INTERNET COMPUTER

Cypherspace as cloud 3.0

ICP | Internet Computer

source https://deck.internetcomputer.org

version September 7, 2023

Dominic Williams

President/Chief Scientist @ DFINITY Foundation


modern societies are run by digital frameworks:
from social media, communications, storage & the sharing economy,
to financial systems, supply chains & medical records.
all delivered by online systems and services,
created by software logic and data…
built on digital infrastructure
– societal foundations

with better foundations, we can build better frameworks for society:

today, systems and services often break, and they are easily hacked.

big corporations run the foundations, giving them control.

developing new systems and services costs too much.

today, social media corps. own our content,

when we should own social media.

can the internet solve this?

ICP drives full stack decentralization on the internet – a future where systems and services:

UNSTOPPABLE	run on the internet, and become unstoppable like the internet
SOVEREIGN	don’t provide Big Tech or government with kill switches and backdoors
TAMPERPROOF	have logic and data that hackers and ransomware can’t corrupt
DAO-POWERED	can be exclusively owned/controlled by community DAOs
AUTONOMOUS	can run without the need for centralized controllers
LOWER COST	require fewer personnel to develop and support

tech history arcs towards public networks

Private Infrastructure → **Public networks**

Information superhighway → **The Internet**

curated walled-garden network proposed by Microsoft and Oracle (1990s)

private routing devices connected by open TCP/IP protocols form a public global network

Legacy IT Stack → **Internet Computer**

cloud services, servers, databases, web servers, CDNs, firewalls...

private node machines connected by open ICP protocols form a public stateful serverless autonomous cloud

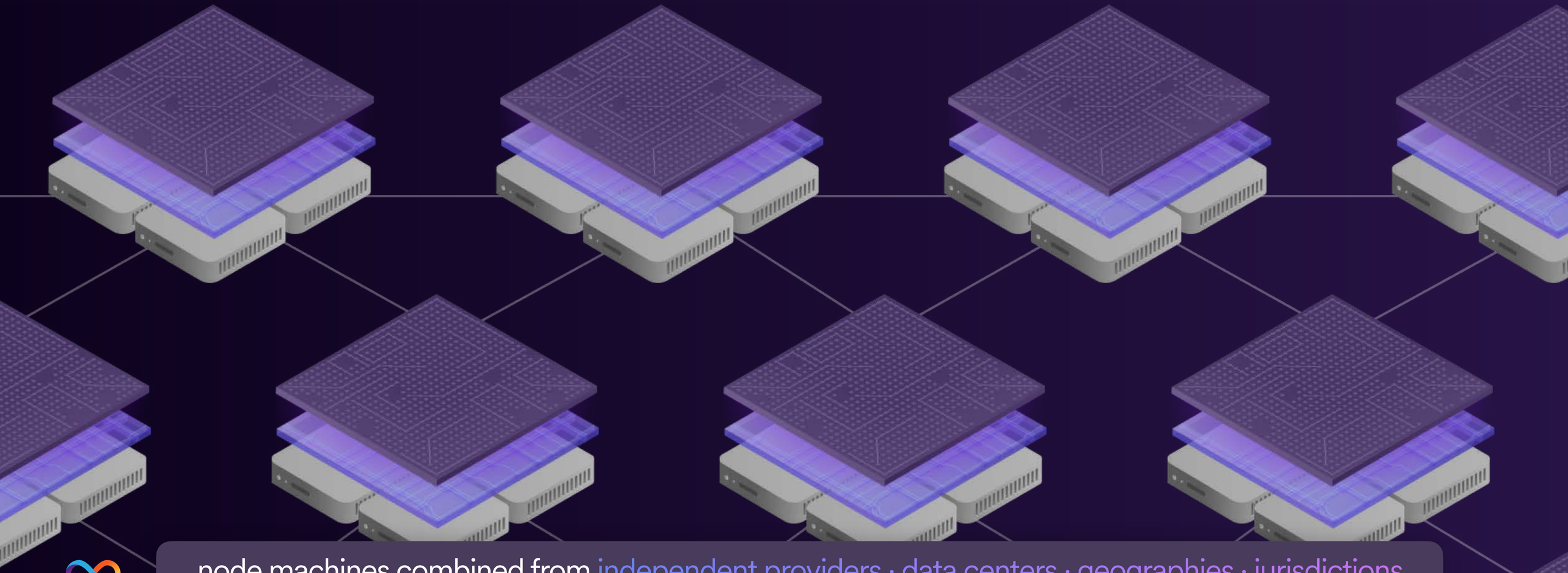
network

The Internet Computer is created by ICP (Internet Computer Protocol)
the most advanced network protocol ever devised

independent node providers own and operate node machines in data centers worldwide

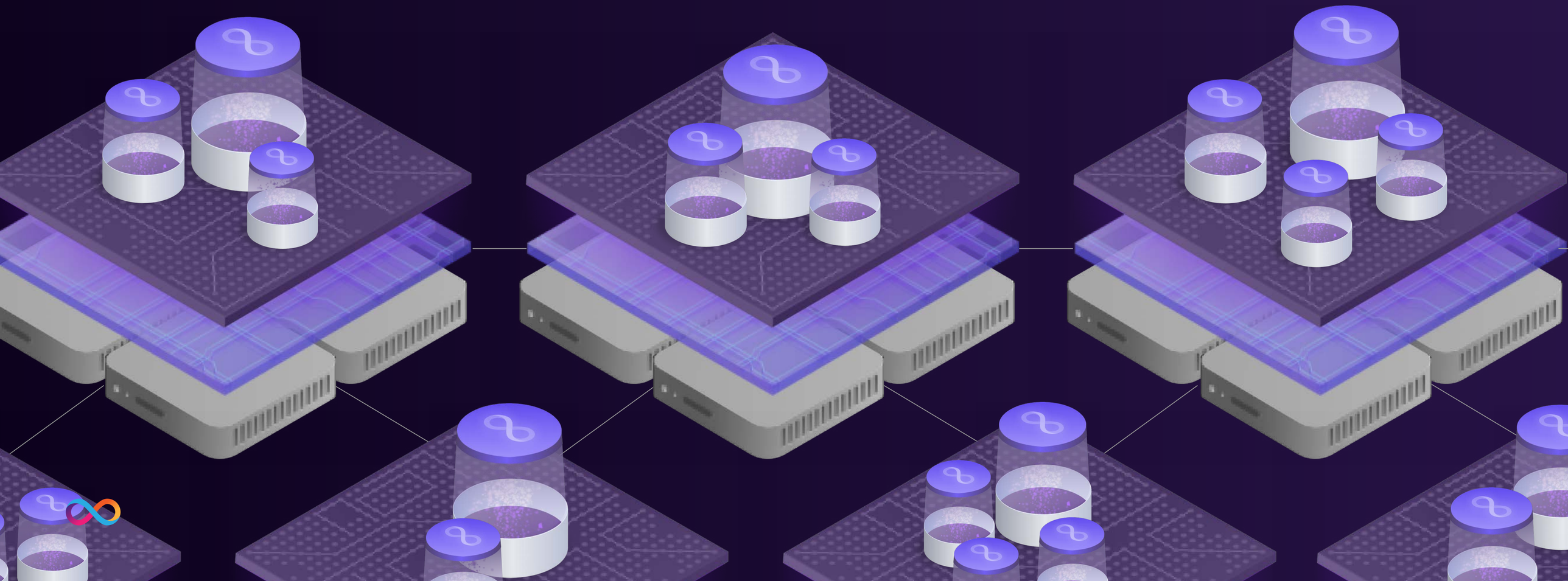
standardized physical hardware – the Internet Computer runs on a sovereign network, not cloud

Internet Computer Protocol (ICP) combines nodes to form efficient subnet blockchains

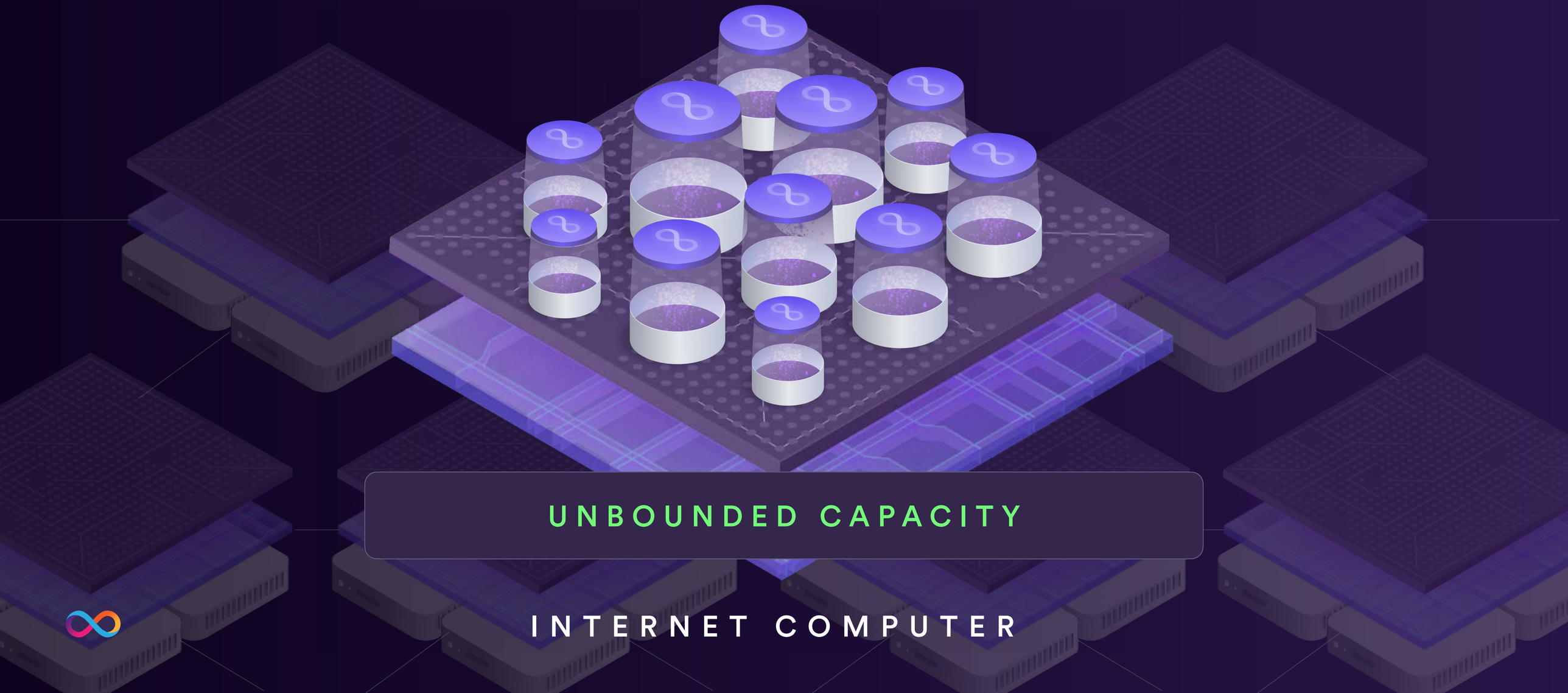


node machines combined from independent providers · data centers · geographies · jurisdictions

subnet blockchains add capacity for hosting *canister* smart contracts



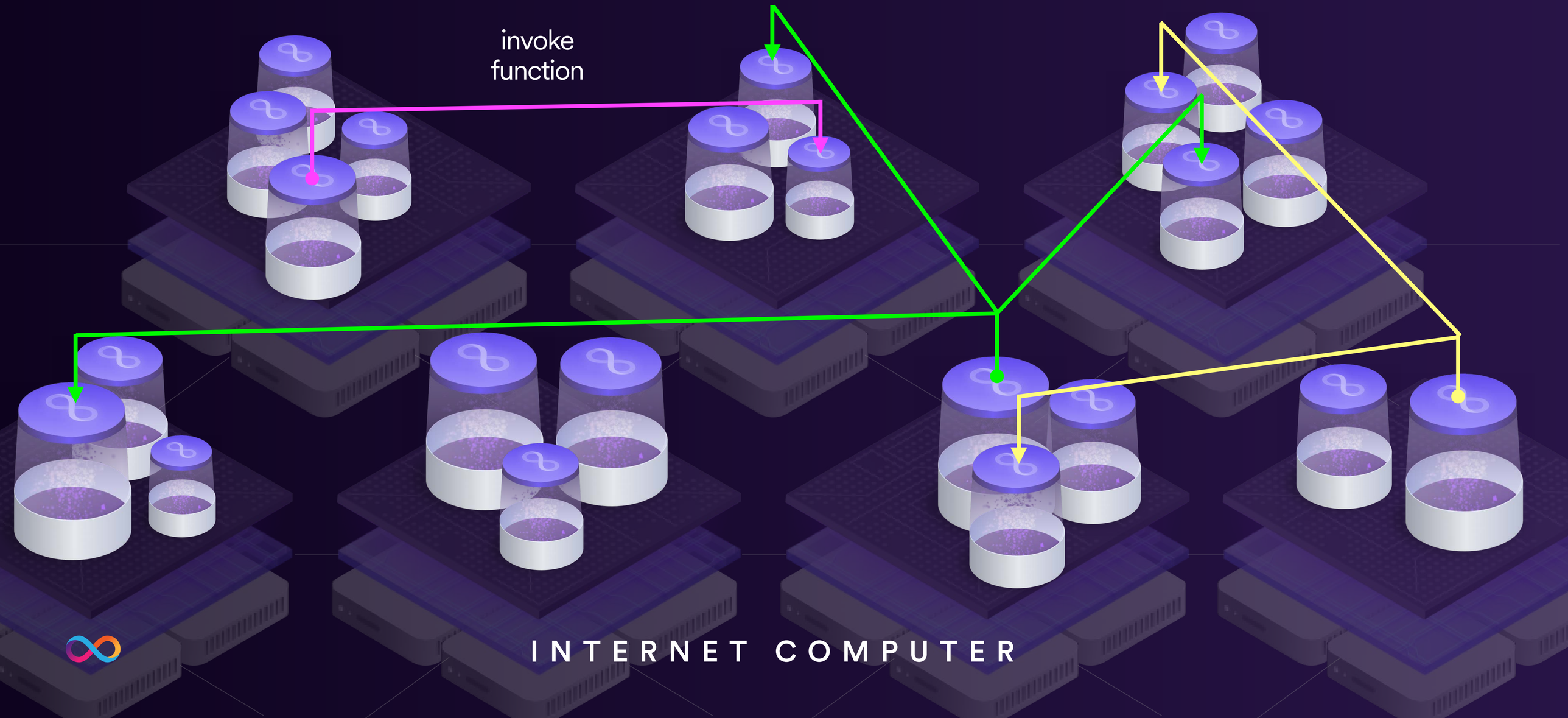
subnets combine into ONE *stateful serverless autonomous* cloud



UNBOUNDED CAPACITY

INTERNET COMPUTER

a seamless universe for tamperproof code units w/o servers or instances



build almost anything

Online systems and services can be built directly on the Internet Computer using smart contract code, without any need for legacy IT, such as cloud services, databases and web servers

a third type of public blockchain network

Bitcoin

2009

digital gold

Ethereum

2015

smart contracts

Internet Computer

2021

autonomous cloud

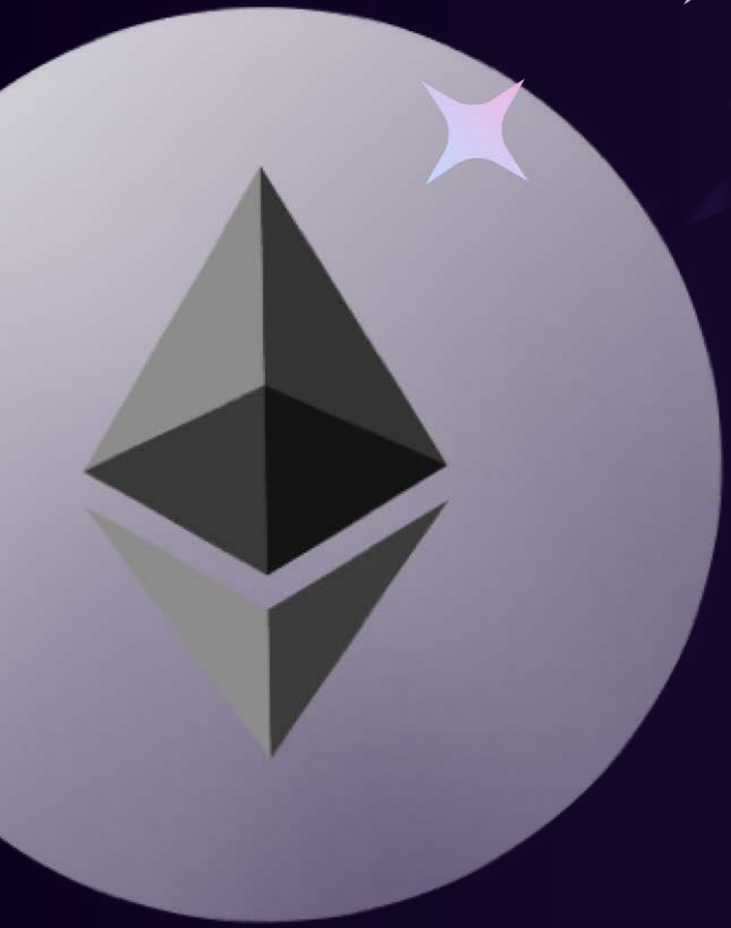
All-new blockchain science and engineering produced by hundreds of person-years effort at DFINITY has solved critical blockchain speed, efficiency, scalability, smart contract and user experience challenges allowing blockchain to act as a "stateful serverless autonomous cloud" that plays the role of a standalone, fully decentralized, alternative IT stack

Autonomous cloud runs tamperproof code without backdoors at scale

canister code

canister software is a new form of smart contract
code that has general application

smart contracts are a new form of software



ETHEREUM SMART CONTRACTS

tamperproof
firewalls aren't needed to protect software and data

tokenization
value can be held, processed and transmitted, like data

unstoppable
nuke-proof thanks to host network's fault-tolerance

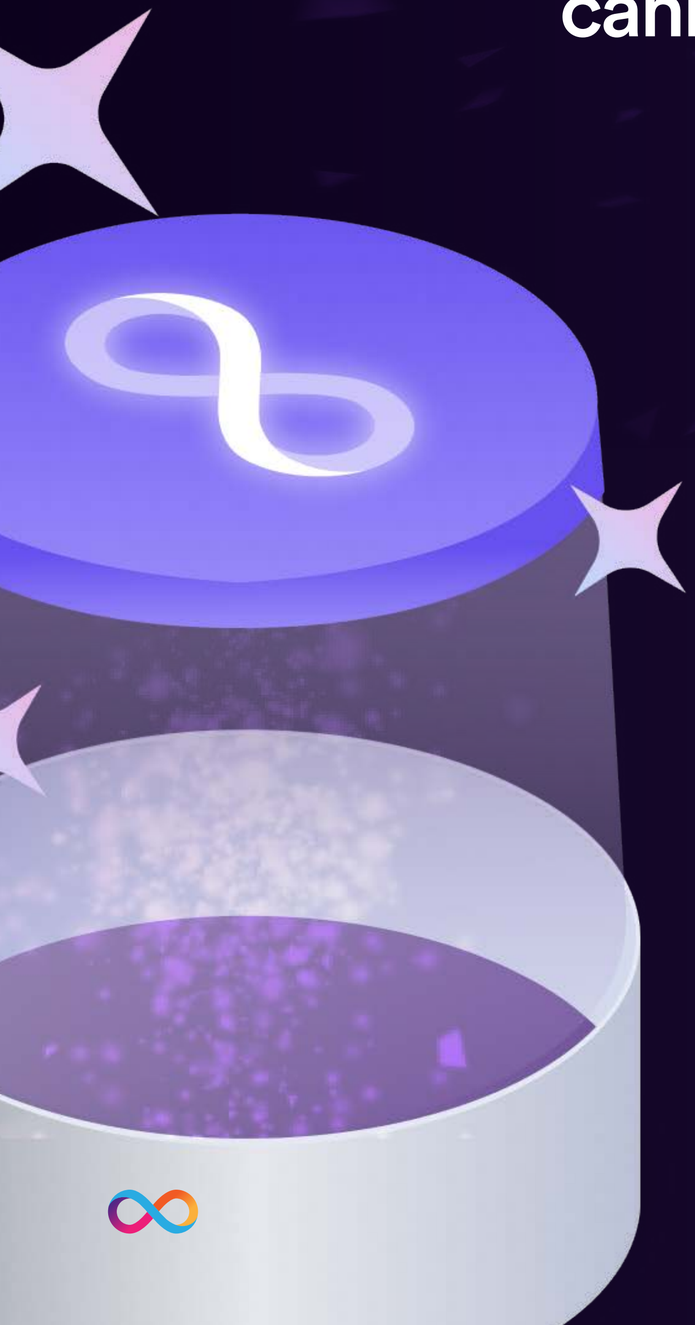
composable
easy collaborative building with less need for trust

autonomous
code can be unmodifiable, or assigned to a DAO

borderless
code and data in cypherspace, without geography

data inside
data lives inside software units, not databases or files

canisters are a new form of smart contracts



CANISTER SOFTWARE

fast
web-speed canister software doesn't make users wait

efficient
can reduce traditional IT carbon footprints

scalable
can support services that scale-out to millions or billions

low cost
costs reduced to < 0.0000001% traditional blockchains

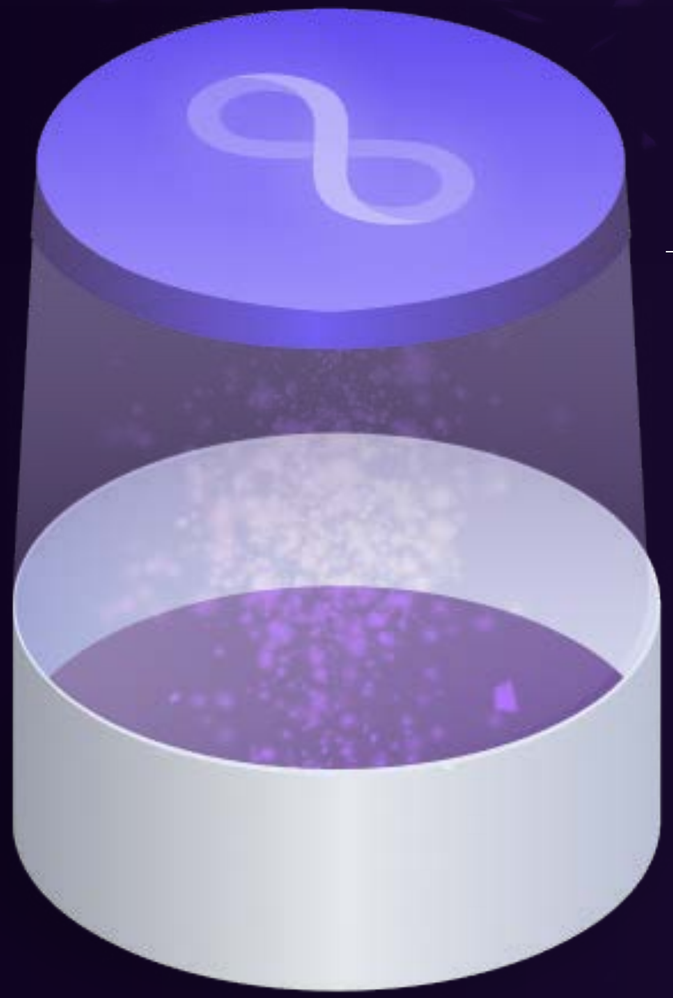
multi-chain
can natively interact with external blockchains

web interaction
directly process HTTP and serve user experiences

actor model
canisters keep data private and run in parallel. data persistence is "orthogonal"

the network runs canister code in parallel (deterministically)

each canister bundles some software logic and data



LOGIC | BYTE CODE

Canister software can be written in a wide variety of languages such as Rust, TypeScript and Motoko, and then compiled into Wasm byte code, which the Internet Computer runs on a WebAssembly virtual machine. Each canister is a “software actor,” which maintains its own data, and they run in parallel.

DATA | MEMORY PAGES

Since a canister is a “software actor” that can only access and process its own data, and communicates with other canisters purely via function calls. The data is held within persistent memory pages inside the canister, which the software logic runs within. In a scheme of “orthogonal persistence” code persists data in simple variables and data collections…

canister smart contracts are tamperproof software

TRADITIONAL SOFTWARE

⚠️ Invoked software may execute hacker-inserted logic.

⚠️ It can also process malicious data from hackers.

⚠️ Ransomware/viruses can encrypt and modify software and its data

Must depend on unreliable firewalls, SIEM logging, regular patching, and other security practices, to keep hackers away from infrastructure

TAMPERPROOF SOFTWARE

✅ Invoked software executes the defined logic accurately

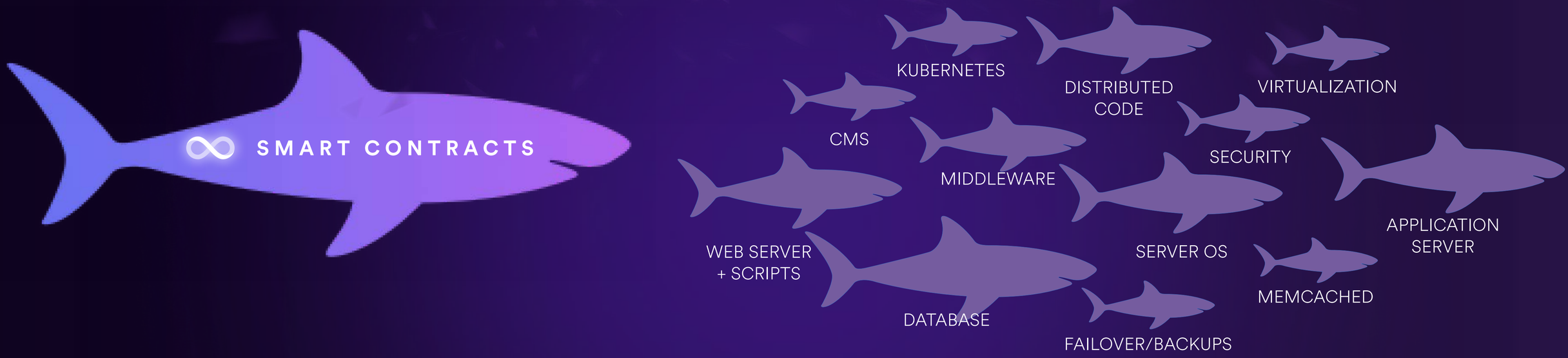
✅ It also processes its own data correctly

✅ Neither ransomware nor viruses can compromise the software or its data

✅ Both are hosted via a fault-tolerant and secure protocol

THE FUTURE

software will eat the world. smart contracts will eat software



Smart contract software will replace the legacy stack due to its overwhelming advantages

beyond web3

what the Internet Computer can solve for web3 builders in today's blockchain ecosystem

ICP solves for the final frontier of decentralization

centralized infrastructure

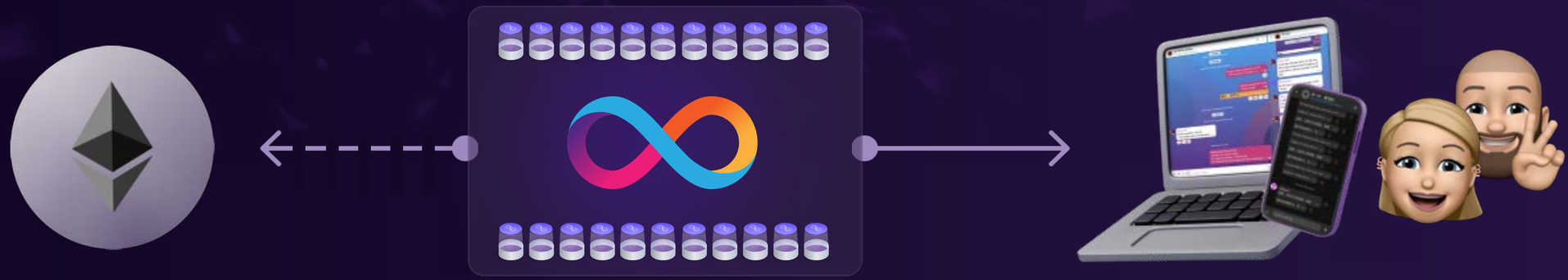
LEGACY IT

SMART CONTRACTS
ETHEREUM

WEB3 EXPERIENCES

hackers
censorship
gatekeepers
vested interests
ransomware virus
must trust developers

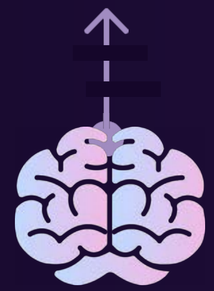
replace legacy IT with canisters on the Internet Computer



SMART CONTRACTS
ETHEREUM

CANISTERS
INTERNET COMPUTER

WEB3 EXPERIENCES



AUTONOMOUS GOVERNANCE
SERVICE NERVOUS SYSTEM

autonomy

The Internet Computer runs autonomously under the control of decentralized governance… and hosted web3 services and systems can too

three forms of Internet Computer autonomy

network autonomy

In order for the Internet Computer to host autonomous canisters, and autonomous systems and services, it must be fully autonomous itself. the network's design incorporates an advanced DAO into its ICP protocols, called the "Network Nervous System" (NNS). The network runs under the full control of the NNS, which updates its protocols, and instructs nodes to form into subnets, among other things.

DAO-modifiable canisters

In a similar way that the Internet Computer network was made autonomous by placing an advanced DAO in control, units of code can be made autonomous by placing a "service nervous system" DAO in full and exclusive control. This can then update and configure the canisters that form a service. A community or enterprise can control the DAO. There are no other ways to control the service.

immutable canisters

What if nothing should be able to modify canisters? For example, what about global financial rails that many other systems and services build on top of, or what about a wallet that must be absolutely secure? the Internet Computer network can host canisters that cannot be modified by anyone, which continue to exist and run so long as they are charged with "cycles" (the network's fuel for computation).

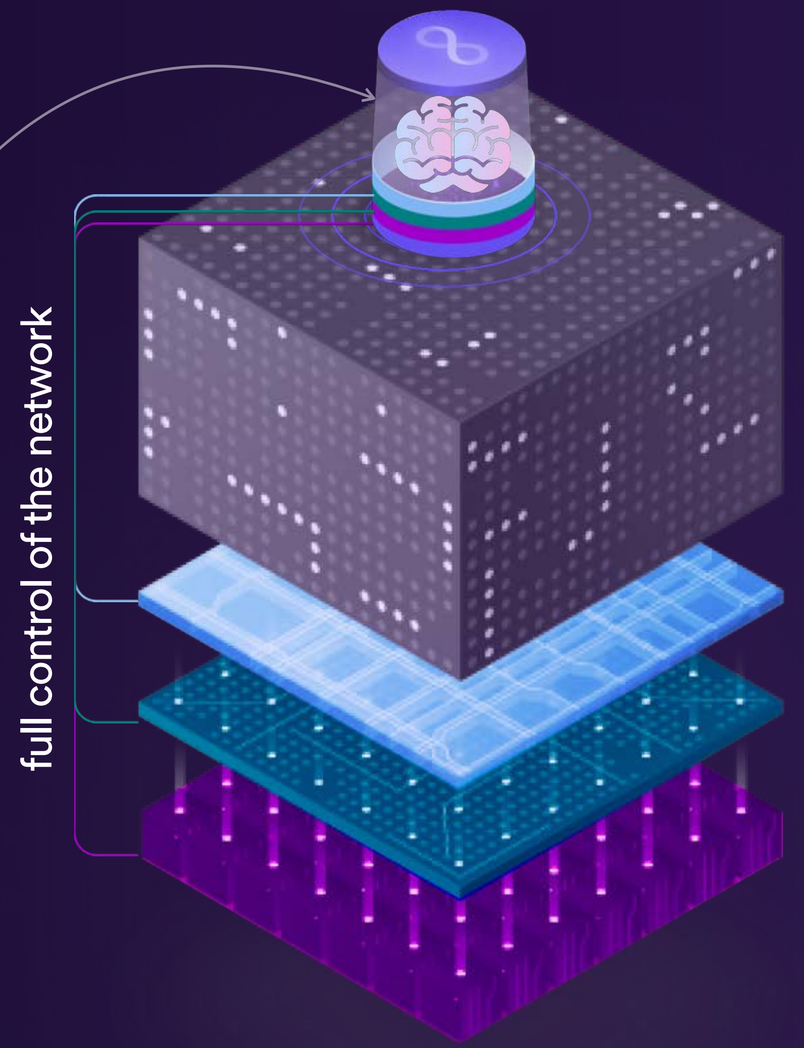
tip a DAO is a "decentralized autonomous organization" providing digital governance or democracy

DAO governance of the network

The “Network Nervous System” (NNS) is special DAO that runs as part of the ICP protocols. It enables the Internet Computer network to adapt and evolve autonomously

- Public, open, transparent and permissionless
- Users lock ICP tokens to create “voting neurons”
- Neurons vote automatically by following other neurons
- Tens of thousands of users have created neurons
- Submitted proposals are adopted or rejected
- Algorithmic liquid democracy decides on proposals
- Adopted proposals are executed automatically
- On instruction, nodes update the ICP protocol
- On instruction, nodes form into new subnets
- In 2 years, mainnet upgraded its protocols 145 times
- The network is autonomous / there are no backdoors

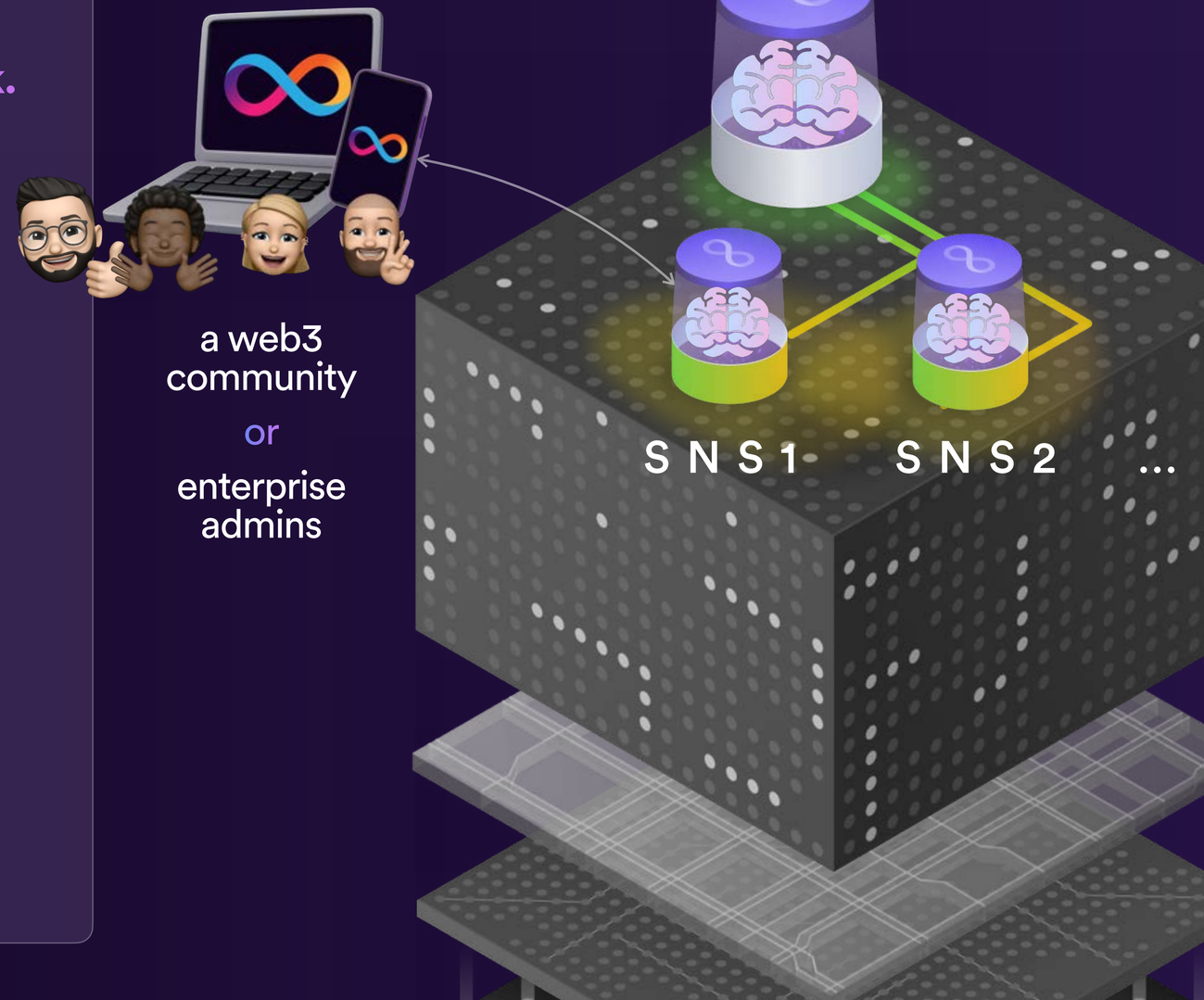
ICP
community



DAO governance of online services

Special “service nervous system” (SNS) DAOs can be given exclusive control of “open internet services,” which run autonomously on the autonomous network. NNS proposals create new SNS DAOs

- Open/permissionless (web3), or private (enterprise)
- The SNS updates its service’s canisters
- The SNS can perform arbitrary configurations
- An SNS can manage a token treasury (value)
- Services can be controlled by communities of millions
- Each SNS creates a ledger of native tokens for its service
- Tokens can incentivize decentralized community workforces
- Community fundraising into the SNS is possible
- Enterprise systems can distribute control for security
- Any complex service can be made autonomous
- NNS proposals create approved SNS DAOs



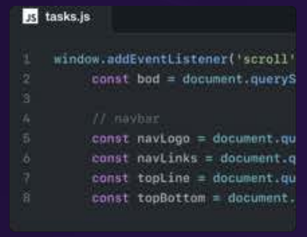
an open internet service (OIS) puts its community in control via an SNS

PUSH

software source code

GitHub

source code manager



code files

open source repository

PROPOSE

updates, fixes, configs,
payments, motions...

service nervous system

running service

open internet service

community

open internet services are a game-changing internet innovation

TRANSPARENT

every OIS is run by its SNS DAO: all updates fixes and configurations, and any uses of e.g. a token treasury, must be proposed, reviewed and adopted, before automatic execution

HIGHLY SECURE

every OIS is tamperproof, and can only be modified through its SNS DAO. only proposals adopted by its web3 community (or enterprise admin community) can e.g. direct it to update its code

SOVEREIGN

every OIS runs autonomously in an adaptive and self-evolving way. there are no backdoors through which decisions can be forced on the community (e.g. by cloud, developers, hackers…)

special web3 applications

PROJECTS CAN MAKE THEIR USERS INTO FOUNDERS

governance tokens created and distributed to decentralize control of an SNS DAO (and thus the OIS), can be used to make the users of an OIS into project founders, who help run and promote the service. millions of users can be founderized

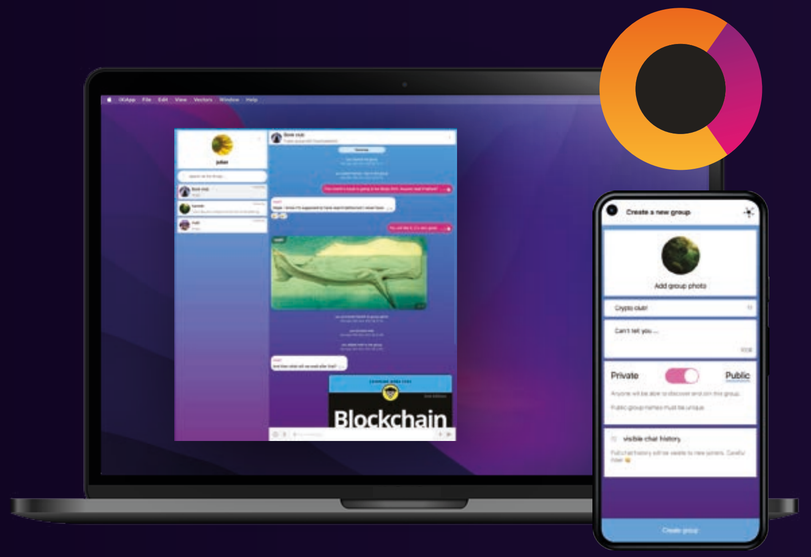
INDUSTRIOUS VIRTUAL WORKFORCES & ECONOMIES

an OIS can disburse tokens to those creating viral content, or moderating content, or submitting improvements that are adopted. tokenomics can create self-sustaining high-growth digital economies

web3 → Web 3.0

the Internet Computer is a Web 3.0 platform that
delivers full stack decentralization

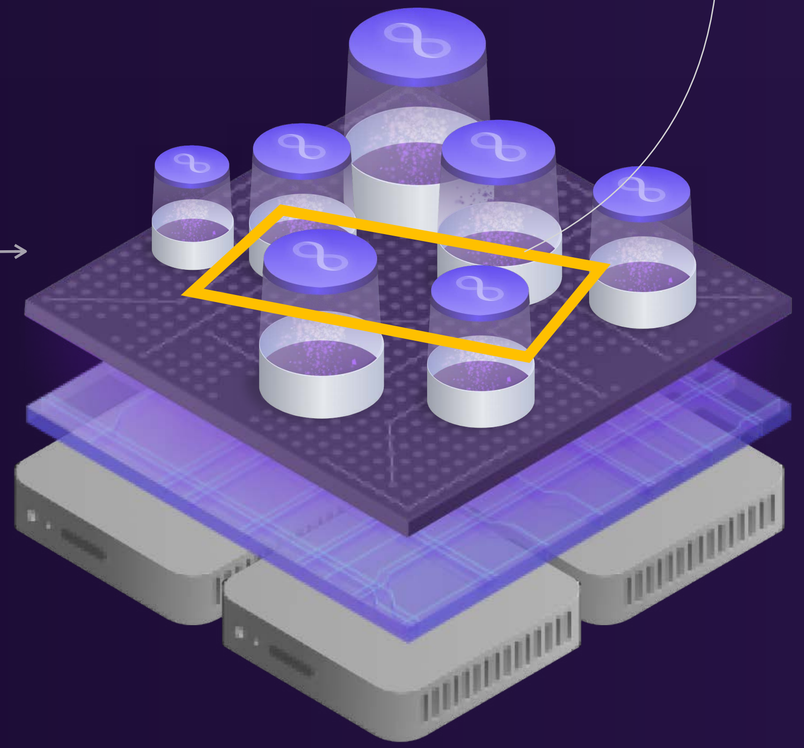
users interact with services over HTTP (the web)



WEB3 EXPERIENCE

Web browsers interact with canisters over HTTP

(100,000s of canisters used by e.g. OpenChat)



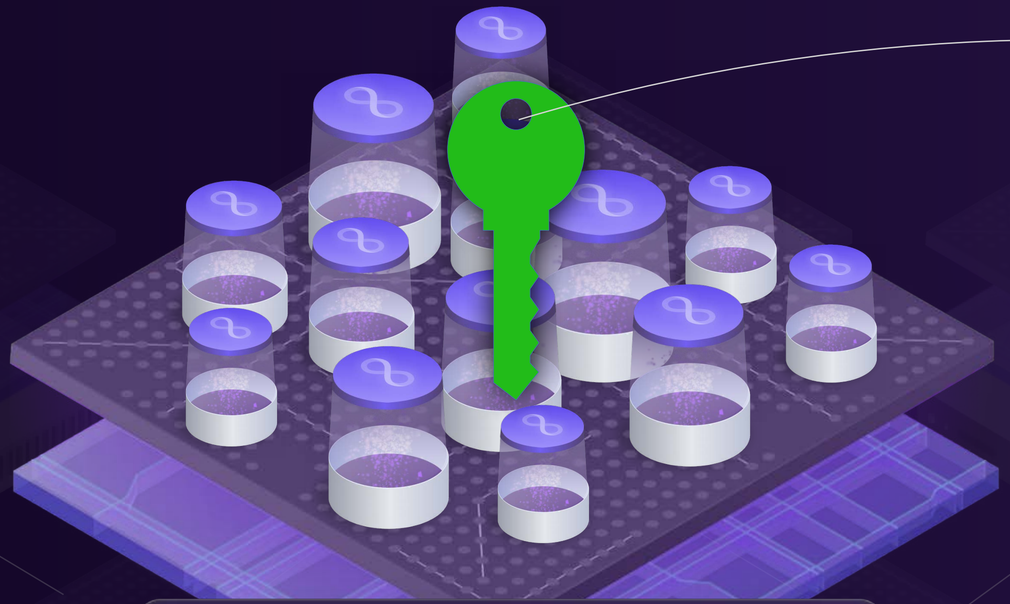
Crypto tip canisters pay for their own computation (“reverse gas”) so end-users don’t need wallets

Internet Identity frameworks create sessions for user interaction

WEB3 EXPERIENCE

Secures sessions allow user experiences to transparently create multiple transactions a second

incredibly, the ICP network has one master 96-byte public chain key



The master chain key is virtual and the private key cannot be stolen: only the network itself can sign

1 MASTER
CHAIN KEY

Unique **chain key cryptography** is what makes the Internet Computer network possible

The Internet Computer's master chain key

```
308182301d060d2b0601040182dc7c0503010201060c2b0601040182dc7c05030201036100814c0e6ec71fab583
b08bd81373c255c3c371b2e84863c98a4f1e08b74235d14fb5d9c0cd546d9685f913a0c0b2cc5341583bf4b4392
e467db96d65b9bb4cb717112f8472e0d5a4d14505ffd7484b01291091c5f87b98883463f98091a0baaae
```

–– any software system with this magic number can ––

VERIFY INTERACTIONS

holders of this master chain key, such as front-end software running in a web browser, can check special signatures on the results of submitted transactions (i.e. the results of invocations of canister smart contracts) to verify that they have not been tampered with

VERIFY CORRECTNESS

when the holder of this master chain key verifies that the results of their transactions (i.e. function invocations) have not been tampered with, it also proves to them that the Internet Computer is running correctly, and that the result was correctly produced

technological breakthrough removes the need to run a local node to securely interact with a blockchain

experience

The Internet Computer is a Web 3.0 platform that decentralized the entire stack – and provides a new experience

INTERNET IDENTITY

Interoperable

Share credentials across different web services and platforms in a privacy-preserving manner.

Easy to use

No need to deal with seed phrases or manage endless usernames and passwords. Simply unlock your device to create a secure session.

Sovereign

Internet Identity relies on key pairs securely maintained within TPM chips on your devices. Because interactions are signed inside the chips, the keys cannot be stolen.

Highly secure

Based on FIDO Alliance and W3C standards, cryptographic key pairs are stored in special secure hardware on your modern device (inside TPM chips).

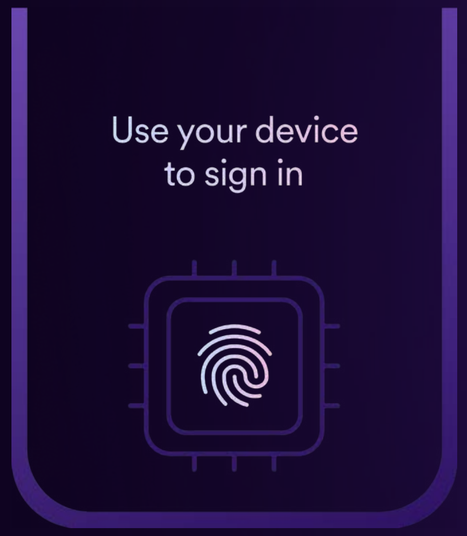
Open source

Developers can audit and contribute to the codebase to ensure that it meets the highest standards of security and transparency.

No tracking

A different pseudonym is created for every service you interact with, preventing services linking their users e.g. as per SSO.

INTERNET IDENTITY



TPM

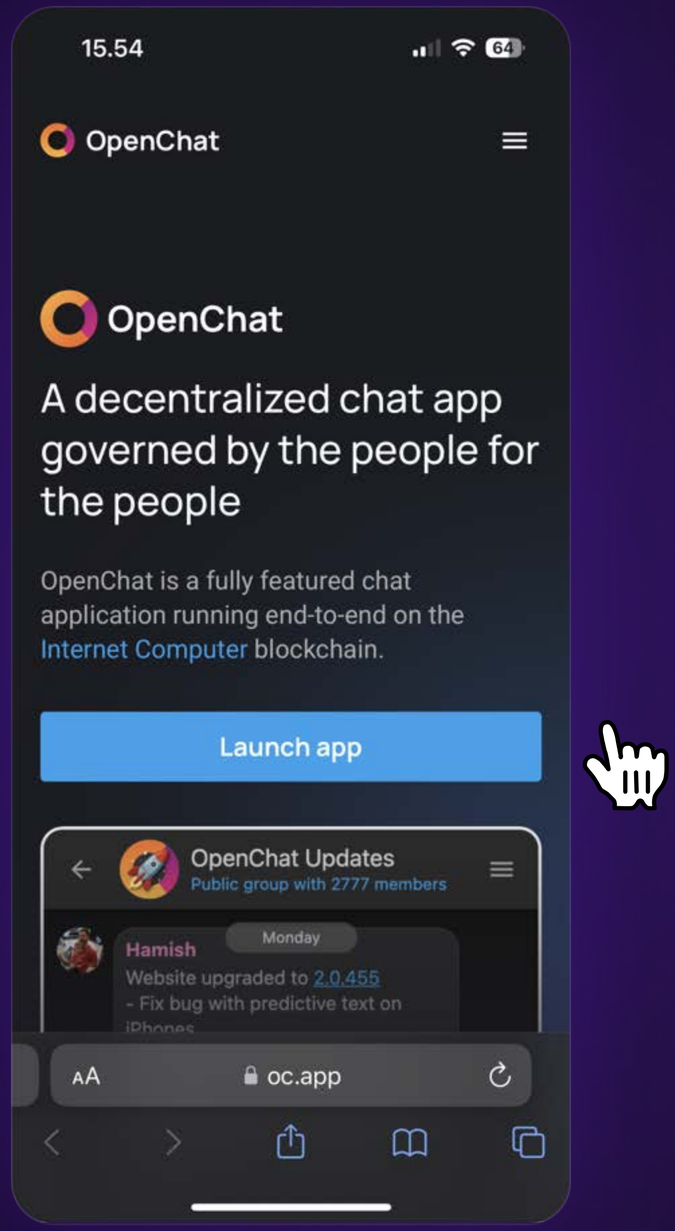
+

WebAuthn (+ FIDO)

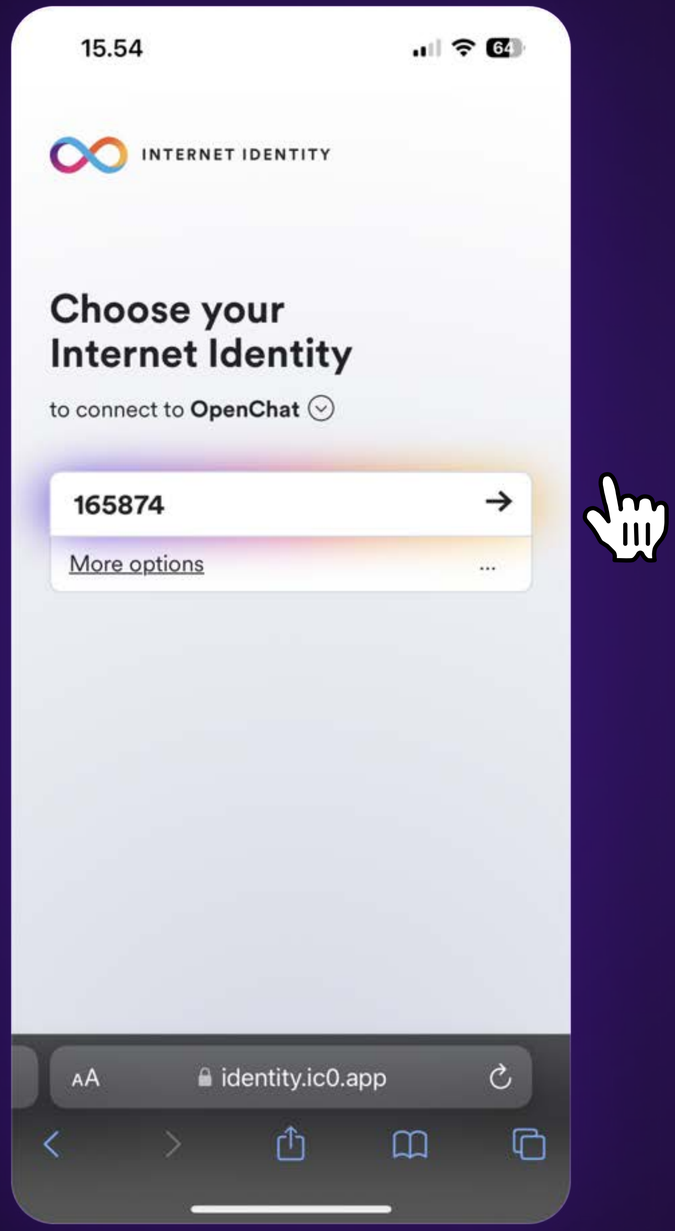
+

Internet Computer

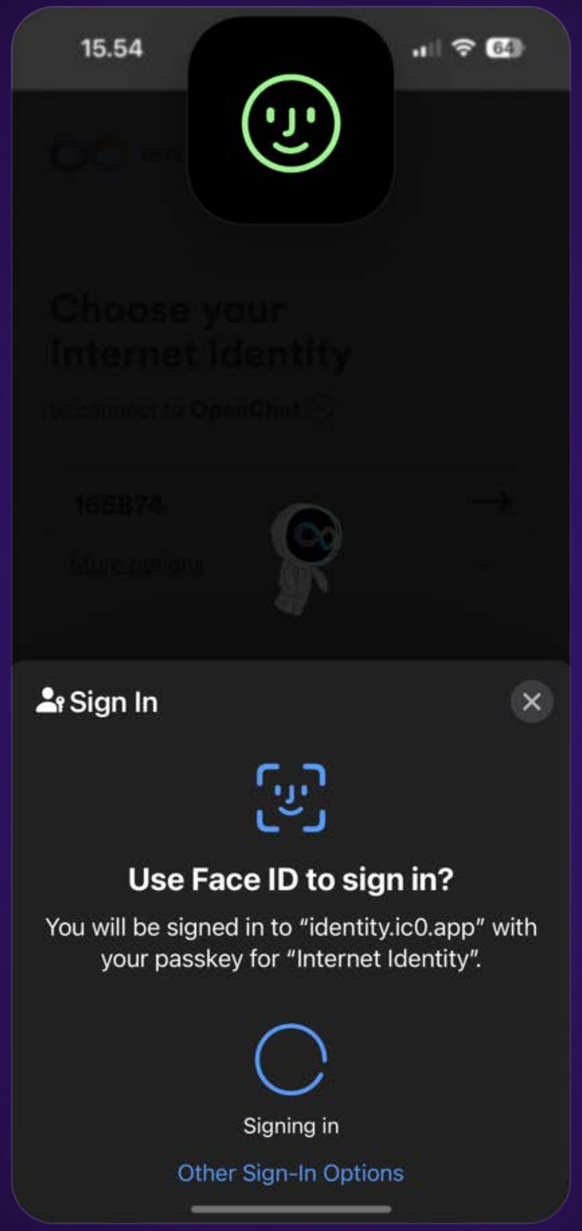
INTERNET
IDENTITY



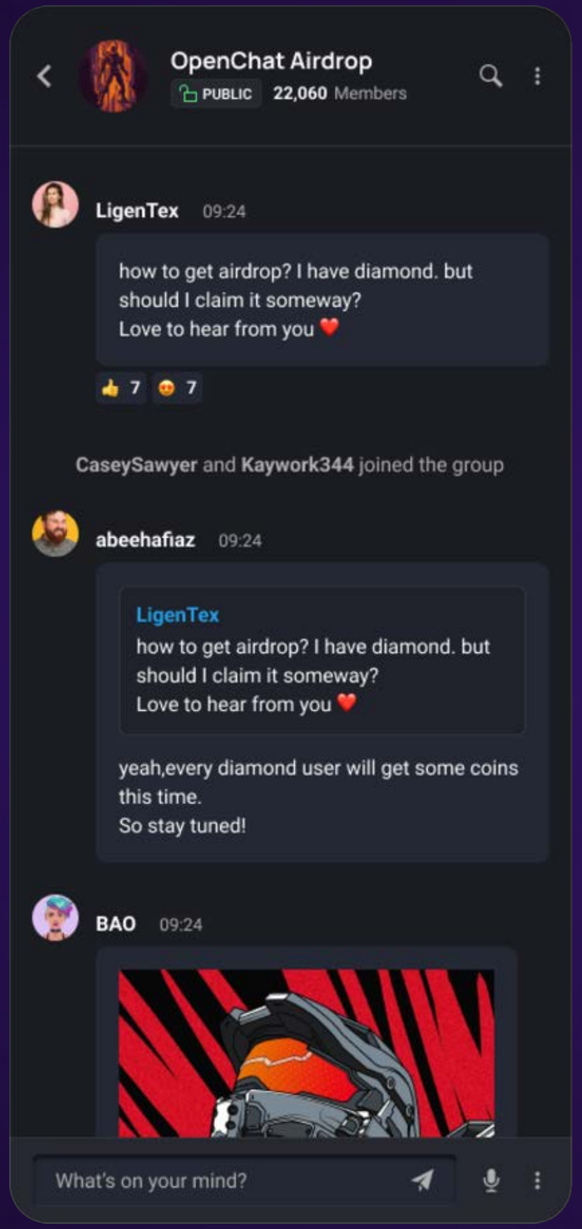
INTERNET IDENTITY



INTERNET IDENTITY



INTERNET
IDENTITY



Where we are now

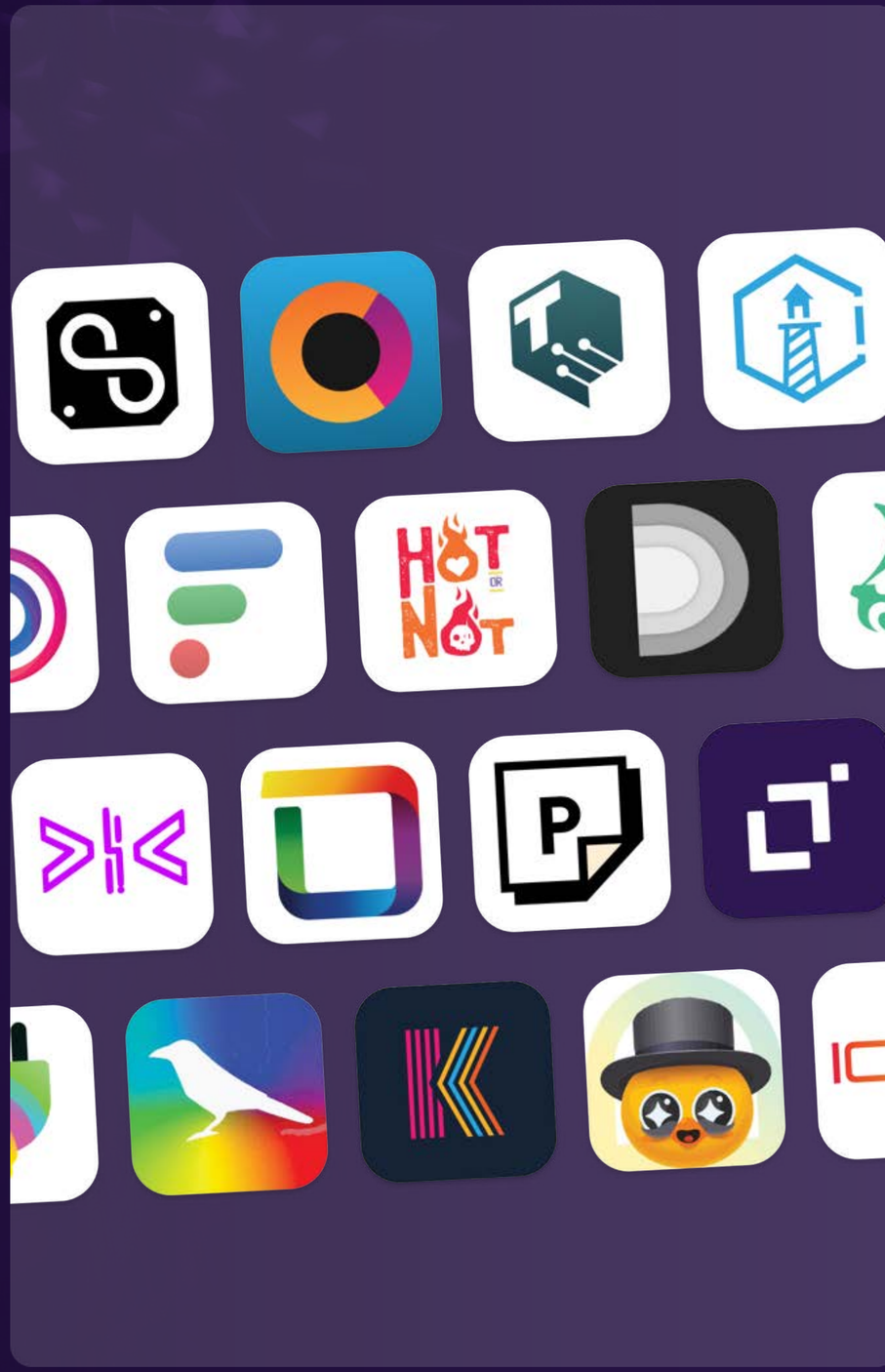
2.2M+

Identities created

100+

Dapps using II for authentication

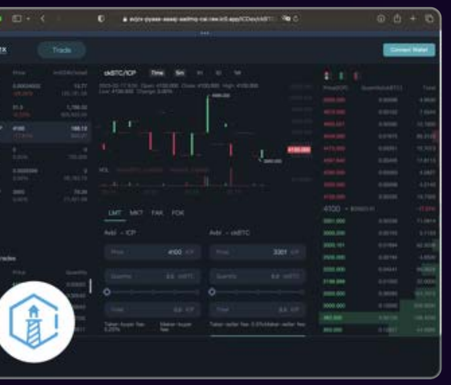
Support for zero knowledge identity attestation coming soon...



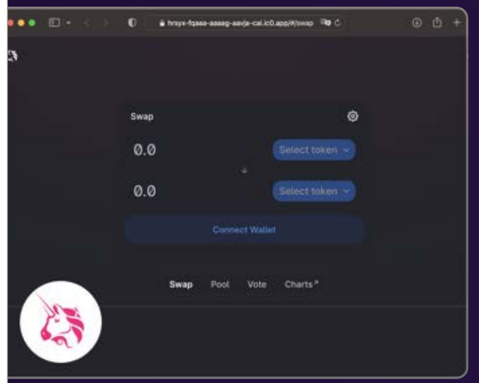
autonomous services are real web3 and can be more compelling

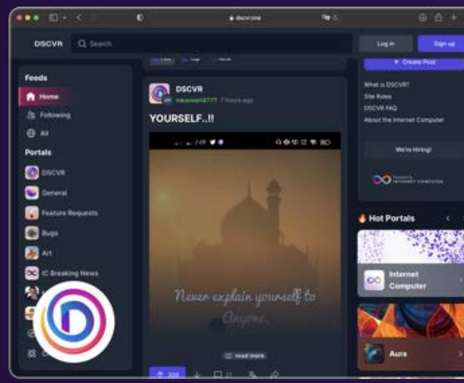
Community DAOs have complete control · tokenization works without crypto wallets or friction

full tokenization can transform user communities into giant industrious virtual workforces



INTERNET COMPUTER



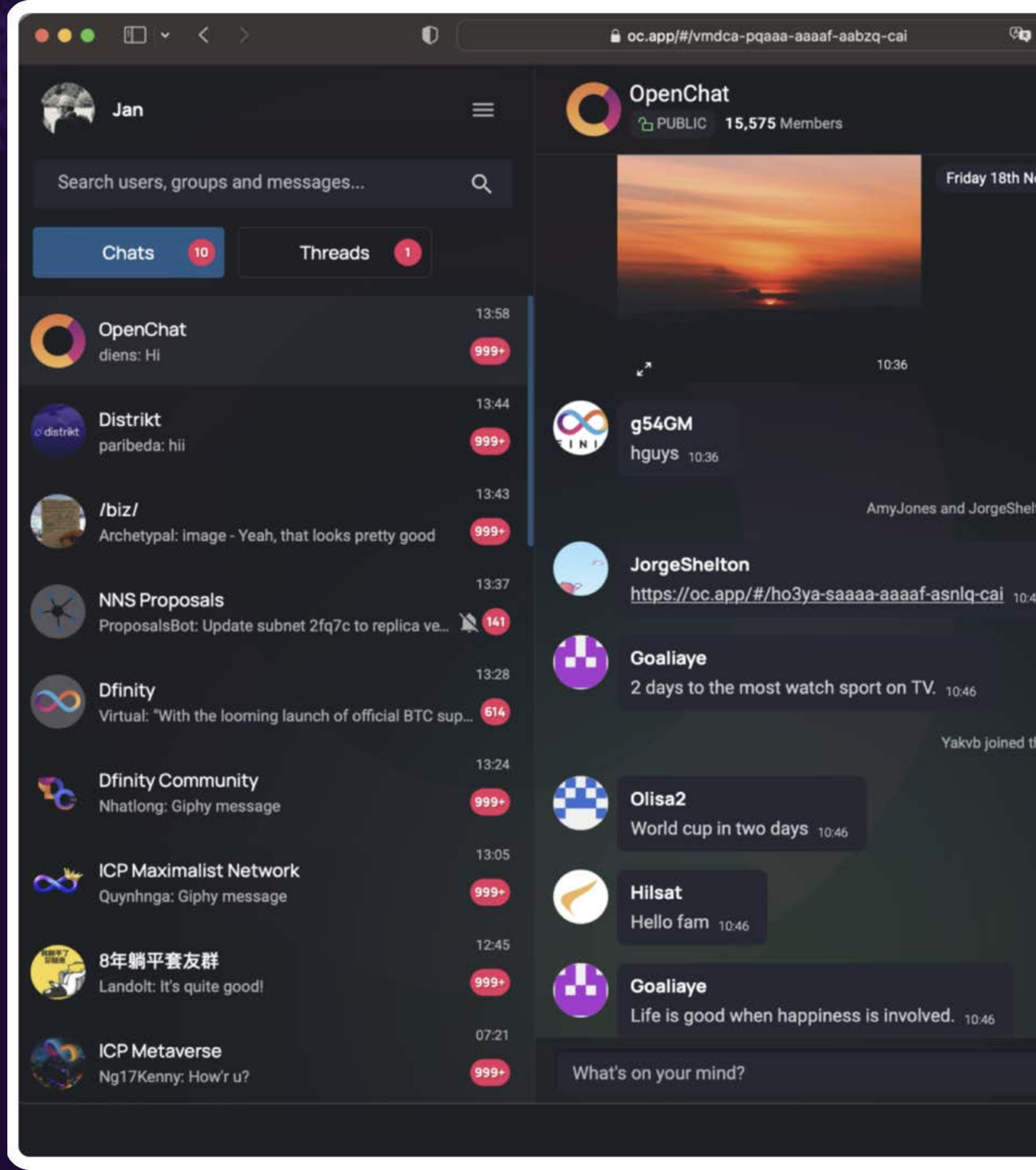


Browse dapps in the ecosystem

OC.app

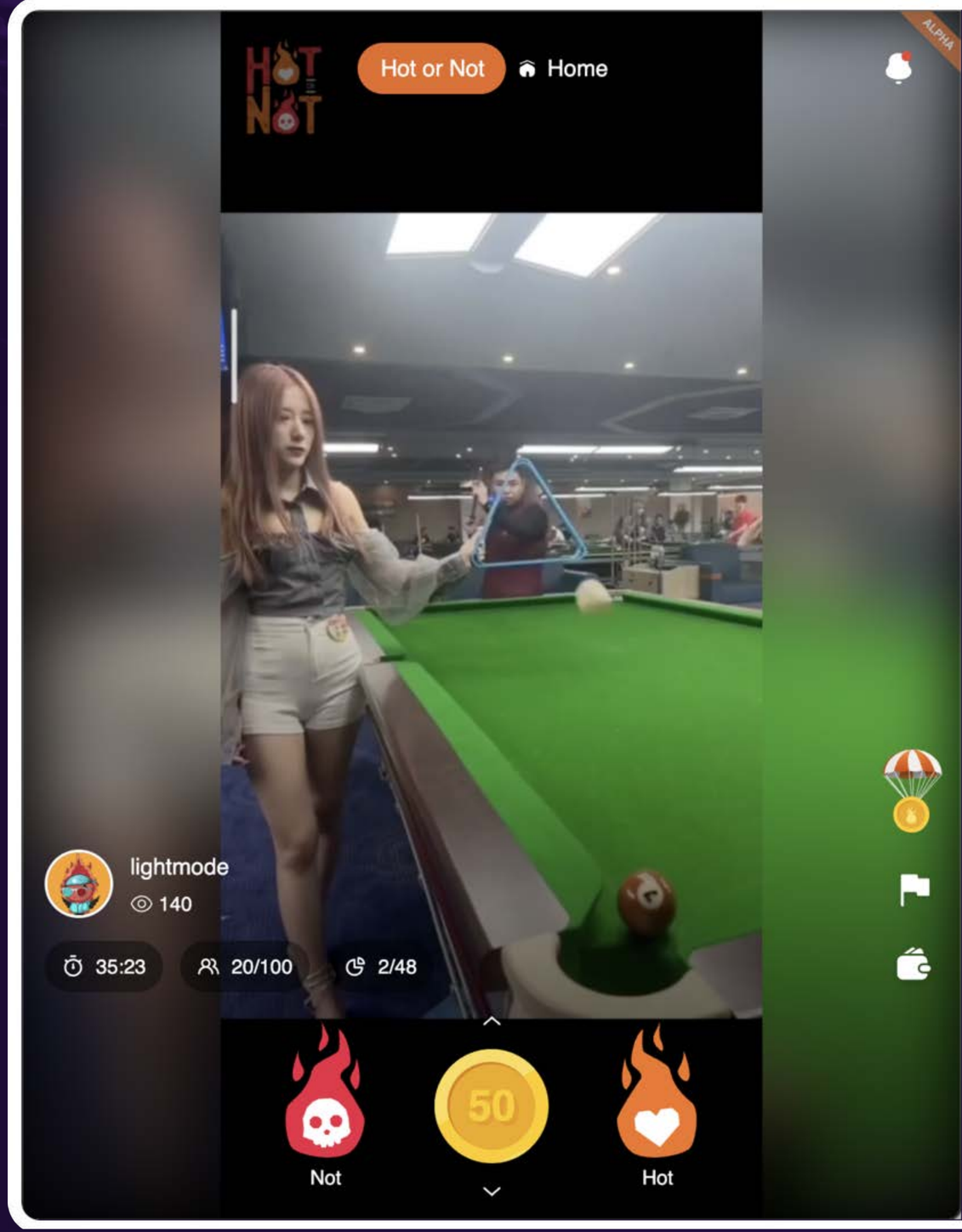
OpenChat was the first true “open internet service” on the Internet Computer

- Messaging service runs 100% on network
- Chat accounts are also crypto wallets i.e. full SocialFi
- Seamlessly send satoshis using chat messages
- Users hold governance tokens (called CHAT)
- Bounties for users promoting OpenChat
- Rewards for those creating viral content
- Updates pass transparently through governance
- Runs as protocol with an SNS in full control
- “Communities” feature is alternative to Slack

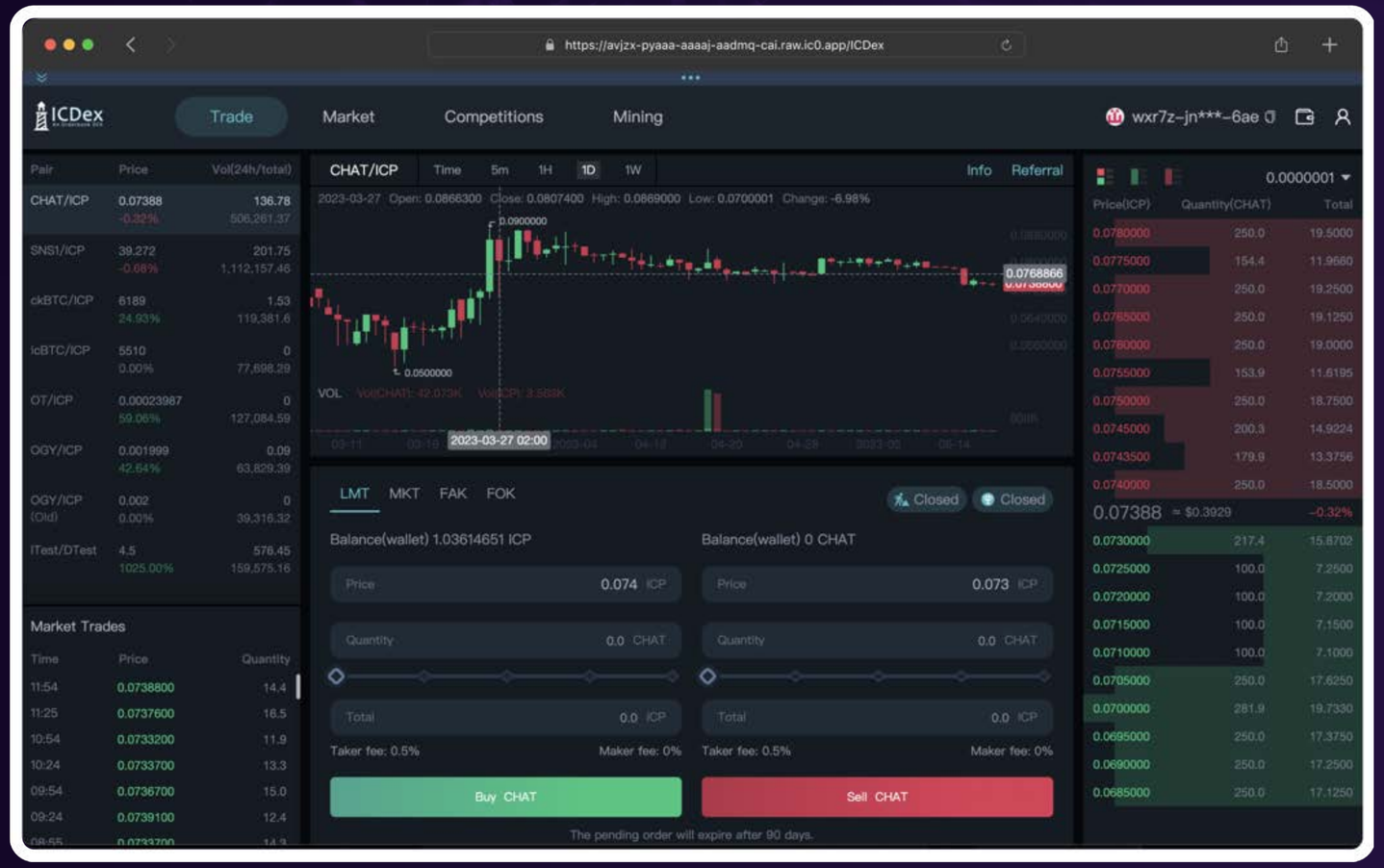


HotOrNot.wtf

- Tokenized TikTok built on the network
- Creates an ingenious decentralized economy
- Users bet HOT on whether videos will go viral
- Users help with content moderation too
- Creators of viral videos get HOT tokens
- Eventually, advertisers will pay with HOT tokens
- The OIS inverts centralized business models...
- Video creators and users are made into founders
- Runs as protocol with an SNS in full control



ICDEX.io – an order book exchange that is a smart contract



- Built exclusively from tamperproof canister smart contracts
- SNS DAO can make transparent and autonomous

Web3 pioneers are building a bright new future on the Internet Computer

Join the movement

WEB 2	WEB 3
TikTok	HOT OR NOT
Gmail	DMAIL
reddit	DSCVR
FTX	ICDex An Orderbook DEX
Telegram	OpenChat
X	distrikt
Spotify	CANISTORE
KICKSTARTER	Funded
eventbrite	CATALYZE
GoDaddy	ICNS ICNAMING
Dropbox	IC-Drive

services built differently...

real world experience demonstrates a giant leap forward

no cloud. no database servers.

web3 services can be built entirely from canister code:

the network is the tech stack

no firewalls or SIEM logging…

web3 services don’t need firewalls to protect them:

canister software is tamperproof software

cool services. tiny tech teams.

web3 services are sophisticated and scale to large numbers of users, but:

far fewer engineers are required to create them

cloud 3.0

the Internet Computer can deliver tremendous advantages to the enterprise sector

building with canister software significantly reduces IT personnel spend

CANISTERS

If everything was built using canister software

$1.35 trillion in potential savings

LEGACY IT STACK

Developers, administrators, security team, maintenance...

2024

$1.8 trillion

Gartner Research

the Internet Computer stack addresses numerous core IT costs

Gartner Research

Software (e.g. databases)

2023

$912 billion

Gartner Research

Cloud services

2023

$600 billion

Gartner Research

Data Center Systems

2023

$224 billion

Reduce IT costs

tamperproof systems and services address security costs

Gartner Research

Cybersecurity

2022

$172 billion

Gartner Research

CPS incident costs

2023

$50 billion

Reduce security costs

sovereignty

countries relying on cloud infrastructure and closed-source software foundations can be spied on and even “switched off”

will corporations issue our future global identities...

=

“I use Google for everything”

A top YouTuber is publicly sparring with the platform after he says 'hundreds' of his fans unfairly lost access to their Google accounts

businessinsider.com

depend on corporations?

The world needs tamperproof open solutions

sovereign societies cannot depend on digital foundations in which other states might have kill switches and backdoors

- ✗ cloud computing services
- ✗ closed-source software

- ✗ SSO (single sign-on)
- ✗ security infrastructure

sovereign subnets coming

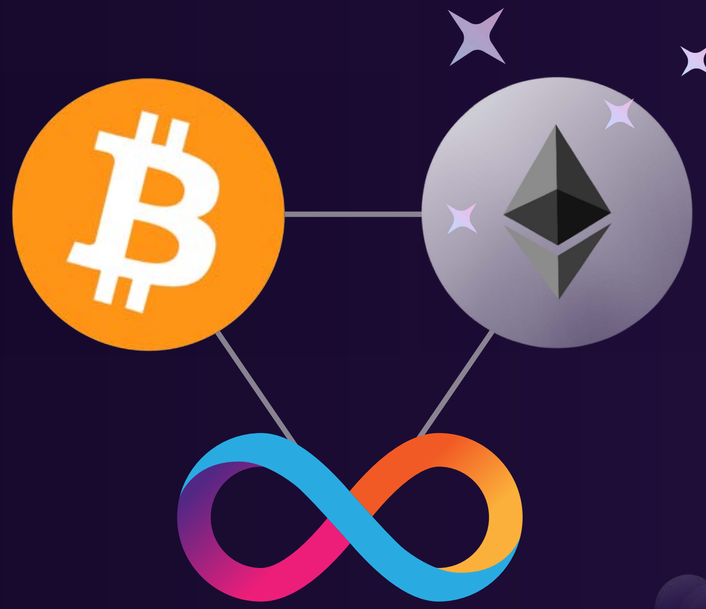
The Internet Computer network will create geographically-local specialized sovereign subnets for nations

No insecure centralized bridges, just trustless cryptography

multi-chain

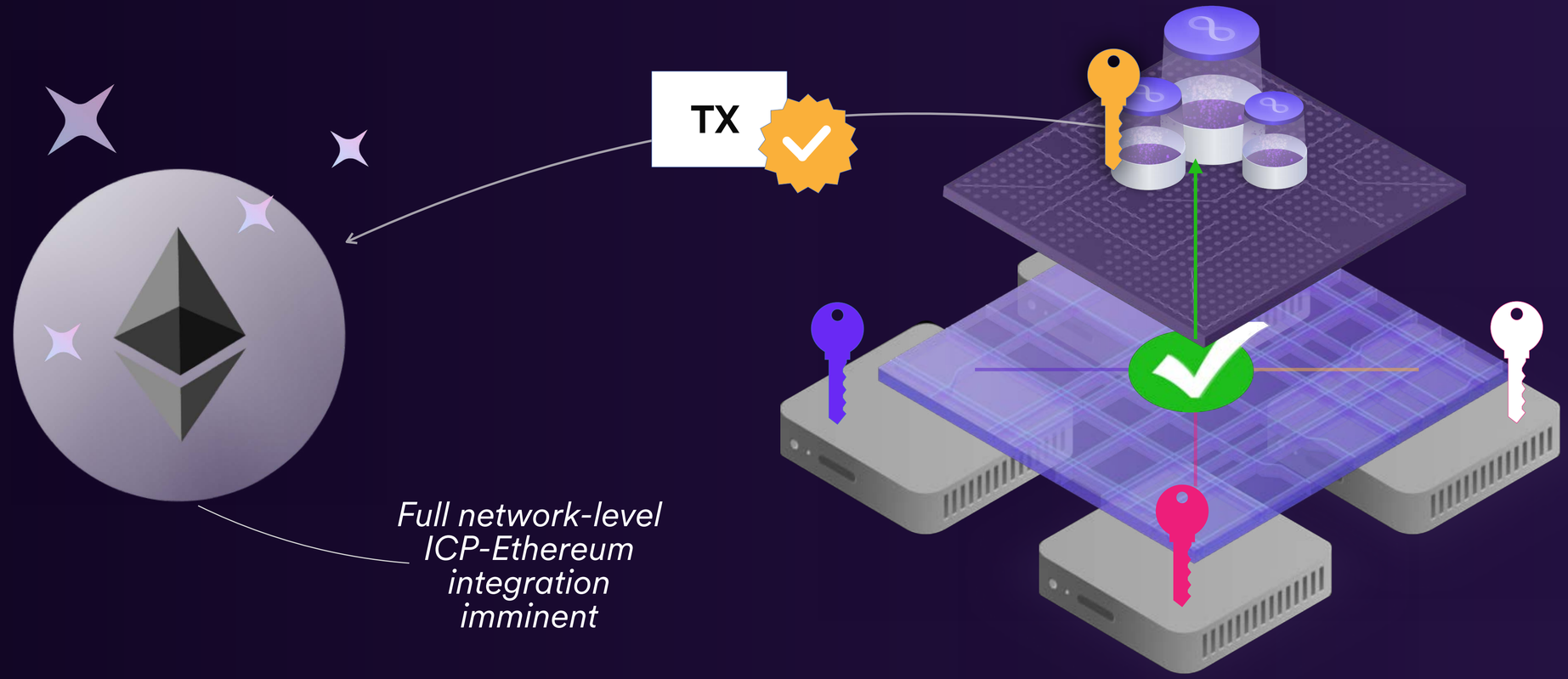
"chain key cryptography" creates transactions on other chains. network-level integrations with Bitcoin and Ethereum

Internet Computer enables the World Computer vision from 2014



NEW

canisters create accounts and sign TXs on other blockchains

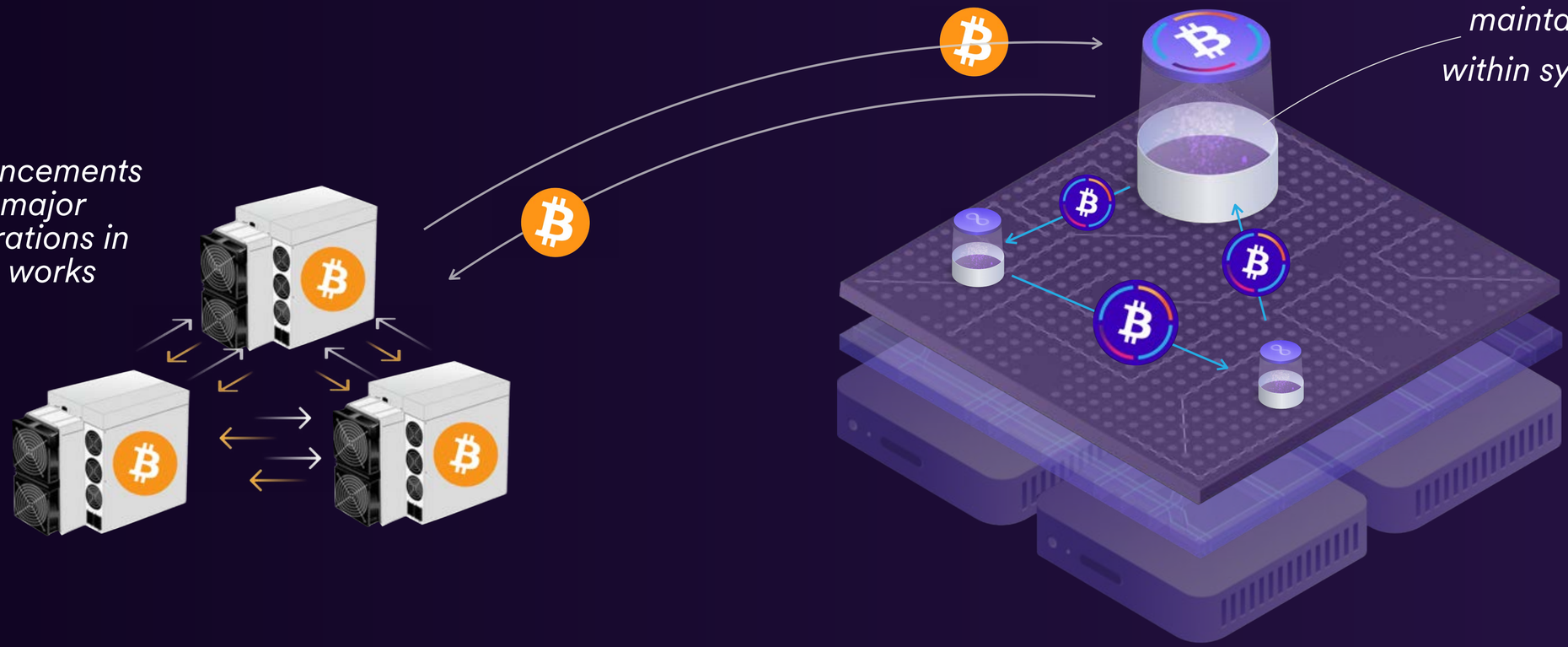


Signing performed by chain key cryptography – without need for traditional private keys

NEW

ckBTC is a bitcoin twin that can be directly processed by canister code

announcements of major integrations in the works



entire UTXO set maintained by ICP within system canister

chain-key bitcoin supports bitcoin DeFi, social media, games, and metaverse TX with 1s finality

Web 3+2

canister smart contracts can trustlessly call into external Web 2.0 systems – the network passes results through consensus

1

Canister code initiates http call to web2

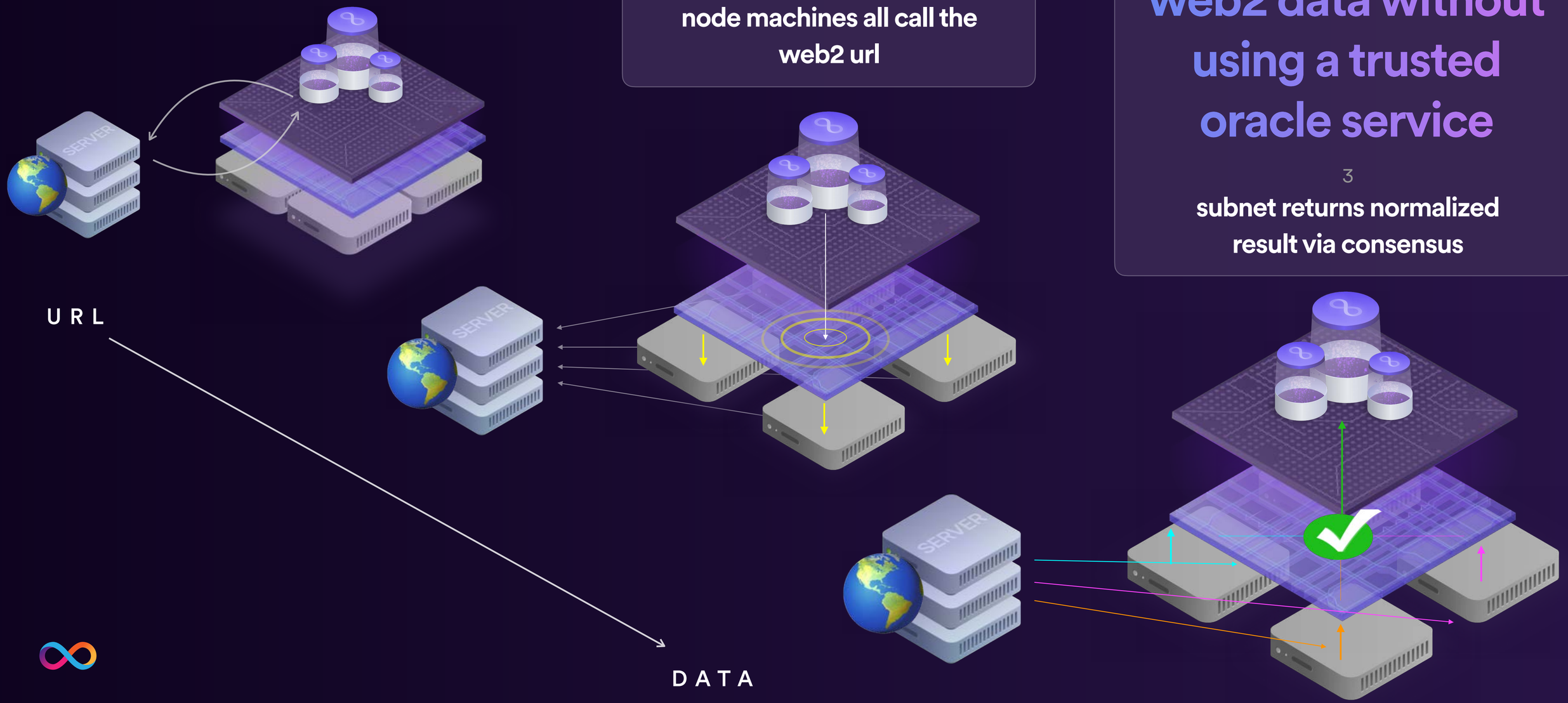
2

node machines all call the web2 url

canister code can directly request web2 data without using a trusted oracle service

3

subnet returns normalized result via consensus



Web 3|2 will be a continuum

DeFi contracts can obtain pricing information from exchanges,
enterprises can integrate ICP systems with legacy systems ...

AI

Projects are already running ai models as canister smart contracts on the Internet Computer

ICP ai compute units under development with a pathway to support for efficient ai smart contracts

trustless models data partitioning web3 integration

AI

by 2030 AI will

increase the productivity of knowledge workers

4X

boost global productivity creating extra value

$200

trillion

In the future ai models will analyze nearly all our business data

In the future ai models will generate nearly all our metaverse content

In the future ai models will be inside systems e.g. compressing media data

Mission

enable the reimagination of humanity’s systems and services through full stack decentralization on the Internet Computer

Internet Computer network growth is substantial

TODAY

250,000

ETH equivalent TX/second

DFINITY Foundation 🇨🇭

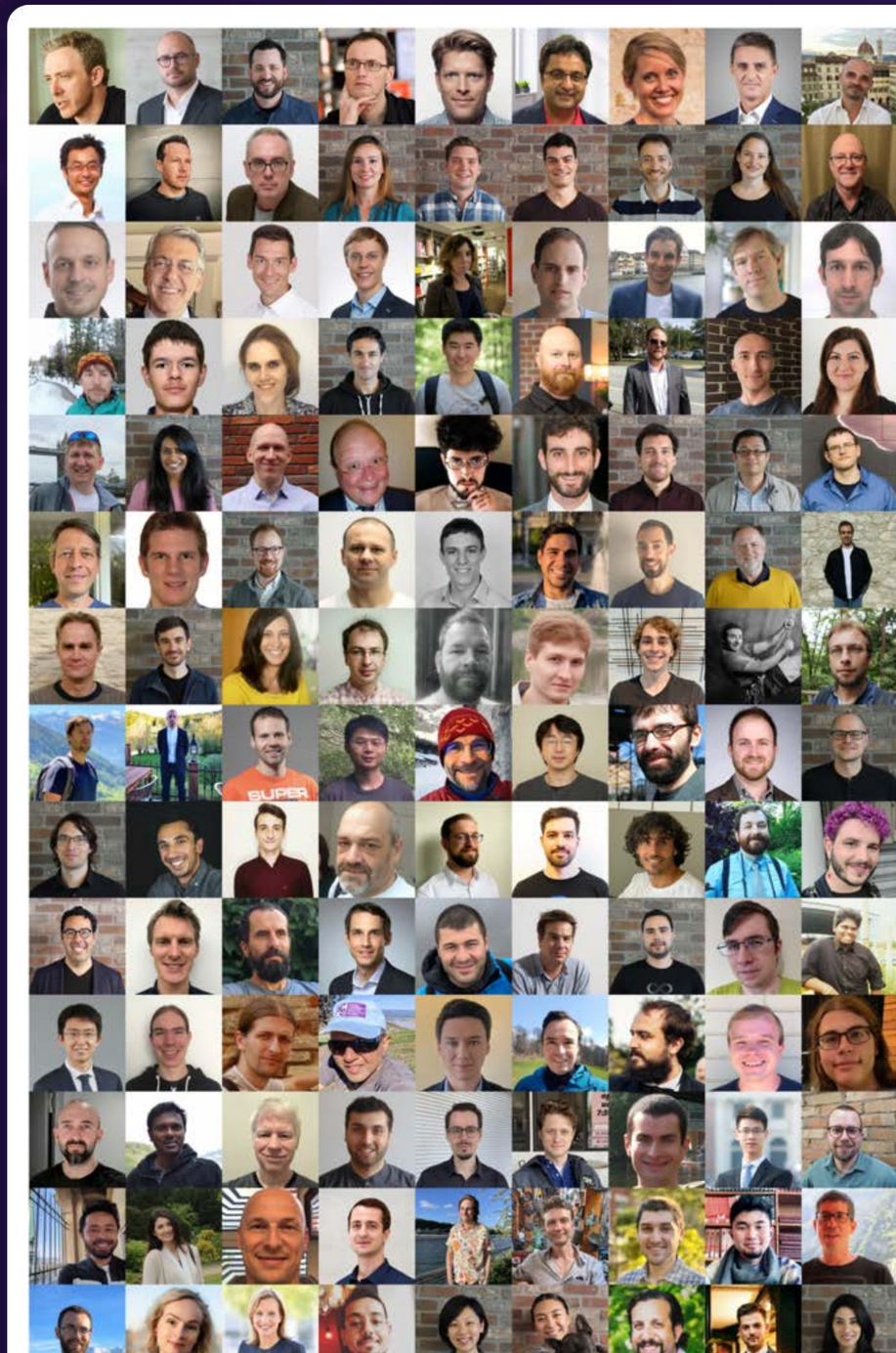
- emerged from early Ethereum community in 2015
- DFINITY Foundation established October 2016
- Swiss not-for-profit foundation, not a corporation
- world’s largest team of cryptographers
- over 140 employees in Zürich HQ
- 270+ team members globally

1600+
research papers

100 000+
academic citations

250+
technical patents

early blockchain community + Google IBM facebook



Build on the network

PARTNERSHIPS

partnerships@dfinity.org

COMMUNITY

community@dfinity.org

GRANTS

grants@dfinity.org

PRESS

comms@dfinity.org

Make everything web3

internetcomputer.org

World Computeris our future