FOSDEM
1 & 2 February, Brussels 2025

Trustchain

Trustworthy Decentralised Public Key Infrastructure

Tim Hobson

Alan Turing Institute

Pam Wochner

TU Delft

Sam Greenbury

Alan Turing Institute

Trustchain Design Goals

Aims and motivation

Aims:

- Public Key Infrastructure (PKI) with no trusted third parties
- Full end-user verifiability
- Free and open access for any user community

Use cases:

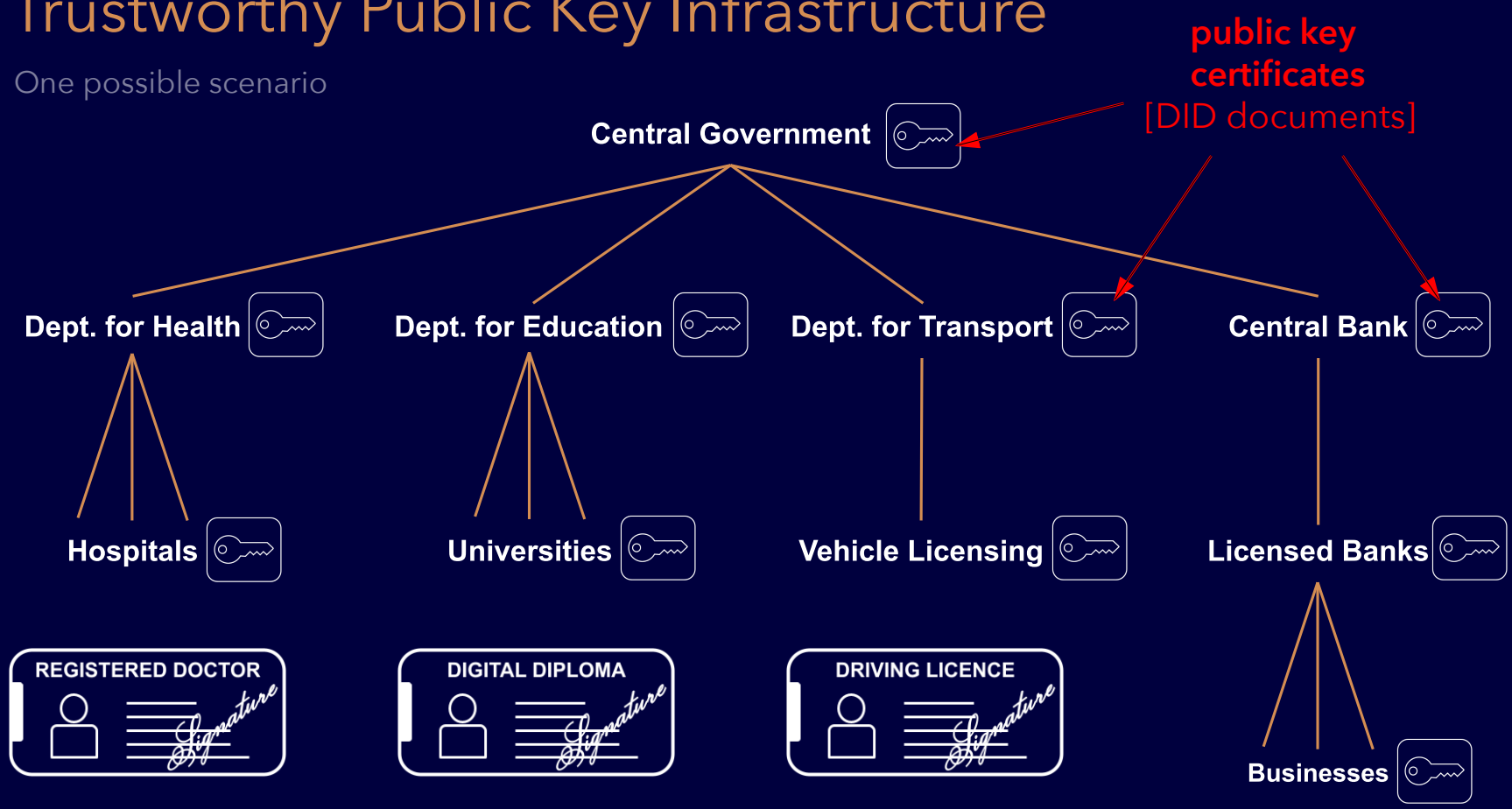
- Trustworthy digital ID
- Verifiable URLs
- Data provenance
- Secure communications

Motivation:

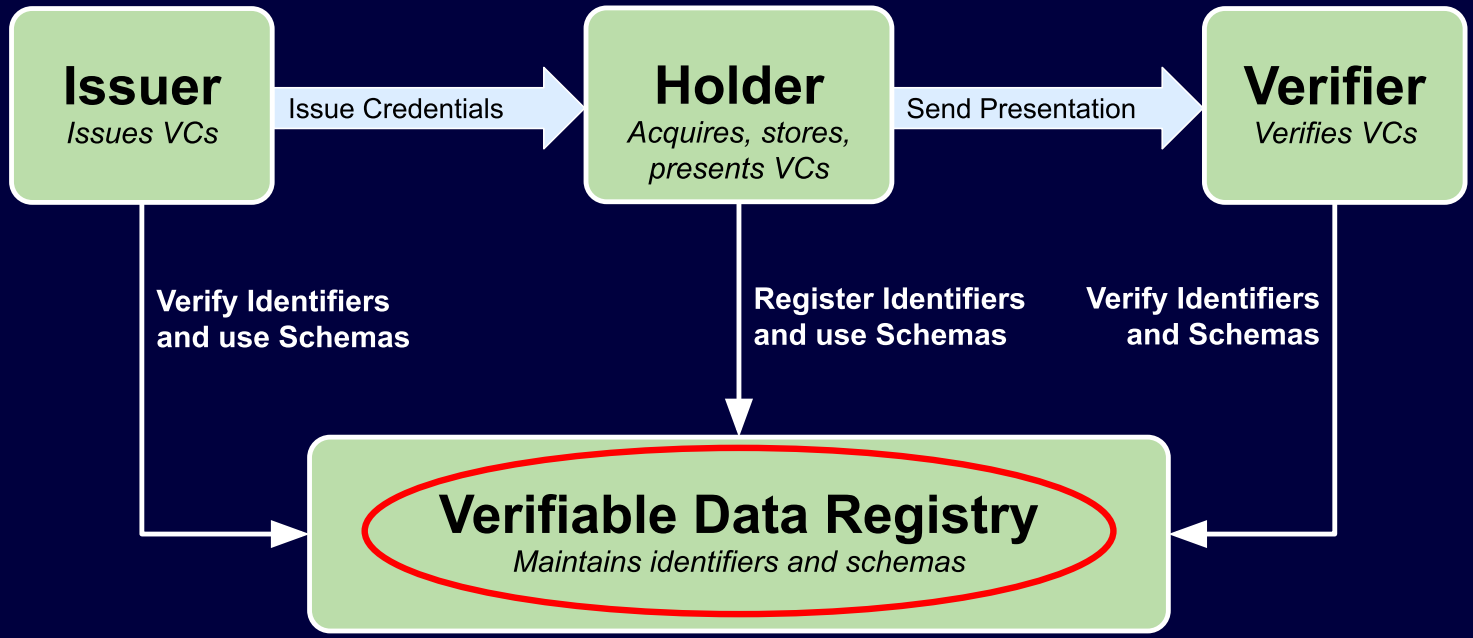
Build an open, decentralised alternative to risky, centralised digital ID.

Trustworthy Public Key Infrastructure

One possible scenario



Verifiable Credentials & Decentralised Identifiers



Decentralised PKI requires end-user verifiability

Verifiable Data Registry for Decentralised PKI

What types of information can be verified cryptographically?

1. Digital signatures

necessary, not sufficient

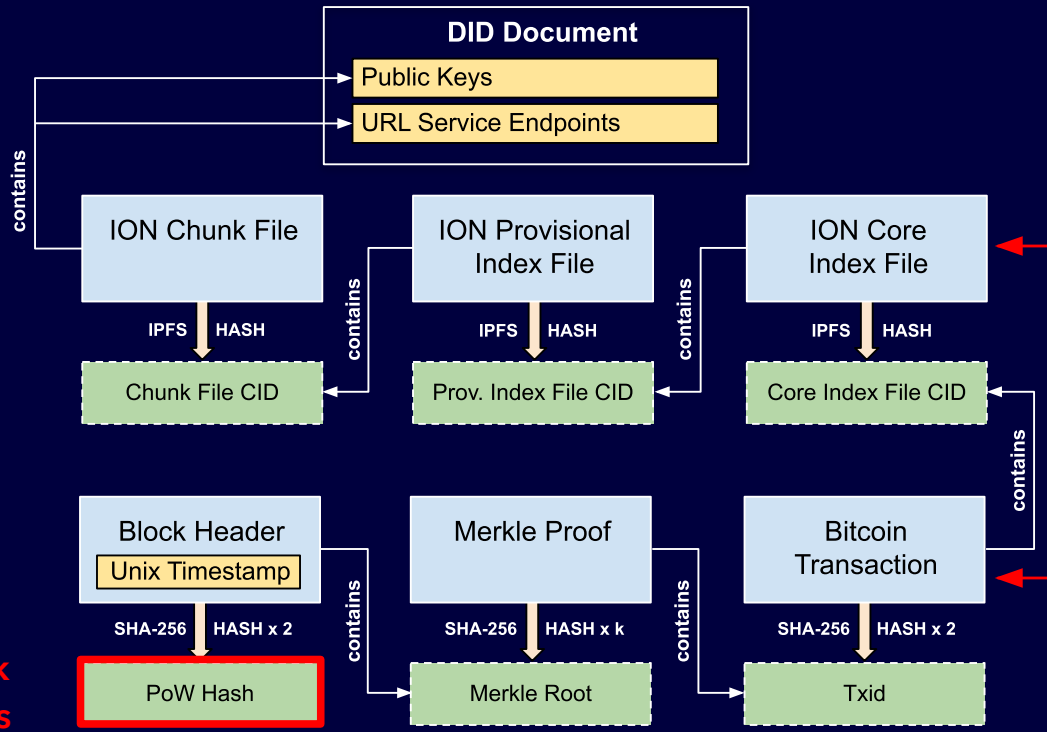
2. Hash digests

necessary, not sufficient

3. Timestamps

Timestamp Verification for DIDs in Trustchain

How to cryptographically verify that certain public keys were published on a given date

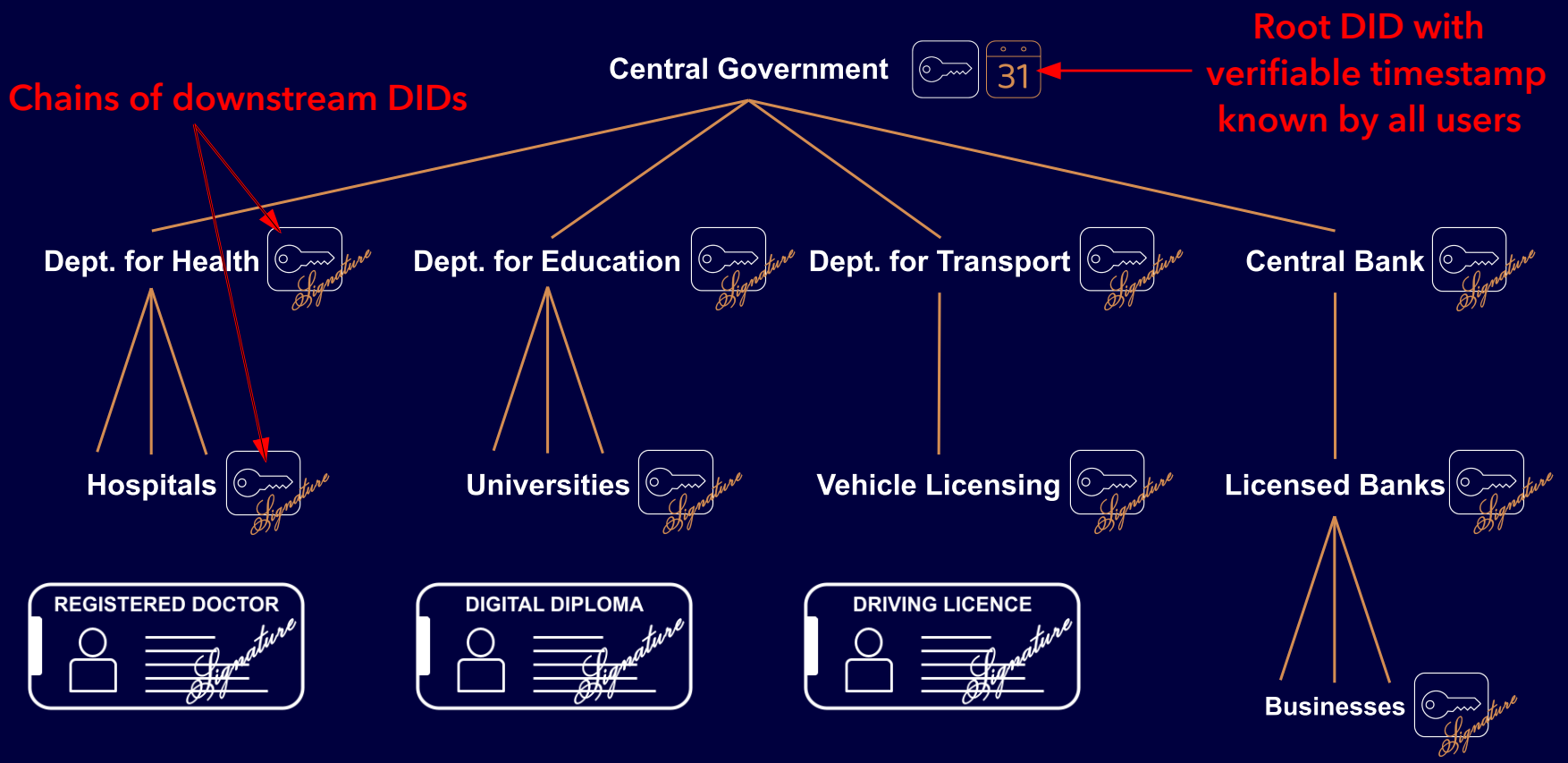


DIDs published by ION are written to IPFS

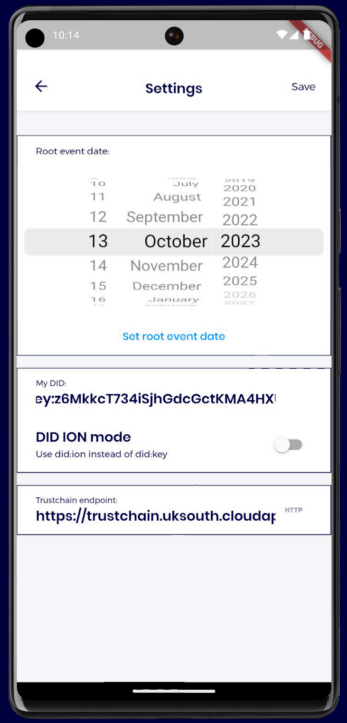
and hashed into a Bitcoin transaction

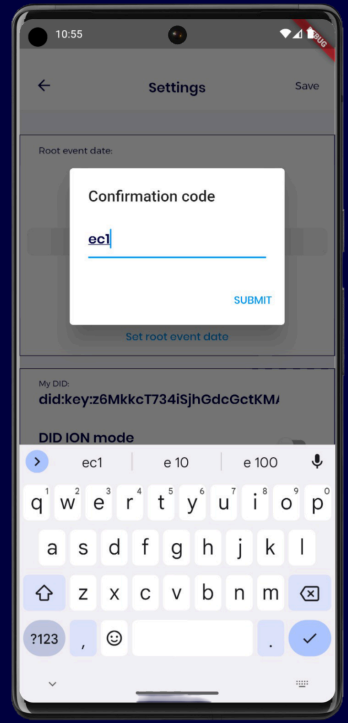
Bitcoin P2P network hash rate ~800 EH/s

Trustworthy Decentralised PKI with Trustchain

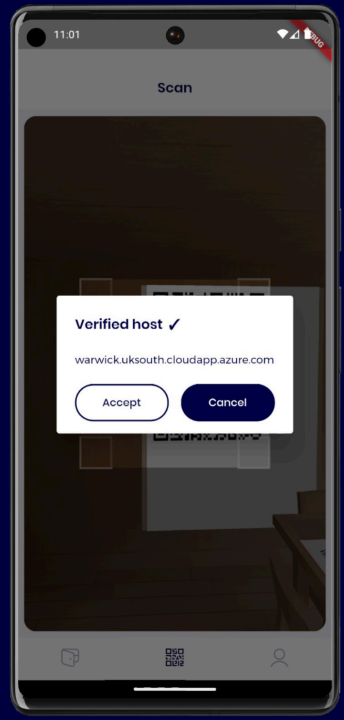


Trustchain Mobile UX





Enter the root DID date



Verify dDID chains, URLs & credentials

Trustchain Tech Stack

- Rust

github.com/spruceid/ssi

github.com/rust-bitcoin

- ION

- Dart

github.com/spruceid/wallet

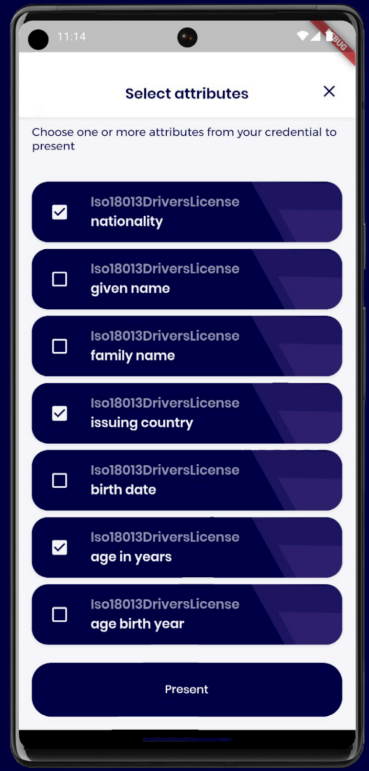
Trustchain Features

Full node:

- **Challenge-response protocol** for dDID issuance
- Unilateral dDID revocation from upstream & DID recovery from downstream
- Verifiably **complete revocation lists**
- **Interoperability** between dDID networks
- Built-in HTTP server for handling mobile requests and credential issuance
- Constrained VC and dDID issuance (in development)

Mobile wallet app:

- **Selective disclosure** via Redactable Signature Scheme
- Offline device-to-device presentation & verification via QR codes
- Light Bitcoin node for Simplified Timestamp Verification (in development)



Come & talk to us

- Developers
- Potential users

Visit the Trustchain Docs site for
code, install guide, how-to, FAQ, etc.

https://alan-turing-institute.github.io/trustchain/