Building a Decentralized, Trusted and Privacy-preserving Computing Infrastructure

Gilles Fedak, PhD, CEO, co-founder
gilles.fedak@iex.ec

FIT-Europe
June, 9 2021

iExec

Decentralized Cloud Computing

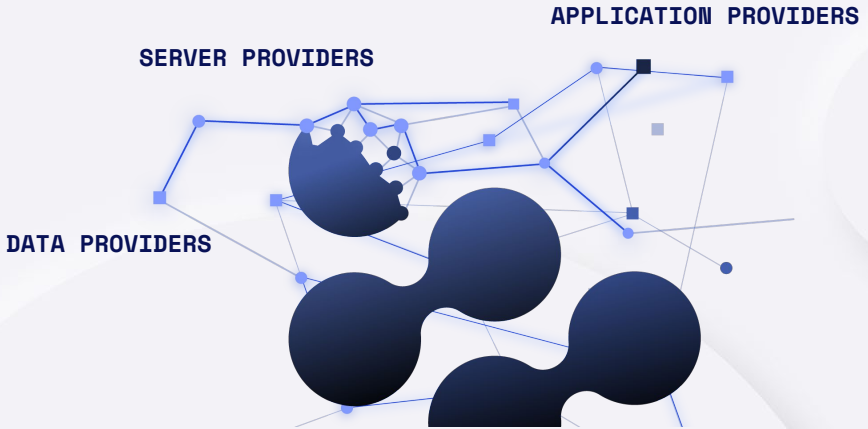
iExec

Decentralized marketplace for computing resources

- servers, applications, datasets providers/consumers can interact in a P2P way, without central authority

Why is it important ?

- transparent, fair, competitive, open, scalable markets



Understanding the Challenges of Decentralized Marketplace

Governance:
- Enforce policies for stakeholders to exchange or trade digital assets

Trust:
- produce, store, share proofs of ownership and usage requests
- traceability, unfalsifiability, security of exchanges of digital assets,

Confidentiality:
- protection of private data and the confidentiality of exchanges

Relevant technologies: blockchain, smart contracts, confidential computing, zero-knowledge proof, etc...

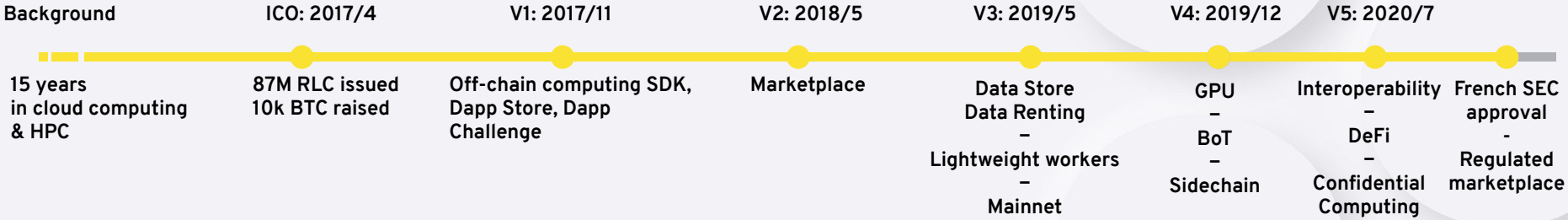
iExec - Timeline and Key Info

Founded in **2016** by Haiwu He (**Chinese Academy of Sciences) &** Gilles Fedak (**Inria)**

- 25 employees, based in France, 7 PhDs

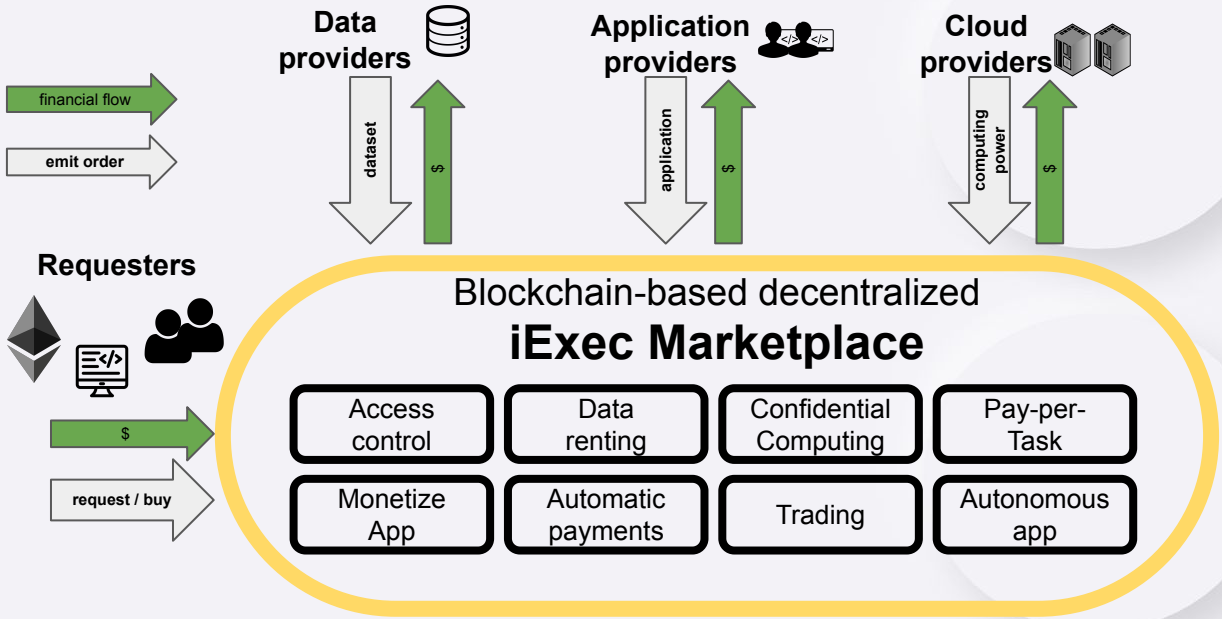
April 2017: RLC ICO raised 10,000 Bitcoins within 3 hours

5-year roadmap completed in 2020



Decentralized Computing on Ethereum

iExec: provide developers with scalable, secure and easy access to decentralized services, datasets and computing resources.



Requesters' Use Cases

Run complex code & DOracles, get a proof of correct execution

Users

Run your code on resources from multiple providers with **no vendor lock-in.**

Run you own apps: not limited to the marketplace

The marketplace gets you the best price

Custom level of confidence for each task

Web 2 applications

Trusted executions prove to you and to others that a result is valid.

Confidential execution keeps data private with TEE enclaves, plus result signature.

Connect any application to the platform with our SDK

Smart Contracts

Program complex oracles with image recognition, multi-source aggregation, etc.

Trigger off-chain tasks directly from your smart contract

Interact with regular IT infrastructures, sensor networks, arbitrary blockchains, etc.

Providers' Use Cases

Open new streams of revenue by monetizing the resources you already have, get paid on the blockchain

Application providers

Monetize apps, dapps, functions, algorithms packaged as **Docker Containers.**

Price set per execution

No vendor lock-in: runs the same on multiple providers.

Data providers

Monetize trained AI models, private data and valuable knowledge.

Arbitrary files & data types supported

Price set per execution

End-to-end encryption with TEE: prevent copy & ensure confidentiality.

Computing providers

Monetize servers and workstations (CPUs, GPUs) when they are not in use.

Instant new revenue stream

Isolated workload with Docker & TEE.

The iExec Token: RLC

Token usage

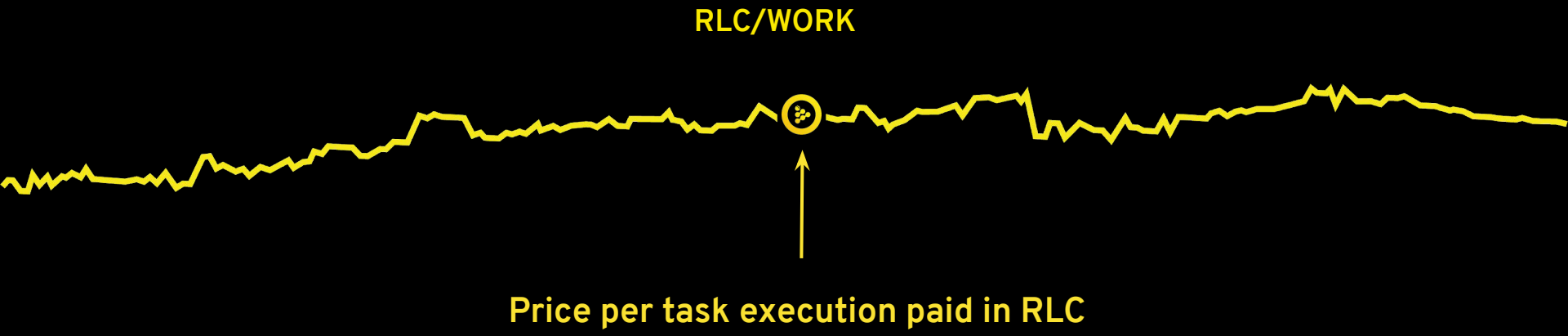
- The RLC Token is the only way to access the iExec decentralized cloud
- Providers are paid with RLC
- Allows to build incentives in the network.

- Issued on main net on April 2017

Marketplace for Computing Power

Allows to trade **computing power as a commodity**

Allows companies and individuals to **monetize their servers/PCs**



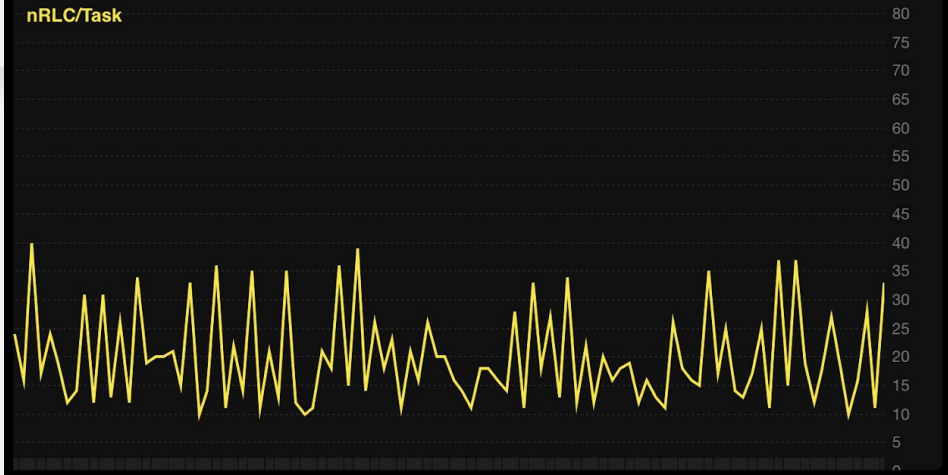
iExec Marketplace

Account

XS S M L XL

TEE CUDA Trust

nRLC/Task



Order Book

Hash	Price	Worker...	Trust	Volume
0xd3ed3...	13	0xCa7c0...	1	1
0x85df95...	13	0xCa7c0...	1	1
0x2f28a8...	10	0xCa7c0...	1	1
0xef885f...	10	0xCa7c0...	1	1
0xe26e5...	10	0xCa7c0...	1	1
0xeb079...	10	0xCa7c0...	1	1
0x8b1fdb...	10	0x9B919...	1	1
0x9e4da...	10	0xCa7c0...	1	1
0x0828a...	10	0xCa7c0...	1	1

Last price: 33 nRLC ↑

Hash	Price	Reques...	Trust	Volume
0x3ce83...	7	0xF048e...	0	1

Recent Trades

ID	Price	Time	Worke...	Volume
0x5c17...	33	10:11:40	0x9B9...	1
0x153b...	11	10:08:52	0xCa7...	1
0x862d...	28	09:42:24	0x9B9...	1
0xf8f8d...	16	09:40:20	0xCa7...	1
0x87f5...	10	09:14:12	0x9B9...	1
0x67c2...	18	09:12:16	0xCa7...	1
0xdc56...	27	08:47:52	0x9B9...	1
0x0979...	18	08:44:28	0xCa7...	1
0x8285...	12	08:21:52	0x9B9...	1
0x5c05...	19	08:19:52	0xCa7...	1
0xbede...	37	08:00:44	0x9B9...	1
0x8ba4...	15	07:57:32	0xCa7...	1
0xfa04...	37	07:30:24	0x9B9...	1
0x4f2e...	11	07:27:20	0xCa7...	1
0xdaab...	25	07:05:24	0x9B9...	1
0x8ab9...	17	07:01:20	0xCa7...	1
0xa7a4...	13	06:39:28	0x9B9...	1
0xf580...	14	06:37:32	0xCa7...	1
0x2b91...	25	06:15:16	0x9B9...	1
0x444e...	17	06:10:44	0xCa7...	1

My Trades

My Open Request Orders

My Open Workerpool Orders

ID	Price	Time	Workerpool	Volume
0xd18f64e536df9cfee4c85ae2b790fbc...	10	14:18:00	0xCa7c0e9a96666bC3636ff3d3E8480...	1
0xd71b06b8ea058192a78036b2cab9...	10	17:45:48	0xCa7c0e9a96666bC3636ff3d3E8480...	1
0xf5155166a1e7f2c06965ec0c001010...	10	17:27:24	0xCa7c0e9a96666bC3636ff3d3E8480...	1
0xdd4b1ca055a547a46530a0ccec524...	10	07:37:04	0xCa7c0e9a96666bC3636ff3d3E8480...	1
0x9c6c4214c7ce1a498e1a51fbca828...	10	00:32:44	0x9B919d74f8Ef49C33343AD305695...	1
0x1a5c8181672ba73c08f94313399c9...	10	00:27:04	0xCa7c0e9a96666bC3636ff3d3E8480...	1

Fill Market Order

Place Limit Order

Order Hash: * 0x0828aa3c7446f21464d4219da7c2f

Request Order Hash: * 0x3ce83e3afcb2ba48d42703d48

Dapp Address: * or name...

Volume: * 1

Dataset Address: * or name...

Workerpool address: *

Work Params: * {"0":""}

Sell computation at market price

Advanced parameters

Applications meet computers

Ultimate goal: give Smart Contract-level trust to any application

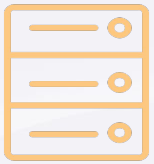
Dapps

Artificial Intelligente | Big Data | Financial Sector | 3D Rendering | Cryptography | Health

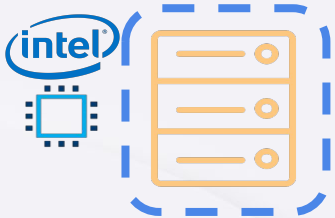
Worker Pools

PRIVATE

HYBRID



PUBLIC



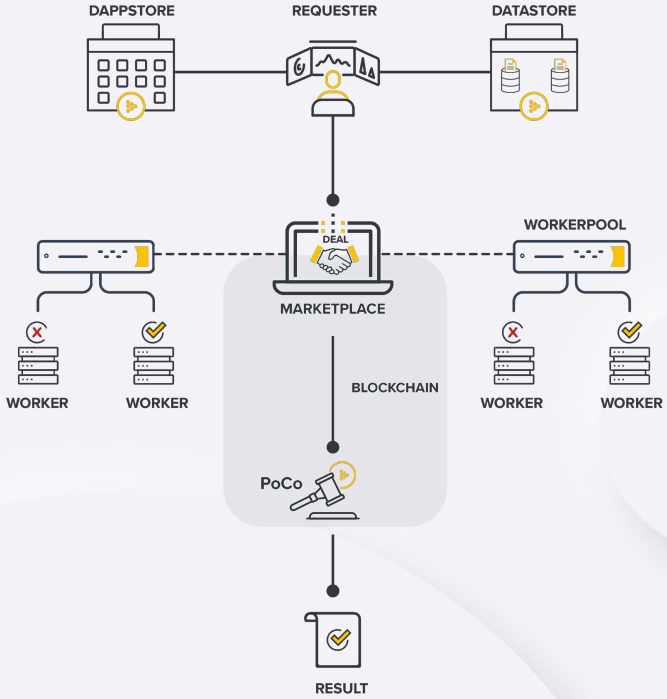
PUBLIC

Tasks execution walkthrough

Proof-of-Contribution (PoCo)

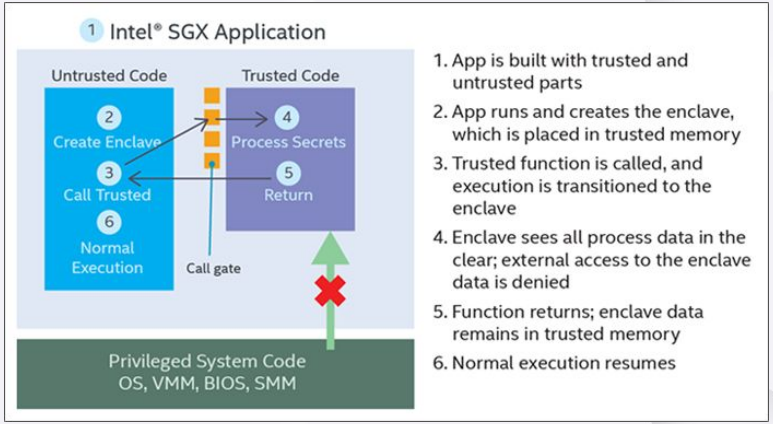
On-chain validation than an off-chain task was performed correctly.

1. One task = 4 orders, signed off-chain with an Ethereum wallet:
   - **`apporder`** signed by the developer
   - (**`datasetorder`** signed by the dataset provider)
   - **`workerpoolorder`** signed by a worker pool scheduler
   - **`requestorder`** signed by a requester
2. Orders are matched on-chain: `poco.matchOrders()`
   (Check signatures, parameters, balances, …)
3. PoCo seals a deal & workers start computing
4. Workers send result hash back to PoCo
5. PoCo compares results, manages reputation, triggers payments.



Trusted Execution Environment

- Secure part of a CPU with encrypted memory space
- Memory & Code protected from host (even root)
- Hardware based security (private key in silico)
- Can be remotely attested
- Available on hardware from various vendors (Intel SGX, AMD SEV)



Intel® Software Guard Extensions application execution flow.

Task Execution Model

Two types of tasks, with configurable confidence and privacy

Standard tasks

Run on untrusted resources, delegate trust to the blockchain

- Replication level depending on desired confidence
- Decentralized consensus
- On-chain reputation
- Staking & economic incentives
- Deterministic

TEE tasks

Run isolated within an Intel SGX TEE (Trusted Execution Environments)

+

- End-to-end encryption of data & result
- Enclave attestation proves that the task was run in TEE
- Result signature with enclave key: no need for replication
- Determinism not required

End-to-end data privacy preserving

Protecting data

at **rest and in transit**

→ **Encryption** (e.g. RSA, DES) and secure communication channels with TLS protocol.

Secure data during

its processing

→ **Trusted Execution Environments**

Data ownership Management

Strict control on its usage

Governance rules.

Auditable transactions

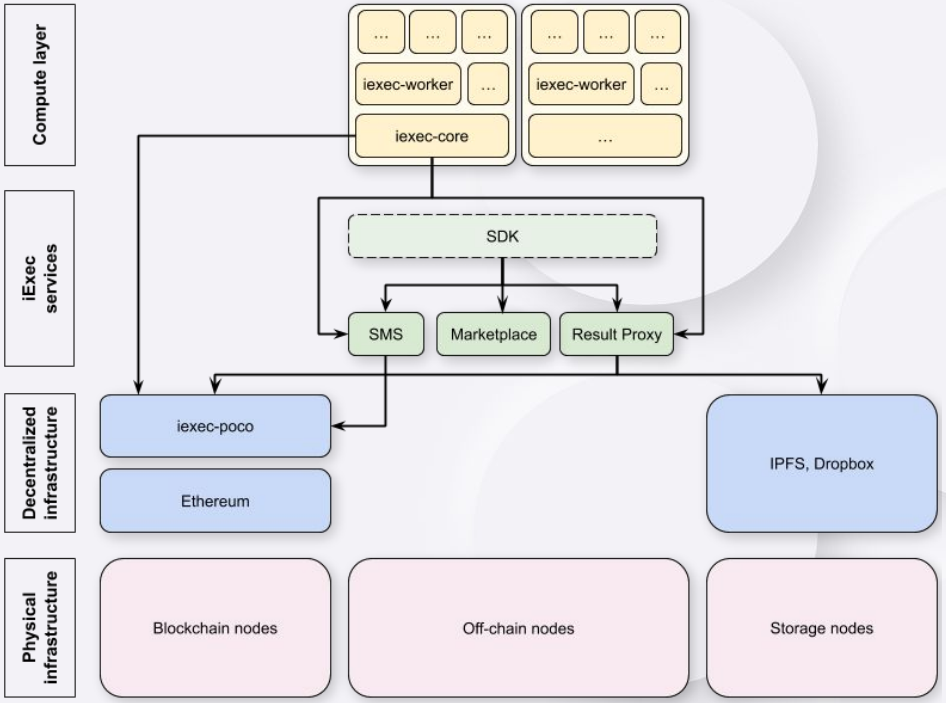
→ **Blockchain**

Architecture Viewpoint

Challenge

Always find the best tradeoff between on- and off-chain:

- **Safest: everything on-chain**
- **Fastest: everything off-chain**



Public vs consortium marketplace deployments

Public Marketplace

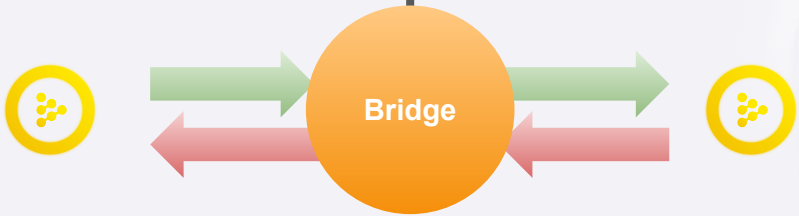
- Ethereum mainnet
- Goerli testnet

- Proof-of-Work
- Expensive gas cost
- Slow (15 to 30 s. per block)

Sidechain

- “Bellecour” (bridged w. Mainent)
- “Viviani” (bridged w. Goerli)

- Proof-Of-Authority
- No gas
- Faster (5 s. per block)

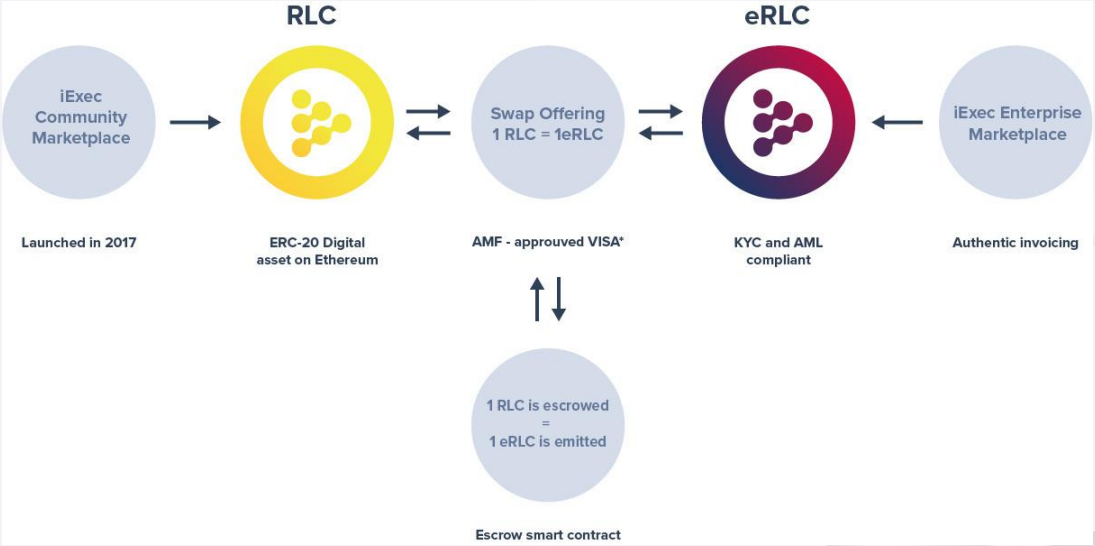


Bringing compliance to decentralized market place

AMF Visa

Many economic players (banks accountant) have strict compliance constraints

- Know Your Customer/Business
- Anti-Money Laundering - Terrorism Financing
- regulated marketplace with a dedicated token
- AMF ICO Visa (French SEC)



AUTORITÉ DES MARCHÉS FINANCIERS

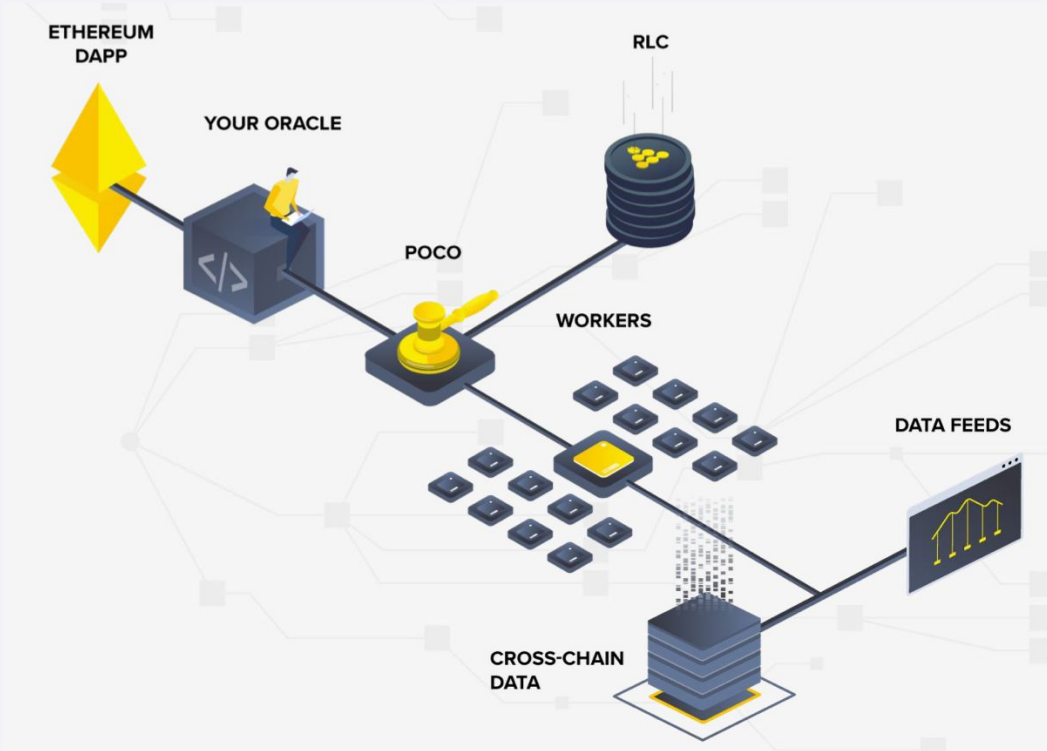
AMF

Some Use-Cases

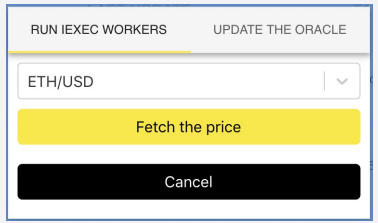
Trusted & Decentralized Oracle

- Oracle: Allows to fetch off-chain information.
- Decentralized: allows several data sources, anyone can update
- Trusted execution ensures that no one can tamper on chain updates
    - on-chain verification

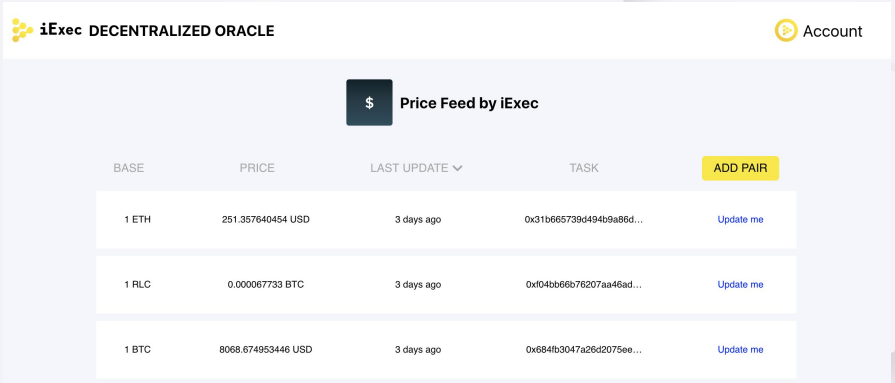
* **Use cases**: random generator (gaming), price feed (Defi), insurances, etc...



Doracle examples



KAIKO



https://blockchain.developers.iex.ec/oracles/

https://price-feed-doracle.iex.ec

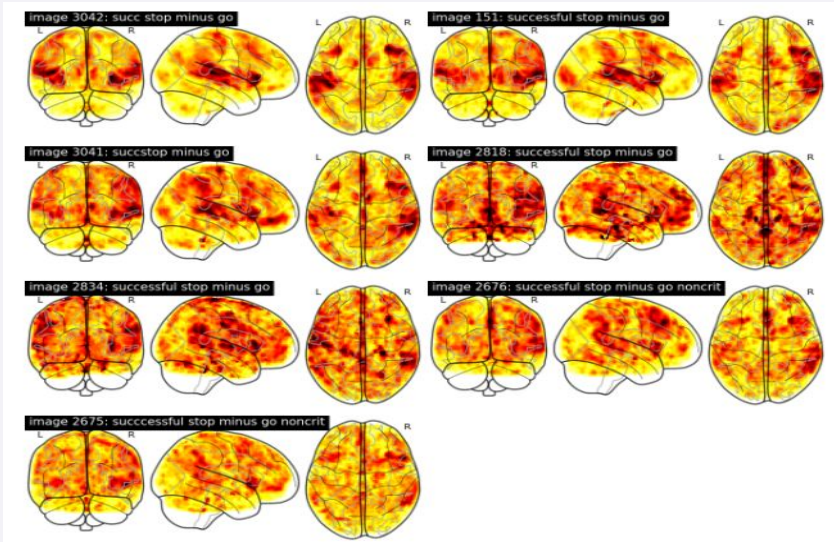
Use Case: confidential computing on private healthcare data

Researchers would like to analyze brain scans of patients. Patients would like their brain scans to remain private.

Application: NiLearn (a Python module for fast and easy statistical learning on NeuroImaging data)
Dataset: Brain scans
Computing power: CPU

Researchers can run statistical learning for diagnosis on the brain scans of patients. Researchers obtain their results **while patient data remains confidential**.

*Demoed at **RSA Conference 2019***.



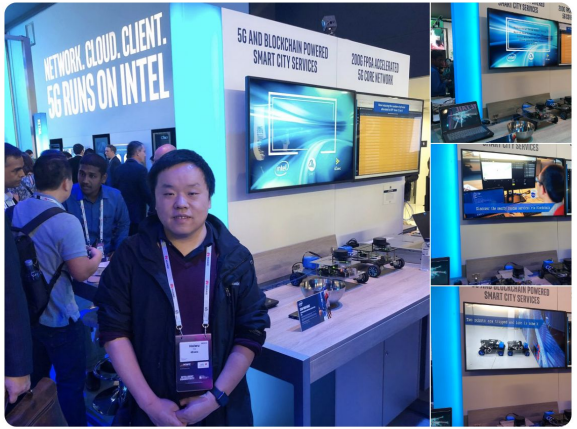
5G Smart City Services

Haiwu HE
@hehaiwu

Abonné

We are demonstrating our 5G smart city services based on blockchain tech on @Intel booth at #MWC2019 , come to meet @iEx_ec team.

Traduire le Tweet



11:44 - 25 févr. 2019 depuis Hall 3.10

22 Retweets **44** J'aime

22 44

www.software.intel.com

R&D and innovation

H2020 Ontochain **(6M€)**

Trusted, traceable and transparent ontological knowledge on blockchain

H2020 Datacloud **(5M€)**

Blockchain-based resources provisioning for Big Data pipelines

REDCHAIN JOINT-LAB (2021)

Confidentiality and scalability for Decentralized MArketplace

“Investment for the future” **(2M€)**

Development of a blockchain-based cloud solution for enterprises.

Academic collaborations

H2020 Ontochain

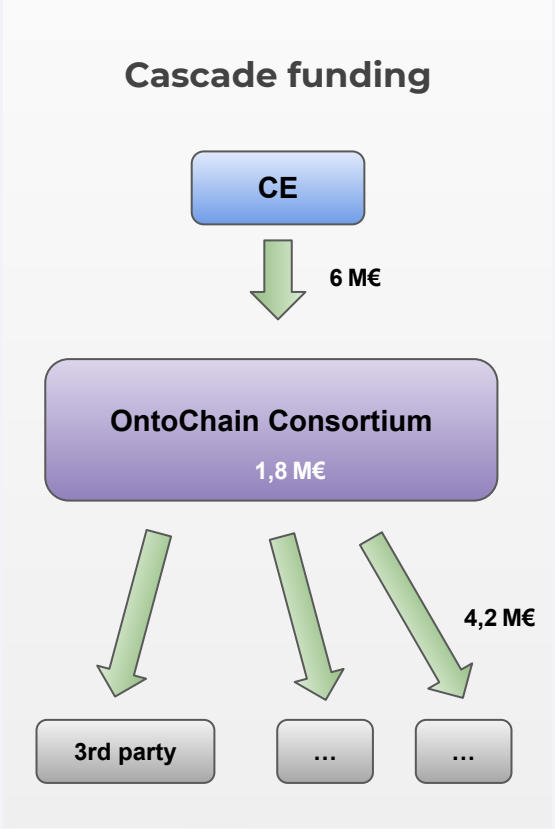
ONTOCHAIN

Building an ecosystem for trustworthy content handling & information exchange

NGI ONTO CHAIN

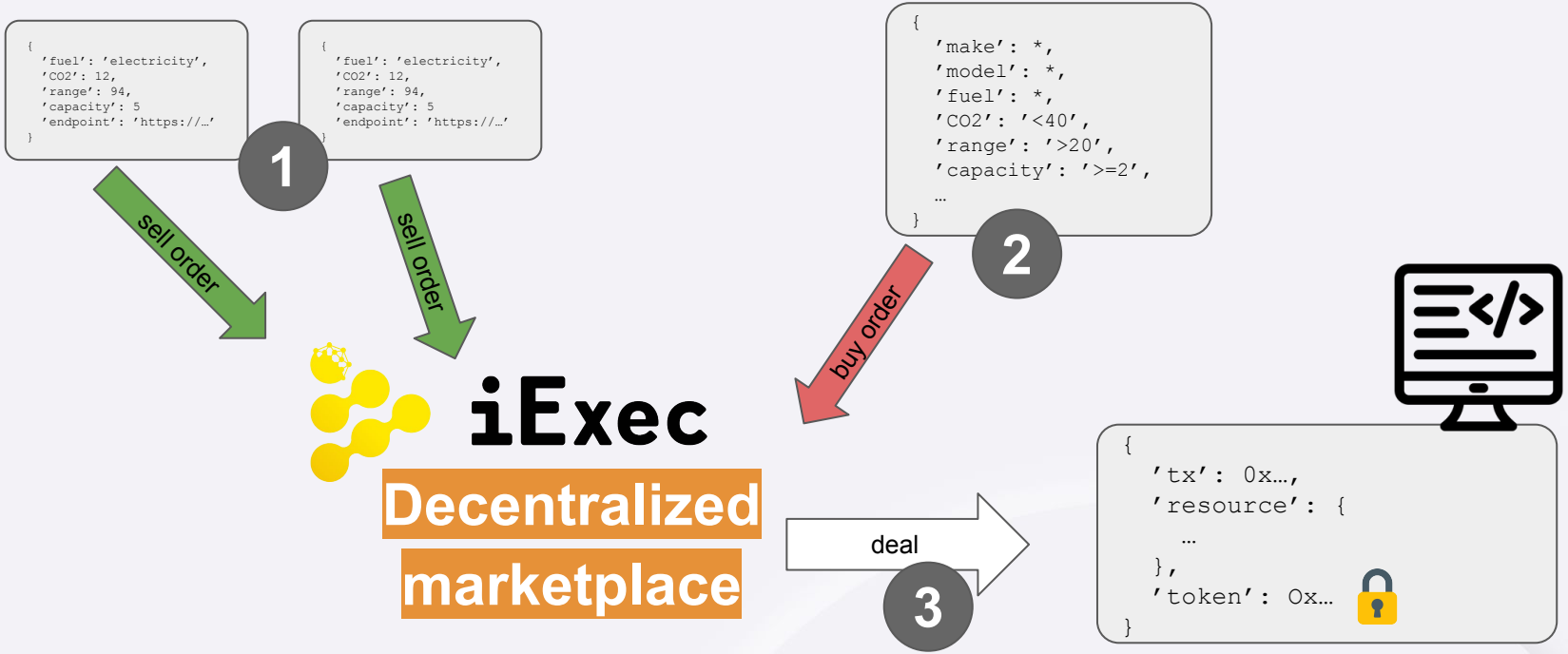
Keywords: Semantic Web, Oracles, Decentralized Identities, integration, applications

2020–2023



3 Open calls for participation

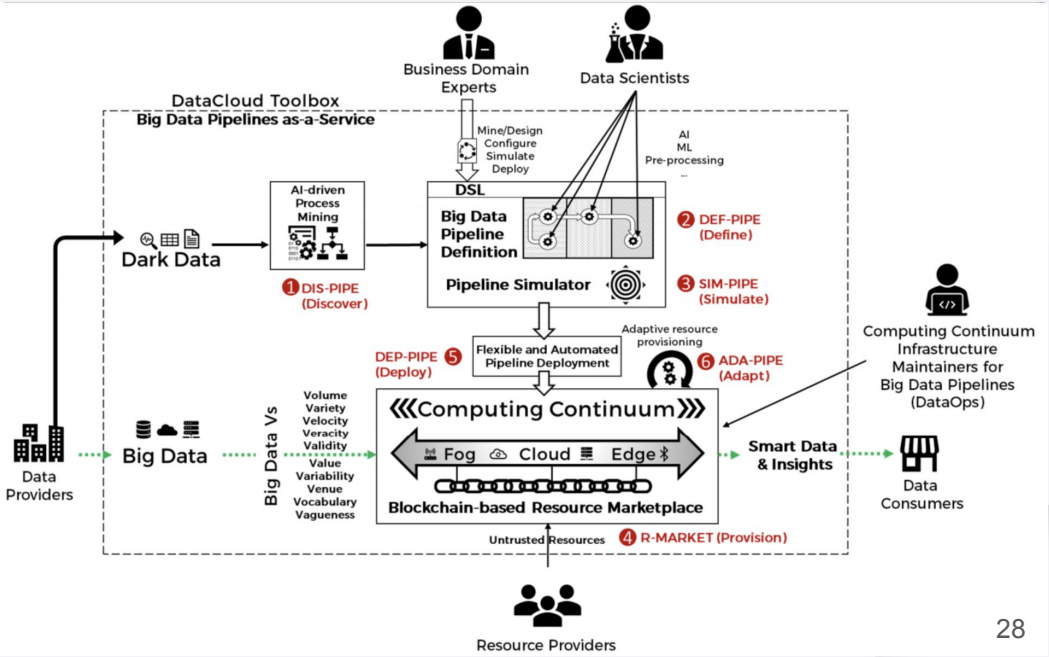
iExec + Ontochain: ontology + decentralized marketplace for everything



DataCloud: A novel paradigm for exploiting data pipeline

Towards a Cloud Computing Continuum

- Decentralized marketplace for resources in the cloud continuum
- PoCo performance & scalability
- On-chain SLA & QoS
- Workflow deployments (task dependencies)
- Services (time-based payment?)



Industrial collaborations & partnerships

Technical partnerships


Expertise

Startups

Standardisation

Blockchain advisor


iExec

Thank you

https://iex.ec

gf@iex.ec