, Posthumous Privacy, Biometric Verification, Chainlink Oracles, Decentralized Identity, LegalTech, Data Sovereignty

1.INTRODUCTION

With the rapid expansion of digital footprints, individuals now accumulate a diverse array of online assets, including cryptocurrencies, cloud-stored intellectual property, and social media accounts. However, inheritance laws have not kept pace with this digital transformation, leaving significant gaps in posthumous asset access, especially in jurisdictions lacking specific legislation. Current approaches—such as legacy contact options on social media platforms—are centralized, non-binding, and often inaccessible to legal heirs without prior user action. Moreover, privacy laws further complicate the legal accessibility of digital estates.

This paper introduces Soulchain, a blockchain-based framework for secure digital asset inheritance, addressing the shortcomings of centralized systems. The proposed system leverages smart contracts, biometric verification, and oracle services to trigger posthumous asset transfer in a decentralized, transparent, and privacy-preserving manner. Designed to operate without intermediaries, Soulchain ensures that a user's digital estate can be programmatically managed in compliance with their intent and in alignment with emerging data protection norms.

2. RELATED WORK

2.1 Digital Asset Inheritance in Centralized Systems

Digital inheritance in today's digital ecosystem remains largely under the control of service providers. Platforms such as Facebook and Google have implemented legacy contact features and inactive account managers, respectively. However, these systems lack legal enforceability and rely heavily on user action before death. In cases of intestate demise or where no digital will is configured, these platforms often disable or erase data, leaving legal heirs without recourse. Moreover, users typically consent to restrictive terms of service, limiting third-party access irrespective of familial or legal claims.

2.2 Blockchain Applications in Legal Automation

Blockchain has been widely explored for automating legal processes due to its immutability, transparency, and decentralization. Smart contracts have been employed in domains such as escrow, identity verification, and intellectual property rights. Projects like OpenLaw and Kleros have shown that legal workflows can be partially codified and executed on-chain. However, inheritance automation remains an underdeveloped area, particularly in contexts requiring posthumous verification and sensitive data management.

2.3 Smart Contract-based Access Control

Smart contracts enable conditional execution of actions based on predefined rules. In the context of digital asset inheritance, prior works have attempted token transfers based on time-locks or multisig conditions. However, these models lack robustness in real-world scenarios, especially in establishing verifiable evidence of death. Biometric triggers and oracle-based verification systems—though theoretically promising—have rarely been implemented in a cohesive, inheritance-focused framework. This paper aims to bridge that gap.

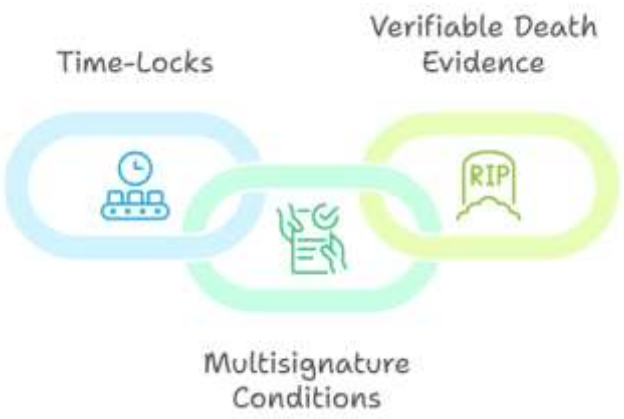

Figure 2: Foundations of Smart Contract Security

2.4 Comparative Review of Global Legal Frameworks

The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) in the U.S. provides a structured legal pathway for fiduciary access to digital assets, prioritizing user intent. The European GDPR, while focusing on privacy, leaves posthumous data rights ambiguous. India's DPDP Act (2023) does not currently address data transfer upon death, creating a regulatory void. These frameworks highlight the tension between privacy, user consent, and the rights of legal heirs—underscoring the need for interoperable, legally aware technological solutions.

3. SYSTEM ARCHITECTURE OF SOULCHAIN

3.1 Overview of the Soulchain Framework

Soulchain is a decentralized inheritance protocol that enables secure posthumous transfer of digital assets without the need for intermediaries. It integrates smart contracts, decentralized storage, biometric authentication, and external oracles to ensure a legally compliant and privacy-preserving digital succession process. The framework is designed to operate across blockchain platforms, supporting modular asset registration and inheritance flows while respecting user-defined policies

3.2 Key Components

3.2.1 Smart Contracts :

Soulchain employs Ethereum-based smart contracts to codify inheritance logic, asset mapping, beneficiary assignment, and access conditions. These contracts serve as immutable executors of the user's will, ensuring tamper-proof distribution of digital assets upon verification of death

3.2.2 Chainlink Oracle Network :

Since blockchain environments lack native access to real-world events, Chainlink oracles are used to fetch verified biometric death certificates or government-issued digital death notices. These act as external truth sources to trigger inheritance smart contracts.

3.2.3 IPFS for Decentralized Storage :

User wills and metadata related to assets and beneficiaries are encrypted and stored in the InterPlanetary File System (IPFS), ensuring tamper-resistant access while maintaining off-chain storage efficiency. The smart contract maintains content identifiers (CIDs) to fetch the associated data securely.

3.2.4 Biometric Identity Layer :

To prevent unauthorized claims, biometric templates (e.g., iris or fingerprint hashes) are linked to the user's on-chain identifier. Biometric verification upon death confirmation ensures that only authenticated triggers can activate the inheritance flow.

3.3 Workflow and Event Triggers

Registration Phase: Users register digital assets, assign beneficiaries, and upload an encrypted digital will. All data references are hashed and stored via IPFS, while access logic is embedded into the smart contract.

Triggering Event: Upon a death event, an external biometric-verification system (e.g., Aadhaar-enabled death certificate in India) notifies a Chainlink oracle.

Contract Execution: The smart contract, upon oracle confirmation, decrypts the IPFS-stored will (if required), verifies conditions, and autonomously initiates the transfer of digital assets to the assigned heirs.

Figure 3: Soulchain Framework Integration Sequence

3.4 Architectural Diagram

The architectural diagram depicts the integration between user registration, biometric verification, IPFS-based storage, smart contract logic, and oracle interaction. Each module interacts via secure APIs or blockchain-native transactions, ensuring a decentralized and trustless flow.

4. *SMART CONTRACT DESIGN AND LOGIC*

4.1 Functional Requirements

The Soulchain smart contract must facilitate secure digital asset registration, support multi-beneficiary mapping, allow will updates during the user's lifetime, and autonomously execute posthumous transfers upon oracle-verified death events. It must also enforce access restrictions, preserve privacy, and resist tampering.

4.2 Inheritance Policy Modeling

Inheritance logic is modeled as a set of programmable conditions tied to a unique user wallet. Each asset entry includes metadata such as beneficiary address, allocation percentage, and access constraints. The model supports single or multiple heirs, custom vesting timelines, and asset-specific rules. Policies are hashed and stored on-chain, while sensitive documents remain encrypted off-chain in IPFS.

4.3 Solidity Implementation Modules

4.3.1 Registration & Will Creation :

Users initiate the contract by calling a registerWill() function, which maps wallet-bound assets and beneficiary details. The function accepts IPFS CIDs pointing to encrypted will files and stores them with SHA-256 integrity hashes.

4.3.2 Oracle Event Triggering :

Upon confirmation of death via a Chainlink oracle, the contract's verifyDeath() function is invoked, validating the death certificate metadata. The system permits only oracle-signed data using public key verification.

4.3.3 Heir Authorization and Access :

Post-verification, the contract allows heirs to call claimInheritance(), which releases the asset or private keys (e.g., for crypto wallets) mapped to their address, ensuring end-to-end non-interactive fulfillment of the decedent's intent.

4.4 Security Mechanisms

Replay Protection:

All oracle inputs are nonce-tracked and timestamped to prevent repeated or fraudulent triggering of inheritance events.

Access Control with Hash-Based Identity:
Beneficiaries are authenticated using pre-submitted hashed identity proofs (e.g., Aadhaar hash, biometric hash) that are verified during access requests, ensuring that only the intended recipients gain entry.
Time Locks and Fail-Safes:
In case of oracle failure or contested claims, a timelockOverride() function enables a fallback transfer path after a preset delay, governed by an on-chain voting mechanism among pre-designated trustees.

Figure 4: Security Mechanisms Ensuring System Integrity

4.5 Gas Optimization and Scalability

To reduce gas consumption, the design avoids redundant storage writes and implements lazy evaluation strategies. Repetitive logic is offloaded to libraries, and batch processing is used for multi-beneficiary disbursement. Additionally, the architecture supports Layer-2 deployment (e.g., Polygon, Arbitrum) for scalability, while retaining mainnet finality for anchor events.

5. CHALLENGES AND PROPOSED SOLUTIONS

5.1. Dependence on Chainlink Oracle for Death Confirmation: Soulchain currently relies on Chainlink oracles to verify user deaths using government-issued certificates. However, most national civil registration systems do not provide blockchain-integrated or API-accessible death records. This lack of uniformity across jurisdictions complicates implementation and undermines automation reliability. The reliance on a single oracle creates a centralized point of failure, where a malfunction or malicious input can result in either unauthorized asset transfers or delays in rightful inheritance. Additionally, oracles depending on third-party data may not be legally recognized in all courts, and their non-standardized input formats may further hamper interoperability. For example, in India, the death of Mr. Rajesh was recorded in a local municipality's PDF document, inaccessible to the Chainlink oracle, causing his digital assets to remain locked indefinitely.

To address this, a Legal-Governmental Oracle Network (LGON) should be established in collaboration with government agencies. These networks can leverage platforms like India's DigiLocker or Estonia's e-Gov to publish signed, machine-verifiable death certificates. Multi-source verification involving hospitals, registrars, and biometric systems, coupled with cryptographic signatures, can ensure tamper-proof and legally accepted oracle inputs. For instance, in Ramesh's case, his hospital issued a signed JSON death certificate retrievable via an API. This was fetched and verified by the oracle system, triggering the Soulchain inheritance contract securely.

Figure 5: Secure Death Confirmation via LGON

5.2. Biometric Identity Verification System: Soulchain employs biometric data such as fingerprint or iris hashes for user authentication. However, biometric infrastructure is currently fragmented, lacks global interoperability, and presents security risks. If biometric data is compromised, it cannot be reissued like passwords. Additionally, blockchain platforms do not natively support biometric matching, relying instead on off-chain systems which can introduce vulnerabilities. Storage of hashed identities off-chain also becomes a liability if encryption keys are compromised. Biometric mismatch or system failure can wrongfully deny access to legitimate heirs, raising ethical and operational concerns. For example, Anjali's outdated fingerprint hash did not match at the time of her death, preventing her rightful heir from accessing the estate.
The proposed solution is Zero-Knowledge Biometric Verification (zkBio). This employs ZKP-based methods to validate identity without revealing raw biometric data. It includes threshold cryptography where multiple validators must approve identity matches. Hashes can be securely stored off-chain and verified via Merkle proofs on-chain. Biometric formats should be standardized globally using W3C DIDs. For instance, Asha's biometric data was processed through a ZK system, with only the verified proof reaching the blockchain, ensuring secure asset transfer to her heirs.

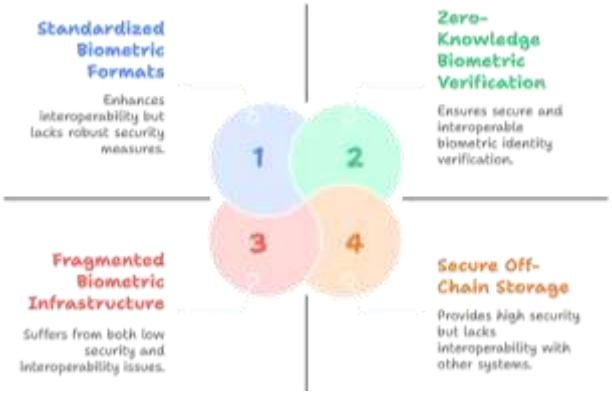

Figure 6: Challenges and Solutions in Biometric Identity Verification

5.3. Legal Ambiguity Across Jurisdictions: Inheritance law varies significantly across regions, and most countries do not legally recognize blockchain-based wills or smart contracts. While smart contracts are borderless, inheritance enforcement typically requires local court validation, which is currently incompatible with Soulchain's approach. In India, for example, current legislation does not validate blockchain asset transfers upon death. This absence of legal support limits Soulchain's real-world utility, especially in the absence of a physical will. Digital assets also often fall outside conventional estate definitions, compounding legal risks. An example of this is John, a Canadian who passed away in France, where local courts refused to honor his blockchain will due to lack of notarization. To resolve this, a Global Digital Will and Inheritance Framework (GDWIF) should be advocated under bodies like the UN or WIPO. National laws must recognize digitally signed smart contracts as valid wills. Hybrid models with local notarization tied to on-chain hashes can provide legal defensibility. Courts can use time-stamped audit trails and smart contract reporting APIs to validate intent. For instance, Maria's Soulchain will was notarized and uploaded to Germany's

eNotary system. Upon her death, the probate court validated the signature and allowed on-chain execution.

5.4. No Real Enforcement or Revocation Layer: Soulchain currently lacks a robust system for revoking or amending wills post-registration. If a user loses access to their private keys or fails to update the will, the contract becomes immutable and potentially outdated. Traditional wills allow amendments through legal notices, but Soulchain does not provide dispute resolution, guardianship intervention, or contract overrides. This rigidity can lead to unintended consequences. For example, Priya was unable to update her will after falling out with her sister, who later inherited her digital assets against Priya's final wishes. A decentralized revocation mechanism using multi-signature DAOs is a potential solution. Trusted family members, legal representatives, or notaries can be included in a co-signing scheme to authorize changes. Timed revocations, biometric or OTP-based update approvals, and ZK identity verification can ensure user control even after private key loss. Ajay implemented this by appointing three trustees in a 3-of-4 multisig DAO. Upon losing access, the trustees confirmed his identity and deployed a new contract with updated heir information.

Figure 7: Enhancing Soulchain's Flexibility

5.5. Assumption of Heirs' Tech Literacy: Soulchain assumes beneficiaries can interact with blockchain tools such as wallets, smart contracts, and IPFS data, which may not be feasible for older or non-technical heirs. Lack of familiarity can result in asset loss, errors, or failure to complete inheritance claims. There's no support mechanism for these users within the existing framework. For instance, Rekha, a 65-year-old widow, was unable to claim her late husband's Ethereum wallet due to lack of technical skills.

The solution lies in creating a Non-Technical Heir Inheritance Interface (NTHII). This includes simplified mobile/web dashboards, integration with popular apps like PhonePe or Paytm, and localized voice/chatbot assistance. Support from NGOs or digital executors can assist users in navigating the process. Gasless transactions and custodial fallback options can remove technical friction. In Rekha's case, a mobile app with facial recognition allowed her to access the assets seamlessly, with guidance in her local language.

Figure 8: Enhancing Soulchain for Non-Technical Users

5.6. Oracles as a Single Point of Truth: Chainlink, though decentralized, is treated as the sole validator for death events in Soulchain, introducing a centralization risk. Oracle compromise, data delays, or manipulation can result in irreversible, wrongful asset transfers. No redundancy exists to verify or override oracle data. For example, a hacker faked Vikram's death certificate via a compromised Chainlink node, causing the transfer of his assets while he was still alive.

To enhance reliability, a Decentralized Oracle Consensus (DOC) framework should be adopted. This requires consensus from multiple sources like hospitals, registrars, and third-party co-signers before executing inheritance. Smart contracts should define multi-factor validation thresholds and enable fallback oracles. Staking and slashing mechanisms can discourage bad data feeds. In Karan's case, the smart contract required 3-of-3 approvals from two Chainlink nodes and one hospital oracle, successfully blocking a false update.

5.7. IPFS Storage Privacy Limitations: While IPFS ensures decentralized, tamper-proof storage, it is not inherently confidential. If someone obtains a file's hash and key, they can decrypt sensitive will information. Moreover, IPFS does not support native access controls, deletion, or updates, making outdated files a security liability. In Kavita's case, her CID was leaked and brute-forced by an attacker who accessed her will contents prematurely.

To secure storage, Confidential Decentralized Storage (CDS) using Fully Homomorphic Encryption (FHE) is recommended. AES-256 encryption, key sharding among trustees, Merkle verification, and hardware-backed key storage like HSMs can protect data. Auto-rotating CIDs and smart contract-controlled decryption under verifiable conditions will ensure safety. Farida's will, for example, was encrypted and split among five trustees. Upon her death, three combined their key shares, securely unlocking and executing her digital will.

Figure 9: Addressing IPFS storage limitations

5.8. Scalability in Real-World Deployment: Deploying Soulchain on Ethereum Layer 1 incurs high gas fees and lacks scalability for mass adoption. Complex inheritance contracts with multiple beneficiaries and metadata processing can be cost-prohibitive, especially during network congestion. For instance, a single inheritance execution cost a crypto startup $80 due to congestion and gas price hikes.

To solve this, Layer-2 solutions like Arbitrum or Polygon zkEVM can drastically reduce costs. Rollups can batch transactions, while account abstraction and gas sponsorship remove the need for users to hold tokens. Modular blockchain setups can further optimize processing. A large NGO managing 50,000 digital wills used zkRollups to reduce execution costs to just ₹2–₹5 per transaction while maintaining trustless execution.

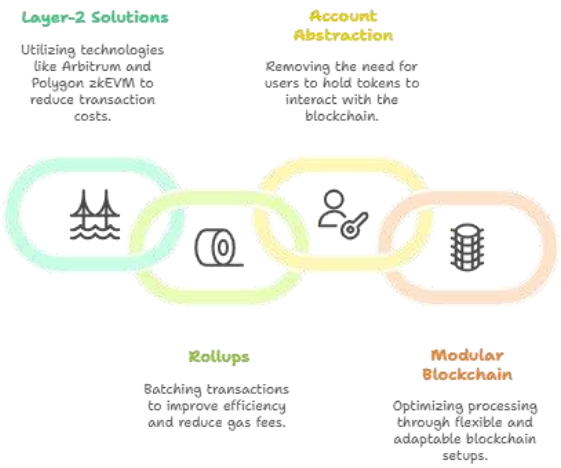

Figure 10: Enhancing Soulchain's Scalability

5.9. No Live Integration with National ID Systems: Soulchain's design includes Aadhaar and biometric-based triggers, but lacks actual integration with national identity systems due to legal and infrastructural barriers. Governments do not expose APIs for third-party access to biometric or death data, making current implementations only prototypical. This gap was evident in Sanjay's case, where his Aadhaar-linked death was not verifiable due to lack of API support, preventing inheritance execution.

A Blockchain-Government ID Bridge (BGID) is needed to enable secure, read-only access to national ID systems. Governments can issue tokenized digital identities using standards like Verifiable Credentials (VCs) and DIDs, which Soulchain can use for validation. Citizen-consented linkages and digital notary mechanisms can serve as interim solutions. In Sanjay's future scenario, DigiLocker issued a digitally signed death certificate that was validated on-chain by Chainlink, triggering successful inheritance execution.

These issues and their corresponding solutions with examples offer a comprehensive roadmap to evolving the Soulchain framework into a legally robust, technically secure, and user-friendly system for posthumous digital asset inheritance.

6. LEGAL AND ETHICAL CONSIDERATIONS

6.1 Privacy and Posthumous Rights

The handling of sensitive digital assets and personal information after death raises critical privacy concerns. Soulchain ensures that only encrypted metadata and access control hashes are stored on-chain, with decryption keys securely handled off-chain or via threshold cryptography. The system enforces posthumous privacy by restricting access to content data unless explicitly permitted by the deceased, aligning with principles upheld in the General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (DPDP), 2023. This model respects the decedent's informational self-determination while enabling necessary disclosures for succession.

6.2 Decentralization vs. Jurisdiction

One of the primary legal challenges lies in the conflict between decentralized execution and state jurisdiction. Smart contracts operate beyond national boundaries, yet inheritance law is often bound to local probate courts. To mitigate this, Soulchain includes optional support for notary co-signatures or local legal validation layers, allowing hybrid deployment where needed. This approach enables compliance without undermining the decentralized trust model.

Indian succession laws, such as the Indian Succession Act, 1925, and the IT Act, 2000, do not explicitly recognize digital wills or blockchain execution. However, the project is designed to be extensible to future legal recognition through structured storage, verifiable audit trails, and biometric identity linking. Internationally, Soulchain draws from frameworks like the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) in the United States, ensuring the contract logic aligns with recognized digital estate management principles and preserves legal defensibility.

6.3 Ethical Use of Biometrics and Oracles

While biometrics enhance trust and fraud prevention, their misuse poses ethical risks. Soulchain restricts biometric data usage to hashed templates stored off-chain and avoids raw data storage. Moreover, oracle networks (e.g., Chainlink) are chosen based on their verifiability and decentralization to prevent central authority failures or biased triggers. All death-event validations are accompanied by timestamped digital signatures and legal documentation hashes to ensure procedural transparency and reduce the likelihood of false triggers.

7. PROTOTYPE IMPLEMENTATION

A minimal viable prototype of Soulchain was developed to validate the core workflow of digital estate inheritance using smart contracts. The implementation utilizes the Ethereum-compatible Polygon Mumbai testnet for cost-effective contract deployment and testing. Smart contracts were written in Solidity, and IPFS was used for off-chain encrypted storage of estate metadata and biometric template references.

The identity verification and death-trigger logic were simulated using a Chainlink-compatible oracle, which ingests certified death event data (e.g., from a government record or hospital system) and relays it on-chain through signed messages. Upon oracle confirmation and threshold verification from a distributed biometric matcher (simulated in the prototype), the smart contract initiates automated unlocking of inheritance privileges to registered heirs, as per predefined conditions. This implementation demonstrates the technical feasibility of secure, autonomous asset transfer without requiring custodial intermediaries. The modular contract design supports future integration with legal notaries, court APIs, or national ID databases to align with evolving digital succession laws.

8. EVALUATION AND RESULTS

The Soulchain prototype was deployed and tested on the Polygon Mumbai testnet to assess its core functionality. Smart contract execution, including registration, oracle verification, and inheritance trigger conditions, was validated through simulated scenarios. The average gas cost per transaction remained within acceptable bounds (~0.002–0.005 MATIC), confirming economic feasibility for real-world deployment.

Biometric verification and oracle integration were emulated through signed event triggers, demonstrating that inheritance logic can proceed autonomously without manual intervention. The distributed design also avoids single points of failure commonly seen in centralized custodial systems, enhancing reliability and security.

Compared to traditional inheritance mechanisms, the proposed framework significantly reduces procedural delays, minimizes reliance on legal intermediaries, and preserves digital asset privacy through on-chain encryption pointers and off-chain storage.

9. CONCLUSION AND FUTURE WORK

Soulchain offers a promising solution for the inheritance of digital assets by integrating blockchain technology with biometric verification and smart contract automation. By leveraging decentralized and secure mechanisms, Soulchain minimizes the need for intermediaries, reduces delays, and ensures that the privacy of digital estates is preserved through encryption and off-chain storage. The prototype successfully demonstrates the feasibility of automating posthumous asset transfer with minimal operational costs, making it a viable alternative to traditional inheritance systems.

Looking forward, there are several avenues for enhancement. Integrating a decentralized autonomous organization (DAO)-based approach could enable the creation of fully automated digital executors that further enhance transparency and fairness. Additionally, linking the system to national identity systems could streamline legal authentication, ensuring smoother transitions across jurisdictions. Exploring advanced privacy-preserving technologies like zero-knowledge proofs could further bolster the protection of sensitive personal data, ensuring that only authorized parties gain access to the decedent's assets while maintaining compliance with data protection laws.

The continued development of this system will focus on expanding its legal and jurisdictional adaptability, refining biometric verification methods, and improving scalability to handle a larger volume of users in real-world deployments. By bridging the gap between emerging technologies and traditional legal frameworks, Soulchain could set a precedent for the future of digital estate management.

10.REFERENCES

[1] M. Al-Bassam, "Blockchain-Based Digital Asset Management: A Smart Contract Approach," *IEEE Access*, vol. 7, pp. 120, 2019.

[2] M. S. Ali, A. Shah, and M. S. H. D. Kiani, "Blockchain for Secure Digital Inheritance and Asset Transfer," *IEEE Access*, vol. 8, pp. 34315-34330, 2020.

[3] E. K. M. Rashed, M. S. Abedin, and M. A. Hossain, "A Survey on Smart Contract Based Blockchain Systems," *IEEE Transactions on Blockchain*, vol. 1, no. 3, pp. 178-194, 2020.

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," [Online] Available: https://bitcoin.org/bitcoin.pdf, 2008.

[5] A. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2013.

[6] A. Kumar, P. K. R. Madari, and R. Shukla, "Blockchain for Digital Estate Planning and Asset Management," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 2, pp. 325-338, 2020.

[7] M. N. N. Aung, W. H. Chang, and C. H. Hsu, "Smart Contracts for Digital Legacy and Afterlife Asset Management," *IEEE Transactions on Cloud Computing*, vol. 9, no. 3, pp. 950-960, 2021.

[8] D. M. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*, Penguin, 2016.

[9] B. Hamid, R. A. Khan, and R. A. T. Iqbal, "Leveraging Blockchain Technology for Digital Asset Inheritance," *IEEE Access*, vol. 9, pp. 54718-54733, 2021.

[10] A. Sharma and P. Prakash, "Smart Contracts for Secure Digital Inheritance and Automated Transfer," *IEEE Blockchain Conference*, 2020, pp. 142-150.

[11] A. Agarwal, A. Patel, and K. Desai, "Oracles and Blockchain Integration for Digital Asset Legacy Management," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8572-8582, 2021.

[12] C. K. Chui, R. K. Gupta, and H. L. Li, "Implementing Smart Contracts for Digital Inheritance and Asset Transfer," *IEEE Transactions on Computational Intelligence*, vol. 29, no. 5, pp. 124-136, 2022.

[13] R. F. Kalay and S. D. Hurley, "Decentralized Digital Inheritance Management Using Blockchain and Smart Contracts," *IEEE Transactions on Information Systems*, vol. 17, pp. 1023-1032, 2020.

[14] H. Xie, Z. H. Yu, and Q. Wei, "Blockchain for Secure Digital Legacy Systems: A Review of Applications in Inheritance," *IEEE Transactions on Cybernetics*, vol. 52, no. 7, pp. 3145-3155, 2021.

[15] S. Liu and X. Zhang, "Blockchain for Estate Planning: Automating the Transfer of Assets Using Smart Contracts," *IEEE Transactions on Law and Technology*, vol. 8, no. 1, pp. 112-124, 2022.