iExec

Building a Decentralized Marketplace: Challenges & Lessons Learnt

P2P Festival

Gilles Fedak
Researcher, Entrepreneur
gf@iex.ec

Agenda

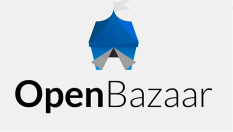
- Introduction to decentralized marketplace
- The iExec example: a marketplace for trading computing resources
- New usages/new business models
- Implementation challenges
- Conclusion

Decentralized Marketplaces on Ethereum

Decentralized marketplace:

truly peer-to-peer transactions without centralized authorities taking their fees.

blockchain and smart contracts to verify sellers/buyers and proceed with payments.



DM are DApps: censorship-resistant, autonomous, transparent, unstoppable, secure, resilient

Decentralized vs centralized marketplace

Marketplace Feature	Blockchain-Based Decentralized Marketplace	Traditional E-Marketplace
Trust through contract enforcement	Distributed validation, including proof-of-work mechanisms or proof-of-stake mechanisms. The network enforces the contract between seller and buyer. The network validates reputation ratings, including reviews and feedback mechanisms.	Third parties (such as a bank, certifying authority, promissory note, transfer systems, or other forms of contractual mechanisms). Usually controlled by the firm. Potential for significant alteration.
Transaction time	Can be instantaneous due to fast network validation. Delays can be mitigated using proof-of-stake/ proof-by-consensus algorithms.[3,19]	Promissory note, letter of credit, or acceptance of credits that can take a long time.
Value	The network can reward participants with tokens or by accepting third-party tokens.	Banking systems (such as national exchanges, currency, and underwriters).
Privacy and security	Identity is not disclosed on the network. Tracking transactions can be facilitated, though with difficulty. Transaction details can be hidden behind layers of encryption. Cost of tampering with the network's validation mechanism is high.[a]	Identity fully disclosed in the marketplace. As secure as the network's components.

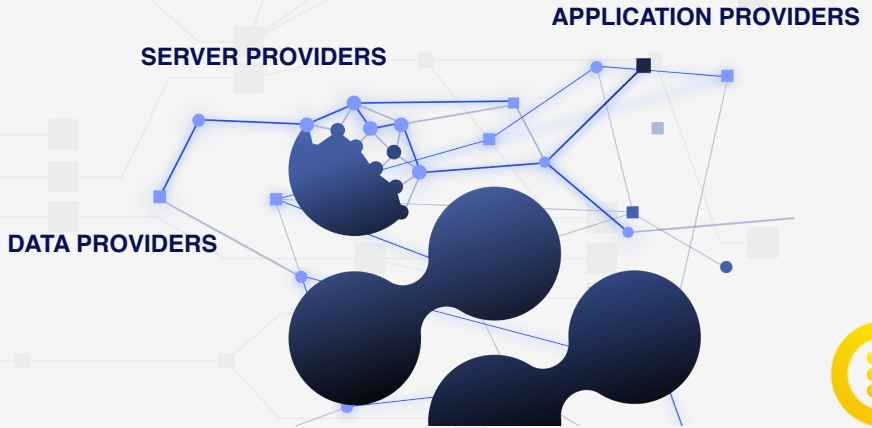
Decentralized Blockchain-Based Electronic Marketplaces, Hemang Subramanian
Communications of the ACM, Vol. 61 No. 1, Pages 78-84

Blockchain-based Decentralized Cloud Computing

- Decentralized marketplace for trading computing resources (servers, applications, datasets)
- Use Ethereum to advertise/provision computing resources
- Providers can interact in a P2P way, without central authority

Why Does it Matter ?

- Decentralized applications need an infrastructure
- Cheaper, greener, more efficient than traditional centralized Cloud



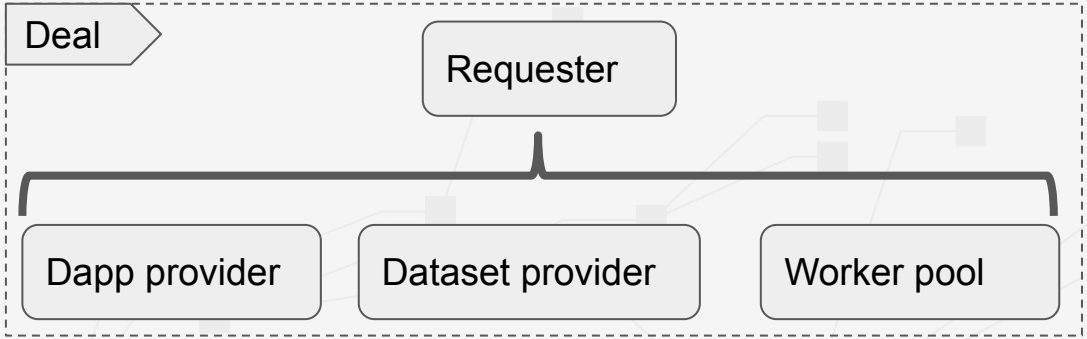
The iExec Token: RLC

Token usage

- The RLC Token is the only way to access the iExec decentralized marketplace
- Providers are paid with RLC
- Allows to build incentives in the network.
- 87 millions emitted and sold during ICO (April 2017)

iExec Walkthrough

Transaction Model



Transaction happens for the execution of a task or a bag-of-tasks (BoT)

- Requesters asks for the execution of task (UserOrder)
- Provider emits counterpart orders (DappOrder, DataOrder, PoolOrder)
- Deal is sealed and registered in the blockchain
- Pricing model-> Pay-per-Task

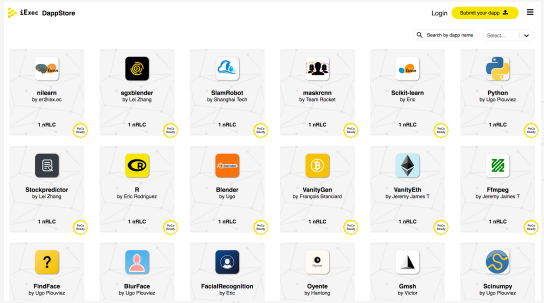
Proof-of-Contribution

staking + reputation + result certification:

- A confidence threshold is associated with each requested execution
- Workers have a reputation
- Before executing a task, workers commit a security deposit (stake)
- The execution confidence threshold is computed by comparing results and computing a function of the credibility and stake
- Task is duplicated as long as the confidence threshold is not met
- Workers who computed an erroneous results loose their stake
- Workers who correctly compute gains the payments + the losers' stake
- Reputation is adjusted

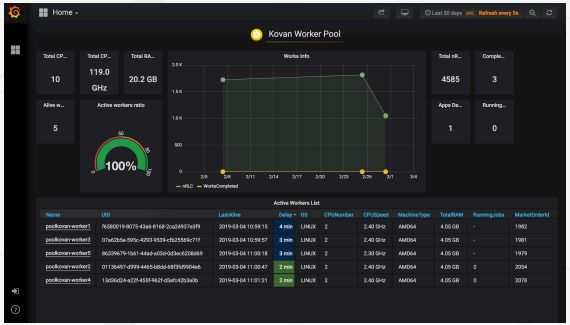
Decentralization != P2P

iExec runs some centralized services/components



Dappstore

- curated list of Dapps
- billing



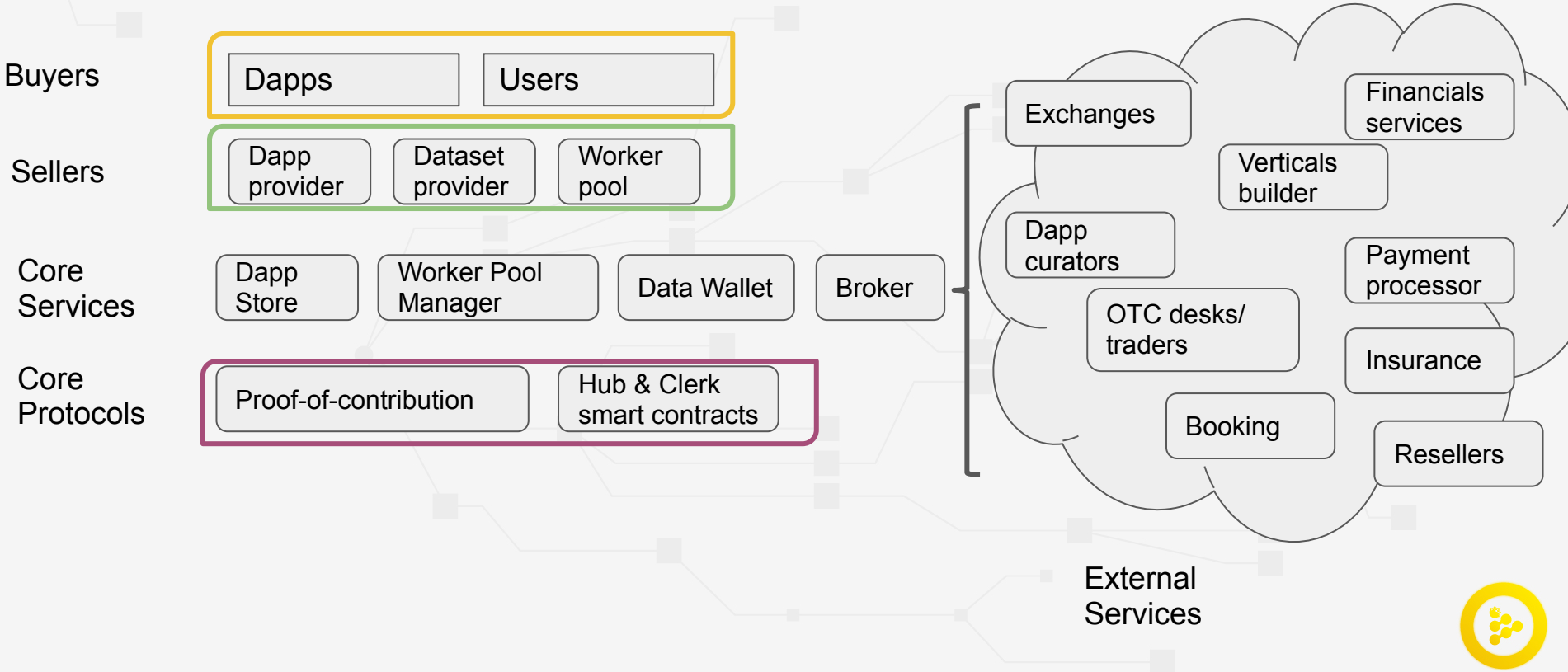
Worker pool manager

- schedule tasks to workers
- fees

Anyone can run these services, and are encouraged to do so !

- Builds verticals where expertise is required: IA, fintech, CGI, etc.
- Public worker pools for volunteer Internet PC

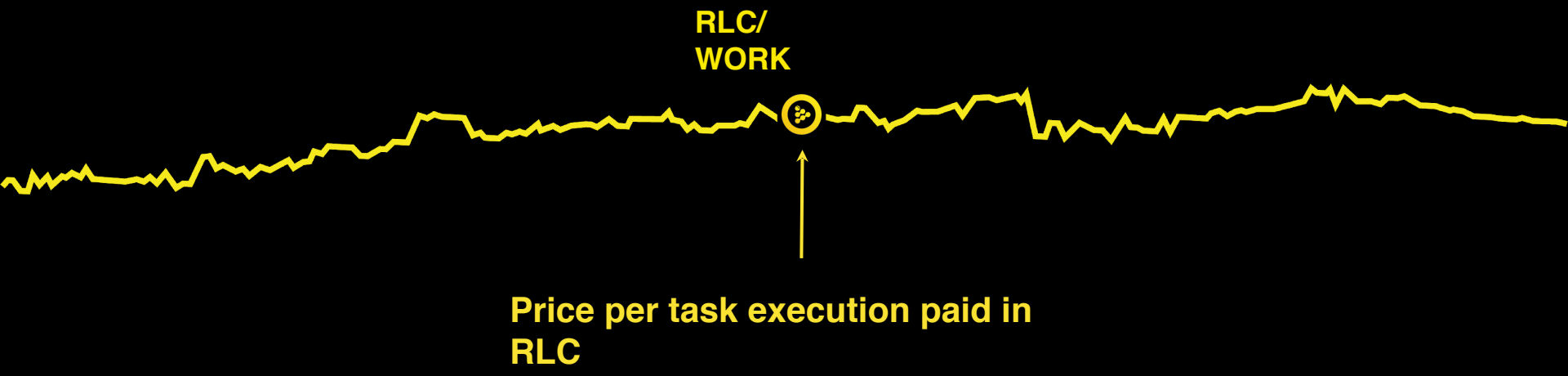
Towards Market Networks



New Usages

Allows to trade computing power as a commodity

Allows companies and individuals to monetize their servers/PCs



iExec Marketplace

Account

Cat1 | Cat2 | Cat3 | Cat4 | TEE

nRLC/WORK

Order Book

Hash	Price	Workerpool	Trust	Volume
0xba0c8f3c617d7…	15	0x4E61C418cFcF…	1	1
0x5080a6a73765…	14	0x4E61C418cFcF…	1	1
0xb69e283a418b…	12	0x4E61C418cFcF…	1	1
0x22c54610c5efe…	12	0x4E61C418cFcF…	1	1
0xcbddbfb16e108…	12	0x4E61C418cFcF…	1	1
0x219fbe85c3da0…	11	0x4E61C418cFcF…	1	1
0xf9b087f07356e…	10	0x4E61C418cFcF…	1	1
0x84a6290086f44…	9	0x4E61C418cFcF…	1	1
0x77a9f9ddd6a24…	9	0x4E61C418cFcF…	1	1
0x301ef5b152b2e…	9	0x4E61C418cFcF…	1	1
0xc9988053eb08…	8	0x4E61C418cFcF…	1	1

Last 8 nRLC ↘

Hash	Price	Requester	Trust	Volume
0xb5242cdfd8998…	3	0xF048eF3d7E3B…	0	1
0x13219f58a6e19…	3	0xF048eF3d7E3B…	0	1
0x4d47803724fad…	3	0xF048eF3d7E3B…	0	1
0xd6706b3e6294…	2	0xF048eF3d7E3B…	0	1
0xf84a1a96069af…	2	0xF048eF3d7E3B…	0	1
0x4f5bf7442f6712…	2	0xF048eF3d7E3B…	0	1
0xc7698012d600…	1	0xF048eF3d7E3B…	0	1
0x1e5eee5706bb…	1	0xF048eF3d7E3B…	0	1
0x6ad4fb9618763…	1	0xF048eF3d7E3B…	0	1
0x50dd517a9de8…	1	0xF048eF3d7E3B…	0	1
0x115f6aecf41ec2…	1	0xF048eF3d7E3B…	0	1

Recent Trades

ID	Price	Time	Workerpool	Volume
0xa9ecd2973b7…	8	11:18:32	0x4E61C418cF…	1
0x86f54eaf5262…	17	16:22:44	0x4E61C418cF…	1
0x33e7187395c…	15	13:17:20	0x4E61C418cF…	1
0x8d0b2b1c112…	15	13:14:56	0x4E61C418cF…	1
0x0e499df6461…	18	13:11:56	0x4E61C418cF…	1
0xb1096448c72…	9	13:04:44	0x4E61C418cF…	1
0x5e2d4f90476…	19	13:03:32	0x4E61C418cF…	1
0x9de7a092499…	8	12:57:16	0x4E61C418cF…	1
0xbfda9a95add…	19	12:54:16	0x4E61C418cF…	1
0x344d2828fb4…	8	12:51:52	0x4E61C418cF…	1
0x96f2c3ad592…	15	11:09:16	0x4E61C418cF…	1
0xbc0de055b72…	8	12:24:32	0x4E61C418cF…	1
0x316cfa55c7c6…	15	12:12:16	0x4E61C418cF…	1
0x5ee0700069e…	15	12:09:52	0x4E61C418cF…	1
0x1a619be8feb…	18	12:09:16	0x4E61C418cF…	1
0xd2170a53f0d…	10	17:37:28	0x4E61C418cF…	1
0x17ed3ab24c6…	10	17:36:52	0x4E61C418cF…	1
0xefa2eeb18e5…	10	17:36:16	0x4E61C418cF…	1
0x123d3971c22…	12	17:35:40	0x4E61C418cF…	1
0xd9d6c71dcdf7…	13	17:34:44	0x4E61C418cF…	1

My Trades

My Open Request Orders | My Open Workerpool Orders

ID	Price	Time	Workerpool	Volume
0xa9ecd2973b71b0b14b3293af5c0d9031bee0744a76d994…	8	11:18:32	0x4E61C418cFcF080DbCA9544AAd64572e68BD9802	1
0xb1096448c72f9df742f805b5fe657e49b5885de1f2a9340c…	9	13:04:44	0x4E61C418cFcF080DbCA9544AAd64572e68BD9802	1

Fill Market Order

Place Limit Order

Order Hash: * 0xc9988053eb0809fa5b8ac0ed075e967dd6(

Request Order Hash: * 0xb5242cdfd8998dcf04cc6062909208c816a2d52

Volume: * 1

Volume: * 1

Dapp Address: * or name...

Workerpool address: *

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

Buy computation at market price

Sell computation at market price

iExec End-to-End Trusted Execution with Intel SGX

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

- SDK that provides full end-to-end privacy preserving computation
  - for application/input/results
  - guarantee execution integrity
  - provide on-chain enclave execution attestation

Dataset Wallet

Renting data-sets while keeping full ownership

Possible thanks to Trusted Execution

Needs Application certification

Trained NN

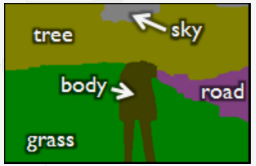
Input

+

TensorFlow

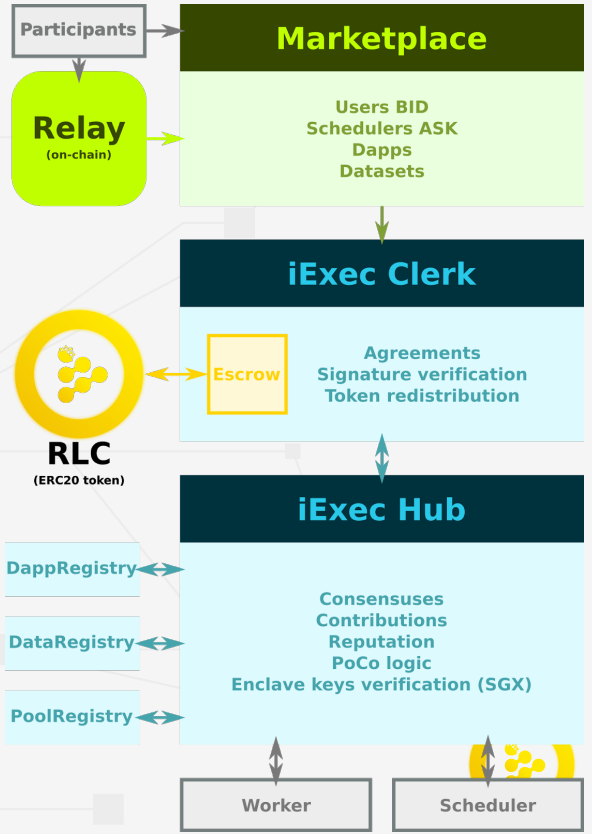
+

Output



Open Decentralized Brokering

- Address scalability problem of the marketplace
- Decouple brokering: 0x-like protocol
  - sealed deals are stored on-chain
  - market management is done off-chain
- Reduce gaz consumption
- Allows for more complex order book management
  - bid/ask
  - In the future: OTC, discount, subscription etc...



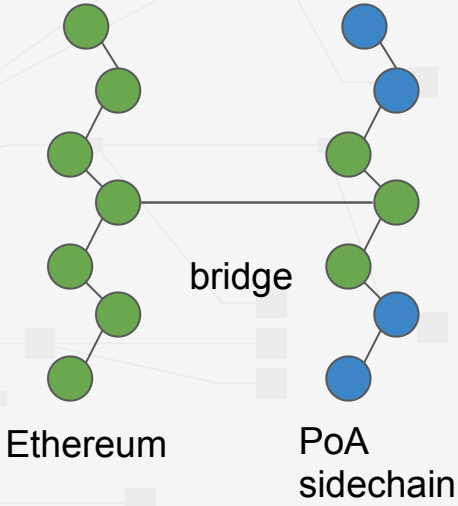
Domain Specific Sidechain (DSS)

Problem:

- Implementing PoCo/MP on mainet is costly (#tx)
- Idea: how better we can be if we sacrifice decentralization for performance ?

Solution:

- Store information needed to establish the consensus on a sidechain with PoA
- Bridge mainchain/sidechain with Parity bridge
- Later: zksnarks



Governance

Hybrid blockchain design:

- Mainnet stores values (tokens), governance and bridges
- Domain Specific Sidechain which is optimized for running the decentralized marketplace stores deals and consensus results

Governance issues:

- Who are the nodes allowed to maintain the DSS ? How to upgrade the consensus protocol? How to tune the reward/punishment ?
- Those questions should be handled by the stakeholders: token holders, traders, users, providers, service operators, etc.

Conclusion

Decentralized marketplace might be the future blockchain killer apps!

Still significant challenges to achieve scalability, reasonable cost overhead, and performance.