Decentralized Inheritance

Protocol: Securing Your Crypto Legacy

Max Mendes, Noah Klaholz, Vicent Schall

University of Basel, November 21, 2025

The Problem

Understanding Crypto Inheritance Issues

Lost Crypto Assets

An estimated **3.7 million Bitcoin** are lost forever due to lack of inheritance access, highlighting the critical need for effective solutions to safeguard digital assets for future generations.

Importance of Decentralized Inheritance

Accessibility

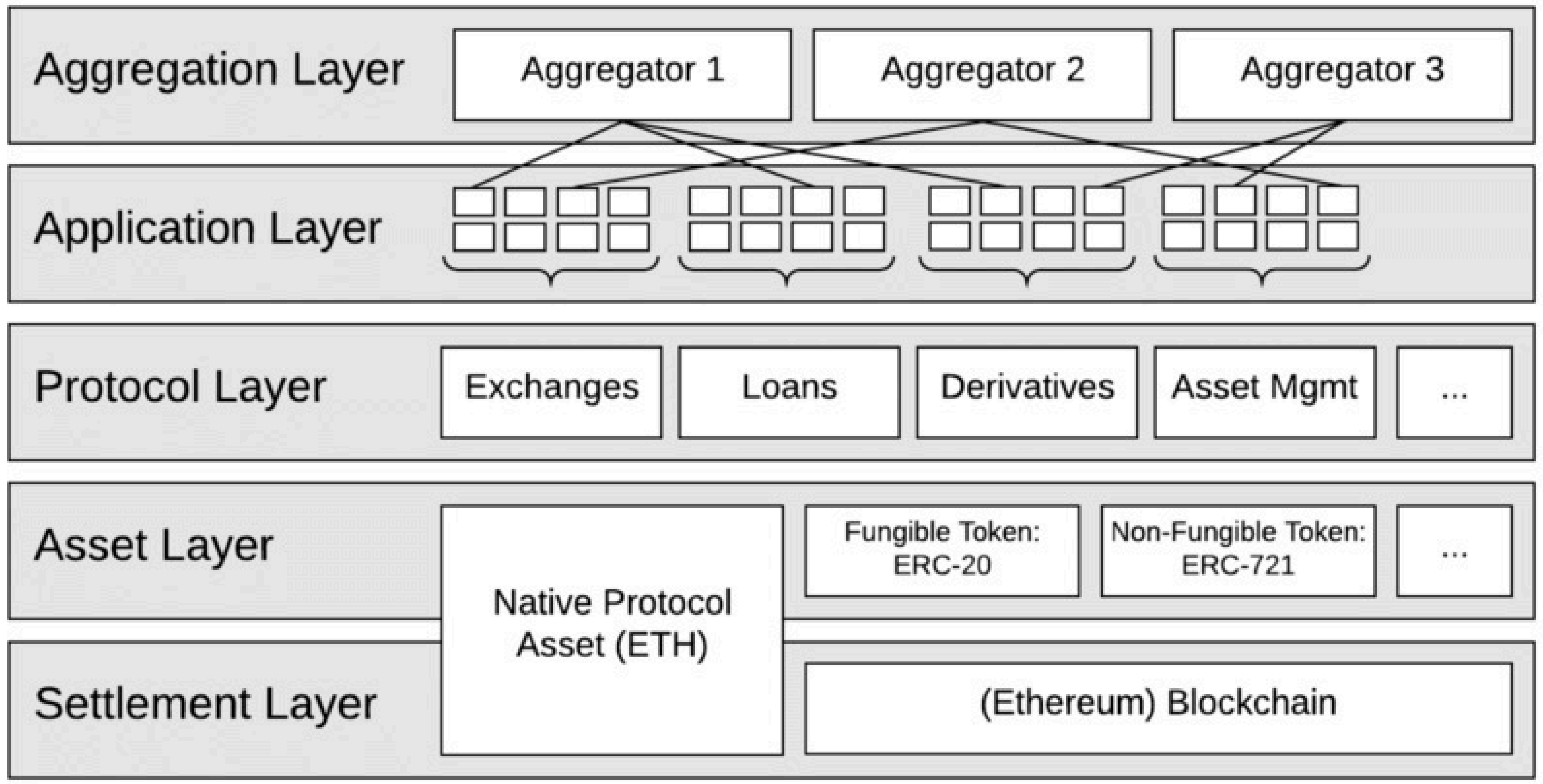
A decentralized solution ensures **inheritance accessibility**, allowing beneficiaries to easily claim assets without bureaucratic delays or legal hurdles that can hinder traditional inheritance processes.

Efficiency

Traditional inheritance methods often involve lengthy legal processes, making them slow and costly. A decentralized approach streamlines asset transfer, providing immediate access to crypto holdings for the heirs.

Solution Overview

The Decentralized Finance Stack



Aggregation Layer

Aggregator 1

Aggregator 2

Aggregator 3

Application Layer

Protocol Layer

Exchanges

Loans

Derivatives

Asset Mgmt

...

Asset Layer

Native Protocol Asset (ETH)

Fungible Token: ERC-20

Non-Fungible Token: ERC-721

...

Settlement Layer

(Ethereum) Blockchain

Smart Contracts

The Decentralized Inheritance Protocol utilizes smart contracts to automate the inheritance process, ensuring **transparency and efficiency** while eliminating intermediaries, thus reducing costs and potential conflicts.

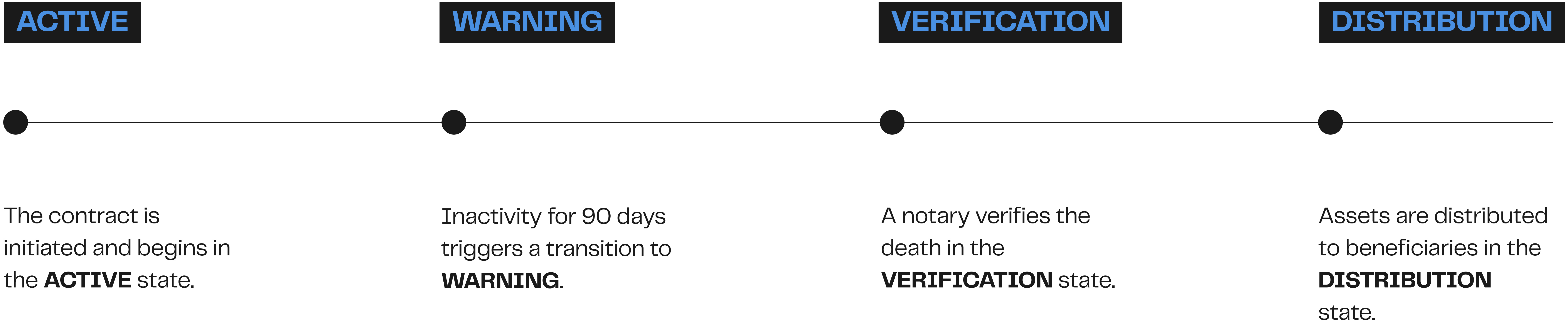
Beneficiary Shares

This protocol allows for **up to 10 beneficiaries** with designated percentage shares, facilitating clear asset distribution and inheritance management, ensuring that each beneficiary receives their rightful share seamlessly.

Automated Processes

By implementing **automated state transitions** within the protocol, the system enhances user experience and ensures timely distribution of assets, providing peace of mind to crypto asset holders and their families.

Smart Contract Lifecycle



ACTIVE

WARNING

VERIFICATION

DISTRIBUTION

The contract is initiated and begins in the **ACTIVE** state.

Inactivity for 90 days triggers a transition to **WARNING**.

A notary verifies the death in the **VERIFICATION** state.

Assets are distributed to beneficiaries in the **DISTRIBUTION** state.

Access Control

Owner vs Notary Responsibilities

Owner Responsibilities

The owner manages the smart contract, creating the will and selecting beneficiaries, ensuring transparency and immediate access to assets, thus avoiding traditional probate delays and complications.

Notary Responsibilities

The notary verifies the owner's death and triggers asset distribution, ensuring legal compliance and upholding the integrity of the process, preventing unauthorized access or fraudulent claims.

Funds Management: Earn Yield

Yield

Deposits earn **competitive yield** ranging from 2% to 6% APY.

Liquidity

Funds remain **fully liquid** and accessible for owner withdrawal anytime.

Growth

Example: $100k grows to **$148,024** over ten years at 4%.

Distribution Logic

Beneficiary Shares

Up to 10 beneficiaries can be assigned percentage shares.

Fund Withdrawal

Withdrawals from Aave will be calculated for distribution.

Legal Handling

Residual funds are managed by the notary for legal purposes.

Design Trade-offs

Balancing Choices

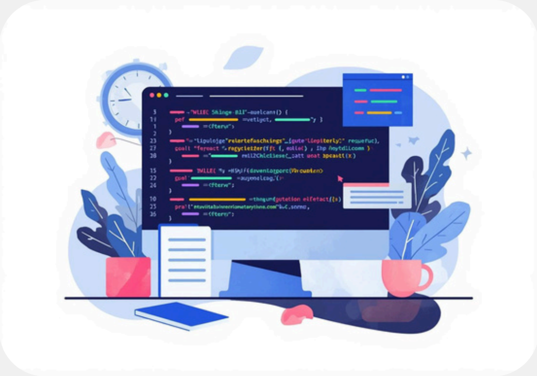
Assessing simplicity vs complexity in protocol design.

Navigating Options

Exploring the impact of choices on user experience.

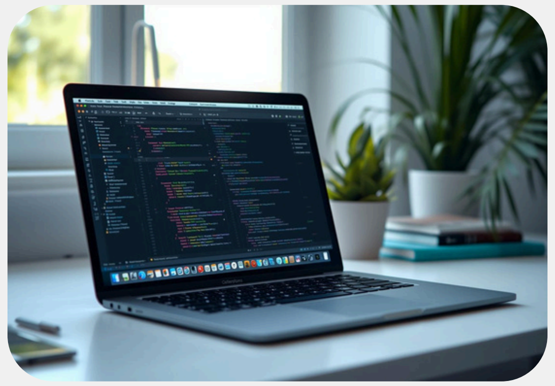
Technology Stack

Tools and Frameworks Used



Frontend Development

Leveraged React and TypeScript for building user-friendly interfaces, enhancing user experience through responsive design and functionality.



Smart Contract Development

Utilized Solidity and OpenZeppelin for secure smart contract creation, ensuring reliability and safety in crypto transactions.

Limitations and Future Work

Multiple Tokens

Expanding support for **multiple ERC-20 tokens** would enhance flexibility, allowing users to manage diverse assets seamlessly within the decentralized inheritance framework, accommodating a broader range of cryptocurrency holdings.

Dynamic Arrays

Implementing **dynamic beneficiary arrays** would enable users to add more than ten beneficiaries, enhancing the protocol's adaptability and accommodating complex family structures, ensuring fair distribution of assets.

Decentralized Notary

Developing a **multi-party or decentralized notary system** could improve trust and reliability, facilitating smoother transitions in inheritance processes while minimizing the risk of disputes among beneficiaries.

Automation

Integrating **Chainlink Keepers** for automated state transitions could streamline the protocol, reducing manual intervention and ensuring timely updates, ultimately enhancing user experience and system efficiency.

UX Improvements

Implementing **gasless approvals** (EIP-2612) would simplify user interactions, enabling seamless transactions without gas fees, thereby attracting a wider audience by lowering barriers to entry in crypto inheritance management.

Enhanced Security

Continuous enhancement of **security measures** is vital, focusing on proprietary techniques to safeguard funds and data against emerging threats, thus ensuring users can confidently rely on the protocol for their inheritance needs.

Live Demo

Demonstrating the Decentralized Inheritance Protocol