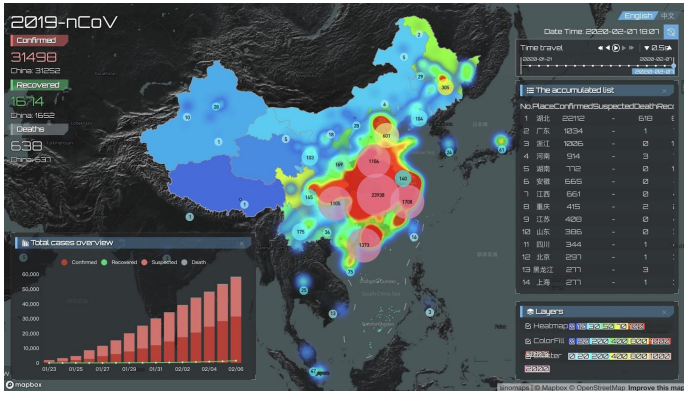
PANDAPP

Privacy preserving data contribution

Contacts:

Grégoire Bailly gb@iex.ec Eric Rodriguez er@iex.ec

an application based on free will ...



Everyone can choose for what his data will being used at the end. He can, for instance, have access to some results as a heatmap aggregating all the available data.

… with reimagined security and data governance

Capitalising on our technical knowledge, use the Trusted Execution Environment (TEE) technologies, associated with a blockchain managed cloud computing infrastructure to bring security and governance to the private data.

Tracking applications, the disaster?

If there is one active subject in the IT world in this time of pandemia, it is surely the tracking applications. Problem is, if it was supposed to be a perfect tool to help reduce the impact of the disease, it has become a big question mark concerning data privacy. And as all questions, it has scared a lot of people.

Basically we have a efficient solution for fighting covid-19 but also a huge security problem concerning the security of personal data.

Value Propositions

PANDapp acts as an open and secure platform providing privacy-preserving access to anonymized mobility data and others...

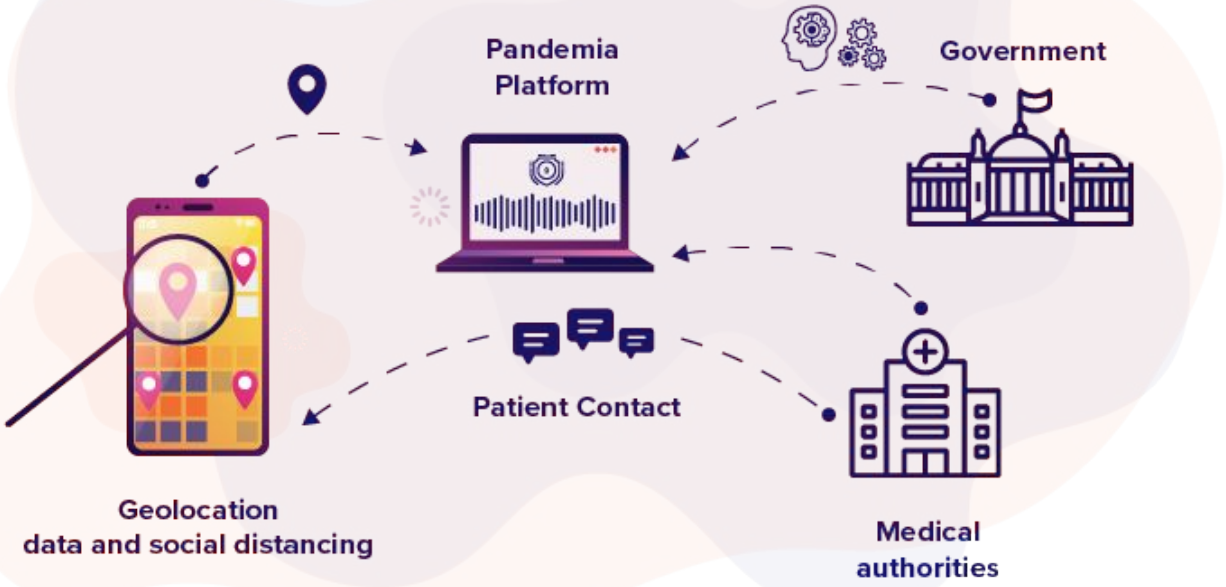
It allows to propose new applications to build additional high-value services such as contagion heatmaps, pandemic evolution forecasts per districts or post lockdown strategy.

Users can decide to share their data and whitelist auditable application.

Individual gets the guaranties that its data has been used only in an authorized purpose.

For governments, academic research or even any individual initiatives, they can propose valuable services or request for real data to support researches and experimentations.

Pandapp:
Privacy preserving data contribution



Our goal here is to prototype some backend services that, using relevant users data, compute some results and make them available to specific users.

All of these using blockchain and TEE to protect data.

Consensys Health Stop Covid-19 Hackathon scope

What we have done

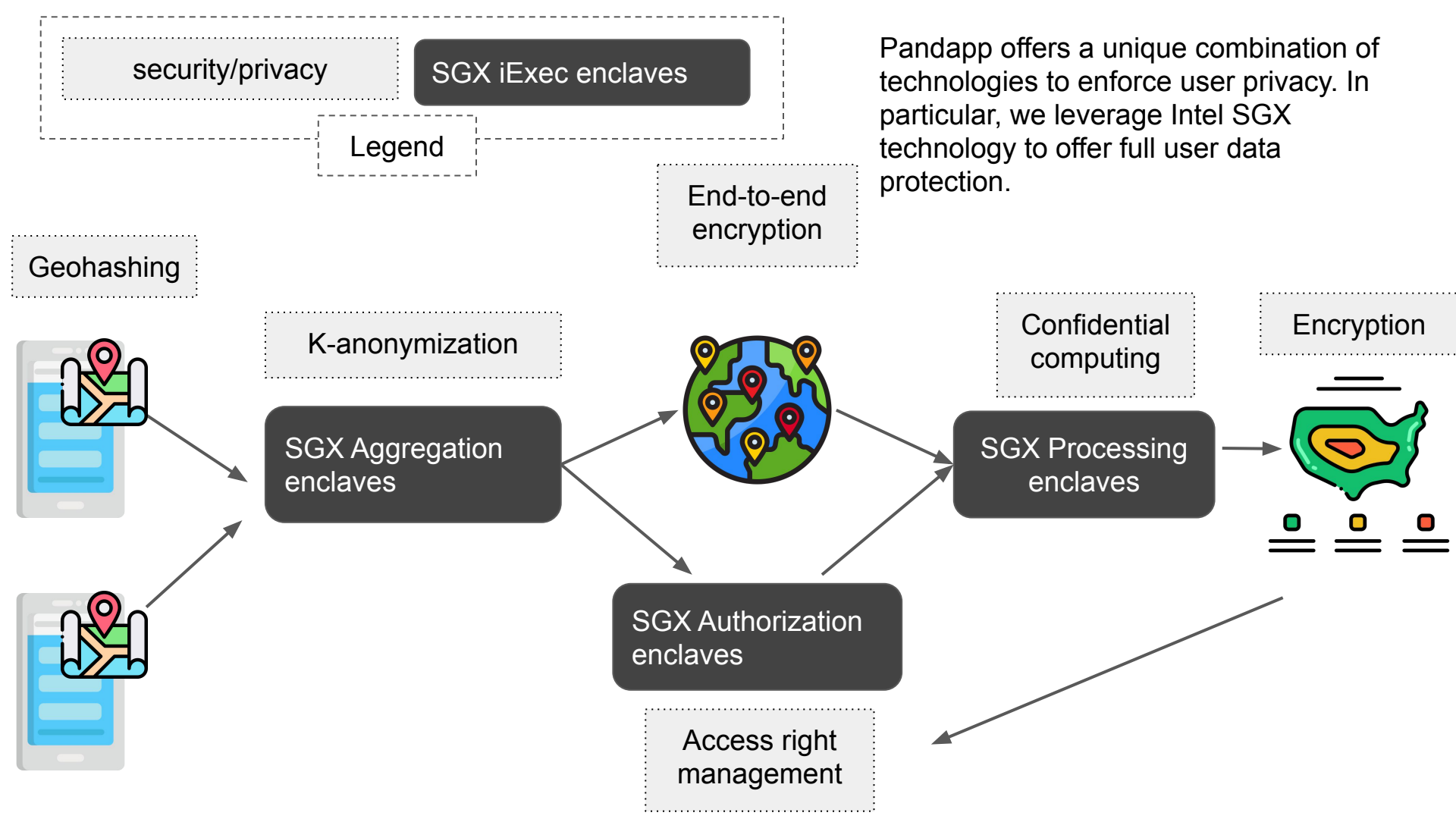
https://github.com/iExecBlockchainComputing/backend_covid

- **Generating sample in encrypted dataset:** simulate *displacement person and generate collection for development.*
- **Confidential Computing (CC) applications:** *developpement of the CC applications that uses data to compute some meaningful score*
- **Data governance:** *when making the data available, manage which application can use them*

Available on Goerli testnet

What we have not done … yet

- **Data collection:** *we are not doing any work on a phone front-end*
- **Data aggregation:** *the data we use are already formatted as one dataset*
- **Pretty frontend:** *this is a code prototype so we may display some result but the beauty/UX is not part of our concerns*


security/privacy
SGX iExec enclaves
Legend
Pandapp offers a unique combination of technologies to enforce user privacy. In particular, we leverage Intel SGX technology to offer full user data protection.
End-to-end encryption
Geohashing
K-anonymization
Confidential computing
Encryption
SGX Aggregation enclaves
SGX Processing enclaves
SGX Authorization enclaves
Access right management

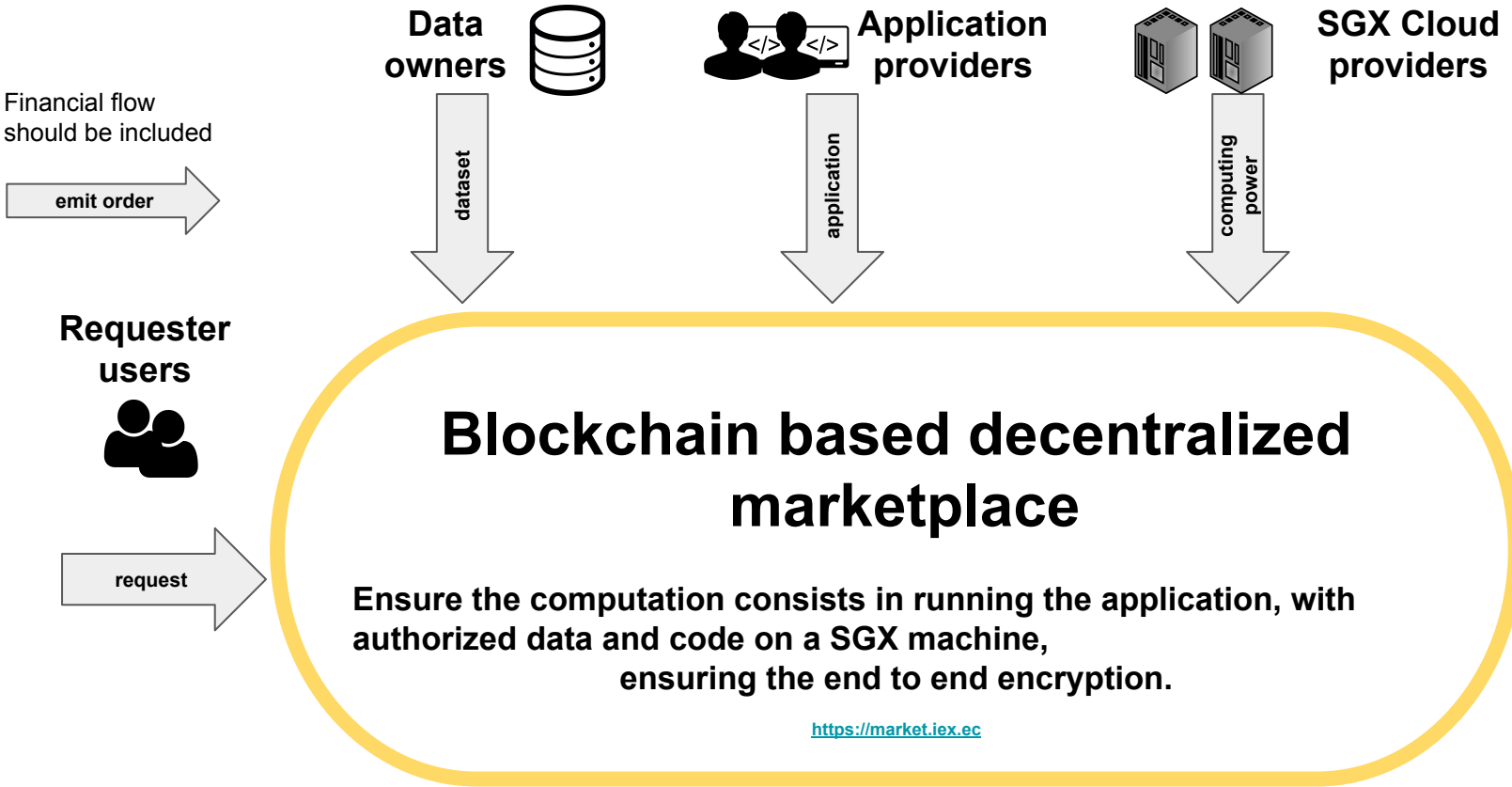
End-to-End Trusted Execution with Intel SGX

What is an enclaves?

Confines execution and data within a encrypted environment: no one can access/tamper the execution

- for application/input/results
- guarantee execution integrity
- provide on-chain enclave execution attestation

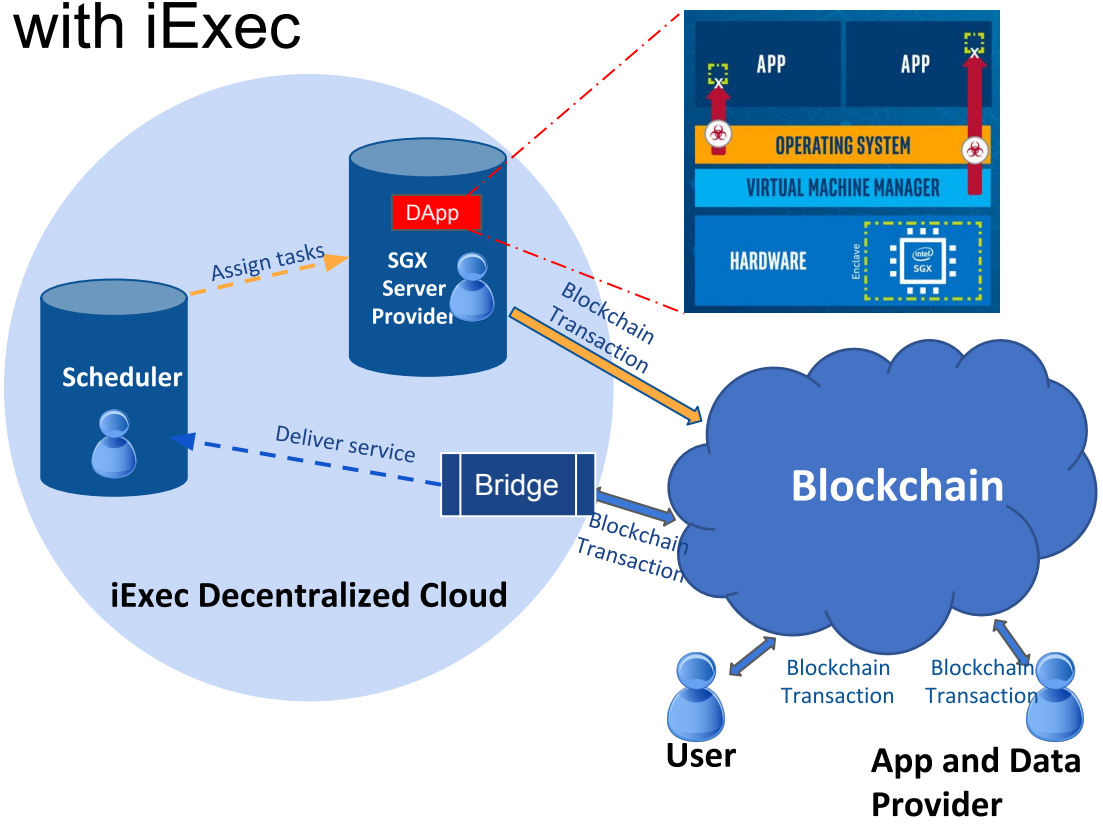
Build on top of off-chain computing infrastructure



Confidential Computing with iExec

+ **Requirement**:
How to protect the DApp (as well as its sensitive data) residing/running on decentralized nodes is becoming a big challenge.

+ **Solution**:
SGX-based solution allows encrypting the DApp / data while deploying them over networks, and the encryption key can be transferred to SGX enclave at run time via a highly secured channel to decrypt the DApp / data.



Public heatmap generation and social distance calculation

Individuals

Share information:

- Status (deseased or not)
- List of authorized app
- List 2-uplet <timestamp, geohash >

SGX Aggregation enclaves

Every day, the server generates encrypted datasets on ipfs, one for each registered application. Dataset orders are published with application restriction

Blockchain based decentralized **marketplace**

Dataset encrypted on ipfs.
App is public on github and docker hub

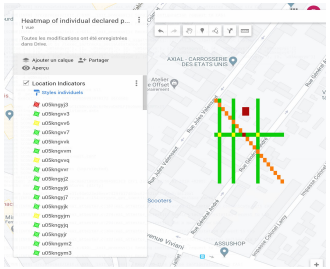
Docker Hub

SGX Processing enclaves

Individuals can ask for social distance information, the result has been encrypted and stored on ipfs, only the requester has access to the result

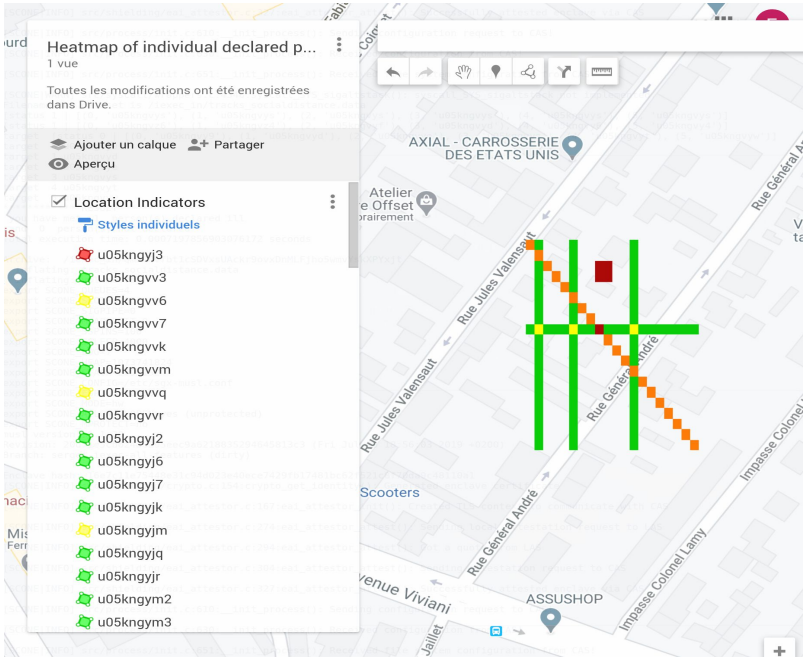
```
target  1 u05kngvyd
target  2 u05kngvye
target  3 u05kngvys
target  4 u05kngvyt
target  5 u05kngvyw
************RESULT**************
 you have met  1  person(s) declared ill
 and  0  person(s) not declared
Total execution time: 0.0007197856903076172 seconds

Archive:  /iexec_in/QmPCQVfbt1cSDVxsUAckr9ovxDnMLFjho5wmvYskXPYxjt
  inflating: tracks_socialdistance.data
```



Every day , a public heatmap is generated, The app currently creates a kml file, viewable on Google maps

Public heatmap of deceased person displacement



Red : hight density of person declared deceased

Green: low density of persondeclared deceased

Apps

https://explorer.iex.ec/goerli/app/0xff74A1De0CD81CA64B767183f4137d455AB0b812

Dataset

https://explorer.iex.ec/goerli/dataset/0x103E387a76E1a5dCb26200432636615B25B46F70

Execution

https://explorer.iex.ec/goerli/task/0x7bb85019a72599ed07759ad0d55bacf3ab57f4ad0a0b4039e37738d0e8828bf0

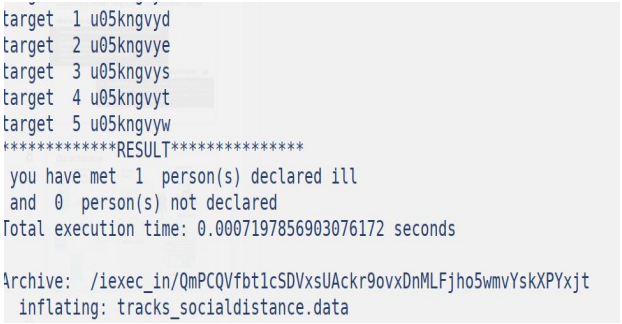
https://explorer.iex.ec/goerli/deal/0x17474864fda125b24ab47623cbd925bcfabc2702b59ac70827480b5e2331f661

Code

https://github.com/iExecBlockchainComputing/backend_covid/tree/master/secure_heatmap

Social distance calculation

This application privately returns how many persons, declared deceased and not, you met during the day.



Apps

https://explorer.iex.ec/goerli/app/0xad11CD28aaC19c5d7fC7D82a5510Be150561A1E1

Dataset

https://explorer.iex.ec/goerli/dataset/0xD19472cb0f214Fd6Cd5B673d1224B427C7F1F570

Execution

https://explorer.iex.ec/goerli/task/0xa366f4509ec1ea44b1d6667f541beb225d4d5d303eb05ab8e6327f08918f7f82

https://explorer.iex.ec/goerli/deal/0xf19dba5208a9b5e6e58ee4ba4b4dfe39e29bad9e5421a1e0fecc56cd0728b1ef

Code

https://github.com/iExecBlockchainComputing/backend_covid/tree/master/secure_socialdistance_calculation

Next steps...

Short term:

- Anyone can propose new applications, or propose improvement of existing apps. The heatmap we propose has clear limitation and needs extra anonymization processing.
- We focus first on data mobility but there is no technical issue to extend the platform in many fields.
- Develop user friendly front end and aggregator servers.

Long term:

- Gamification to incentivise users involvement trough rewards
- Build a decentralized infrastructure and governance

PANDAPP

Privacy preserving data contribution

Question?

Contacts:

Grégoire Bailly gb@iex.ec Eric Rodriguez er@iex.ec