



愿乘风破万里浪，重塑下一代互联网

Introduction to DFINITY & Internet Computer Protocol (“ICP”)



Herbert Yang
GM of Asia, DFINITY Foundation

 @herbertyang

Herbert Yang

GM Asia, DFINITY 基金会

Head of BD for VC/Startup, Amazon Web Services, Greater China

Director, 云锋基金

副秘书长, 吴作人国际美术基金会

CEO, “宝狄”动画系列 (under 香港鹰君集团 Great Eagle Group)

CFO, 中移动“12580” / “印象”系列 (张艺谋, 王潮歌, 樊跃)

GE Capital / GE Corporate Audit Staff / 斯坦福 / 新加坡国立大学

创始人, Linkqlo / 群熠创想 / 龙之梦动画工作室



@yangherbert



@herbertyang



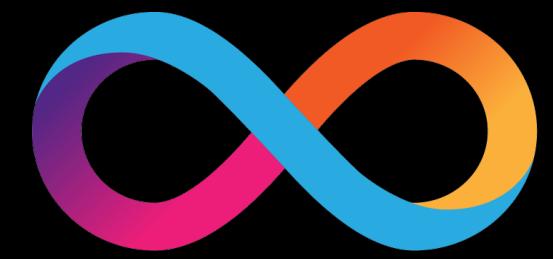
www.linkedin.com/in/herbertyang

Blockchain Singularity

Where the majority of the humanity's online
systems run 100% on blockchain

区块链奇点

人类大部分的网络应用100%运行在区块链上



DFINITY

DFINITY基金会（非盈利组织），成立于2016年10月
创始人，Dominic Williams, 英国人
总部，瑞士苏黎世
区块链行业最大的R&D组织
dfinity.org

1,600 research papers

100,000 academic citations

250 technical patents

270 FTEs

a16z POLYCHAIN CAPITAL

ELECTRIC CAPITAL

GREYCROFT



SCALAR CAPITAL

WANXIANG BLOCKCHAIN LABS
万向区块链实验室

SNZ FENBUSHI CAPITAL

ZhenFund
真格基金

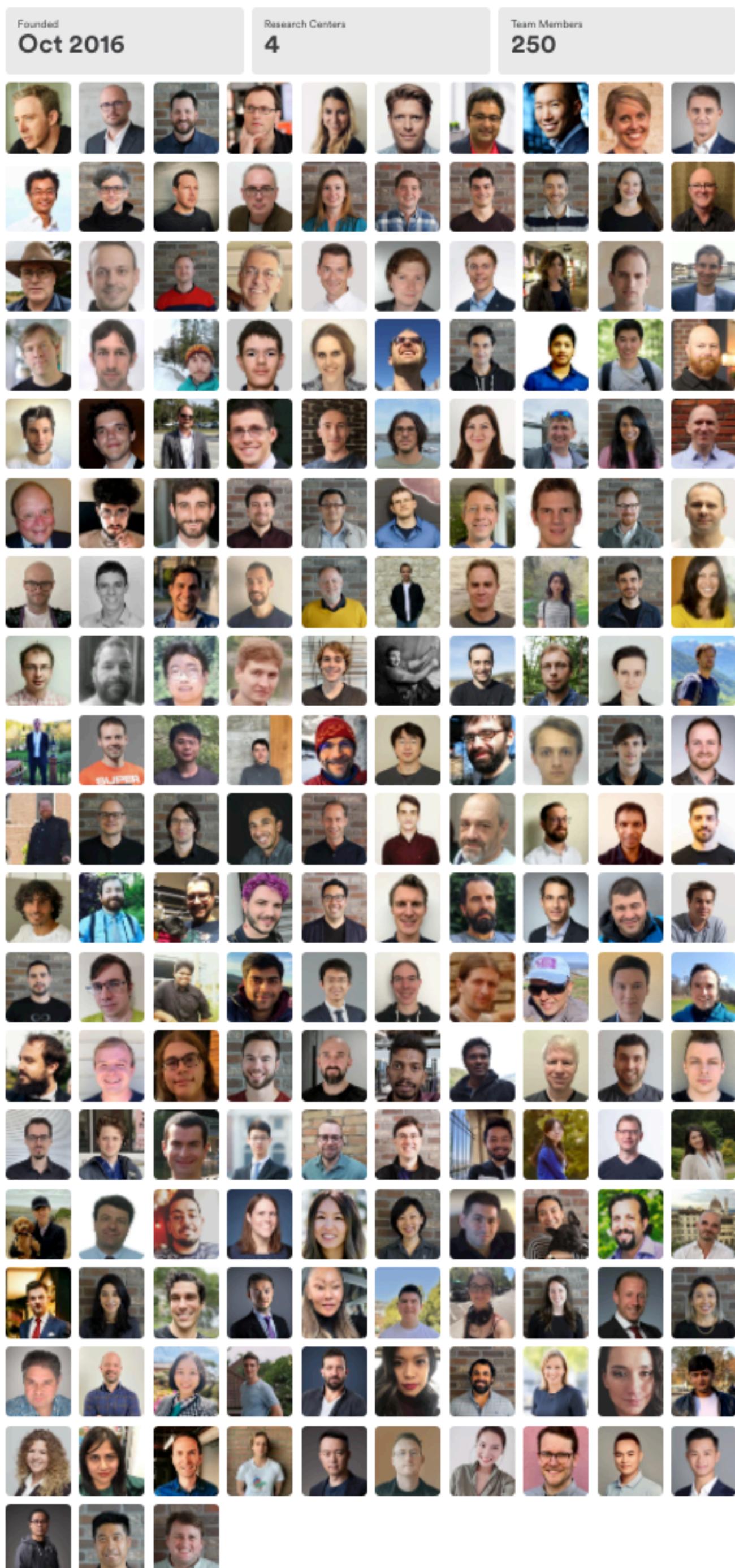
ANMI Capital

Aspect VENTURES

SVAngel

CAPITAL AMINO

Our Team



区块链行业的格局 > 2021年5月 @2023

应用层

钱包

数字藏品 NFT

去中心化金融应用 DeFi

稳定币 (USDT, USDC, DAI, BUSD, TUSD)

元宇宙 + 游戏

数据存储

预言机

L2

闪电网络
Stacks

L0/1

数字黄金

BTC

Polygon Optimism
Arbitrum ZkSync
ImmutableX Loopring
Aztec Base

以太坊体系

ETH, Solana, Avalanche, NEAR, Algorand,
BNB, Polkadot, Cosmo, Cardano, Aptos,
Sui, Klaytn, EOS, Conflux

ICP

基础设施

Filecoin, Arweave,
Chainlink, Helium,
Golem

什么是互联网计算机 Internet Computer (“IC”)?



连锁密码学技术

Chain Key Technology

网络神经系统

Network Nervous System (“NNS”)

容器封装(智能合约)

Canister x Smart Contract

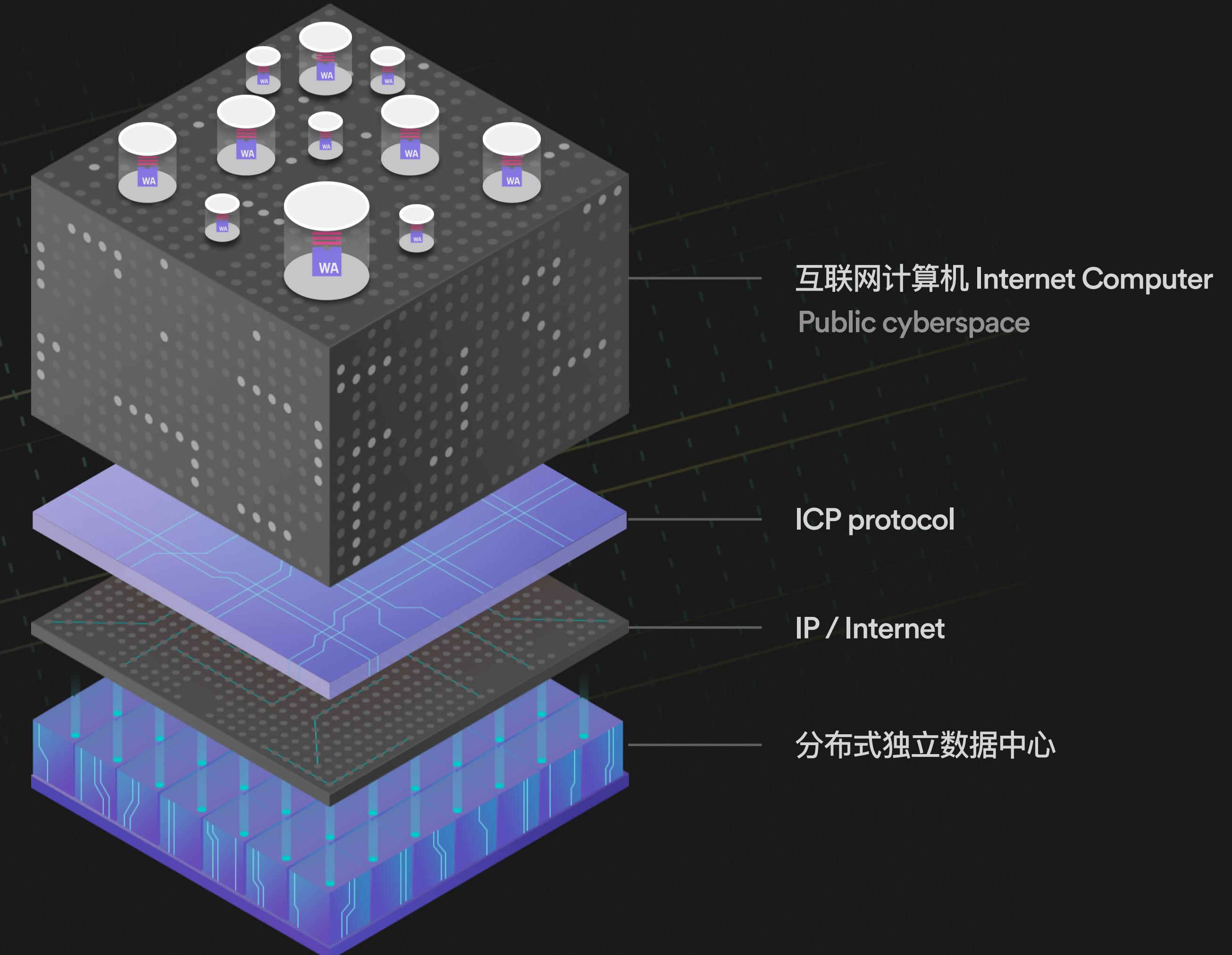
反向手续费模式

Reverse Gas Model

互联网计算机身份

Internet Identity (“II”)

IC打造了一个由全球多个数据中心共同组成的虚拟超级主机，相当于在阿里云和AWS等传统的云厂商之上抽象构建了一个去中心化的超级虚拟云，用于承载未来大规模Web3应用和数据



欢迎加入互联网计算机生态
完成V神未尽的事业：
世界计算机



internetcomputer.org

追随业界大牛的脚印，加入最具颠覆性的行业技术前沿阵营



Jan Camenisch



Ben Lynn



Jens Groth



Victor Shoup



Andreas Rossberg

直接在区块链上部署网络应用前端，远低于云计算架构成本

以太坊

互联网计算机

分布式账本



分布式算力



分布式存储



传统互联网开发经验无缝迁移，真正的Web3全栈技术平台

反向手续费模式 (Reverse Gas Model)

网络神经系统 (DAO)

容器型智能合约 (Smart Contract)

互联网身份 (DID)

连鎖密码学技术 (Chain Key Technology)

使用场景涵盖互联网所有垂直领域，解锁广阔职业发展空间

mora.app dmail.ai edgematrix.pro shiku.com

oc.app dscvr.one icdex.io hotornot.wtf

Big Bang for True Web3 DApps on ICP



谢谢！

Traditional Web2

微信, Telegram, Whatsapp

Youtube

MetaMask

Linkedin

Gmail, Protonmail

Reddit

Medium, Substack

Binance

Spotify

Decentraland, Sandbox

ETH L2

TickTok

chatGPT/OpenAI

Built on ICP

OpenChat

DSocial

AstroX ME

Distrikt

Dmail

DSCVR

Mora

IC Lighthouse

Itoka

Shiku

Bitfinity Network

Hot-or-Not

Edge Matrix (“EMC”)

Site

oc.app

dsocial.app

astrox.me

distrikt.io

dmail.ai

dscvr.one

mora.app

icdex.io

beta.itoka.xyz

shiku.com

bitfinity.network

hotornot.wtf

edgematrix.pro

Appendix

互联网计算机的区块链技术可以满足互联网用户需求么？

更安全的数据

每个用户的所有数据封装在自己的容器里 => 真正拥有自己的所有数据

互联网身份 (Internet Identity) 将用户身份和应用使用权限分离开，不再需要公钥/私钥 => 保护用户隐私

SNS实现将应用的所有权移交到社区控制的容器 => 真正的代码即法律

门限椭圆曲线加密签名方式 => 信任子网，而不是单个节点

PoUW (Proof-of-Useful-Work)的共识机制 => 按需付费

智能合约直接从传统网络获取数据 => 不再依赖第三方预言机

数据隐私权的决定留在应用层，而不是协议层 => 更尊重用户隐私

边缘节点的去中心化 => 定制化根域名

更低廉的使用成本

正交持久性 (Orthogonal Persistence) 的数据结构，状态直接写在内存 => 不再需要文件，节省大量存储空间，可以处理冷+热数据

将网络开发涉及的多层中间模块抽象化并写入协议层 => 大幅度降低开发者的开发难度

反向手续费模式 => 将应用的使用，维护和升级成本转移到开发者

更多样的使用场景

容器型智能合约可以直接运行前端网络程序 => 打通跟Web2之间的隔阂

可不断添加的子网 => 无限扩容

IDC级别的节点硬件要求 => 承载企业级的网络应用

智能合约封装在容器里 => 可以升级

没有历史的链 => 达到更高的出块效率

互联网计算机的区块链技术可以满足互联网用户需求么？

更安全的数据



每个用户的所有数据封装在自己的容器里 => 真正拥有自己的所有数据

互联网身份 (Internet Identity) 将用户身份和应用使用权限分离开，不再需要公钥/私钥 => 保护用户隐私

SNS实现将应用的所有权移交到社区控制的容器 => 真正的代码即法律

门限椭圆曲线加密签名方式 => 信任子网，而不是单个节点

PoUW (Proof-of-Useful-Work)的共识机制 => 按需付费

智能合约直接从传统网络获取数据 => 不再依赖第三方预言机

数据隐私权的决定留在应用层，而不是协议层 => 更尊重用户隐私

边缘节点的去中心化 => 定制化根域名

更低廉的使用成本



正交持久性 (Orthogonal Persistence) 的数据结构，状态直接写在内存 => 不再需要文件，节省大量存储空间，可以处理冷+热数据

将网络开发涉及的多层中间模块抽象化并写入协议层 => 大幅度降低开发者的开发难度

反向手续费模式 => 将应用的使用，维护和升级成本转移到开发者

更多样的使用场景



容器型智能合约可以直接运行前端网络程序 => 打通跟Web2之间的隔阂

可不断添加的子网 => 无限扩容

IDC级别的节点硬件要求 => 承载企业级的网络应用

智能合约封装在容器里 => 可以升级

没有历史的链 => 达到更高的出块效率

BTC / 支付网络

ETH / 资产网络

ICP / 应用网络

Layer-1 Performance Comparison

| |  |  |  |  |  |  |
|--|---|---|---|---|---|---|
| | Ethereum | Cardano | Solana | Avalanche | Algorand | Internet Computer |
| Transaction Speed | 15-20 TPS | 2 TPS | 2,000-3,000 TPS | 4,500 TPS | 20 TPS | 11,500 TPS 250,000 QPS |
| Transaction Finality | 14 minutes | 10-60 minutes | 21-46 seconds | 2-3 seconds | 4-5 seconds | 1 second |
| Scalability | Not very scalable | Not very scalable | Not very scalable | Not very scalable | More scalability | Indefinite scalability |
| Node Count | 6,000 nodes | 3,173 nodes | 1,603 nodes | 1,243 nodes | 1,997 nodes | 443 nodes |
| Storage Costs | \$73,000,000 / GB | Inadequate data storage | \$1,000,000 / GB | \$988,000 / GB | IPFS off-chain storage | \$5 / GB |
| Cloud Service Dependency | 70% of nodes run on AWS | Unclear how many are cloud | Most nodes run on cloud | Unclear how many are cloud | Most nodes run on cloud | Independent data centers |
| Energy Efficiency | 238 kWh per transaction | 0.5 kWh per transaction | 0.00051 kWh per transaction | 488,311 kWh in total | 512,671 kWh in total | 1.3 kWh per transaction running on-chain |
| <i>Each of these blockchains outsources storage and hosting to centralized servers, however, signaling a hidden carbon footprint</i> | | | | | | |

| | | | | | | |
|--------------------------------|--|-------------------------------------|--|-------------------------------------|-------------------------------------|-------------------------------------|
| End-User Key Management | Relies on centralized corporations to store keys and manage accounts | Users need to manage their own keys | Relies on solutions like Torus (leverages Facebook or Google accounts to provide access to the platform) | Users need to manage their own keys | Users need to manage their own keys | Set up an Internet Identity locally |
|--------------------------------|--|-------------------------------------|--|-------------------------------------|-------------------------------------|-------------------------------------|