



Identity and Blockchain

at the Toronto French Business Network

By Marc Lijour

June 12, 2019

Metamesh Group, your Trusted Advisors for Technology Transformation across the globe



This panel is brought to you by



<https://www.tfbn.ca>



<https://gowlingwlg.com>

Access these slides online

<https://bit.ly/2usZm3G>

or at

<https://github.com/marclijour/presentations>



Table of Contents

1 What is Blockchain?

2 Identity and Blockchain

3 Some Solutions Provider

- Shyft Network
- Evernym / Sovrin / Indy
- uPort
- SecureKey
- Microsoft ION
- KABN

4 Case Studies

- Switzerland
- Canada



The Trust Machine



But how does it work?

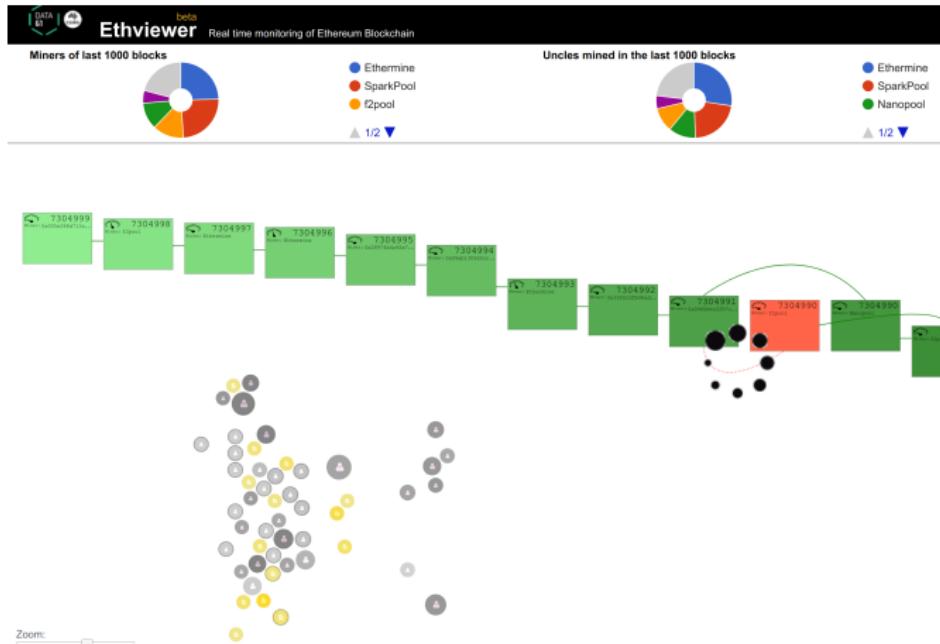


Figure: Source : <http://ethviewer.live>

Reference books

Blockchain in practice

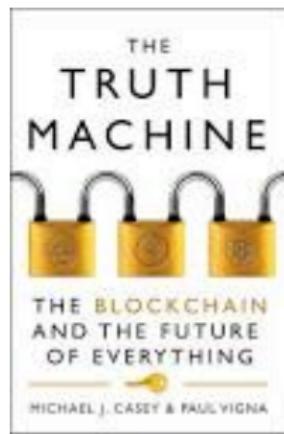


Figure: Book from Vigna and Casey,
2018

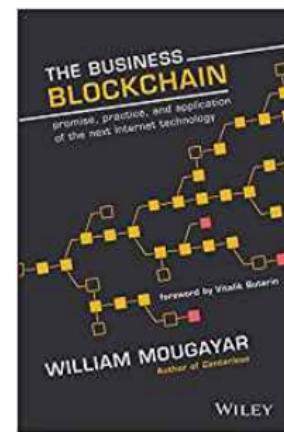


Figure: Book from Mougayar, 2016

Ultimate references

The must-read white paper from legendary Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System* ([2008](#)),

the Ethereum white paper from home-town Toronto Vitalik Buterin: *A Next-Generation Smart Contract and Decentralized Application Platform* ([2013](#)),

and the yellow paper authored by Prof. Gavin Wood: *Ethereum: A secure decentralised generalised transaction ledger* ([2014](#)).



Table of Contents

1 What is Blockchain?

2 Identity and Blockchain

3 Some Solutions Provider

- Shyft Network
- Evernym / Sovrin / Indy
- uPort
- SecureKey
- Microsoft ION
- KABN

4 Case Studies

- Switzerland
- Canada



Blockchain is not the solution to everything



Digital identity



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

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

Why is Digital Identity important?

From Christine Leong (2019), MD and Global Lead for Identity Innovation

WHY IS IDENTITY IN A DIGITAL WORLD IMPORTANT?

\$ 12 bn

Estimated expense to achieve worldwide identification by 2020

Source: Project ID2020 documentation, 2017

21

Different digital identity instances per person (on average)



Source: FinTechStage Festival, 2018

20 bn

connected “things” by 2020 with consumer applications to represent 63% of IoT applications



Source: Gartner Newsroom, 2017

The global **multi-factor authentication services market** is expected to grow at a CAGR of close to 23% from 2017 to 2021 **up to \$ 14.2 bn**

Source: Businesswire

130

Average number of security breaches each year

Percentage increase over last five years

+91%

Source: 2017 Cost of Cyber Crime Study - Accenture, 2017

1.9 bn

usernames and passwords exposed via data breaches and traded on black-market forums between Mar 16 – Mar 17



Source: Google, 2017

Identity theft 69%

of all data breach incidents, with over **600 million records** impacted resulting in a 73% increase from 2016

Source: Gemalto, 2018



\$141

average cost for each lost or stolen record containing sensitive and confidential information

Source: IBM, 2018

Digital identity Management Paradigms

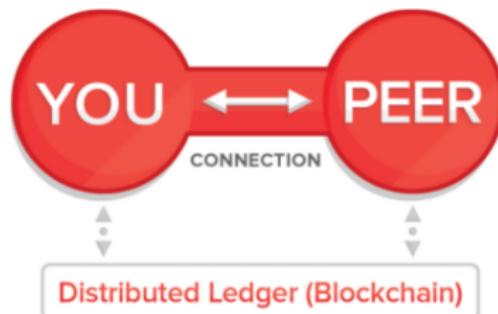
Model #1: Siloed / Traditional



Model #2: Third-Party IDP



Model #3: Self-Sovereign / Peer-to-Peer



Main benefits

- Stronger authentication (credentials vs shared secrets)
- UX (seamless login, no need for "security questions")
- Phishing protection (verification works both ways)
- P2P secure communication
- Same or lower risk profile for corporate issuers

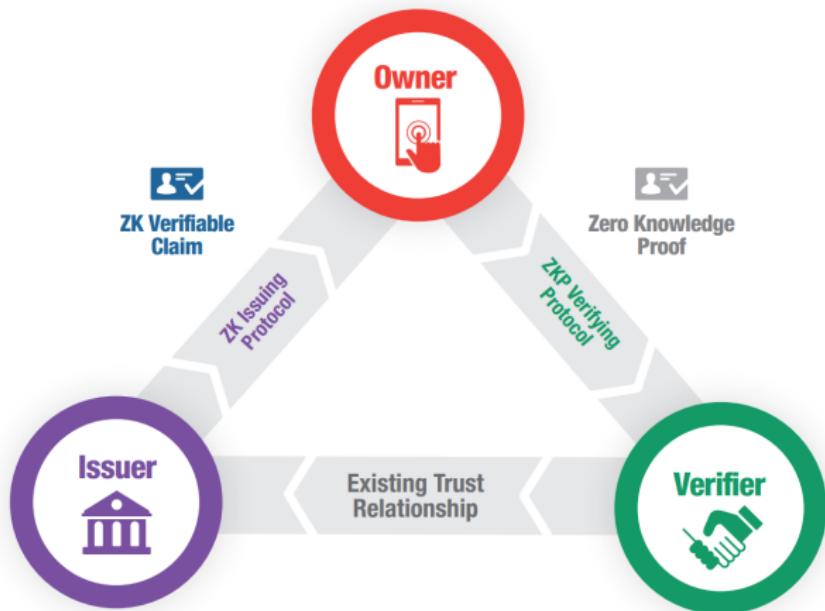
See Timothy Ruff's article at <http://bit.ly/2rB180M>

Figure: extract from Ruff, 2018



Self-Sovereign Identity in practice

Extract from the white paper from The Sovrin Foundation, 2018



The SSI Stack for portable identities

From Terbu, 2019

Layer	Examples
Application	Selective disclosure, music app, rideshare service, extensions, etc.
Implementation	DIF Hubs, Indy Agents, uPort app, etc.
Payload	JSON-LD, JWT, CWT
Encoding	ProtoBuf, Cap'n Proto, MessagePack, JSON, CBOR, etc.
Encryption	Ciphersuites, JWE, etc.
DID AuthN	Key ownership, verification, challenge/response, etc.
Transport	QR Code, HTTP, BLE, NFC, FTP, SMTP, etc.
DID Resolution	DID -> DID Doc / service and key resolution
DID Operations	CRUD support for a DID Doc
Storage	Optional, separate storage of DID metadata, e.g., IPFS
Anchor	Bitcoin, Ethereum, Veres.One, Sovrin, etc.



Figure: based on the results of the workshop (...) provided by Kyle Den Hartog (Evernym) and Daniel Buchner (Microsoft)

Ten Principles of Self-Sovereign Identity

From Web of Trust, 2016

- ① Existence
- ② Control
- ③ Access
- ④ Transparency
- ⑤ Persistence
- ⑥ Portability
- ⑦ Interoperability
- ⑧ Consent
- ⑨ Minimization
- ⑩ Protection



The W3C work on DIDs and Verifiable Credentials

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

A Primer for Decentralized Identifiers

An introduction to self-administered identifiers for curious people



Draft Community Group Report 19 January 2019

Latest editor's draft:

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

Editors:

[Andrew Hughes \(ITIM Consulting\)](#)

[Manu Sporny \(Digital Bazaar\)](#)

[Drummond Reed \(Evernym\)](#)

Author:

[Credentials Community Group \(W3C\)](#)

Participate:

[GitHub w3c-ccg/did-primer](#)

[File a bug](#)

[Commit history](#)

[Pull requests](#)

Copyright © 2019 the Contributors to the A Primer for Decentralized Identifiers Specification, published by the [Credentials Community Group](#) under the [W3C Community Contributor License Agreement \(CLA\)](#). A human-readable [summary](#) is available.



Decentralized Identity Foundation

<https://identity.foundation>

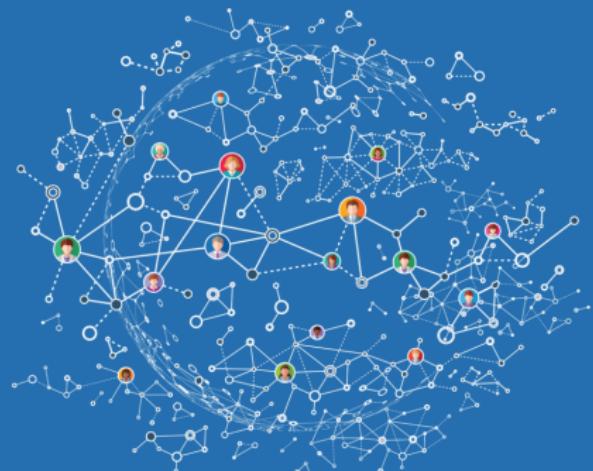


[Home](#) [Our Focus](#) [Working Groups](#) [Contact Us](#)

Together we're building a new identity ecosystem

Join us in developing the foundational components of an open, standards-based, decentralized identity ecosystem for people, organizations, apps, and devices.

[BECOME A MEMBER](#)



Digital Identification and Authentication Council of Canada (DIACC)

<https://diacc.ca>

Digital Identity Ecosystem Principles

The Digital Identification and Authentication Council of Canada (DIACC) believes it is imperative that Canadian institutions protect and promote Canadian values and perspectives as the digital economy develops. The DIACC leverages the following Canadian and universal principles as guidance with regard to initiatives that support our mission and vision.



Principles of a digital identity ecosystem for Canada, and solutions within:

1. Robust, secure, and scalable
2. Implement, protect, and enhance Privacy by Design
3. Inclusive, open, and meets broad stakeholder needs
4. Transparent in governance and operation
5. Provide Canadians choice, control, and convenience
6. Built on open, standards-based protocols
7. Interoperable with international standards
8. Cost effective and open to competitive market forces
9. Able to be independently assessed, audited and subject to enforcement
10. Minimize data transfer between authoritative sources and will not create new identity databases

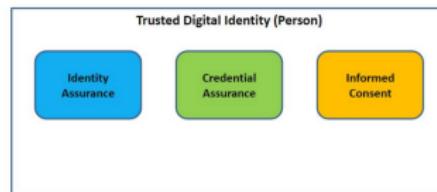
Pan-Canadian Trust Framework — Cadre de Confiance pancanadien

<https://canada-ca.github.io/PCTF-CCP/>

PCTF-CCP

Pan-Canadian Trust Framework | Cadre de Confiance Pancanadien

[View the Project on GitHub](#)
canada-ca/PCTF-CCP



The Pan-Canadian Trust Framework

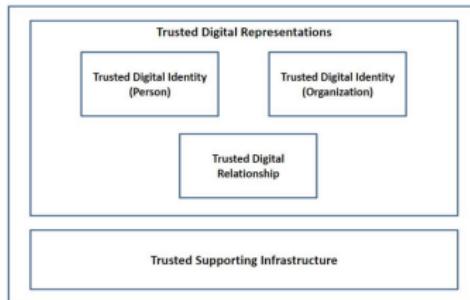


Table of Contents

1 What is Blockchain?

2 Identity and Blockchain

3 Some Solutions Provider

- Shyft Network
- Evernym / Sovrin / Indy
- uPort
- SecureKey
- Microsoft ION
- KABN

4 Case Studies

- Switzerland
- Canada



Shyft Network

<https://shyft.network>



Building the global network of trusted information

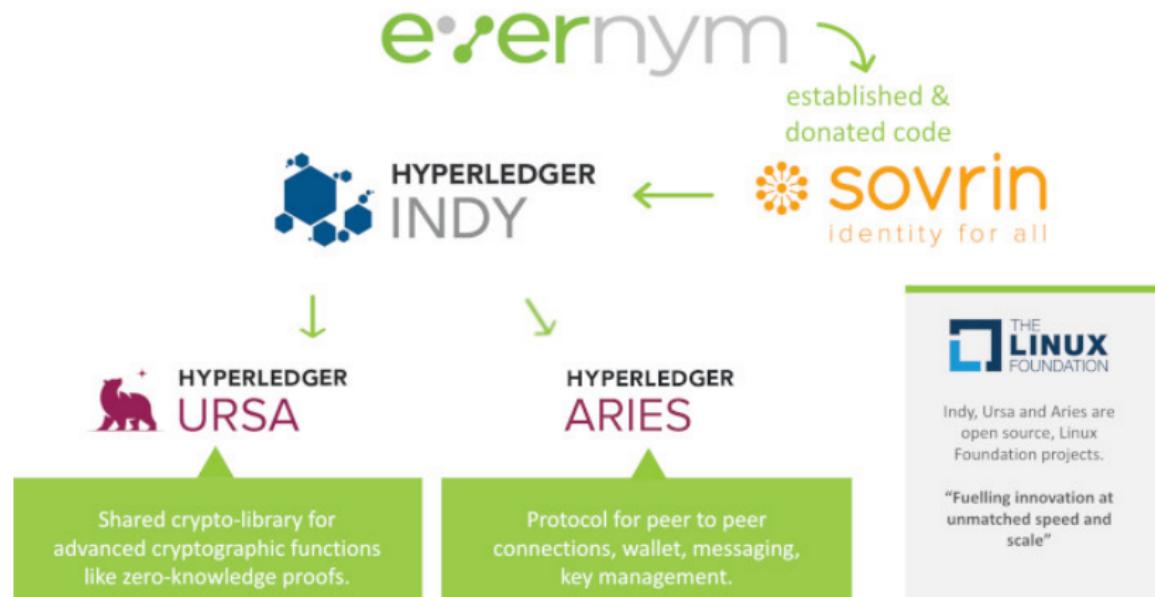
Trust is an essential component of connectivity in communication. As we've become more dependent on technology, we've also become more distrustful due to numerous breaches of trust in the form of cybersecurity failures and widespread theft.

The way we treat data is broken; Shyft will fix it.



Evernym / Sovrin / Indy

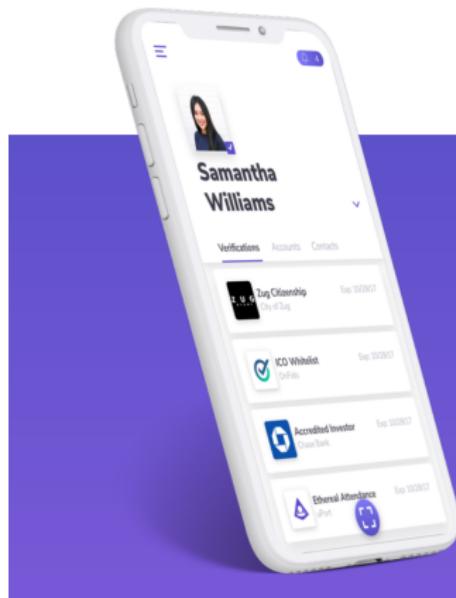
<https://www.evernym.com>, <https://sovrin.org>, and
<https://www.hyperledger.org/projects/hyperledger-indy>



Try it at <https://try.connect.me>

uPort

<https://www.uport.me>



**Take back control
of your identity.**

Download the uPort Wallet app for iOS and Android.

[Download on the App Store](#) [GET IT ON Google Play](#)

Try it at <https://uportlandia.uport.me>



SecureKey

<https://securekey.com>

[Exit](#) | [Français](#) | [Help](#) | [FAQ](#) | [Switch My Sign-In Partner](#) | [Contact Us](#)



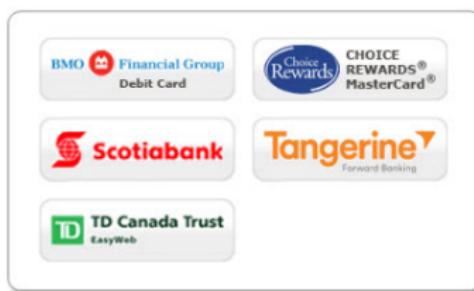
Concierge

Online Access Made Easy

Select Sign-In Partner

By selecting a Sign-In Partner, you are agreeing to the [Terms and Conditions](#) and [Privacy Notice](#) of SecureKey Concierge.

Notice to BMO Credit Card Users



SIMPLE | CONVENIENT | SECURE

- ✓ It's easy to use
- ✓ We protect your privacy
- ✓ No passwords or personal information (i.e.: name, address, date of birth, etc.) are exchanged during this process
- ✓ Your Sign-In Partner won't know which government service you're accessing and the government won't know which Sign-In Partner you're using

[Terms and Conditions](#) | [About SecureKey Concierge](#) | [Privacy Notice](#)



Microsoft ION

<https://github.com/decentralized-identity/ion>



Figure: from Cuen, 2019

KABN — Blockchain Identity

<https://medium.com/@secdegulleri/kabn-blockchain-identity-daf70ee0eb4>

KABN NETWORK



KABN is a financial service platform with neo banking type solutions which has received approval by Visa to launch its crypto-linked card and banking wallet program.

KABN has its private Network which is an integrated suite of financial services that includes the *Pegasus Flyte Visa Card*, an approved crypto-linked prepaid Visa card and mobile integrated multi-currency banking wallet; **KABN KASH**, a robust loyalty & engagement program and the network anchor, *KABN ID*, a patent pending, Always On, GDPR compliant, blockchain & biometrically based, identity

verification and validation platform. **KABN ID** is free to use service for consumers & provides continuous monitoring and proof of identity online and in conventional marketplaces.

Table of Contents

1 What is Blockchain?

2 Identity and Blockchain

3 Some Solutions Provider

- Shyft Network
- Evernym / Sovrin / Indy
- uPort
- SecureKey
- Microsoft ION
- KABN

4 Case Studies

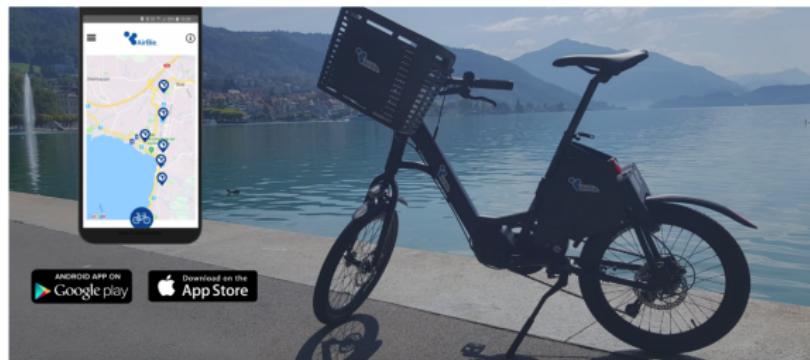
- Switzerland
- Canada



The first e-bike service worldwide powered by decentralized identity

See full article from Nawfal, 2018

AirBie, a crypto bike-sharing service, just launched the first e-bike service worldwide powered by decentralized identity



Last November, the Swiss city of Zug officially launched its Zug eID, an opportunity for its residents to register for a decentralized, digital identity powered by uPort.



The Verifiable Organizations Network (VON)

<https://vonx.io>

The screenshot shows the homepage of the VON website. At the top left is the VON logo, which consists of a stylized network icon followed by the acronym 'VON' and the full name 'Verifiable Organizations Network'. To the right are three navigation links: 'About', 'Get Started', and 'Clicky Things'. The main title 'Verifiable Organizations Network: Global digital trust for organizations' is centered in large, bold, white font. Below the title are two buttons: 'Learn More About VON' with a computer monitor icon and 'Get Involved' with a person icon. A horizontal line with the word '— or —' separates these buttons. At the bottom, there is a section titled 'Founding community partners' featuring logos for British Columbia, Public Services and Procurement Canada, and Ontario.

VON
Verifiable Organizations Network

About Get Started Clicky Things

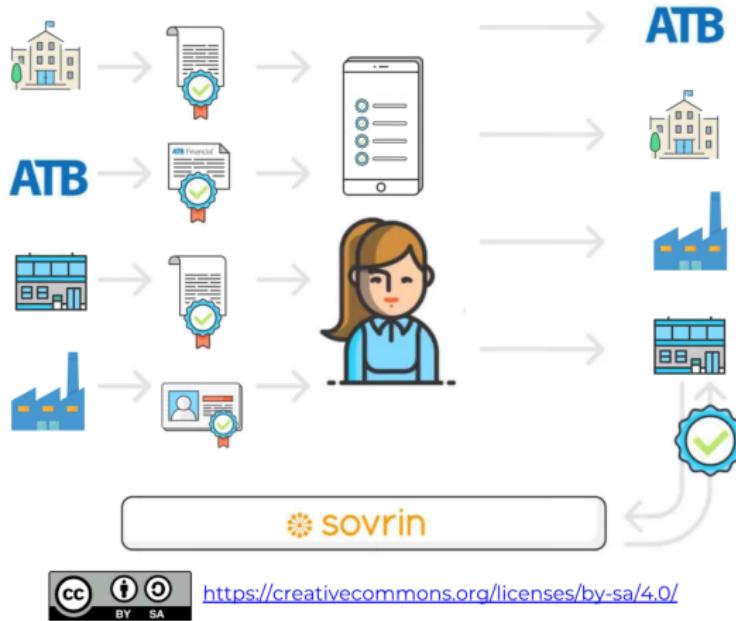
Verifiable Organizations Network: Global digital trust for organizations

Learn More About VON — or — Get Involved

Founding community partners

BRITISH COLUMBIA Public Services and Procurement Canada Ontario

SSI in Alberta



Alberta Credentials Ecosystem:

ATB in leading the engagement of universities, telcos, utilities, insurance, municipal gov and provincial gov

Looking to build out a robust ecosystem issuing and verifying diverse set of credentials



<https://creativecommons.org/licenses/by-sa/4.0/>



SSIMeetup.org

Figure: from Brown, 2019



Want to learn more about Blockchain?



Tech Trends Peer Group

BLOCKCHAIN-ENABLED PREDICTION MARKETS

THIS TALK WILL PROVIDE AN INTRODUCTION TO PREDICTION MARKETS AND HOW THEY WORK UNDER THE HOOD. WE'LL DIG DEEPER INTO SOME MATURE TECHNOLOGIES SUCH AS GNOSIS.

HOSTED BY: MARK CAMBALL, METAMESH GROUP

MODERATOR: MARC LIJOUR, METAMESH GROUP

TUESDAY JUNE 25TH, 2019



 TechConnex



Thank you!

Email: marc@metameshgroup.com

Twitter: [@marclijour](https://twitter.com/marclijour)

www.metameshgroup.com



References |

- Brown, M. (2019). A banking approach to decentralized identity and building a credential ecosystem. Retrieved from
<https://www.slideshare.net/SSIMeetup/a-banking-approach-to-decentralized-identity-and-building-a-credential-ecosystem-mike-brown>
- Buterin, V. (2013). A next-generation smart contract and decentralized application platform. Retrieved from
<https://github.com/ethereum/wiki/wiki/White-Paper>
- Cuen, L. (2019, May 13). Microsoft launches decentralized identity tool on bitcoin blockchain. Retrieved from <https://www.coindesk.com/microsoft-launches-decentralized-identity-tool-on-bitcoin-blockchain>
- Leong, C. (2019, June 10). Blockchain and identity the impact of the technology on the bottom billion. Retrieved from <https://isoc.live/date/2019/06/>
- Mougaray, W. (2016). *The business blockchain: Promise, practice, and application of the next internet technology* (1st ed.). Wiley.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from
<https://bitcoin.org/bitcoin.pdf>

References II

- Nawfal, A. (2018, November 14). Zug residents can now ride e-bikes using their uPort-powered Zug Digital IDs. Retrieved from <https://medium.com/uport/zug-residents-can-now-ride-e-bikes-using-their-uport-powered-zug-digital-ids-7ed31ac9d621>
- Ruff, T. (2018, April 24). The three models of digital identity relationships. Retrieved from <https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186>
- Terbu, O. (2019, January 27). The Self-Sovereign Identity stack. Retrieved from <https://medium.com/decentralized-identity/the-self-sovereign-identity-stack-8a2cc95f2d45>
- The Sovrin Foundation. (2018, January). SovrinTM: A protocol and token for Self-Sovereign Identity and decentralized trust. Retrieved from <https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf>
- Vigna, P., & Casey, M. J. (2018). *The Truth Machine: The Blockchain and the future of everything* (1st ed.). St. Martin's Press.



References III

- Web of Trust. (2016, April 26). The path to Self-Sovereign Identity. Retrieved from <https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/topics-and-advance-readings/the-path-to-self-sovereign-identity.md#the-evolution-of-identity>
- Wood, G. (2014, April). Ethereum: A secure decentralised generalised transaction ledger. Retrieved from <https://ethereum.github.io/yellowpaper/paper.pdf>