



Emali

9 Dec 2019
Hong Kong

Blockchain-based Registry Systems with User-Centric Verifiable Digital Credentials

Peter Woo

 <https://www.linkedin.com/in/peter-woo>



- Strategist of *EMALI.IO* (Blockchain & Cryptography)
- Co-Founder of *Hong Kong Blockchain Society* (HKBCS.ORG)
- Mentor for *International Blockchain Olympiad* (IBCOL.ORG)
- University of Calgary, Bachelor of Science
- 25+ years' experience in IT, Internet, Telecommunications
- Worked for several multinational firms: *AT&T Asia-China* as a Director, *DoubleClick Asia-Pacific* as Managing Director
- Founded 4 startups; won numerous global blockchain competitions and the inaugural Social Innovation Award

Dr. Lawrence Ma

 <https://www.linkedin.com/in/dr-l-ma>



- Chief Scientist of *EMALI.IO* (Blockchain & Cryptography)
- President of *Hong Kong Blockchain Society* (HKBCS.ORG)
- Mentor for *International Blockchain Olympiad* (IBCOL.ORG)
- Mathematics: Yale (BA), Stanford (MS), Cornell (PhD)
- Former professor: National University of Singapore (math)
- 25+ years' academic and professional experience in Fintech
- Worked for several multinational firms in USA and PR China: *American Bourses Corporation, Bain & Company*

Identity is the new money... the gold rush has begun

Recap: The Biggest Data Breaches of 2017

1. Equifax. Arguably the most buzzed about **breach** of **2017**, Equifax really managed to shake a nation. ...
2. Verizon. In July, the personal **data** of more than 14 million Verizon customers was exposed. ...
3. Uber. Nope, **2017** was not Uber's year. ...
4. RNC Contractor. ...
5. Deloitte. ...
6. Dun & Bradstreet.

Dec 31, 2017

Recap: The Biggest Data Breaches of 2017 - Checkmarx

<https://www.checkmarx.com › 2017/12/31 › recap-biggest-data-breaches-2017>



Identity is the new money... the gold rush has begun

Revealed: The 21 biggest data breaches of 2018

- GooglePlus – 52.5 million.
- Cambridge Analytica – 87 million.
- MyHeritage – 92 million.
- Quora – 100 million.
- MyFitnessPal – 150 million.
- Exactis – 340 million.
- Marriott Starwood hotels – 5 million.
- Aadhar – 1.1 billion users **data breach**.

[More items...](#) • Dec 19, 2018

[Revealed: The 21 biggest data breaches of 2018 / Digital ...](#)

<https://www.digitalinformationworld.com> › 2018/12 › biggest-data-breaches...



Identity is the new money... the gold rush has begun

Here are the biggest 2019 data breaches — and there are still nearly four months yet to go.

- January 21: Elasticsearch cloud storage. ...
- March 29: Verifications.io. ...
- April 2: Facebook. ...
- May 25: First American Corp. ...
- May 24: Canva. ...
- May 29: Flipboard. ...
- July 29: Capital One. ...
- **2019 data breaches:** Protect yourself.

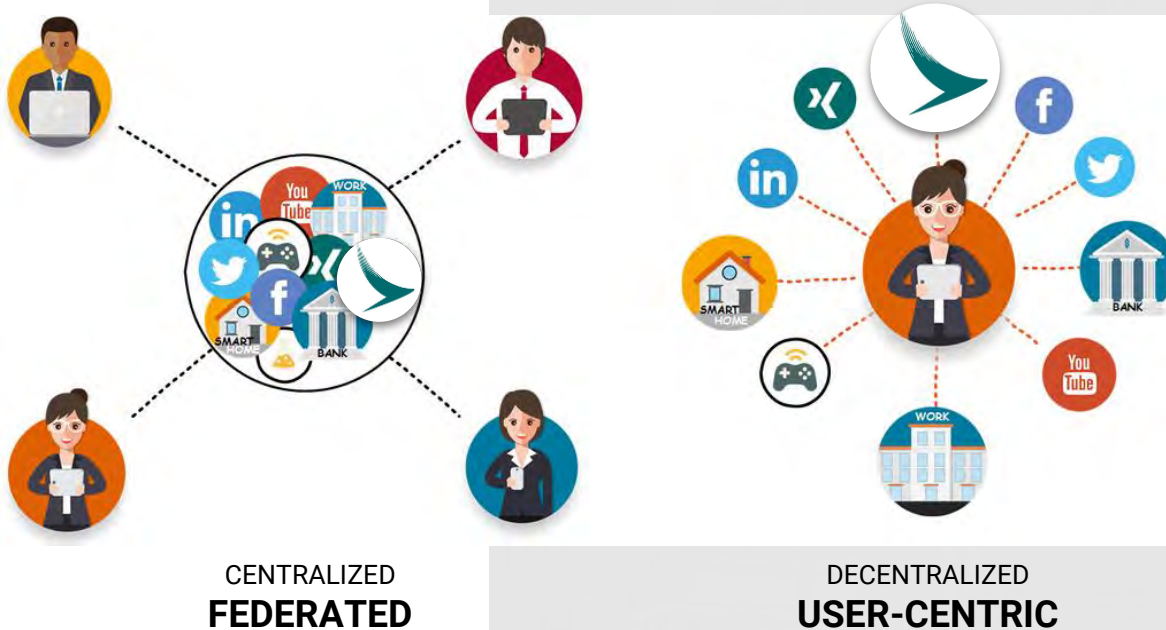
[More items...](#) + Sep 5, 2019



Great year for hackers: Top 2019 data breaches so far

[techgenix.com](https://techgenix.com/2019-data-breaches) › 2019-data-breaches

Configuration is Correlated with Security (or lack thereof)



Centralized models are **vulnerable** to data leaks from hacking and corruption

What is Identity?



Name	James Bond
License #	007
Sex	M
Height	6'2"
Weight	180
Hair	Brown
Eyes	Brown



Name	Air Force One
Make	Boeing
Model	747-200
Length	231'10"
Height	63'5"
Wingspan	195'8"
Fuel	53,611 gallons

Personnel records & aircraft records **both** have identity attributes, from which credentials can be issued

Blockchain-based Registry System



1. Examine (By Issuer)

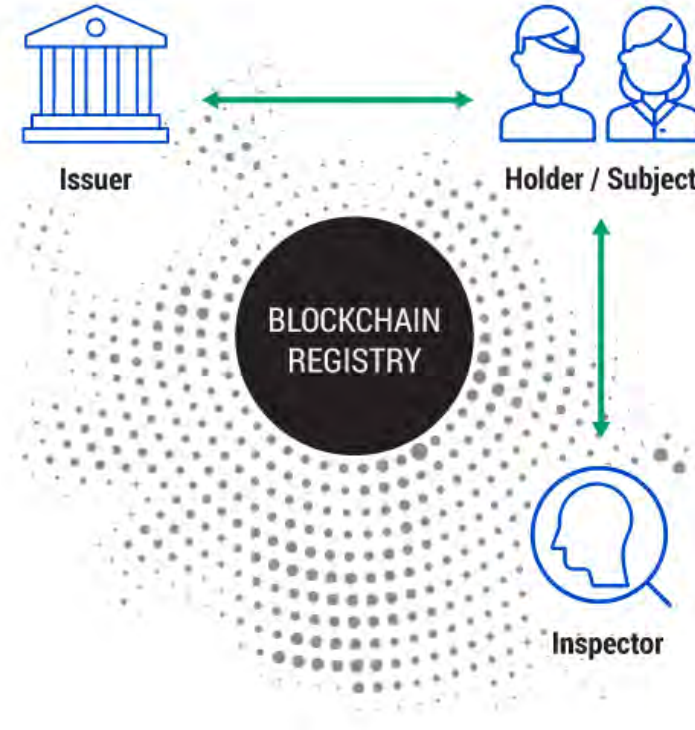
Issuer **examines** or attests to an identity attribute.



Issuer



Holder / Subject



2. Issue (By Issuer)

Issuer has *de facto* or *de jure* authority to **issue** a credential based on the examined attribute.



3. Hold (By Holder / Subject)

Identity owner **holds** his/her own credentials.

The **holding tool** is software that can be used on mobile devices or web browsers.

Subject & Holder can be different entities.



4. Use (By Holder)

The holder who wants access or privileges can **use** his/her credentials via zero-knowledge proof.



5. Verify (By Inspector)

The inspector **verifies** the zero-knowledge proofs via protocol and the issuer identity.



This system is **private by design** throughout in adherence to the principles of EU GDPR

Example: Ontario e-ID (Canada)

1. EXAMINE

Service Ontario performs regulated process for determining identity of Ontario citizen



2. ISSUE

Service Ontario generates and delivers a digital credential in accordance with predefined schema

3. HOLD

Citizen holds digital credentials in a digital token wallet called a digital passport



4. USE

Ontario citizen presents “over 18 years old” zero-knowledge proof upon check-out



OCS ONTARIO CANNABIS STORE

Please read and accept the following to proceed.

MY DATE OF BIRTH IS:

Select DAY Select MONTH Select YEAR

I confirm that this is my legal date of birth.

I acknowledge that I must be 19 or older to enter this website and to buy and receive products from OCS.ca.

CONFIRM AND SUBMIT

5. VERIFY

Point-of-sale validates authenticity of issuer (Service Ontario) and holder (Ontario citizen), consume data (“over 18 years old”), and sells product (liquor or marijuana).



Example: Proof-of-Airworthiness

1. EXAMINE

An OEM or MRO organization via technicians and engineers examine the components, attest to its conditions, and signs off with a ring signature.



2. ISSUE

An OEM or MRO organization issues and delivers a new record using a commitment scheme according to predefined schema.

3. HOLD

An aircraft operator holds & controls the attested records to prove compliance and for processes internally or between partners, contractors, subcontractors, etc.

5. VERIFY

The aircraft operator approves the request for information to prove airworthiness from the inspector, and sends zero-knowledge range proofs of requested records for inspection.

4. USE

An inspector requests documentation regarding a specific aircraft to verify airworthiness.

Example: Certification & Licensing Inspection

1. EXAMINE

An institution (e.g. Cathay Aviation Certificate Programme) performs a process to determine if a credential is earned or not



2

2. ISSUE

The institution shall –upon satisfactory fulfilment of requirements– generate and deliver a digital credential in accordance with predefined schema.



3. HOLD

The certified individual holds the credentials in a personal digital pouch containing all credentials issued to the individual



4

4. USE

An inspector (e.g. aircraft operator or regulator) would like to confirm that an individual is certified for some role or tasks, etc.



5

5. VERIFY

The certified individual complies with the request and provides zero-knowledge range proofs of relevant data for inspection.



Example: Human Resources Background Checks

1. EXAMINE

An institution performs a process to determine if a credential is earned



2. ISSUE

The institution generates and delivers a digital credential in accordance with predefined schema



3. HOLD

A prospective worker (**holder**) is being background checked by a potential employer (**verifier**), who requests certain and specific credentials from relevant institutions (**issuer**) from the candidate.



4. USE

The candidate presents zero-knowledge proofs of requested attributes drawn from verifiable digital credentials issued by the institution.

5. VERIFY

The prospective employer validates the authenticity of the **issuer** (institution) and the **holder** (candidate), inspects the **data** (zero-knowledge proofs of credential attributes), and decides to hire the candidate (or not).



Example: Declaration of Business Interests

1. EXAMINE

Declarations are affidavit by Council Members.

2. ISSUE

The HKTDC Secretary co-signs the affidavit before sealing record.

3. HOLD

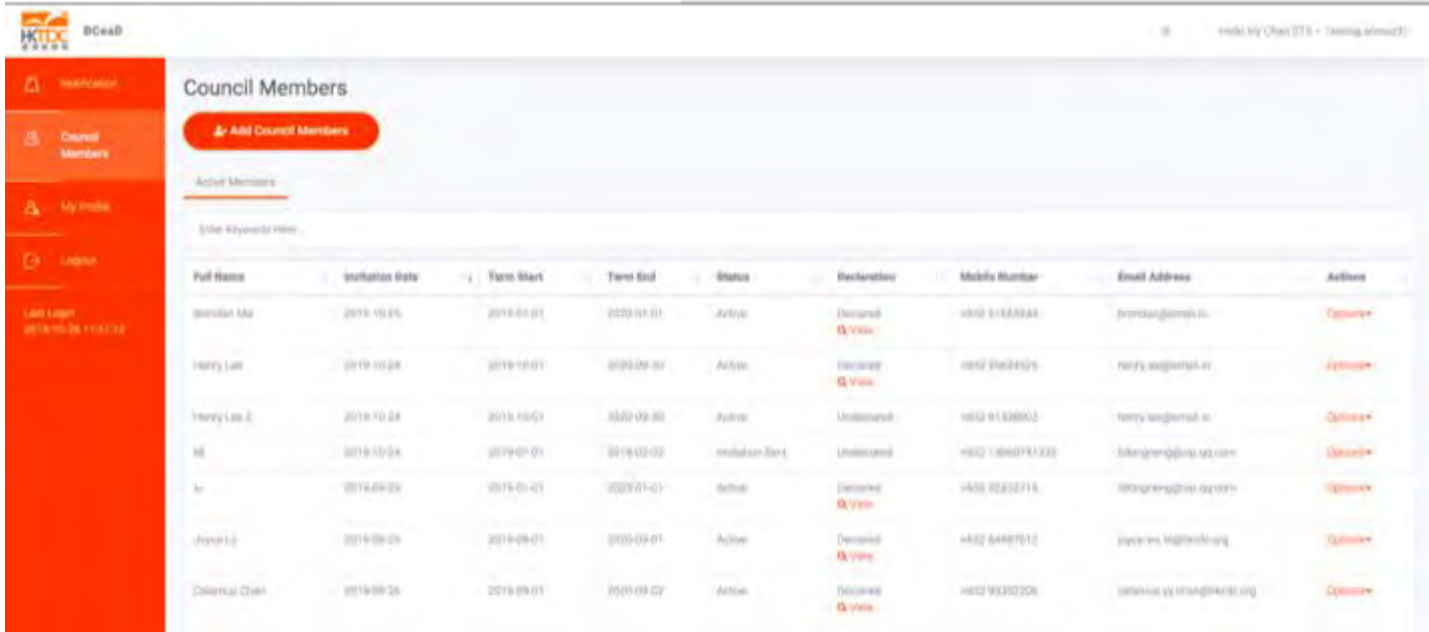
The Council Member holds their affidavits on their own devices.

4. USE

The Council Member may provide data via zero-knowledge proof.

5. VERIFY

The ICAC may inspect the records as part of an investigation.



The screenshot shows a web interface for 'Council Members' with a sidebar on the left containing navigation options: Home, Council Members, My Profile, and Logout. The main content area has a search bar and a table of council members. The table columns are: Full Name, Initiation Date, Term Start, Term End, Status, Declaration, Mobile Number, Email Address, and Actions. The table contains seven rows of data.

Full Name	Initiation Date	Term Start	Term End	Status	Declaration	Mobile Number	Email Address	Actions
Sherrill Ma	2019-10-25	2019-01-01	2020-01-01	Active	Declared & View	+852 51335544	sherrill@hktdc.hk	Options+
Henry Lee	2019-10-24	2019-01-01	2020-09-30	Active	Declared & View	+852 51624425	henry.leeh@hktdc.hk	Options+
Henry Lee E	2019-10-24	2019-01-01	2020-09-30	Active	Undeclared	+852 61326602	henry.leeh@hktdc.hk	Options+
Ng	2019-10-24	2019-01-01	2019-02-02	Initiation Term	Undeclared	+852 13860741232	tsikongng@hktdc.hk	Options+
Li	2019-09-29	2019-01-01	2020-01-01	Active	Declared & View	+852 92227115	li@hktdc.hk	Options+
Joyce Li	2019-09-29	2019-09-01	2020-09-01	Active	Declared & View	+852 54987012	joyce@hktdc.hk	Options+
Colman Chan	2019-09-26	2019-09-01	2020-09-02	Active	Declared & View	+852 93202206	colman@hktdc.hk	Options+

Example: Food Safety Assurance



1. EXAMINE

An applicant company (**holder**) applies to the FDA for certification for a certain product (**subject**). FDA approval processes determine if a certain product is compliant with specific regulations.

2. ISSUE

Upon passing the approval process, FDA (**issuer**) issues certificates indicating that the product is FDA-approved, and also issues a digital certificate (**credential**) to the applicant (**holder**).

3. HOLD

On behalf of the product (**subject**), the applicant (**holder**) holds the digital FDA certificate (**credential**) in a repository for verifiable digital credentials (**passport**).

4. USE

A consumer (**verifier**) wants to know if the product (**subject**) is FDA-approved. It asks the company (**holder**) to provide proof that the product is compliant.

5. VERIFY

The company (**holder**) sends a zero-knowledge proof linked to the digital FDA certificate (**credential**), which the consumer (**verifier**) can see that the FDA (**issuer**) did issue the certificate and that the certificate is valid.

Example: Health & Medical Insurance Claims



4. USE

Patient presents one or more credentials (e.g. owning a policy, pre-approval amount) to a clinic / hospital or lab

3. HOLD

Patient holds credentials in a digital wallet



**Portable Credentials
In A Digital Wallet**



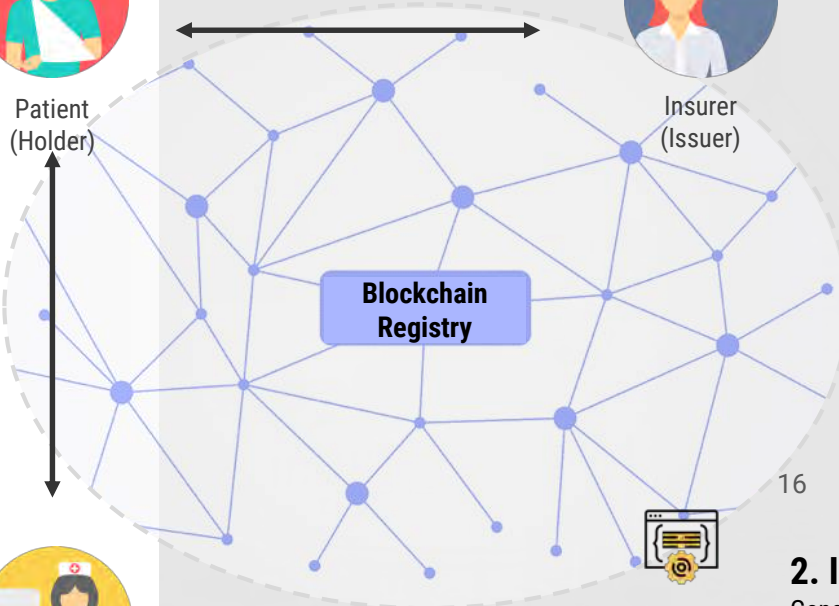
Patient
(Holder)



Insurer
(Issuer)



Hospitals & Clinics
(Inspector)



5. VERIFY

Validate authenticity of issuer and holder and then consume data

1. EXAMINE

Perform required vetting, due diligence, and other tasks needed to establish confidence in making an attestation about an identity/credential trait



Identity
Trait



Insurance
Policy

16

2. ISSUE

Generate and deliver a digital credential (e.g. owning an insurance policy, in-patient pre-approval amount) in accordance with some predefined schema

Example: Proof-of-Vaccination

PROBLEM



- Paper Records:
- Incomplete
 - Unverifiable



- Current Validation
- Time (gather records)
 - Money (replacement records)
 - Vaccines (better safe than sorry)



- Acceptance
- No recognition of records across borders
 - Standards between jurisdictions vary

SOLUTION



- Blockchain Records:
- Permanent & Immutable
 - Trusted & Verifiable

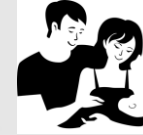


- Blockchain Validation
- Accurate & Fraud Reduced
 - Complete & Privacy Protected
 - Accessible Standards



- Blockchain Acceptance:
- Verifiable source of vaccines
 - Verifiable administration of vaccination

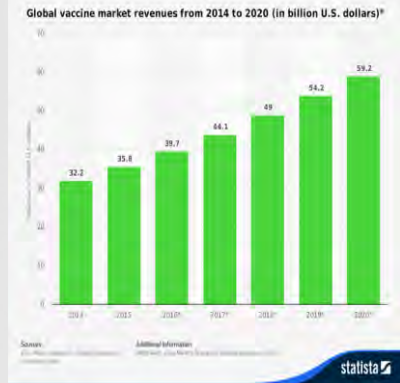
TARGET MARKET



Young Parents



Medical Tourists

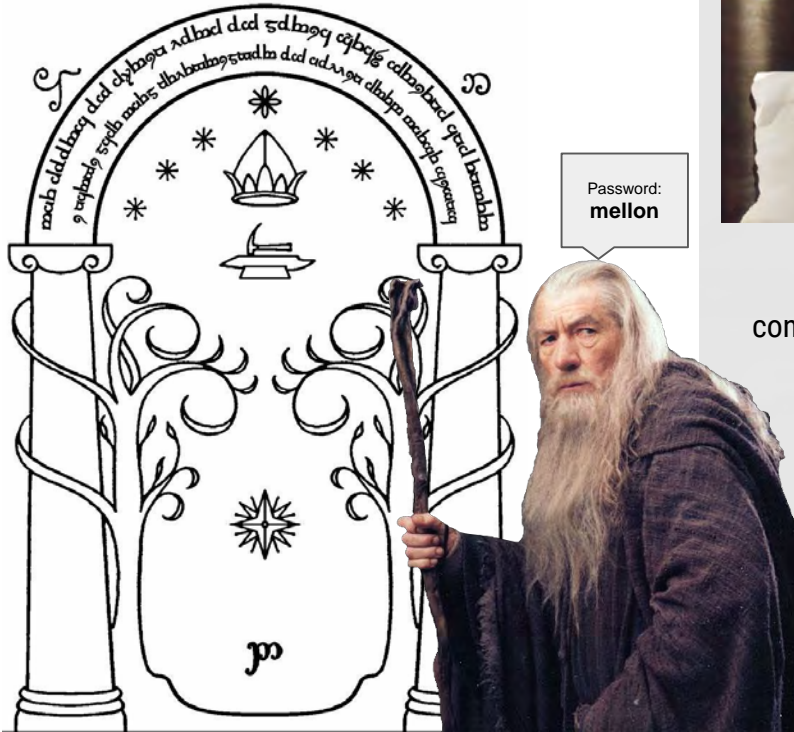


Distribute through insurance and bancassurance partners, subsidized by labs and pharmaceutical companies

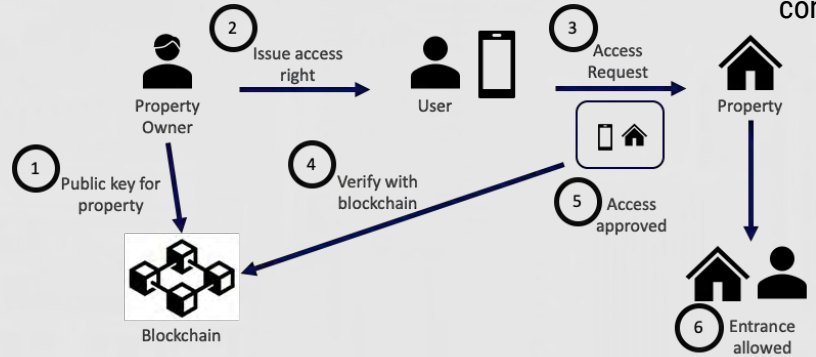
Example: Trusted Physical Access Control

PROBLEM: how do gates know who to open for?

CURRENT METHODS: hilariously insecure, unverifiable, unportable, unreliable!



BLOCKCHAIN SOLUTION: password-less, reliable logging, dynamic access control, no single point-of-failure, no potentially-corruptible centralized agent of control!





Emali

Let's continue our conversation

info@emali.io
www.emali.io

Blockchain-based Registry Systems with User-Centric Verifiable Digital Credentials