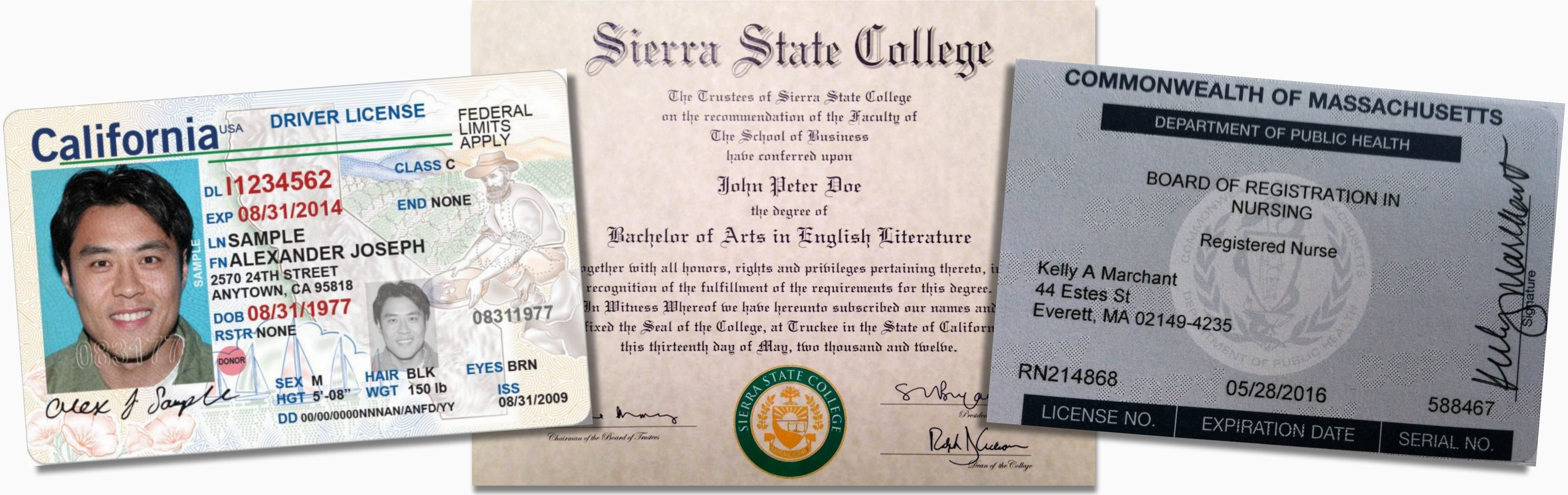
Verifiable Credentials
and
Decentralized Identifiers

What do we mean by Credential?



California USA DRIVER LICENSE

FEDERAL LIMITS APPLY

DL I1234562

CLASS C

EXP 08/31/2014

END NONE

LN SAMPLE

FN ALEXANDER JOSEPH

2570 24TH STREET
ANYTOWN, CA 95818

DOB 08/31/1977

RSTR NONE

08311977

DONOR

SEX M

HGT 5'-08"

HAIR BLK

WGT 150 lb

EYES BRN

ISS 08/31/2009

DD 00/00/0000NNNAN/ANFD/YY

Alex J Sample

Sierra State College

The Trustees of Sierra State College
on the recommendation of the Faculty of
The School of Business
have conferred upon

John Peter Doe

the degree of

Bachelor of Arts in English Literature

ogether with all honors, rights and privileges pertaining thereto, i
recognition of the fulfillment of the requirements for this degree.
In Witness Whereof we have hereunto subscribed our names and
fixed the Seal of the College, at Truckee in the State of Califor
this thirteenth day of May, two thousand and twelve.

Chairman of the Board of Trustees

SIERRA STATE COLLEGE

Preside

Dean of the College

COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF PUBLIC HEALTH

BOARD OF REGISTRATION IN NURSING

Registered Nurse

Kelly A Marchant
44 Estes St
Everett, MA 02149-4235

RN214868	05/28/2016	588467
LICENSE NO.	EXPIRATION DATE	SERIAL NO.

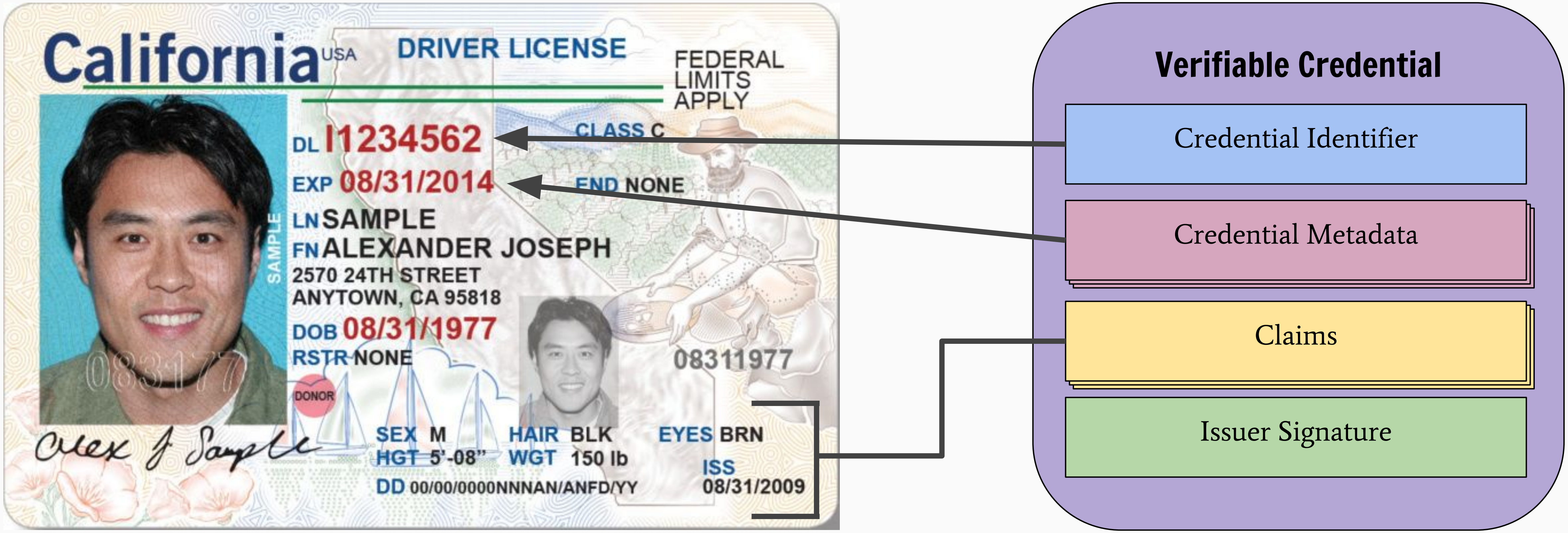
Signature

W3C Verifiable Credentials

The mission of the W3C Verifiable Claims Working Group:

Express credentials on the Web in a way that is cryptographically secure, privacy respecting, and automatically verifiable.

Anatomy of a Verifiable Credential

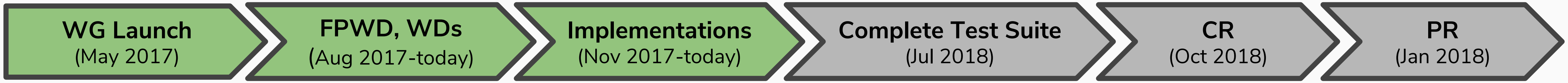


Verifiable Credential

- Credential Identifier
- Credential Metadata
- Claims
- Issuer Signature

Verifiable Credentials Status

Roadmap



WG Launch
(May 2017)

FPWD, WDs
(Aug 2017-today)

Implementations
(Nov 2017-today)

Complete Test Suite
(Jul 2018)

CR
(Oct 2018)

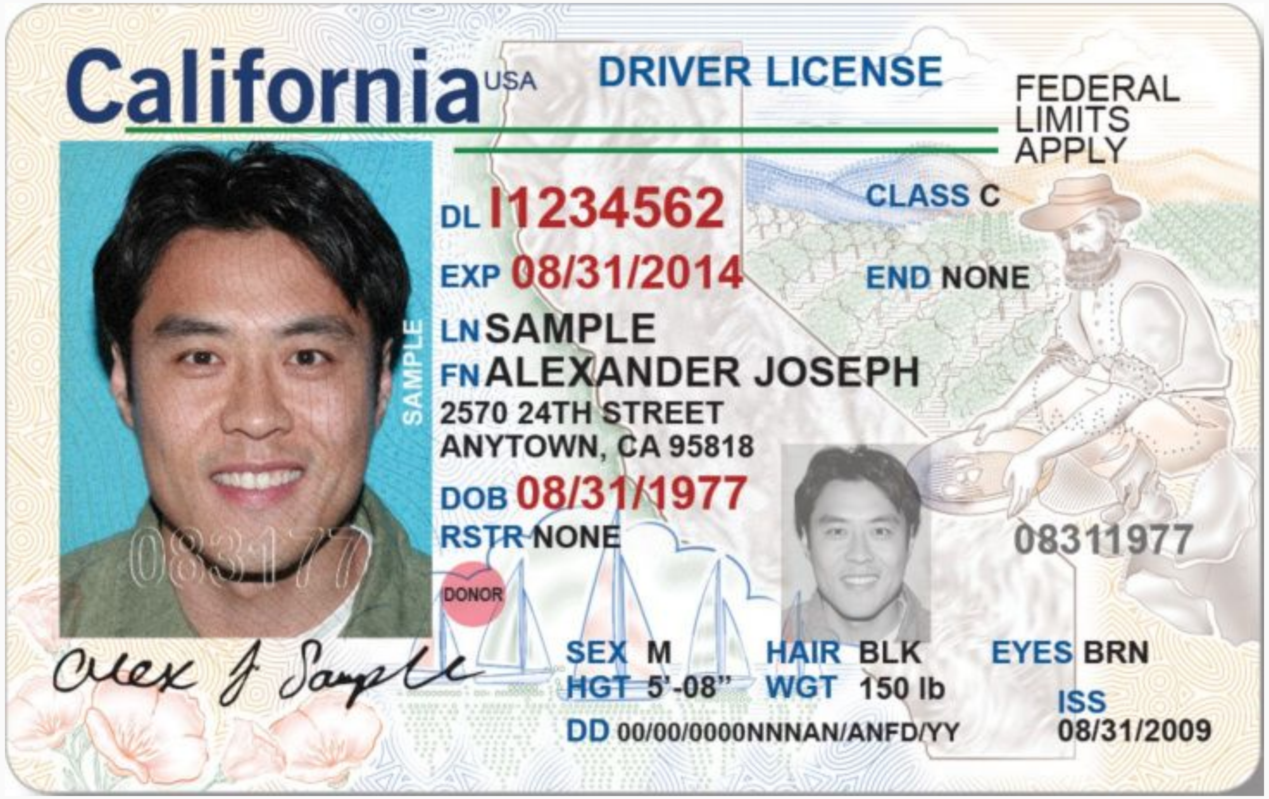
PR
(Jan 2018)

Weekly WG Participants: **12-18 / 50**

Spec/Issue Regular Contributors: **15**

Known Corporate Implementation Commitments: **10**

Anatomy of a Verifiable Credential



California USA DRIVER LICENSE

FEDERAL
LIMITS
APPLY

DL I1234562

CLASS C

EXP 08/31/2014

END NONE

LN SAMPLE

FN ALEXANDER JOSEPH

2570 24TH STREET
ANYTOWN, CA 95818

DOB 08/31/1977

RSTR NONE

SAMPLE

08311977

DONOR

Alex J Sample

SEX M
HGT 5'-08"

HAIR BLK
WGT 150 lb

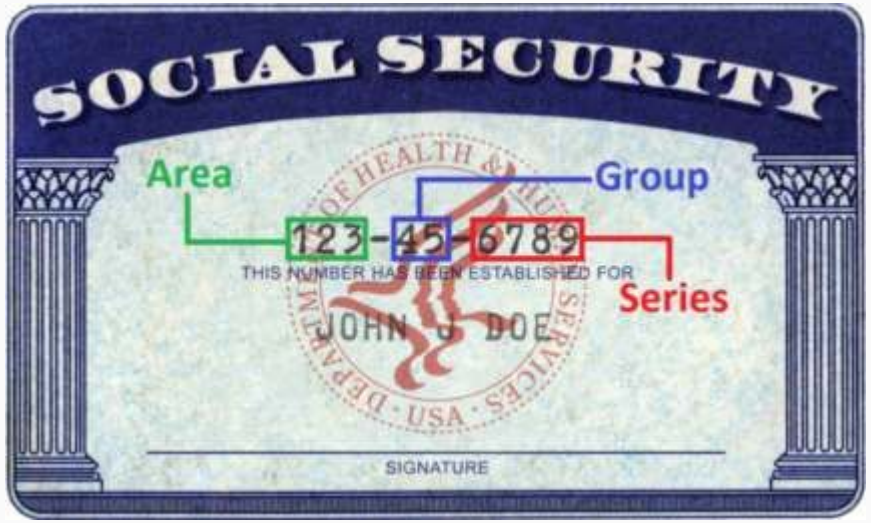
EYES BRN

ISS
08/31/2009

DD 00/00/0000NNNAN/ANFD/YY

- <IDENTIFIER>
  - license: I1234562
  - hair: BLK
  - name: ALEXANDER JOSEPH
  - address: 2570 24th STREET ...
  - date of birth: 08/31/1977
  - issued by: California DMV
  - digital signature: MIIB7ZueKqp...

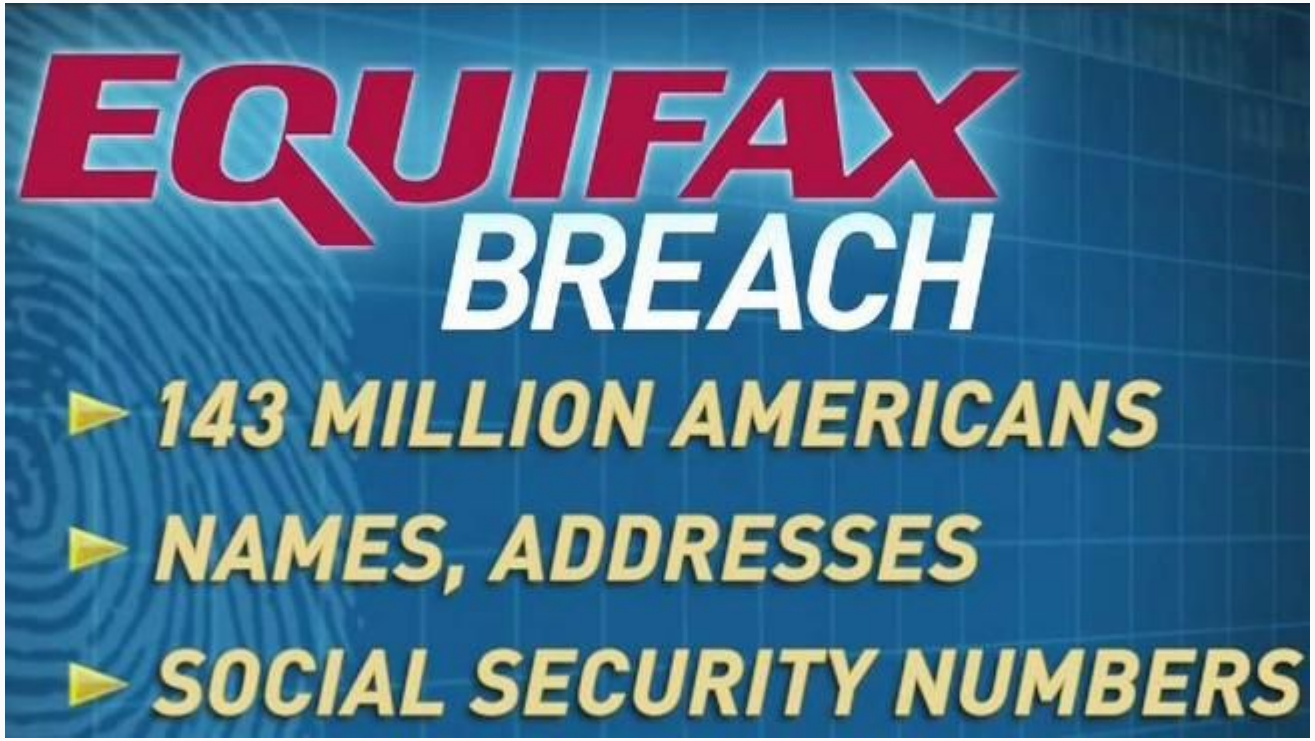
Which identifiers do we use today?



jdoe@bigcorp.com

https://flitter.com/jdoe

Why is this a problem?

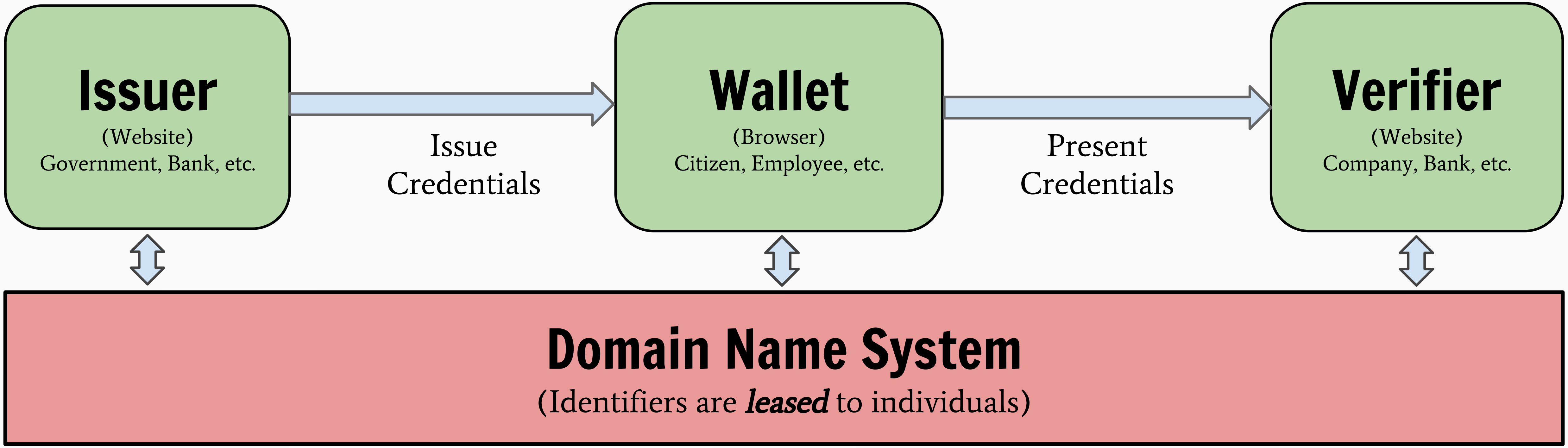


The Web’s Identifier Problem

To date, every identifier you use online does not belong to you; it belongs to someone else.

This results in problems related to cost, data portability, data privacy, and data security.

Web Identifiers Today



Issuer

(Website)
Government, Bank, etc.

Issue Credentials

Wallet

(Browser)
Citizen, Employee, etc.

Present Credentials

Verifier

(Website)
Company, Bank, etc.

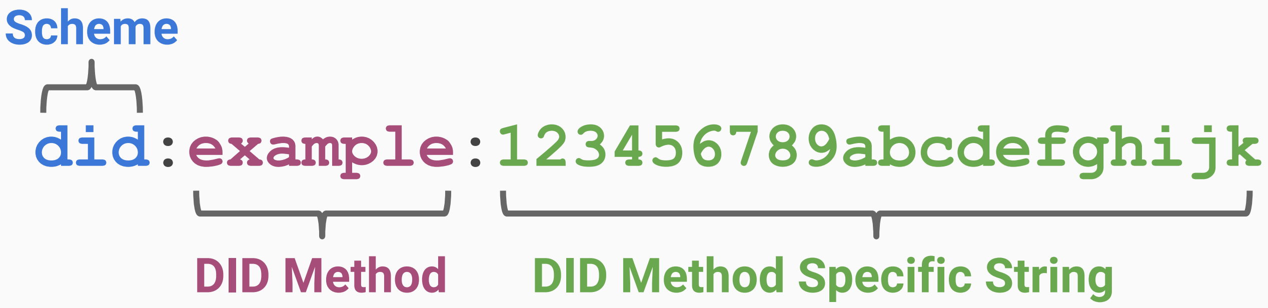
Domain Name System

(Identifiers are ***leased*** to individuals)

A Compelling Solution

Lifetime portable identifiers for any person, organization, or thing that does not depend on any centralized authority, are protected by cryptography, and can never be taken away.

What does a DID look like?



Scheme

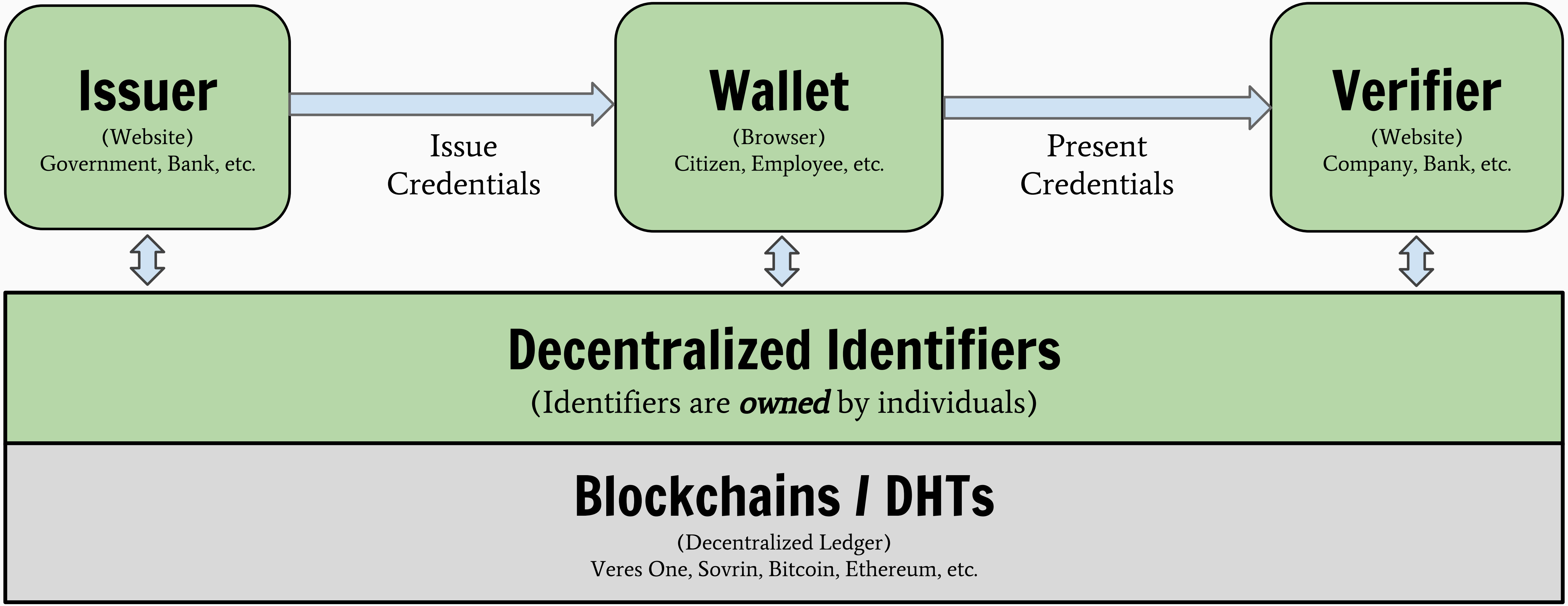
did:example:123456789abcdefghijk

DID Method

DID Method Specific String

did:v1:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD

Decentralized Identifiers



Issuer

(Website)
Government, Bank, etc.

Issue Credentials

Wallet

(Browser)
Citizen, Employee, etc.

Present Credentials

Verifier

(Website)
Company, Bank, etc.

Decentralized Identifiers

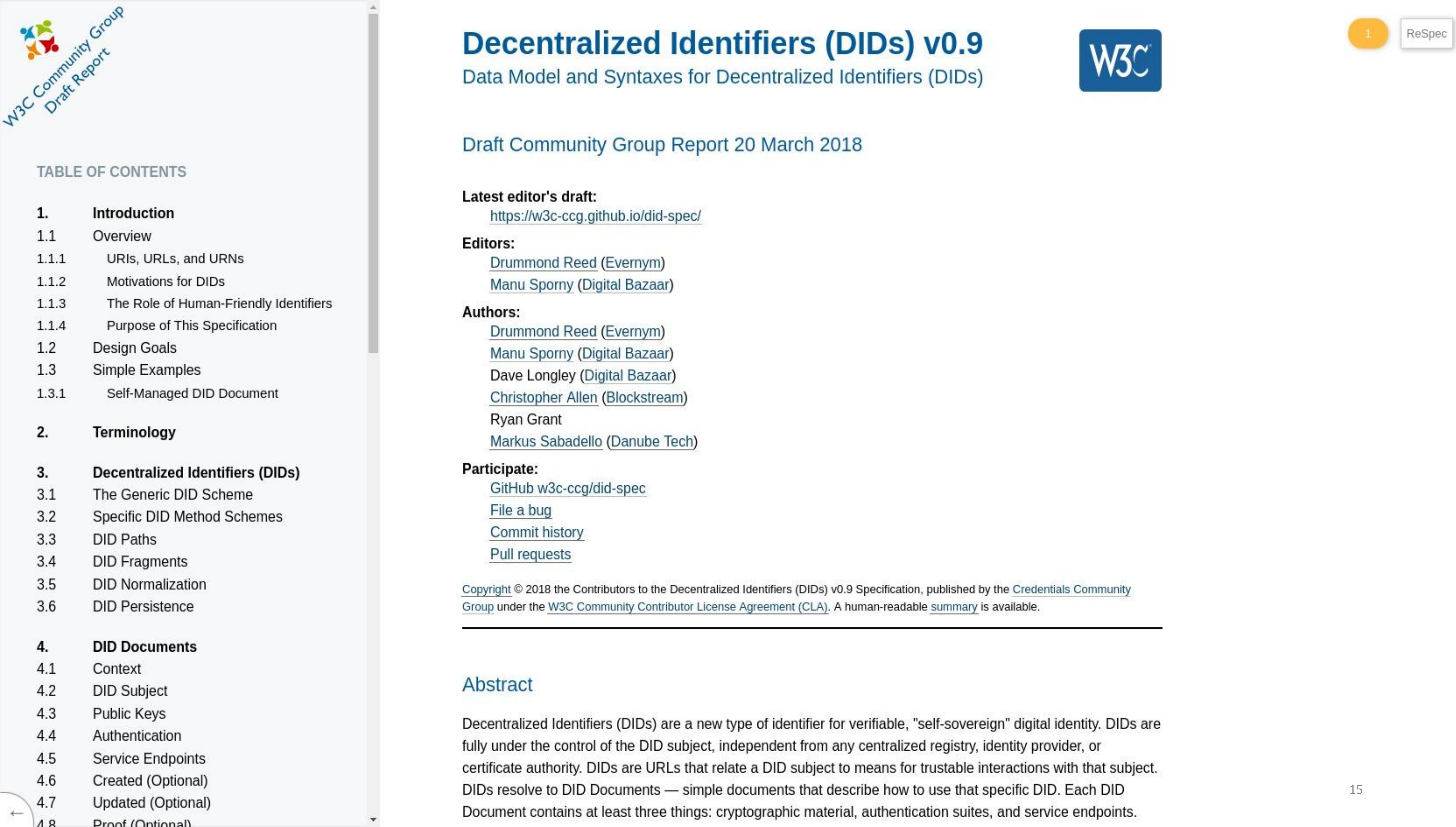
(Identifiers are *owned* by individuals)

Blockchains / DHTs

(Decentralized Ledger)
Veres One, Sovrin, Bitcoin, Ethereum, etc.

Decentralized Identifiers

A new type of globally resolvable, cryptographically-verifiable identifier, registered directly on a distributed ledger (aka Blockchain)



W3C Community Group Draft Report

Decentralized Identifiers (DIDs) v0.9

Data Model and Syntaxes for Decentralized Identifiers (DIDs)

Draft Community Group Report 20 March 2018

Latest editor's draft:
https://w3c-ccg.github.io/did-spec/

Editors:
Drummond Reed (Evernym)
Manu Sporny (Digital Bazaar)

Authors:
Drummond Reed (Evernym)
Manu Sporny (Digital Bazaar)
Dave Longley (Digital Bazaar)
Christopher Allen (Blockstream)
Ryan Grant
Markus Sabadello (Danube Tech)

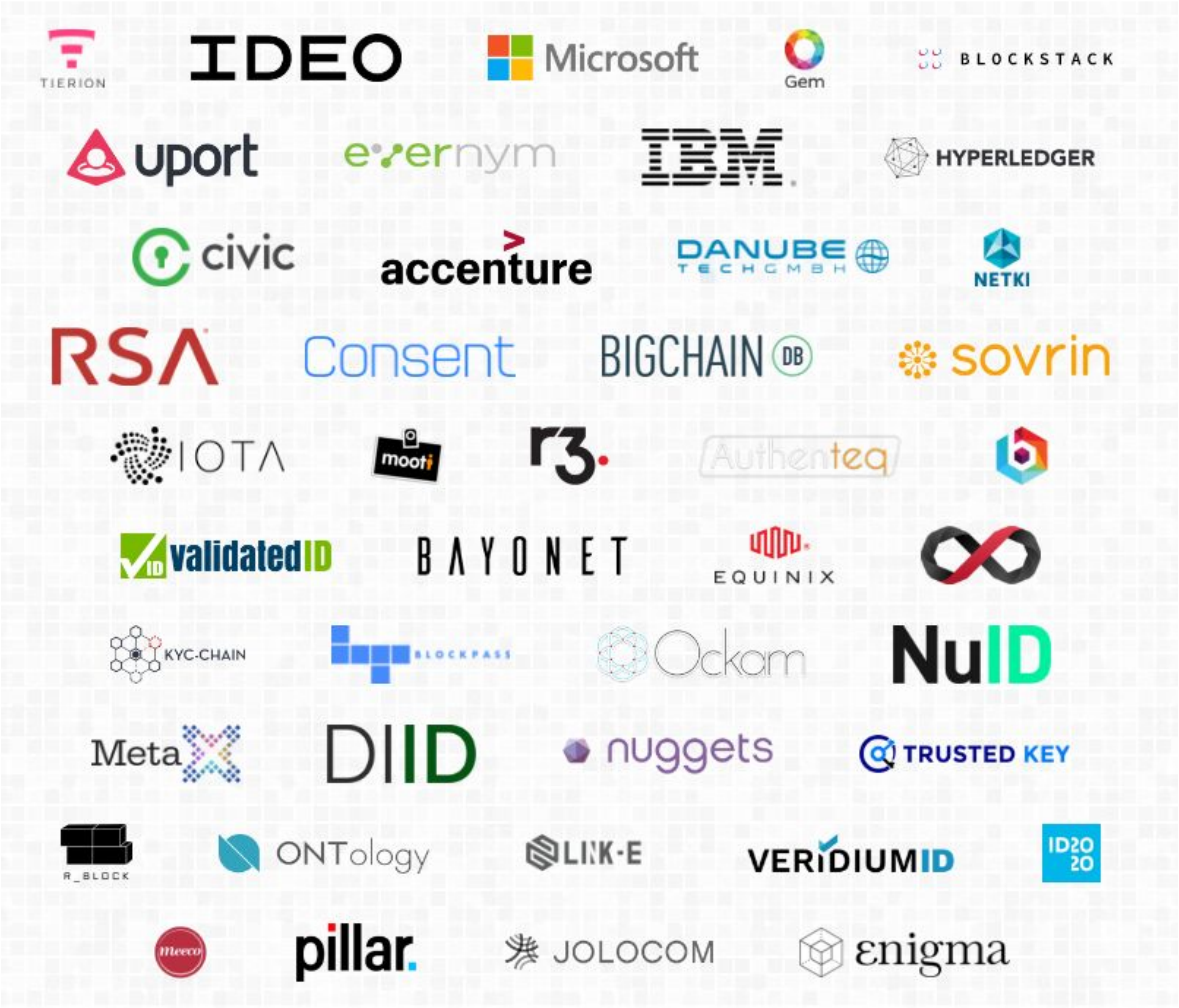
Participate:
GitHub w3c-ccg/did-spec
File a bug
Commit history
Pull requests

Abstract

Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document contains at least three things: cryptographic material, authentication suites, and service endpoints.

Implementers

Method	DID prefix
Veres One	**did:v1:**
Sovrin	did:sov:
Bitcoin Reference	did:btcr:
Ethereum uPort	did:uport:
IPFS	did:ipfs:
IPDB	did:ipdb:


TIERION
IDEO
Microsoft
Gem
BLOCKSTACK
uport
evernym
IBM
HYPERLEDGER
civic
accenture
DANUBE TECH GMBH
NETKI
RSA
Consent
BIGCHAIN DB
sovrin
IOTA
mooti
r3.
Authenteq
validatedID
BAYONET
EQUINIX
KYC-CHAIN
BLOCKPASS
Ockam
NuID
Meta
DIID
nuggets
TRUSTED KEY
R_BLOCK
ONTology
LINK-E
VERIDIUMID
ID2020
meeco
pillar.
JOLOCOM
enigma

Break for Questions

Any questions related to Verifiable Credentials or Decentralized Identifiers?

VERES ONE

A Globally Interoperable Blockchain for Identity

VISION

A world where people and organizations create, own, and control their identifiers and their identity data

PROBLEM

Every identifier you have created online does not belong to you; it belongs to someone else.

The Internet was not designed with interoperable identity systems in mind, resulting in identity siloes

SOLUTION

Utilize Blockchain technology and multistakeholder governance to create a public good for self-administered identity management.

Blockchain governance models

		Validation	
		Permissionless	Permissioned
Access	Public	Bitcoin, Ethereum, IOTA, **Veres One**	Sovrin, IPDB
	Private	Hyperledger Sawtooth* * in permissionless mode	Hyperledger (Fabric, Sawtooth, Iroha), R3 Corda, CU Ledger

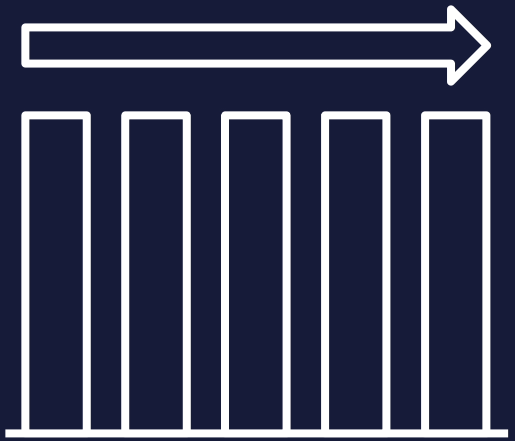
Slide credit: Drummond Reed, Sovrin Foundation

FIT-FOR-PURPOSE

Veres One is a **fit-for-purpose** blockchain optimized for identity.

COST EFFECTIVE

NON-SPECULATIVE



SUSTAINABLE

Fee-based revenue models ensures long term operation of the network

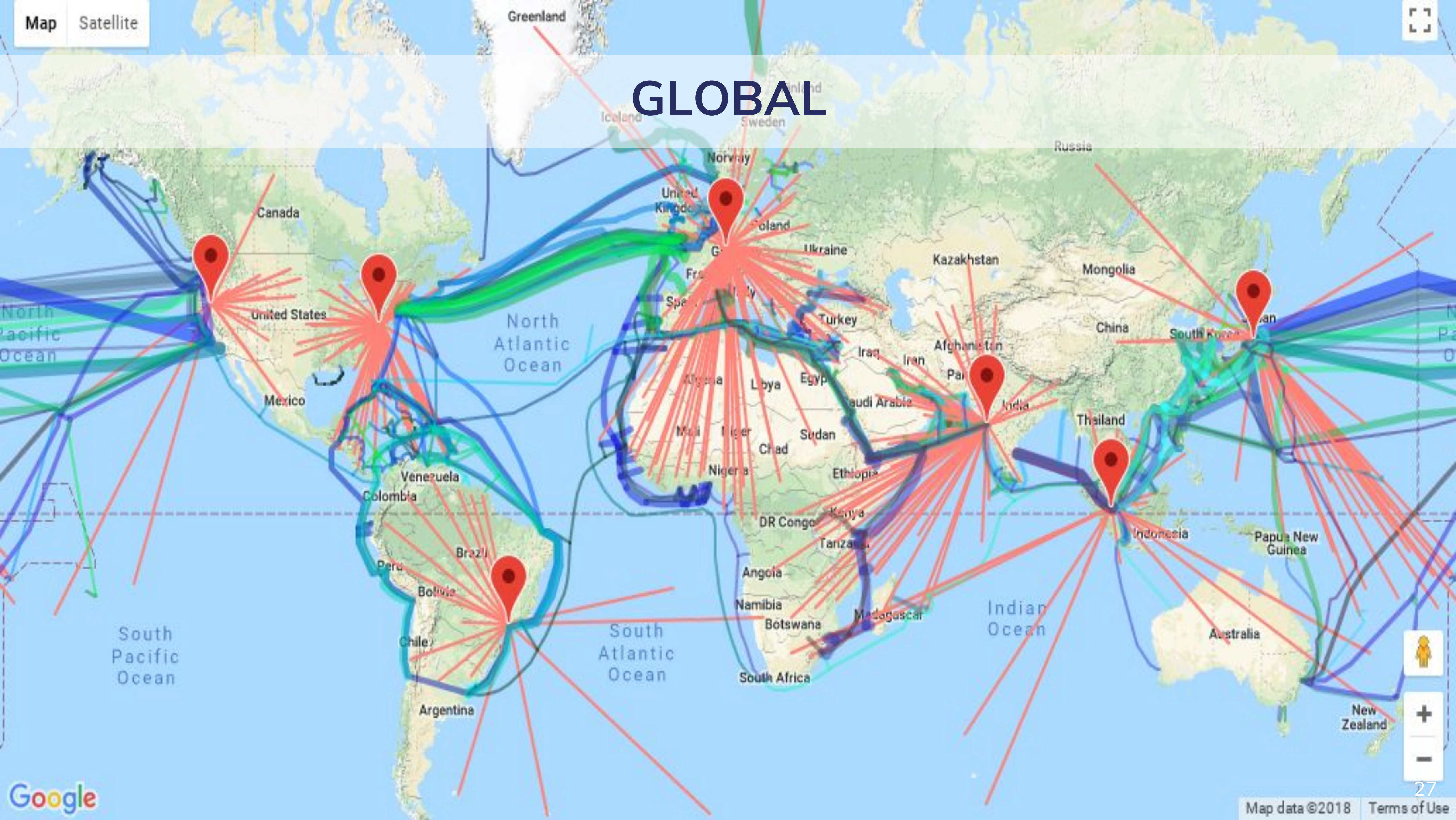
LOW COST

DID Creation	
Bitcoin	~$15
Ethereum	~$4
Veres One	~$1

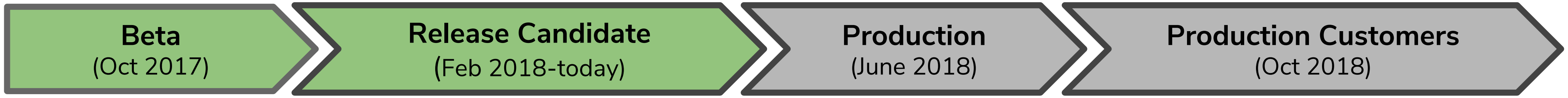
FAST

DID Creation		
DID Ledger	*Operations / day*	*Consensus delay*
Bitcoin	0.6M / day	~3,600 seconds
Ethereum	2.1M / day	~375 seconds
Veres One	**18M / day**	**~30 seconds**

GLOBAL


Map
Satellite
Greenland
Iceland
Finland
Sweden
Norway
Russia
Canada
United Kingdom
Poland
Ukraine
Kazakhstan
Mongolia
United States
North Pacific Ocean
North Atlantic Ocean
Spain
Italy
Turkey
China
South Korea
Japan
Afghanistan
Iraq
Iran
Mexico
Algeria
Libya
Egypt
Saudi Arabia
India
Thailand
Mali
Niger
Chad
Sudan
Venezuela
Colombia
Nigeria
Ethiopia
DR Congo
Kenya
Tanzania
Indonesia
Papua New Guinea
Brazil
Peru
Bolivia
Angola
Namibia
Botswana
Madagascar
Indian Ocean
Chile
South Pacific Ocean
South Atlantic Ocean
South Africa
Australia
Argentina
New Zealand
Google
Map data ©2018
Terms of Use

VERES ONE ROADMAP

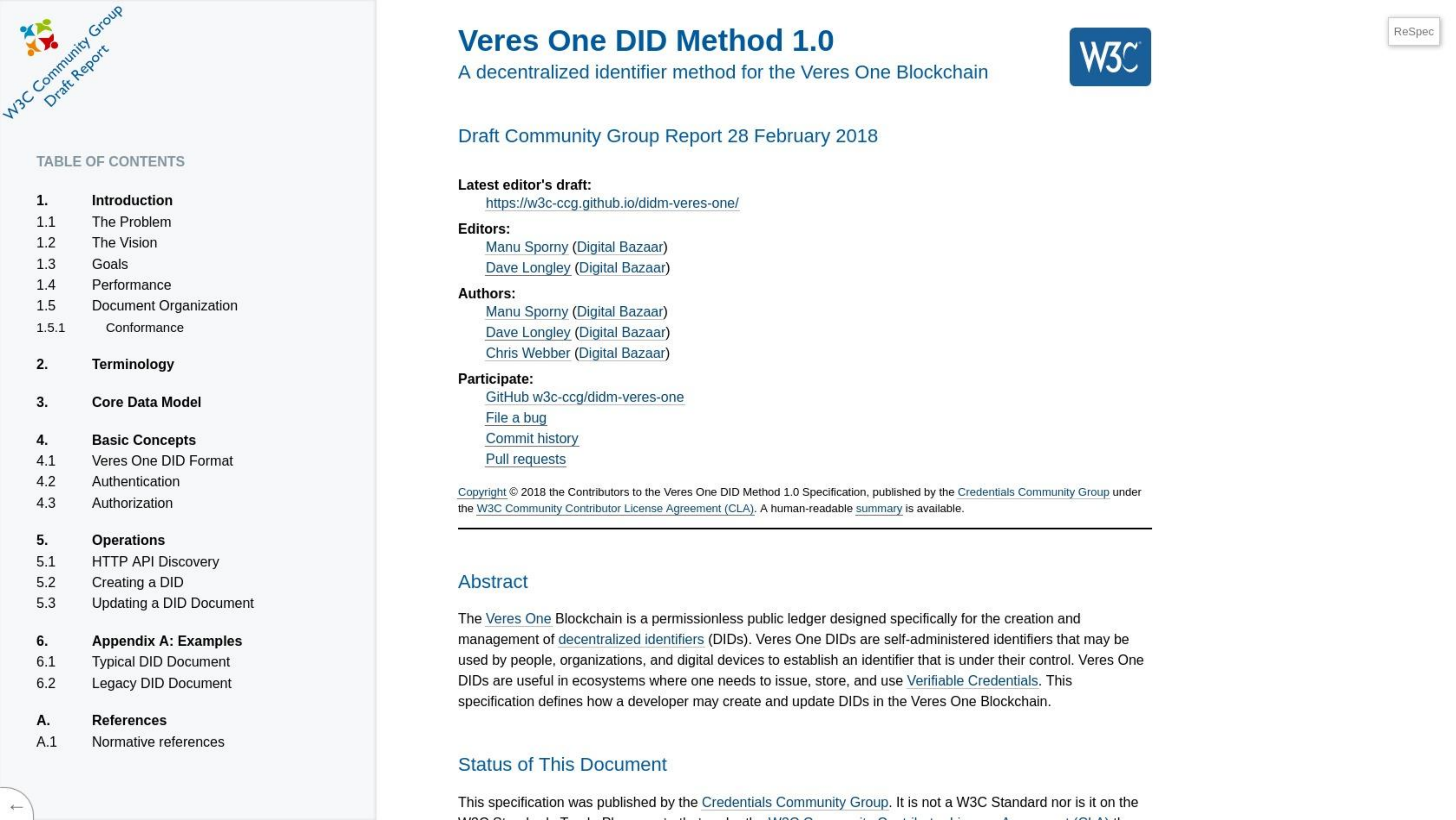


Beta
(Oct 2017)

Release Candidate
(Feb 2018-today)

Production
(June 2018)

Production Customers
(Oct 2018)



Veres One DID Method 1.0

A decentralized identifier method for the Veres One Blockchain

Draft Community Group Report 28 February 2018

Latest editor's draft:
https://w3c-ccg.github.io/didm-veres-one/

Editors:
Manu Sporny (Digital Bazaar)
Dave Longley (Digital Bazaar)

Authors:
Manu Sporny (Digital Bazaar)
Dave Longley (Digital Bazaar)
Chris Webber (Digital Bazaar)

Participate:
GitHub w3c-ccg/didm-veres-one
File a bug
Commit history
Pull requests

Abstract

The Veres One Blockchain is a permissionless public ledger designed specifically for the creation and management of decentralized identifiers (DIDs). Veres One DIDs are self-administered identifiers that may be used by people, organizations, and digital devices to establish an identifier that is under their control. Veres One DIDs are useful in ecosystems where one needs to issue, store, and use Verifiable Credentials. This specification defines how a developer may create and update DIDs in the Veres One Blockchain.

Status of This Document

This specification was published by the Credentials Community Group. It is not a W3C Standard nor is it on the

Break for Questions

Any questions related to Veres One and other Decentralized Identifier Blockchains?

Manu Sporny | CEO | Digital Bazaar

- Co-Inventor of Verifiable Credentials & Decentralized Identifiers
- Co-Inventor of JSON-LD
- Co-Founder of Veres One
- 10+ Years in Web Standards
- Customers in Finance, Government, Education, and Healthcare

Email: msporny@digitalbazaar.com

Twitter: @manusporny

https://www.linkedin.com/in/manusporny/