

Blockchain on the Spanish Public Sector

What's going on?

Tomás García-Merás
Capote



Blockchain on Spanish Public Sector



What's going on?

We've talked the talk, but... Will we walk the walk?

On eGovernment:

- Creating the needed software infrastructure.
- Developing the much needed formal regulation.
- Starting with real projects.

For helping the private sector:

- Several research project grants and subsidies.
- Developing a SME-friendly juridical framework.



Blockchain on Spanish eGovernment



Not much, really

The target is to evolve the current eIDAS identity and electronic signature schemes to do also Blockchain, fully integrating all technologies



- Use eIDAS authorities for the Blockchain identity.
 - Reuse the known PKI model: Certification Authorities, Registry Authorities, Validation Authorities, Timestamp Authorities...
 - Explore the remote onboarding model for eIDAS registry.
- Use eIDAS key pairs not just for authentication or electronic signatures, but also for Blockchain transactions signing.
 - Private keys are not *bearer bonds*, not even in Blockchain.
 - Treat the usual Blockchain transaction signing as a qualified signature.
- Boost the use of eIDAS-compliant cloud-based keys and certificates.
 - Avoid the nightmare of key keeping.



Blockchain Software Infrastructure



Blockchain-enabled software developed by the Central Administration as Open Source (EUPLv1.1)

The Central Administration will begin shortly evolving the current electronic signature software for compatibility with elliptic curve cryptography, as a first step towards Blockchain

- There is a large collection of open source (mainly EUPL licensed) high quality software for electronic signatures, developed in-house by the Spanish Central Administration which is used by almost all Spanish public administration (from the central government to the smaller city hall) which will soon begin his adaptation to support elliptic curve cryptography:
 - “@firma” for validating electronic signatures and certificates.
 - “Cliente @firma” and “AutoFirma” for performing electronic signatures with local certificates and keys.
 - “FIRe” for performing electronic signatures with cloud-based certificates and keys.
 - The Spanish national ID card: DNIE

Blockchain Legal Framework

The public sector really needs a juridical framework to rely on



The Central Administration will begin shortly evolving the current electronic signature software for compatibility with elliptic curve cryptography, as a first step towards Blockchain

- ◊◊ Spanish National Security Scheme
- ◊◊ Spanish National Interoperability Scheme and its Interoperability Technical Rules
- ◊◊ Spanish Central Administration Electronic Signature Policy (and its subordinate policies)

There is no support for elliptic curve cryptography, mandating the use of RSA keys, giving no room for Blockchain adoption

- ◊◊ Central Administration Policy for the Electronic Document (currently WIP)

By enforcing the use of hashes and cryptographic digests it paves the way to Blockchain adoption



Small regional projects

For eProcurement, distributed registries, popular vote, etc.



While the central government seems to be waiting for something, some small public administrations are starting using Blockchain on pilot projects

JUST A FEW EXAMPLES,
THERE ARE MANY OTHERS



Pushing Blockchain on the Private Sector from the Public Sector



Much more than giving money away

- ◻◻ By now, we just ~~wasting~~ spending money (Spanish and European) on funding Blockchain projects (mainly on the Smart Cities arena).
- ◻◻ We all love money, but it's clearly not enough:
 - ◻◻ Blockchain is expensive, mainly for SMEs.
 - ◻◻ As a SME, we cannot do Blockchain alone, we need a network.
 - ◻◻ And public networks (like Ethereum) are way too expensive.
 - ◻◻ As a SME, we don't want to let our business lay on a network where we have no voice or no right to vote.
 - ◻◻ Joining an existing Blockchain network consortium is not always the way to go.

Pushing Blockchain on the Private Sector from the Public Sector



Let's roll!

- ◻◻ We need to push our government for easing building Blockchain networks as Cooperative Societies, Mutual Associations or Partnerships where SMEs can adopt Blockchain lowering the costs while keeping the right internal democracy for its management.
- ◻◻ We should have social or fiscal benefits on the Cooperative Societies aimed at technological modernization of SMEs.
- ◻◻ We need specific regulation for boosting this kind of models to avoid the dictatorship of large enterprises on the big Blockchain consortiums.

Pushing Blockchain on the Private Sector from the Public Sector



No more technology breach by promoting inclusive models

Governments should promote the creation of inclusive Blockchain networks to prevent them from becoming a new technological barrier and to promote the social economy and equal opportunities.

This promotion must land as specific regulations (including taxes) to favor this kind of initiatives versus closed networks.

The key is the cooperative network governance.

Thanks!

Tomás García-Merás
+34 619 98 00 58
clawgrip@hotmail.com

<https://www.linkedin.com/in/tomas-gmeras/>
<https://github.com/clawgrip/>



BAES

Blockchain
Lab