Distributed Ledger Technologies Workshop
(**DLT 2025**)

Beyond DID/SSI: Bridging Web2 and Web3 Transparently

Pierpaolo Della Monica
Sapienza University of Rome

Ivan Visconti
Sapienza University of Rome

Andrea Vitaletti
Sapienza University of Rome

Marco Zecchini
Sapienza University of Rome

do you want to know more about it?
visconti@diag.uniroma1.it

November 27, 2025

La Parola di Nakamoto

E' necessario un sistema di utilizzo del **denaro** che sia accessibile per tutti, quindi **censorship resistant**

La Parola di Nakamoto

E' necessario un sistema di utilizzo del **denaro** che sia accessibile per tutti, quindi **censorship resistant**

Non devono esserci organizzazioni in grado di **censurare** una transazione tecnicamente legittima

La Parola di Nakamoto

E' necessario un sistema di utilizzo del **denaro** che sia accessibile per tutti, quindi **censorship resistant**

Non devono esserci organizzazioni in grado di **censurare** una transazione tecnicamente legittima

La **decentralizzazione** è la via per realizzare questi sistemi

Oltre il denaro: DID, SSI

Un **DID** (***Decentralized*** *Identifier*) è un identificatore digitale autonomo, non dipendente da un'autorità centrale, è verificabile tramite blockchain o altri decentralized ledgers

Oltre il denaro: DID, SSI, VC

Un **DID** (***Decentralized*** *Identifier*) è un identificatore digitale autonomo, non dipendente da un'autorità centrale, è verificabile tramite blockchain o altri decentralized ledgers

SSI (*Self-Sovereign Identity*) è un modello di identità digitale in cui l'utente ha pieno controllo sulle proprie credenziali e sul modo in cui le condivide, e può usare **Verifiable Credentials (VC)**, attestazioni firmate e non falsificabili

Prima domanda su DID / SSI / VC

DID, SSI e VC sono concetti proposti da quasi 10 anni, sono ampiamente noti e studiati oltre 5 anni e sono stati anche standardizzati dal W3C

Chi li usa oggi?

Prima domanda su DID / SSI / VC

DID, SSI e VC sono concetti proposti da quasi 10 anni, sono ampiamente noti e studiati oltre 5 anni e sono stati anche standardizzati dal W3C

Chi li usa oggi?

In concreto: **nessuno**!
Ci sono progetti ancora **sperimentali o in fase pilota**, nulla in produzione che sia “mainstream”

Seconda domanda su DID / SSI VC

Le **Verifiable Credentials** rispettano la parola di Nakamoto circa la decentralizzazione per avere **censorship-resistance**?

Seconda domanda su DID / SSI VC

Le **Verifiable Credentials** rispettano la parola di Nakamoto circa la decentralizzazione per avere **censorship-resistance**?

In concreto: **No**! Il problema è che ti serve un issuer ma:

A) Potrebbe **non** esserci nessuna organizzazione (con sufficiente reputazione) **interessata** a tale attività (es., chi ti rilascia una VC che attesti che hai fatto un ordine su amazon?)

Seconda domanda su DID / SSI VC

Le **Verifiable Credentials** rispettano la parola di Nakamoto circa la decentralizzazione per avere **censorship-resistance**?

In concreto: **No**! Il problema è che ti serve un issuer ma:

A) Potrebbe **non** esserci nessuna organizzazione (con sufficiente reputazione) **interessata** a tale attività (es., chi ti rilascia una VC che attesti che hai fatto un ordine su amazon?)

B) Gli issuer interessati a quelle specifiche credenziali possono essere motivati (es., dai poteri forti) a **negartela** (vedi US vs Francesca Albanese e/o TornadoCash)

Bridging Web2 and Web3 (il nostro contributo)

I nostri dati sono in gran parte sul **Web2**, ossia memorizzati e gestiti da servizi esterni ai quali accediamo con un browser usando **TLS**

Possiamo ottenere credenziali sui **dati del Web2**?

Bridging Web2 and Web3 (il nostro contributo)

I nostri dati sono in gran parte sul **Web2**, ossia memorizzati e gestiti da servizi esterni ai quali accediamo con un browser usando **TLS**

Possiamo ottenere credenziali sui **dati del Web2**? **Si**
Possiamo riuscirci **senza censura**?

Bridging Web2 and Web3 (il nostro contributo)

I nostri dati sono in gran parte sul **Web2**, ossia memorizzati e gestiti da servizi esterni ai quali accediamo con un browser usando **TLS**

Possiamo ottenere credenziali sui **dati del Web2**? **Si**
Possiamo riuscirci **senza censura**? **Si**
Anche se i server **non sono interessati** a rilasciare credenziali?

Bridging Web2 and Web3 (il nostro contributo)

I nostri dati sono in gran parte sul **Web2**, ossia memorizzati e gestiti da servizi esterni ai quali accediamo con un browser usando **TLS**

Possiamo ottenere credenziali sui **dati del Web2**? **Si**
Possiamo riuscirci **senza censura**? **Si**
Anche se i server **non sono interessati** a rilasciare credenziali? **Si**
Queste credenziali sono verificabili con strumenti **standardizzati**?

Bridging Web2 and Web3 (il nostro contributo)

I nostri dati sono in gran parte sul **Web2**, ossia memorizzati e gestiti da servizi esterni ai quali accediamo con un browser usando **TLS**

Possiamo ottenere credenziali sui **dati del Web2**? **Si**
Possiamo riuscirci **senza censura**? **Si**
Anche se i server **non sono interessati** a rilasciare credenziali? **Si**
Queste credenziali sono verificabili con strumenti **standardizzati**? **Si**

La via tracciata da Nakamoto va oltre l'uso del denaro

Teoria o Pratica?

ACTS: Attestations of Contents in TLS Sessions

Della Monica, **Visconti**, Vitaletti, Zecchini
Sapienza Universtià di Roma

Apparirà in *The Network and Distributed System Security (**NDSS**) Symposium 2026*
Sperimentazione su un **PDF** di alcuni KB, ottenendo un **PAdES**

Tecnologia sottostante: **2-party computation** di un client TLS client (già industrializzato da ChainLink ed altri, partendo da DECO), **predicate blind signatures**, **zero-knowledge proofs**

Limiti degli altri progetti: **TLSNotary** è inadeguato perché ha almeno una delle seguenti due criticità: 1) richiede advanced crypto per un verifier di credenziali; 2) penalizza la privacy dell'utente

SAPIENZA UNIVERSITÀ DI ROMA

Lavori in corso:

- Rivisitare gli standard su DID/VC sulla scia di Nakamoto (decentralizzazione ==>no censura)
- Decentralizzare il "Notary" (problema del single point of failure dell'issuer)
- Ottimizzare ed industrializzare l'architettura su una generalità di casi d'uso rilevanti

THANKS!

November 27, 2025

This presentation has been proudly generated with the help of ChatGPT