TRANSMUTE

Introduction to Self-Sovereign Identity

INTERNET IDENTITY WORKSHOP #IIW31 | FALL 2020

WELCOME

Nice to Meet You

HOSTS

Karyl Fowler
CEO @Transmute
@TheKaryl
karyl@transmute.industries

Juan Caballero
Comms @Decentralized ID Fdtn
Advisor: Domi Labs, Spruce ID, Spherity GmbH, Korsimoro
@by_caballero
communication@identity.foundation

AGENDA

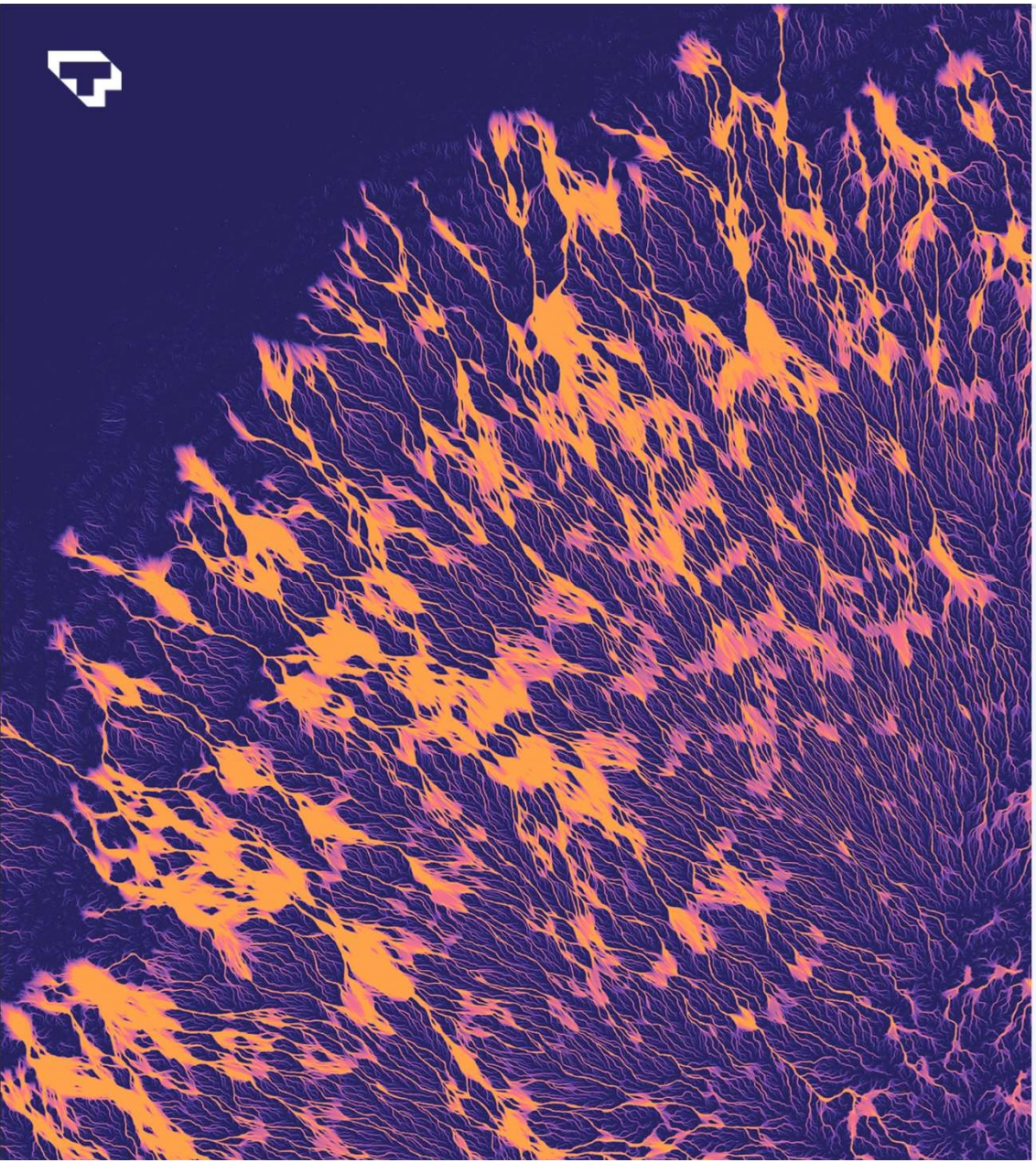
1. Two Tales: Self-Sovereign Identity
2. SSI: The Movement
3. SSI: The Technology
4. Pairing the Two: Uses & Applications
5. Where to Learn More & Get Involved
6. Audience Q&A

TWO PARTS

Self-Sovereign Identity (SSI)

The Movement

The Technology



SELF – SOVEREIGN IDENTITY

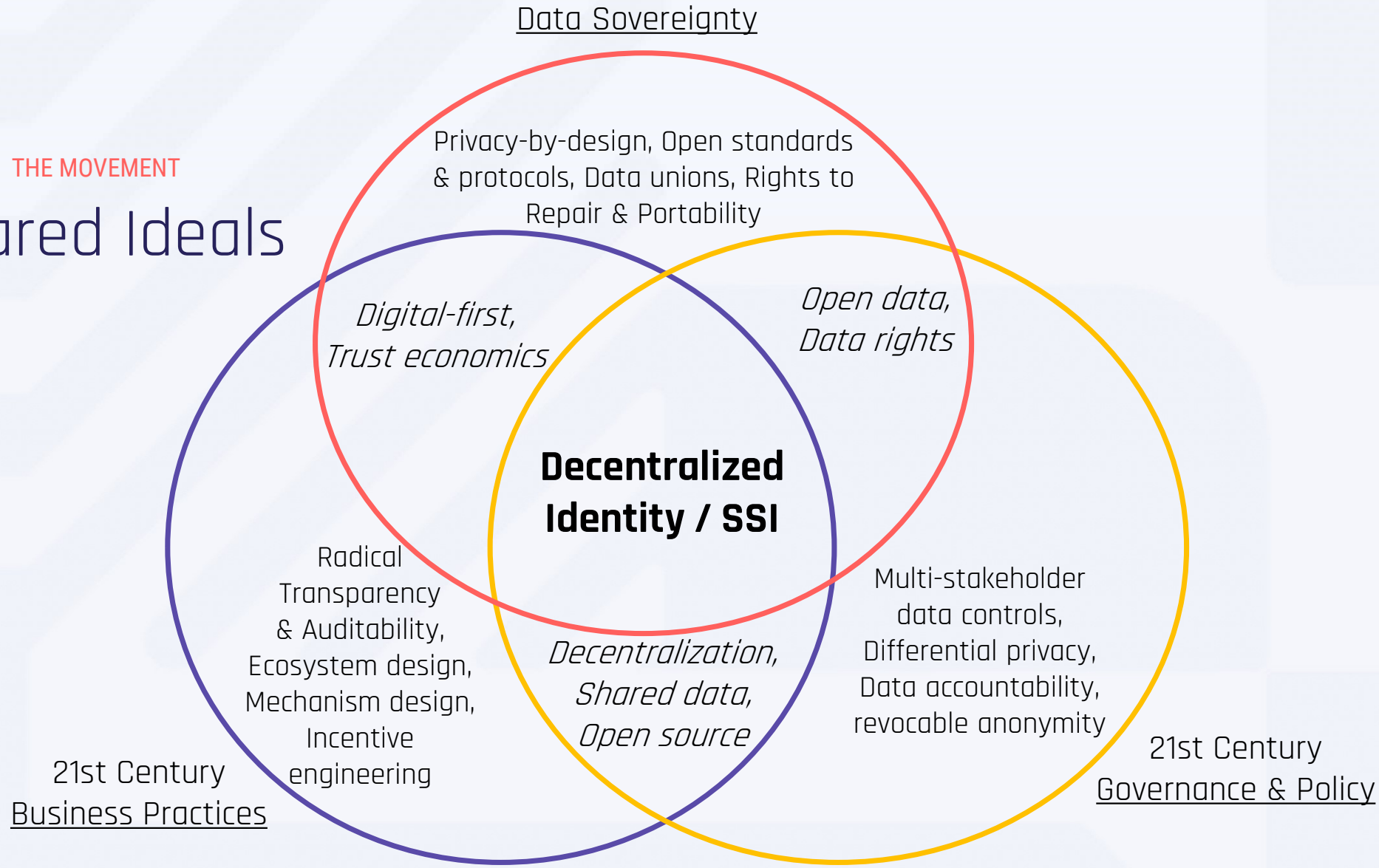
The Movement

Influential writers and essayists:

- **Kim Cameron** ("Laws of Identity", 2005)
- **Doc Searls** (co-founded IIW in 2005 with...)
- **Kaliya Young** (...who gives this talk some years!)
- **Christopher Allen** (author of "10 principles" and of slide #6!)

THE MOVEMENT

Shared Ideals



TWO MAJOR TRACKS

Less Identity + **Trustless** Identity

*"Legally-Enabled Self-Sovereign" Identity**

Key characteristics:

- Minimum Disclosure
- Full Control
- Necessary Proofs
- Legally-Enabled

Or more properly "Trust Minimized" Identity

Key characteristics:

- Anonymity
- Web of Trust
- Censorship Resistance
- Defend Human Rights vs. Powerful Actors (nation states, multi-national corps, mafias, etc.)

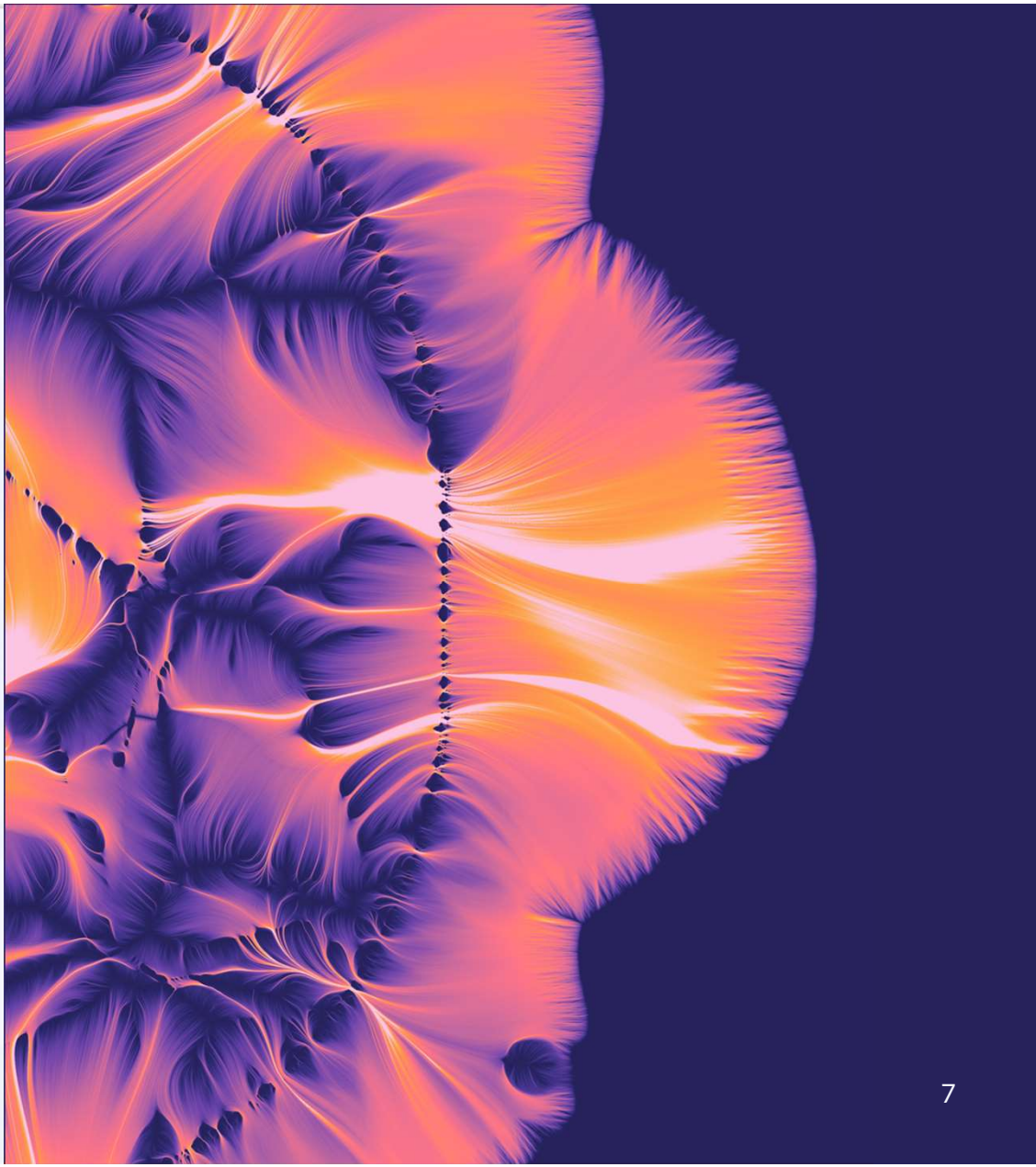
IMEETUP Self-Sovereign Identity

- *Originally coined by Tim Bouma (@trbouma) https://medium.com/@trbouma/less-identity-65f65d87f56b*
- *See also Christopher Allen's presentation at Odyssey 2020*

SLIDE CREDIT: CRISTOPHER ALLEN'S ODYSSEY PRESENTATION 2020

SELF – SOVEREIGN IDENTITY

The Technology



Identity is the gene of software applications.

EXISTING WAY OF DOING THINGS

Centralized Identity

Our “identities” (assembling into “profiles”) are stored away on the servers of identity providers, which own the structure, the content, and the access rights to everything we do.

They lend us a key, but they can change the locks, or throw away the contents. We are but lowly subjects of the data barons.

EXISTING WAY OF DOING THINGS 2.0

Federated Identity

By linking together silos into a “federation,” managers of businesses, platforms and services can outsource the “ID checks” at the door, making them interchangeable and interoperable. Authentication is tricky business, and most relying parties are happy to offload this headache...

...onto ever more powerful middlemen who now hold richer, multi-silo identities on all of us in exchange for this convenience. Single-Sign On makes the data barons into data emperors.

PAST WAY OF DOING THINGS CAUSED

Today's Problems

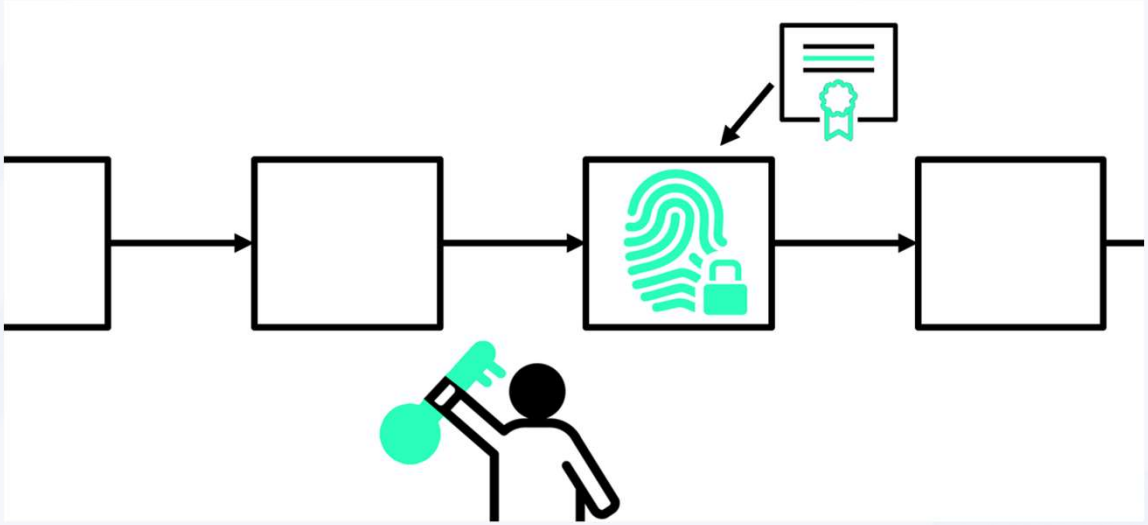
- Usage data collected to create detailed profiles with **all-or-nothing access,** often without any consent, much less **informed** consent
- Who **owns** user data & decides how it's used?
- Difficult to delegate or attenuate access or privileges dynamically or retroactively
- Users **can't control** how their data is secured or shared (or notified if there is a breach)
- Single points of failure and **honeypots** everywhere
- Usernames + Password databases are an attack surface
- **Data bloat:** businesses taking on liability for more data than they need
- There is no identity layer that persists across all systems
- Lacking data portability

SLIDE INSPIRATION: HEATHER VESCENT + KIM HAMILTON DUFFY + KALIYA YOUNG

WEB 3.0 WAY OF DOING THINGS

Decentralized Identity

Blockchains and DLTs aren't perfect, but they're the best way currently stable and production-ready for self-publishing and self-controlling the cryptographic keys for our identity. Some work (such as KERI and Sidetree) are pushing the envelope on other ways of decentralizing public key infrastructure.



Tech Foundations

Decentralized Identifiers (DIDs): self-controlled, digital fingerprints assigned to people, entities, or things

Verifiable Credentials (VCs): Like "files" but with granular controls baked in. Timothy Ruff's "shipping container" analogy is apt.

Resolvers ("Mini DNS"): can function as local namespaces (or not)

Secure Data Storage ("lockers/vaults"): Extend granular controls to underlying data
(new name being announced... tomorrow?)

Cutting-edge **Privacy-preserving Crypto**: Zero-Knowledge, Differential Privacy, MPC, etc

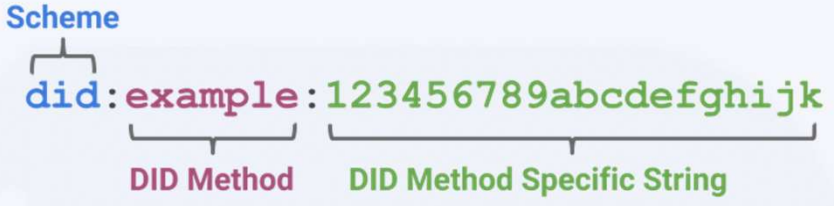
Wallets and/or Agents: Web interfaces beyond the "browser"/"app" paradigm

DEFINITION

Decentralized Identifiers

- A **Decentralized Identifier (DID)** is a new type of identifier that is *globally unique*, *resolvable* with high availability, and cryptographically *verifiable*.

- The purpose of the DID document is to describe the public keys, authentication protocols, and service endpoints necessary to bootstrap cryptographically-verifiable interactions with the identified entity.




```
{
  "@context": ["https://www.w3.org/2019/did/v1", "https://w3id.org/security/v1"],
  "id": "did:example:123456789abcdefghi",
  ...
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }, {
    "id": "did:example:123456789abcdefghi#keys-2",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:example:pqrstuvwxyz0987654321",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }, {
    "id": "did:example:123456789abcdefghi#keys-3",
    "type": "Secp256k1VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyHex": "02b97c30de767f084ce3080168ee293053ba33b235d7116a3263d29f1450936b71"
  }],
  ...
}
```

https://w3c-ccg.github.io/did-primer/

DIFFERENT STROKES FOR DIFFERENT FOLKS

>70 DID Methods Today

Method Name	Status	DLT or Network	Authors	Link
did:abt:	PROVISIONAL	ABT Network	ArcBlock	ABT DID Method
did:btcr:	PROVISIONAL	Bitcoin	Christopher Allen, Ryan Grant, Kim Hamilton Duffy	BTCR DID Method
did:stack:	PROVISIONAL	Bitcoin	Jude Nelson	Blockstack DID Method
did:erc725:	PROVISIONAL	Ethereum	Markus Sabadello, Fabian Vogelsteller, Peter Kolarov	erc725 DID Method
did:example:	PROVISIONAL	DID Specification	W3C Credentials Community Group	DID Specification
did:ipid:	PROVISIONAL	IPFS	TranSendX	IPID DID method
did:life:	PROVISIONAL	RChain	lifeID Foundation	lifeID DID Method
did:sov:	PROVISIONAL	Sovrin	Mike Lodder	Sovrin DID Method
did:uport:	DEPRECATED	Ethereum	uPort	
did:ethr:	PROVISIONAL	Ethereum	uPort	ETHR DID Method
did:v1:	PROVISIONAL	Veres One	Digital Bazaar	Veres One DID Method
did:com:	PROVISIONAL	commercio.network	Commercio Consortium	Commercio.network DID Method
did:dom:	PROVISIONAL	Ethereum	Dominode	
did:ont:	PROVISIONAL	Ontology	Ontology Foundation	Ontology DID Method
did:vvo:	PROVISIONAL	Vivvo	Vivvo Application Studios	Vivvo DID Method
did:aergo:	PROVISIONAL	Aergo	Blocko	Aergo DID Method
did:icon:	PROVISIONAL	ICON	ICONLOOP	ICON DID Method
did:iwt:	PROVISIONAL	InfoWallet	Raonsecure	InfoWallet DID Method
did:ockam:	PROVISIONAL	Ockam	Ockam	Ockam DID Method
did:ala:	PROVISIONAL	Alastria	Alastria National Blockchain Ecosystem	Alastria DID Method
did:op:	PROVISIONAL	Ocean Protocol	Ocean Protocol	Ocean Protocol DID Method
did:jlinc:	PROVISIONAL	JLINC Protocol	Victor Grey	JLINC Protocol DID Method
did:ion:	PROVISIONAL	Bitcoin	Various DIF contributors	ION DID Method
did:jolo:	PROVISIONAL	Ethereum	Jolocom	Jolocom DID Method
did:bryk:	PROVISIONAL	bryk	Marcos Allende, Sandra Murcia, Flavia Munhoso, Ruben Cessa	bryk DID Method
did:peer:	PROVISIONAL	peer	Daniel Hardman	peer DID Method
did:selfkey:	PROVISIONAL	Ethereum	SelfKey	SelfKey DID Method
did:meta:	PROVISIONAL	Metadium	Metadium Foundation	Metadium DID Method
did:tys:	PROVISIONAL	DID Specification	Chainyard	TYS DID Method
did:git:	PROVISIONAL	DID Specification	Internet Identity Workshop	Git DID Method
did:tangle:	PROVISIONAL	IOTA Tangle	BiiLabs Co., Ltd.	TangleID DID Method
did:emtrust:	PROVISIONAL	Hyperledger Fabric	Halialabs Pte Ltd.	Emtrust DID Method
did:ttm:	PROVISIONAL	TMChain	Token.TM	TM DID Method
did:wlk:	PROVISIONAL	Weelink Network	Weelink	Weelink DID Method
did:pistis:	PROVISIONAL	Ethereum	Andrea Taglia, Matteo Sinico	Pistis DID Method
did:holo:	PROVISIONAL	Holochain	Holo.Host	Holochain DID Method
did:web:	PROVISIONAL	Web	Oliver Terbu, Mike Xu, Dmitri Zagidulin, Amy Guy	Web DID Method
did:io:	PROVISIONAL	IoTeX	IoTeX Foundation	IoTeX DID Method
did:vaultie:	PROVISIONAL	Ethereum	Vaultie Inc.	Vaultie DID Method
did:moac:	PROVISIONAL	MOAC	MOAC Blockchain Tech, Inc.	MOAC DID Method
did:omn:	PROVISIONAL	OmniOne	OmniOne	OmniOne DID Method
did:work:	PROVISIONAL	Hyperledger Fabric	Workday, Inc.	Workday DID Method
did:vid:	PROVISIONAL	VP	VP Inc.	VP DID Method
did:ccp:	PROVISIONAL	Quorum	Baidu, Inc.	Cloud DID Method
did:jnctn:	PROVISIONAL	Jnctn Network	Jnctn Limited	JNCTN DID Method
did:evan:	PROVISIONAL	evan.network	evan GmbH	evan.network DID Method
did:elastos:	PROVISIONAL	Elastos ID Sidechain	Elastos Foundation	Elastos DID Method
did:kilt:	PROVISIONAL	KILT Blockchain	BOTLabs GmbH	KILT DID Method
did:elem:	PROVISIONAL	Element DID	Transmute	ELEM DID Method
did:github:	PROVISIONAL	Github	Transmute	GitHub DID Method
did:bid:	PROVISIONAL	bif	teleinfo caict	BIF DID Method
did:ptn:	PROVISIONAL	PalletOne	PalletOne	PalletOne DID Method
did:echo:	PROVISIONAL	Echo	Echo Technological Solutions LLC	Echo DID Method
did:trustbloc:	PROVISIONAL	Hyperledger Fabric	SecureKey	TrustBloc DID Method
did:san:	PROVISIONAL	SAN Cloudchain	YLZ Inc.	SAN DID Method

(Soon to be un:DID?)

https://w3c-ccg.github.io/did-method-registry/

DEFINITION

Verifiable Credentials

- A **verifiable credential (VC)** is a set of *tamper-evident* claims and metadata about real life achievements, qualifications, or attributes that includes a *cryptographic proof* about who issued it.

- Examples of verifiable credentials include digital employee identification cards, digital birth certificates, and digital educational certificates, authentication and authorization bearer tokens, logistics or shipping certifications.


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.gov/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu",
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.com/jdoe/keys/1",
    "jws": "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19
      ..DJBMvvFAIC00nSGB6Tn0XKbbF9XrsaJZREWvR2aONYTQQxnyXirtXnlewJMB
      Bn2h9hfcGZrvnC1b6PgWmukzFJ1IiH1dWgnDIS81BH-IxXnPkbuYDeySorc4
      QU9MJxdVkY5EL4HYbcIfwKj6X4LBQ2_ZHZIu1jdqLcRZqHcsDF5KKylKc1TH
      n5VRWy5WhYg_gBnyWny8E6Qkrze53MR7OuAmmNJ1m1nN8SxDrG6a08L78J0-
      Fbas5OjAQz3c17GY8mVuDPOBIOVjMEghBlgl3nOi1ysxbRGhHLEK4s0KKbeR
      ogZdgt1DkQxDFxxn41QWDw_mmMCjs9qxg0zcZzqEJw"
  }
}
```


https://www.w3.org/TR/vc-data-model/#credentials

SO WHAT?

DIDs + VCs Can...

- Reduce database security risks and business process risks
- Give users increased to total **control** over their identity data and credentials
- Increased **data portability** and near-global scope (for reputation and history)
- Increase business efficiency through **streamlined onboarding & auditing**
  - Reduce fraud by confirming multiple data points
  - Streamline confirmation of compliance data/documentation
- **Increase trust** of any verified data that must be shared downstream, in a form more persistent than the legal persons involved
  - Key use cases: Drug trials, Compliance documents, Provenance data

SLIDE INSPIRATION: HEATHER VESCENT + KIM HAMILTON DUFFY + KALIYA YOUNG

FRAMEWORK FOR ADOPTION

1. Is **selective disclosure** or **privacy** a priority?
2. Is there high **coordination** burden?
3. Is **traceability** or **auditability** important?

Application Areas	
Chains of Custody Commercial + Defense Supply Chain Logistics Cold Chain (pharma to agriculture) Contract Management (Legal, HR, Real Estate) Software	**Data Infrastructure & Governance** Cloud roles + access management Microservices monitoring
Telco 5G + IoT Enablement Identity/Data-as-a-Service Anti-Fraud (verification + roaming)	DIF has a discussion group now! **Healthcare** Insurance + Billing Verifiable Clinical data and/or Device data Patient-centric data sharing + management

RESOURCES

Get Involved

Ideas
(2-10 years)

Meetup

Internet Identity Workshop

eiC 2018

MyData 2018

kantara INITIATIVE

Conversations

Incubation
(6-18 months)

Rebooting the Web of Trust

HYPERLEDGER

Whitepapers, position papers

Refinement
(1-3 years)

W3C Community Groups

DIF

IEEE

Experiments, Specifications, Pilots

Standardization
(~18-24 months)

W3C Word Wide Web Consortium

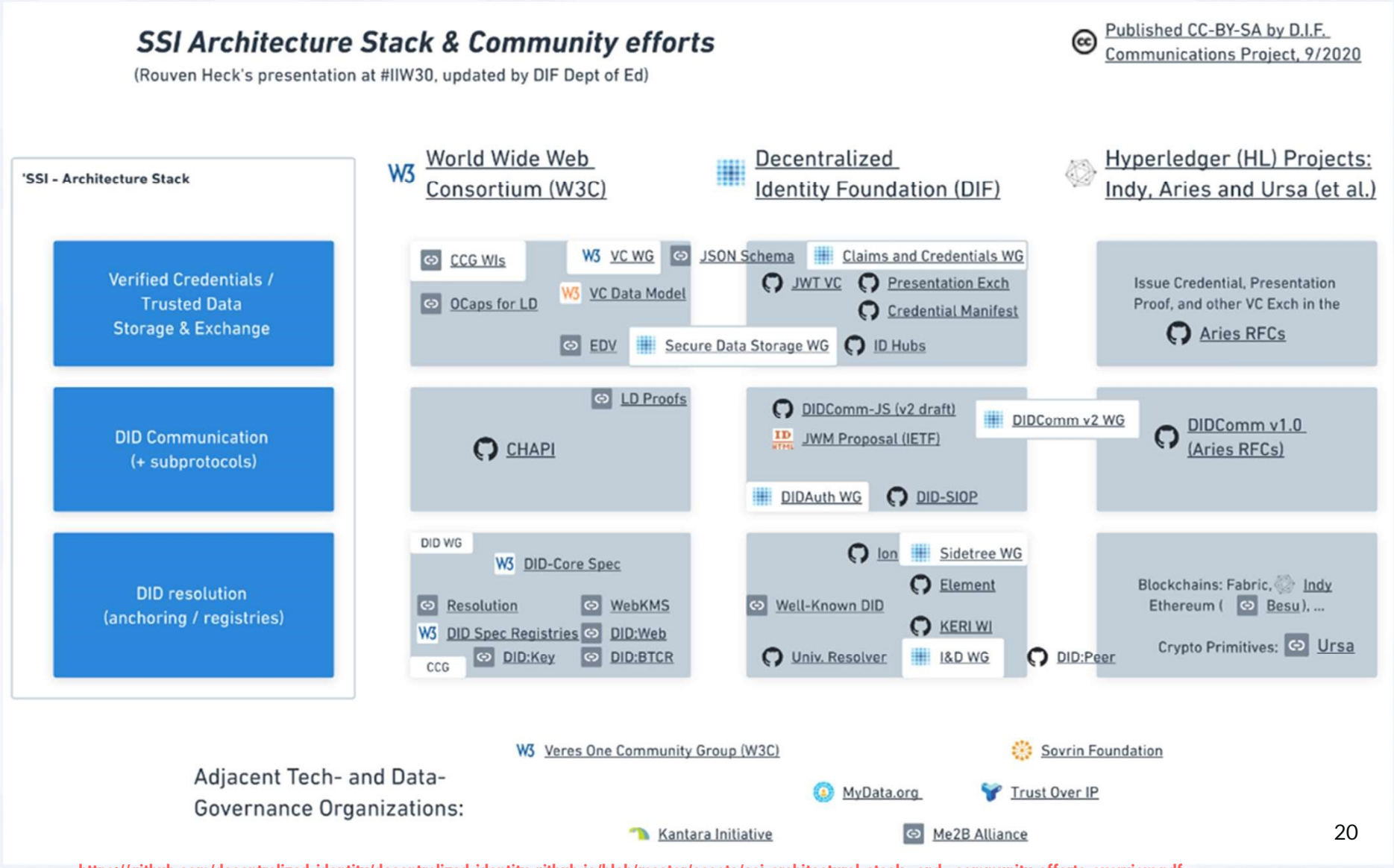
IETF

OASIS

Standards

SLIDE CREDIT: HEATHER VESCENT @ THE PURPLE TORNADO

Get Involved



https://github.com/decentralized-identity/decentralized-identity.github.io/blob/master/assets/ssi-architectural-stack--and--community-efforts-overview.pdf

Knowledge Bases + Educational Materials

More educational diagrams and cheatsheets at https://github.com/decentralized-identity/decentralized-identity.github.io/tree/master/assets/

Primary Sources:

- W3C Credentials Community Group
- DIF Working Group Records
- Rebooting the Web of Trust Conference, Proceedings & Digests
- Internet Identity Workshop (You are here) Conf & Notes

Secondary Sources & Commentaries:

- 2019 IIW Intro to SSI Deck by Heather Vescent + Karyl Fowler + Lucas Tétreault
- 2018 IIW Intro to SSI Deck by Heather Vescent + Kim Hamilton Duffy
- 2018 IIW Intro to SSI Deck by Drummond Reed +
- Infominer's Resources: https://decentralized-id.com/
- The Purple Tornado reports for US DHS (2019)
- PSA (Privacy, Surveillance, Anonymity) Podcast (Kaliya Young, Seth Goldstein)
- SSIMeetup Webinar series (Alex Preukschat)
- Definitely Identity podcast (Tim Bouma)
- One World Identity ("KNOW") Podcast
- MyData Slack and Conference series
- CyberForge (includes some great posts by Anil John, US DHS S&T)
- Transmute TechTalk: On Enterprise Use + Integrations

Monographs:

- Comprehensive Guide to Self Sovereign Identity (2019) - Heather Vescent / Kaliya Young
- Spherity's SSI 101 Series on Medium (2020) - Juan Caballero
- Self Sovereign Identity (2021) - Alex Preukschat / Drummond Reed

Technical Resources:

- W3C DID Specification & Use Case guidance
- W3C VC Data Model Specification
- Digital Credential Consortium whitepaper (Kim Hamilton Duffy)
- Secure Data Storage Specification WG (DIF-W3C)
- Credential Handler API (CHAPI)
- Universal Resolver (Danube Tech)
- Trust Over IP Foundation (TBD)
- DIDcomm WG (DIF-HL Aries)
- Aries RFCs (Hyperledger)

Compiled by Karyl Fowler (Transmute) & Juan Caballero (Spherity)
For #IIW30, 4/28/20

https://github.com/decentralized-identity/decentralized-identity.github.io/raw/master/assets/knowledge-base--april-2020.pdf

Thank You!

QUESTIONS?