DIGITAL TRUST

The Underlying Technology
For More Information

VON Project Information - https://vonx.io

Individuals:
John Jordan – john.jordan@gov.bc.ca
Stephen Curran – swcurran@cloudcompass.ca
Ian Costanzo - ian@anon-solutions.ca

References provided on the last slide of this deck.
Benefits for Government

- Data Integrity
- Data Utilization
- Savings

Benefits for Business

- Clarity
- Convenience
- Data Control
Think of the various enablers and influencers to identity as a solar system.
WEB STANDARDS

AUTHENTICATION STANDARDS

DIACC
DIGITAL ID AND AUTHENTICATION COUNCIL OF CANADA

PAN-CANADIAN TRUST FRAMEWORK

VERIFIABLE PERSON

VERIFIABLE ORGANIZATION

VERIFIABLE RELATIONSHIPS
1. Who issued the claim
2. To whom it was issued
3. Not altered
4. Not revoked
Digitally signed and sealed **verifiable credentials**

TheOrgBook

Welcome to British Columbia's verifiable organizations.

**search**

A global, open blockchain registry
Stored in the digital wallet of the credential holder
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.
Systems for verification are overly complex ... and create privacy problem.
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.
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 CONNECTION.
What’s on the Ledger: DIDs

• Decentralized Identifiers – DIDs (W3C Spec)
• Created by their owner – no central issuer
  Globally Unique (GUID)
  Resolvable (like a URL) to a DID Document (DIDDoc)
• DIDDoc contains:
  Public Keys – owner holds the private keys
  Endpoint – a location to contact the owner
• Result: A peer-to-peer, secure communication path

• Hyperledger Indy Optimization
  Limited DIDs on Ledger; most are peer-to-peer
  In our scenario – only one Issuer DID is on the ledger
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.
What’s on the Ledger: Schema, CredDef

• Schema – list of claims in the Credential
• Credential Definition – Links:
  1. DID of the Issuer
  2. Schema
  3. Public keys used to sign each claim
  4. Revocation Registry
• Enables:
  Who issued the Credential – by resolving the Issuer’s DID
  Claim has not been altered – keys signed the data
  Claim has not been revoked – tricky!

• Result: Three of four elements of the Verifiable Credential Proof
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.
What’s NOT on the Ledger: Data, Link Secret

• Claims Data
• Blinded Link Secret
  Cryptographic data inside credential that only the Holder can prove
  Holder keeps the Link Secret (a private key) in their wallet
  Public keys used to sign each claim

• Enables:
  Proving to whom the credential was issued – must have Holder’s Link Secret

• Result: Four of four elements of the Verifiable Claim Proof
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?
HERE IS THE PROOF.
ONE MOMENT ... I AM CHECKING THE CREDENTIAL DEFINITION ON THE BLOCKCHAIN
CONFIRMED! YOUR CREDENTIAL IS VALID.
HL Indy privacy enhancing capabilities:

- Selective Disclosure
- Zero-Knowledge Proof (ZKP)

VERY complex cryptography
Hyperledger Project Ursa
When mainstream...

Verifiers will be able to hold less toxic data. Data from breaches won’t be accepted.

*Prove that this SIN was issued by CRA to you.*
Database coordination becomes easier...

Authoritative data pivots around the subject – you.
The gatekeeper becomes you.
Systems for verification are simpler ... and privacy preserving.
References

Slide 4:
DIACC - https://diacc.ca/
Pan-Canadian Trust Framework - https://diacc.ca/pan-canadian-trust-framework/

Slide 5:
Linux Foundation - https://www.linuxfoundation.org/
Hyperledger - https://www.hyperledger.org/
Hyperledger Indy - https://www.hyperledger.org/projects/hyperledger-indy

Slide 6:
W3C Verifiable Claims Working Group - https://www.w3.org/2017/vc/WG/
DID Spec. - https://w3c-ccg.github.io/did-spec/

Slide 7:
Sovrin Foundation - https://sovrin.org
VON Project Information - https://vonx.io

Slide 8:
Verifiable Credentials Data Model and Explanation - https://w3c.github.io/vc-data-model/

Slide 42: