A Blockchain-based Dead Man's Switch Storage System

dWill
Your will, at your fingertips.

School of Computer Science, University Of Nottingham Malaysia

Anshana Manoharan, Adyan Dean bin Wafdi Kamil, Carmel Natasha Barnabas, Lai Ken Siang, Dr El Ioini Nabil

BLOCKCHAIN

dWill offers a sophisticated **decentralized** storage solution that is deployed on a blockchain. It offers users the capability to designate beneficiaries for a *secure*, *streamlined* transfer of assets in the event of unforeseen circumstances.
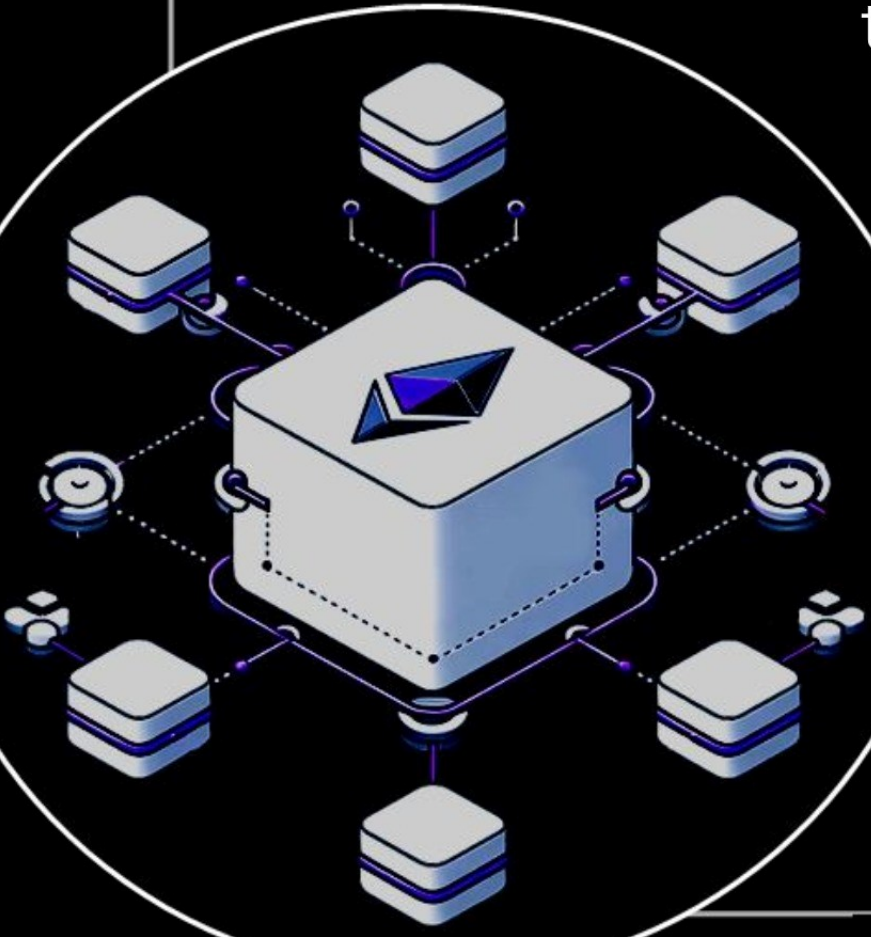
USERS

A **benefactor** is responsible for allocating files and beneficiaries.
A **beneficiary** is responsible for triggering countdowns and collecting their assets when the benefactor is incapacitated.
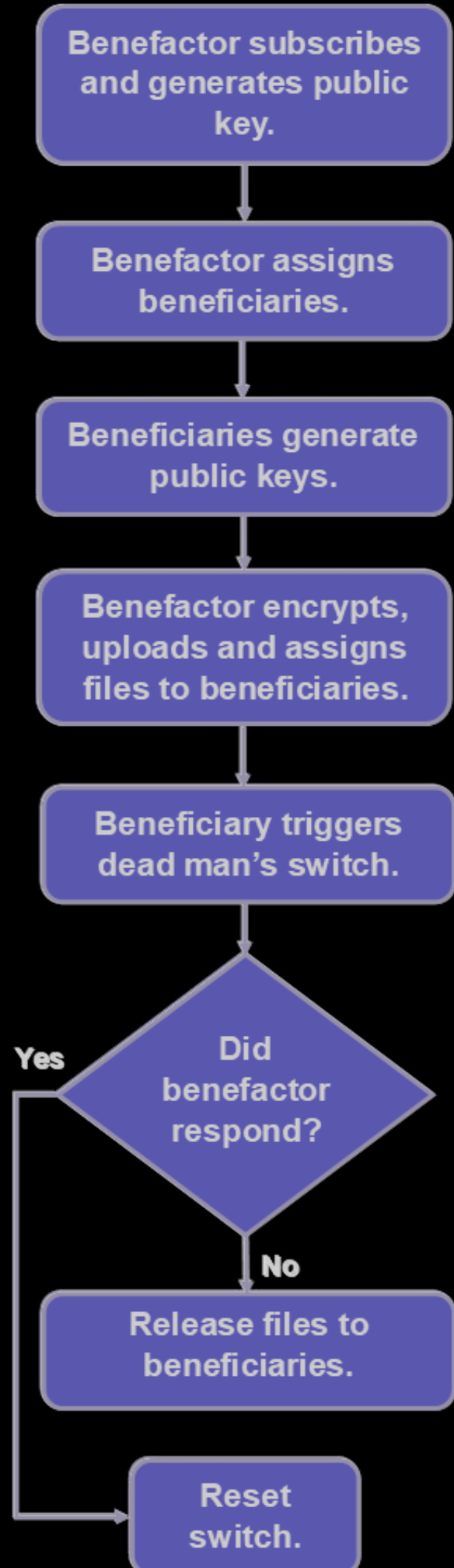
SMART CONTRACTS

1. **dWill** utilises a **subscription** contract enabling users to become benefactors.
2. The **dead man's switch** contract uses a **benefactor-beneficiary** framework.
3. The **upload** contract ensures the files are uploaded to IPFS (a distributed file storage system).

APP FLOW

- Benefactor subscribes and generates public key.
- Benefactor assigns beneficiaries.
- Beneficiaries generate public keys.
- Benefactor encrypts, uploads and assigns files to beneficiaries.
- Beneficiary triggers dead man's switch.
- Did benefactor respond?
  - Yes
  - No → Release files to beneficiaries. → Reset switch.

Dead Man's Switch

Allows beneficiaries to trigger a countdown if the benefactor has been inactive. It triggers the release of assets to the beneficiaries if no response recorded.

ENCRYPTION

To ensure security, public keys are exchanged through the **Diffie-Hellman Key Exchange Algorithm.** Files are encrypted when uploaded and their respective hashes are also encrypted upon storing in the smart contract.

ARCHITECTURE

Internet

IPFS Storage

User → Browser → Front-end (HTML, CSS, React, Vite, Typescript) ⇅ Providers (Ethereum, Thirdweb, Polygon, Pinata) → Ethereum Blockchain (Smart contracts) → Ethereum Virtual Machine

Authentication MetaMask

thirdweb · Pinata · METAMASK · ethereum · polygon