TRUST
Over IP
FOUNDATION

Digital Trust

A Trust over IP Foundation Primer

Chapter 1: Pre-Internet Era

In-Person Credentials

- Have worked for centuries
- Institutions and technologies are well understood

Understanding Trust

How we make trust decisions

Technology

- Is it a legitimate representation?

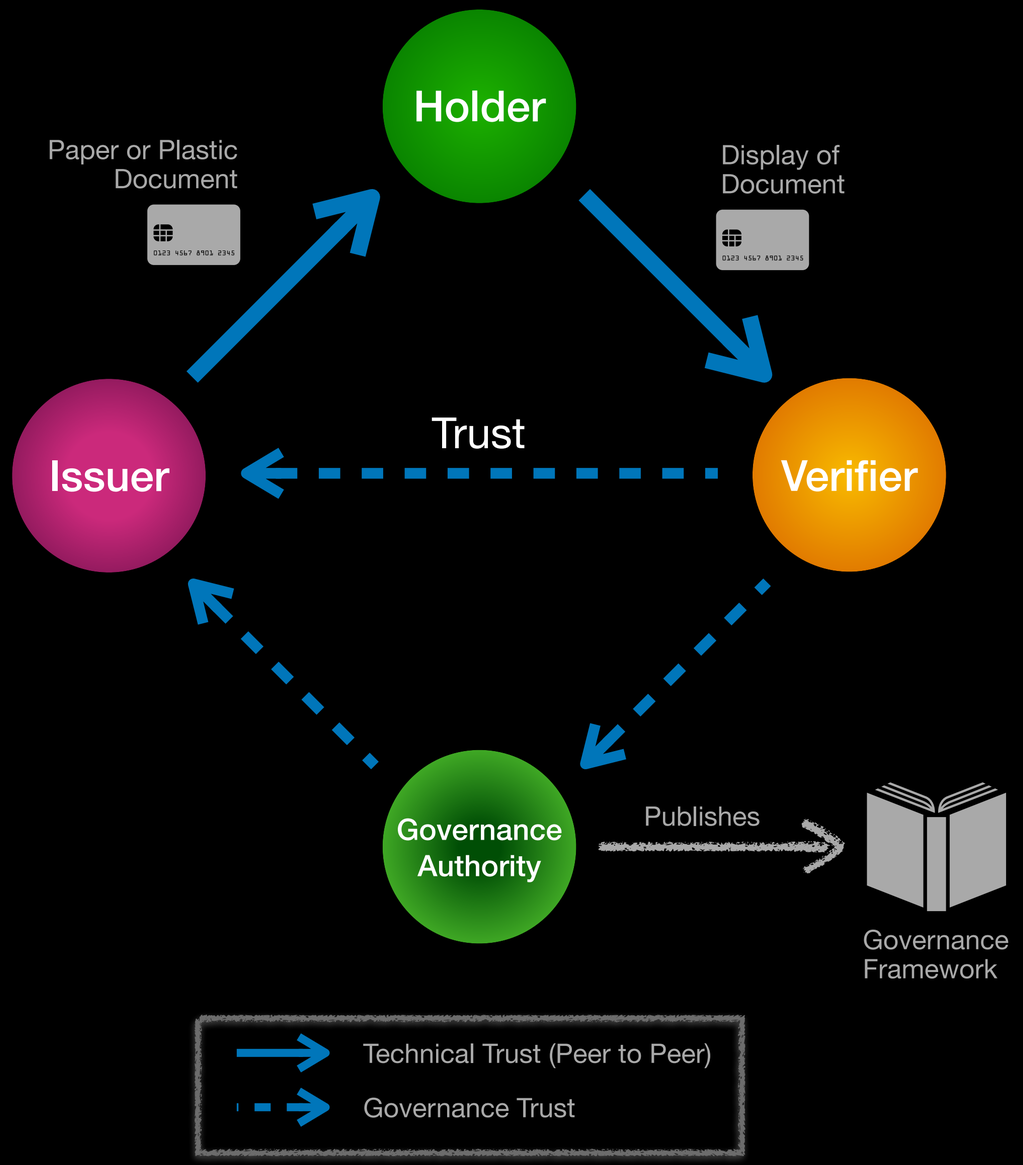
Governance

- Is the source of the representation trustworthy?
- Where does their authority come from?
- Do they have trusted processes?

In-Person Trust

A familiar model

- Each role in this model operates independently (Issuer, Holder, Verifier)
- Governance is the basis for trust decisions
  - Legislation, Policy, Regulations, Process, Reputation
- Issuers create physical representation of permission
  - Can’t replicate when needed (sharing)
  - Can’t prevent replication when you don’t want (fraud)
- Verifiers carry a good amount of risk
  - Fraudulent documents
  - Expense of paper
  - Biological viruses live on paper and plastic credentials (puts law enforcement at risk)



In-Person Ceremonies

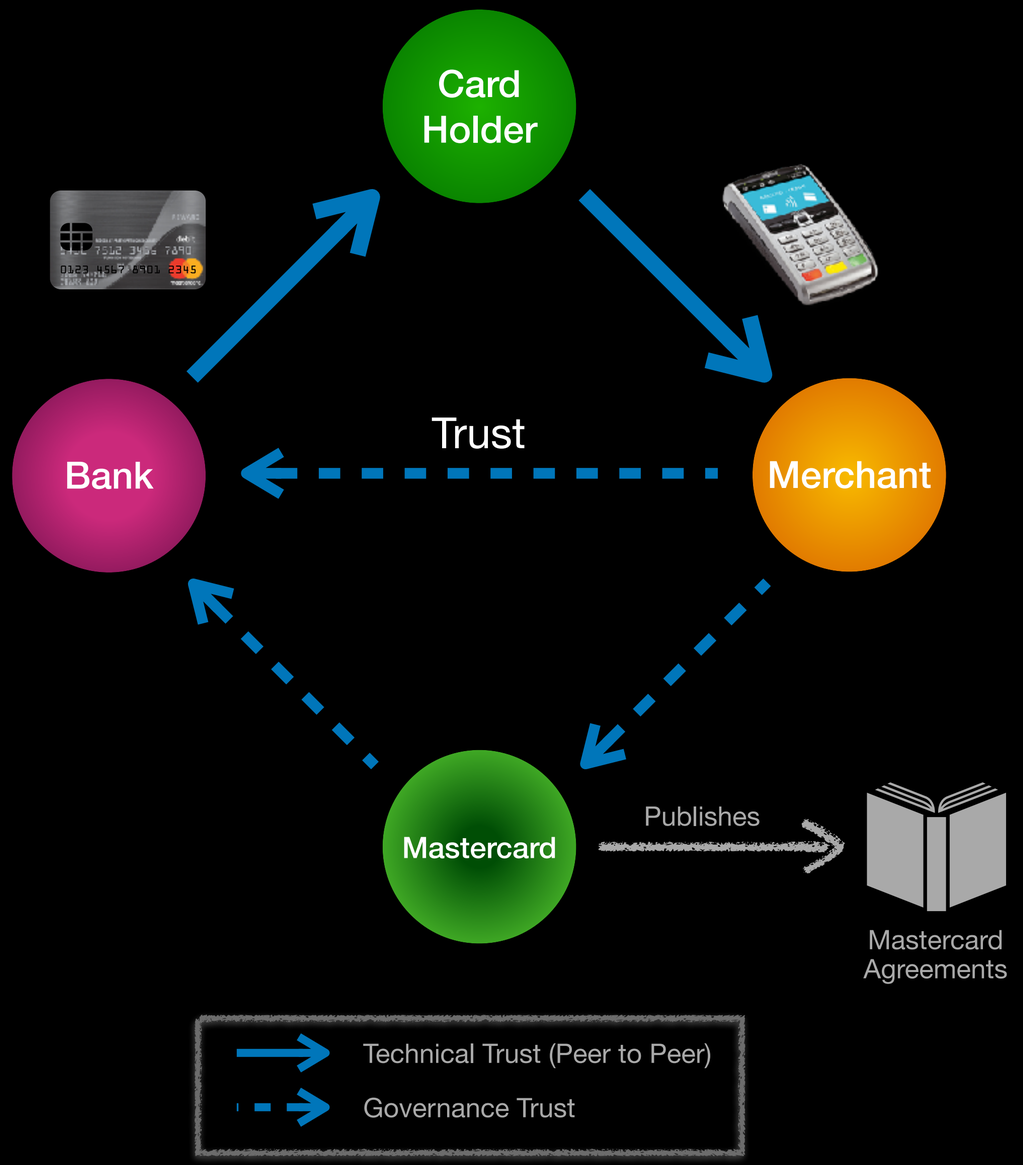
Wax through to Fax

- Signatures on written transactions originates in the 6th century as a means to validate an agreement
- Came into broader use in England with the 1677 Statute of Frauds which stipulated that contracts must exist in writing and bear a signature.
- This general practice continues on to the present day.
- Fundamentally, this is an action taken between the parties directly involved in the transaction, sometimes witnessed by a third party that also provides a signature

Financial Services

Case study

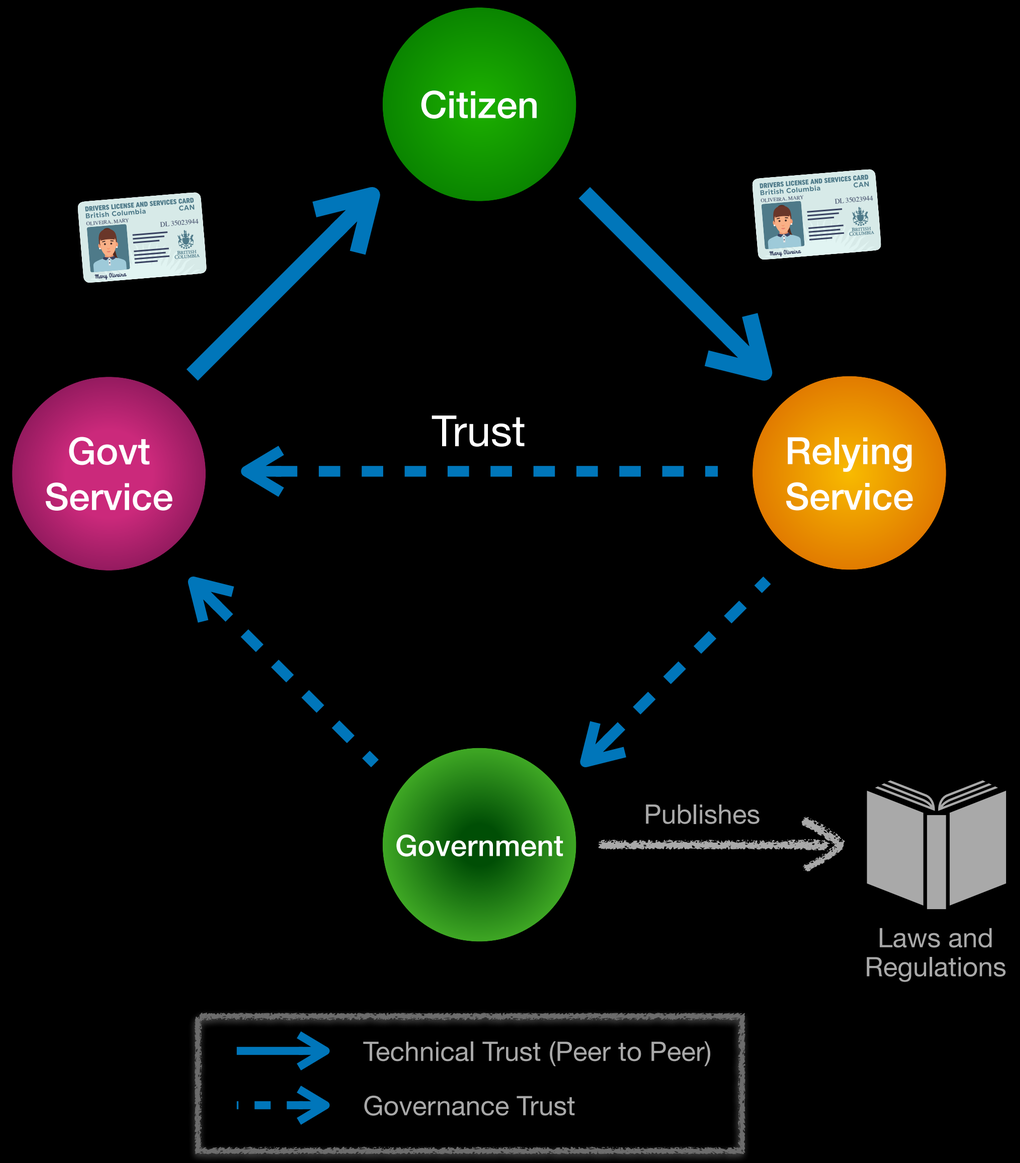
- Governance
  - Mastercard is the authority for their payment processing network
  - Issuers: Banks (~25,000)
  - Holders: Cards (~926 M)
  - Verifiers: Merchants (~50 M)
- Technology
  - Physical Card has distinctive design and embedded security measures
  - Fraud risks mitigated by various techniques including PIN, transaction monitoring, merchant behaviour



Government

Case study

- Government issues many types of permissions and authorizations
- Foundational Issuances
  - Birth, Death Certificates
  - Legal Entities Registrations
  - Land Registration
- Hundreds of others grounded in foundational credentials
  - Health, Drivers Licences, Education, Social Services, etc.
  - Business licencing, Natural Resources, Climate, etc.
- Economy is underpinned by Government



Chapter 2: Internet Era

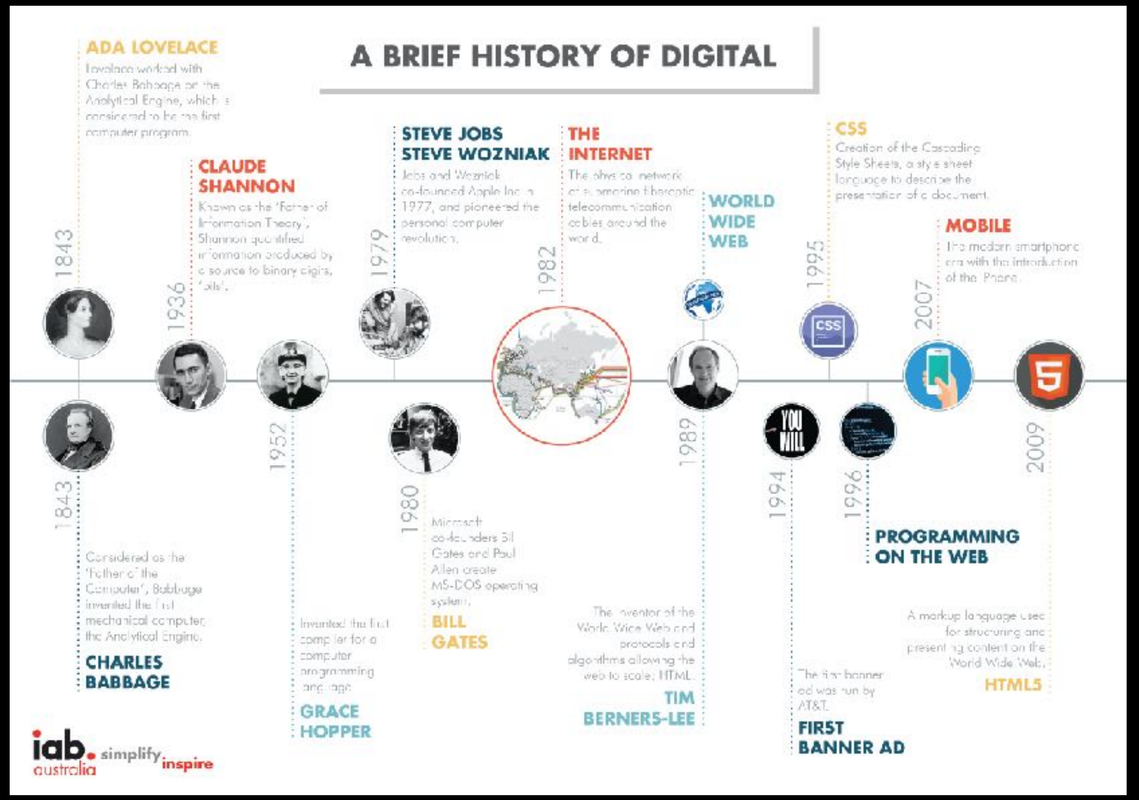
Information Technology

Benefits and Gaps

- Benefits to production efficiencies are clear
- Markets and jobs created

<u>However there is a “Trust Gap”</u>

- Internet is primary driven by E-Commerce and Online Advertising
- Large gap when it comes to “High Value” / “High Risk” transactions … those that we know well how to do In-Person

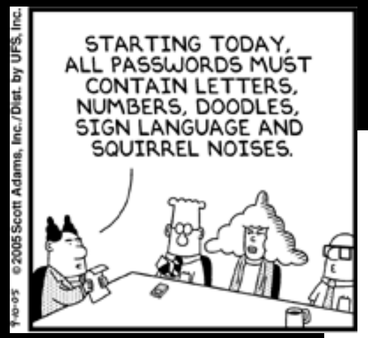


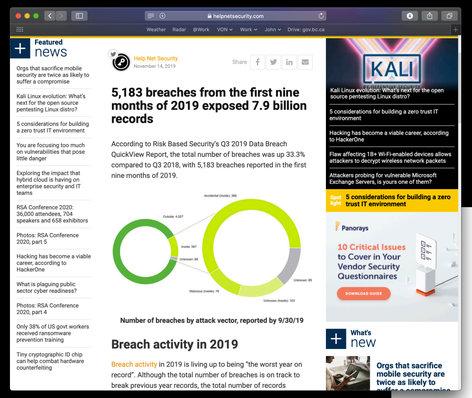
https://www.iabaustralia.com.au/iab-blog/blog-articles/entry/a-brief-history-of-digital-it-s-always-good-to-reflect

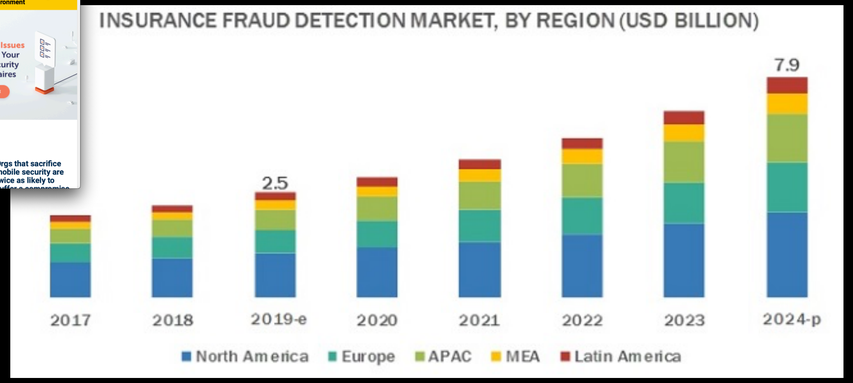
New Risks

Global Scale Computing

- Unprecedented scale and global connectivity comes with some new concerns
  - Usability challenges with so many passwords
  - Identity theft risks due to duplication of personal data … everywhere
  - Unintended side effects of large scale surveillance







Old Challenges

Government Service Delivery

- Many efforts, over the years, to find a way to deliver a simple approach for businesses faced with a multi-service/jursidiction journey
  - None have succeeded at any scale (more than a few services)
  - Economy and Government services are constantly changing
  - Our governance model is aligned to In-Person trust
- All these services have one thing in common …

BizPaL
Business starts here

one stop
bc business registry.ca

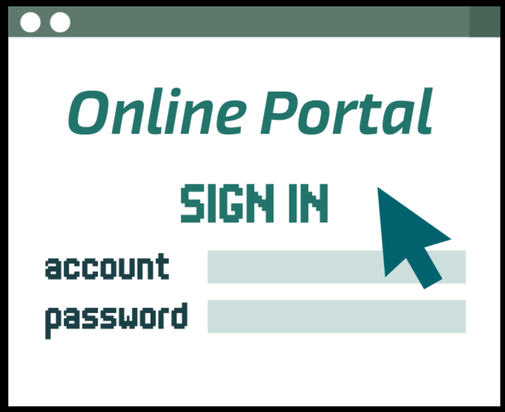
The Accidental Actor

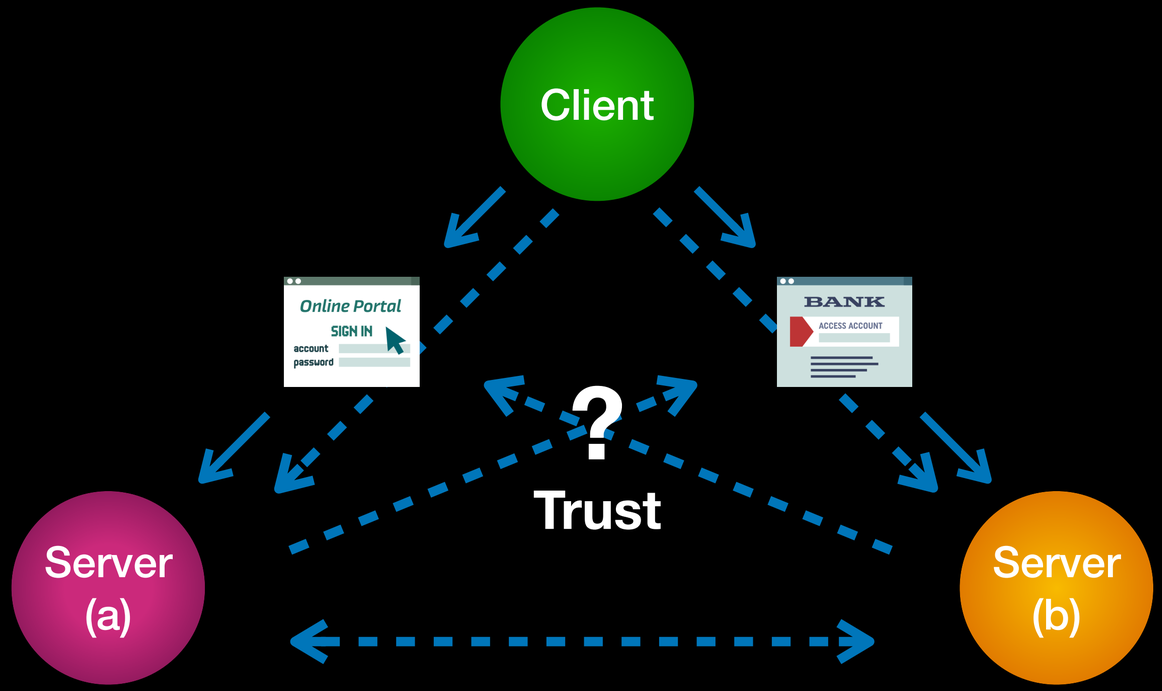
Login Account Service

- The operator of the Login Account provider is implicitly part the trust model
- We have no way to systemic means to evaluate the trustworthiness of Login Account providers

Why?

- Originally computers were large, expensive and could only be accessed on-premise and therefore relied on In-Person trust - e.g. physical access control to the “login” terminals
- As remote off-premise “login” to the computer become possible, no solution to the assumption of trusted in-person access to the login terminal arose introducing a “trust gap”
- As computing and networking scaled to global levels new problems and risks emerged as a result of never solving this trust gap

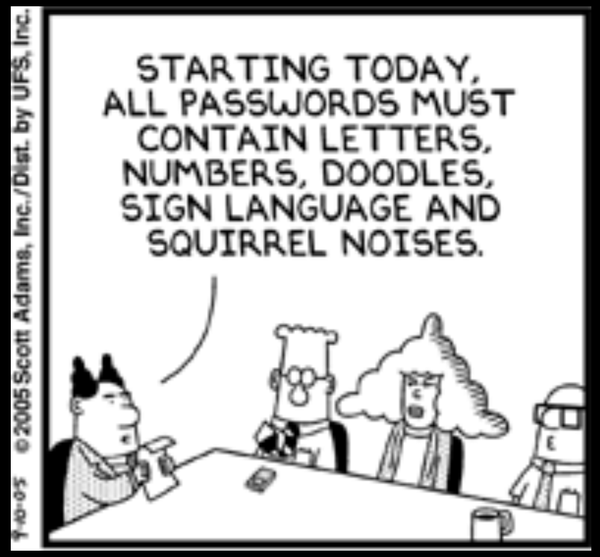




Internet Ceremonies

Frustration and Risk

- We simply don’t have a comparable ceremony to the In-Person signing ceremony
- All kinds different approaches to trying to create “trusted” interaction but they all involve an intermediary
- The intermediary is strongly incented to monetize these previously private interactions thus creating the risks identified earlier
- A common term used to describe these intermediaries is “platform”

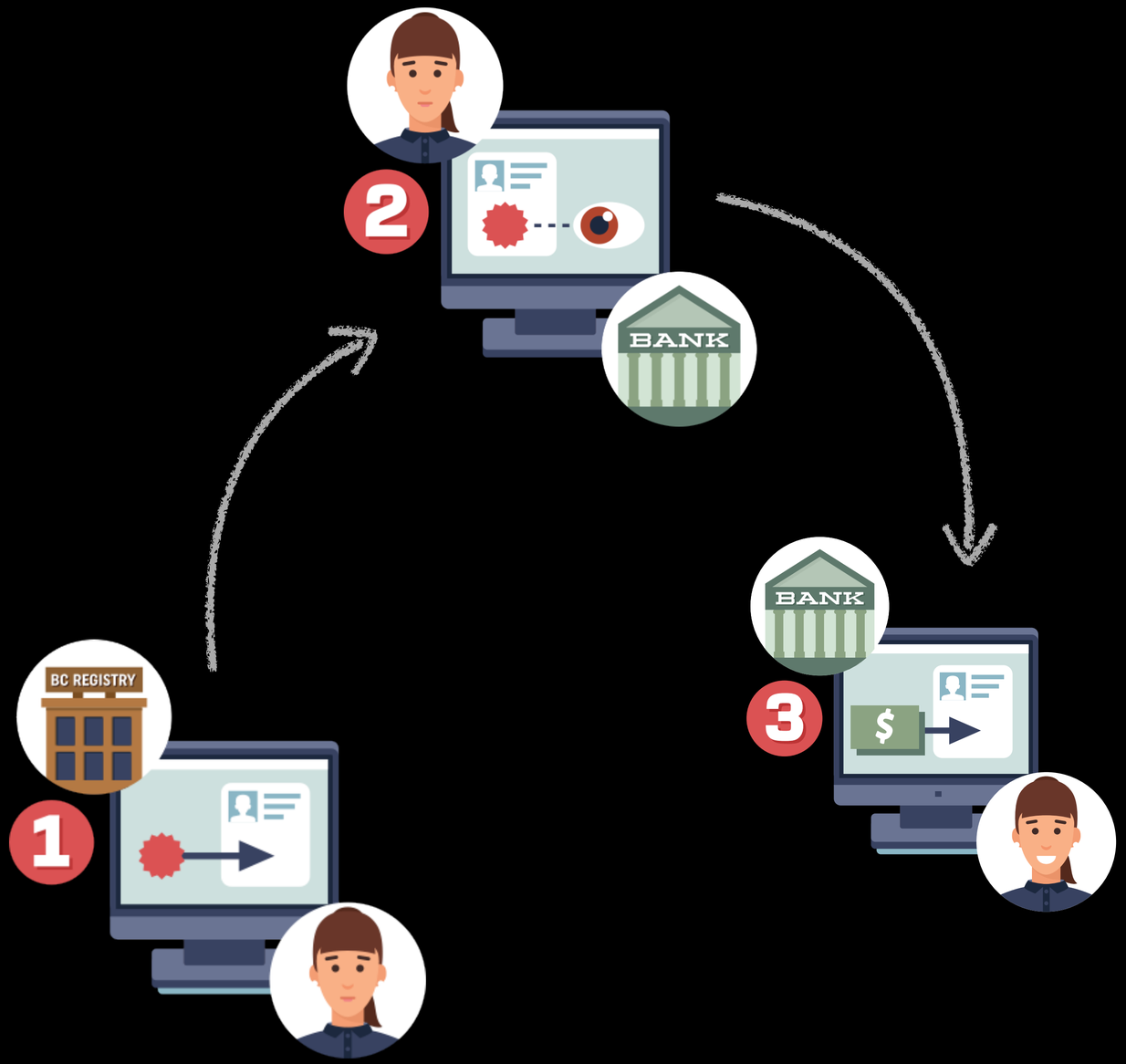


Chapter 3: The Digital Trust Era

A New Approach

Back to the Future

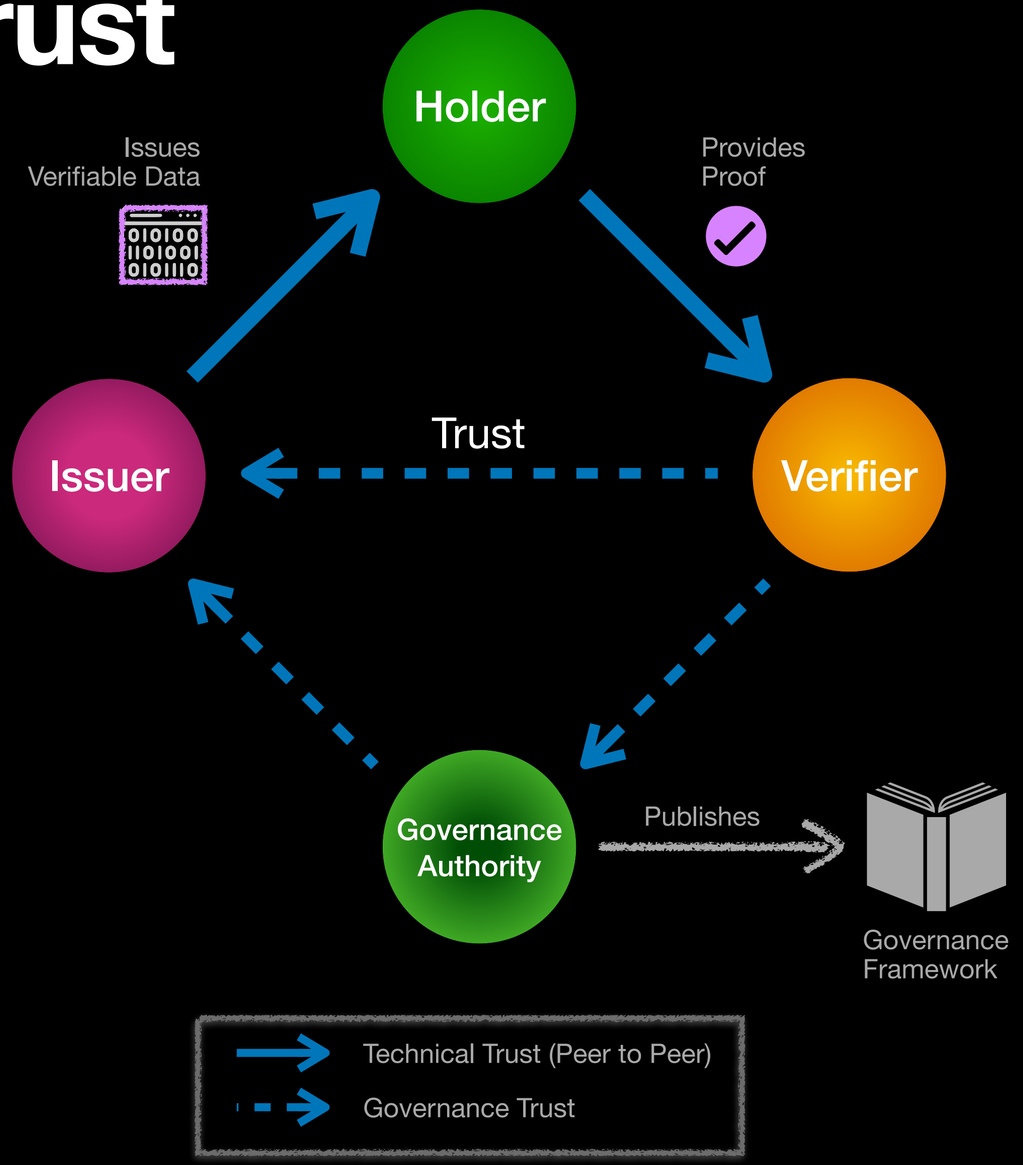
- Quite simply … solutions to digital trust, at scale, and over the Internet are not addressable with the technology approaches we have currently at hand
- “Paper-based” solutions clearly aren’t going to work (faxing medical test requisitions is still the policy and norm)
- Applying more effort towards existing Internet-era technology models is a dead-end
    - Centralized login account models often runs afoul of our legislative and policy governance models
    - Can’t span jurisdiction, legislative, sector and other boundaries people and businesses regularly traverse very easily
    - Can’t scale to global levels without massive privacy issues
- **<u>What if we had a digital means to allow a person to receive and carry their data to the next stage of their journey?</u>**



Economy-scale Digital Trust

Trust over IP (the Internet)

- **<u>Same end-user mental model as we have with physical wallets, licences, reports and cards</u>**
- Each role in this model operates independently (Issuer, Holder, Verifier)
- Governance is the basis for trust decisions
  - Legislation, Policy, Regulations, Process, Reputation
- Privacy preserved, security enhanced, via open standards which enables independence and scale
  - Private cryptographic peer to peer connections (surveillance resistant)
  - Standard cryptographic data exchange protocols between peers (impersonation resistant)
  - Holder is in control of providing verifier with proof of data (privacy preserving)
  - Verifier verifies data from holder without contacting issuer (surveillance resistant)
  - Verifier determines what data they need to verify from what set of issuers (fraud resistant)



Trust over IP Foundation

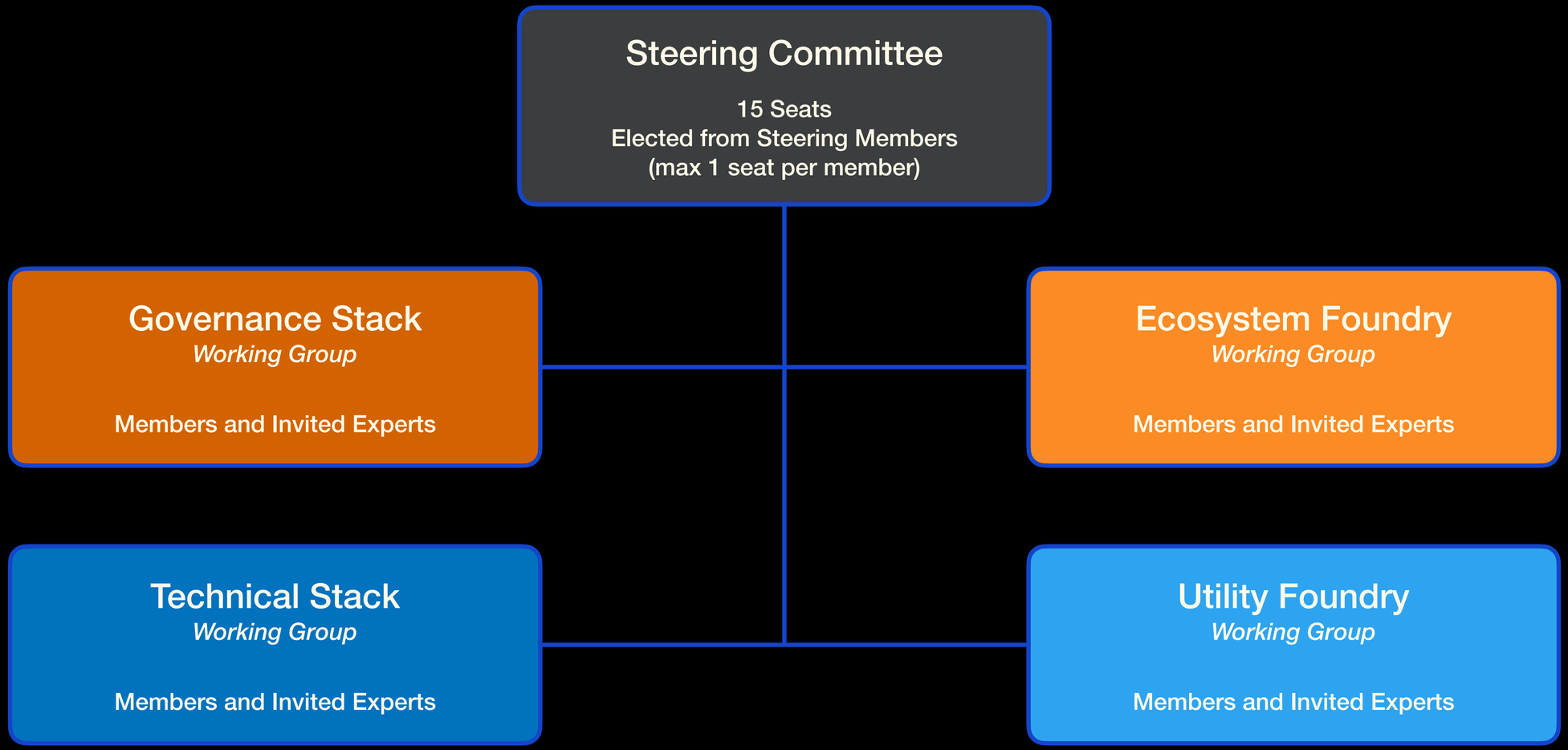
Driving global adoption

- The purpose of the Trust over IP Foundation is to define a complete architecture for Internet-scale digital trust that combines both cryptographic trust at the machine layer and human trust at the business, legal, and social layers.
- Part of the over 200 projects governed by the Linux Foundation the Trust over IP Foundation provides the market signal need to drive global adoption

TRUST
Over IP
FOUNDATION

Trust over IP Foundation

Working Groups: getting it done



Trust over IP Stack

The Lens for Digital Trust

Layer 4

Layer 3

Layer 2

Layer 1

Trust over IP Governance Stack

Ecosystem Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Member Directory
- ✓ Auditor
- ✓ Auditor Accreditor

Credential Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Credential Registry
- ✓ Authoritative Issuer
- ✓ Insurer

Provider Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Hardware Provider
- ✓ Software Provider
- ✓ Agency

Utility Governance Frameworks

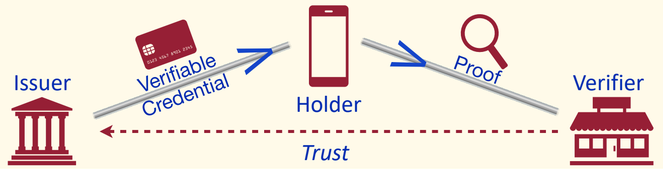
Governance Authority — Publishes → Governance Framework

- ✓ Transaction Author
- ✓ Transaction Endorser
- ✓ Steward

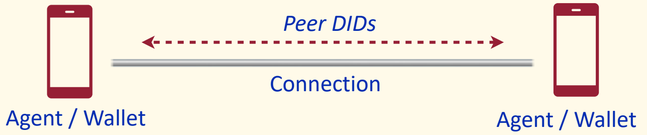
Trust over IP Technology Stack

Application Ecosystems

Data Exchange Protocols



DIDComm Peer to Peer Protocol

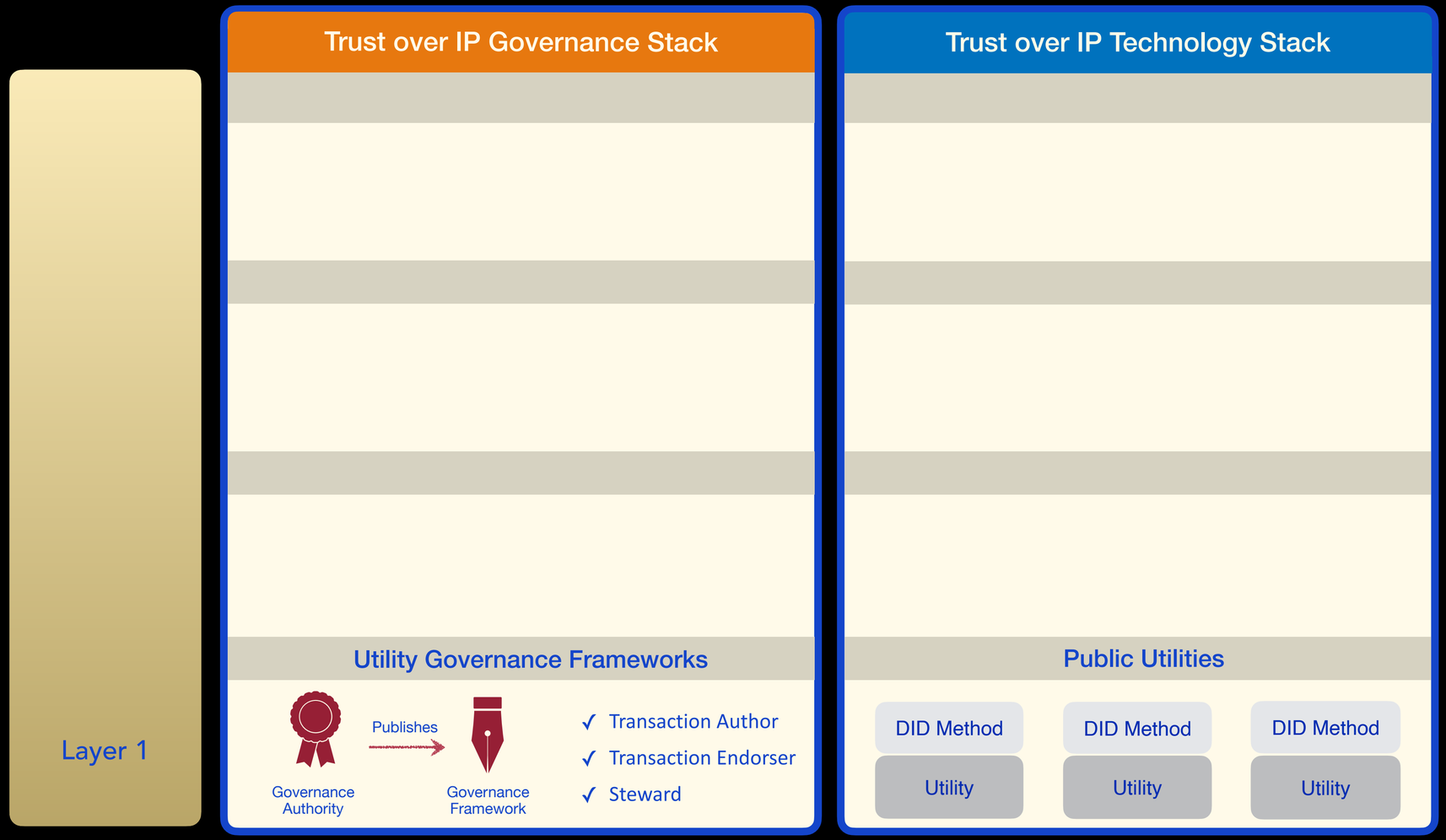


Public Utilities

DID Method	DID Method	DID Method
Utility	Utility	Utility

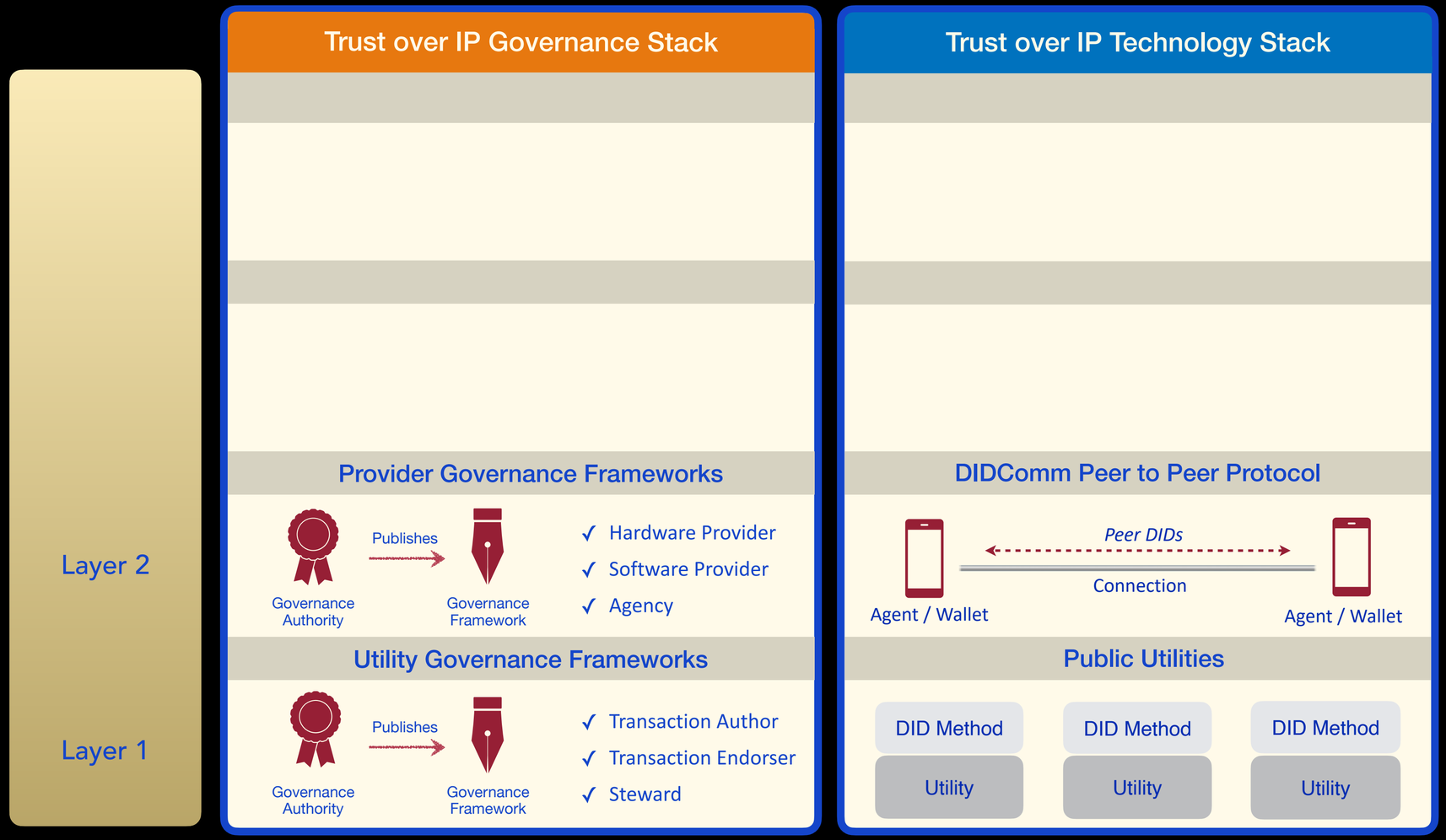
Trust over IP Stack

Layer 1 - Rooting Trust



Trust over IP Stack

Layer 2 - Trusted Peer to Peer Communications



Trust over IP Stack

Layer 3 - Trusted Exchanges

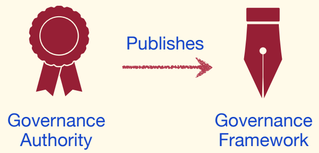
Layer 3

Layer 2

Layer 1

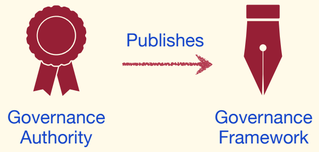
Trust over IP Governance Stack

Credential Governance Frameworks



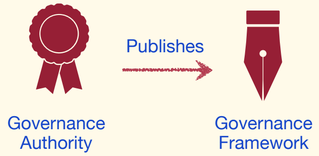
- ✓ Credential Registry
- ✓ Authoritative Issuer
- ✓ Insurer

Provider Governance Frameworks



- ✓ Hardware Provider
- ✓ Software Provider
- ✓ Agency

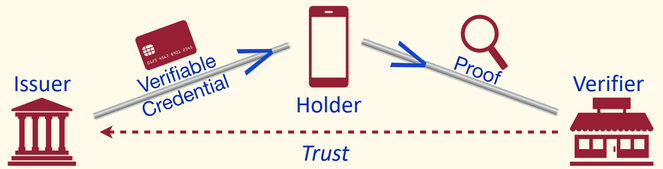
Utility Governance Frameworks



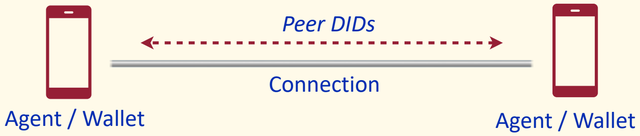
- ✓ Transaction Author
- ✓ Transaction Endorser
- ✓ Steward

Trust over IP Technology Stack

Data Exchange Protocols



DIDComm Peer to Peer Protocol



Public Utilities

DID Method	DID Method	DID Method
Utility	Utility	Utility

Trust over IP Stack

Layer 4 - Trusted Services

Layer 4

Layer 3

Layer 2

Layer 1

Trust over IP Governance Stack

Ecosystem Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Member Directory
- ✓ Auditor
- ✓ Auditor Accreditor

Credential Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Credential Registry
- ✓ Authoritative Issuer
- ✓ Insurer

Provider Governance Frameworks

Governance Authority — Publishes → Governance Framework

- ✓ Hardware Provider
- ✓ Software Provider
- ✓ Agency

Utility Governance Frameworks

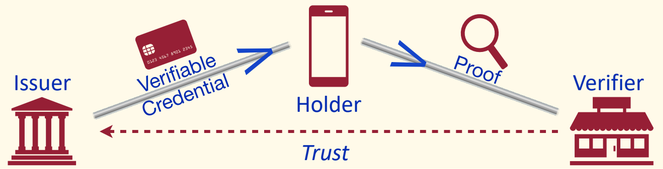
Governance Authority — Publishes → Governance Framework

- ✓ Transaction Author
- ✓ Transaction Endorser
- ✓ Steward

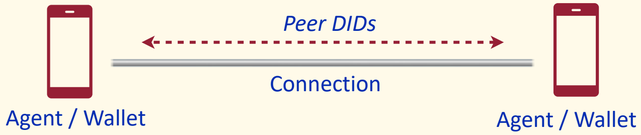
Trust over IP Technology Stack

Application Ecosystems

Data Exchange Protocols

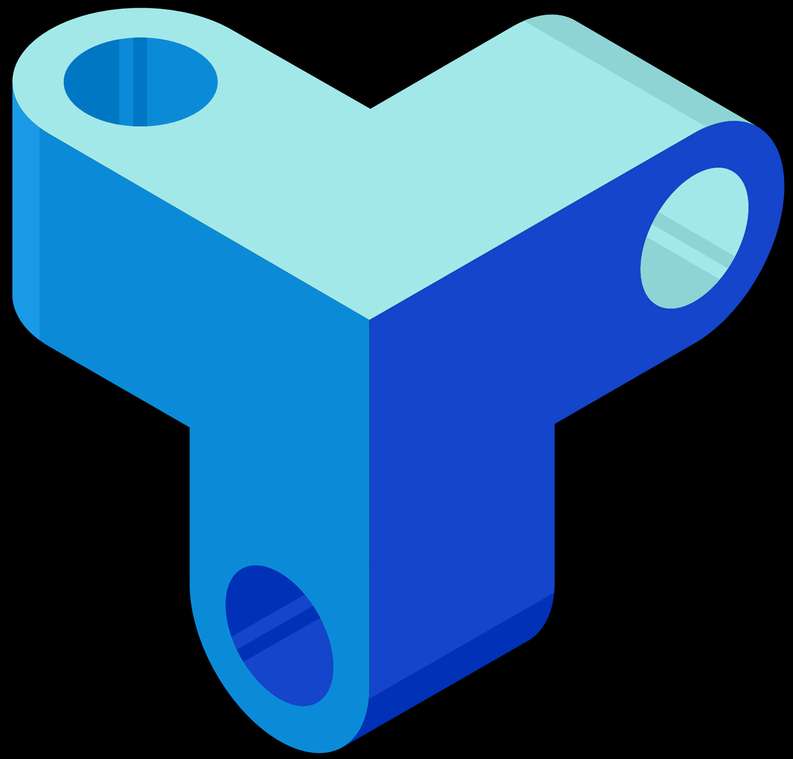


DIDComm Peer to Peer Protocol



Public Utilities

DID Method	DID Method	DID Method
Utility	Utility	Utility



TRUST Over IP FOUNDATION