Rebooting the Web of Trust

Design Workshop 11, The Hague September 21-25th 2020

Why Now?

A confluence of problems and opportunities make now the time for protected digital identity

Covid-19
The world is reacting to Covid-19 crisis by applying technology to anything and everything it can. Having a design led workshop in September provides the perfect opportunities for us to take a step back and consider the implications of what we have built and are currently trying to build.

Human Rights
United Nations SDG 16.9 targets identity for all by 2030.

GDPR
European General Data Protection Regulation requires continuous attention and action on data protection.

RWOT workshops are collaborative, ‘co-opetition’ environments

How do we establish decentralized digital identities?

RWOT brings together experienced global leaders and researchers in technology, sociology, and industry with veterans of the Web of Trust to answer questions such as:

- How can we establish identities controlled by the individual, but trusted by strangers?
- How can we replace usernames and passwords with globally recognized secure-access methods?
- How can digital identity systems be used to replace current expensive identification methods, to address the legitimate use for access control and risk management, without increasing the attack surface for bad actors?
- How do we enable the benefits of digital identity without the harms of ubiquitous surveillance?

RWOT measures its success through concrete outputs in the form of white papers, specifications, and software repositories, with the aim of influencing standards organizations and enabling its members to develop industry leading solutions.

Sponsorship opportunities are available in three tiers

PLATINUM SPONSOR

€30,000

- Designation of one topic for research and presentation by workshop researchers
- Two attendee passes
- Two passes for external experts related to your topic
- Plus All benefits of Gold Sponsorship

GOLD SPONSOR

€10,000

- Opportunity at the beginning of the workshop to present current work, topical research and other ideas to inspire topic selection
- Plus all benefits of Silver Sponsorship

SILVER SPONSOR

€5,000

- Name & logo on event research papers, also on event media
- Share freebies and marketing materials with attendees
- Access to community communications channels, e.g., Discourse and Signal

RWOT has demonstrated ability to achieve success in its outcomes

- 50+ collaborative white papers published from 9 Workshops in the topic areas of Identity, Reputation, Privacy & Digital Rights, Verification, Public Key Infrastructure, and more (complete list at http://www.weboftrust.info/papers.html)
- 250+ topic papers shared to participants before events
- Both the new *W3C Verifiable Credentials* standard and the newly chartered *W3C Decentralized Identifier Working Group* have adopted the technologies incubated during RWOT for International Standards
- 10+ active major platform providers building on technologies created or incubated at RWOT.

"Digital human rights are a recent topic and they still need to be developed to a great extent. SSI is an essential part of that. More security, more privacy; these are very important parts of digital human rights..." — **Rhodia Maas**, General director of the National Office for Identity Data

The Hague Rebooting the Web of Trust Design Workshop Sep 21-25

Design led workshop

The design process will help attendees explore their creativity and collaborative, multidisciplinary powers. They'll be facilitated breaking up in teams working closely together on the subject of interest, either with code or a paper.

The goal is to

- Collaboratively create at least five technical papers or specifications on topics that will have the greatest impact on the future.
- Showcase the scope of use cases and requirements for decentralized identity and trust.
- Discuss and suggest approaches to the legal implications.

"It's time to recognise the web of trust as a basic human right. That means guaranteeing affordable access for all, ensuring connectivity without commercial or political discrimination, and protecting the privacy and freedom of web users regardless of where they live.."
— **Tim Berners-Lee**

Topics currently submitted for consideration: https://bit.ly/rwot10topics

waardevolle toepassingen van deze technologie.

Self-Sovereign Identity (SSI)

Digitale identiteit is van cruciaal belang. De SSI is het puzzelstukje dat diverse vraag-stukken rondom blockchain kan verbinden. Bijvoorbeeld de bevestiging dat jij jij bent en/of dat jij 18+ bent.

Logistiek

Transparante, betrouwbare en eerlijke ketens. Minder administratieve lasten en efficiënter transport.

Onderwijscertificaten en diploma's

Officiële documenten zoals diploma's, certificaten en registers betrouwbaar delen en verifiëren.

Pensioen

Een simpele vraag zoals: "Hoeveel pensioen heb ik waar opgebouwd?" kan door blockchaintechnologie makkelijker beantwoord worden dan met de huidige systemen.

Compliance by design

Meer transparantie en automatisering van subsidie-processen zodat het voor iedereen makkelijker, eerlijker en efficiënter wordt. Blockchain biedt die mogelijkheid. In de taal van technologie: 'Compliance by design'.

Hypotheken

Bij een hypotheekaanvraag kan de tijdrovende (papieren) administratie vervangen worden door een digitaal en dus sneller proces.

Bij vaak wisselen van baan kunnen de

Dutch Blockchain Coalition


INTERNATIONAL CITY
OF PEACE AND JUSTICE
FOR A BETTER WORLD
VREDE EN RECHT
The Hague

SPONSORING RWOT11:

ICTU is working on an improved digital government

Together with our clients we achieve high quality digital services. We connect knowledge to skill and solutions to problems, whilst observing the balance between technology and use, and innovation and workable solutions. So that any business conducted with the government, by either an individual or a company is done safely, easily and digitally. As independent consultant and executor within the government, we look for the right combination of expertise for every assignment so that both the government and society benefits.

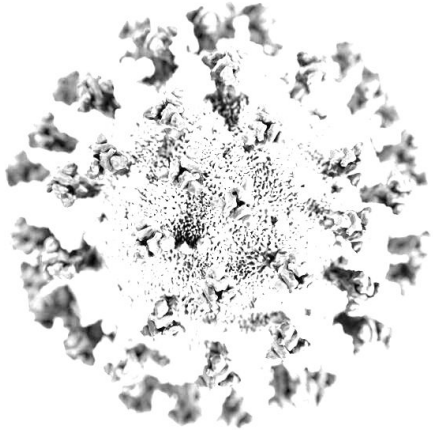
How to Participate in RWOT Community?

- Website: www.WebOfTrust.info
- GitHub: github.com/weboftrustinfo
- More Info: ChristopherA@LifeWithAlacrity.com

Submit Advance Reading Topics (1 or 2 pages) for:

- Next Event: September 21-25 2020 The Hague
- Following: Spring 2020, TBA
- Submit to: https://bit.ly/rwot10topics

Covid disclaimer



We are preparing in case Covid related issues cause disruptions due to travel restrictions and quarantines

- Online participation
- Refundability

We commit to a good faith effort to refund any sponsorship money that hasn't been spend proportionally in the event that we have to cancel.

Your sponsorship is helping this move forward despite these difficult times. It is even more important that we are exploring these ideas together.

Appendix

Design Workshop 11, The Hague September 21-25th 2020

RWOT Leadership

CHRISTOPHER ALLEN

FOUNDER & CHAIRMAN RWOT
W3C CREDENTIALS CO-CHAIR
PRINCIPAL ARCHITECT,
BLOCKCHAIN COMMONS

As a pioneer in internet cryptography, Christopher has initiated cross-industry collaborations and created industry standards that influence the entire internet, including jointly developing SSL and co-authoring the IETF TLS internet draft that is now at the heart of all secure commerce on the World Wide Web.

JOE ANDRIEU

W3C CREDENTIALS CO-CHAIR
BOARD MEMBER

Joe is CEO of Legendary Requirements. He leads requirements efforts for the W3C Decentralized Identifiers WG, W3C Credentials CG and RWOT. He is the creator of the Information Lifecycle Engagement Model, the lead author of Joram 1.0.0, Amira 1.0.0, and the Functional Identity Primer.

DAN BURNETT

W3C DID WG CO-CHAIR
W3C VER CRED CO-EDITOR

Over the past 20 years Dan has edited and authored over a dozen web and Internet standards. Having recently edited and chaired the W3C Verifiable Credentials work, he is now Co-chairing the DID WG at W3C. He currently works at ConsenSys as a Blockchain Standards Architect.

DMITRI ZAGIDULIN

W3C DID RESOLUTION SPEC
CO-EDITOR

Dmitri is a distributed systems engineer, specializing in decentralized identity, authentication and personal data storage. Veteran of numerous standards bodies, community groups and working groups.

Who are we?

- A 501(c)4 social benefit organization based in the United States
- A semi-annual collaborative writing workshop
- A volunteer organization advancing the cause of decentralized identity
- A safe space for companies, organizations, and governments to explore new ideas in identity

Rebooting the Web of Trust gathers passionate professionals to define, explore, and advocate for decentralized identity. We hold workshops and salons where we discuss, collaboratively write, and ultimately publish ground-breaking papers and software to help shape the future of identity.

Examples of our Work: Self-Sovereign Identity principles

- ***Existence:*** Users have an independent existence — they are never wholly digital
- ***Control:*** Users must control their identities, privacy or celebrity as they prefer
- ***Access:*** Users must have access to their own data — no gatekeepers, nothing hidden
- ***Transparency:*** Systems and algorithms must be open and transparent
- ***Persistence:*** Identities must be long-lived — for as long as the user wishes
- ***Portability:*** Information and services about identity must be transportable by the user
- ***Interoperability:*** Identities should be as widely usable as possible; e.g. cross borders
- ***Consent:*** Users must freely agree to how their identity information will be used
- ***Minimalization:*** Disclosure of claims about an identity must be as few as possible
- ***Protection:*** The rights of individual users must be protected against the powerful

Examples of our Work: Identity Use Cases

Fundamentally, the Web of Trust is about digital identity in its many forms. Several of the outputs of the workshops have tackled the topic directly.

Michael Lodder has written about ***verifiable offline credentials***. He covers various scenarios where some or all parties have intermittent, unreliable, untrusted, insecure, or no network access, but require cryptographic verifcation (message protection and/or proofs). Applicable situations include marine, subterranean, remote expeditions, disaster areas, refugee camps, and high-security installations. He then recommends solutions for addressing offline deployments.

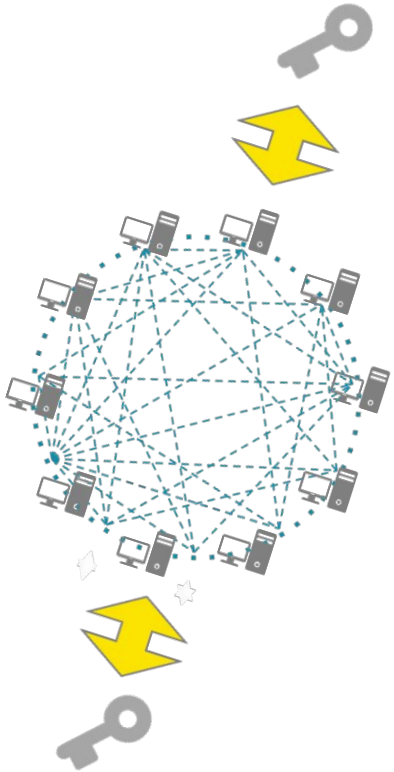
Sean Gilligan has written about ***social key recovery***. He focusses on the social recovery of control of an identifier. There are several techniques to re-assert control over identifiers including key recovery and issuance of a new key. In many situations it is preferable to establish a new key than recover the old one. He proposes a rubrik for evaluating such schemes, and give a brief overview of possible schemes to consider.

Examples of our Work: Decentralized Public Key Infrastructure

Today's Internet places control of online identities into the hands of third-parties. Email addresses, usernames, and website domains are borrowed or "rented" through DNS, X.509, and social networks. This results in severe usability and security challenges Internet-wide.

This paper describes a possible alternate approach called *decentralized public key infrastructure (DPKI)*, which returns control of online identities to the entities they belong to. By doing so, DPKI addresses many usability and security challenges that plague traditional public key infrastructure (PKI).

DPKI has advantages at each stage of the PKI life cycle. In usage, it can help "Johnny" to finally encrypt thanks to its relegation of public key management to secure decentralized datastores. Finally, it includes mechanisms to recover lost or compromised identifiers.

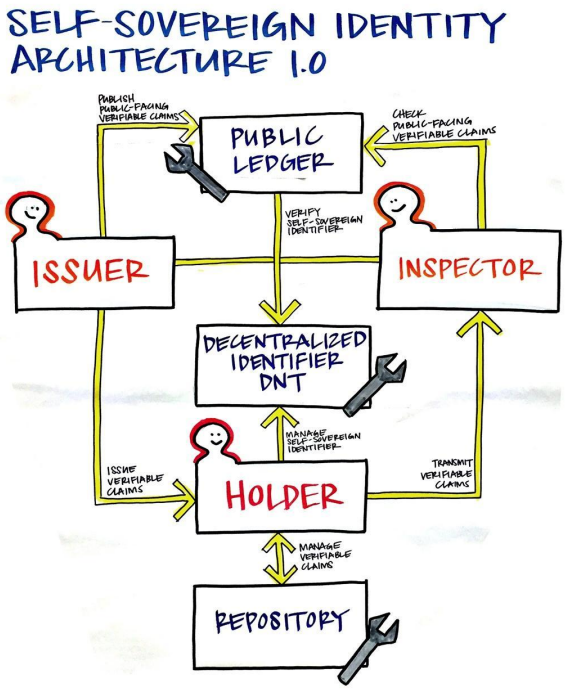


Examples of our Work: Data models for Decentralized Identifiers

DIDs (Decentralized IDentifiers) are a new type of identifier intended for verifiable digital identity that is "self-sovereign".

DIDs resolve to DDOs (DID descriptor objects)—simple JSON documents that contain all the metadata needed to prove ownership and control of a DID. Specifically, a DDO contains a set of key descriptions, which are machine-readable descriptions of the identity owner's public keys, and a set of service endpoints, which are resource pointers necessary to initiate trusted interactions with the identity owner.

One of the most successful RWOT incubations, DID is now on a W3C standards track, under development by the Decentralized Identifier Working Group
https://www.w3.org/2019/did-wg/



Examples of our Work: Smart Consent Protocol - Personal data as digital intellectual property

Personal Data are valuable resources for creating digital intellectual property (IP). Rights over this IP have generally been unclear, resulting in systematic abuse or unfair use of people's personal data by third parties. But new regulations are changing this - most notably, the European Union General Data Protection Regulation (EU GDPR). Third parties must now obtain explicit and documented consent from people (data subjects) to collect, process, store or disclose their personal data.

A specification for operationalizing these regulatory requirements, using digital Consent Receipts, is being developed through the Consent and Information-Sharing Working Group of the Kantara Initiative.

```
{   "@type": { "/": "<hash pointing to RDF-Schema of Right>" },
    "usages": "all|copy|play|stream|...",
    "territory": { "/": "<hash pointing to the Place>" },
    "context": "inflight|inpublic|commercialuse…",
    "exclusive": "true|false",
    "manifestation": { "/": "<hash pointing to the Manifestation>" },
    "license": { "/": "<hash pointing to the License>" }
}
```

Example format