A Trusted, Decentralized Marketplace for Cloud Computing

By **Anthony Simonet-Boulogne, PhD**
Research Scientist, iExec Blockchain Tech

Revisited by **Matthieu Bettinger**

iExec

INSA Lyon
Dec. 7th 2021

What we do

iExec provides an **open** and **decentralized** cloud computing **marketplace**.

Connects **providers** with **users**: anyone can trade **computing power**, **datasets**, and **applications**.

No need to trust iExec or anyone else: just **trust the blockchain** and the code.

Blockchain & Decentralisation

A decentralised, immutable and verifiable digital ledger consisting of transaction records distributed across many computers.

Decentralised

Immutable

Verifiable

Smart contracts?

Self-executing and self-enforcing programs that can read and write the state of a blockchain.

- ☑ Transparent
- ☑ Auditable
- ☑ Autonomous
- ✗ Hard to program
- ✗ Limited in size
- ✗ Often extremely critical
- ✗ **Cannot access external data**

```
contract Coin {
    address public minter;
    mapping (address => uint) public balances;

    function Coin() public {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) public {
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) public {
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
    }
  }
```

Blockchains

What they are

- ☑ A way for arbitrary people and organisations to collaborate without having to trust anyone.
- ☑ A tool for transparency and democracy.
- ☑ A platform for deploying unstoppable programs.

What they (usually) are not

- ✕ Fast
- ✕ Cheap
- ✕ Easy to program
- ✕ User friendly

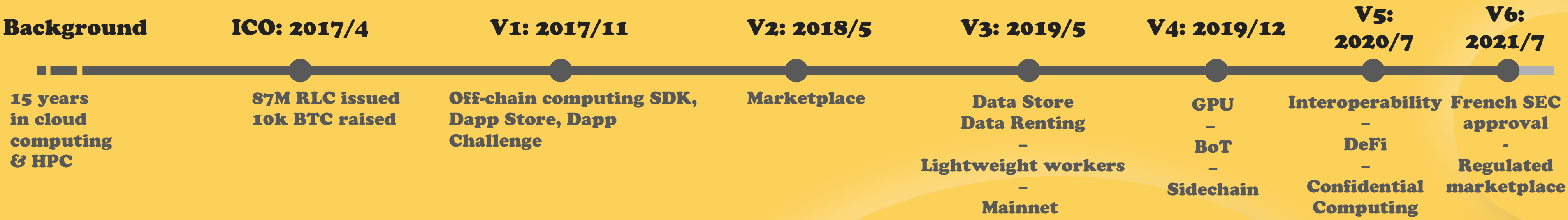
But we’re working on it ;-)

iExec history

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

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

Based in Lyon



Background

15 years in cloud computing & HPC

ICO: 2017/4

87M RLC issued
10k BTC raised

V1: 2017/11

Off-chain computing SDK, Dapp Store, Dapp Challenge

V2: 2018/5

Marketplace

V3: 2019/5

Data Store
Data Renting
–
Lightweight workers
–
Mainnet

V4: 2019/12

GPU
–
BoT
–
Sidechain

V5: 2020/7

Interoperability
–
DeFi
–
Confidential Computing

V6: 2021/7

French SEC approval
-
Regulated marketplace

A not so new idea...

We described a computational model based upon the classic science-fiction film, ***The Blob: a program that started out running in one machine, but as its appetite for computing cycles grew, it could reach out, find unused machines, and grow to encompass those resources.*** *In the middle of the night, such a program could mobilize hundreds of machines in one building; in the morning, as users reclaimed their machines, the "blob" would have to retreat in an orderly manner, gathering up the intermediate results of its computation. (This affinity for night-time exploration led one researcher to describe these as "vampire programs.")*

(John F. Shoch and Jon A. Hupp, 1982)

iExec allows individuals and enterprises to monetize their computing power, applications and datasets.

Computing power

Applications

Datasets

Why decentralise the cloud?

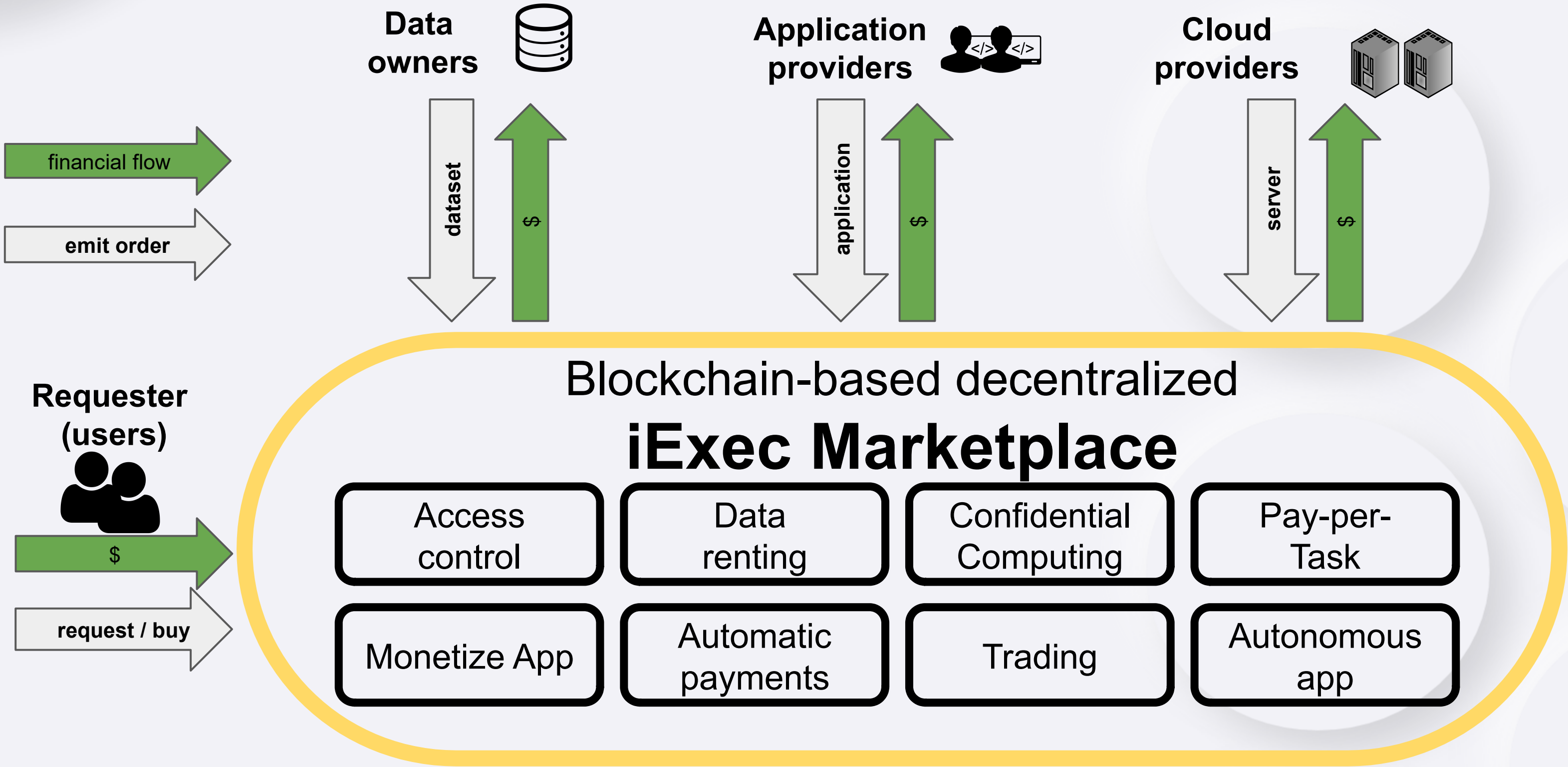
Centralized Computing

- ✗ Unfair pricing
- ✗ Vendor lock-in
- ✗ Limited transparency
- ✗ Limited accountability
- ✗ No provenance information
- ✗ Possible censorship

Decentralised Cloud Computing

- ☑ Market-based prices
- ☑ Fair competition between providers
- ☑ Smooth business agreements
- ☑ Complete execution history on the blockchain
- ☑ *Unstoppable* marketplace: censorship is impossible

iExec overview



Data owners

Application providers

Cloud providers

financial flow

emit order

dataset

$

application

$

server

$

Requester (users)

$

request / buy

Blockchain-based decentralized

iExec Marketplace

Access control

Data renting

Confidential Computing

Pay-per-Task

Monetize App

Automatic payments

Trading

Autonomous app

The iExec token: RLC

RLC is an ERC-20 utility token.

- ➜ RLC is necessary to access the iExec decentralised cloud
- ➜ Providers are paid with RLC
- ➜ RLC allows to build incentives in the network
- ➜ RLC creates a specific market for cloud computing

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

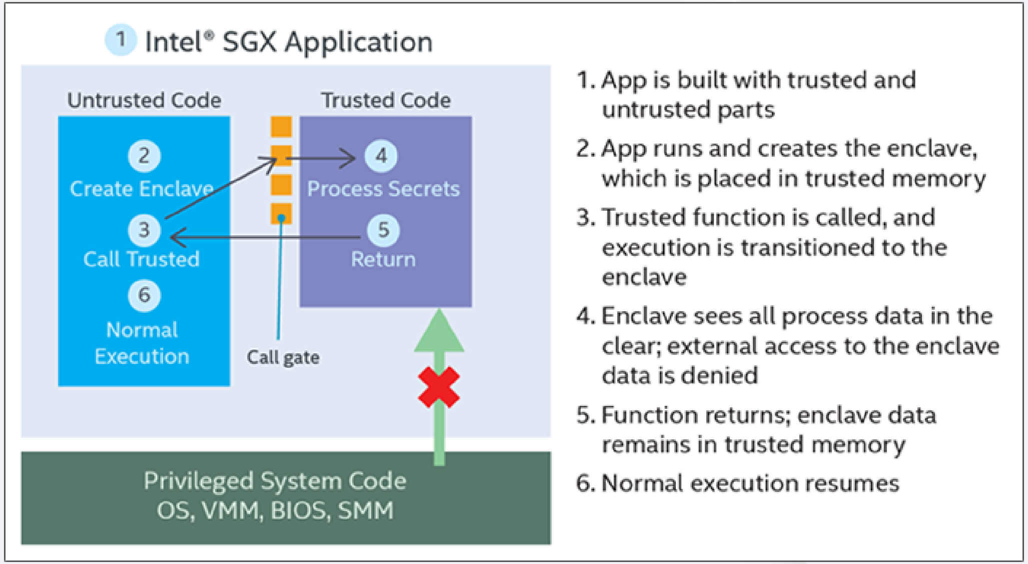
Run isolated within an Intel SGX TEE (Trusted Execution Environments)

+

- 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

Trusted Execution Environments?

- ➜ 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
- ➜ (Soon) available on hardware from various vendors

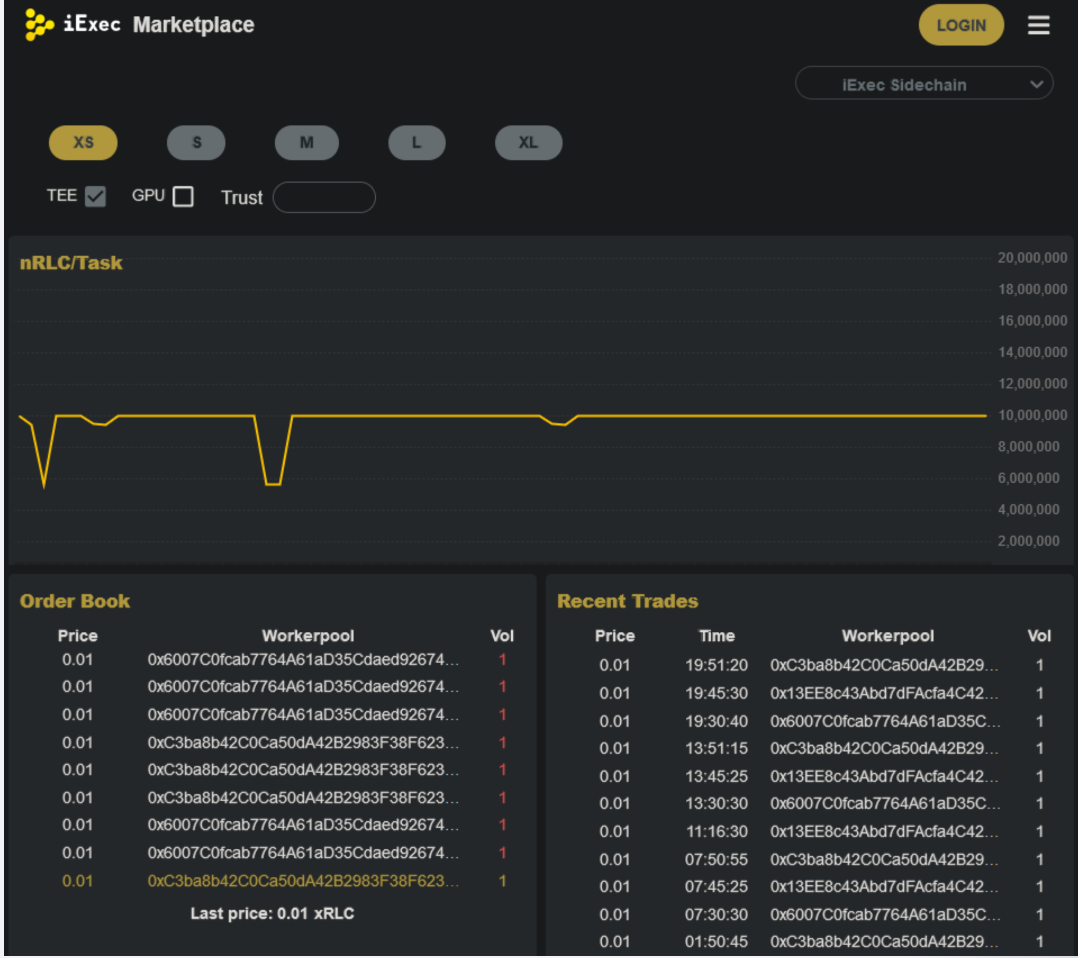


1. App is built with trusted and untrusted parts
2. App runs and creates the enclave, which is placed in trusted memory
3. Trusted function is called, and execution is transitioned to the enclave
4. Enclave sees all process data in the clear; external access to the enclave data is denied
5. Function returns; enclave data remains in trusted memory
6. Normal execution resumes

Intel® Software Guard Extensions application execution flow.

Components: iExec hub

- ➜ Managed by Smart contracts
- ➜ Repository of registered resources (dApps, workerpools, ...)
- ➜ Storage of task results and metadata
  - Task specifications
  - Execution details
  - Off-chain storage link



Order Book

Price	Workerpool	Vol
0.01	0x6007C0fcab7764A61aD35Cdaed92674...	1
0.01	0x6007C0fcab7764A61aD35Cdaed92674...	1
0.01	0x6007C0fcab7764A61aD35Cdaed92674...	1
0.01	0xC3ba8b42C0Ca50dA42B2983F38F623...	1
0.01	0xC3ba8b42C0Ca50dA42B2983F38F623...	1
0.01	0xC3ba8b42C0Ca50dA42B2983F38F623...	1
0.01	0x6007C0fcab7764A61aD35Cdaed92674...	1
0.01	0x6007C0fcab7764A61aD35Cdaed92674...	1
0.01	0xC3ba8b42C0Ca50dA42B2983F38F623...	1

Last price: 0.01 xRLC

Recent Trades

Price	Time	Workerpool	Vol
0.01	19:51:20	0xC3ba8b42C0Ca50dA42B29...	1
0.01	19:45:30	0x13EE8c43Abd7dFAcfa4C42...	1
0.01	19:30:40	0x6007C0fcab7764A61aD35C...	1
0.01	13:51:15	0xC3ba8b42C0Ca50dA42B29...	1
0.01	13:45:25	0x13EE8c43Abd7dFAcfa4C42...	1
0.01	13:30:30	0x6007C0fcab7764A61aD35C...	1
0.01	11:16:30	0x13EE8c43Abd7dFAcfa4C42...	1
0.01	07:50:55	0xC3ba8b42C0Ca50dA42B29...	1
0.01	07:45:25	0x13EE8c43Abd7dFAcfa4C42...	1
0.01	07:30:30	0x6007C0fcab7764A61aD35C...	1
0.01	01:50:45	0xC3ba8b42C0Ca50dA42B29...	1

Components: Workerpool

- ➜ Composed of a scheduler and multiple workers
- ➜ Incentives:
  - Staking
  - Reputation

- ➜ Scheduler objective:
  - Listen to incoming work
  - Distribute work fairly among workers
- ➜ Worker objective:
  - Correctly execute tasks given by the scheduler

Components:
Secret Management Service

➜ Secured inside in a Trusted Execution Environment (not yet, but in V7)

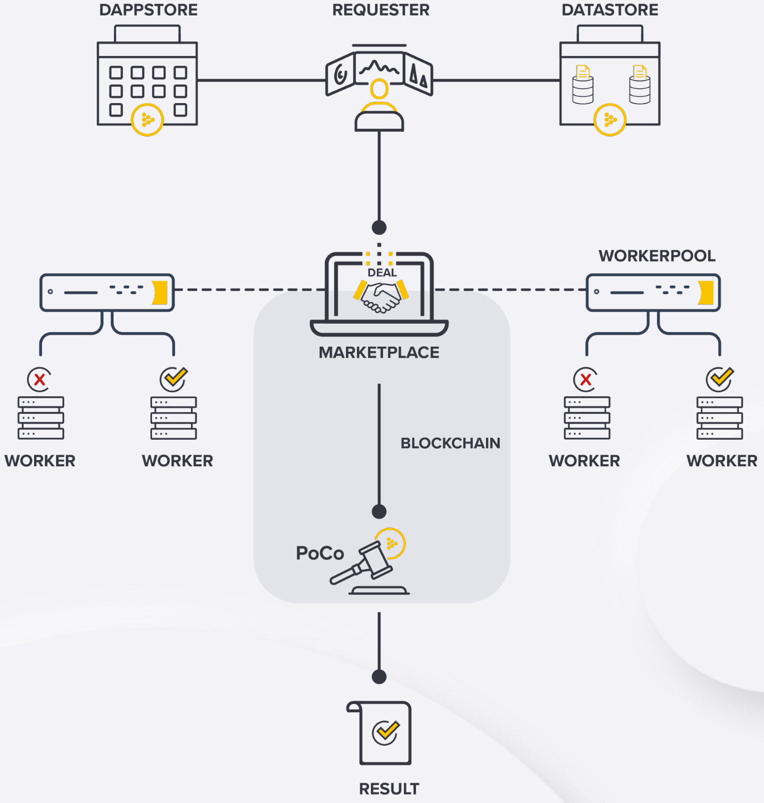
➜ Stores secrets of stakeholders:
  - Dataset decryption keys
  - Input files decryption keys
  - Output files/Results encryption keys

➜ Attests TEE workers

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.



Adjusting trust: Sarmenta Voting

- Deterministic execution replicated **N** times: only one correct result exists

- Given **R** distinct results (1≤**R**≤**N**):
  - For each result **r**, obtained by **n** among **N** workers:
    - Probability that **r** is correct and all others are false

- User-defined threshold **t**:
  - If no proposed result has Crt(**r**)>**t**
  - Then more workers are dispatched

$$Cr_t(r) = \frac{\tilde{P}_t(r)}{1 + \sum_{h \in R_t} \tilde{P}_t(h)}$$

https://github.com/iExecBlockchainComputing/PoCo/blob/v5/audit/docs/iExec_PoCo_and_trustmanagement_v1.pdf

iExec Research Projects

H2020 ONTOCHAIN

Building an ecosystem for trustworthy content handling & information exchange

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

2020−2023

H2020 DATACLOUD

Enabling the Big Data Pipeline Lifecycle on the Computing Continuum

Keywords: Fog/Edge Computing, Big Data pipelines, self-* cloud computing, Industry 4.0

2021−2024

ANR RedChainLab

Scalable, trusted and privacy preserving decentralized marketplaces

Joint laboratory between the **DRIM research team** (LIRIS, CNRS) and **iExec**

Keywords: blockchain, decentralized cloud computing, edge computing, security, TEE, Federated Learning

2021−2024

Try us!

https://developers.iex.ec/

https://iex.ec/grants/

Join us!

https://iexec.flatchr.io/

https://gitcoin.co/explorer?
network=mainnet&idx_status=open&applicants=ALL&key

iExec

Anthony Simonet-Boulogne
anthony@iex.ec