Project Aurum Phase 2

Privacy for central bank digital currencies

Motivation

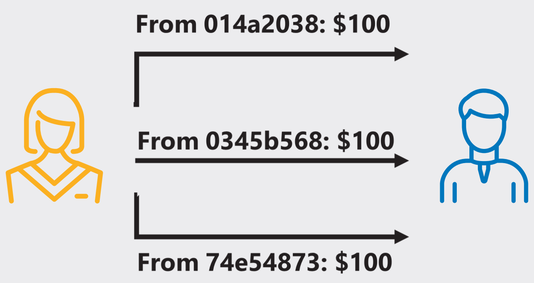
Privacy is a major consideration in the adoption of a digital form of cash. The public wants as much "cash-like" anonymity as possible.

Project Aurum Phase 2 will focus on a privacy by design principle exploring various privacy enhancing technologies.

Architecture

Pseudonymisation

Unique, bank-verified pseudonym for digital cash transactions to hide the real identity of end-users

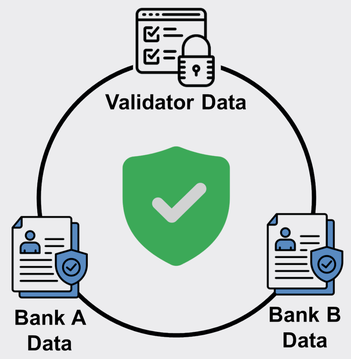


Zero-knowledge proof

Digital cash tokens protected by non-interactive active succinct proofs hiding transaction data

Minimal Data Exposure

Each party holds only essential information to ensure privacy



Key elements

Cash-like properties

Research on cash-like features in digital cash transactions to achieve:

- **Confidentiality and anonymity**
- **Transaction unlinkability**
- **Conditional privacy**

Privacy-enhancing technologies

Innovative technologies to enhance privacy and protect end users' personal identifiable information (PII) from access or derivation by third parties.

Aligned with compliance need

Addresses illicit activities such as money laundering or fraud, given valid regulatory powers.

BIS Innovation Hub

HONG KONG MONETARY AUTHORITY
香港金融管理局

Project Aurum Phase 2