Private Digital Identity on Blockchain

Tom Hamer, Kerry Taylor, Kee Siong Ng, Alwen Tiu

Australian National University

The Global Identity Crisis

- In order to access critical services such as finance and social security, people need to have an identity
- **1.5 billion** people do not have an officially recognized identity
- The UN sustainable development goals include “ensure a unique legal identity and enable digital ID-based services to all”

Problems with current identity systems

- Getting a new identity document requires a previous identity document
- Individuals can be linked across multiple independent uses of their identity, without consent: *Linkability*
- Basic attributes such as address cannot easily be cancelled or changed and so a fresh identity is very hard to establish.

Aahaar project

- Over 1.2 billion citizens have been registered
- Each individual has one identity number, which creates linkability
- Not interoperable with other identity systems

Blockchain and Identity

Source: Hyperledger Indy

Blockchain provides a mechanism to prove claims about identity, such as a shared ledger for the exchange of public keys, revocation of claims and proof parameters

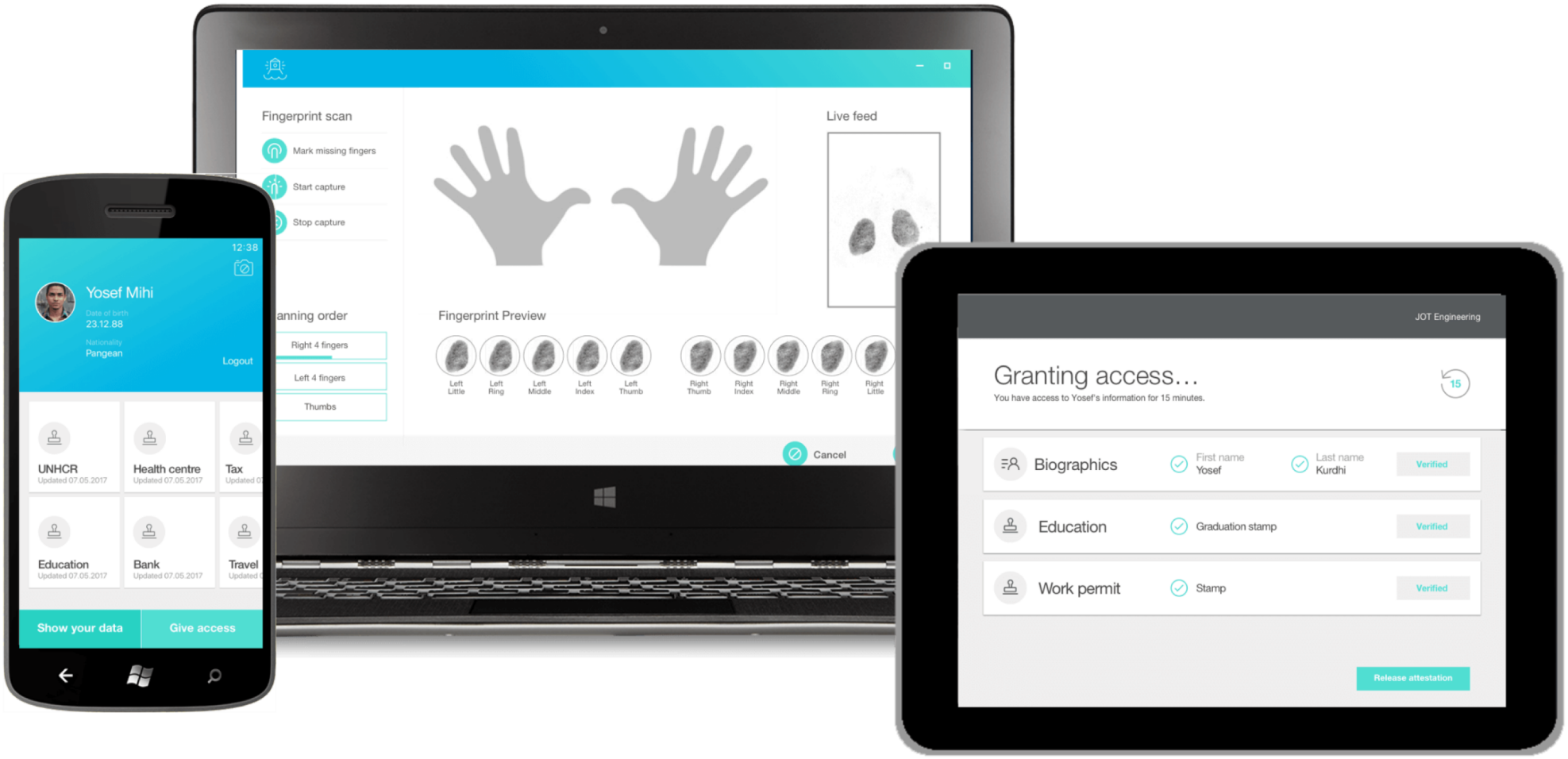
This is can be done with no central authority

Self-sovereign Identity

- Individuals have ownership of their identity, and control over how their personal data is used *for the purposes of identity*

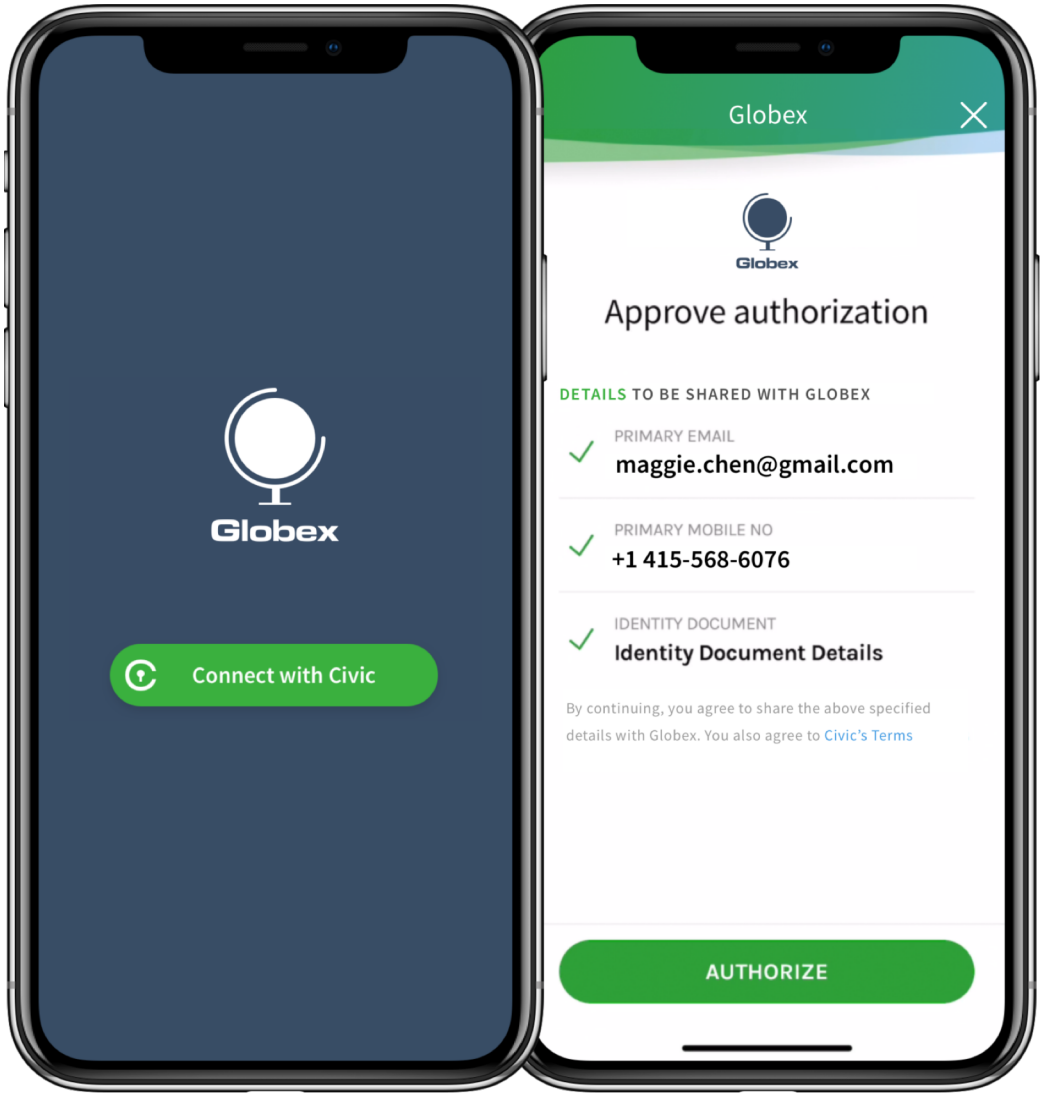
- Minimal disclosure of identity (via mechanisms such as zero knowledge proof)

Self-sovereign Identity – ID2020



Source: ID2020

Self-sovereign Identity - Civic



Source: Civic

Unique Self-sovereign identity

USI means that a user can have at most one identity in a particular context, but identities cannot be linked between contexts without permission from the user.

Context is defined by a shared business or organisational function which requires transactions to be linked

Biometrics - Background

Biometrics have the capacity to produce a unique identifier for each individual

However, biometric technology has a drawback - if it is stolen you can be impersonated or linked across contexts

How to Achieve USI

Strategy: *combine biometrics and cryptography to achieve USI*

Cancelable Biometrics

- *Cancelable biometrics* are a method for obfuscating biometric signatures when they are stored through applying a non-invertible function

Biometric Verification vs Identification

Verification: 1-to-1 matching in biometrics. *Verifies you are who you say you.*

Identification: 1-to-n matching in biometrics. *Discovers who you are by comparing biometrics to existing biometrics in a database.*

Issue: *cancelable biometrics rely on the user trusting the other party to correctly apply the transformation/store the biometrics.*

Solution: we propose allowing the user to transform their own biometric themselves

Verifiable Claims - Background

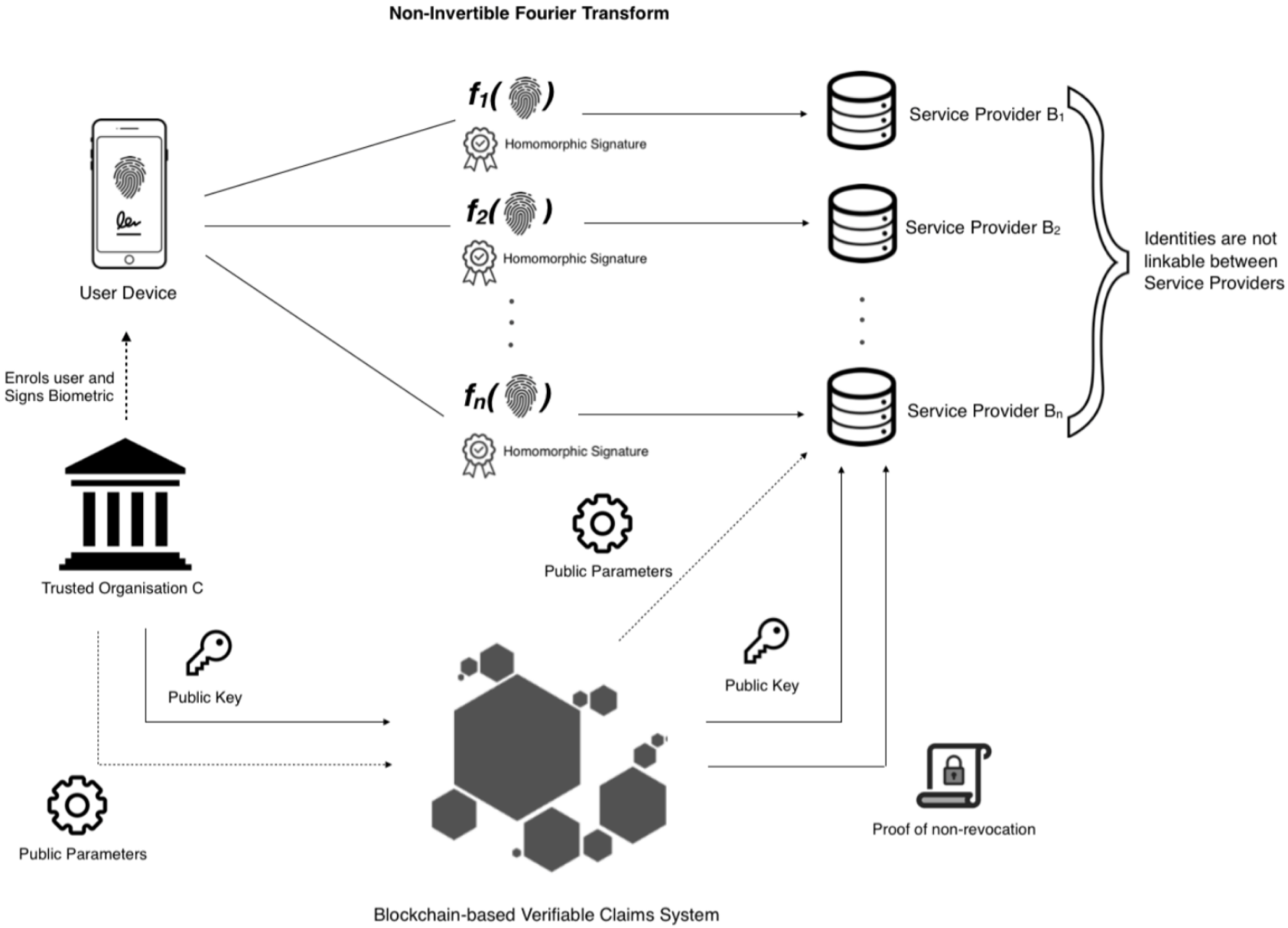
- Verifiable Claims are a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable
- We use verifiable claims to let the user assert ownership over an already transformed biometric signature

Homomorphic Signatures - Background

- Homomorphic signatures allow a verifier to prove that a calculation has been done correctly without having to access the underlying data
- We employ homomorphic signatures as the proof mechanism for the verifiable claims of the transformed biometrics

Combining Cancelable Biometrics and Homomorphic Signatures to achieve USI

- The user is able to transform their own biometric using a partial discrete Fourier Transform and prove that they have transformed it correctly
- The proof is via a homomorphic signature, as theorized by Gorbunov et al (STOC 2015 – 47th ACM Symposium on the Theory of Computing)


Non-Invertible Fourier Transform
$f_1($)
Homomorphic Signature
$f_2($)
Homomorphic Signature
$f_n($)
Homomorphic Signature
Service Provider B_1
Service Provider B_2
Service Provider B_n
Identities are not linkable between Service Providers
User Device
Enrols user and Signs Biometric
Trusted Organisation C
Public Parameters
Public Key
Public Key
Public Parameters
Proof of non-revocation
Blockchain-based Verifiable Claims System

Features of our USI System

Self-sovereignty: The identity holder has complete control over storage and use of their identity.

Privacy: Verifier is unable to reverse the transformation and discover the individual's actual biometric signature.

Non-linkability: if transformations have different parameters across different Service Providers, cross matching is impossible.

Unique Identification: The transformation will always map back to the same identifier, subject to an error rate.

Decentralisation: The trusted organisations do not communicate or agree for the **Unique Identification** property to hold.

Biometrically Derived: the system does not depend on individuals holding previous identity documents in order to enrol.

Non-linkability

If transformations have different parameters across different Service Providers, cross matching is impossible.

Using the framework proposed by Gomez—Barerro et al. we show that registrations in our protocol are unlinkable:

$$LR(d) = \frac{p(d|H_m)}{p(d|H_{nm})}$$

Further work

- Blind signatures for trusted organizations
- Collision probability and error rates for biometric identification at scale
- Reference implementation for experimental analysis

Conclusion

- With further work, it will be a feasible protocol for large scale privacy preserving identification
- The protocol would augment existing procedures
- Potential for KYC, government services, displaced persons, social media, whistleblowers, fair voting

For Further Reference

Hamer, T. (2019). *Private Digital Identity on Blockchain.* Honours thesis submitted to the Australian National University, Canberra, Australia.