Use Case 1: Blockchain & GDPR Compliance

Overview: Blockchain based transaction platform for P2P lending which is compliant with the recent General Data Protection Regulation (GDPR) regulations, implemented in the European Union (EU), supporting modification and deletion of user specific data on a blockchain.

Current Challenges:

Governments all over the world have recently been introducing, or proposing, legislation in regard to data privacy and storage. In recent years, legislation has been moving clearly in the direction of giving data ownership back to people. That is especially visible in Europe, where with GDPR, which started was brought into effect in May `18, a person is legally entitled to move his/her data from any one platform to another (called **"data mobility"**) and he/she can request that companies delete all his/her data (**"right to be forgotten"**). There is increased focus to ensure compliance with the guideline as there is an imposition of extremely hefty fees for companies not abiding by it. Furthermore, its reach goes far beyond the EU as it also applies to any form of information (e.g. PII, transactions) that go through data processors (corporates, analytics platforms etc.) and data regulators (government, compliance firms) pertaining to EU individuals.

While Blockchain shares the goal of putting the control back in the hands of the user by decentralizing information, another of its key feature, immutability is counter intuitive to the user's right to be forgotten. Immutability basically means that transactions once recorded on Blockchain can't be modified or deleted. With that in mind, the question is how do we design a Blockchain solution that can be made to comply with this regulation and provide a feature where a user's data can be masked or deleted should the user choose the right to be forgotten.

Business Requirements

- Basic P2P lending platform facilitating exchange of value/tokens on a blockchain based network. While the basic functionality of a P2P lending/transaction platform should be available, the key area of focus should be around how can we make the solution compliant with GDPR regulation.

- Solution should be flexible enough to allow movement of user specific data from one platform to another.

- Solution should be flexible enough to allow deletion or anonymization of user specific data in case a user withdraws consent

Use Case 2: Blockchain Platform for Certificate Issuance and Verification

Overview: Blockchain based platform for storing digital certifications and real time analysis for document verification and fraud detection with analytical capabilities.

Current Challenges:

Certificates are not only a proof of achievements or capabilities that one might possess but also can be used to validate these credentials to a third party. At the moment most of the certificates are issued in a paper format, which makes it susceptible to manipulation. Thus, one of the major concerns is not only issuing the documents to the right candidate but rather assessing whether it has been tampered with or duplicated for personal gains. We would like to leverage the potential of Blockchain to create a Platform that digitizes the process of issuance, endorsement and consent based sharing of certificates. Amongst others, the key questions that need to be addressed are –

1. Can we prove that a certificate hasn't been tampered with or altered?
2. Can we ensure that only genuine parties can issue, endorse, store and consume the certificates?

A stakeholder ecosystem must be created which allows adding/modifying certification authorities and real time users/verifiers based on ad hoc requests.

Business Requirements

- Basic blockchain platform facilitating storage of the digital certificate connected to a user/ organization.
- Certificate verification
- User Interface to connect the different stakeholder in the ecosystem.
- The digital certificate can be of different file formats (PDF, Word, JSON) or rather file format agnostic.
- Solution should be flexible enough to allow addition/deletion of different stakeholders in the system.