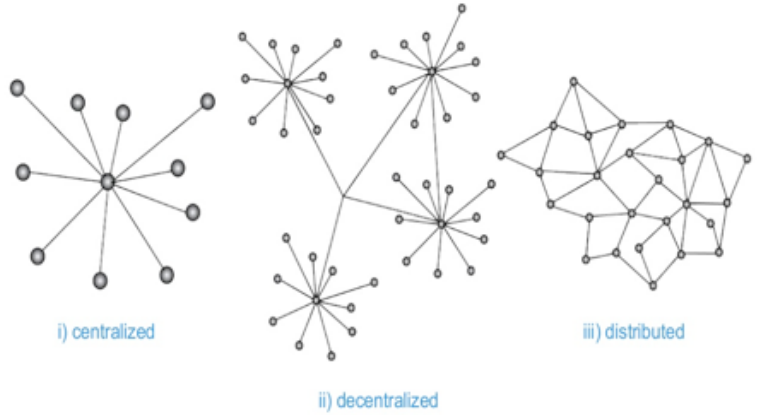
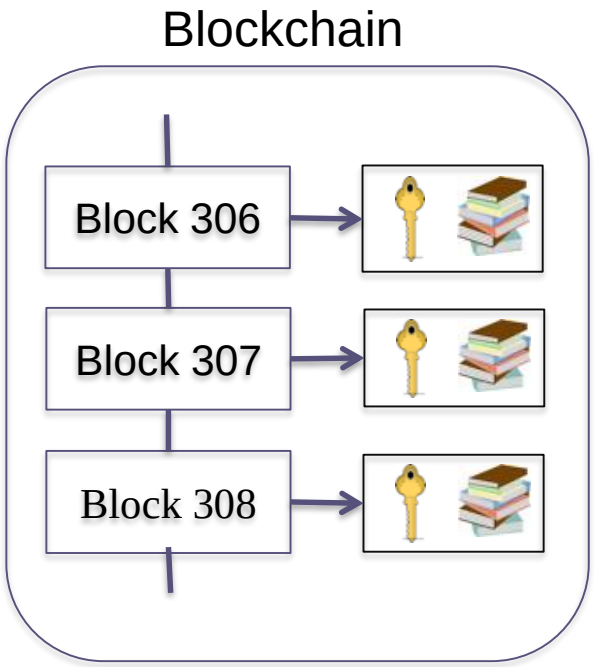
Blockchain & Decentralised Identity (trust framework)

David Pollington, Head of Service
Access Technology

Blockchain – a recap



- A distributed and decentralised ledger (a linked transaction database)
- The transaction blocks are cryptographically protected for immutability
- A protocol for the distributed ledger management – ensuring only valid transactions are added and are immutable

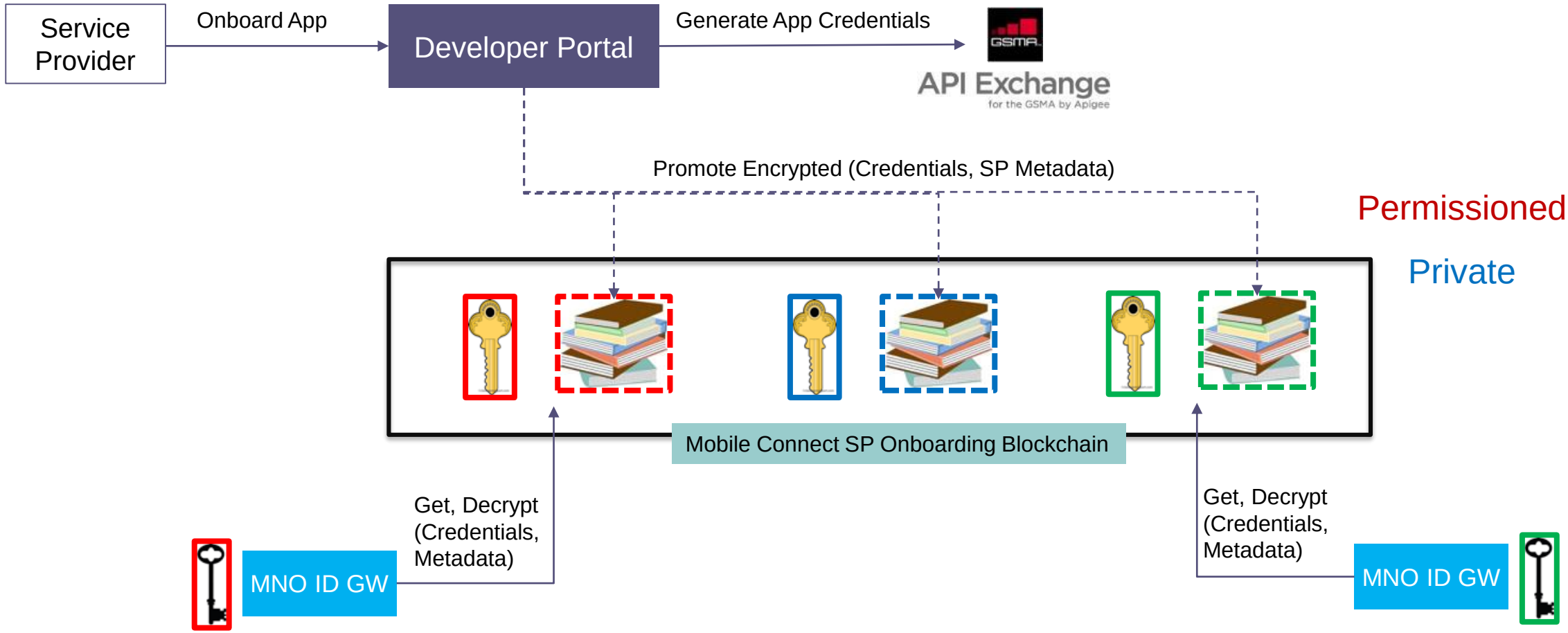


Types of Blockchain… drawing parallels with network types

	Permissionless	Permissioned
Public	 Internet	 Extranet
Private	 Home network	 Intranet

Trend

Example use case: application of Blockchain to Mobile Connect SP Onboarding



Application of Blockchain to Identity?

Key challenges that digital identity faces:

1. Establishing trust in a trustless digital world
2. Decentralisation: control and ownership of the identity attributes (self-sovereign identity)
3. Immutability of the operations related to the digital identity

=> Blockchain/Distributed Ledger Technologies well placed to address these requirements

Source: Peter Steiner's cartoon, as published in *The New Yorker*

- Note though that personal information is NOT stored on the Blockchain (not even in hashed form)
- => the value that Blockchain provides is in ensuring authenticity and privacy:
  - Data integrity proofs
  - Provenance
  - Blinding
  - Zero-knowledge proofs
  - Resiliency

Why do it? => establishment of trust frameworks unlocks the digital economy

Government Services
Digital access to government services

Banks
Reduced KYC/AML compliance costs and fraud losses

Businesses
Proving identity of a business to another business

Citizens
Reduced online profiles, and simplified onboarding to digital services

eCommerce
Growth in eCommerce from trusted identities and verified info

Healthcare
Digital access to patient records and healthcare services

Verified.Me

$15 Billion (CAD)
or ~1% of GDP

EIC Conference 2018

Source: The Economic Impact of Digital Identity in Canada (DIACC, 2018)

Why do it? => trust eroding in existing online identity players

If you had the right to erase your personal data from any company, which of the following situations do you think would motivate you to take action?

45% Finding their data was sold or shared with other companies

14% Receiving a robo call or telemarketing call for a product/ service I am not interested in

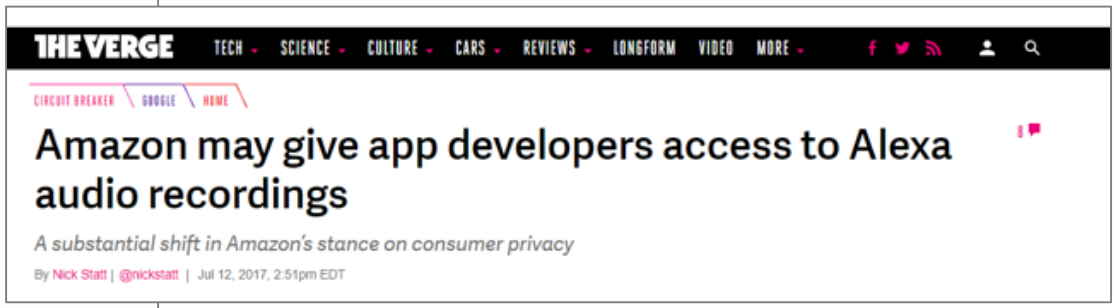
12% Being marketed to for irrelevant or wildly inappropriate products

11% Being marketed to, via social media in an intrusive way

9% Being marketed to, too frequently

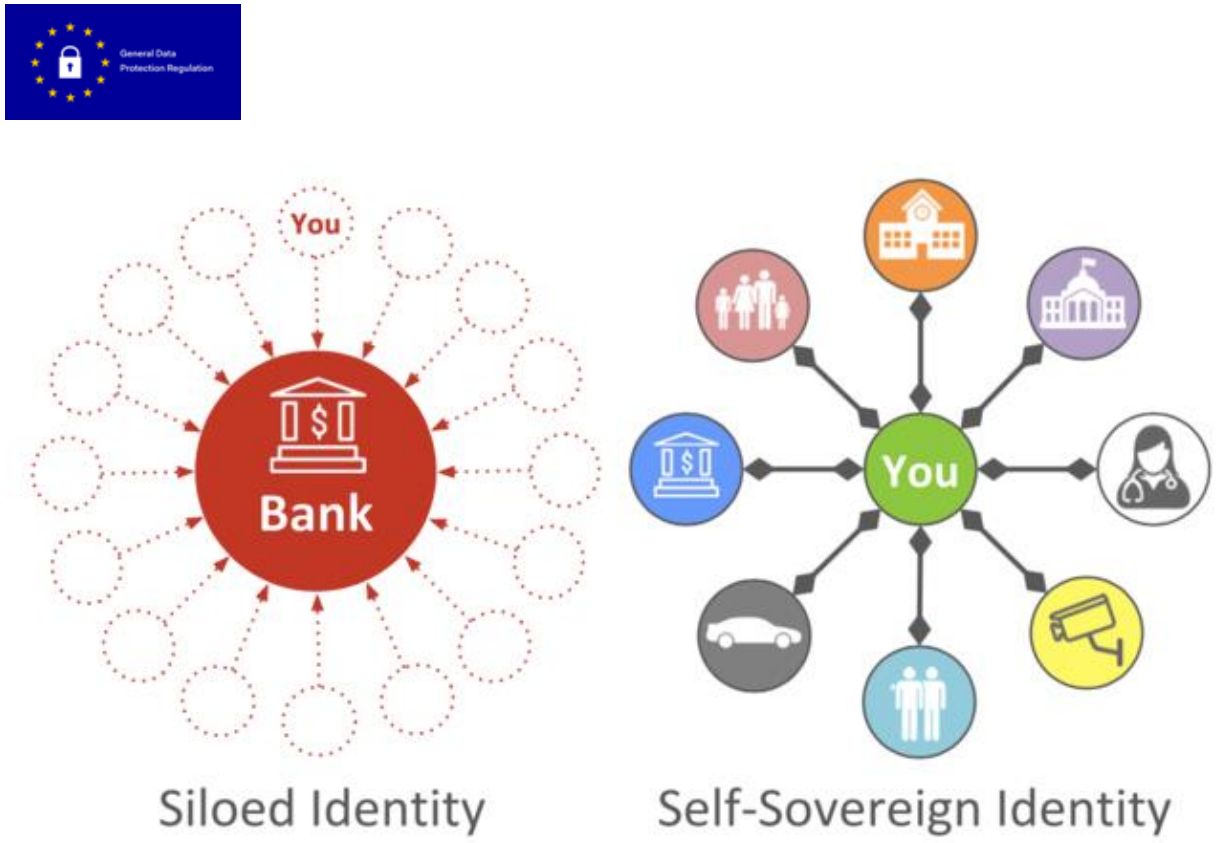
7% Receiving bad customer service

3% Being marketed to, for a product/ service I have already purchased



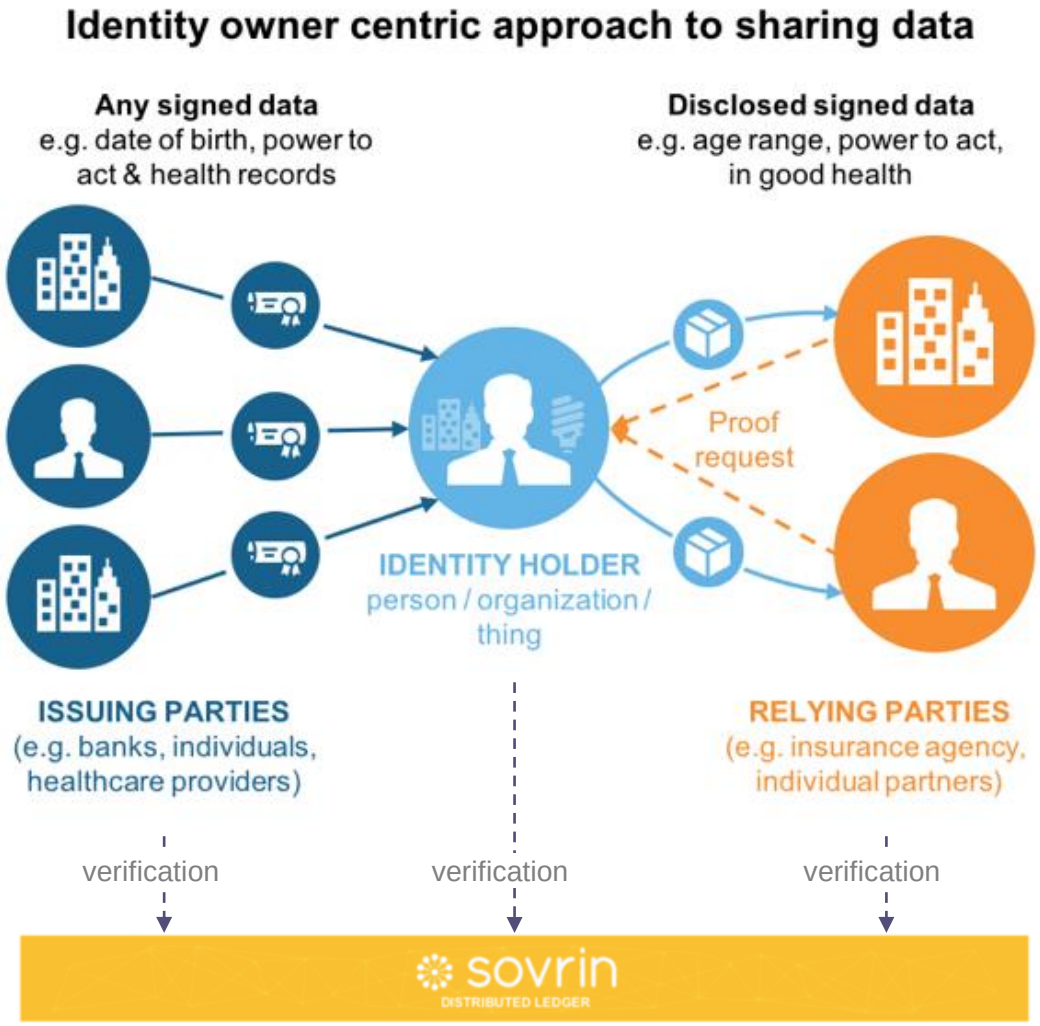
Why do it? => move to a decentralised approach (SSI)

- GDPR and public sentiment over the increasing number of data breaches driving popularity in the concept of Self-Sovereign Identity (SSI)
  - => user takes responsibility and ownership of their identity and uses a range of 3rd party issuers to vouch for the user's claims



Introducing Sovrin (DLT-based trust framework)

- Uses a distributed ledger for managing decentralised identifiers (DIDs) and ensuring authenticity of the parties interacting via the framework and the information (claims) that are exchanged



Introducing Sovrin (DLT-based trust framework)

- Open standards approach (W3C, DIF) and gaining significant momentum through support from the likes of IBM and DT

- …but many issues still remain around usability, commercialisation and faith in the technology

Unlikely that there'll be just one global trust framework for identity…

National

Verified.Me

verimi

GOV.UK VERIFY

RealMe®

its me

Global

uport

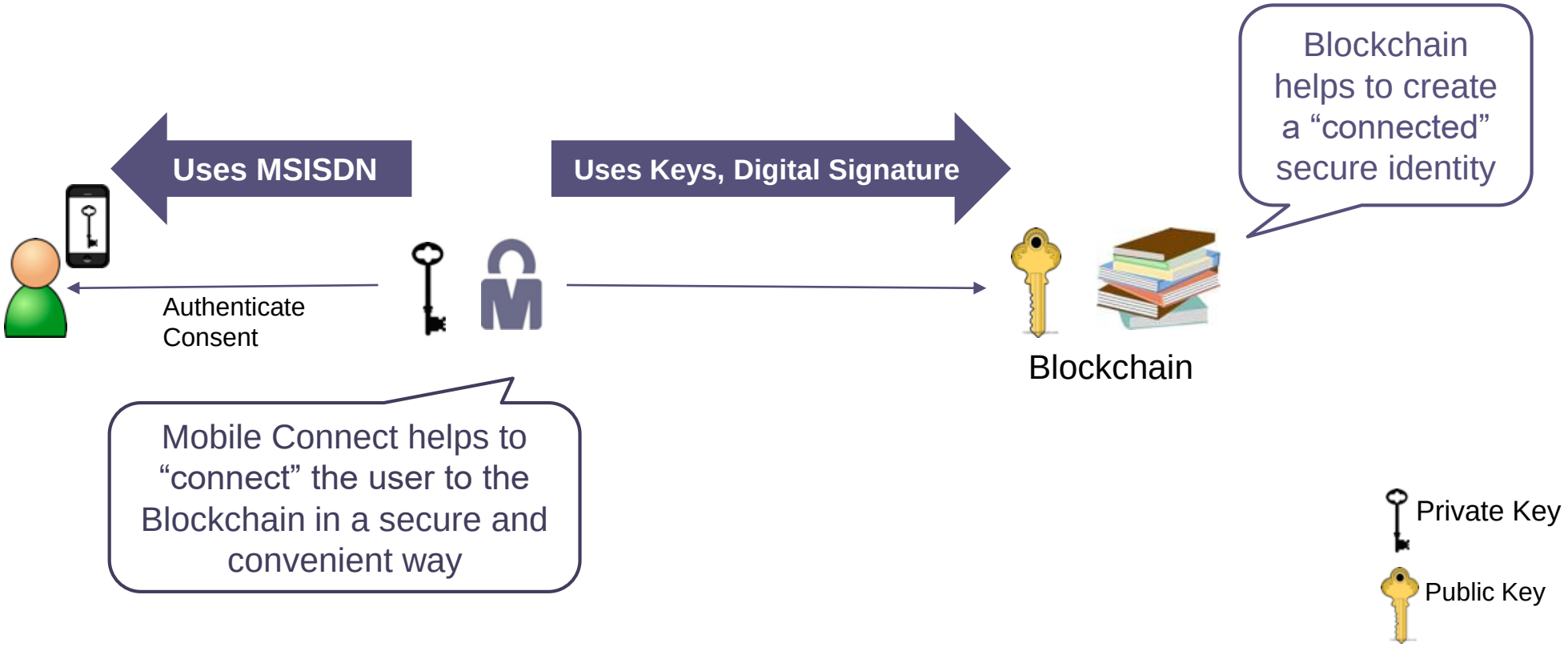
sovrin
identity for all

Sector

MOBI

IBM | MAERSK

Key role for Mobile Connect: **Humanising Blockchain**



…and MNOs acting as issuer/verifiers of claims (attributes)