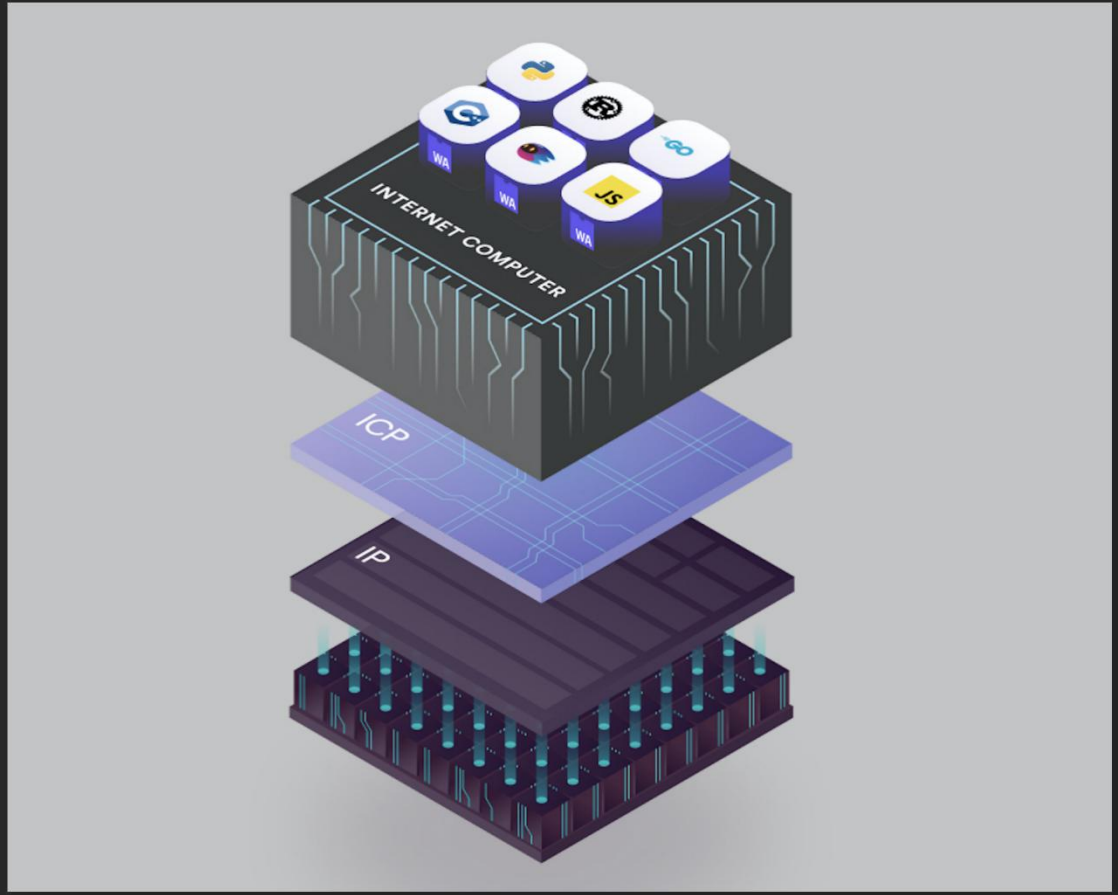
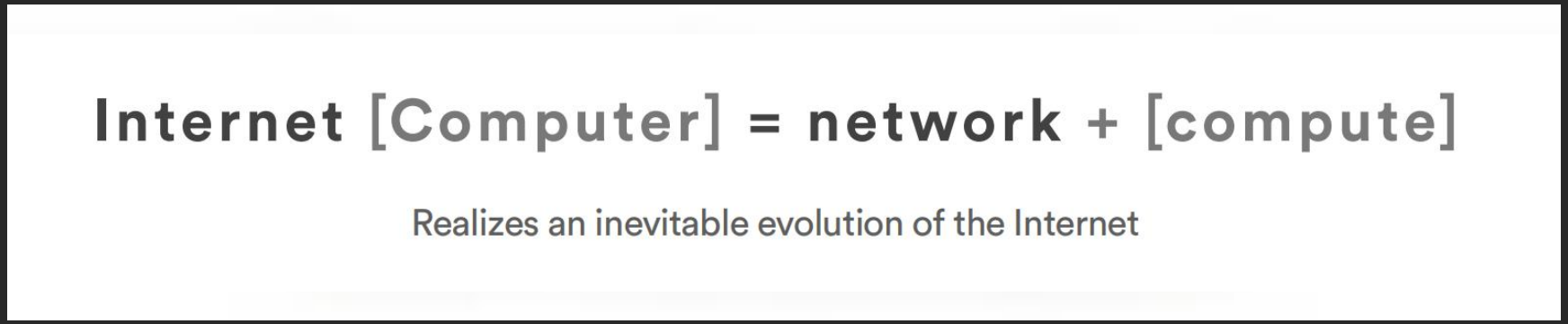
Internet Computer Protocol 简介



DFINITY 是什么?

DFINITY指DFINITY Foundation，是ICP区块链的基金会。

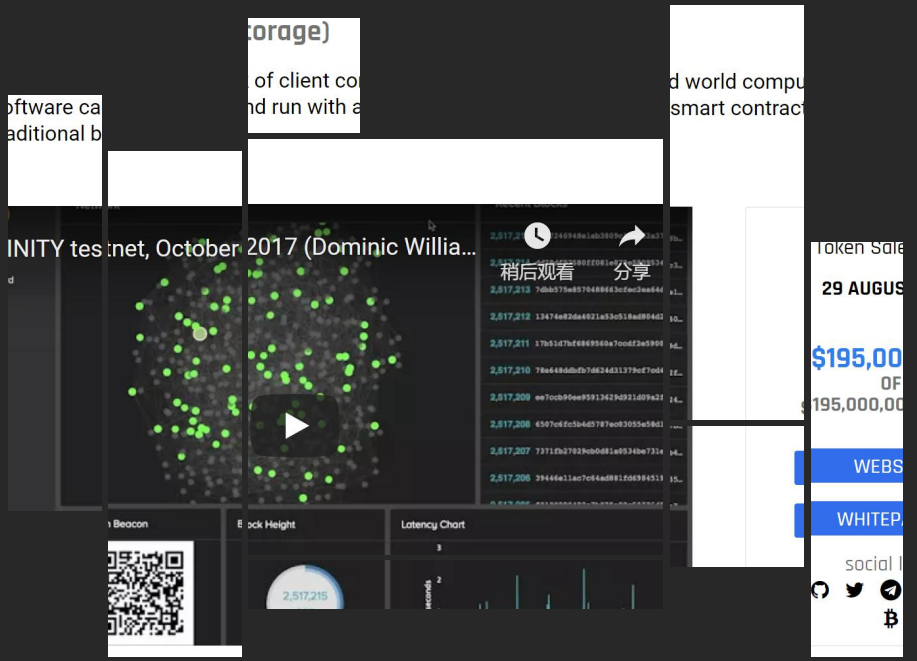
DFINITY Foundation的目标是打造一款真正的“世界计算机”，具有高性能，去中心化，无限拓展性等特征，以实现新一代互联网技术革命，这就是ICP协议。



团队介绍：

- DFINITY最早的起源，是来自String Labs所孵化的一个项目。
- 团队成员包含当前区块链领域顶尖科学家以及来自google，amazon，IBM等知名企业的工程师

项目融资：
近2亿美金


INITY tes net, October 2017 (Dominic Willia...
稍后观看
分享
Beacon
Latency Chart
2,517,215
29 AUGUS
$195,00
WEBS
WHITEP

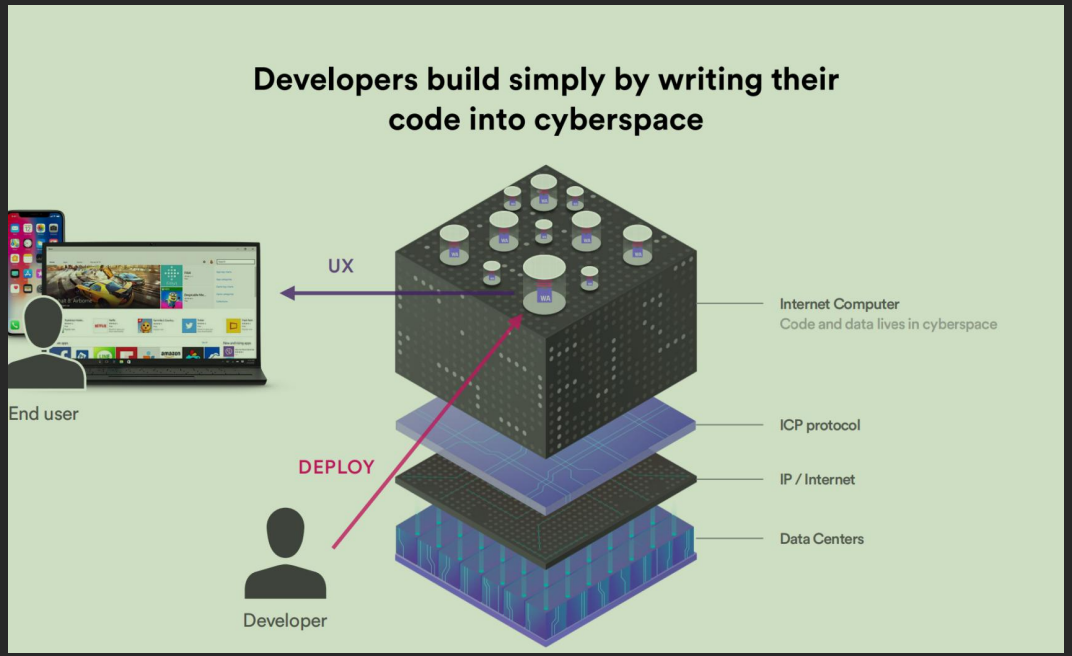
被认为是真正的区块链3.0

- BTC：数字黄金，解决价值存储问题
- ETH：去中心化资产发行，清结算平台
- Dfinity：去中心化应用生态平台

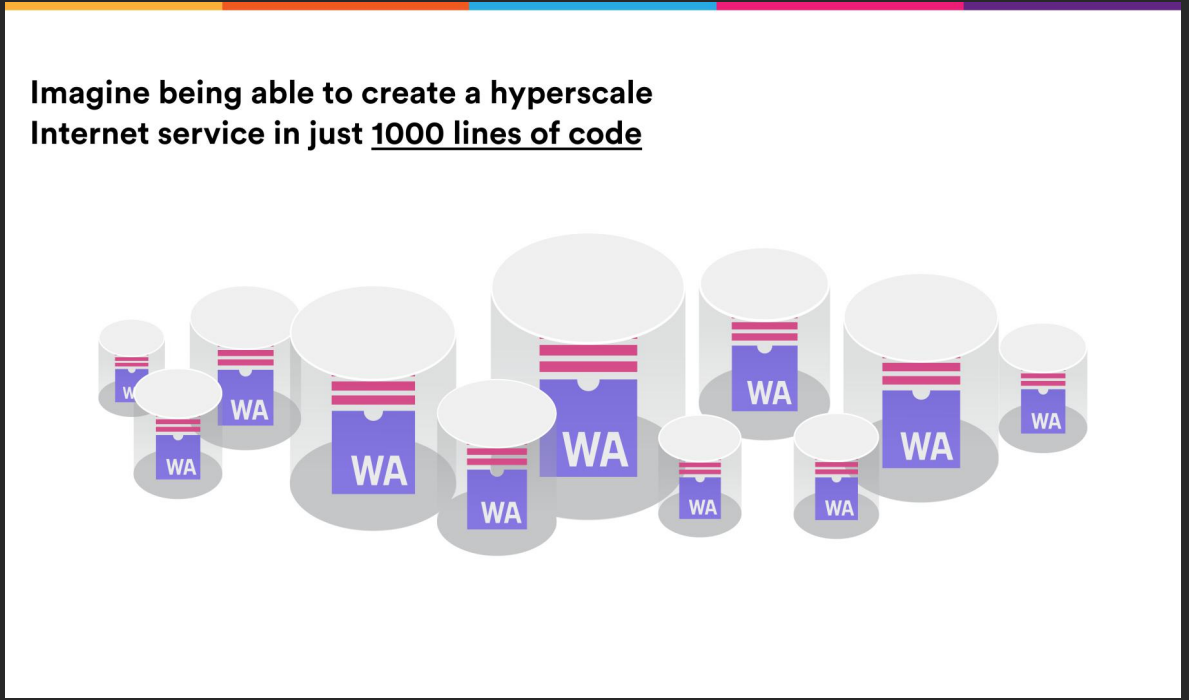
DFINITY想做什么？

Dfinity要打造一个由世界上的数据中心共同组成的虚拟超级主机，在阿里云和AWS等传统云厂商之上抽象了一个去中心化的超级虚拟云

在Internet Computer上开发软件有什么优势?



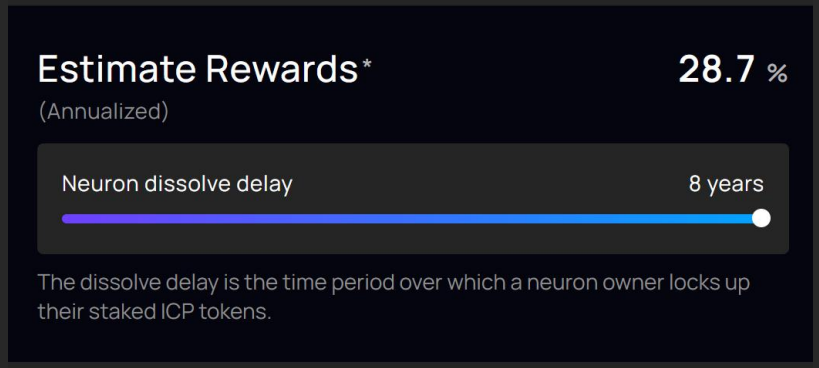
- 降企业IT运维成本
- 提高应用的去中心化程度
- 低用户门槛，更容易出圈

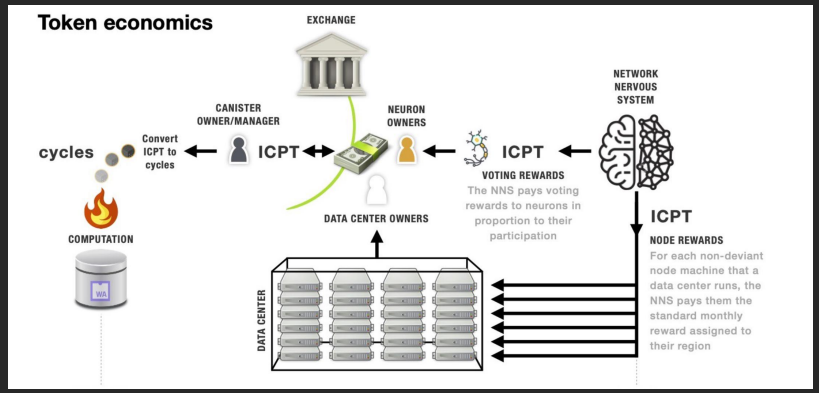


ICP区块链技术概述

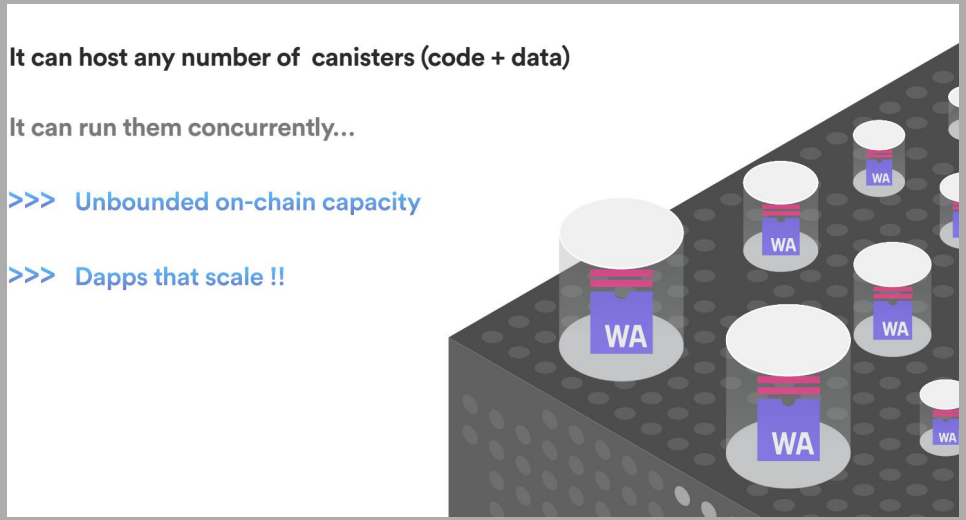
经济模型

- 在ICP区块链中， 主要有两种代币：
- Cycle：
  - 价值与XDR进行锚定， XDR是综合一系列法币进行加权求和得到的稳定币。
  - 作用主要为给Canister充值， 维持Canister运行
- ICP ：
  - 可以通过兑换为Cycle， “充值”给Canister（智能合约容器）， 维持Canister的运行。
  - 质押ICP，成为神经元，参与投票。投票可以得到新的ICP奖励。





Canister - 更强大的智能合约

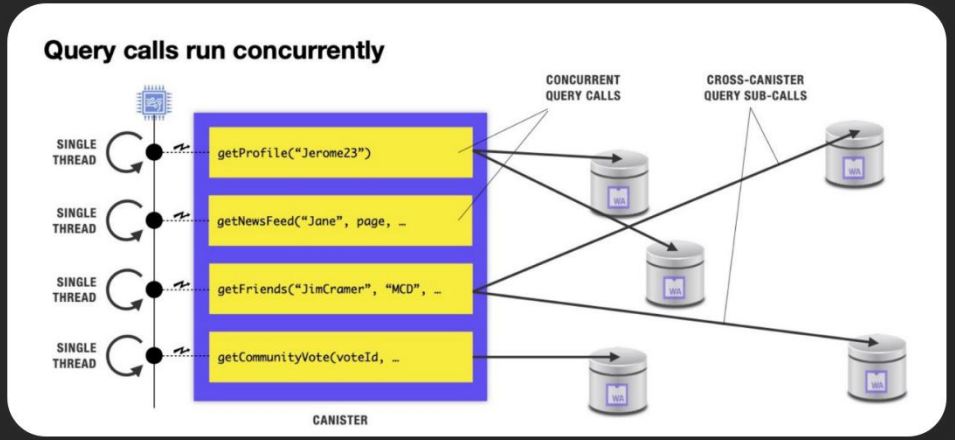


每个Canister都具有4G的运行时堆栈，以及4G的持久性存储内存空间(最大可至300G)。

DAPP的前后端都可以部署到区块链节点上，从而使前后端都具有由链保证的安全性。

可并发，可升级的智能合约

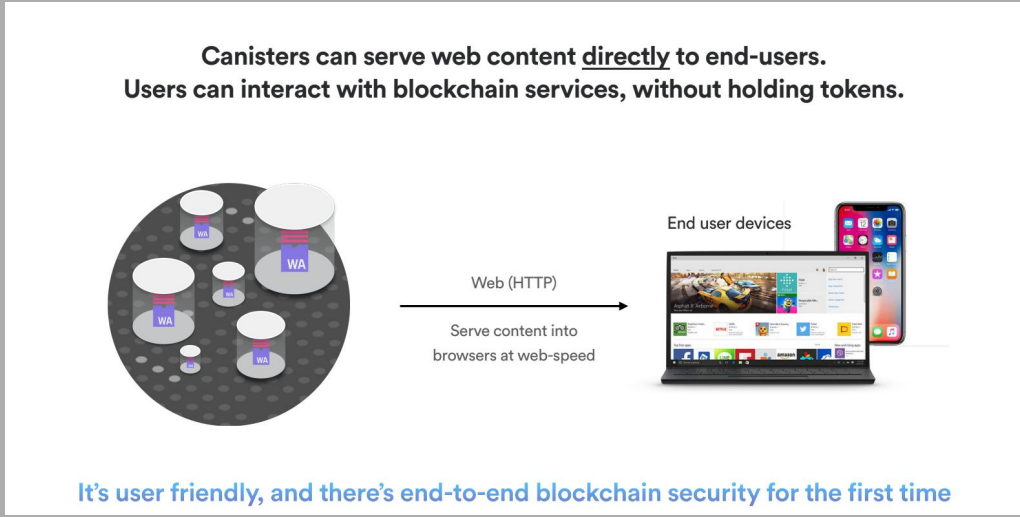
Query & Update & Upgrade



- Update： 这种方法将对内存数据进行状态修改，需要子网内达成共识，消息处理为单线程。
- Query： Canister使用Actor模型， 每个query方法会在节点内对当前数据状态进行一次“内存快照”，然后进行任意复杂操作。这种方法的调用不修改数据状态， 可并行处理。
- Upgrade: Canister智能合约可以被升级，升级前后的数据状态可以持久保存不丢失。

反向Gas模型

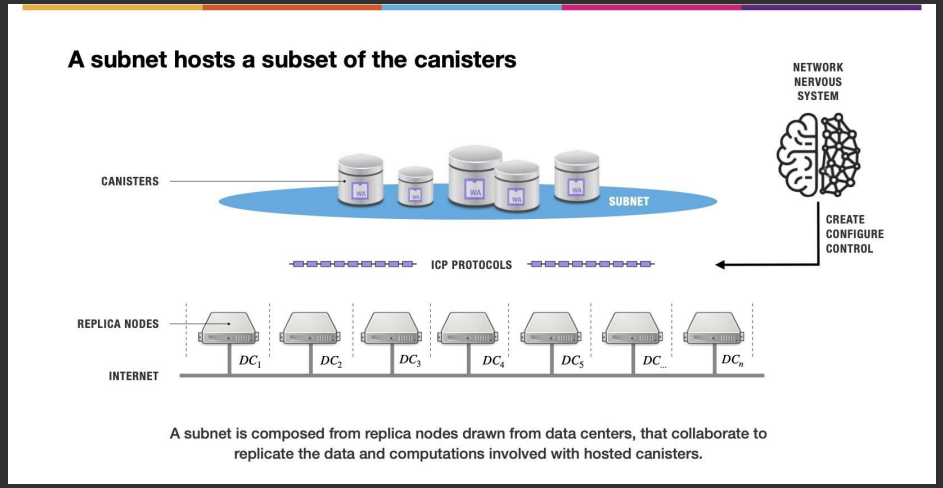
- 用户可以没有钱包，就直接访问由区块链提供的新一代Web服务。
- Canister的Cycle消耗由开发者，或者DAPP提供商提供



开发语言

- ICP合约原生合约开发语言为Motoko。由于Canister的本质为WebAssembly。因此，所有可以编译为wasm的语言都可以写ICP合约，当前Rust cdk比较成熟。

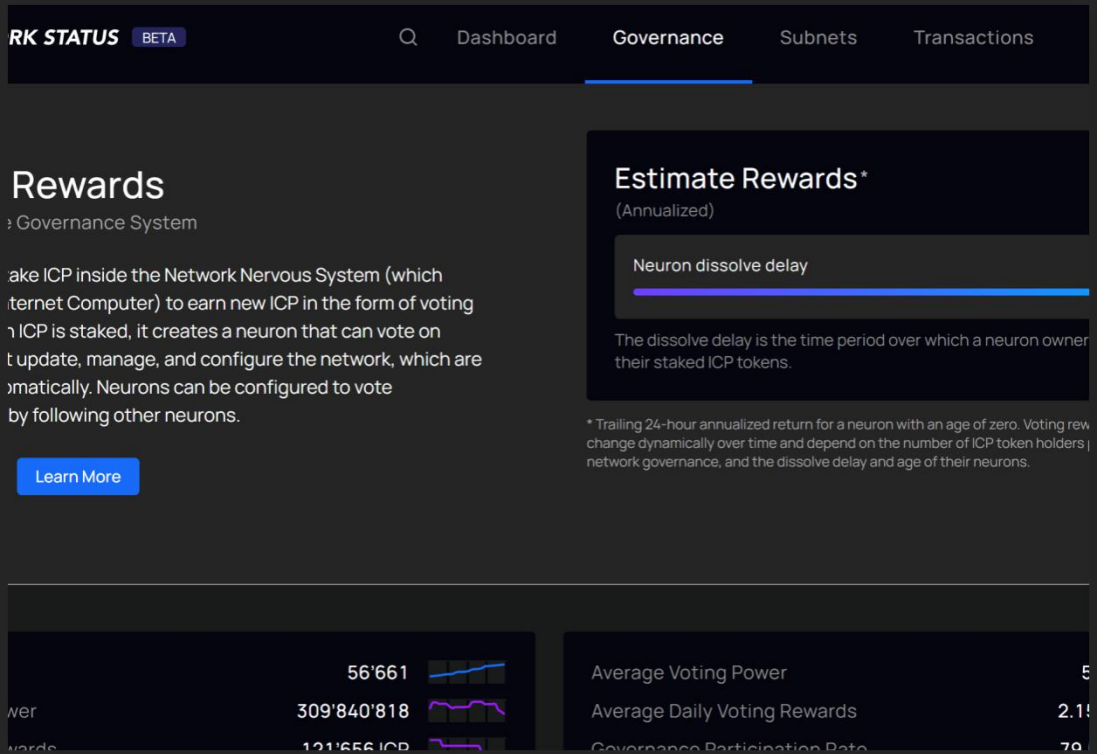
子网



ICP区块链包含很多对等服务的子网，主要类型有System子网和Application子网，每个子网都是一条独立的区块链。

我们的DAPP可以部署到应用子网上，子网内的每个节点都会运行一份Canister副本以提升Canister的服务性能和安全性。

Net Nervous System



- NNS是位于System子网上的一个特殊的Canister合约，主要负责对节点加入的审批，IC子网的生成和重组，ICP协议的升级等。
- 我们可以通过质押ICP成为神经元参与NNS的投票

Chain Key

- Chain Key技术是ICP区块链的核心技术之一。
- ChainKey利用阈值BLS密码，为ICP的共识协议提供服务，使每个子网可以快速达成共识。
- 用户通过ChainKey提供的技术底层，使前端/用户可以通过IC的公钥就可以验证消息是否为IC发出的，而不用知道是哪个子网发出的。

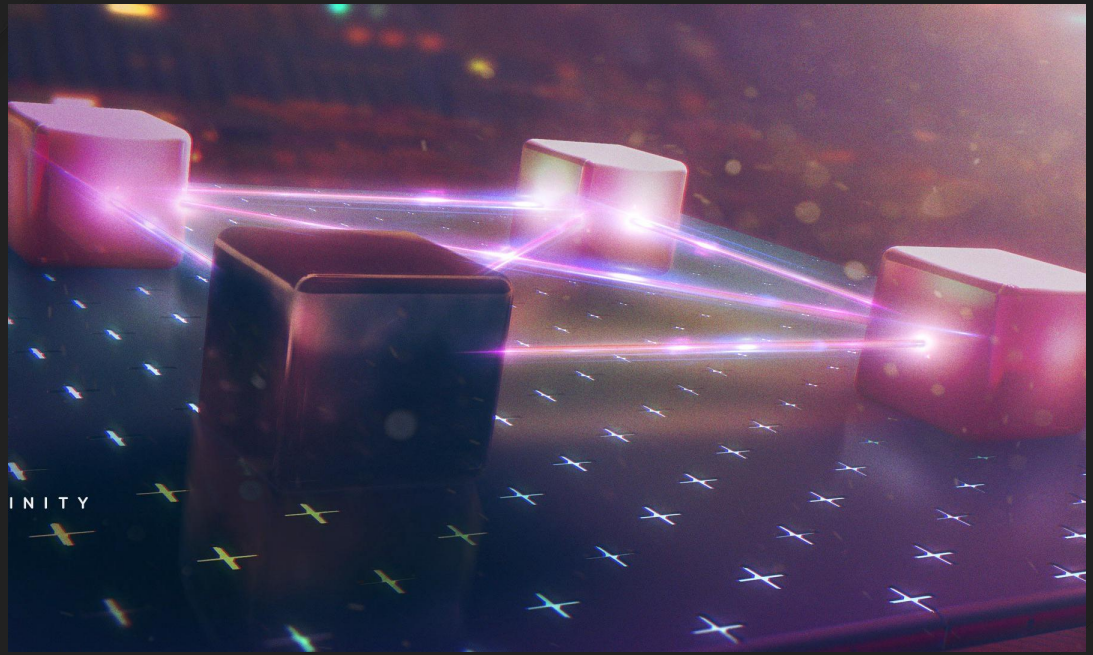
Catch Up Packge & 不保留旧区块的区块链

- 每个子网每隔200个区块进行一次“打包”， 这次打包将包含当前所有副本的一致性数据， 打包后子网内进行阈值签名，超过2f+1个节点签名后， 就认为达成一致， 此时就可以删去以前的区块，只保留这个新的世界状态。
- Catch up包可以用来恢复数据， 同步数据，重组子网等。

Internet Identity

- Internet Identity 是位于System子网上的一个特殊Canister，为用户提供DID服务。
- 通过Internet Identity(II)， 用户可以通过一次注册，登陆所有的DAPP，并且通过II提供的代理签名，SessionKey，WebAuthn等技术，为用户在不同的DAPP上赋予不同的用户地址，以保护隐私，避免追踪。

共识协议



- Block Maker：子网内节点通过运行ChainKey提供的VRF(TBLS)提供随机性，随机选出不可预测的出块节点，出块节点根据自身优先级打包出块并广播。
- Verify & Certificate：子网内其他节点收到区块后进行验证和输出，将输出整理为Merkle Tree后广播，子网内再通过阈值签名进行认证。

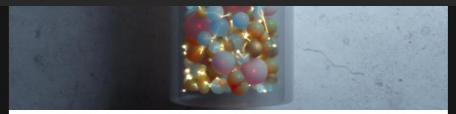
RoadMap

RoadMap

Deployed

EXPANDED INTERNET IDENTITY SUPPORT

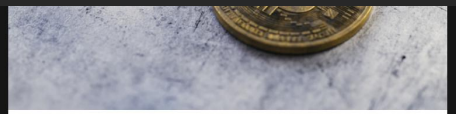
Continued expansion of supported devices for Internet Identity to include



Developing

INCREASED CANISTER SMART CONTRACT MEMORY

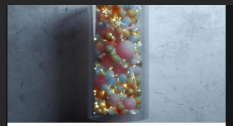
Currently, canister smart contract stable



Developing

DIRECT INTEGRATION WITH BITCOIN

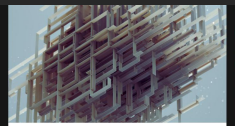
The Internet Computer will add smart contracts to Bitcoin through an



Developing

ENABLE CANISTER SMART CONTRACTS TO CONTROL ICP

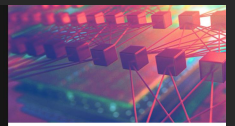
Enabling all canister smart contract types to interact with the ICP ledger to control ICP tokens. Currently, for security reasons, only NNS canister smart contracts and users may interact with the ICP ledger on the NNS subnet.



Developing

THRESHOLD ECDSA SIGNING

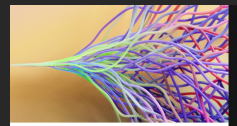
ECDSA signatures are widely used in the blockchain industry. This feature will enable canister smart contracts to have an ECDSA public key and to sign with regard to it. The corresponding secret key is threshold-shared among the nodes of the subnet holding the canister smart contract. This is a prerequisite for the direct integration between the Internet



Voting Soon

SERVICE NERVOUS SYSTEM | GOVERNANCE FOR DAPPS

Adding a feature to the NNS that allows entrepreneurs and developers to create an NNS-like permissionless tokenized governance system with its own token ledger for their dapps and services.



Discussing

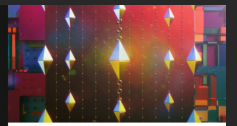
BIG MAP

BigMap is an advanced scaling solution for linking an unbounded quantity of Canisters together. However, the Foundation is first prioritizing increasing canister smart contract memory which will address immediate developer pain points.

Discussing

AMD SEV VIRTUAL MACHINE SUPPORT

Enable node images to be run as virtual machines, improving data center adoption while continuing to support privacy-protecting subnets.

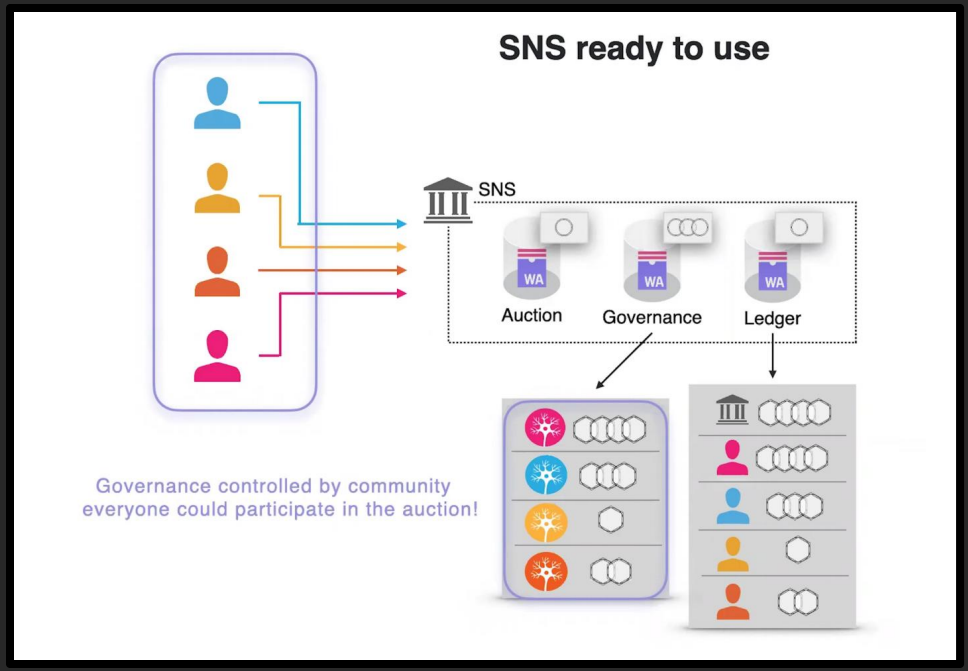


Discussing

DIRECT INTEGRATION WITH ETHEREUM

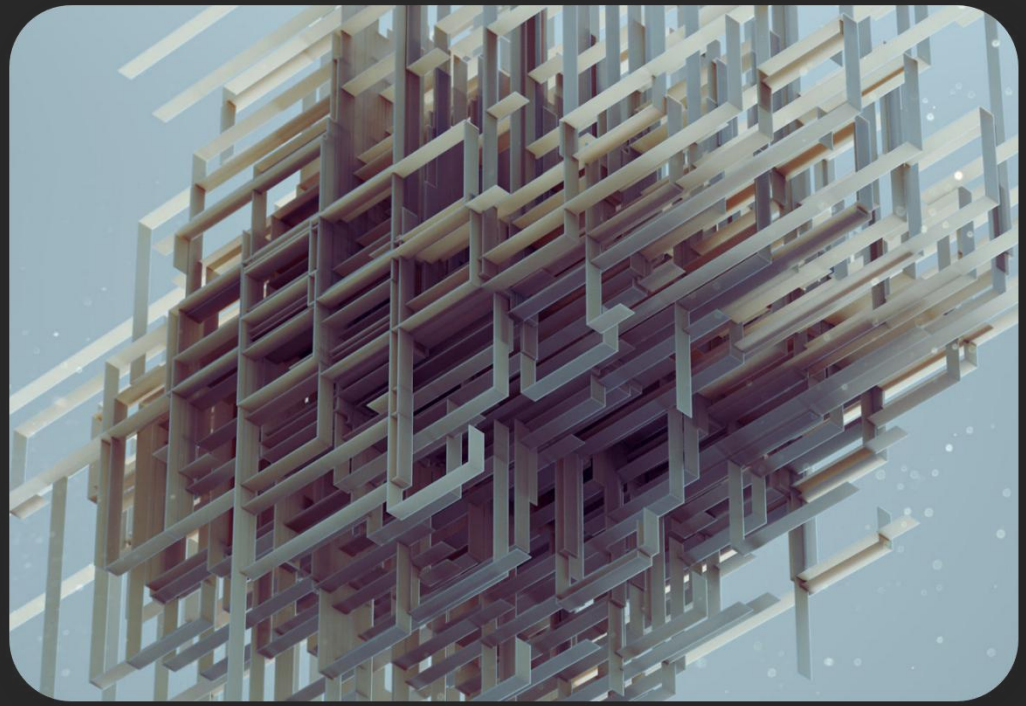
Smart contracts on the Internet Computer and Ethereum will be able to interact, thanks to direct integration enabled by Chain Key cryptography. In a revolutionary step, Chain Key cryptography will enable smart contracts on the Internet Computer to be able to submit transactions to Ethereum.

Service Network System



- DFINITY Foundation团队将推出SNS治理系统，为ICP区块链上的DAPP设立新一代的DAO治理系统。
- SNS将提供Token Ledger管理，DAO投票治理，Token竞拍拍卖功能，帮助开发者更快更好的建立他们自己的DAO治理。

Threshold ECDSA



ICP开发者团队目前正在开发，测试阈值ECDSA解决方案，使Canister智能合约可以通过ChainKey技术持有，发送，接收BTC，为BTC加载智能合约，让ICP真正成为新一代的互联网计算机。

Canister Stable Storage

- Canister受制于wasm32的限制，Canister当前运行时堆栈内存为4G，ICP开发团队对此进行了优化：

  每个Canister除了运行时的4G内存还可以加上4G的Stable内存，可以理解为硬盘内存(当前方案为8G Stable内存，但当前API只可获取4G Stable内存)，并且Canister的Stable内存将随着Canister的后续升级，可以最大扩容到300G存储空间(子网最大内存)。

生态优势

- 矿工
- 开发者
- 投资者
- 用户

节点运营商

- 未来全球最大的去中心化云平台的基础设施建设者
- 网络安全的维护者
- Dfinity生态建设参与者

开发者

- 更低的开发运维成本
- 更多的方向：Defi，NFT，SocialFi，gameFi等
- 更大的创业机会

“

投资者

- 更多的投资选择
- 更容易看懂的市场
- 更广阔的市场前景

”

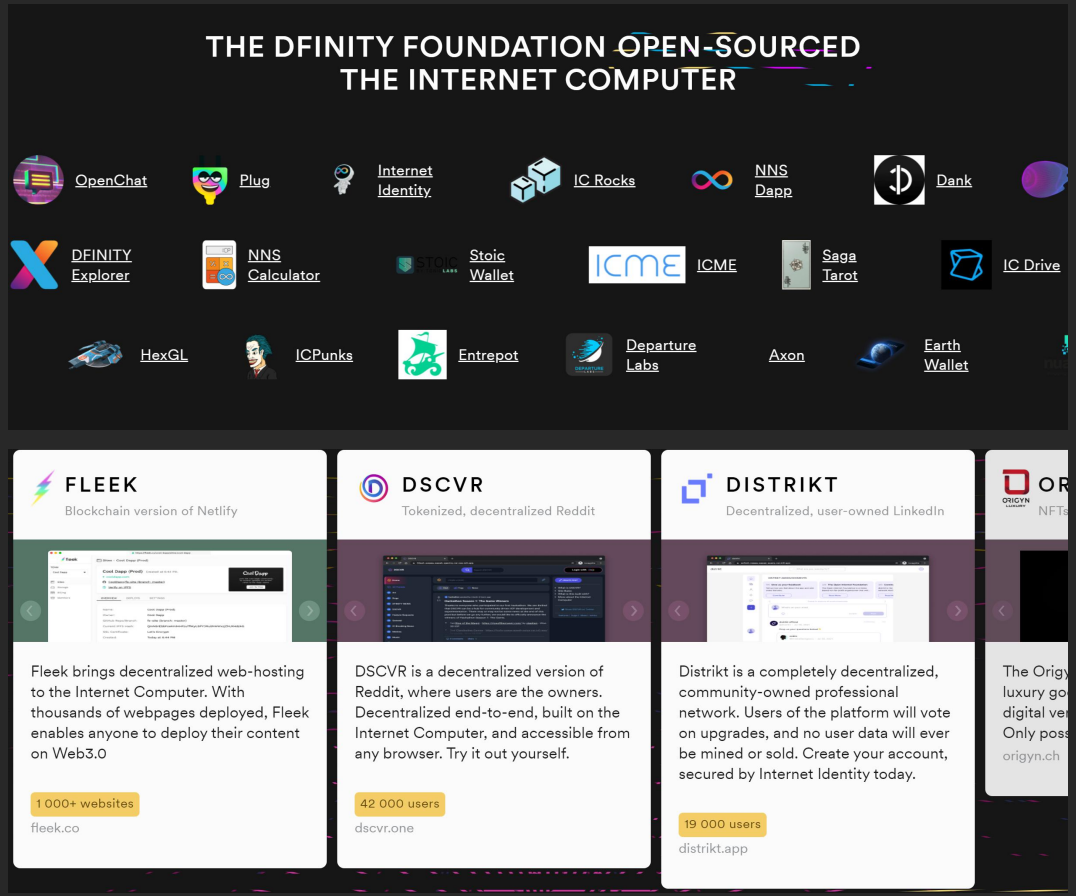
“

用户

- 低门槛
- 可玩性更高
- 参与去中心化应用迁移浪潮

”

许多新一代DAPP已经在ICP区块链上建立起来



社区贡献

- Motoko中文文档：https://shuzhichengspace.gitbook.io/dfinity/yi-kuai-su-ru-men
- IC Token 标准：
  - Fungible Token : https://github.com/rocklabs-io/ic-token
  - Non-Fungible Token: https://github.com/rocklabs-io/ic-nft

Reference：

- *[1] Money, blockchains, and social scalability, Nick Szabo*
- *[2]https://vitalik.ca/general/2017/09/14/prehistory.html*
- *[3] https://medium.com/DFINITY/DFINITY-in-a-nutshell-a-non-technical-introduction-ec45ec5967c1*
- *[4]https://medium.com/@dominic_w/part-iii-of-daos-new-horizons-and-challenges-in-depth-15bdc669c4*
- *[5]https://blog.csdn.net/shangsongwww/article/details/88567510?ops_request_misc=%257B%2522request%255Fid%2522%253A%252216145011931678026981237 2%2522%252C%2522scm%2522%253A%252220140713.130102334.pc%255Fall.%2522%257D&request_id=161450119316780269812372&biz_id=0&utm_medium=distribute.pc_search_result.none-task-blog-2~all~first_rank_v2~rank_v29-1-88567510.first_rank_v2_pc_rank_v29&utm_term=dfinity%E6%B7%B1%E5%BA%A6*
- *[6]Dfinity分散云愿景*