

Self-sovereign identity and Verifiable Credentials

Stepan Gershuni
CEO Credentia

credentia.me

About me

Education

- РЭУ им. Плеханова
- Hult International Business School, San Francisco

Experience

Blocknotary



Credentia.

CRYPTOECONOMICS RESEARCH GROUP

Speaking

Финансовый Университет, МИФИ, Корпоративный Университет
Сбербанка, Ericsson, РосАтом



Existing problems

— Fraud

Paper documents, signatures, certificates, attestations and diplomas can be faked. Information could be tampered with.

— Bureaucracy costs

Expensive and lengthy process that hurts different agents involved in issuing and updating documents

— Credentialing system is unfit for digital age

Digital credentials are internationally recognizable, machine-readable and provable

— Digital economy requires digital infrastructure

In order to benefit from technologies like AI, machine learning, big data analysis and predictive models, data has to be in digital and standardized form.



Printed documents



Could be tampered with

Might get lost

Non extendable

No proof system

Long process of verification

Now way to collect statistics

Digital credentials



Tamper-proof

Immutable and accessible

Easily extended and shareable

Instantaneously verifiable

Cheap issuance process

Automated analytics

Owned by user, no centralized registry

Key concepts

Identity

DID — *a sequence of characters, which is worldwide unique and cryptographically verifiable*

DID Document — *a resource which is associated with a decentralized identifier. The DID Document usually phrases methods of verification and services, which are offered by the entity represented by the DID Document*

Decentralized: Decentralized identities are worldwide redundantly distributed in storage media in a decentralized manner.

Immutable: A decentralized identity cannot be deleted or modified, the only way to change the information associated with it (within the DID Document) is to register an updated variant of the DID Document which becomes valid by a signature from an (group of) authorized agent(s). The complete history of the DID Document is permanent.

Open: Anybody with access to a computer and to the internet can create a decentralized identity.

Censorship-resistant: Nobody, except the owner or an (group of) agent(s) which were authorized by the owner, can change the DID Document associated with the DID of the owner.

CERTIFICATE OF BIRTH

This is To Certify That

Weighing _____ lbs. _____ oz. was born on the _____ day of _____
_____ at _____
_____ and _____
Mother Father

HealthCare+		HMO
Name JANE DOE	Group # xxx-xxx-xx	
ID # xxx-xxx-xxxx	Effective xx-xx-xxxx	
	Coverage INDIVIDUAL	
	Plan HMO	
Copay \$xxx.xx	Rx YES	
	RXBIN xxxxx	
	RXPCN xxxxxxxx	

Pennsylvania
aSPMA.com USA

DRIVER'S LICENSE

4d DLN: 99 999 999
3 DOB: 08/04/1969
4b EXP: 08/05/2020
4a ISS: 10/05/2016

1 SAMPLE
2 JANCIE ANN
3 123 MAIN STREET
4 HARRISBURG, PA 17101-0000

10 SEX: F 11 EYES: BRO
16 HGT: 5-06
9a CLASS: C
9b END: NONE
12 RESTR: NONE

DL

Jancie Sample

4 DO: 1234567891123
867890123

ORGAN DONOR

Michigan State University

Upon the recommendation of the faculty of the
Graduate School
confers upon
Jouvan Kullarni
the degree of
Master of Science
Industrial Engineering


With all the honors, rights, and privileges appertaining thereto.

In the witnesses whereof, the seal of Michigan State University and the proper signatures are hereto affixed.

Given at Michigan, Kansas, this twenty-second day of December A.D. 1928.

Frank E. Frank
Dean, Kansas State University

J. Stuart D. Donald
Dean



Donald H. Hopper
President of Michigan State University

George L. Miller
Vice-President, Kansas State

EMPLOYEE NAME / ADDRESS		SSN (LAST 4)	REPORTING PERIOD	PAY DATE	#2494
Demo Employee		1234	05/12/2017 - 05/26/2017	6/2/2017	Employee # 36266
INCOME	RATE	HOURS	CURRENT PAY	DEDUCTIONS	TOTAL
GROSS EARNINGS			17.50 75 1312.50	STATUTORY DEDUCTIONS	
				FICA-MEDICARE	19.03 209.39
				FICA-SOCIAL SECURITY	81.38 895.18
				FEDERAL TAX	142.33 1565.63
				STATE TAX	40.29 443.19
				LOCAL TAX	16.41 180.51
YTD GROSS	YTD DEDUCTIONS	YTD NET PAY	TOTAL	DEDUCTIONS	NET PAY
14437.50	3299.84	11143.66	1312.50	299.44	1013.06



Self-sovereign Identity

*Ability for people to
create, manage and control
their own **credentials** just like they
do with their physical ones, but with
added **cryptographic**
superpowers*

...Because paper doesn't work online

Architecture

Verifiable Credential

Issuer

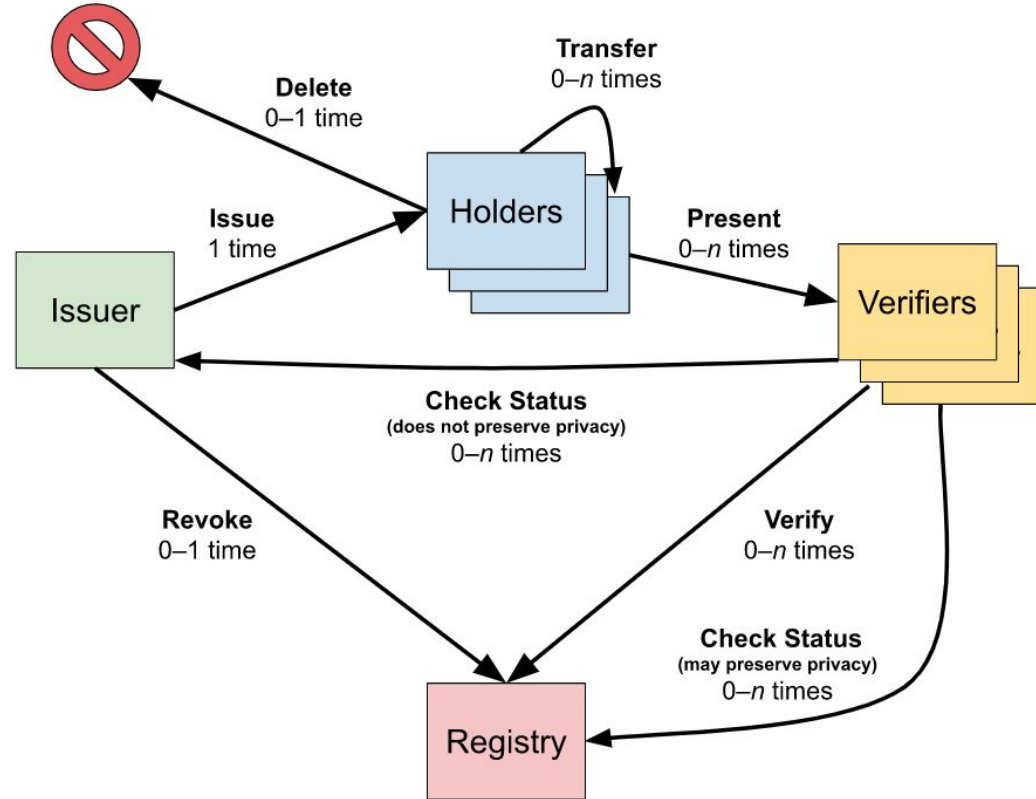
Holder

Credential Subject

- Data
- Evidence
- Disputes
- Zero-knowledge presentation
- Etc.

Proof

VC Structure



VC Lifecycle

Decentralized Stack

Verifiable Credentials (VC)

W3C[®] **Credentia.**

Decentralized Key
Management (DKSM / dPKI)

OASIS   HYPERLEDGER
INDY

Decentralized Identifiers
(DID)

W3C[®]  **sovrin**
identity for all

Distributed Ledger
(Blockchain)



cc2cd0ffde594d278c2d9b432f4748506a7f9f25141e485eb84bc1
88382019b6



did:sov:3k9dg356wdcj5gf2k9bw8kfg7a



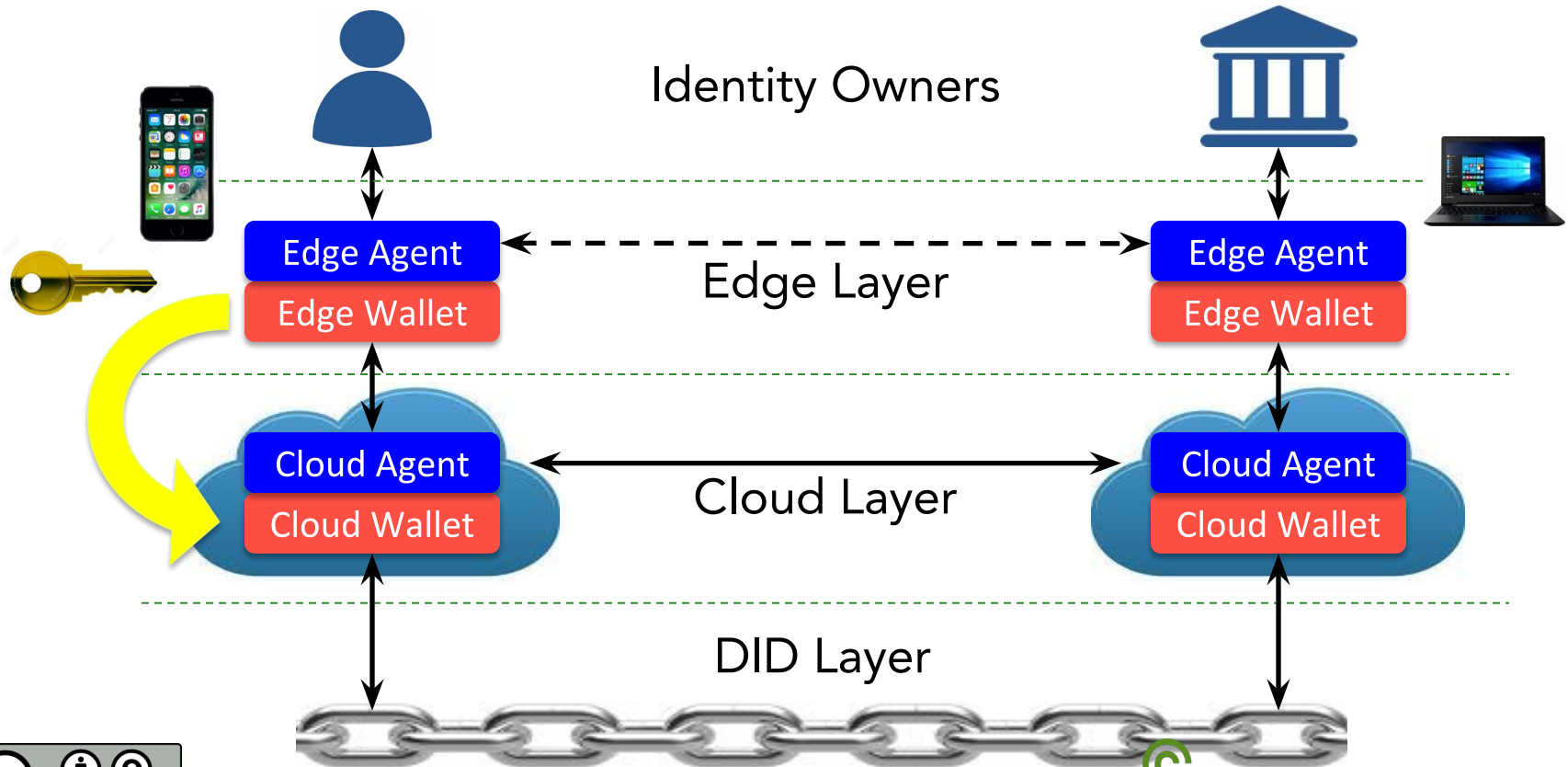
047d599d4521480d9e1919481b024f29d2693f272d19473dbef97
1d7d529f6e9

You will not have just one DID.
You will have thousands.
One per relationship.

Each one will give you a
lifetime encrypted private channel
with another person, organization,
or thing

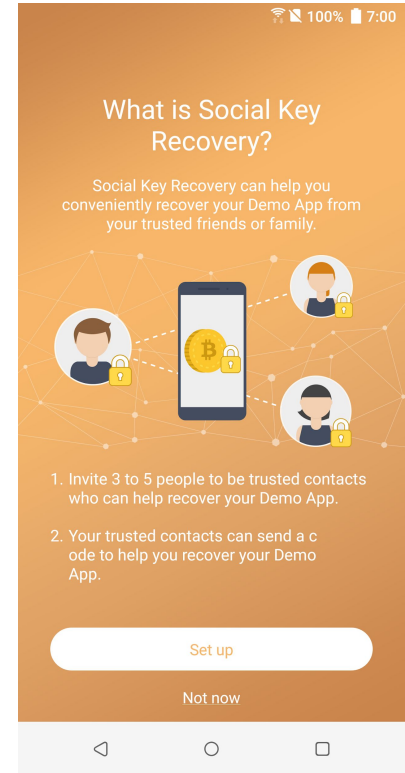
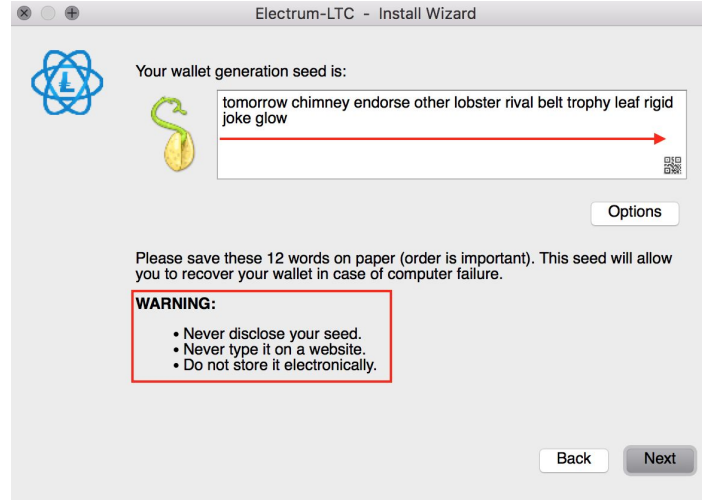
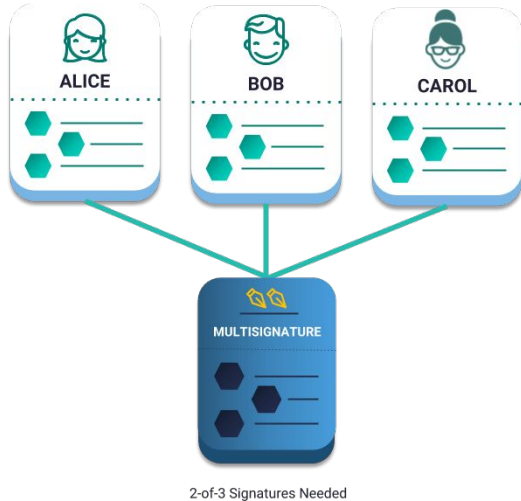
So how will you manage all those
DIDs and private keys?
And what will you do
if you lose them?

The decentralized identity stack



Key recovery

Multisig • Seed backup • Social recovery



We are hiring!

- Fullstack Software Engineer (JavaScript)
- Team Lead
- Project Manager
- Senior Software Engineer (Blockchain)
- Technical Lead

jobs@credentia.me

Real World Examples

Credentia is a tool to create, issue, and verify digital verifiable documents

Design and batch issue digital documents • Store and use lifelong credentials • Programmable and cryptographically secured • Immutable and blockchain-enabled

The future of credentialing is digital.

We want to enable all of the world documents to be digital, easily verifiable, programmable and available to users for a lifetime with just one tap.

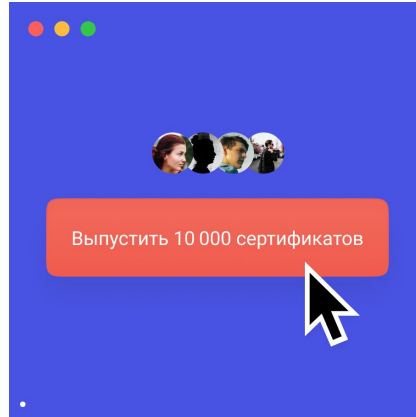
Credentia is a blockchain-agnostic tool that allows to easily deploy digital document creation and verification process using public key infrastructure.

(5) 🐾 Training batch 10				
Training certificate Alex Fork <i>Certificate</i>	Attachments: 1 Change	Signed	Published	>
Training certificate Ruqayyah Holland <i>Certificate</i>	No attachments Change	Signed	Published	>
 Training certificate Zofia Velazquez <i>Certificate</i>	Attachments: 2 Change	Not signed Sign	Not published	>
 Training certificate Elodie Sampson <i>Certificate</i>	No attachments Change	Not signed Sign	Not published	>
 Training certificate Israel White <i>Certificate</i>	No attachments Change	Not signed Sign	Not published	>

How it works?



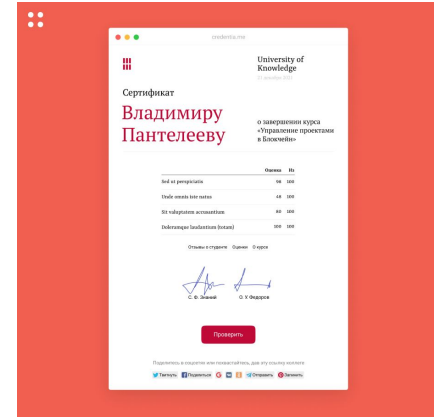
1. Document template is created



2. Documents are issued to the holders, enriched with files and metadata, updated when necessary



3. Digital documents are issued. Cryptographic proof is recorded onto blockchain.

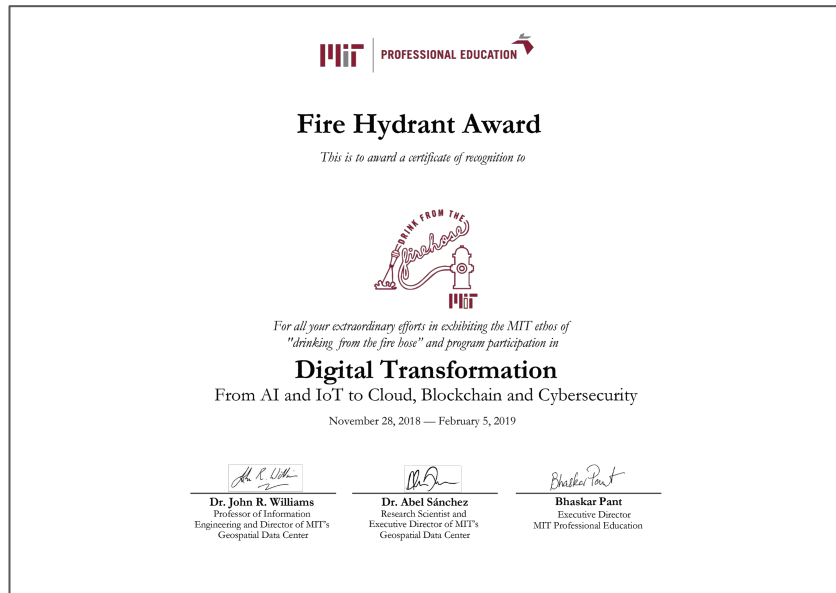


4. With owner's permission anyone can verify document validity and trace its origin.

Documents continue being provable and available forever

Digital diplomas

Digitally signed • Stored on the blockchain • Tamper-proof • Cost efficient • Lifelong student portfolio



Digital badges

Marketing awareness and HR-branding tool • Easily demonstrate skills & competencies • Authenticity proof • Skill portfolio



Certificates and licenses

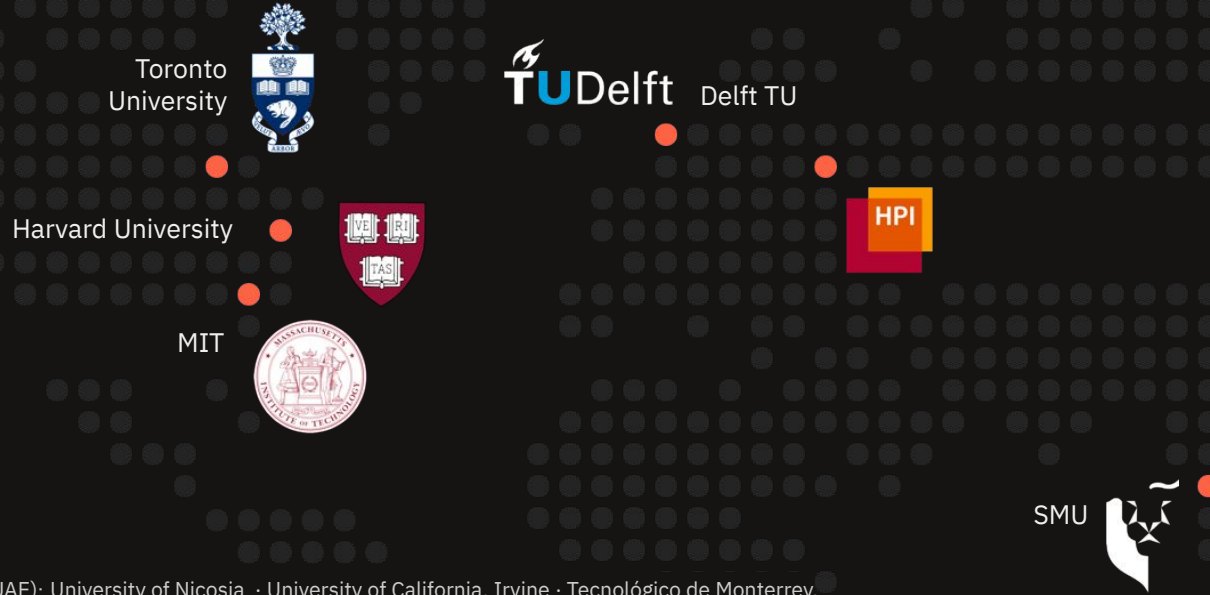
Optimization of creation and verification of digital documents • Fraud reduction



- Worker safety
- Construction
- Pharmacy
- Product certification
- Declaration
- Licensing

Open global standard

Gartner: 2% of higher education institution issue blockchain-based credentials



The British University (UAE) · University of Nicosia · University of California, Irvine · Tecnológico de Monterrey, Мексика · Singapore University of Technology and Design · Singapore Polytechnic

Why now?

1. Global digital documents standards are ready. W3C will [release Verifiable Credentials standard](#) within next 2 months.
2. Public blockchains are immutable databases currently securing \$100's of billions in value.
3. Paper documents and proprietary digital standards are painful to use and seem inappropriate in digital age. (When did you verify PDF or paper signature authenticity last time?)

Public Key Cryptography (1973)

Public Blockchains (Jan 3, 2009)

W3C's Verifiable Credentials (Q4 2019)



