decode

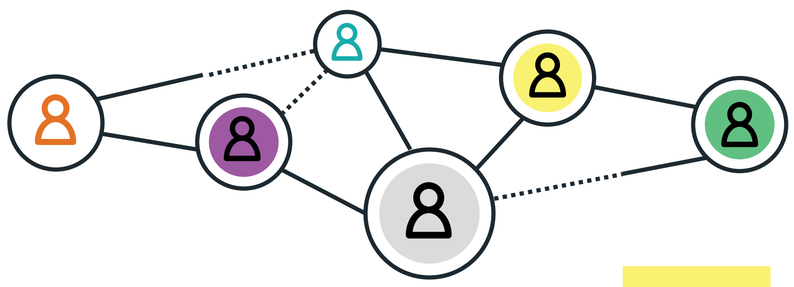
Giving people control of their personal data

DECODE (DEcentralised Citizen-owned Data Ecosystems) will develop technology that puts people in control of their personal data, giving them the ability to decide how it is shared.

In DECODE, entitlements attached to private data, including from Internet of Things devices, will be searchable in the public domain but will grant access only to those parties that have the entitlement to access it.

Architectural Principles

- Free and open source
- Modularity and interoperability
- Reuse don't invent
- Decentralisation and federation
- Privacy by design
- User friendliness



Tech Foundations

- Decentralisation of trust
- A distributed ledger
- Zero knowledge proofs
- Attribute Based Credentials
- Cryptographically verifiable entitlements
- A "Smart Rules" language to express governance of participants' data
- A highly verifiable and controlled execution environment

Attribute Verification Using ABCs

Identity within DECODE inverts the current world position whereby participants know little about the operators of the services they are registered with but the services know everything about the identity of the participants.

Attribute Based Credentials (ABCs) allow people to prove properties (aka attributes) about themselves in a secure and privacy friendly fashion. For example, they allow someone to prove that they are over 18 without revealing their full identity.

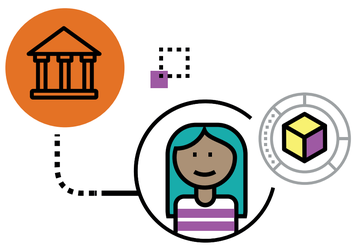
ABCs are based on foundational work by David Chaum in the 1980s, followed by research from Jan Camenisch and others at IBM Research. Practical implementations were developed by the IRMA project of Radboud University.

In DECODE, ABCs will be used to enable people to authenticate certain attributes without fully revealing them, and as a result remain anonymous but trusted.

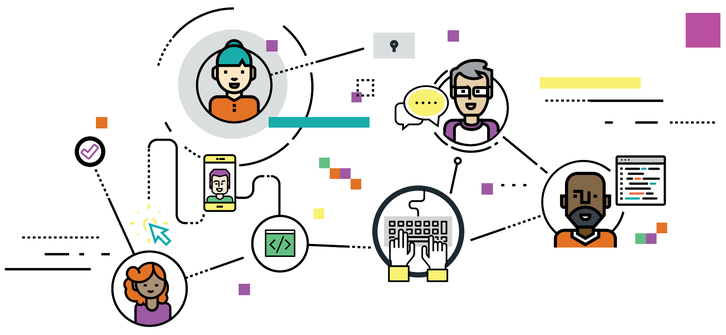
"Smart Rules" Language

The main way to communicate with a DECODE node and operate its functions is via a "Smart Rule" language, rather than an API. All read and write operations affecting entitlements and accessing attributes can be expressed in this language, which we will design and develop to become a robust open standard for authorisation around personal data.

We intend to run the code in a controlled manner. Computer language and cryptography are at the core of many developments done in the field of distributed computing and are often their weak link, because people can make numerous mistakes when writing smart contracts that hide bugs and unpredicted behaviour. We want to limit this condition by constraining the operations that the language can execute in a sandboxed environment.



The DECODE technology has four key principles



Secure Operating System

The DECODE OS enables easy development and deployment of distributed applications, without any constraint on the blockchain stack being used. It is a GNU+Linux distribution geared towards security and low consumption, with modular UNIX components. It is capable of establishing automatically a peer-to-peer network among other running nodes, offering micro-services to the inside and outside.

The same software can be run on a RaspberryPI class computer, a cloud virtual machine or a laptop without any change to the underlying software.

Additional build features include a Linux kernel patched for extra security (grsec public fork), a snapshot capable filesystem (btrfs), open source hardware (olimex), a static toolchain and alternative privilege escalation tools (musl-libc and sup) into a compact OS requiring less than 64MB of RAM to run.

It uses Tor "hidden service directories" networking technology for anonymity, privacy and resilience of connectivity. There is a system to propagate automatic signed updates and a "Simple Development Kit" with instructions for people to install, modify and adapt.

Distributed Ledger

As part of the mission of DECODE, we present a distributed ledger implementation Chainspace (http://chainspace.io), which provides a highly scalable, Byzantine fault tolerant ledger that separates transaction *execution* from *verification*. In implementation it provides for this in an entirely technology neutral and decoupled manner.

Thanks to advances in modern cryptography, it is possible to ensure that operations were correctly performed on a ledger, without divulging private user data - a family of techniques known as zero-knowledge

Within DECODE, the use of a distributed ledger provides for two characteristics, integrity and availability. In short a participant can perform an action (transaction) and record a verifiable proof of that transaction which has no relation to the data used within the transaction. The resulting system has a high degree of integrity because the ledger provides a Byzantine fault tolerant replication mechanism, and a high degree of availability because it is decentralised and therefore not under the control of a single party or system.

DECODE applications

- **Participatory democracy through anonymous but authenticated signing of petitions**
- **Collecting, managing and anonymously sharing citizen-sensed data with others**
- **Peer to peer ID and reputation verification**
- **Controllable sharing of personal data into a digital commons**

Ajuntament de Barcelona · City of Amsterdam · ARDUINO · cnrs · dyne.org · eurecat Centre Tecnològic de Catalunya · nesta · Nexa Center for Internet & Society Politecnico di Torino · PI.lab Privacy & Identity Lab · thingful · ThoughtWorks · UOC R&I IN3 Internet Interdisciplinary Institute · UCL · waag society

DECODE is funded by the European Union's Horizon 2020 Programme, under grant agreement number 732546.