DIGITAL TRUST

HOW THE ORGBOOK ENABLES THE DIGITAL ECONOMY
Carol Prest
Registrar & Executive Director
Registries & Online Services
John Jordan
Executive Director, Services Strategy, Office of the CIO
A proof of concept was developed in Fall, 2016.
Paper documents are cumbersome as proof of legal compliance and permission.
Let's look at an example
Mary requires a variety of documents in order to establish her bakery. Some requirements are not obvious, so she’ll have to do her homework.
This journey involves multiple sources ... 

... and modes of service delivery.
All of this activity is a major burden for all involved.
So, how do we create this?
We have been developing technical capacity ...
... we are collaborating ... and generating interest ...
... and exploring **blockchain** as a decentralized ledger.

Blockchain uses cryptographic codes (hashes) to prevent undue manipulation of a sequence of text records.

Decentralized record keeping is possible once privacy, security, and permissions are settled.
Contrary to the hype, blockchain is **not** about ...

- Crypto-currencies
- Ransomware Scams
- Trustless Anarchy
What if ... businesses could provide verifiable proofs about qualifications when transacting online?

Mary *owns* this proof-of-status for her business.
Open registry of decentralized identifiers.
We have a *chicken-or-egg* dilemma.

How do we kickstart one side of the market?
What can services plug into to get things rolling?
TheOrgBook fills that role and *unlocks* the hidden value of BC Registries data.

Registration, permit, and license services can plug into incorporated businesses.
Digitally signed and sealed verifiable claims

Welcome to British Columbia's verifiable organizations.

A global, open blockchain registry
The new enrollment experience is more convenient ...

... with a global, open blockchain registry.
Mary will ultimately own her proof-of-status and store it in her own digital wallet ...

... which opens up even more service possibilities ...
So what is the difference?

And what is different about the role of government?
And in what sense is the credential “owned” by each person?
In the **centralized model**, the credential is stored in a record in a database on a server.
Well-managed databases are backed up routinely ...

but still pose a **single point of failure** that is vulnerable to corruption or security threat.
Database coordination is a logistical headache ...

and create access and verification complexities.
Centralized databases also create gatekeepers who act as bottlenecks in the system.
When a credential is shown to a verifier with a proof of ID, verification is highly fallible.
Fancy print gimmicks might make a credential seem authentic but these are easy to forge these days.
Systems for verification are overly complex ... and create privacy problem.
A decentralized verifiable credential is carried by the holder on a smart phone or other computing device. The phone does a lot of the work as the holder’s agent.
The credential definition is *created* and published on the blockchain (ledger) by an issuer.
The blockchain is just a folder full of text files.

The folder is public.

No sensitive information is put on the blockchain.

Once written, cryptographic codes (hashes) prevent changes.

The blockchain is permissioned: only authorized entities can add to it
Getting a credential is back-and-forth ceremony.
HI ... I'D LIKE TO ESTABLISH A RELATION.
OKAY ... WHO ARE YOU?
I'M MARY ... HERE IS A CREDENTIAL I ALREADY HAVE TO PROVE WHO I AM.
CONFIRMED ... HERE ARE SOME QUESTIONS FOR OUR OWN RECORDS.
OKAY ... HERE ARE THE ANSWERS.
GREAT! YOU QUALIFY.

HERE IS THE CREDENTIAL.
The credential is a package of data that is now on the phone.

The credential is given directly to the holder by the issuer. No data was put on the blockchain.
A similar *ceremony* happens with the verifier.
I WOULD LIKE PROOF YOU HOLD THE CREDENTIAL.
HEY, MARY ... HE WANTS PROOF. DO I HAVE PERMISSION TO SEND?
YES.
Here is the proof.
ONE MOMENT ... I AM CHECKING THE CREDENTIAL DEFINITION ON THE BLOCKCHAIN
CONFIRMED! YOUR CREDENTIAL IS VALID.
In this scenario, the identity information can be the minimum required, with no extra “data exhaust” divulged. It is like showing an ID card with parts redacted.
... so that Mary can focus on what she does best.