Paving the road to self-sovereign identity with blockchain: The Hellenic Distributed Ledger Technology Infrastructure (ELEDGER) & EBSI Conformant wallets

> Dr. Konstantinos Votis, Senior Researcher Head of Blockchain Lab, CERTH/ITI







The Commission has decided to award a grant, the terms and conditions set out in the Special Conditions, the General Conditions and the othe Annexes to the Agreement, number 2020-EL-IA



/www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/

Information Technologies Institute

Self-Sovereign Identity (SSI) Brief Introductory Note

The Digital Identity Problem

...quantity over quality

- Every platform makes users to enroll themselves for accessing the services.
- Reality is that multiple identities stored in proprietary systems refer to the same person.
- These identities are based on user's inputs and their validation may be inaccurate or obsolete.
- Companies perform the same procedure which is vastly costly.



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

The Digital Identity Problem

...disclosing too much

- There are unnecessary information that users share for a verification.
- Simple questions tend to require more information.
- The answer to the question if a person is adult is simply a yes or no.
- Current identities require the user's date of birth to verify the question revealing the actual age.
- Data disclosure should be minimised to the necessary.





When we think of digital identity we therefore need to see it not as a single thing. It is rather the sum total of all the attributes that exist about us in the digital realm, a constantly growing and evolving collection of data points.

Definition digital identity

EU blockchain observatory report on digital identity and blockchain <u>https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf</u> The digital identity problem

6

Identity Evolution

The models for online identity have advanced through three broad stages since the advent of the Internet

Phase One Centralized Identity <SILOS> The IDP relationship model adds a thirdparty to act as an "identity provider" between you and the organization or service you're trying to access. The IDP issues the digital credential, providing a single sign-on experience which can then be seamlessly used elsewhere, reducing the number of separate credentials you need to maintain. Self-sovereign identity is a twoparty relationship model, with no third party coming between you and the organization, now considered your "peer". SSI begins w/a digital "wallet" that contains digital credentials.

Traditional "siloed" identity is simple: an organization issues to you a digital credential that you use to access a service. Trust between you and the organization is typically established through shared secrets, usually via a username and a password.



Phase Two Federated Identity

<THIRD-PARTY IDP>



<PEER2PEER>



Federated Identity Model









Pain Points

- Registration w/ Username & Password
 - Weak security (low entropy)
 - Password management
- Different login credentials per online service
- No control over what data is shared
- Identity (credentials) depend on issuer liveness & permissions
 - Think: Facebook/Google ban your account
- Financial incentive to collect & sell user data:
 - All kinds of privacy violations
- Centralized storage of credentials:
 - Hackers love it
 - No fault-tolerance





'Self-Sovereign Identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity." - Christopher Allen

Self-Sovereign Identity (SSI) Model



10 PRINCIPLES OF SELF-SOVEREIGN IDENTITY



Standards



SSI Architecture: Overview



From Physical to Digital Credentials



Blockchain technology as a secure root of trust





EBSI use cases

Overview of functionalities



European Self-Sovereign Identity

Implement a generic Self-Sovereign Identity capability, allowing users to create and control their own identity without relying on centralized authorities.



Use case: European Self-Sovereign Identity

Overview of core functionalities



• Request verifiable consent / mandate

Issuers can:

- Verify identifications
- Suspend / revoke credentials



shared with whom) Issuers can request

their registration

elD)

- Request / obtain / present

European Blockchain Services Infrastructure

...investing in Blockchain

eLedger Connected European Facility Project

EUROPEAN BLOCKCHAIN PARTNERSHIP

What is the European Blockchain Services Infrastructure (EBSI) 2019-2020?





Notarisation of Documents for Auditing Purposes

Leveraging the power of blockchain to create trusted digital audit trails, automate compliance checks in timesensitive processes and prove data integrity.



Certification of Diplomas

Giving control back to citizens to validate their education credentials, significantly reducing verification costs and improving authenticity trust.



EU Self-Sovereign Identity Framework

Implementing a generic Self-Sovereign Identity capability, allowing users to create and control their own identity without relying on centralized authorities.



Leveraging blockchain technology to securely share data (e.g. IOSS VAT identification numbers and import onestop-shop) amongst customs and tax authorities in the EU.

2 official EBSI installations (GRNET, CERTH)

European

EBSI conformant wallet & identities

- EBSI requires the use of Decentralised Identifiers (DIDs) as the cornerstone of selfsovereign identity (SSI).
- Promoting the use of openness with open standards use from W3C. Specifically, Credential Issuance is compliant with OIDC 4 Verifiable Credential Issuance.
- Identities are a core component in every service.



EBSI Verifiable Credentials – OpenID Connect



On January 23, CERTH's digital wallet had its compliance report published on EBSI.



Credential Issuance guideline n OIDC for Verifiable Credentia Verifiable Presentation exchar sed on OIDC for Verifiable Pr

Issuer: any entity that creates and issues digital credentials. They are responsible for verifying the identity and publish a digital credential. **Identity owner:** The person who controls the digital identity. They decide what information to share and whom accesses them.

Verifier: any entity that verifies the authenticity of the document presented by the identity owner.

Comparing contemporary digital identities with SSI



Privacy

Personal information are shared with third-parties. **SSI** allows individuals to control the information to share and with whom.

Security

Traditionally, centralised entities are a point for attacks (hacks, data breaches). **SSI** uses cryptographic technology to secure digital identities and prevent unauthorized access.

Interoperability

Contemporary systems' identities are in siloes and are not transferable. **SSI** is based on standardisation for usability across platforms.

Access

Access can phase barriers for marginalized communities since they are based on traditional identity systems. **SSI** aims to create a system that is inclusive and accessible to all individuals, regardless of their background or circumstances.

Trust

Individuals put their trust on third parties to manage identities and underlying data. On the other hand, **SSI** have individuals to verify their identities using trusted credentials.

EBSI conformant wallet requirements

- Support for the EBSI network
- Compliance with EBSI standards
- Secure storage of private keys
- User control over data
- Interoperability
- Compliance with data protection regulations



Openness, security, and cross-border applicability are essential.

CERTH/ITI Self-Sovereign Identity (SSI)

Solution Overview & Use Cases



On January 23, CERTH's digital wallet had its compliance report published on EBSI.

Technologies

Self-Sovereign Identities \rightarrow Security, Controllability and Portability of an identity \rightarrow No Central Authority

SSI Decentralized Identifiers (DIDs) - unique global identifiers, cryptographically verifiable

SSI Verifiable Credentials (VCs) - Machine-readable digital credentials, cryptographically verifiable, tamperproof, no need for the issuer to mediate the presentation and verification of the VC

SSI Zero-knowledge Proofs (ZKP) - prove the truthfulness or possession of a claim to a verifier without conveying any further information about the claim itself or revealing the actual claim

Hyperledger Aries (HLA) - Shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials.

Hyperledger Indy (HLI) - Interoperable distributed ledger for purpose-built for privacy-preserving digital identities.

Solution Benefits & Overview

- It is a set of services that allow implementing Self-Sovereign Identity systems in order to establish digital trust
- It allows entities to share data between each other in a trustworthy, standardized and privacy-preserving way
- Using these services, the entities are able to:
 - Obtain secure wallets for controlling and managing their DIDs and VCs
 - Create and use private communication channels based on DIDs for information exchange
 - Issue, prove and verify VCs



Solution Components

- Credential Issuer Platform:
 - Issue, revoke & verify credentials
- Credential Holder (Web & Mobile Wallet):
 - Receive, prove & verify credentials

Ancillary Services:

- Mediator Service
 - Cloud messaging mix network (similar to Tor).
- Verifiable Credentials Verification Service (VCVS):
 - Bridge between credentials & OAuth 2.0 & OpenID Connect as a service

Issue Credential Definition	➡ Credentials						
Connection	Add Schema Add Creeder	ntial Defection				Issue Predentials	
Samsung							2
Credential Definition						C) search keyword	4
UniversityDegreeCredentialDefinition	Credential Definition	Schema	Connection	issued	State	Actions	
Available Attributes	CredentialDefinitionTest	SchemaTest	Poco	12 days ago	Issued	0 0	
degreeTitle	LoginDefinition Name	LoginSchema	Poco	12 days ago	Issued	0	
	LoginDefinition Name	LoginSchema	Xamarin	8 days ago	Issued	00	
universityName	CredentialDefinitionTest	SchemaTest	Xamarin	7 days ago	Issued	00	
	CredentialDefinitionTest	SchemaTest	Samsung	5 hours ago	Issued	0	
lastName	LoginDefinition Name	LoginSchema	Samsung	5 hours ago	Issued	0	
	UniversityDegreeCredentialDefr nition	UniversityDogreeSchema	Samoung	3 hours ago	Issued	00	
grade			Showing 1 to 7 of 7 entries	- 66 - 1 - 5 - 50	10 🗸		
			Issue Credential				
(Carte) = Connections			Wallet: Pharmatedger IoT				I
Contention Contention Instation Accept Connection Condeman Werfordion Plasmaledger Instarr Agent	tion Invlation					Search Search Convertion By Norte.	
Authoritations						• •	0
Plasmaledger baser Agent							•
• Adve						000	9
	Please, Ent	er a PIN to initialize your must consist of four(4) numb	wallet	+645 ■ ← Credential	10 10 10 10 10 10 10 10 10 10 10 10 10 1		
		Litter Pill		Pharmaled	iger Issuer Agent		
		* * * *		Issuer DID: 4sSDdf Date Acquired: 2022	Fvmhgrb2pmuA94MN 03-29		
		Initialize		Credential	LogisSchome 10		
				Date Issued:	2022-03-29		
				Status:	Valid		
				city	Thessaloniki		
				lastName:	Πατιαδότιουλος		
				email:	cpapado@hotmail		
				firstName:	Χρήστος		
	•	•		⊲			

Problem statement

- Time-consuming and error-prone work involved around procurements
- Fragmented process, limited use of technology, communication silos among civil servants and departments
- P

?

- Lack of transparency about timeline, procedures, requirements and fund allocation
- Limited citizen participation in decision making processes



CERIH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS









ACTORS



PROCUREMENTS



E-VOTING

🔀 Token 🛛 🗙 (civil_servant) * PROCUREMENTS Procurements စ် Users Votings
 Q Search... Assignment Type Announcement ۵ Outcome Invitations Requests Quotations \$ ۰ Actions Title Status Approved Procurements Date Procurement procurer001@gmail Yes 0 Apr 19, 2022 Direct assignment closed 3 0 3 19-4-2022 Quotations .com Procurement procurer001@gmail Yes 0 0 1 Apr 20, 2022 Direct assignment closed 20-4-2022 Scontracts .com Procurement procurer2004@mail Yes 6 2 Apr 20, 2022 2 0 Direct assignment closed 20042022 - 2 සි Payments .com Procurement Waiting ٨ 0 **Direct assignment** oper 0 0 19-4-2022 - 2 My Account
Procurement ٨ Yes Apr 25, 2022 Direct assignment open 0 0 0 25042022 🖃 Logout 1 🕨 H н ч Token has received funding from the European Union's Horizon 2020 S Token research and innovation programme under the Grant Agreement Nº 870603

VIEWS

(Civil Servant –

Procurement Process)

S Token 🗙 Procurer Procurer (procurer)
 Reference
 Reference PROCUREMENTS Procurements Procurements Q Search... Assignment Type Announcement My Quotations Title ≜ Outcome Invitations Requests Quotations Approved Actions \$ Date Procuremen procurer001@gmail Yes 0 My Account
Apr 19, 2022 0 3 Direct assignment closed 3 19-4-2022 .com Procurement procurer001@gmail Yes 0 🗄 Logout Apr 20, 2022 0 1 Direct assignment closed 20-4-2022 .com Procurement procurer2004@mail Yes 0 0 2 Apr 20, 2022 2 Direct assignment closed 20042022 - 2 .com Procurement Yes 00 Apr 25, 2022 Direct assignment open 0 0 0 25042022 н ∢ 1 ▶ н Token has received funding from the European Union's Horizon 2020 S Token research and innovation programme under the Grant Agreement Nº 870603

VIEWS

(Procurer –

Procurement Process)

× i S Token 🗙 ② Citizen Citizen (citizen) POLLS Polls 🚖 Votings Q Search. My Account
Poll Title State ٠ Title Demo voting Demo voting Active Expiration Date 🖃 Logout Apr 28, 2022, 12:43:10 PM Choose location for new fountain Finished Description 1 🕨 🗏 Please answer Is this demo ok? Topic Yes No Select a choice Submit My Vote to submit your vote. Token has received funding from the European Union's Horizon 2020 S Token research and innovation programme under the Grant Agreement Nº 870603

VIEWS

(Citizen – Evoting Process)



VIEWS

(Citizen – Evoting Process)



Evoting Process)



MOBILE APPLICATION

(Citizen – Evoting Process through Mobile Application)





Track&Trace @Agrifood

...investing in Blockchain Research and Development



Track&Trace Waste Assets

...investing in Blockchain Research and Development





Digital identity & Blockchain in Freight

...investing in Blockchain Courier Platform



Digital identity & Blockchain in Transport

...investing in Blockchain Research and Development



Container Pick-Up application (COREOR requests)

🖪 DataPorts	≡							shippingAgent1_admin 🛕 💄 🇮
A Home	COREOR Rec	luests						
COREOR Requests								+ New COREOR Request
Booking Requests		Status:						
Organization	Y Show							
🛎 Users								
▲ Profile	Search							
Notifications	Request ID ↑↓		Registration Date ↑↓	Origin Port ↑↓	Destination Port ↑↓	Permit ID ↑↓	Status ↑↓	Approval/Rejection Date ↑↓
	22026741751718	34160	Wed Feb 15 2023 11:56:00 GMT+0200	ITBRI	GRSKG		pending	
	2249670074318	73020	Tue Feb 14 2023 14:16:00 GMT+0200	AEAUH	ARBUE		pending	
	38909191189852	21200	Wed Feb 15 2023 15:08:00 GMT+0200	ARUAQ	ARRGA		pending	
	52325411097754	14400	Wed Feb 15 2023 12:15:00 GMT+0200	ITPMO	GRSKG		pending	
	57662374848113	35400	Wed Feb 15 2023 15:04:00 GMT+0200	AEAUH	AU888	AHNDBOR81GVFMS3C	accepted	Wed Feb 15 2023 15:09:00 GMT+0200
	57777155628268	37200	Tue Feb 14 2023 13:07:00 GMT+0200	AEJEA	ARLPS		rejected	Wed Feb 15 2023 11:38:00 GMT+0200
	5808131358990	51800	Tue Feb 14 2023 14:16:00 GMT+0200	BRFOR	AFKBL		rejected	Tue Feb 14 2023 14:24:00 GMT+0200
	67206719190058	38000	Wed Feb 15 2023 14:17:00 GMT+0200	AEJEA	ARPMD		pending	
	76612439512902	2420	Tue Feb 14 2023 13:05:00 GMT+0200	AEAJM	AUADL		pending	
	7841809126500	05600	Tue Feb 14 2023 18:22:00 GMT+0200	NLAMS	GRSKG		pending	
					<pre><< 1 2 > >></pre>			





Container Pick-Up application (new COREOR) request)





research and innovation programme under the Grant Agreement Nº 871493

Blockchain in Microfinancing

...investing in Fintech

BLOCKCHAIN BASED CREDIT SCORING WEB APPLICATION FOR MICROFINANCING / loans to tokens....



Decentralized credibility and		
microcredit		
	₿	Dashboard
Blockchain based credibility evaluation	٥	Διακείριση Ερωτήσεων
lobal lacinity for the sharing econom	lts.	E-Statement Actricewv
in our list to stay informed	lh.	E-Statement Δοντίων
Your Email	¢	Reports
	-28	Ρόλοι Χρηστών
	•	Marketplace
	:	Προφίλ

(-) Αποσύνδεση

SSI-Enabled Passwordless Login

- Login Page
- Click on "Mobile App" button
- Scan QR-code with Mobile App

Tap Roboten Logged-in user redirected to the platform

Κωδυκός Δανείου		Score Card	Σύνολο Πληρωμής (δόσης)			Αναζήτηση	
	Κωδικός Token			KAddoc	Εξόφληση	Κατάσταση	
			Δεν υπόρχουν κατακωρημένες δόσεις				

Thank you

Information Technologies Institute Centre for Research & Technology Hellas

Dr. Konstantinos Votis Senior Researcher Head of Blockchain Lab, ITI EU Blockchain Observatory and Forum Member kvotis@iti.gr



The Commission has decided to award a grant, under the terms and conditions set out in the Special Conditions, the General Conditions and the other Annexes to the Agreement, number 2020-EL-IA-