BLOCKCHAIN PRACTICES

#BLING #blockchainpilot

Generating Health Certificates

Oldenburg

Oldenburg is a city of 170,000 in north-west Germany, and is the cultural and administrative hub of the area. It is the region's centre of education, with the Carl von Ossietzky University, the Jade University of Applied Sciences, the Private University of Applied Sciences for Business and Engineering, and more than 70 schools, vocational colleges, and technical colleges. Oldenburg was Germany's *City of Science* 2009. The local government is keen to build a 'digital future' for the city.

BLING and the development of local blockchain use-cases

New technologies usually present new ways to develop and deliver services that benefit the local community and government. However, we can't find out how practical these new technologies are until we try them out. As deploying those technologies at scale can sometimes have unintended consequences, piloting use-cases makes sense.

In the BLING project, partners – both academic and municipal – from seven different Northern-European countries are assessing how they can improve processes in their governments or municipalities by applying the unique properties of blockchain technology to either improve existing services or to develop innovative new services that lever the technology's unique properties. Every partner has chosen at least one use-case to design a blockchain-enabled service solution which can be tested in a local pilot study.

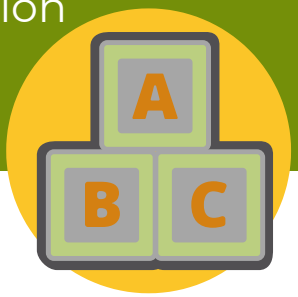
FOLLOW US

Interreg North Sea Region BLING
European Regional Development Fund

EUROPEAN UNION

BLOCKCHAIN PRACTICES

#HealthCertificates #DataValidation



Supporting delivery of the 'Prostitutes Protection Act' in Oldenburg

Like other Cities in Germany, Oldenburg has to register local sex workers as required by the 'Prostitutes Protection Act' (Prostituiertenschutzgesetz) - a German Federal Law that came into force in July 2017. Sex workers are required to register and receive a registration certificate, and are required to have regular health tests.

It is estimated that there are more than 400.000 sex workers in Germany, but government data suggests that only approximately 40.000 were registered by the end of 2019. Sex workers have voiced considerable concern about the privacy implications of registering, and that their personal information will become public.

One of the problems that health organizations in Oldenburg are dealing with is that of fake or invalid registration certificates. At the moment, every city provides a different form of registration certificate, which makes it difficult for other regions etc. to authenticate certificates and determine if certificates are valid or spoofed.

The municipality shared this problem with the University of Oldenburg, and asked us to design and develop a solution. They were looking for a solution where a user could verify or validate a registration certificate, and ensure the integrity and source of the registration certificate. Our initial thought was to digitize the registration certificate, and then cryptographically sign it so it could not be modified or tampered with, and then store it on a decentralized public ledger.

Why a blockchain-based solution?

The aim of the BLING project is to develop and assess blockchain solutions, and naturally we tend to use blockchain in this use-case as well – given the privacy and trust implications of data-sharing in this area. However, we first needed to make sure that using blockchain was an appropriate solution and would add value to our approach. In many cases we see that organisations are using blockchain when they don't need to – and this would add unnecessary complexity to our solution.

For this solution evaluation, we began by answering the question of what our solution would have looked like before distributed ledger technologies became available. In a traditional solution – before the invention of blockchain – we would have had to design a centralized database that was manged by either the local Registration Office or the Health Organization that provided health checks for the sex workers. Neither of these approaches were desirable, since these two organizations should not necessarily be forced to 'trust' each other – by making them share their information between the organisations.

BLOCKCHAIN PRACTICES

#UseCase #BlockchainPilot

An additional concern we had to address in the design of the system was preserving the privacy of the sex workers. We had to address questions like: 'should the City's Ordnungsamt – public order office - have access to the sex worker's health data?', and 'should the Gesundheitsamt – the Public Health Department - have access to the sex worker's identity details'? This convinced us that using blockchain technology would add value to our solution. In a blockchain network, we can ensure that the trust relationship is based on the network itself, without the need for any third parties reviewing/validating data etc. By using blockchain, we could ensure the source and the integrity of the certificate, as well as protecting the privacy of the sex worker.

Blockchain gives us real solutions

Because this approach uses blockchain, this solution has some real strengths that make it valuable for both sex-workers and the organisations that register and support them:

• This solution ensures the accuracy, integrity, and source of the certificates, while also maintaining the sex worker's privacy – particularly if they want to use an alias.
• It provides a way to prove that the sex worker's health certificate is up to date.
• The sex worker is the owner of the certificate - they are the only person that holds the cryptographic key which points to the certificate. They cannot change the content of the certificates, but as the owner of the certificate they can revoke the access to it when they want to – which supports their right to be forgotten.
• The sex worker can decide what information is stored in their record, and can decide who is able to access the certificate, and what information is shared and with who it is shared with.

This system should make certificates more portable and easier to authenticate, and could be expanded to support other cities and other relevant information and certificates.

But the next question we had to answer, after deciding to prototype a blockchain-enabled system, was: what platform/infrastructure would we use to store the electronic certificate?

What type of Blockchain? How we chose IOTA

Now that we had decided to pilot a blockchain-enabled solution, it was time to think about implementation details – like what type of blockchain technology would be appropriate? There are a range of different blockchain technologies - such as private blockchains or public blockchains. Blockchain is a distributed ledger, in which the ledger itself is designed to be the source of trust (through its cryptographic design).

BLOCKCHAIN PRACTICES

#BLING #DistributedLedger

However, blockchain is just a type of distributed technology, and not the only one. Blockchain is more popular than other distributed ledger technologies because of the popularity of bitcoin, and all the hype around bitcoin.

Nevertheless, blockchain technology has always had to work within the trilemma of security, scalability and decentralization. In a Public blockchain (e.g. Ethereum, bitcoin), the amount of transactions per second are limited, since the validation of transactions depends on “miners” – work done by other computers that use their computing power to validate transactions – these receive a fee in cryptocurrency for their validation work. So in a public blockchain, a fee is charged for every transaction. To avoid this limitation, there are private blockchains, in which transactions are validated by consensus among participating members. Transactions on these private blockchains do not incur a validation/transaction fee. However, as the name suggests, private blockchains are not open to the public, and thus are not truly decentralized.

Other types of distributed ledger have been developed to address these underlying questions of security, scalability and decentralization - like IOTA. IOTA is an open, feeless, data and value transfer protocol for blockchain that is designed so that every transaction in a IOTA distributed ledger will validate two other transactions in the ledger when it is recorded. This allows IOTA to overcome the cost and scalability constraints of public blockchains. This means the ledger does not require miners or transactions fees. The unique design of the IOTA network means that as the number of transactions increases, the speed and the capacity for transactions also increases.

For the Oldenburg use-case, the blockchain solution should be publicly accessible, so the registration certificates are accessible by different organisations and users. As sex workers move from place to place, the solution should be expandable as well so that other registrars and health workers outside of Oldenburg can use it.

Scalability, no transaction fees, and security make IOTA a very attractive solution for our use-case. By using IOTA, we can have the advantages of both public and private blockchain. We can have a public secure decentralized ledger, in which there are no costs involved for writing new records on the ledger.

How IOTA controls access to private information

In our pilot, every party in the system (sex worker, Health Office, or Registration Office) would create their own restricted channel in our IOTA network - this is similar to a publisher/ subscriber model. The Registration Office R1 issues an anonymous certificate for sex-worker S1 (based on S1’s unique ID) and puts it on R1’s own channel. S1 has his/her own channel as well. On this channel, when they claim the registration certificate created by R1, the system creates a pointer to the relevant certificate in the authorities' channel. Since the certificate is hosted by the Registration Office, S1 can remove access/link to that certificate at any time

BLOCKCHAIN PRACTICES

#UseCase #HealthCertificates

they wish, and the Registration Office – as the certificate issuer, also has the right to revoke the certificate – e.g. when it has expired.

Certificate viewers have to install a smartphone app, and to register an ID on the IOTA network – this ID will be anonymous (a username and password are required to login to the app). Once they have an anonymous ID, they can scan a QR code generated by the sex worker's app and will receive one-time access to the certificates the sex worker wants to share with the user – the worker will decide what certificates they share.

Pilot delivery and additional use-cases

We are currently in the development phase of the pilot and will deliver the initial prototype in March 2021. We expect to test the pilot with 5-10 sex workers, along with officials issuing registration and health certificates for a two to three-month period. As it's not compulsory to use the pilot system, we'll need to be able to convince users of the benefits of using the system we've developed so they'll help by testing it.

The broad approach we have taken is transferrable to other situations/use-cases where a user needs to verify that they have received a certificate from another source – e.g. the approach we have designed can also be applied to situations where a user needs to provide evidence that they have had a recent Covid test, for example, or that the user does not have any convictions or criminal records. Changing the focus to add these additional capabilities will require the development of relationships with additional organisations to ensure we meet their needs and requirements. Discussions about expanding our pilot to additional geographical areas and of potential additional uses for our approach to registration/certificate verification are ongoing and will be developed once the pilot is live.