Decentralized Inheritance Protocol

Smart Contract for Crypto Asset Inheritance

Noah Klaholz Vincent Schall Max Mendes

University of Basel

November 2025

Outline

The Problem

- **3.7 million Bitcoin** are estimated to be lost and unrecoverable
- Major cause: owners passing away without sharing access
- Traditional inheritance systems are:
  - Slow (months to years)
  - Expensive (legal fees, court costs)
  - Prone to conflict

Question: What happens to your crypto when you die?

The Decentralized Inheritance Protocol

Key Features:

- Deploy personal will contract
- Define beneficiaries with percentages
- Automated state machine
- Yield generation via Aave
- Death verification by notary

Benefits:

- No intermediaries
- Transparent rules
- Assets grow over time
- Immediate distribution

State Machine

$$\texttt{ACTIVE} \rightarrow \texttt{WARNING} \rightarrow \texttt{VERIFICATION} \rightarrow \texttt{DISTRIBUTION}$$

- **ACTIVE**: Normal operation, owner manages funds
- **WARNING**: Missed check-in (90 days), 30-day grace period
- **VERIFICATION**: Awaiting death certificate from notary
- **DISTRIBUTION**: Automatic payout to beneficiaries

`updateState()` is public – anyone can trigger transitions

Access Control & Security

Roles:

- **Owner**: Manage beneficiaries, deposit/withdraw, check-in
- **Notary**: Upload death verification only

Security Measures:

- OpenZeppelin's `Ownable` and `ReentrancyGuard`
- Phase guards (`onlyPreDistribution`, `onlyActiveWarning`)
- Bounded iteration (max 10 beneficiaries)
- Solidity 0.8.x overflow protection

Funds Management

- Accepts ERC-20 tokens (USDC)
- Deposits supplied to Aave lending pool
- Earns yield while waiting (2-6% APY on stablecoins)
- Fully liquid – owner can withdraw anytime

Example: $100,000 at 4% for 10 years = $148,024

Distribution Logic

- Up to 10 beneficiaries with percentage shares
- Total must not exceed 100%
- On distribution:
  1. Withdraw all funds from Aave
  2. Calculate each beneficiary's share
  3. Transfer tokens to each address
- Residual (if $< 100\%$) sent to notary for legal distribution

Key Trade-offs

Removed: Vesting Schedules

- Requires off-chain automation (Chainlink Keepers)
- Adds recurring costs and complexity
- Focus on core value: preventing total asset loss

Manual State Transitions

- No automation fees over years/decades
- Beneficiaries incentivized to call `updateState()`

Single Notary

- Simpler than multi-sig
- Narrowly scoped permissions

Technology

Smart Contracts:

- Solidity 0.8.28
- Hardhat v3
- OpenZeppelin Contracts
- Hardhat Ignition

Frontend & Testing:

- TypeScript / React
- Next.js
- Mocha / Chai
- ESLint

Limitations & Future Improvements

- **Single-asset**: Extend to multiple ERC-20 tokens
- **Max 10 beneficiaries**: Dynamic array with gas optimization
- **Oracle centralization**: Multi-party notaries or decentralized attestation
- **Automation**: Optional Chainlink Keepers integration
- **UX**: EIP-2612 permit for gasless approvals

Live Demo

Demo of the Inheritance Protocol Client

- Connect wallet
- Deposit funds
- Add beneficiaries
- Check-in mechanism
- State transitions

Questions?

Q & A