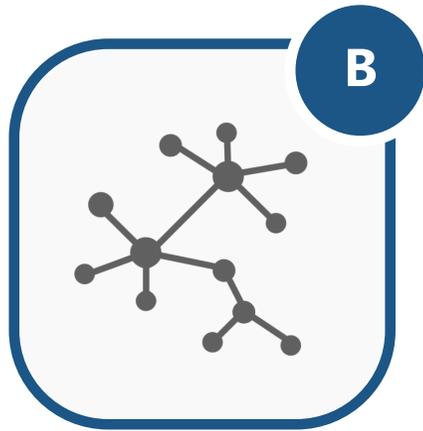# DIGITARY

Secure online credentials

Presentation to ARUCC GDN Group

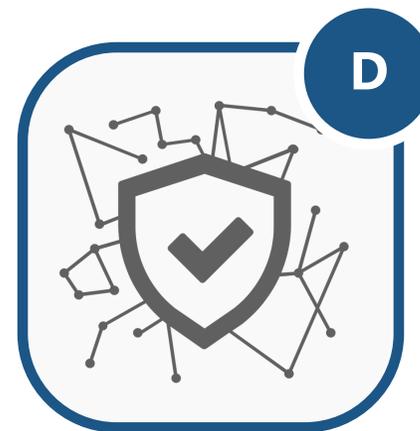Andy Dowling, CEO, Digitary

Digital credential models

A CENTRAL REPOSITORIES

B EXCHANGE NETWORKS

C BADGE FRAMEWORKS

D BLOCKCHAIN

E HUB AND SPOKE

DIGITARY

My eQuals

A. Central Repositories

1 Scope

Credential verification tool

Central database populated by participants

Manual online lookup by third parties

2 Learner-centric

Learner is **not** part of the process

No digital artefacts for learners to share with others

A. Central Repositories

3 Security, Trust, Privacy

Central database accessible via a web portal

Learner **consent** is a challenge
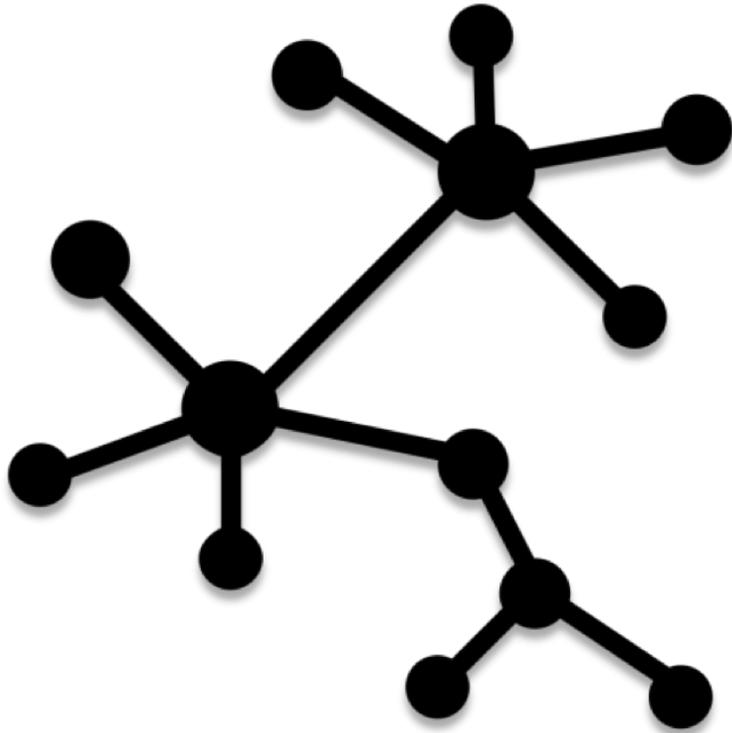
Communications are key to online validation portals

4 Participation

Relatively simple to build – no learner involvement
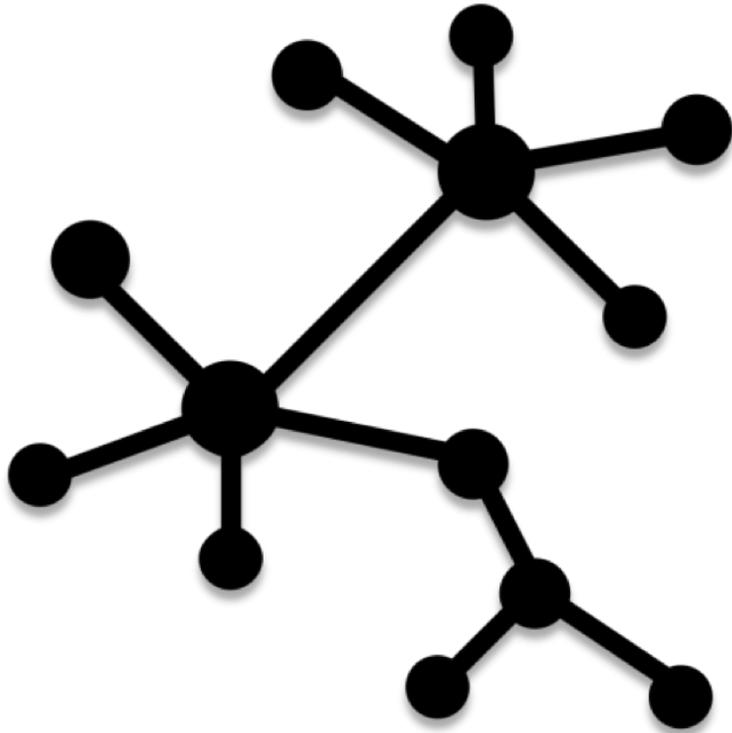
Simple data set = easier on-boarding

B. Exchange Networks

1 Scope

Credential exchange capability

Participants send and receive from the network

System to system transfer of information

2 Learner-centric

Institutions usually initiate delivery via the network

Students can request a push with **peripheral systems**

B. Exchange Networks

3 Security, Trust, Privacy

Closed network of trusted participants

Secure delivery of information

Passive verification over a trusted channel

4 Participation

High technical bar to adoption:

APIs for senders and receivers

Data standards, particularly with data-rich payload

C. Badge Frameworks

1 Scope

Micro-credentialling framework

Badges are image files with embedded data

Badges are issued, stacked, shared, and verified

2 Learner-centric

Badges are issued to learners by issuers

Learners store their badges online

Learners share their badges with third parties

C. Badge Frameworks

3 Security, Trust, Privacy

Badges are hosted, signed, or endorsed

Anybody can issue a badge for anything

Negative perception in a formal context

Long-term security

4 Participation

Easy to issue badges

D. Blockchain

1 Scope

Certifying and verifying "learner-owned" credentials

Uses public blockchain crypto to certify and independently verify records

2 Learner-centric

Learners **possess** their records -> their own registrar

Learners **must not lose** their keys or records

D. Blockchain

3 Security, Trust, Privacy

Strong on privacy

Trust: Not designed to identify issuers

Verification: complex and removed from issuer

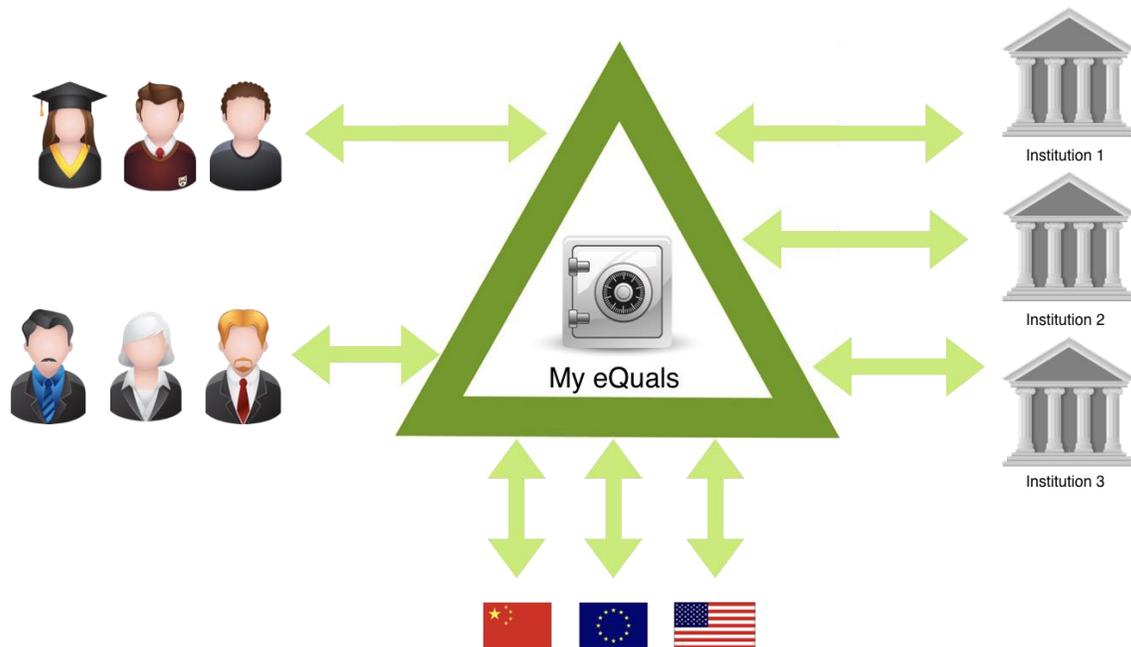Risky: Assumes today's crypto will never be broken

4 Participation

Easy to issue "fire and forget" blockchain records

Issuers need to accept cost of disintermediation

E. Hub and Spoke

1 Scope

Certification, storage, exchange, learner access

2 Learner-centric

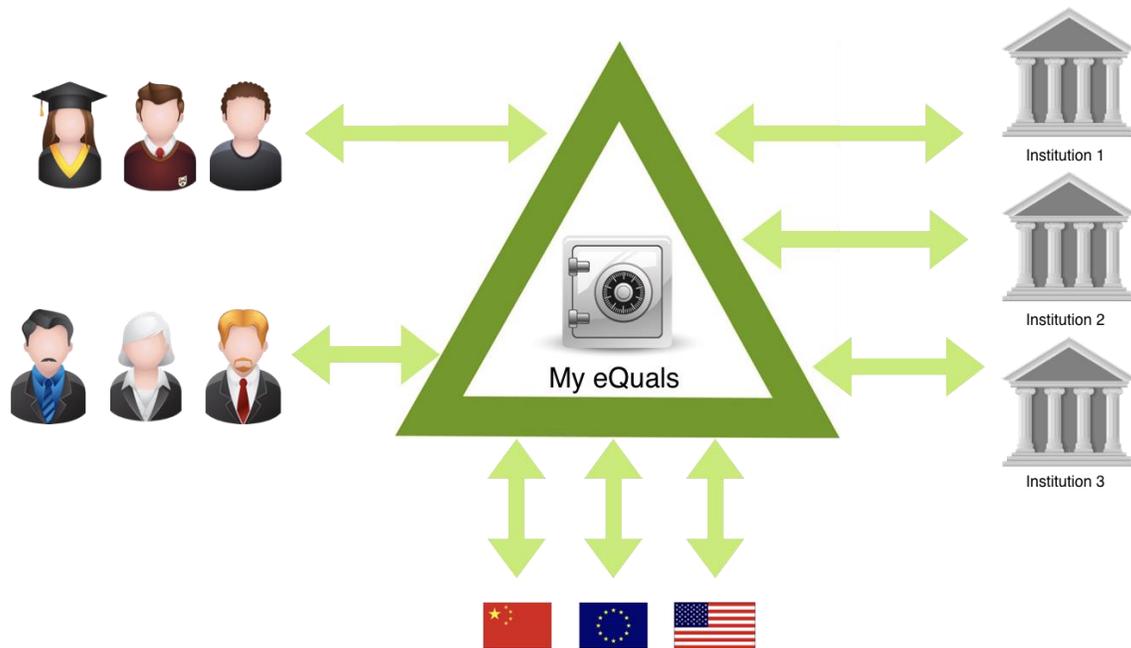Issuers **certify** and **maintain** records in their repository

Learners **access** their records via portal and **control sharing** with others

Issuer does **not** need to get involved in sharing or verification

E. Hub and Spoke

3 Security, Trust, Privacy

Issuers keep their own records

Cryptographic signing and long-term validity

Back to source verification via portal
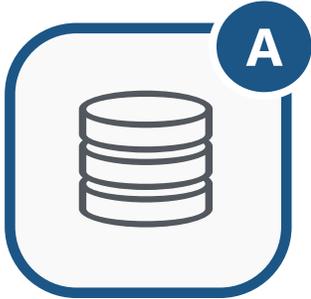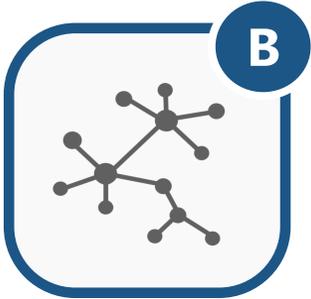
Secure exchange via network

4 Participation

Spectrum of capability amongst providers:

1. Simple: PDF drag and drop
2. Complex: API integration with PESC XML

In summary..

	CENTRAL REPOSITORIES	EXCHANGE NETWORKS	BADGE FRAMEWORKS	BLOCKCHAIN	HUB AND SPOKE
	A	B	C	D	E
SCOPE	VERIFICATION STORAGE EXCHANGE	VERIFICATION STORAGE EXCHANGE	VERIFICATION STORAGE EXCHANGE	VERIFICATION STORAGE EXCHANGE	VERIFICATION EXCHANGE STORAGE
LEARNER CENTRIC	NO	DEPENDS	YES	YES	YES
SECURITY	CONSENT ISSUES	STRONG	LONG-TERM SECURITY ISSUES TRUST ISSUES	LONG-TERM SECURITY ISSUES TRUST ISSUES	STRONG
PARTICIPATION	SIMPLE	INVOLVED	SIMPLE	SIMPLE	VARIABLE

13

Q & A

DIGIT△RY

Secure online credentials

Thank You!

Andy Dowling, CEO, Digitary

(andy.dowling@digitary.net)