# Block This Way: Securing Identities using Blockchain

James Argue, Stephen Curran

●

BC Ministry of Citizens' Services

February 7, 2018

# The Identity on the Internet Challenge

***The Internet was built without a way to know who and what you are connecting to.[1]***

"On the Internet, nobody knows you're a dog."

[1] Kim Cameron – Architect of Identity, Microsoft Corporation
https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

# The Evolving Addition of Identity to the Internet

- Fundamentals: Modern Cryptography
  - Data encryption for safe storage and transfer
  - Key management – traditional approaches
- Self-Sovereign Identity - Verifiable Digital Identity
  - Requirements
  - Enabling Technologies – Decentralized IDs, Blockchain and Verifiable Claims
  - Building the concept of “Web of Trust”
- Along the Way: Performances and Demonstrations
  - Cryptography basics , Blockchain and Verifiable Claims

# Your Guides

- James D. Argue, Ministry of Citizen Services, BC Government
  - Team Lead, Network Security Architect, Information Security Branch
  - CISSP, MCSE
- Stephen Curran, Cloud Compass Computing, Inc.
  - The Verifiable Organizations Network (VON) Project
  - Ministry of Technology, Innovation and Citizens’ Services, BC Government
- Maher Bouidani, University of Victoria (Co-Op)
  - The Verifiable Organizations Network (VON) Project
  - Ministry of Technology, Innovation and Citizens’ Services, BC Government

# Over to James...

Block This Way: Securing Identities using Blockchain

# Decentralized Identity, Blockchains and Verifiable Claims

Verifiable Organizations Network (VON)
MTICS - Government of BC
February 7, 2018

# The Evolving Addition of Identity to the Internet

- ✅ Fundamentals: Modern Cryptography
  - Data encryption for safe storage and transfer
  - Key management – traditional approaches
- Self-Sovereign Identity - Verifiable Digital Identity
  - Requirements
  - Enabling Technologies – Decentralized IDs, Blockchain and Verifiable Claims
  - Building the “Web of Trust”
- Along the Way: Performances and Demonstrations
  - Cryptography basics , Blockchain and Verifiable Claims

# Self-Sovereign Digital Identity

Lifetime portable identity for any person, organization, or thing that does not depend on any centralized authority and can never be taken away

# Current Identity Handles

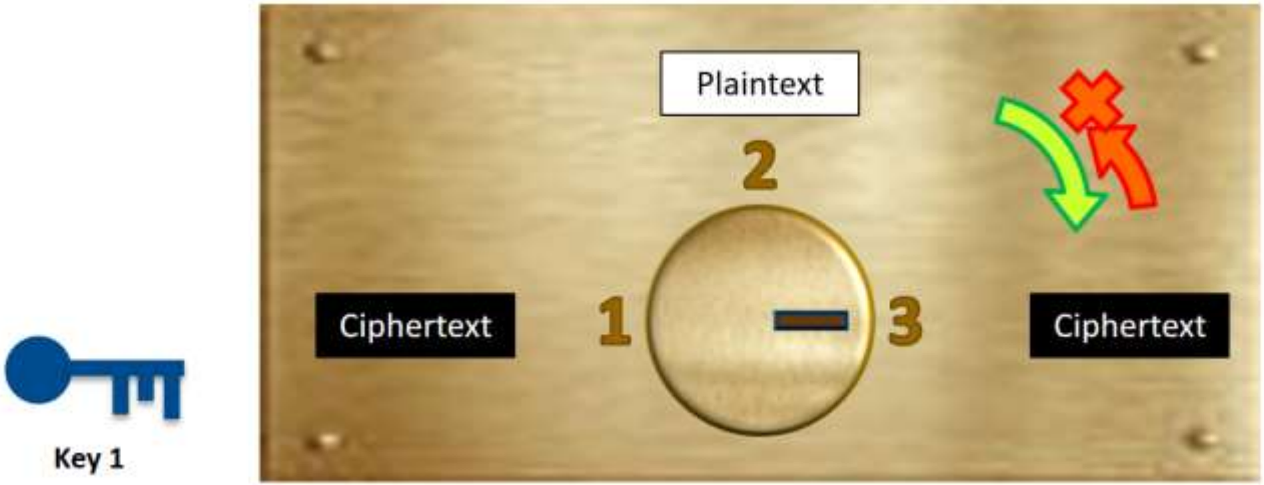
- Name - Stephen Curran (not unique)
- Phone Number - 250-857-1096 (changes, central auth, can be taken away)
- Email Address - swcurran@cloudcompass.ca (changes, central authority)
- URL - www.linkedin.com/in/stephen-curran-4146321 (same issues)
- SIN/SSN/DL - Unique, central authority
- Biometrics - Unique, but if compromised...

# From Centralized to Decentralized

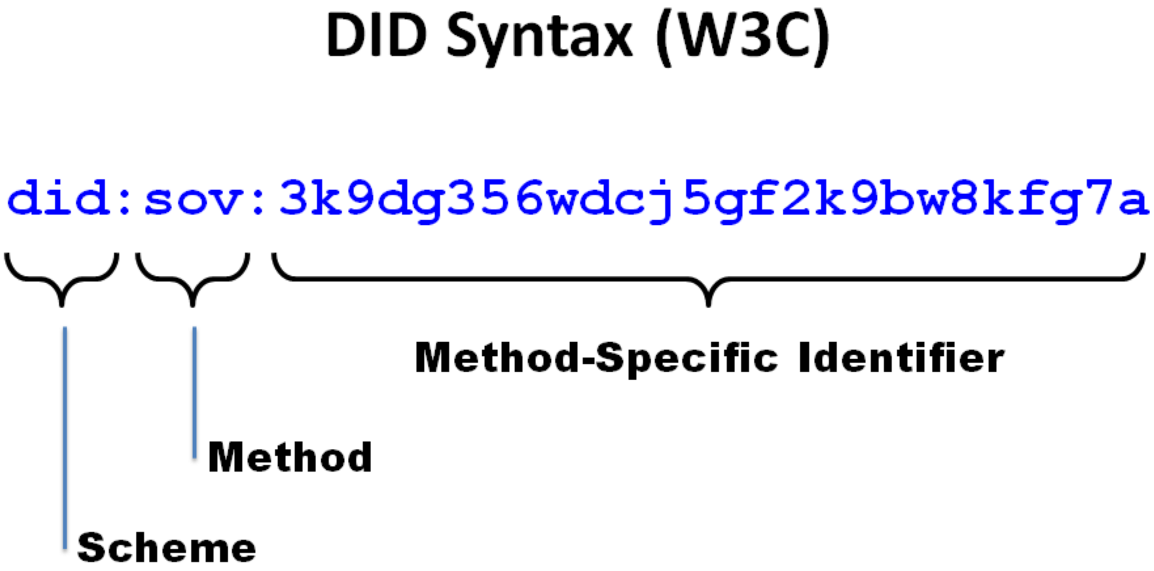
- CAs are out as the suppliers of authority
- Elements:
    - Asymmetric keys (crypto) for all identity owners - including citizens
    - Decentralized IDs - DIDs - are the promised SSI Identifiers
    - Blockchain - the Distributed Key Management System (DKMS) platform
    - DIDs are registered and found on a Blockchain
    - Non-Correlation is paramount
    - Verifiable Claims
    - Trust built on evidence

# Asymmetric Crypto - Keys

- What James talked about...
- Public and Private Keys
- Proof of Digital Identity = Proof of Control of Private Key
    - Can read and respond to messages encrypted with Public Key



# Decentralized Identifiers (DIDs)



**DID Syntax (W3C)**

did:sov:3k9dg356wdcj5gf2k9bw8kfg7a

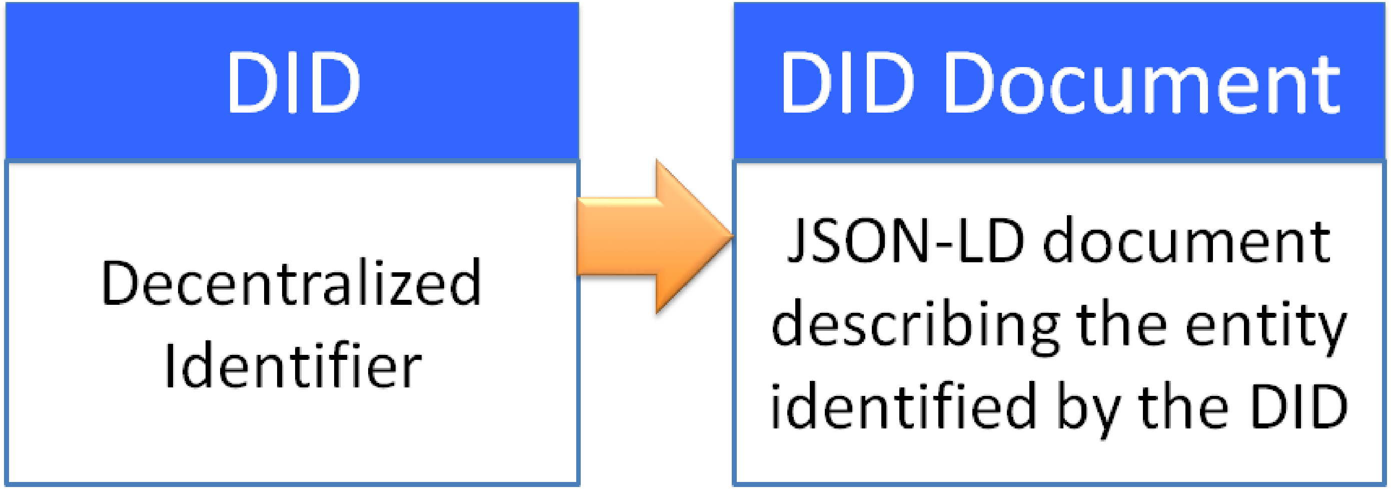
Method-Specific Identifier

Method

Scheme

# DIDs and DID Documents

{ “Key”: “Value” }



DID

Decentralized Identifier

DID Document

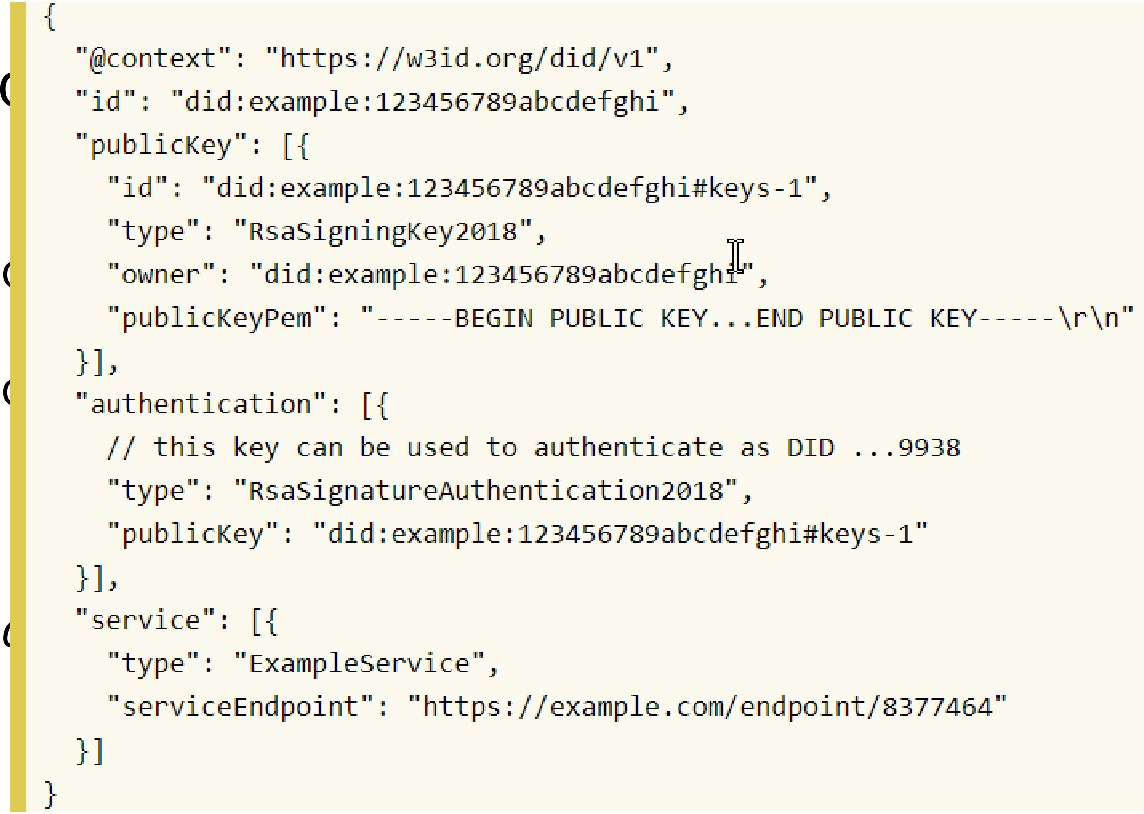
JSON-LD document describing the entity identified by the DID

# Lookup a DID to find a (JSON) DID Document

DID Do containing:

1. DID
2. Set c
    a.
3. Set c

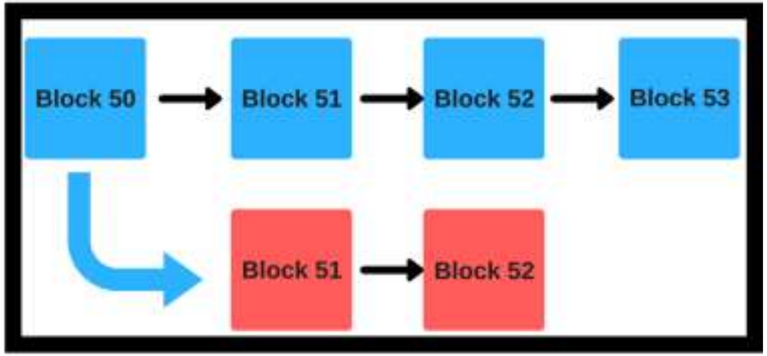
*Publishe*



```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaSigningKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    // this key can be used to authenticate as DID ...9938
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

# Blockchain - in 60 seconds (120? More?)

- A write-once (immutable) database – a shared ledger
- Implemented across many nodes on a peer-to-peer network
- Write process:
  - Pending writes (transactions) are broadcast to all write nodes
  - Hashing applied to build chained immutable blocks – broadcast back to network
    - Demo of mining: [https://anders.com/blockchain/hash.html](https://anders.com/blockchain/hash.html)
- Consensus algorithm to agree on the “next block” to create a single chain



# Blockchain - in 60 seconds (120?) (more??)

- “Chaining” makes it really, really hard to change historical records
    - and really easy to detect when someone is trying to do so
- Public/Private Key used to prove:
    - Identity – prove control
    - Access rights – prove you have the resource

# Blockchain Governance Models

| | | Validation | |
|---|---|---|---|
| | | Permissionless | Permissioned |
| Access | Public | Bitcoin, Ethereum, IOTA, Veres One | Sovrin, IPDB |
| | Private | N/A | Hyperledger (Fabric, Sawtooth, Iroha), R3 Corda, CU Ledger |

# Blockchain and DIDs

- Public DIDs and DID Documents go on the Blockchain
    - We'll get to private ones
- Result: Distributed Key Management System with no central authority
    - If I have your DID, I can:
        - Find out your public keys (that's a good thing!)
            - Only you will understand my message (you have the private key)
        - Find out endpoints I can use to contact you
    - Warning: Many details glossed over…

- General rule - on any public Blockchain - NO PRIVATE DATA
    - Even if it is encrypted!

# DIDs and Non-Correlation

- Prevent monitoring public activity to learn about identities
    - Data at rest - e.g. DIDs on the Blockchain, DIDs in databases
        - Email, SSN, Phone Number, etc.
    - Data in motion – e.g. connections between websites
- Solution - pair-wise DIDs
    - Each identity owner doesn’t have just one DID
    - They have one ***per*** relationship
        - Bank, Government Service 1, Gov’t Service 2, Email Server, Father, etc.
        - Pair-wise DIDs are private between the participants
            - No way to understand them
            - No way to correlate activities between them
    - Private DIDs need not go on the Blockchain - just shared between the participants
        - Protocol to establish connection between identities

# REVIEW: From Centralized to Decentralized

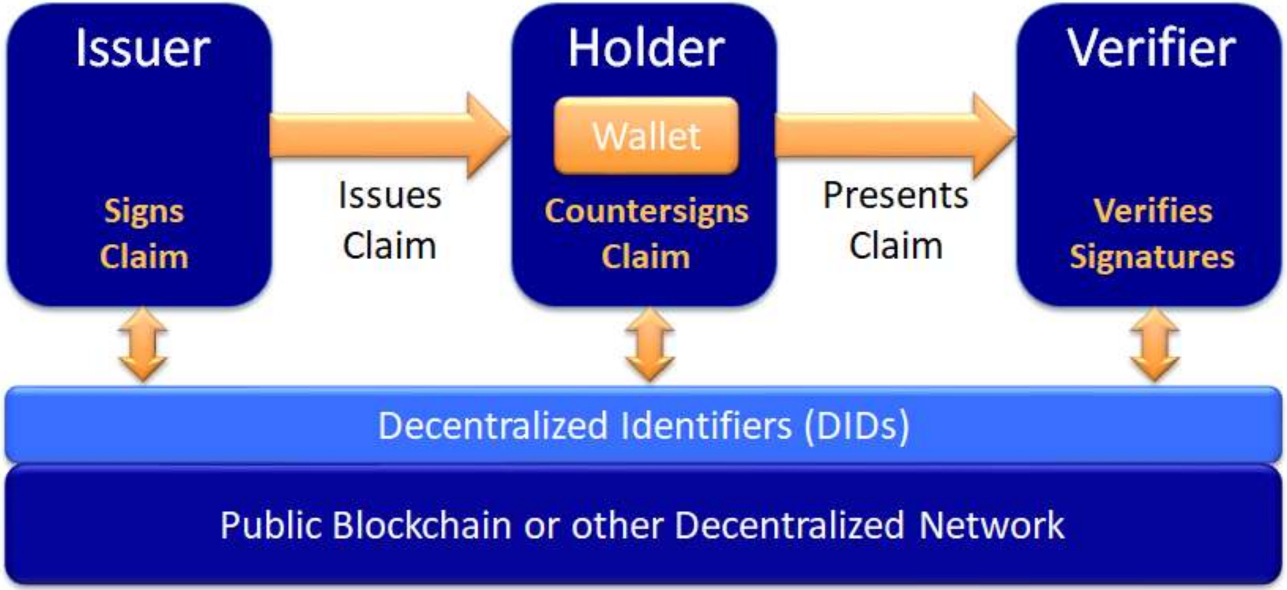
- CAs are out as the suppliers of authority
- Elements:
    - ✅ Asymmetric keys (crypto) for all identity owners - including citizens
    - ✅ Decentralized IDs - DIDs are the promised SSI Identifiers
    - ✅ Blockchain - the Distributed Key Management System (DKMS) platform
    - ✅ DIDs are registered and found on a Blockchain
    - ✅ Non-Correlation is paramount

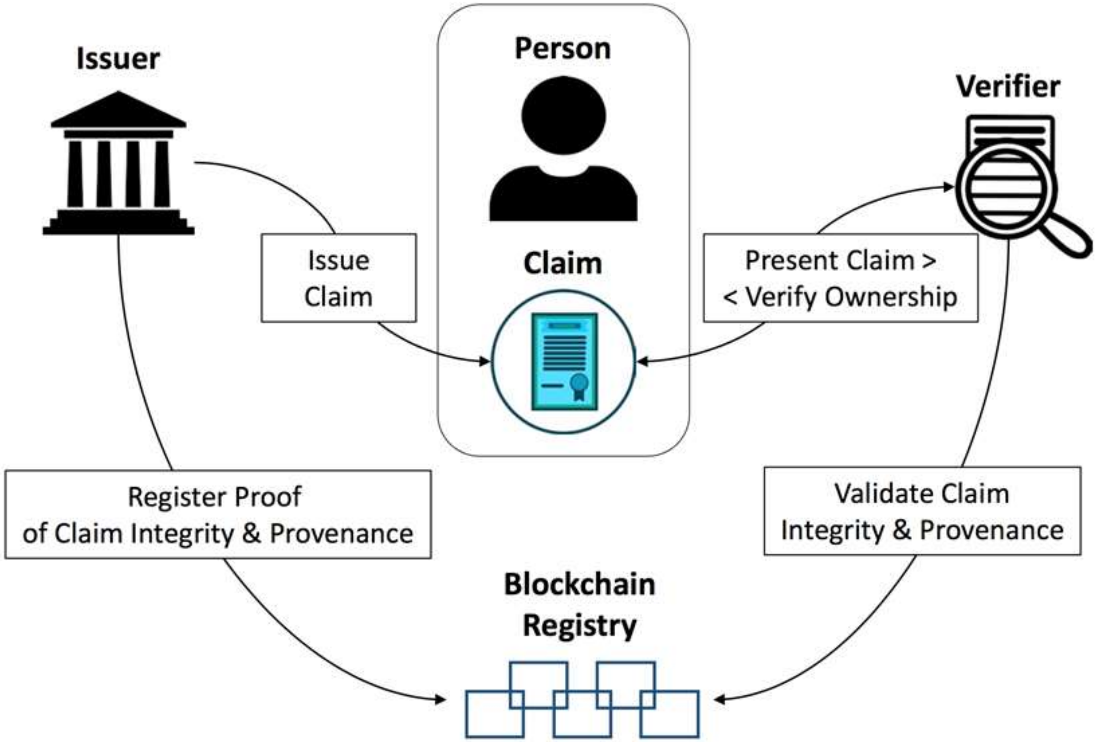
Private, asymmetric key encrypted, pairwise communication channels.
What can we do now?

- Verifiable Claims
- Trust built on evidence

# Verifiable Claims - W3C Standard

Cryptographically signed data exchanged between identities



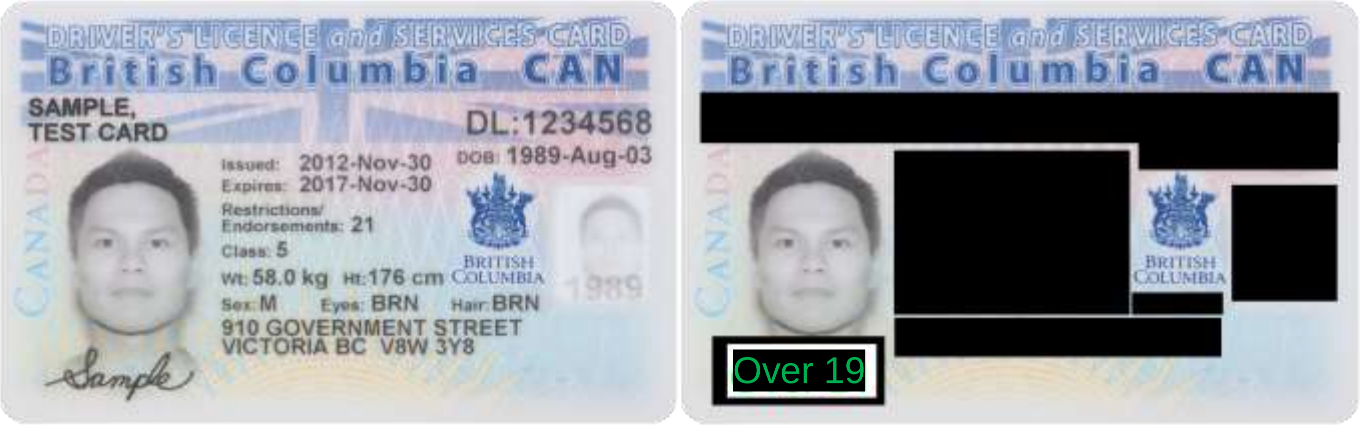


- Cryptographically signed:
  - Disclosed with consent of Person
  - Issued by the Issuer (via DID)
  - Held by the Prover
    - Name: John Smith
    - Has Bank Account: True
    - Client For > 3 Years: Yes
  - Not tampered with
  - Not revoked

- Exercise for Verifier
  - Do I trust the issuer?

# Features of Verifiable Claims

- Deep, deep crypto
  - Not just encrypt/decrypt but use of signing and beyond for proof of issuer, holder
- Selective Disclosure
  - Select information - only some fields from claim – eg. at Pub



DRIVER'S LICENCE and SERVICES CARD
British Columbia CAN
SAMPLE,
TEST CARD
DL:1234568
Issued: 2012-Nov-30
Expires: 2017-Nov-30
DOB: 1989-Aug-03
Restrictions/
Endorsements: 21
Class: 5
Wt: 58.0 kg Ht: 176 cm
Sex: M Eyes: BRN Hair: BRN
910 GOVERNMENT STREET
VICTORIA BC V8W 3Y8

DRIVER'S LICENCE and SERVICES CARD
British Columbia CAN
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
Over 19

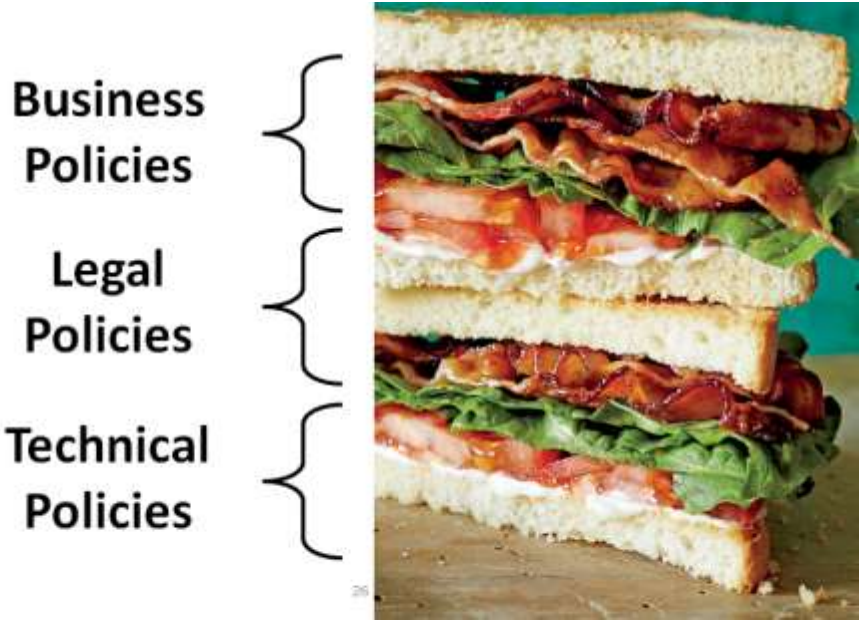
# Features of Verifiable Claims

- Verification is between ***Holder*** and ***Verifier***
  - No information goes to the Issuer
  - Information on the blockchain is accessed:
    - Schema Information - structure of the data
    - Claim Issuer Data - links Schema, Issuer, Revocation Registry

Exercise for the Verifier – do they ***TRUST*** the Issuer?

# Trust Framework

A set of business, legal, and technical rules which members of a community agree to follow in order to achieve trust online



# Trust Framework Examples

- DIACC Pan-Canadian Trust Framework
  - https://diacc.ca/2016/08/11/pctf-overview/
- Sovrin Trust Framework
  - International Non-Profit - http://www.sovrin.org
  - Board of Trustees - 12 Members - Governs Trust Framework
    - Controls selection of Stewards - permissioned blockchain operators
  - Technical Governance Board
    - Governs Open Source foundation code
      - Linux Foundation’s HyperLedger Indy project
    - Sets technical policies implemented in software
- There are others building decentralized identity frameworks and systems

# From Centralized to Decentralized

- CAs are out as the suppliers of authority
- Elements:
  - ✅ Asymmetric keys (crypto) for all identity owners - including citizens
  - ✅ Decentralized IDs - DIDs are the promised SSI Identifiers
  - ✅ Blockchain - the Distributed Key Management System (DKMS) platform
  - ✅ DIDs are registered and found on a Blockchain
  - ✅ Non-Correlation is paramount

Private, asymmetric key encrypted, pairwise communication channels.

  - ✅ Verifiable Claims
  - ✅ Trust built on evidence

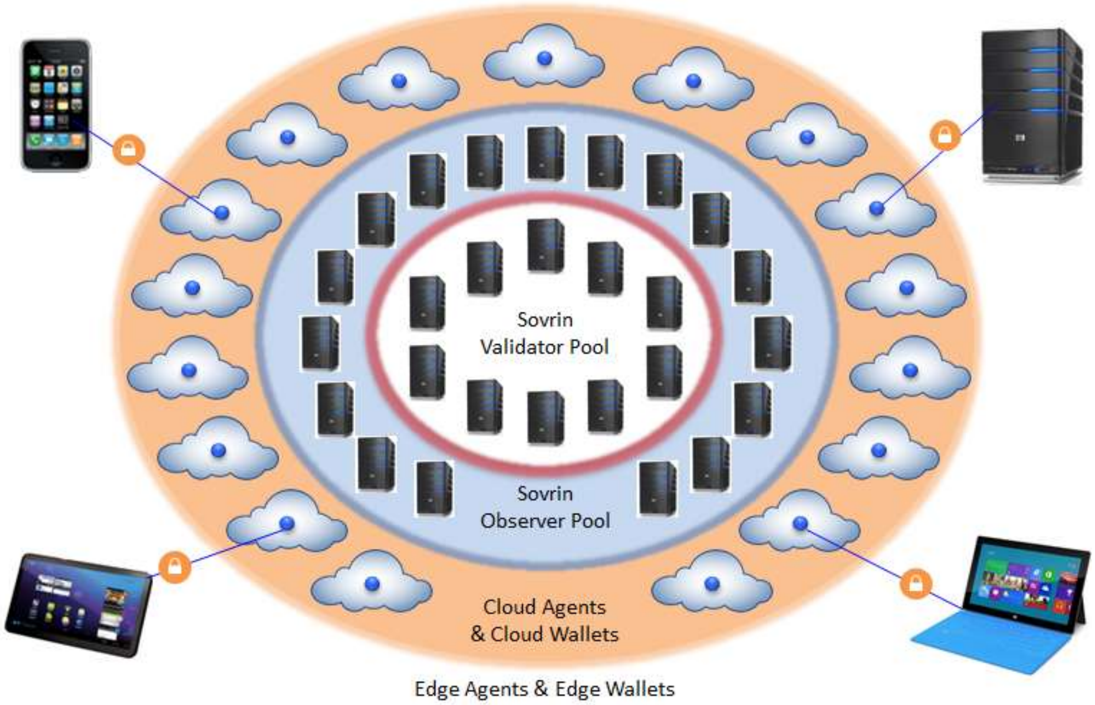
Exchange trusted, signed, verifiable data

# Privacy By Design

- DIDs and Keys - proof of identity - controlled by Identity Owner
    - Not by central stores - Google, Facebook
    - Nirvana: No passwords - just a connection based on DIDs
        - Adding the currently missing Identity Layer to the Internet

- Verifiable Claims - held by Identity Owner
    - Data may not need to be held by issuer - risk mitigation
        - Retrieve data from Owner only as needed - as Verifiable Claim
            - E.g. Name, Address, Credit Card number
        - The only data held - a bunch of uncorrelateable DIDs - no value to hackers
    - Data disclosure controlled by Identity Owner
        - Consent
        - Selective disclosure
    - Nirvana: Unverifiable data is useless - must include proof of issuer/holder

# Sample Self-Sovereign Network Architecture



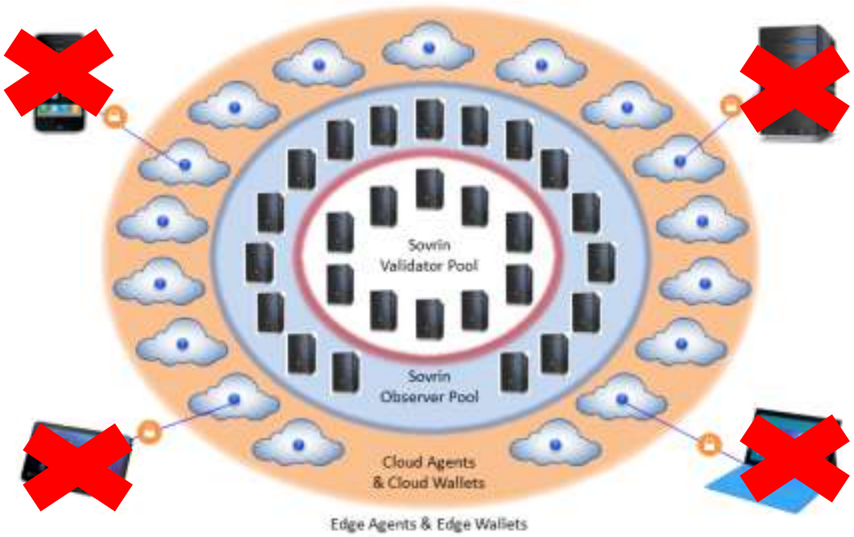
# SSI In Action - BC Government’s VON Project

VON

Verifiable Organizations Network

# Chicken and Egg Problem

- Citizens don’t have wallets so can’t interact with SSI-enabled Services
- Services aren’t SSI-enabled because citizens don’t have wallets



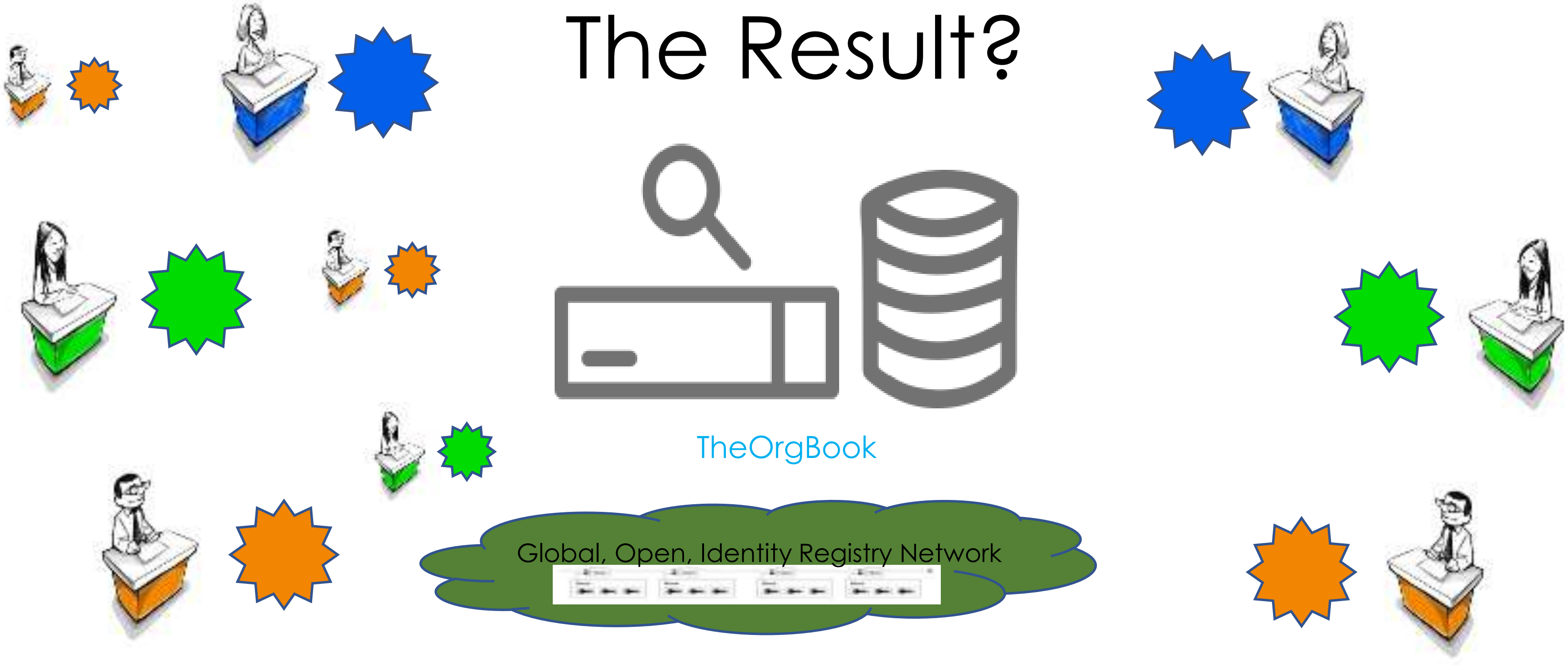
# VON Project - BC Government Experiment

TheOrgBook[1] is to bootstrap Verifiable Claims for Organizations using Public Data

- Government services that print permits extended to “print” verifiable claims
- **Public** Verifiable Claims sent to TheOrgBook - a central claims repository
- Other services can use Verifiable Claims from TheOrgBook
  - Clean data
  - No repeated typing
  - Very lightweight integration - no MOU
- A discovery service for Organizations

**[1] TheOrgBook is to SSI as TheFaceBook was to Social Networks**

# The Result?



TheOrgBook

Global, Open, Identity Registry Network

✓ Identity-Enabled Services – one-side of the market

✓ Services receiving, creating Verified Claims

✓ Patterns (and code!) to SSI-enable more Services

# Demo - TheOrgBook

https://devex-von-test.pathfinder.gov.bc.ca/home

# Workshop- What’s on the Ledger?

- Use Case: Permitify - Getting a Restaurant Permit in Surrey
- Traditional
  - Contact multi-levels of government - in order
  - Enter same information over and over
  - Bring necessary paperwork to prove steps completed
- With TheOrgBook
  - Services are SSI-enabled and can use TheOrgBook
    - Future: Can use Organization’s Wallet or TheOrgBook
  - Recipes of steps to meet business goal: Open A Restaurant
  - Retrieve claims from TheOrgBook based on foundational ID – BC Registries Incorporation
  - Reduce re-typing, need for in-person proofs

# Workshop – What's on the Ledger?

- We'll go Step by Step through process
  - Initialize the Blockchain
  - Initialize the services
  - Generate claims
  - Request proofs - deliver proofs based on claims
- Throughout Showing:
  - What goes on the Blockchain?
- Want to play along?

http://138.197.170.136

# Recap - Looking Forward

- Foundational Technology - Asymmetric Keys - Public/Private
- Centralized and Decentralized Key Management Systems
- Self-Sovereign Identity
    - DIDs, DID Documents and Blockchains
    - Verifiable Claims
- Privacy by Design
    - Data controlled by Identity Owner
    - Used for login
    - Used for proofing “things” to verifiers
- Trust Frameworks
    - You can trust the mechanics (e.g. issuer, holder, tampering, revoked)
    - Can you trust the participants of the network?

# Interested in Learning More?

https://von.pathfinder.gov.bc.ca/

swcurran@cloudcompass.ca