Ten minutes “under the hood”

Andy Dowling, CEO, Digitary
What are we trying to achieve?

01 Digital Student Data Portability
Kill paper! Give students and graduates access to and control over their authentic qualifications. Provide statistics to feed policy decisions.

02 Security, Privacy, and Trust
Making digital credentialing secure
Ensuring that systems and methods are trusted
Preserving the privacy of individuals

03 Participation
Getting buy-in from all stakeholders: education providers, students, employers, governments, etc.
Delivering real solutions with long-term benefits.
Some recurring themes

Verification
How to verify somebody's achievements digitally?

Content
What’s in a digital credential and what does it look like?

Storage
How to store a learner’s qualifications for the long term?

Exchange
How to exchange credentials quickly, securely, and reliably?
Some existing architectures

A. CENTRAL REPOSITORIES
B. EXCHANGE NETWORKS
C. HUB AND SPOKE
D. BADGING PLATFORMS
E. PUBLIC BLOCKCHAIN
A. Central Repositories

1. **What?**
   - Central database populated by participants
   - Online lookup by third parties

2. **Mobility**
   - Student is not part of the digital process
   - so does not have a digital artefact
   - Can generate usage stats on verifications

3. **Security, Trust, Privacy**
   - Student consent is implied, or paper-based
   - Single central data store = riskier
   - Communications are key

4. **Participation**
   - Simpler to build
   - Participants need to populate data
   - Complexity depends on data set
B. Exchange Networks

1. **What?**
   - Secure network between by participants
   - Send and receive capability
   - System to system transfer

2. **Mobility**
   - Student “push” of records over the network possible via peripheral systems
   - Can generate usage stats over the network

3. **Security, Trust, Privacy**
   - Closed network with participant vetting
   - Secure protocols for exchange
   - Recipients can trust what they receive

4. **Participation**
   - Higher technical bar involving data standards and protocols to send or receive via APIs
C. Hub and Spoke

1. **What?**
   - Repositories AND network
   - Student & third party portals
   - Regional integration hub

2. **Mobility**
   - Students have 24/7 access to their records
   - Zero intervention required by issuer
   - Student has control over sharing
   - Can generate usage stats

3. **Security, Trust, Privacy**
   - Issuers have their own repositories
   - Cryptographic signing + access control
   - Student controls sharing
   - Trusted portal for verification -> comms

4. **Participation**
   - Participants must export data to API
   - Complexity is dictated by data to be exported
   - Simpler alternatives available (PDF)
D. Badge Frameworks

What?
Badges are images with embedded data according to an open standard
Supporting workflow elements

Security, Trust, Privacy
Cryptographic signing / hosted on a trusted platform
Anybody can issue a badge for anything
- negative perception in a formal context
Endorsement model

Mobility
Students store and control sharing
Badges are fine-grained, shareable, and stackable credentials

Participation
Easy to issue badges
Not so easy to trust badges?
E. Public Blockchain

1. What?
Blockchains are distributed ledgers...
Issuers write hashes to blockchain...
Third parties verify against the blockchain

2. Mobility
Students possess the record itself
Decentralised verification means no usage stats

3. Security, Trust, Privacy
Depends 100% on cryptography
Comprehensive trust via issuers website

4. Participation
Easy to issue records onto blockchain
Management burden shifts to the student and the verifying party
Cost of disintermediation
In summary..

“Convergence, not uniformity”

Collaborative opportunities!