基于区块链技术的分布式云计算

贺海武[1]　　Gilles Fedak[2]
haiwu.he@cnic.cn, gilles.fedak@inria.fr

1 中国科学院计算机网络信息中心(CNIC/CAS)
2 法国国家计算机及自动化研究院(INRIA)

区块链

- 狭义

  区块链是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账

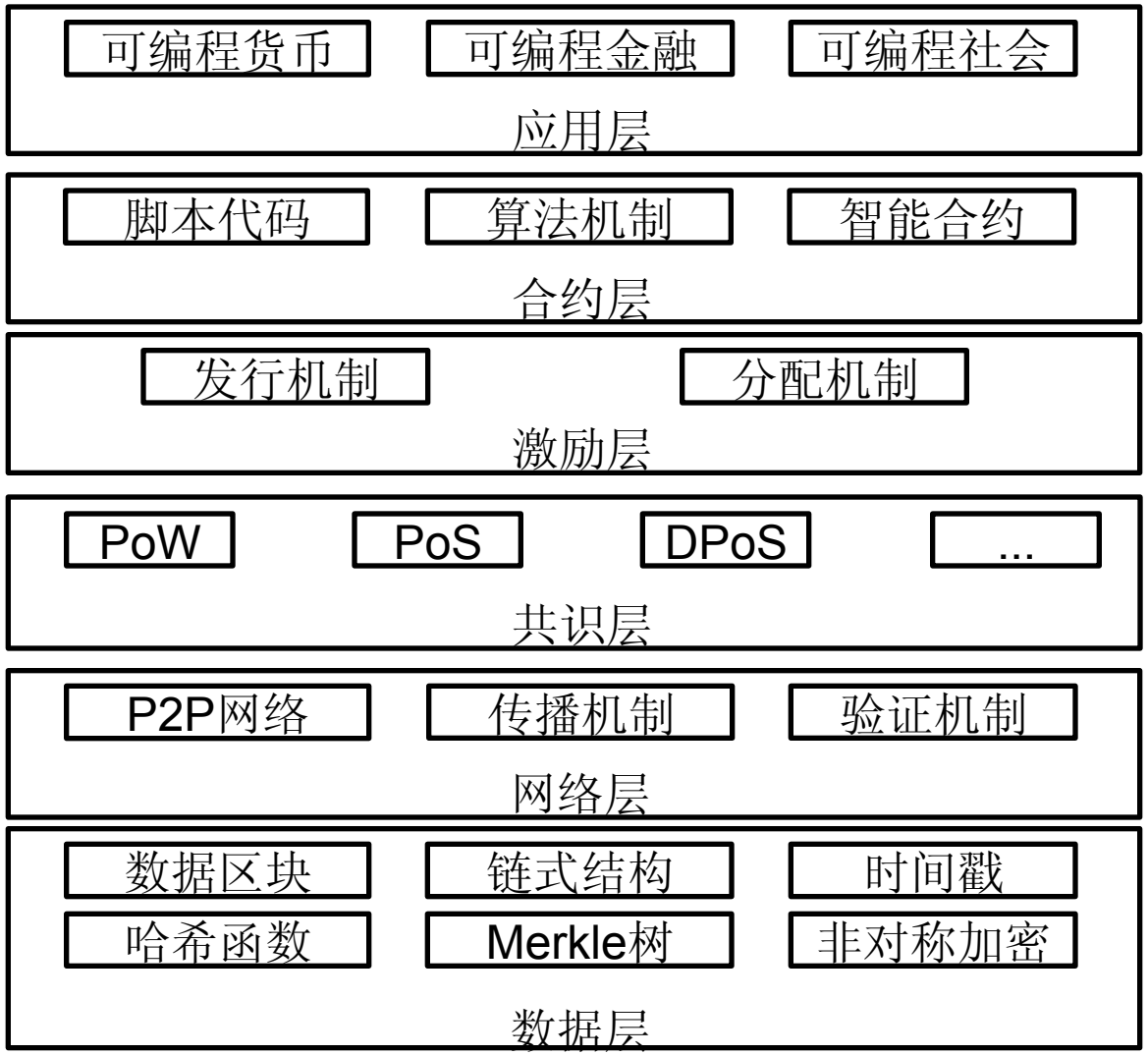
- 广义

  区块链技术是利用加密链式区块结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用自动化脚本代码（智能合约）来编程和操作数据的一种全新的去中心化基础架构与分布式计算范式

- 特点：

  去中心化、时序数据、集体维护、可编程、安全可信

区块链的基础模型与关键技术



区块链基础架构模型

- 数据层
- 网络层
- 共识层
- 激励层
- 合约层
- 应用层

区块链的现存问题

- 安全问题
  - 基于 PoW 共识过程的区块链主要面临的是 51 % 攻击问题
  - 基于 PoS 共识过程的区块链主要面临N@S (Nothing at stake) 攻击问题

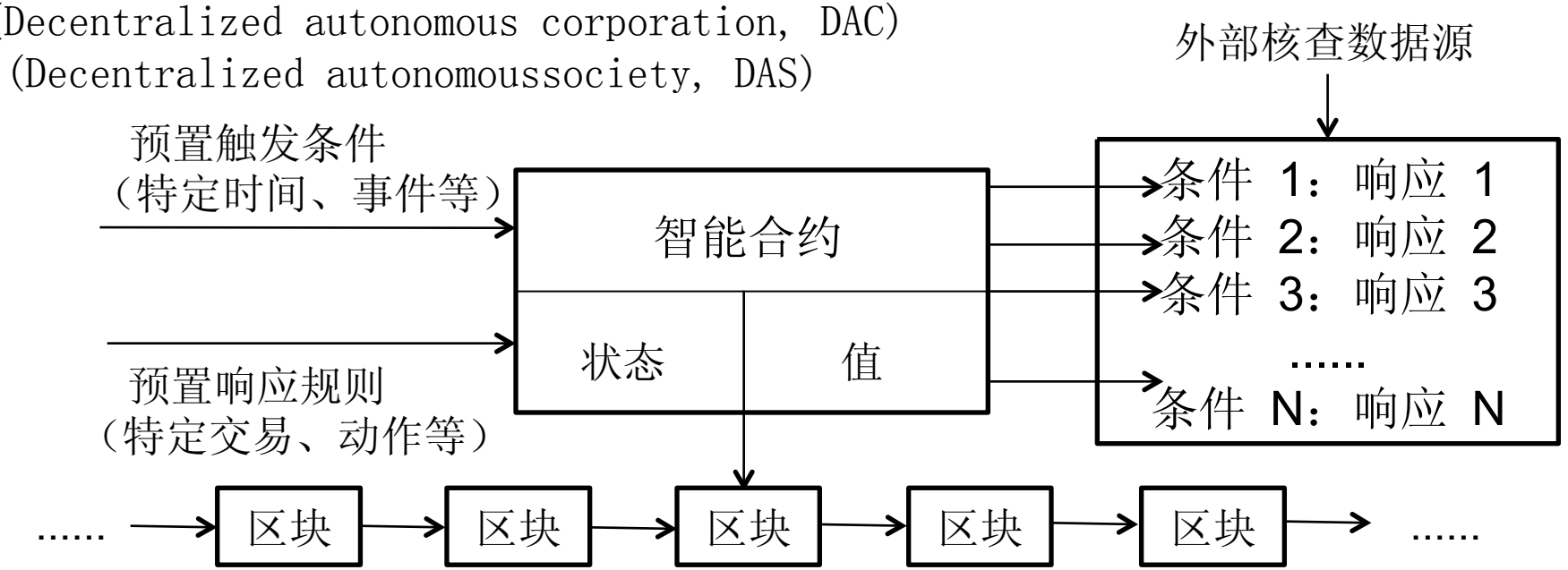
- 效率问题
  - 区块膨胀问题
  - 交易效率问题
  - 交易确认时间问题

- 资源问题
  - 算力资源、电力资源

基于区块链的智能合约

- 由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的计算机程序，能够实现主动或被动的处理数据，接受、储存和发送价值，以及控制和管理各类链上智能资产等功能.
- 特征：自治、自足、去中心化

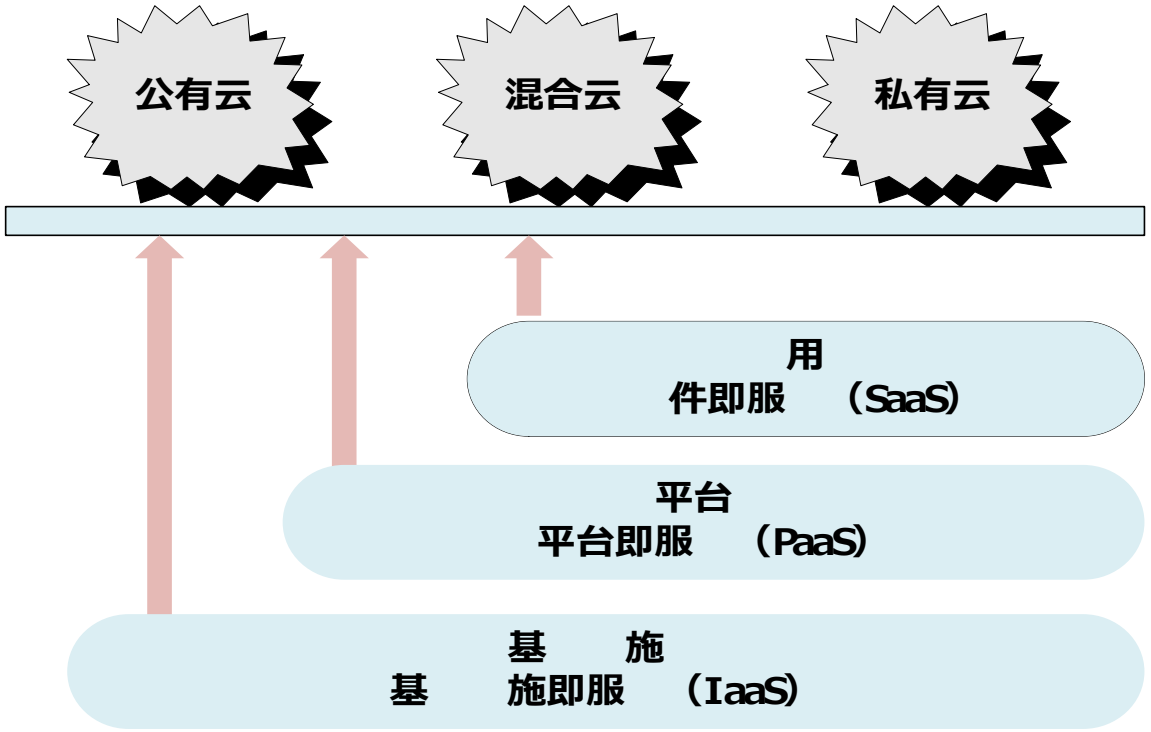
去中心化应用 (Decentralized applica-tion, Dapp)
去中心化自治组织 (Decentralized autonomous organization, DAO)
去中心化自治公司(Decentralized autonomous corporation, DAC)
去中心化自治社会 (Decentralized autonomoussociety, DAS)



智能合约的运作机理

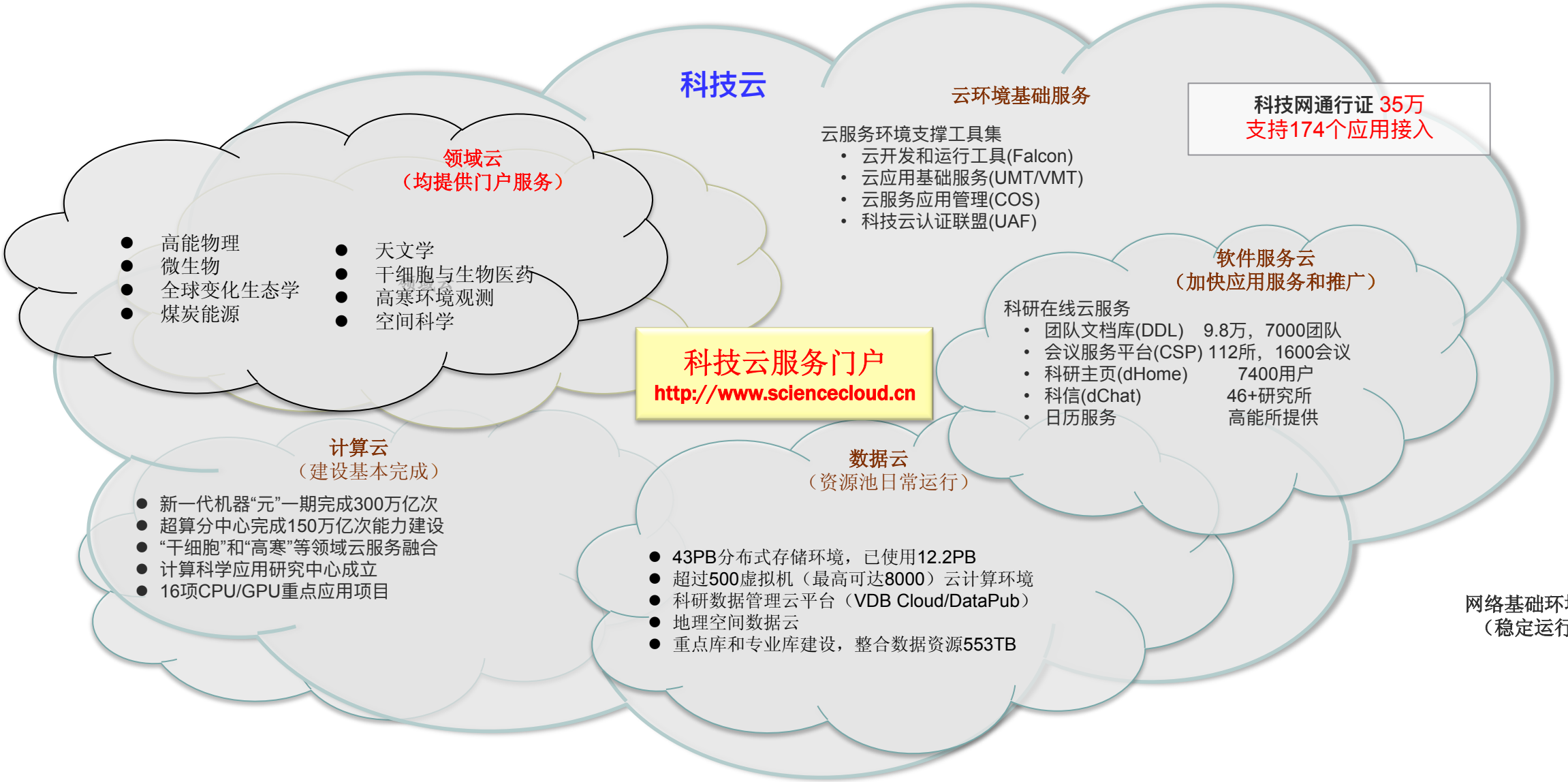
云计算

- 云计算实现了通过网络提供可伸缩的、廉价的分布式计算能力，用户只需要在具备网络接入条件的地方，就可以随时随地获得所需的各种IT资源



云计算的服务模式和类型

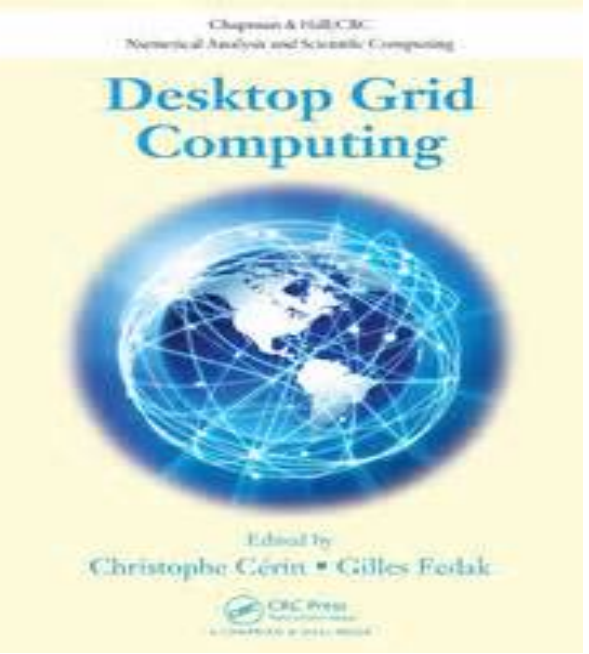
中国科学院科技云


科技云
领域云
（均提供门户服务）
高能物理
微生物
全球变化生态学
煤炭能源
天文学
干细胞与生物医药
高寒环境观测
空间科学
云环境基础服务
云服务环境支撑工具集
云开发和运行工具(Falcon)
云应用基础服务(UMT/VMT)
云服务应用管理(COS)
科技云认证联盟(UAF)
科技网通行证 35万
支持174个应用接入
软件服务云
（加快应用服务和推广）
科研在线云服务
团队文档库(DDL) 9.8万，7000团队
会议服务平台(CSP) 112所，1600会议
科研主页(dHome) 7400用户
科信(dChat) 46+研究所
日历服务 高能所提供
科技云服务门户
http://www.sciencecloud.cn
计算云
（建设基本完成）
新一代机器“元”一期完成300万亿次
超算分中心完成150万亿次能力建设
“干细胞”和“高寒”等领域云服务融合
计算科学应用研究中心成立
16项CPU/GPU重点应用项目
数据云
（资源池日常运行）
43PB分布式存储环境，已使用12.2PB
超过500虚拟机（最高可达8000）云计算环境
科研数据管理云平台（VDB Cloud/DataPub）
地理空间数据云
重点库和专业库建设，整合数据资源553TB
网络基础环境
（稳定运行）

源起:桌面网格计算（志愿计算）

使用Internet上的空闲资源执行分布式或并行应用：

- 成熟技术 （SETI@HOME, XtremWeb）
- 实现高级属性：安全, 虚拟化, 服务质量(QoS)
- 众多应用: 金融, 生物制药, 化学, 高能物理等…
- 欧洲桌面网格设施 European Desktop Grid Infrastructure
  - http://desktopgridfederation.org

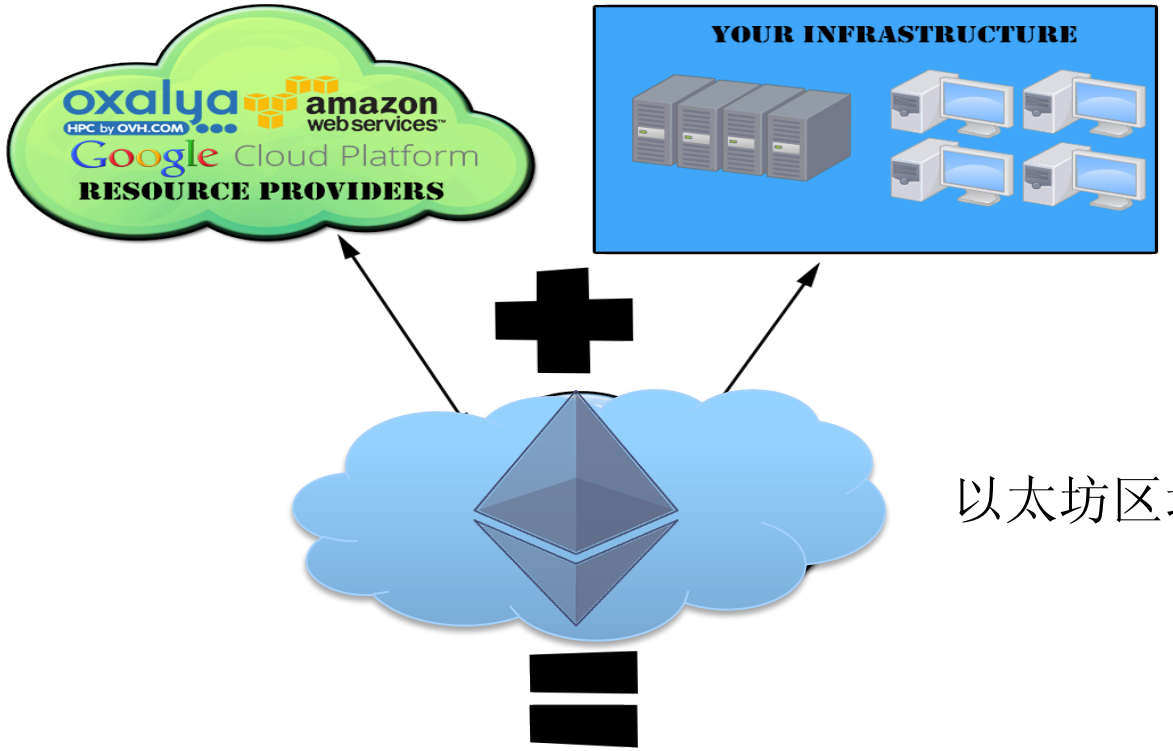


Book on Desktop Grid Computin. Ed. C. Cérin & G. Fedak, CRC/Chapman and all

桌面网格计算(志愿计算)面临问题

- 混杂计算资源(需求和资源匹配难)
- Internet计算资源不稳定(资源使用审计难)
- 贡献计算资源用户不足(无合适激励机制)

全球的计算资源市场



以太坊区块链

价格低，安全，按需分配，完全分布式的云计算

分布式云计算

- 去中心化的数据中心
  - 更加节能
  - 数据更加接近用户

- 下一代数据中心

a) Rutgers

b) Stimergy

c) Qarnot

研究基础

Since 1999

2000 — **MPICH-V**
- Parallel computing
- N-faults resilience

2001 — **XtremWeb**
- 1st Internet P2P Global Computing Platform
- Bag-of Task Application
- Multi-users & multi-applications

2003 — **XtremWeb-HEP**
- Grid & Cloud
- Highly secure
- Virtualization
- Hybrid public/private Infrastructure

2008 — **BitDew**
- Large Scale Data Management

2010 — **MapReduce**
- Big Data
- 1st Implementation of MapReduce for Internet Computing

2012 — **SpeQuloS**
- QoS for Best-effort infrastructure

>1M€ 欧盟、法国研究经费 ≈100 学术论文发表

金融应用 E-FAST : E-Services Framework for Knowledge-bAsed Decision SupporT in Finance

面向金融服务的平台:

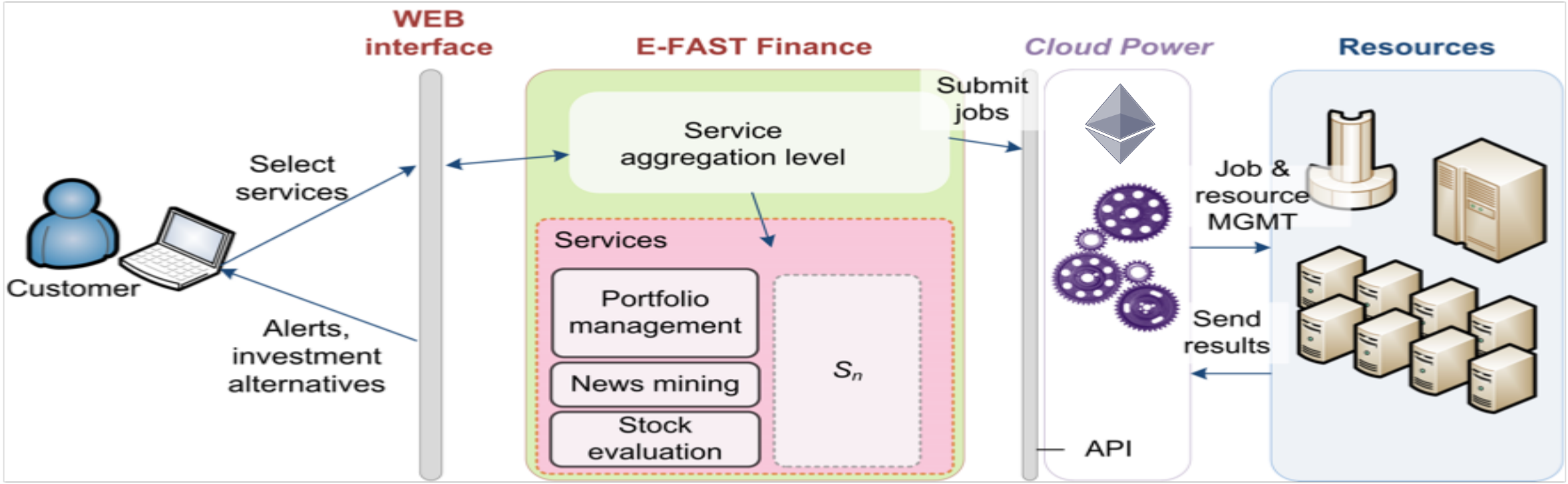
集成了高级的金融市场分析工具及数据, 根据市场变化及时为用户提供投资建议

数据及金融计算:

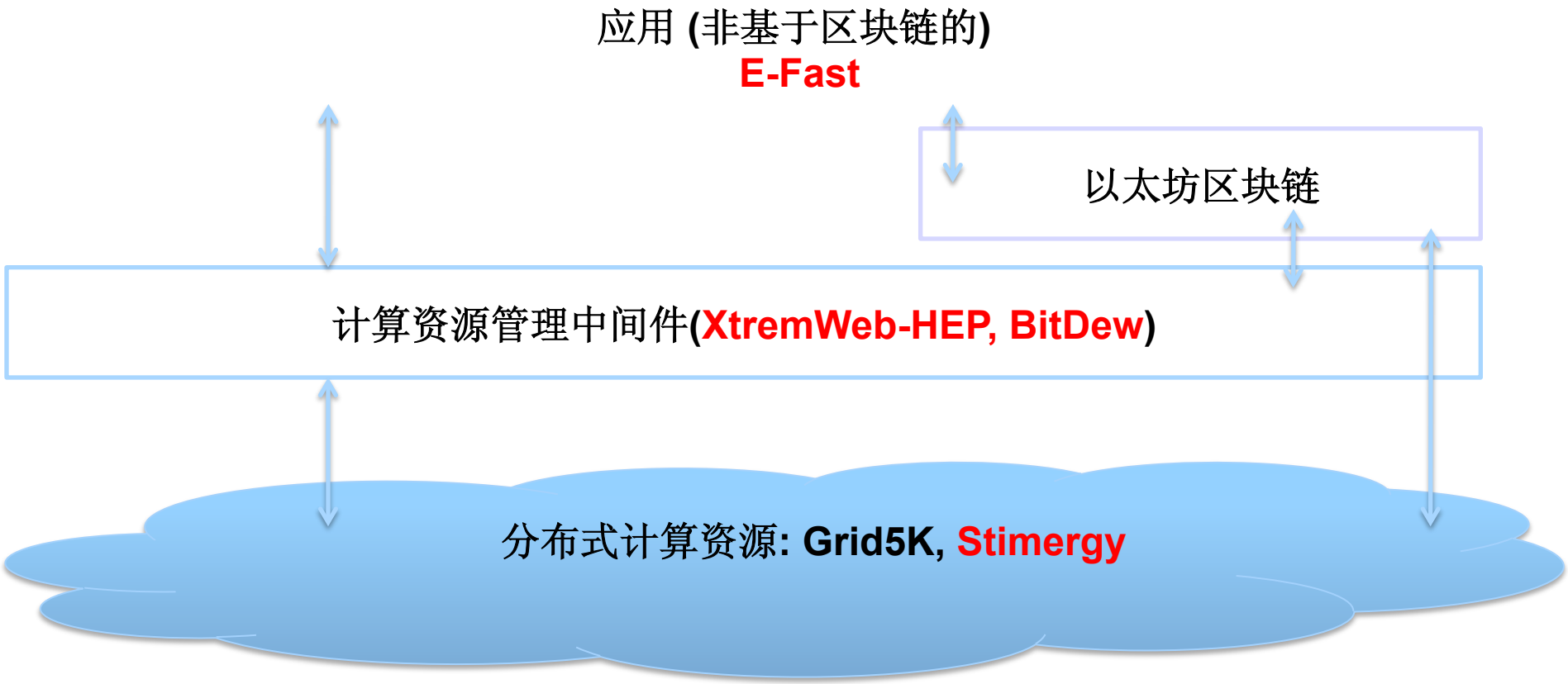
文本信息挖掘, 神经网络算法, 根据有效市场理论计算等

E-FAST 使用分布式云平台

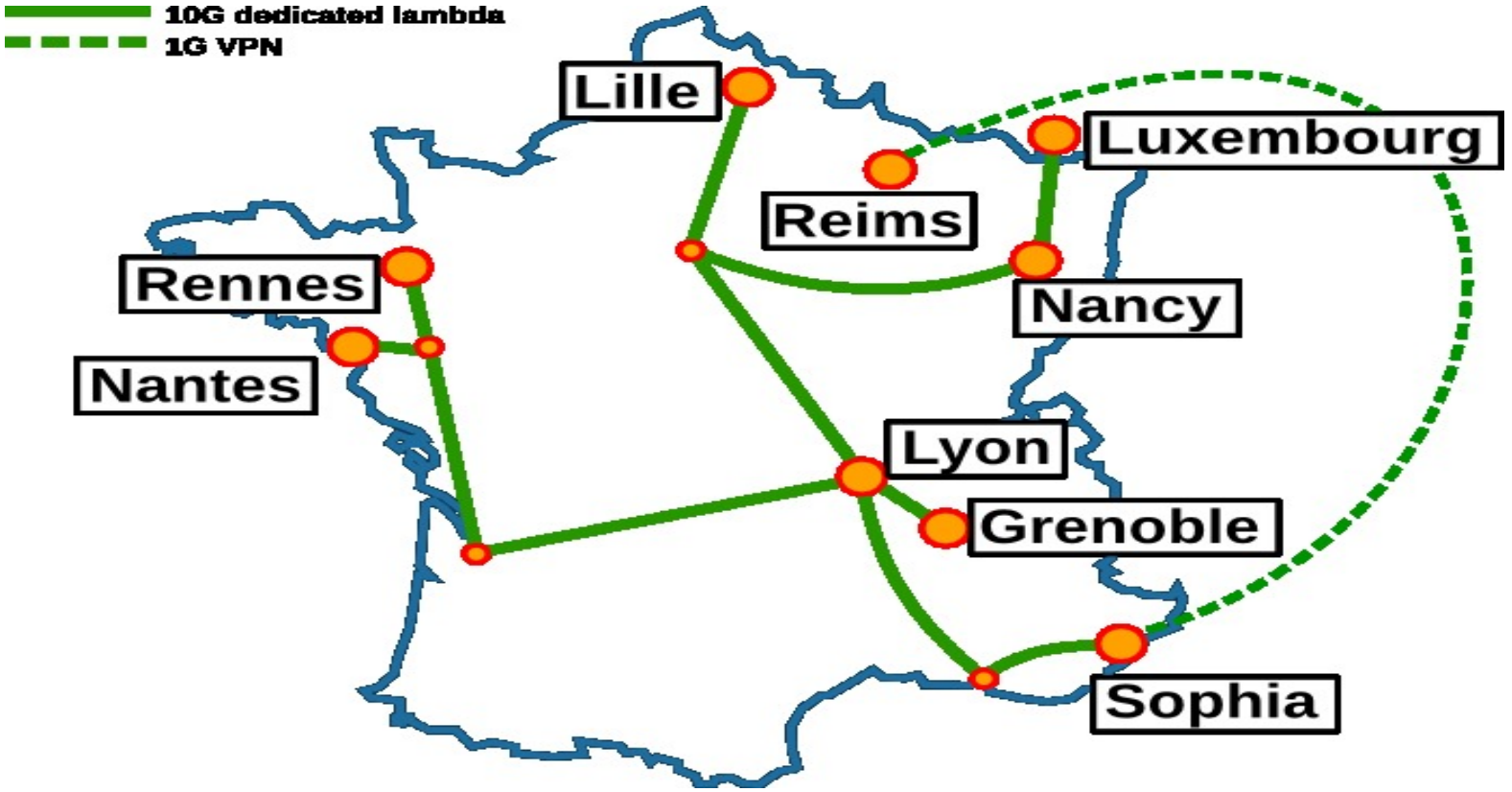
用户使用E-FAST 服务，相关计算通过分布式云平台运行: 精确匹配、按需计算、低价格



基于区块链的分布式云平台实验



实验平台



Grid5000
法国国家计算机系统实验平台:
- 9 城市, 1000 计算节点, 8000 内核
- GPU, Xeon Phi, SSD
- 10G 骨干线
- 完全可重新配置

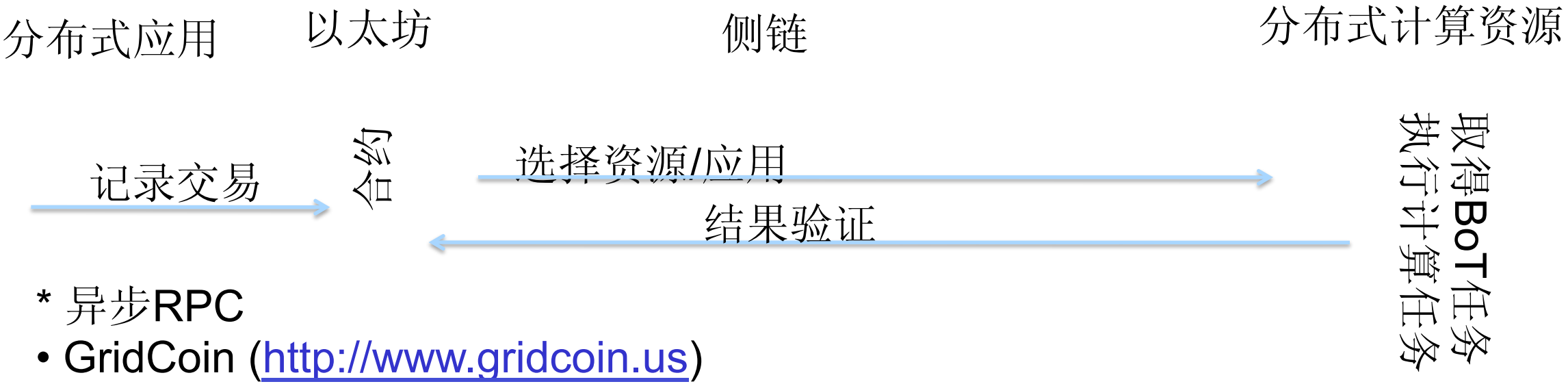
Use Case

Stimergy

Stimergy:安装10到100kW 服务器作为楼宇或游泳池供热设备和原有供热系统配合，实现零排放

使用Stimergy服务器作为我们的分布式云计算资源

工作贡献证明(Proof-of-Contribution)



* 异步RPC
- GridCoin (http://www.gridcoin.us)
- 以太坊计算市场(见 Github)
- 名声 + 结果验证(多数投票, 黑名单等)

基于区块链的分布式云平台架构

基于区块链的分布式应用(Dapps)

以太坊区块链

分布式云平台侧链(Proof-of-Contribution)

计算资源管理中间件(XtremWeb-HEP, BitDew)

结论

区块链+分布式+云计算=新一代绿色智能云计算平台

谢谢

Haiwu.He@cnic.cn