NGI

Partnership for innovative technological solutions to ensure privacy & enhance trust for the human-centric Internet

Webinar, 19 November 2020

NGI TRUST

NGI_Trust projects presentations (1/2)

Project	Third party
DeepFake	Sentinel (Sidekik OU)
AnonymAI	CELI
Casper 2.0	University of Belgrade – School of electrical engineering
Cassiopeia	IT-Av - Instituto de Telecomunicações - Aveiro
DAppNode	DAppNode Association
FAIR-AI 2.0	The University of Cambridge
GeoWallet	Blocs et Compagnie
IoTrust	Odin Solutions SL
IRIS	Resonate Co-operative
Chiff (Keyn 2.0)	Chiff B.V. (Keyn BV)

NGI_Trust projects presentations (2/2)

Project	Third party
MedIAM	Fabien Imbault
MidScale	Evolveum
MW4ALL 2.0	Least Authority
PaE Consent Gateway	Trinity College Dublin
PRIMA	Cognitive Innovations
PY - 2.0	Panga
Solid4DS	STARTIN'BLOX
TOTEM	Feron Technologies P.C. (FERON)
TruVeLedger	RISE Research Institutes of Sweden AB

Deepfake

Sentinel

© Sergei Zjuganov

Protecting Democracies Against the Threats of Deepfakes and Information Warfare

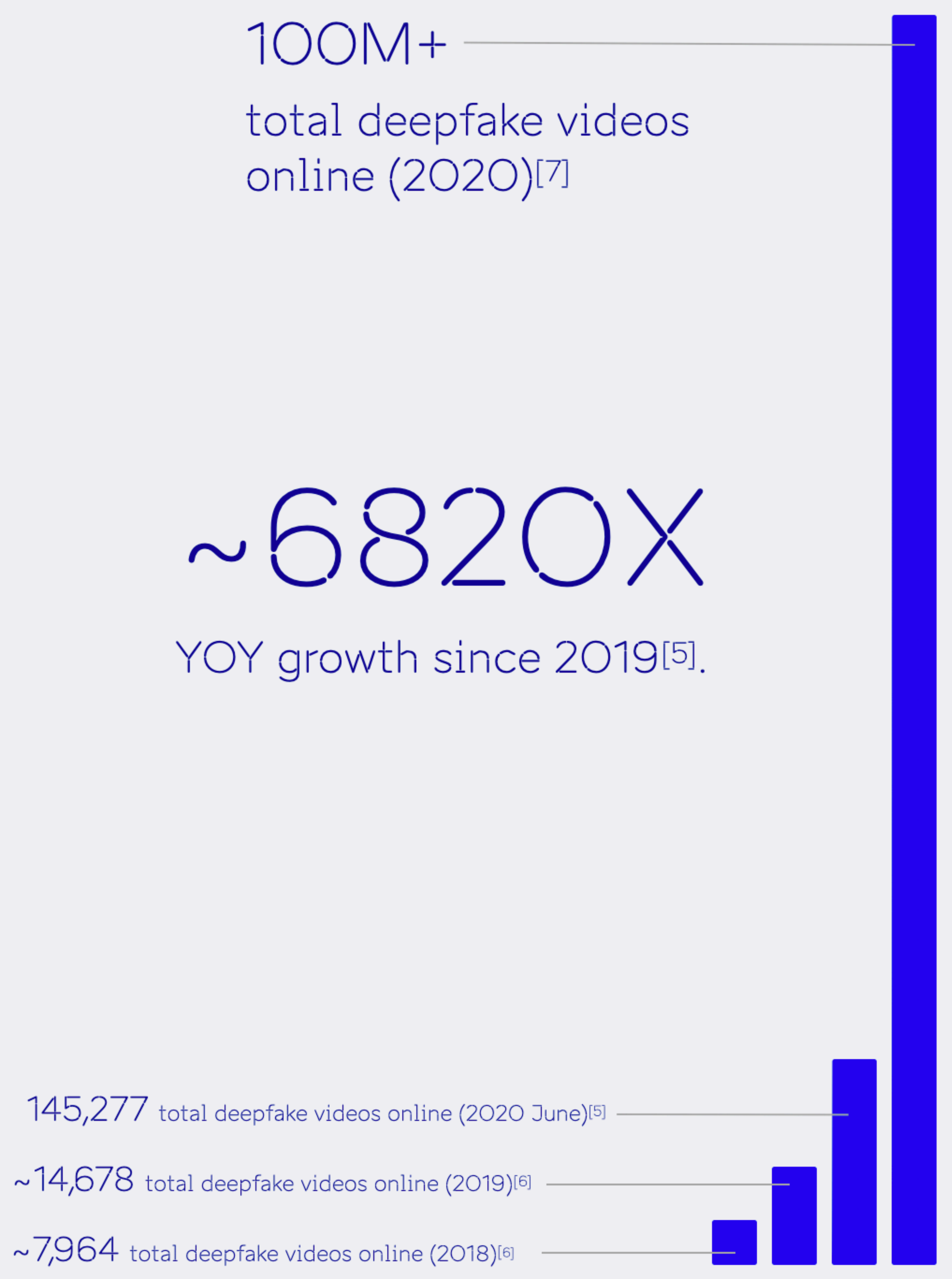
Henry Rõigas
Chief Strategy Officer

SENTINEL

FOR NONPUBLIC USE ONLY

Challenges addressed

- AI-enabled disinformation (deepfakes): a growing threat to democracy
- Detection tools for deepfakes not available to the public
- Private citizens, journalists, public officials, researchers etc. need to make informed decisions



100M+ total deepfake videos online (2020)[7]

~6820X YOY growth since 2019[5].

145,277 total deepfake videos online (2020 June)[5]

~14,678 total deepfake videos online (2019)[6]

~7,964 total deepfake videos online (2018)[6]

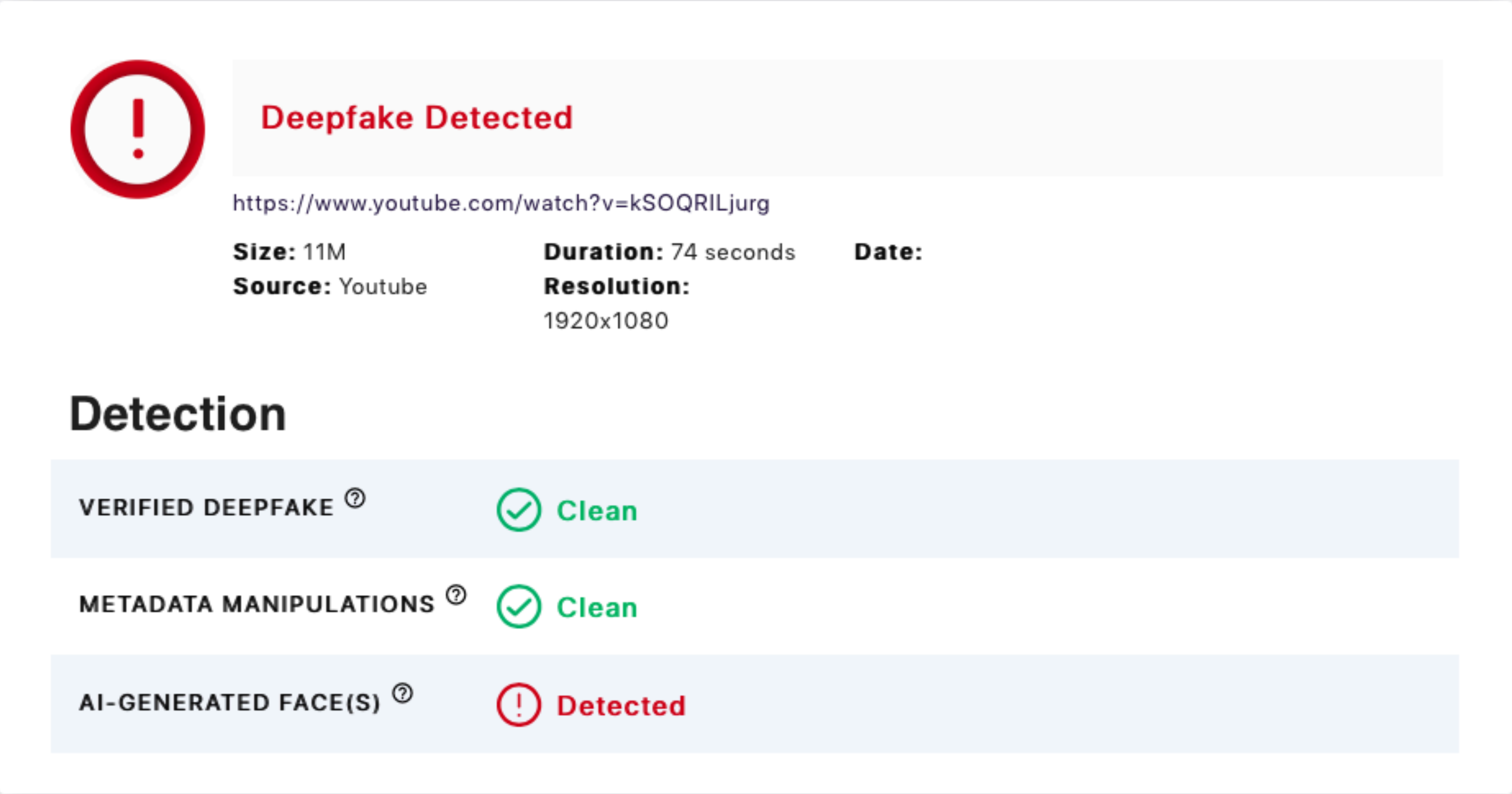
Results expected

Society:

- A publicly available, easy-to-use, free deepfake detection platform
- Power to the individuals: enhance media literacy etc.
- Submit video via webpage and receive easy-to-understand verification and analysis

Sentinel:

- Improve backend (e.g. detection accuracy and speed)
- Develop suitable UI for public
- Basis for broader user adoption, testing, publicity



Deepfake Detected

https://www.youtube.com/watch?v=kSOQRILjurg

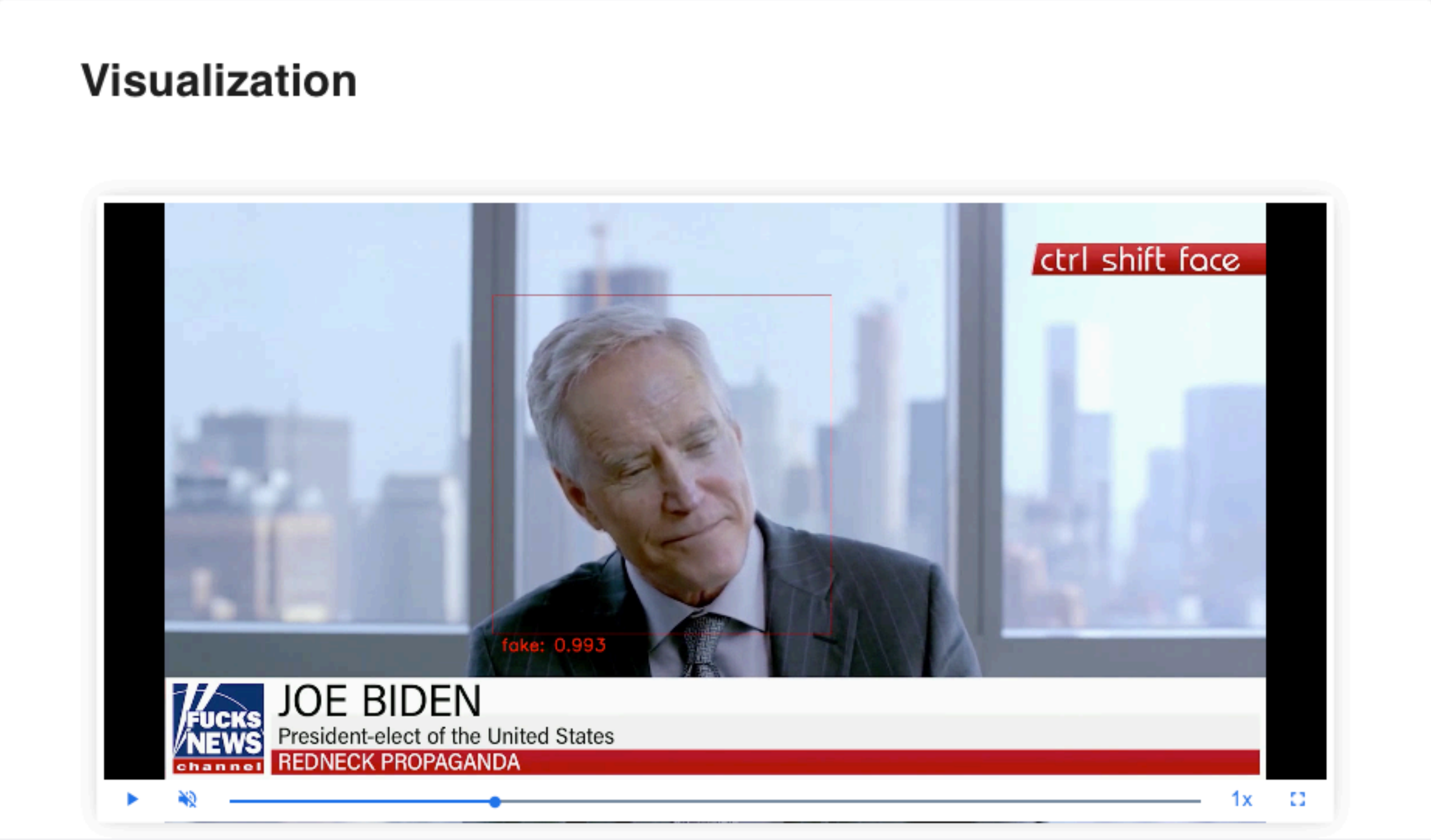
Size: 11M
Source: Youtube

Duration: 74 seconds
Resolution: 1920x1080

Date:

Detection

VERIFIED DEEPFAKE ⓘ	✓ Clean
METADATA MANIPULATIONS ⓘ	✓ Clean
AI-GENERATED FACE(S) ⓘ	! Detected



Visualization

FOR NONPUBLIC USE ONLY

SENTINEL

Protecting Democracies Against the Threats of Deepfakes and Information Warfare

Thank you!

Henry Rõigas
Chief Strategy Officer
Sentinel
henry@thesentinel.ai

© Sergei Zjuganov

FOR NONPUBLIC USE ONLY

AnonymAI

CELI

19 November 2020

AnonymAI
Welcome to NGI_Trust webinar

Andrea Bolioli, Roberta Lanzi, Milad Botros, Alessio Bosca

CELI LANGUAGE TECHNOLOGY

A company of H-FARM

AnonymAI: Legal Compliant Text and Voice Anonymization through Artificial Intelligence

Aim: Developing a legal compliant anonymization service that includes the automatic anonymization of documents and voice transcriptions, and providing guidelines and checklists to support the regulatory and anonymization processes.

Use cases:
1) anonymization of evaluation reports of customer and employee experience
2) anonymization of linguistic resources created for research or business purposes

Supported languages: English, Italian

Duration: 9 months from August 2020 to April 2021

Partners:

CELI (Coordinator): an Italian company based in Turin, specialized in the field of AI and Language Technology.

ICT Legal Consulting: an international law firm based in Milan, specialized in Privacy, Data Protection/Security and Intellectual Property Law in the ICT field.

AnonymAI

Challenges addressed:

- retaining the benefits of using data (and therefore maintaining data-driven procedures), mitigating the privacy risks that come with the processing and storing of personal data through anonymization
- conducting anonymization (which itself is data processing) in compliance with privacy regulations and in a correct way (involving all personal data, including special categories)

Results expected:

- automatic anonymization service that can be customized based on domains and use-cases (business or research relevant information are not lost, while privacy is guaranteed)
- guidelines and checklists for the correct use of the anonymization strategy and tool (for future sustainability and scalability of the project)

TORINO
Via S. Quintino, 31
10121 Torino
+39 011 5627115
info@celi.it

MILANO
Via Giosuè Borsi, 9
20143 Milano

CELI LANGUAGE TECHNOLOGY

A company of H-FARM

CASPER 2.0

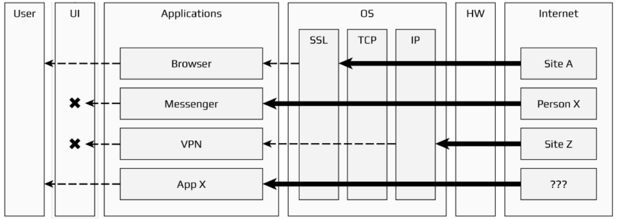
University of Belgrade – School of electrical engineering

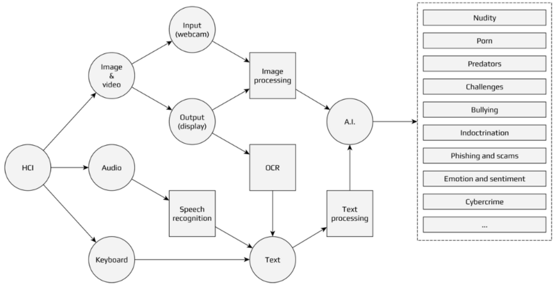
CASPER

NGI TRUST

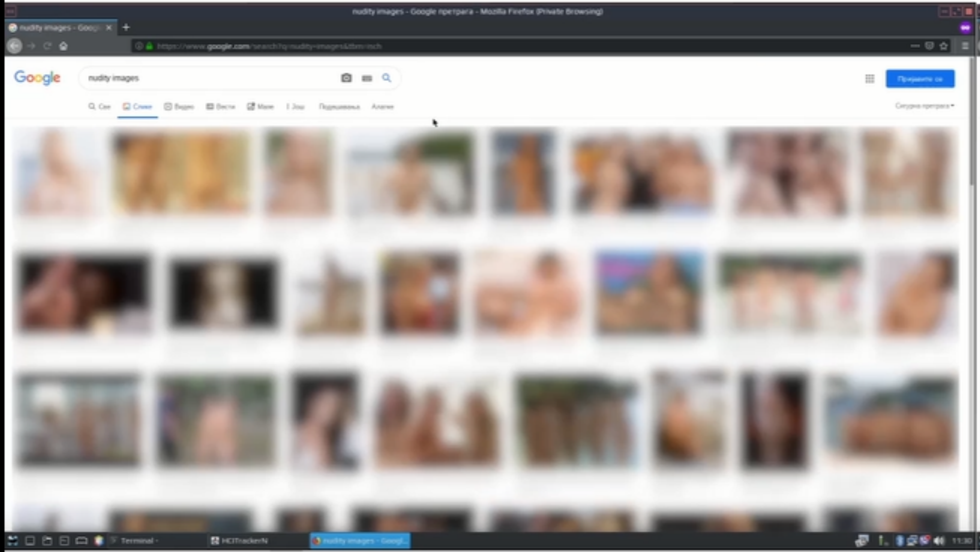
This project has received funding from the European Union's Horizon 2020 research and innovation programme under the NGI_TRUST grant agreement no 825618.

- In shell, it is an A.I. based ghost
- Using A.I. at the HCI level to protect children
- Modular architecture
- Can analyze image/video/audio/text content
- Different types of threats can be detected

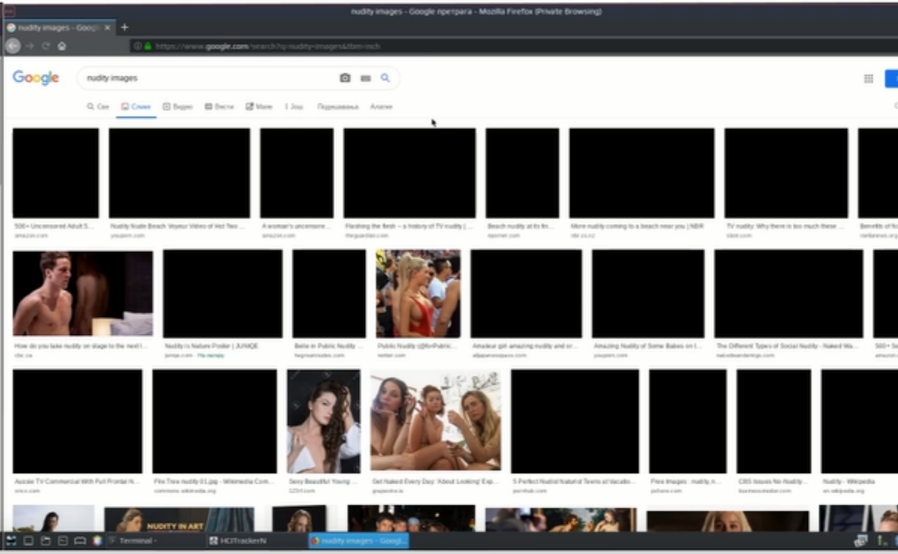




ORIGINAL


nudity images - Google претрага - Mozilla Firefox (Private Browsing)
Google
nudity images

CASPER


nudity images - Google претрага - Mozilla Firefox (Private Browsing)
Google
nudity images

0:00:18

Cassiopeia

IT-Av - Instituto de Telecomunicações - Aveiro (affiliated with University of Aveiro)

Main research actions

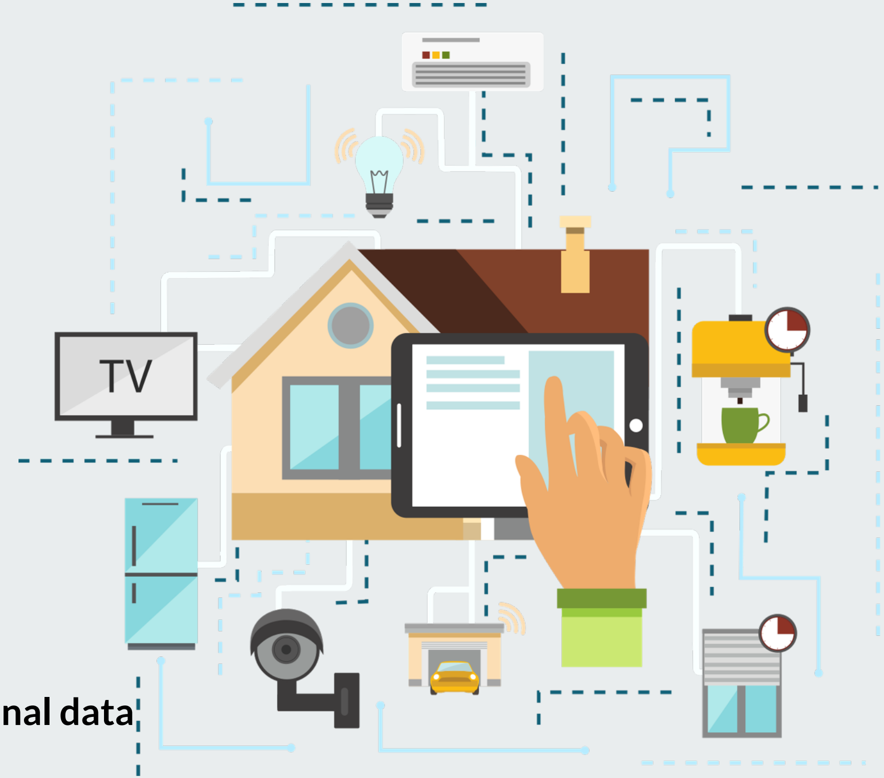
How **open-standard/open-source technologies** can be used to create usable and transparent architectures

How device owners can **selectively** collect, share and retain data from users

How to delegate the control of device features to the users from whom data is being obtained

How to manage **consent receipts** for transparency and auditability of personal data

Airbnb Scenario



Host gives short-lived **degrees of access** to the guest

Selected data is shared, with the guests' consent

- users get consent receipts when **sharing personal data**

Host has **restricted view of the house** while the guest is renting

Data is deleted as consented and guest **receives deletion confirmation**

Parties **cannot repudiate** their actions

Image: macrovector

Expected Outcomes

An analysis of relevant **use-cases** and an architecture for trusted operations

A web based **proof-of-concept demonstrator** of an Airbnb scenario.

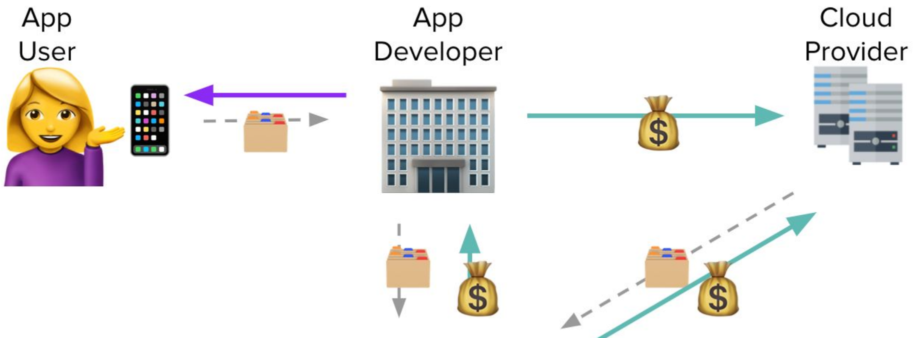
A **report** detailing challenges, innovations and future directions

Contributions of findings and software to **standards groups**

DAppNode

DAppNode Association

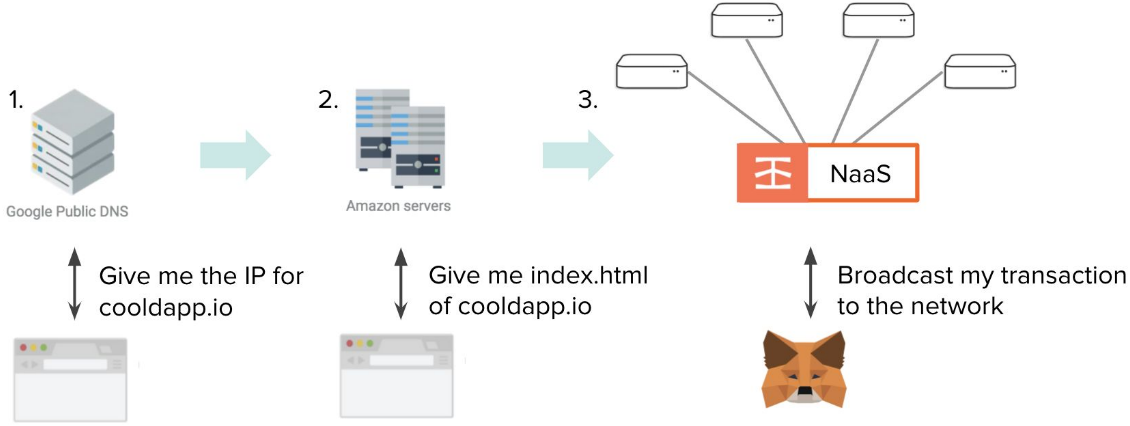
The Infrastructure problem: *Where* do DApps work?



Advertisers, Data Brokers, Insurers, Employers...

Web2.0

Web3.0



1. Give me the IP for cooldapp.io

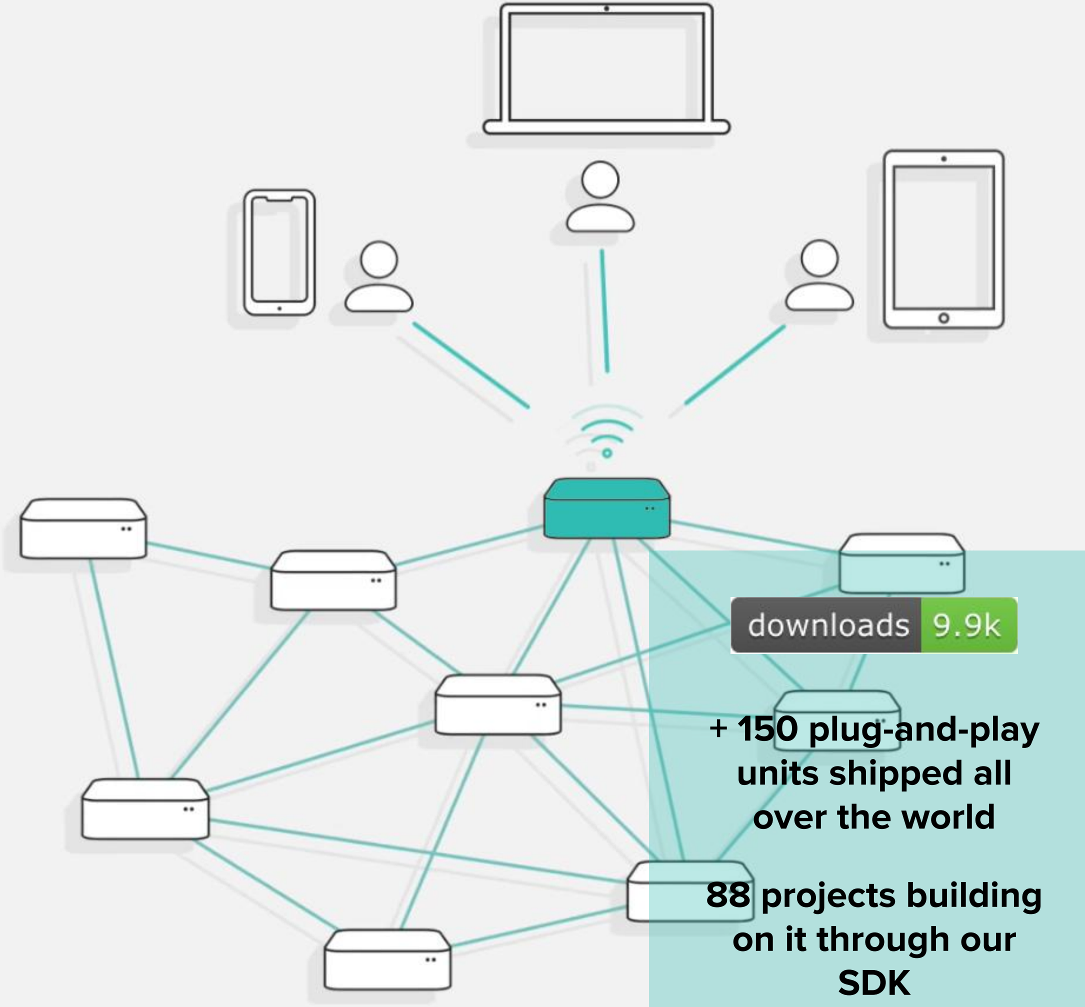
2. Give me index.html of cooldapp.io

3. Broadcast my transaction to the network

DAppNode

DAppNode’s goal is to create a layer of **decentralized hardware infrastructure.**

- Anyone can install the OSS or buy a plug-and-play device
- Users host dapps in an uncensorable, private and decentralized way
- Users provide distributed access to nodes and dapps to others
- DApps don’t have to rely on centralized services and can pass the $ value to nodes/hosters
- **DAppNodes are federated, redundant, and failure resistant.**



downloads 9.9k

+ 150 plug-and-play units shipped all over the world

88 projects building on it through our SDK

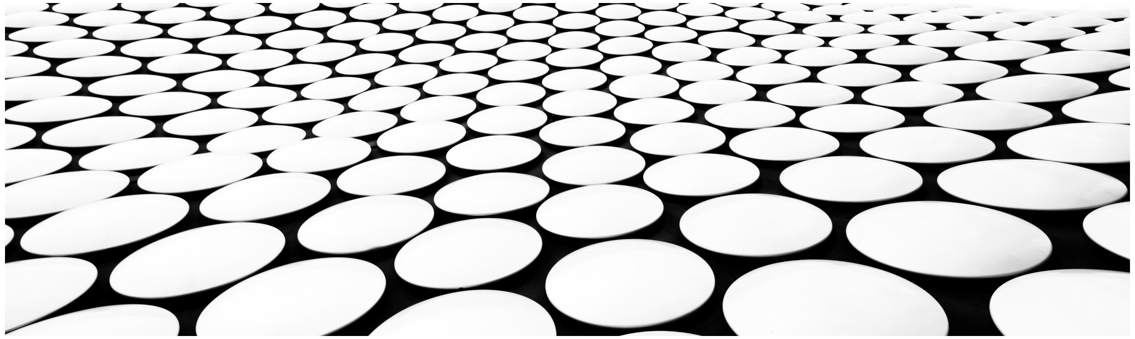
FAIR-AI 2.0

The University of Cambridge

UNIVERSITY OF CAMBRIDGE

NGI

Horizon 2020 Programme
DG CNECT
Next-generation Internet



FAIR – ARTIFICIAL INTELLIGENCE

DR. AHMED IZZIDIEN

DR. DAVID STILLWELL.

“CAN AN AI INTERPRET FAIRNESS?”

- A common feature of human-centric AI design is the necessity of using humans to assess where **fundamental rights and responsibilities** are in a situation.
- From which, rules are programmed into an AI to avoid potential legal problems or harms (Bauer, 2020).
- We argue, that this bottle-necks AI, and forgoes the power afforded by this technology.
- We put forward the project that an AI ought to be able to perceive fairness, so that it can make **fundamental rights and responsibilities** assessments by itself.
- Such a perception would allow the AI to use its power to become truly human-centric <u>by default.</u>

OUTCOME

Software to allow an AI to make a universally accepted assessment of sentences (*e.g. contract clauses*), answering:

<u>*Is this fair?*</u>

An Academic Peer-Reviewed Paper – Accepted and currently *in review*

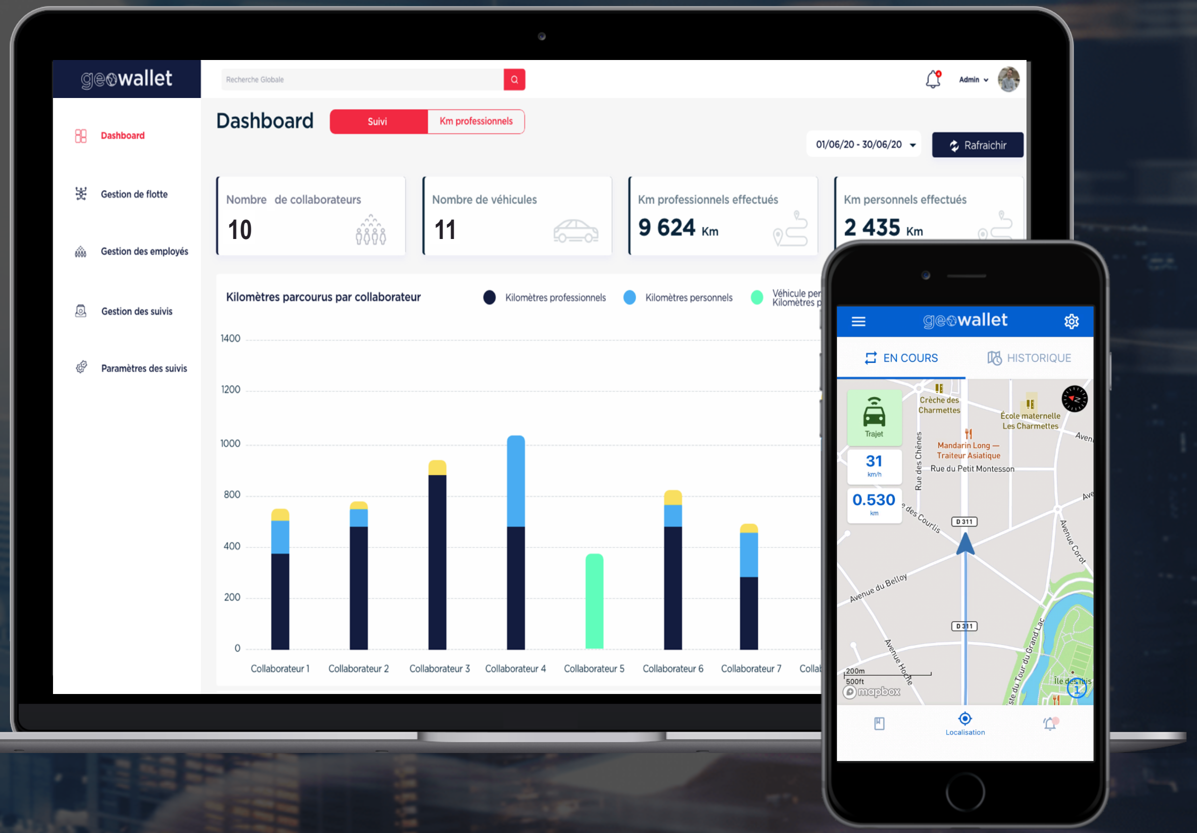
GeoWallet

Blocs et Compagnie

NGI TRUST

geowallet

Geolocation / Trust / Privacy



Nombre de collaborateurs 10

Nombre de véhicules 11

Km professionnels effectués 9 624 Km

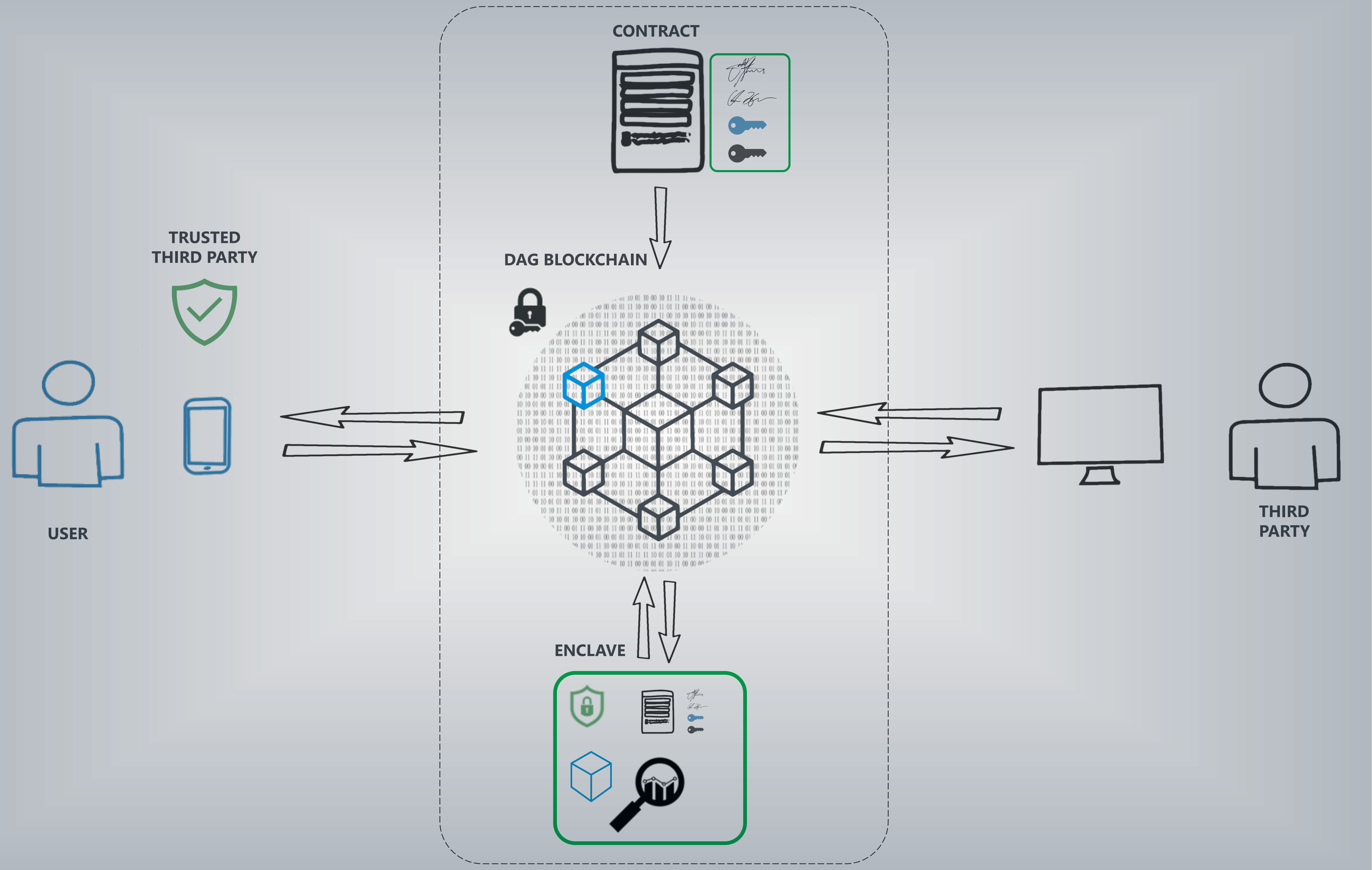
Km personnels effectués 2 435 Km

31 km/h

0.530 km

✉ nicolas.reffe@blocsetcie.com

www.blocsetcie.com/geowallet



OBJECTIVES

Validate and scale Data Trust & Privacy Platform architecture

- Enclaves (TEE) performances - queries complexity and volume
- Front end performances - asynchronous DAG Blockchain node
- Queries on NoSQL databases - fully anonymized data
- Front end pre-treatment - relieve enclave workload
- Define and implement penetration tests
- Customer Tests

EXPECTED RESULTS

Mobility Data management platform - Trust & Privacy

- Scalable
- Security Reviewed independent Third Party
- Field tested
- Q2 2020

IoTrust

Odin Solutions SL

Odin Solutions SL (ODINS) - Spain	OdinS
Digital Worx GmbH (DW) - Germany	digital worx

IoTrust – NGSITRUST Webinar

Rafael Marin Perez - ODINS

Challenge & Objectives

- **Main Challenge:** a **trustworthy solution to setup and maintain IoT networks** based on the development of *novel technologies (Bootstrapping, Peer-to-Peer and Distributed Ledger)* in order to **provide secure initialization of IoT devices, vulnerabilities detections and software patching/reprogramming.**

- **[O1]** To increase the user trust and application of secure IoT networks in worldwide sectors like Smart Cities, Industry 4.0, etc.
- **[O2]** To achieve trustworthy IoT networks and keep decentralized Internet infrastructure.
- **[O3]** To validate the IoTrust minimum viable product (MVP) using laboratory testbed and real-world pilots.
- **[O4]** To perform dissemination activities and joint exploitation plan.

OdinS

digital worx

Results & Deliverables

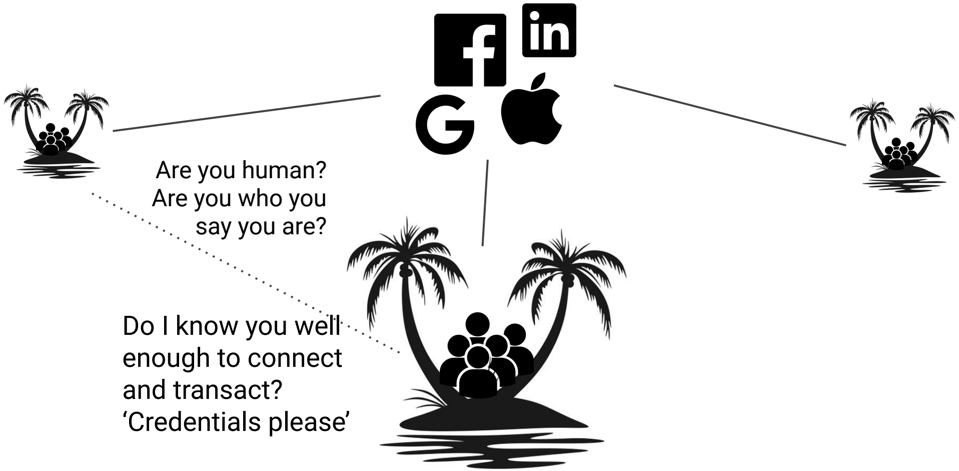
- **Deliverables List**

D1. IoTrust Architecture Design	- January 2021
D2. Open Standards-based Development	- March 2021
D3. MVP Testbed & Pilot Validation	- April 2021
D4. Dissemination and Exploitation	- April 2021

- **Two real-world pilots:**
  - Smart City of Murcia (Spain) - ODINS
  - Application in Industry 4.0 (Germany) - DW

IRIS

Resonate Co-operative

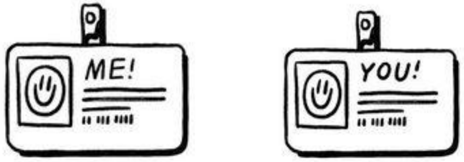


Are you human?
Are you who you say you are?

Do I know you well enough to connect and transact?
'Credentials please'

The Problem: Islands of Community Identity

The Solution: Community Credentials



Chiff (Keyn 2.0)

Chiff BV (Keyn BV)

Chiff

- Making it easier to be secure online
- Login with your smartphone as a hybrid authenticator
  - No masterpassword
  - End-to-end encrypted
  - Privacy-by-design
  - Independent of underlying authentication method (passwords / OTP / WebAuthn)

NGI_Trust project

- Solution available for B2C and B2B market
- Open sourcing the core of Chiff
- Bridging the gap to WebAuthentication
- Test the solution with five pilot companies
- Design a scalable solution for commercialization

Chiff

https://chiff.app
wouter@chiff.app

MedIAM

Fabien Imbault

MedIAM: the problem we’re facing

Healthcare suffers 2-3X more cyberattacks than the average amount for other industries, because the data has more value for hackers.

Cyber regulations such as the EU Cybersecurity Act provide mandatory requirements to protect sensitive information and systems. Beyond traditional clinical systems of electronic health records (EHR), it remains really difficult to extend that line of requirements to connected devices people carry around as part of their treatments. If those medical devices aren’t properly secured, people may unknowingly be broadcasting their health status, as well as many other personal sensitive data, everywhere they go. Or even be directly harmed by hacked devices. Existing protocols available for IoT are unable to meet the complete requirements from regulators.

MedIAM: our expected results

We’re working on the IAM (identity and access management) of machines/things

- Website dedicated to the project (for dissemination)
- Opensource prototype(s)
  - Review/adapt IAM protocols and metadata (e.g. SBOM) to the IoT/edge/cloud
  - Handle the lifecycle of machine identities and state
  - Use case : remote device update to apply a security patch
  - Document best practices in line with EU cybersecurity act
- Demonstrations within the healthcare sector and the IAM professionals (IETF/DIF)
- Build a new startup (acert.io)

Feel free to reach out if interested to know more / Contact : @fimbault

MidScale

Evolveum

midScale: Challenge addressed

- MidPoint: open source identity management and governance platform
- Increase midPoint scalability by an order of magnitude
  - Routinely manage: ~1 million identities
  - Possible deployments: ~10 million identities
- Identify scalability and performance obstacles
  - Performance testing environment
- Overcome scaling obstacles
  - Data store: data model, indexing, partitioning, etc.
  - Clustering / multithreading
  - Stability: thread safety, tooling
  - Visibility & usability: UX, GUI performance, diagnostics

midScale: Expected results

- We need seamless: multi-threading, clustering, multi-node tasks
- MidPoint supports clustering, but improvements are needed
  - Better and more reliable per-node multi-threading
  - Smarter multi-node tasks (load distribution)
  - Cluster auto-scaling
  - Misc multi-node improvements (e.g. thresholds)
- Stability in large deployments
  - We are observing instability under high load, thread safety suspected
  - Focus: Prism – midPoint data representation layer
- Visibility and usability
  - Diagnostics: needed for both development and deployment
- GUI performance
  - UX for administrators to handle massive data sets

midScale: Project Resources

- Project home page

https://docs.evolveum.com/midpoint/midscale/

- Solution Architecture (work in progress)

https://docs.evolveum.com/midpoint/midscale/architecture/

- MidPoint source code

https://github.com/Evolveum/midpoint

- Evolveum Blog

https://evolveum.com/blog/

MW4ALL 2.0

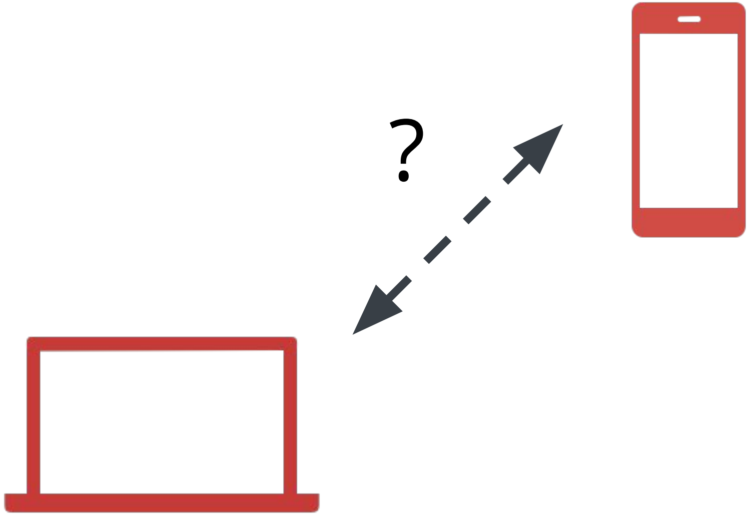
Least Authority

Least Authority
PRIVACY MATTERS

consulting services / open source products
with a focus on security / privacy

The challenge: File transfer is hard

- Not easy to use
- Speed issues
- File size limitations
- Security concerns
- Privacy concerns
- Receiver needs the same app



MW4ALL

With Magic Wormhole, transfer (large) files easily, fast and securely

- Project phase 1 (completed):
  - Technical scaling assessment
  - User research
  - Market exploration
- Phase 2 (now - July 2021):
  - Iterative testing
  - MVP development
  - Go-to-market strategy

Any feedback or ideas? contactus@leastauthority.com

PaE Consent Gateway

Trinity College Dublin

NGI TRUST

Privacy-as-Expected: Consent Gateway

This proposal will develop an end-to-end, user-centric, comprehensive, open source solution to managing Consent for Personal Data. We will deliver a concept we call Privacy-As-Expected (PaE) by creating, implementing and demonstrating a novel system to make online privacy practices accountable.

Whenever a User accepts a Privacy Notice and starts sharing personal data, they will receive a cryptographic Consent Receipt (based on a secure architecture [2] and open standards [3]) which, with non-repudiation and unforgeability proves, at any time, who-what-how any conditions were accepted.

Trinity College Dublin
The University of Dublin

Harshvardhan J. Pandit, David Lewis
ADAPT Centre, Trinity College Dublin
https://adaptcentre.ie/
pandith@tcd.ie

OPEN CONSENT

Mark Lizar, Salvatore D'Agostino
Open Consent Group
mark@openconsent.com

BIRMINGHAM CITY
University

Vitor Jesus
http://www.trustless-team.com
vitor.jesus@bcu.ac.uk

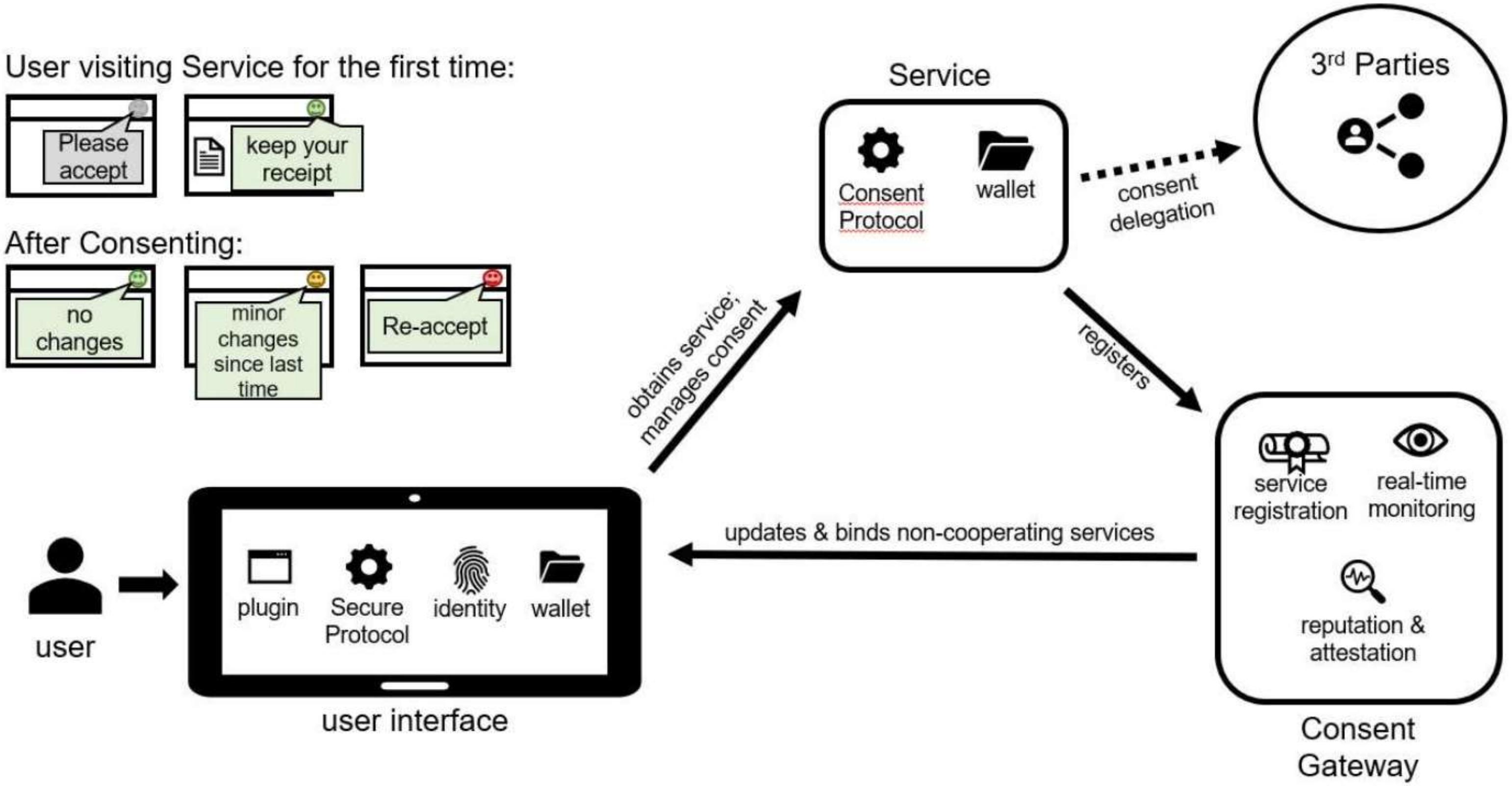
The key deliverables are open software, a public demonstrator, real-world trials and publications.

results will be open source

with a public demonstrator of receipts

results will be contributed to Standards and Community (notably Kantara Initiative)

- ✓ **organisations**: low friction demonstration of compliance
- ✓ **users**: keep data usage accountable and transparent
- ✓ **regulators**: naturally enforce compliance
- ✓ **ecosystem**: enforces good practices



PRIMA

Cognitive Innovations

PRIMA – PRIvacy preserving IoT data analysis using federated MAchine learning protocol

Cogninn

Cognitive Innovations Private Company

Kifisias Av. 125-127, 11524

Athens, Greece

http://cogninn.com/

Challenge addressed

1. **Future Internet** will be able to integrate the ML knowledge from the surrounding environment.
2. **Distributed ML** will be able to train models both to the IoT devices and edge servers.
3. **PRIMA protocol** will specify all the required distributed rules among the IoT and edge computing infrastructures to train ML in a distributed fashion as provided by federated learning.

Results expected

- A federated learning specification for IoT devices, where the edge intelligence with the IoT are integrated in an efficient manner.
- Constrained and non-constrained devices will be considered for the protocol specification and implementation.
- PRIMA will target advanced IoT use cases such as Augmented Reality (AR) services in future smart cities, where the users will be able to integrate knowledge from the surrounding city environment.
- PRIMA will be tested to a Fed4Fire testbed and evaluated in terms of federated training and communication performance.

PY - 2.0

Panga

PY

PY : Protect Yourself

NGI phase III launch

Panga

mydataball

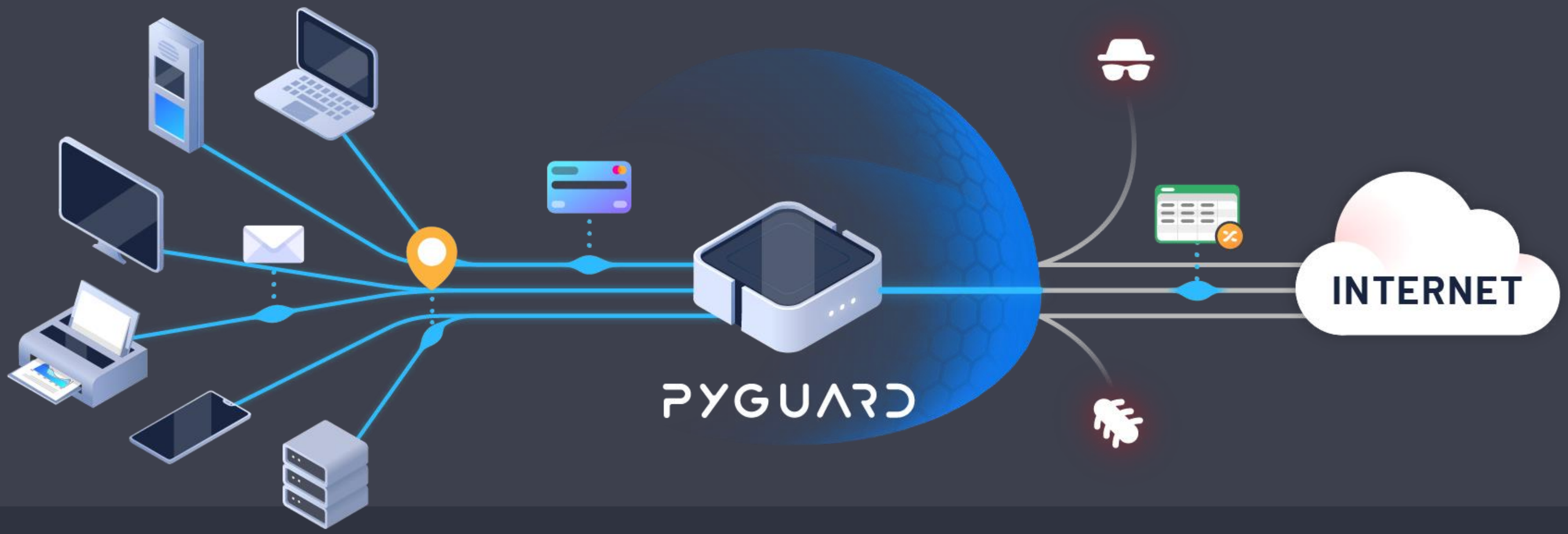
NGI TRUST

Challenges addressed

With the advent of the Internet, the « Big Techs » brought many « free » digital services to users. These services are of course not actually free : their business models relies on the exploitation of their users personal data, for example by providing targeted advertising.

Europe missed that data market, and must now prevent the massive data leak of its citizens and companies to GAFAM and BATX.

Project PY 2.0 : Protect Yourself



The goal of the PY : Protect Yourself project is to protect connected devices and the personal data they generate, while raising user awareness about digital risks.

A hardware platform to process and store users data locally, insuring data sovereignty

A web platform, to occasionally manage or supervise one's data privacy, connections and devices

A browser plugin to make PY more user-friendly and raise daily awareness

PYGUARD

Reclaim your privacy

www.pyguard.fr

Solid4DS

STARTIN’BLOX

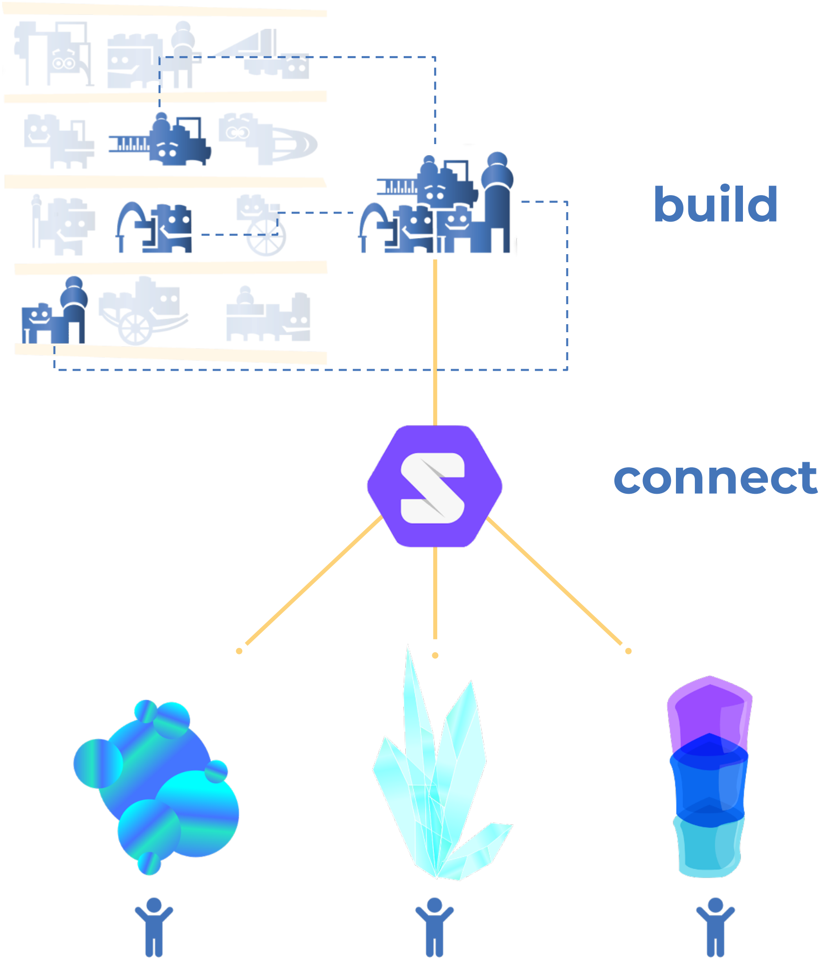
STARTIN' BLOX

SOLID4DS PRESENTATION

November 2020

Build apps faster, connect with the world

Powered by Happy Dev



Startin'blox : The Solid CMS

Startin'Blox is the first CMS leveraging Solid technology. It empowers organizations to swiftly create a new breed of web and mobile apps via its components suite.

One can easily assemble them to create tailor-made applications and harness the power of Solid to onboard numerous users effortlessly.

Startin'blox enables its users to reach far broader audiences by:

- offering a richer user experience from day one by sourcing data from partners and Solid peers
- pushing data beyond the frontiers of their applications.

Solid user dashboard

Developing a pilot user dashboard

1. User controls who can access his/her data
2. User controls what apps can use its data
3. ID authentication key verification
4. Protection of features against malicious plugins
5. Trusted server-to-server exchanges

TOTEM

Feron Technologies P.C. (FERON)

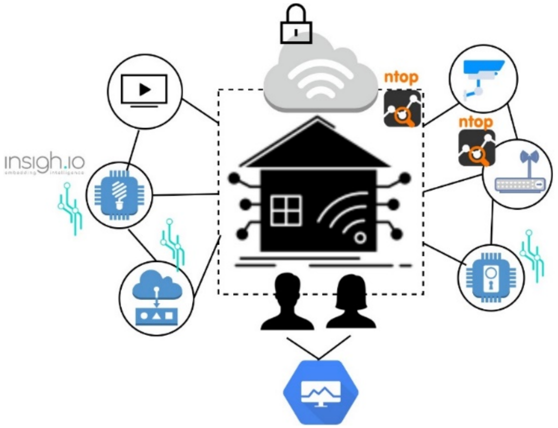
TOTEM

Trust-Enhancing TechnOlogies CommodiTization for IncrEasing Security Awareness in Connected HoMes

NGI TRUST

feron TECHNOLOGIES

ntop



Welcome to NGI_Trust webinar, 19/11/2020

FERON TECHNOLOGIES & ntop

Dr. Antonis Gotsis

antonis.Gotsis@feron-tech.com

Setting the scene

- □ **A Connected Home with many heterogeneous end-points for**
  - □ connectivity/networking
  - □ media/entertainment
  - □ physical security
  - □ energy monitoring
  - □ healthcare/fitness/wellness
  - □ tele-working

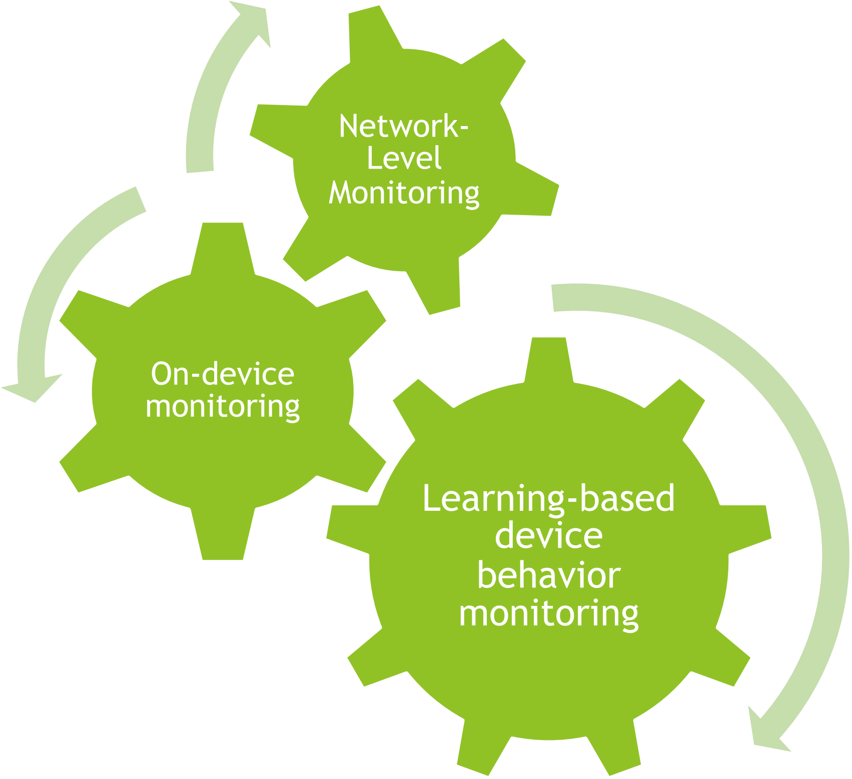
- □ **The Challenge:** *As more and more connected things are incorporated in our digital environment, there is a need to develop new robust, open, and easy to use tools to help users increase trust and achieve greater control over fleets of connected home end-points.*

Today's Landscape

- ✓ Conventional security approaches relying on firewall rules blocking unwanted traffic from external networks.
- ✓ Low-end end-points lacking security-by-design features and having no way to warn about potential misbehavior
- ✓ Various chip manufacturers, device makers, and solution integrators are involved in the creation of a commercial IoT solution, each one bringing his own security design
- ✓ By shifting functionality to the edge, we can't expect from the end user to have the skills to detect, prevent or remove potential security threats.

Our Value Proposition:
Simplify, automate and eventually make accessible to non-expert users all the necessary tools required for proper control of end-points and early identification of potential malicious operation.

Approach & Expected Results



Main Technology Innovations

- ✓ Bringing and extending our in-house platforms (ntopng, insigh.io)
- ✓ Systematically profiling of various connected home devices traffic (IoT protocols)
- ✓ Automating the creation of a set of simple policies, with input provided by network sniffing
- ✓ Empowering the end-points with advanced monitoring capabilities (CPU, RAM, temperature) inferring potential breaches
- ✓ Collecting different kind of information related to connected home devices in a common back-end
- ✓ Applying statistical analysis to detect suspicious behavior and raise warnings

Main Outcomes

- ❑ **End-User Tools :** Web-based UI, Dashboards, Alerts
- ❑ **Community Contributions :** Open-Source Tools & Datasets
- ❑ **Demonstration:** Smart-home testing environment

TruVeLedger

RISE Research Institutes of Sweden AB

TruVeLedger (Trusted Platform for Disruptive Vehicular Ad Hoc Networks using Distributed Ledger Technology)

Background and Challenges

- Trusted communication important for Vehicular Ad Hoc Network (VANET) applications (trusted source of sensor data, etc)
  - Focus on data collection for accident analysis and prevention
- Decentralised operation desireable
  - Large data volumes, so processing at edge beneficial
  - Potentially sensitive data, so don’t want all data stored centrally
- Blockchains/Distributed Ledger Technology has potential to provide trust
  - Both VANETs and DLTs are inherently decentralized, so good fit, but…
  - Current DLT solutions not optimal in terms of robustness for scenarios with network disruptions/partitioning, or where you want to keep data local.

FUNDED BY NGI

Activities and Expected Results

- Identification of use case and candidate technologies for using in framework
  - More detailed scenario definition, extended survey of existing DLT technologies
- DLT development and framework definition
  - Extend existing DLT architecture to be able to handle the characteristics of VANET operation
  - Define communication protocols (based on existing VANET protocols) that are needed to exchange data
- Conceptual implementation of framework in simulator
- System evaluation and testing

FUNDED BY NGI

More information/contact us

- Project coordinator : Mr Alasdair Reid @ EFIS Centre - www.efiscentre.eu
- Email : NGI-Trust-support@lists.geant.org
- Twitter: @NgiTrust
- NGI_TRUST wiki : https://wiki.geant.org/display/NGITrust
- NGI.eu website : https://www.ngi.eu/about/

The NGI_TRUST project has received funding from
the European Union's Horizon 2020 Research and
Innovation Programme under Grant Agreement No 825618

NGI TRUST