BLOCKCHAIN PRACTICES

#BLING #blockchainpilot

The Financial Emergency Brake

CJIB - Dutch Central Judicial Collection Agency

The CJIB (Centraal Justitieel Incassobureau/Central Judicial Collection Agency) is part of the Dutch Ministry of Justice and Security. It is responsible for collecting a range of fines and penalties in the Netherlands, and is the designated Dutch authority for the EU's Cross Border Enforcement Directive. The CJIB is the national coordination service for custodial sentences, arrest warrants, community service orders, and probation services; it also provides a Victims Information Service.

In 2017 the CJIB founded an Innovation Lab to find solutions for complex issues – like 'how can government agencies exchange information that will help vulnerable citizens, whilst still complying with GDPR?' - using a combination of data and new technologies – like blockchain.

Introducing the 'Financial Emergency Brake'

With funding of two parts of the Ministry of Justice (Innovation-team J&V and DGSenB) , BLING, the Cyber Security Group of the Delft University of Technology (TU Delft), Ledger Leopard, and Blockchainprojects.nl were able to develop the 'Financial Emergency Brake', a sustainable new service for citizens and government organizations that helps support citizens with financial or debt problems.

The Financial Emergency Brake allows citizens to directly flag to the CJIB when they are unable to pay government fines. The system allows citizens to maintain their privacy, while linking this declaration with certification from local services that they are providing debt support.

The service uses blockchain's identity- and information management tools, together with a zero-knowledge proof (a system where one party can prove to another that they know a piece of information, without conveying any other information apart from the fact that they know the information).

FOLLOW US

Interreg North Sea Region BLING
European Regional Development Fund
EUROPEAN UNION

BLOCKCHAIN PRACTICES

#FinancialEmergencyBrake

Addressing personal debt and finance problems

Nearly 1.4 million Dutch households have financial problems. The impact of financial problems and having debts on people is worrying; this is why the Dutch government wants to help people to avoid - and get out of - debt. The Dutch government aims to balance the interests of the debtor and those of the creditor, and not to overlook the social causes of debt. All creditors should be more aware of the circumstances of debtors and collect debts in a socially responsible manner - this includes government organizations, such as the tax authorities and the CJIB.

For these reasons, the CJIB distinguishes between those people who want to pay their debts but can't, and those people in debt who are able to pay but won't. People who cannot pay a claim can now come to an agreement as to how to the debt can be paid, which helps prevent debt problems from worsening. To identify people who want to pay their fines to the CJIB, but can't, and to provide them with services and time to fulfil their obligations, the CJIB needs a timely signal that the citizen is in debt. The CJIB has developed an algorithm call Debt Alert, which can predict whether someone is at risk of either going into debt or being in debt.

The problem the CJIB faces is that many citizens with debt problems do not tell the CJIB, and letters to them are often left unopened. The gravity of their debt problems often only becomes apparent very late in the debt collection process – when it reaches bailiffs or the courts. If the CJIB had known the scale of the individual's debt problem earlier, a lot of time, money, and stress could be saved, and the debt issue could be managed in a better way.

However, CJIB has found out that these citizens are often in contact with their municipalities and using local debt help/debt relief services. Knowing this, CJIB developed the idea of the 'Financial Emergency Brake'. The Financial Emergency Brake can help with timely identification of debt problems. In addition, it can potentially prevent someone's debts from worsening. As such, this application contributes towards the Dutch government's wider debt reduction strategy. In 2019 the prototype was developed using blockchain technology, based on the principles of privacy and citizen-centred sharing.

Why blockchain?

For the CJIB, technology is a means to an end, and not and end in itself – so they investigate how different technologies can help them achieve their objectives. For the Financial Emergency Break-pilot, the CJIB looked for a suitable technological alternative to using centralized or siloed data stores. Any solution needed to allow participating organisations to easily exchange information in a safe and legal manner, whilst maximising citizen's control over their data. These two requirements "GDPR-proof" the solution.

BLOCKCHAIN PRACTICES

#UseCase #DigitalDataSafe

The CJIB decided to use blockchain as part of our solution for three main reasons:

1. It was important that no single partner should have control over all of the data - a decentralized chain of trust is required.

2. Blockchain-enabled solutions can provide citizens with tools to control their own data in a private and secure way.

3. The solution would be more stable because it uses a distributed approach, so there would not be a single point of failure.

Our blockchain solution for the Financial Emergency Brake used two key features of blockchain: it is based on a combination of *Self Sovereign Identity* with a *Zero Knowledge Proof*.

Self Sovereign Identity (SSI) is an approach where people and businesses can store, manage and share their attributes or credentials on a blockchain. These credentials can be efficiently shared with other parties that can then validate these credentials, without having to rely on a central repository of user or system data. SSI is a digital way of doing what people do today when they hand over their paper-based driver's licence or passport as part of a verification/identification process.

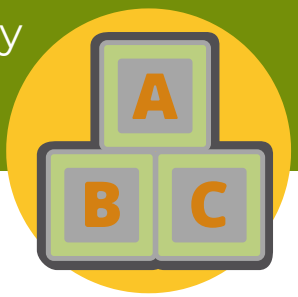
Zero knowledge proof (ZKP). Any information claim or credential can be proven using a zero-knowledge proof – a computer-based algorithmic solution. This means that a computer 'game' can be designed between a prover and a verifier where the prover has knowledge of some information (e.g. in this situation particular details about their financial situation – perhaps that they are receiving a certain type of financial support – the 'claim'), and is able to prove that their claim to know this is true - without revealing the actual details of the information to the verifier.

Lessons learned during prototype development

CJIB learned two main lessons during the development of this pilot. Firstly, that there are multiple blockchain technology stacks, each with different structural/design/architectural properties. Which one to use is a matter of deciding what stack is most 'fit for purpose' – i.e. which meets most of the pilot's requirements. Unfortunately, there was no single technology stack that covered all of our different requirements: authentication, access control, secure communication, confidentiality related mechanisms, and so on. CJIB thus had to choose between two options:

BLOCKCHAIN PRACTICES

#BLING #SelfSovereignIdentity



a) wait until there is a complete blockchain stack/solution is developed that meets all of the pilot's requirements (this might take some time),
b) adopt one specific blockchain technology stack, and then customize it by adding the desired components.

CJIB chose to do the latter.

Secondly, CJIB learned that the privacy related tools that they wanted to use - such as Zero Knowledge Proofs – proved to not to be as mature as hoped, and that existing implementations were very limited and not 'ready-to-use' off the shelf. What was required to deliver practical solutions for private data sharing in a distributed network was joint work between researchers and software developers, particularly focusing on:
• Development of a more complete blockchain technology with needed components,
• Development of secure and properly implemented, computationally efficient cryptographic protocols, including Zero-Knowledge Proofs.

This is what the CJIB did in a triple-helix collaboration between the government, the private sector and the knowledge sector.

Next steps

For the final part of our project CJIB has started a pilot with two Dutch municipalities – Eindhoven and The Hague, with 80 testers. This pilot will verify whether - and how - this solution works in reality, moving from a controlled design and testing environment into complex real-world settings. CJIB hopes to finish the pilots before the end of the summer in 2021, and will plan to go live after that, if the pilot results are positive.

With the support of these municipalities, this pilot will give their citizens control over the sharing of their debt information and make a contribution to tackling an important an important social problem. CJIB's project is a first - important - application of Self Sovereign Identity and zero-knowledge proofs by the Dutch government. Using the same methodology and building blocks (no pun intended), organisations can create a wide range of privacy-preserving governmental services. Any situation where information-sharing between organisations can benefit vulnerable citizens would be a good candidate for this type of solution.

Over the next few months and years our challenge will be deploying a fully operational application which is scalable and embedded in a collaboration or consortium that can continue to expand the ecosystem. At the same time, CJIB will need to make the approach and technology available for other applications that benefit citizens and governments.

For the CJIB, the Financial Emergency Brake project was an excellent example of the Triple Helix approach - collaboration between the government, the private sector and the knowledge sector. They've shown that this type of collaboration can deliver rapid results.