INTERNET COMPUTER

Build on the network

ICP | Internet Computer

Main deck version: 12 August 2023

Dominic Williams

President/Chief Scientist @DFINITY Foundation

tech history arcs towards open networks

PRIVATE INFRASTRUCTURE		OPEN NETWORKS
INFORMATION SUPERHIGHWAY curated walled-garden network proposed by Microsoft and Oracle (1990s), AOL…	→	**THE INTERNET** private routing devices connected by TCP/IP create an open public global network
TRADITIONAL IT cloud services, databases, middleware, web servers, CDNs, firewalls…	→	**INTERNET COMPUTER** private node machines connected by ICP create an open public serverless autonomous cloud

INTERNET COMPUTER

INTERNET IDENTITY

build on the network

OPEN INTERNET SERVICES

build transparent autonomous web3 services that communities run using powerful decentralized governance, with no backdoors for devs, organizations or CEOs

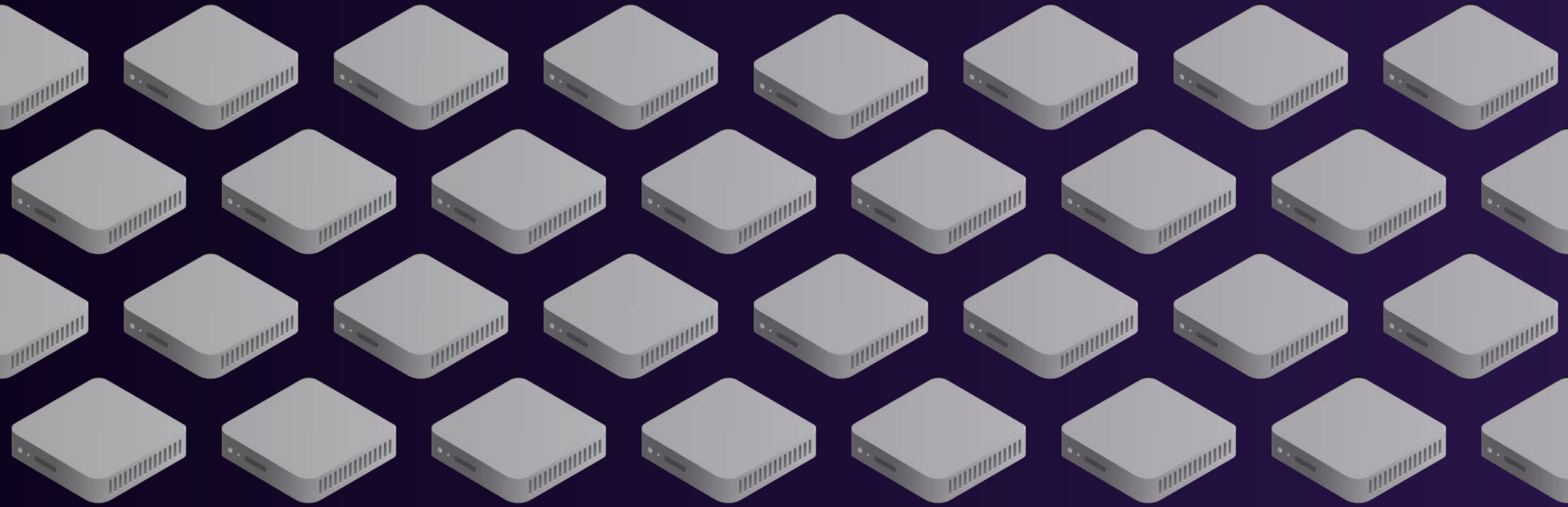
SOVEREIGN ENTERPRISES

build unstoppable infrastructures on an open network using tamperproof software without the third party backdoors and kill switches of closed source and cloud

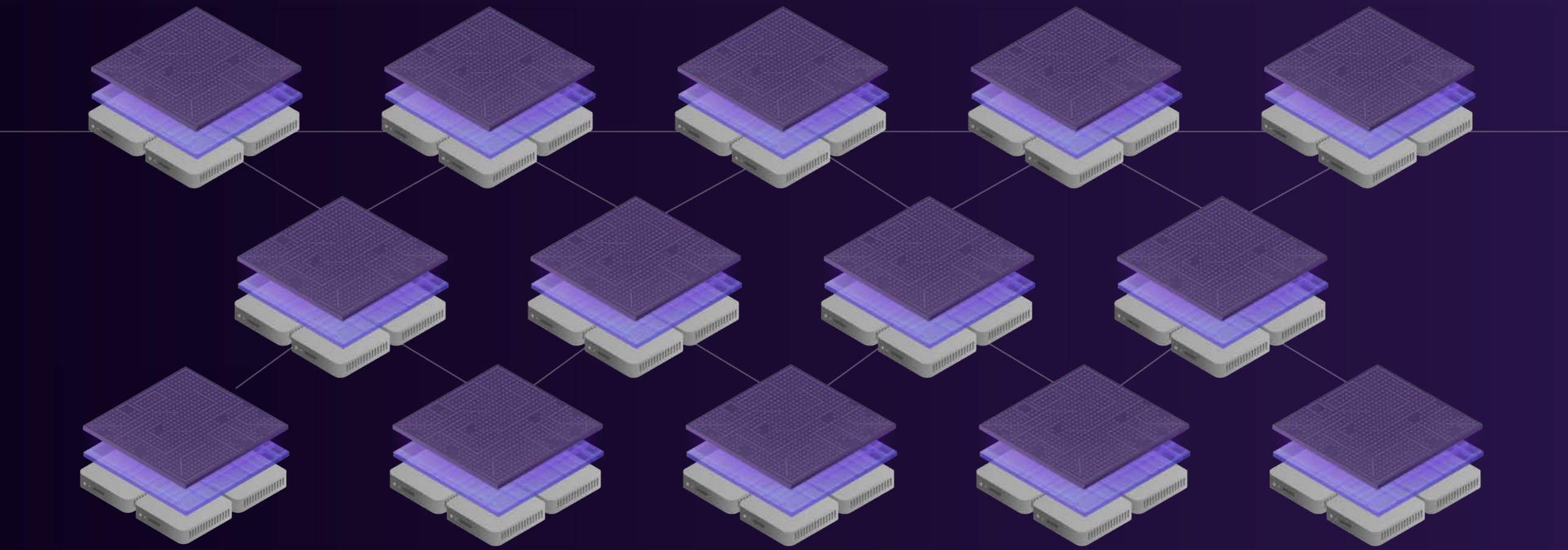
network

the Internet Computer is created by the Internet Computer Protocol, the most advanced network protocol ever devised

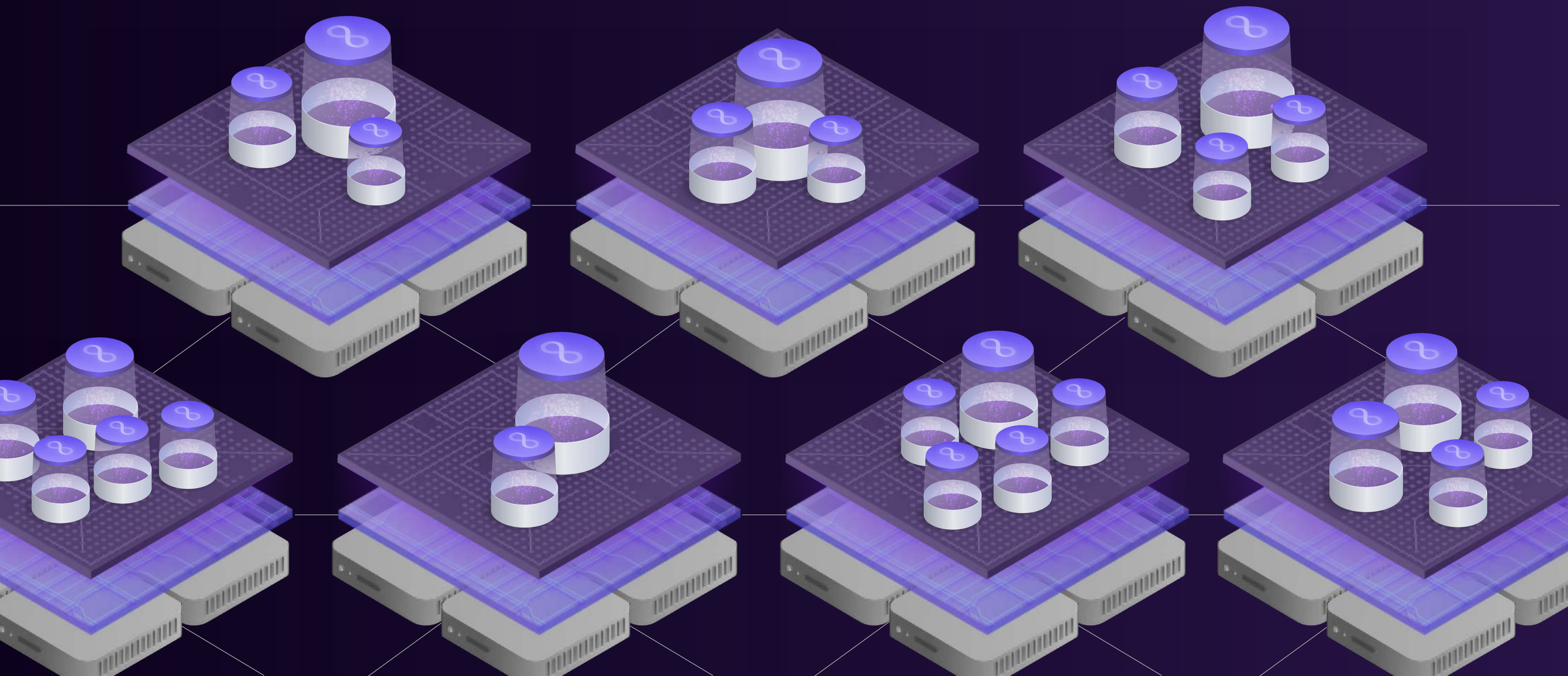
independent node providers own and operate
node machines in data centers worldwide



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



subnet blockchains add capacity for running *canister* smart contracts



subnets combine into ONE serverless *autonomous* cloud

a new form of blockchain network emerges

Bitcoin

2009

digital gold

Ethereum

2015

smart contracts

Internet Computer

2021

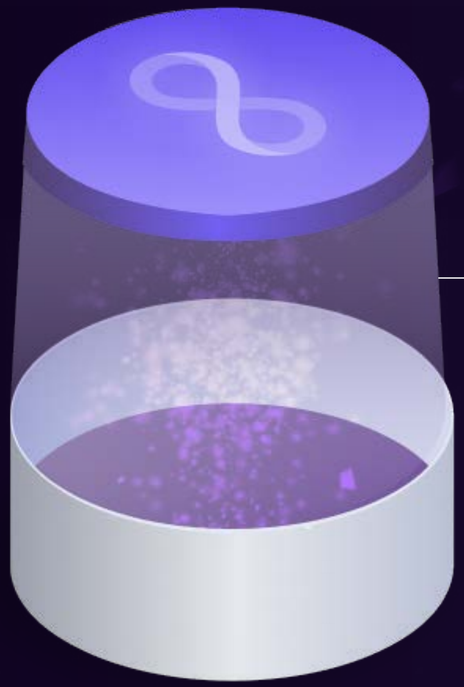
autonomous cloud

autonomous cloud runs tamperproof code without backdoors at scale

canister code

canisters are a new form of smart contract
that have general application

each canister bundles some software logic and data



LOGIC

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

Since a canister is a “software actor” that maintains its own data, which communicates with other canisters purely via function calls, it has private memory pages inside. These memory pages are persistent. Software logic transparently maintains data inside memory in a scheme of “orthogonal persistence” – data can be persisted in any data structure.

canisters are tamperproof software

TRADITIONAL SOFTWARE

when software is invoked, sometimes it executes logic a hacker inserted

when software is invoked, sometimes it processes a hacker's malicious data

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

when software is invoked, it correctly executes the defined logic

when software is invoked, it correctly processes its own data

ransomware/viruses cannot encrypt or modify software and its data

software and data are hosted using a mathematically secure protocol

THE FUTURE

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

canisters are a new form of smart contracts

CANISTER SOFTWARE

fast
web speed canisters don’t make users wait

efficient
can reduce traditional IT carbon footprints

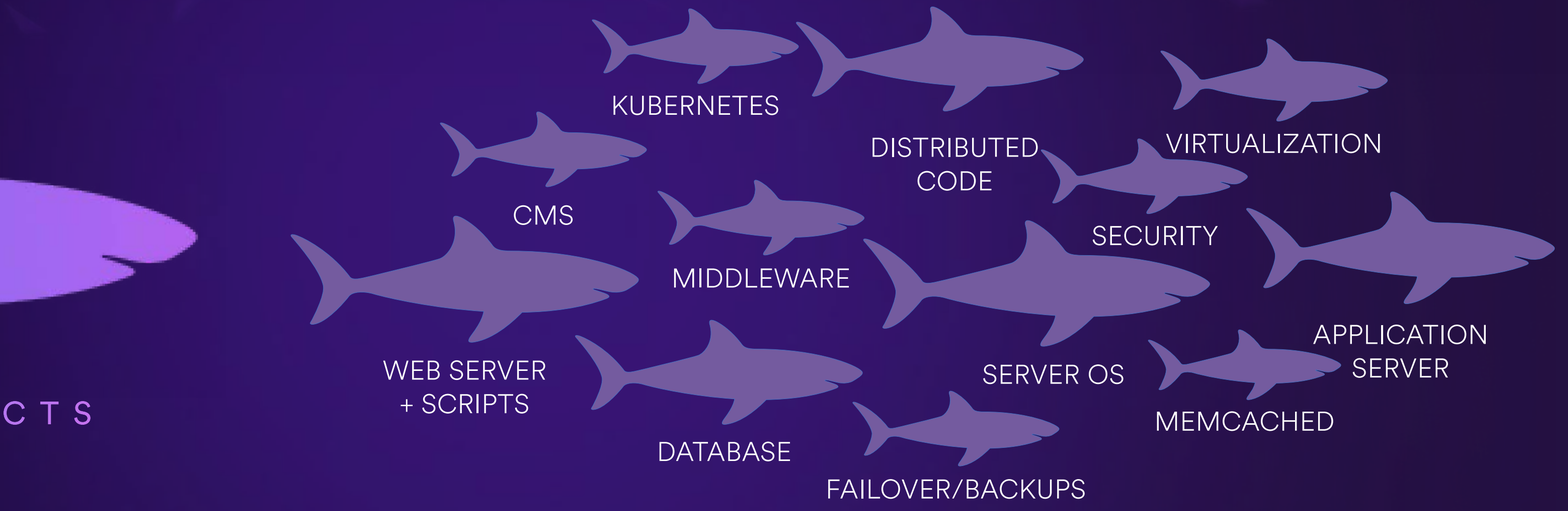
scalable
can support services that scale-out to millions or billions

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

software will eat the world. smart contracts will eat software



the advantages of smart contract software will enable it to replace the traditional stack

web3+

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

ICP solves for the final frontier of decentralization

CENTRALIZED IT

SMART CONTRACTS

ETHEREUM

WEB3 EXPERIENCES

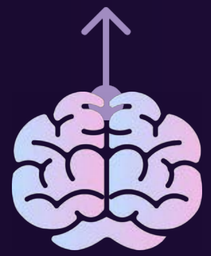
hackers
censorship
gatekeepers
vested interests
ransomware virus
must trust developers

replace centralized IT using Internet Computer canister contracts

SMART CONTRACTS
ETHEREUM

CANISTERS
INTERNET COMPUTER

WEB3 EXPERIENCES



AUTONOMOUS GOVERNANCE
SERVICE NERVOUS SYSTEM

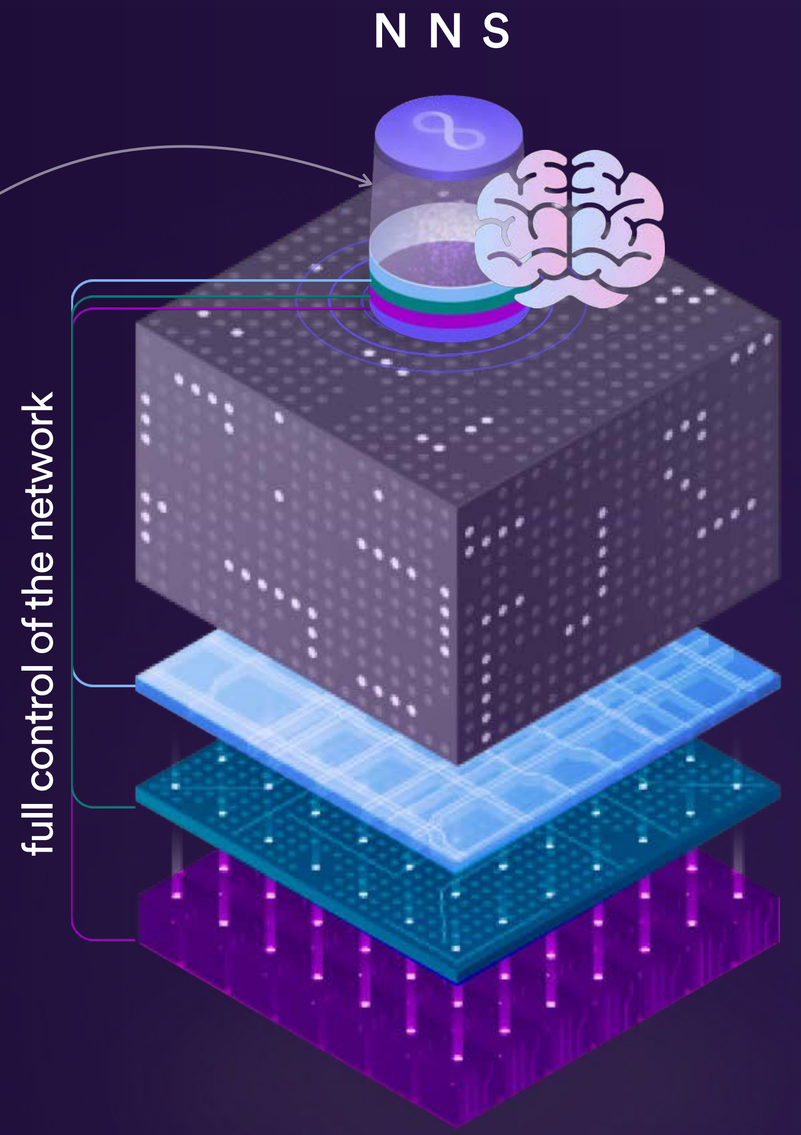
autonomy

the Internet Computer runs autonomously under the control of decentralized governance… so can web3 online services and systems

the Network Nervous System (NNS) DAO

the NNS DAO is integrated into the Internet Computer's protocols, and enables it to adapt and evolve autonomously, without need for forks and social backdoors:

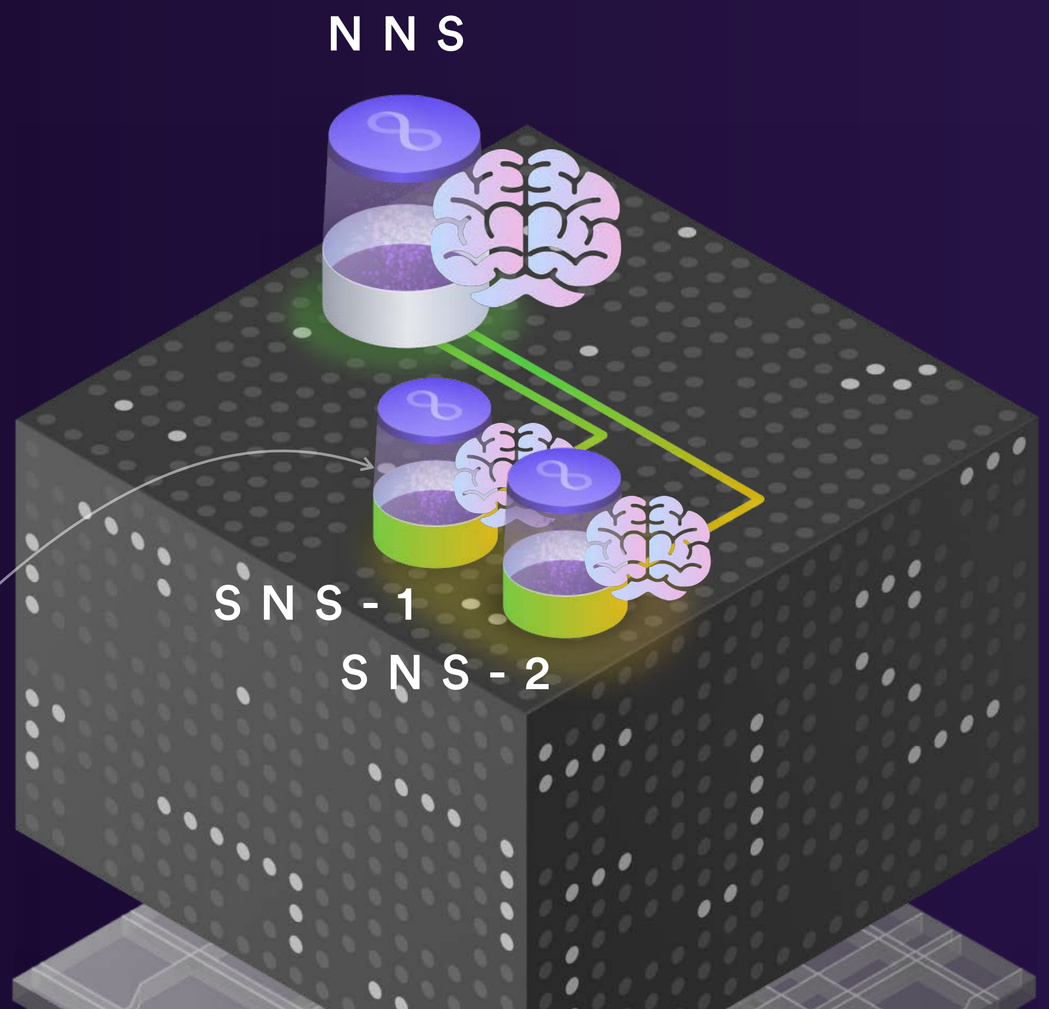
- public, open, transparent and permissionless
- proposals submitted and adopted or rejected
- adopted proposals are executed automatically
- on instruction, nodes update ICP protocol
- on instruction, nodes form into new subnets
- decisions made by algorithmic liquid democracy
- users lock ICP tokens to create "voting neurons"
- neurons can vote automatically by following others
- tens of thousands of users have created neurons
- in 2 years, mainnet upgraded its protocols 145 times
- human control removed to make network autonomous



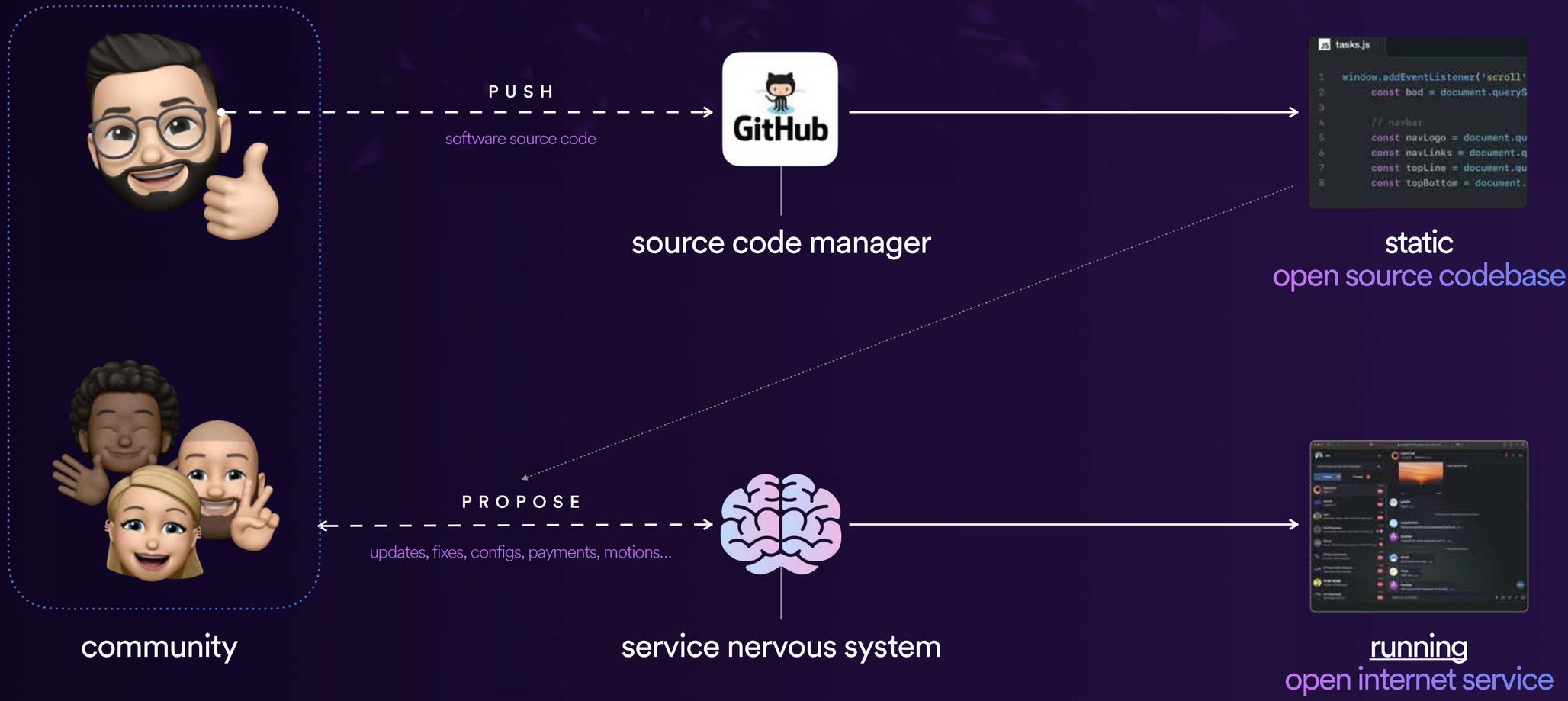
SNS DAOs (service nervous systems) enable a democratic web3

SNS DAOs work similarly to the NNS, but each is used to create and manage one “open internet service,” or secure enterprise system:

- open/permissionless or private
- 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 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
- the NNS is an SNS factory



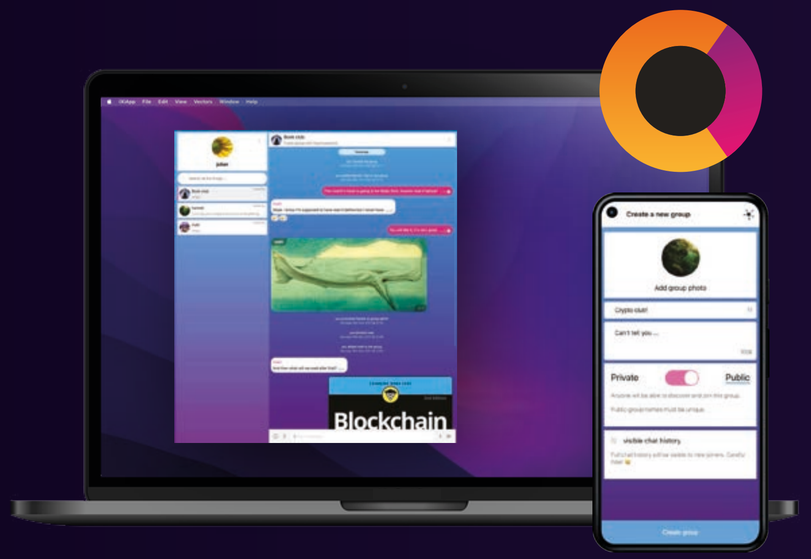
an open internet service (OIS) gives its community 100% control



pure web3

the Internet Computer is a Web3 platform that provides a complete alternative to the traditional IT stack

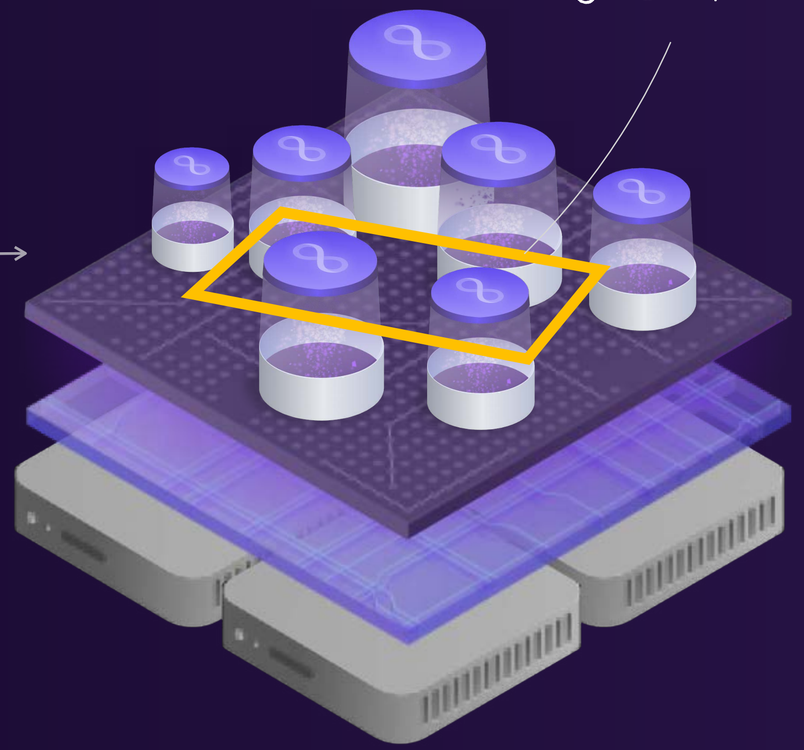
end-users interact with services over HTTP (the web)



WEB3 EXPERIENCE

web browsers interact with canisters over HTTP

(1000s of canisters used by e.g. OpenChat)



tip users don't need wallets to interact: canisters pay for their own computation ("reverse gas")

“Internet Identity” creates a session for user interaction

WEB3 EXPERIENCE

the session allows the user experience to transparently submit multiple transactions a second

actually, the entire network has 1 (one) master 96-byte chain key!!

breakthrough depends on hash trees and chain key threshold BLS assemblies...

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 is relies on key pairs securely maintained within TPM chips on the user's 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).

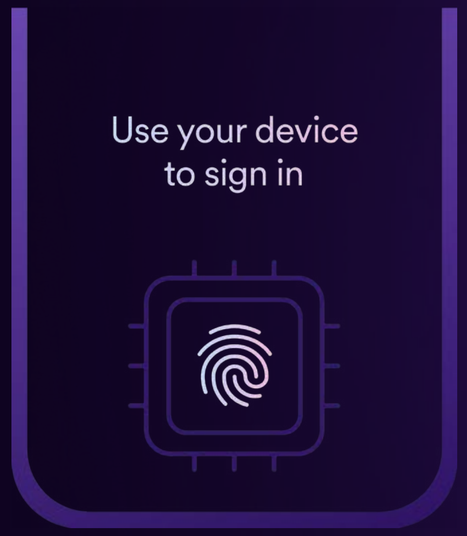
Open source

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 the user interacts with, preventing services linking their users e.g. as per SSO.

INTERNET IDENTITY



TPM

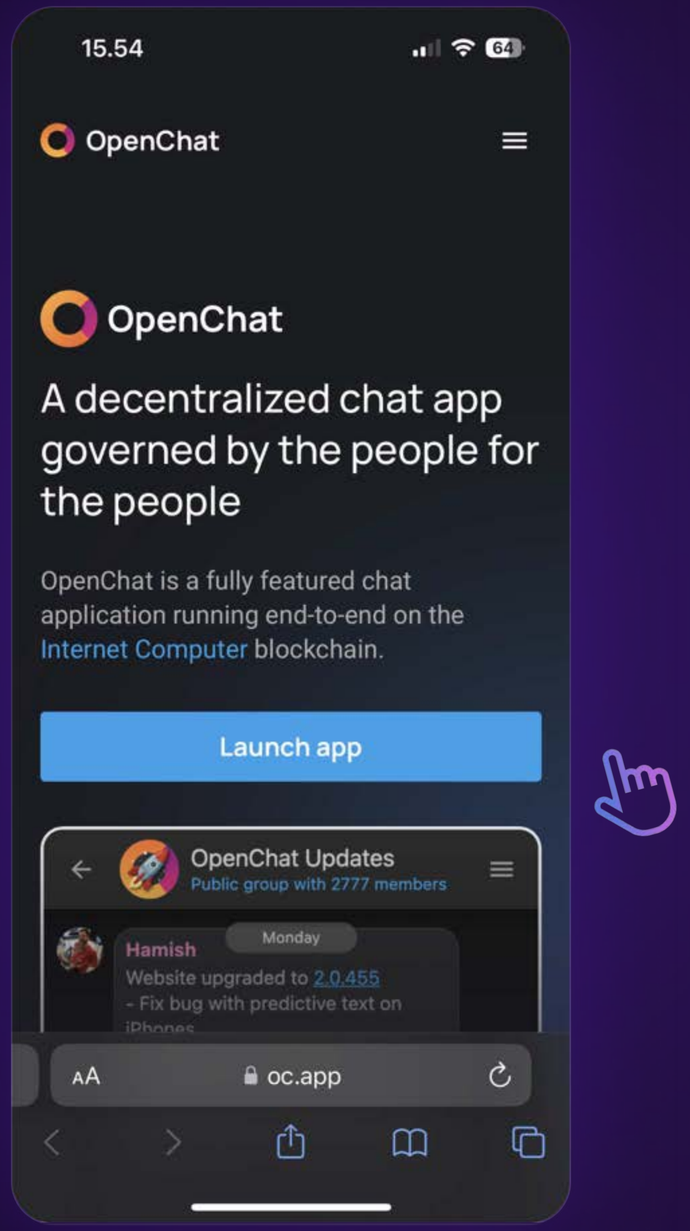
+

WebAuthn (+ FIDO)

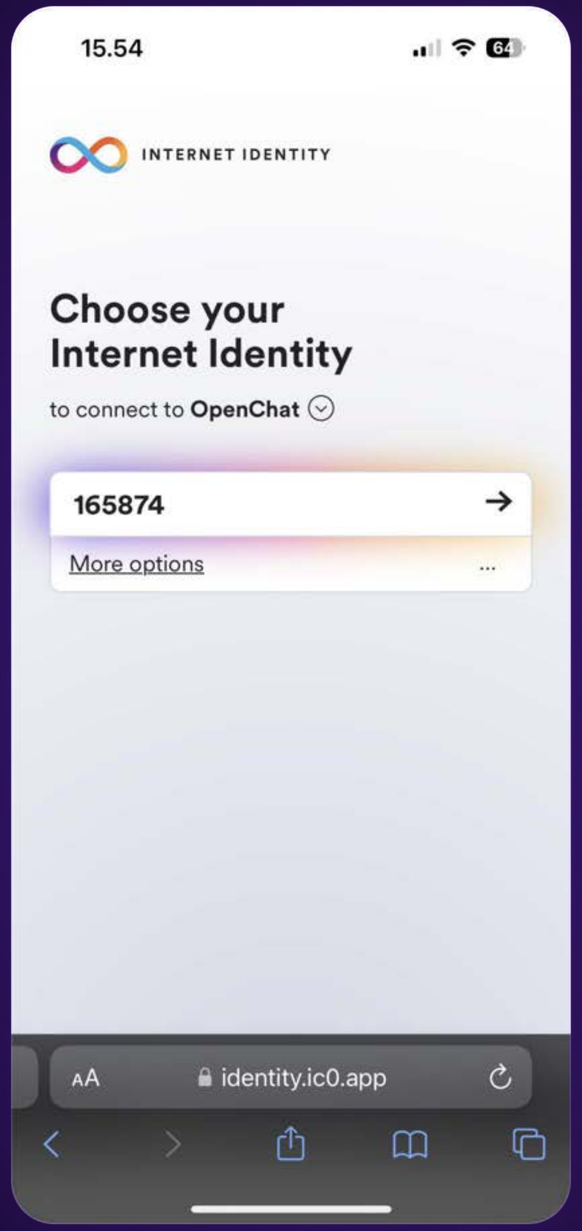
+

Internet Computer

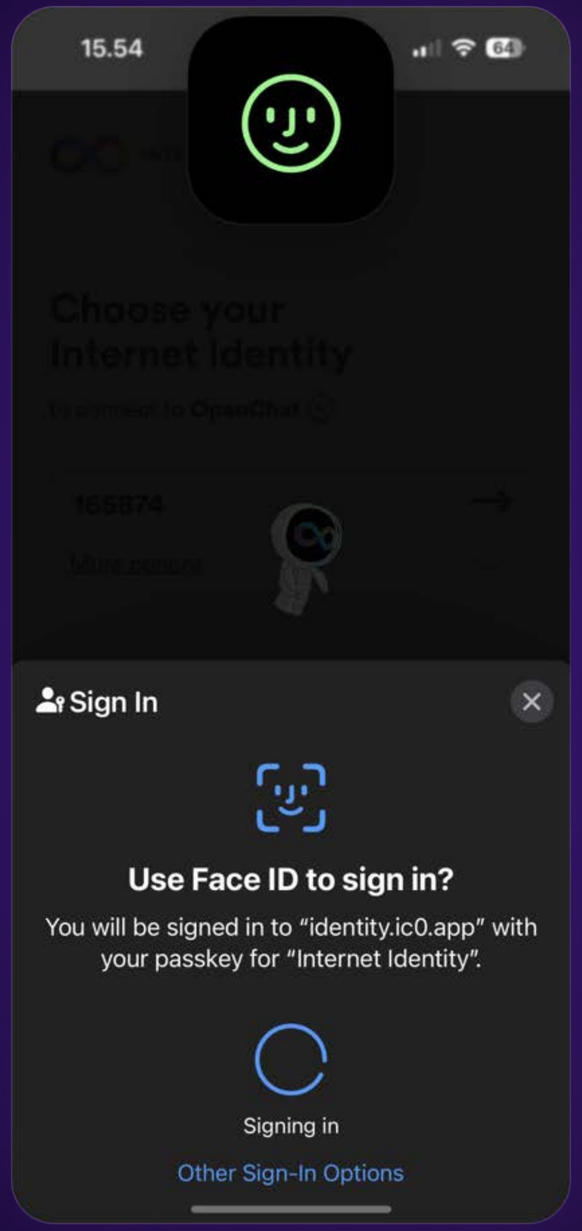
INTERNET IDENTITY



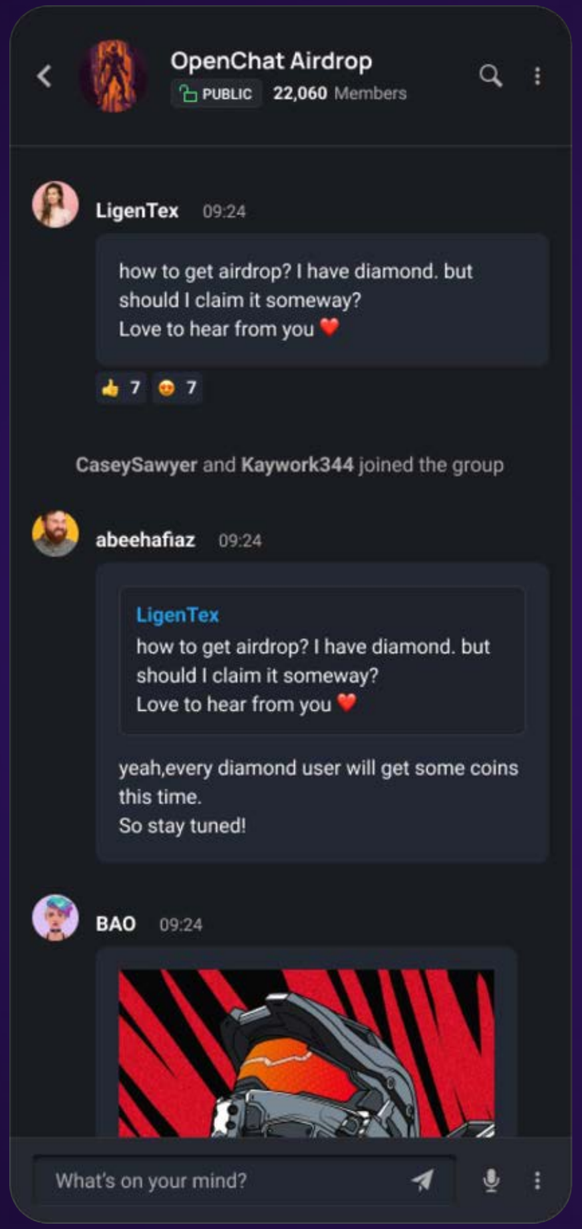
INTERNET IDENTITY



INTERNET IDENTITY



INTERNET
IDENTITY



Where we are now

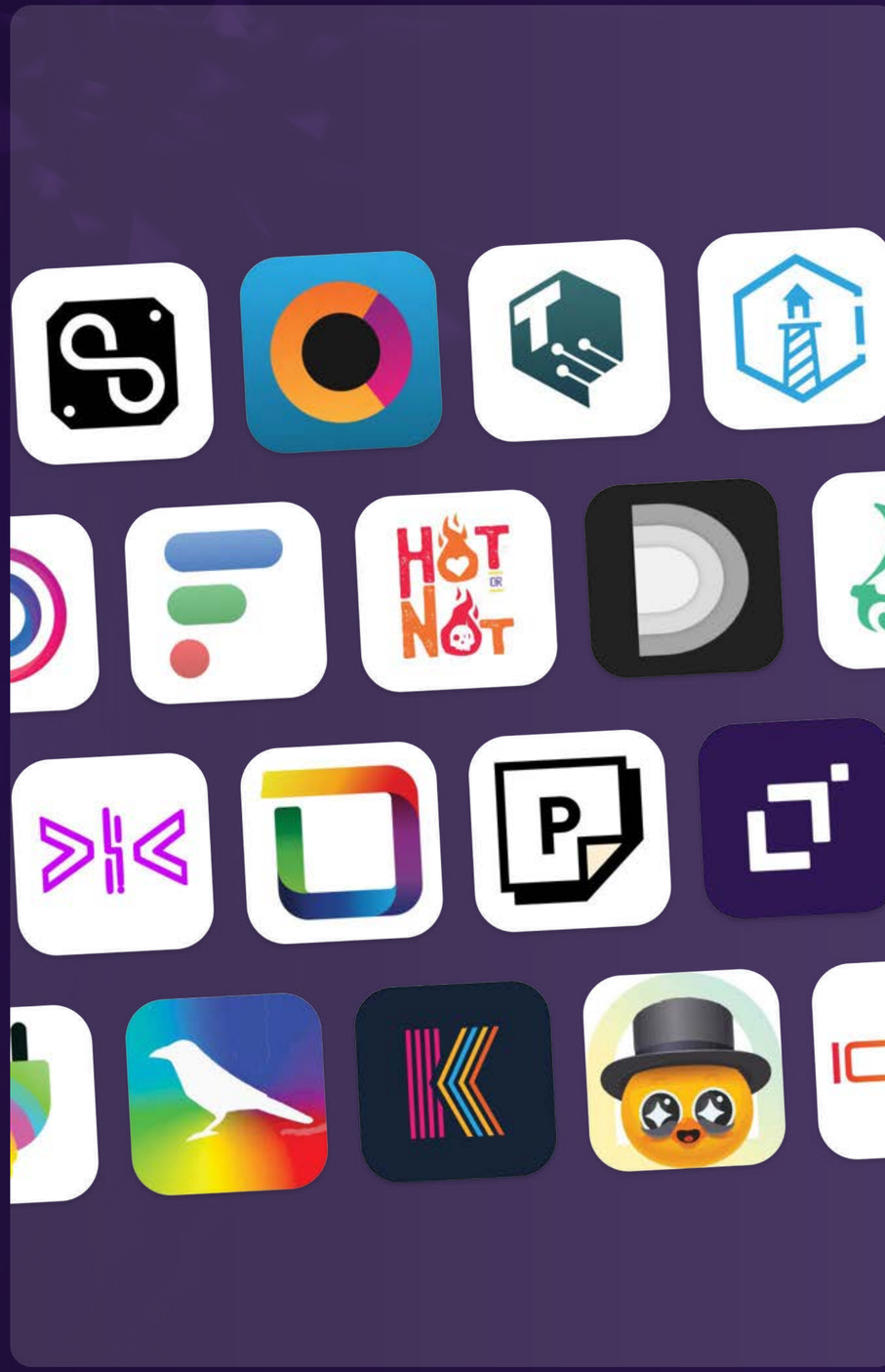
2.2M+

identities created

100+

dapps using II for authentication

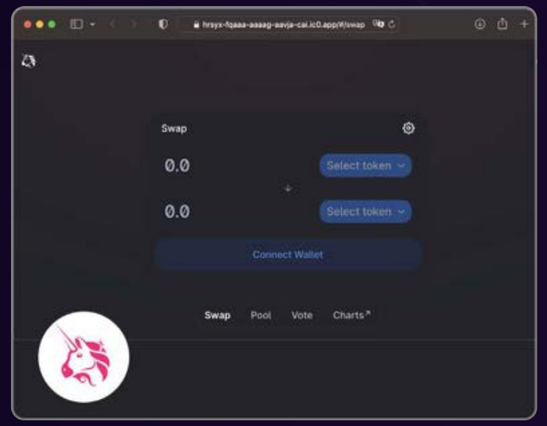
Support for relying parties and identity providers coming in 2023...

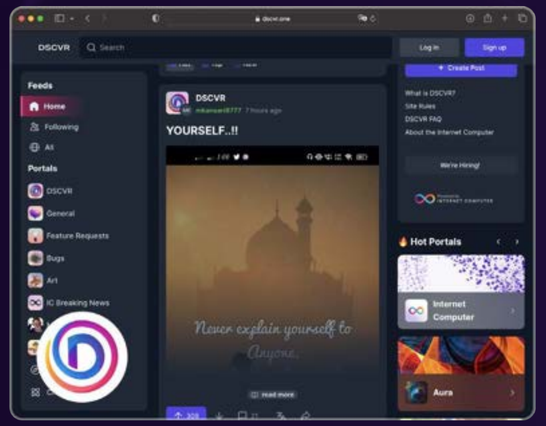


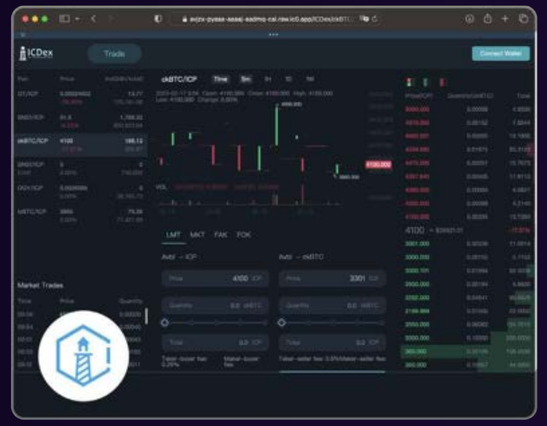
end-to-end software autonomy enables more compelling web3

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

full tokenization can transform user communities into giant industrious virtual workforces







internetcomputer.org

build on the network

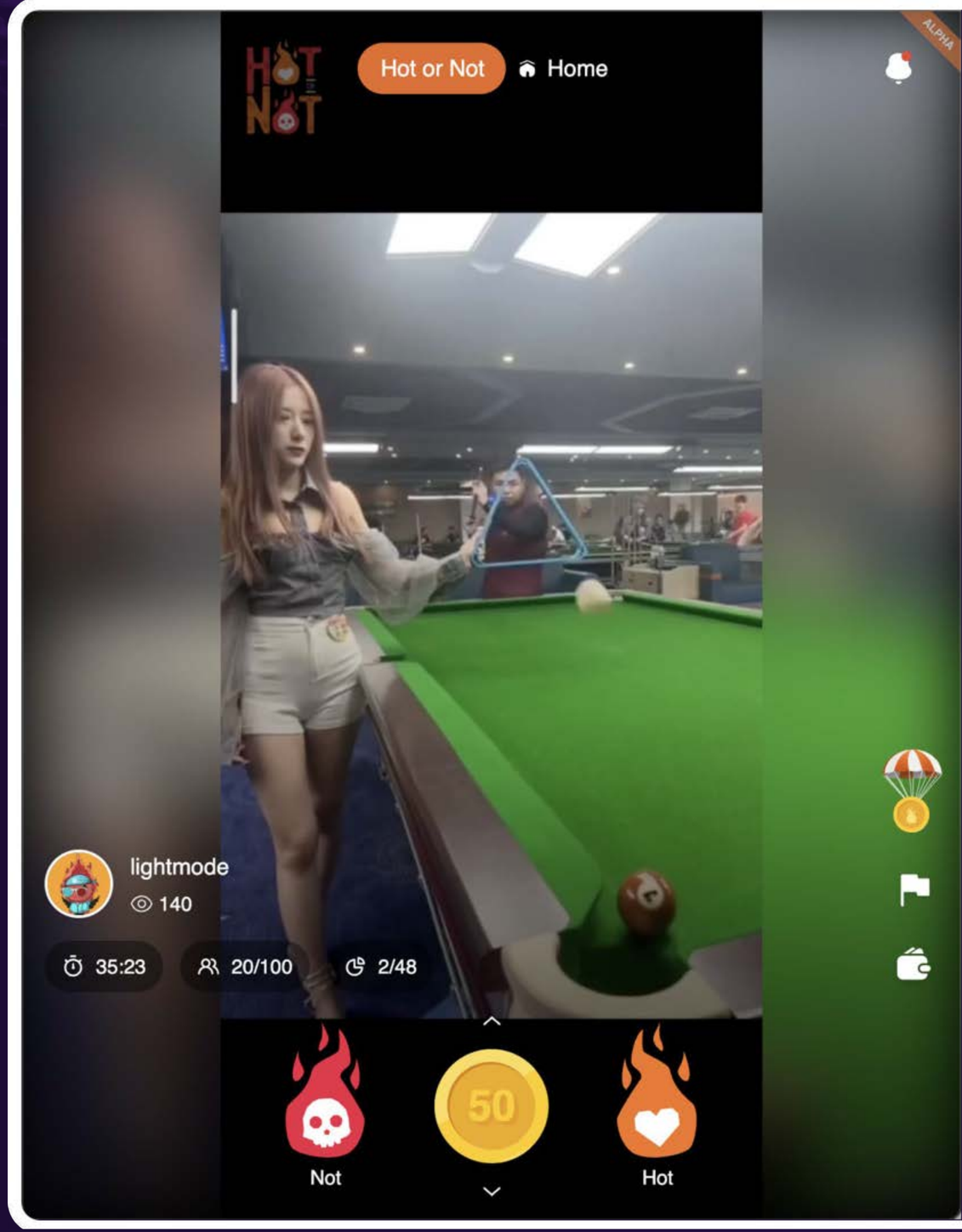
OC.app

was the first
"open internet service"
on the Internet Computer

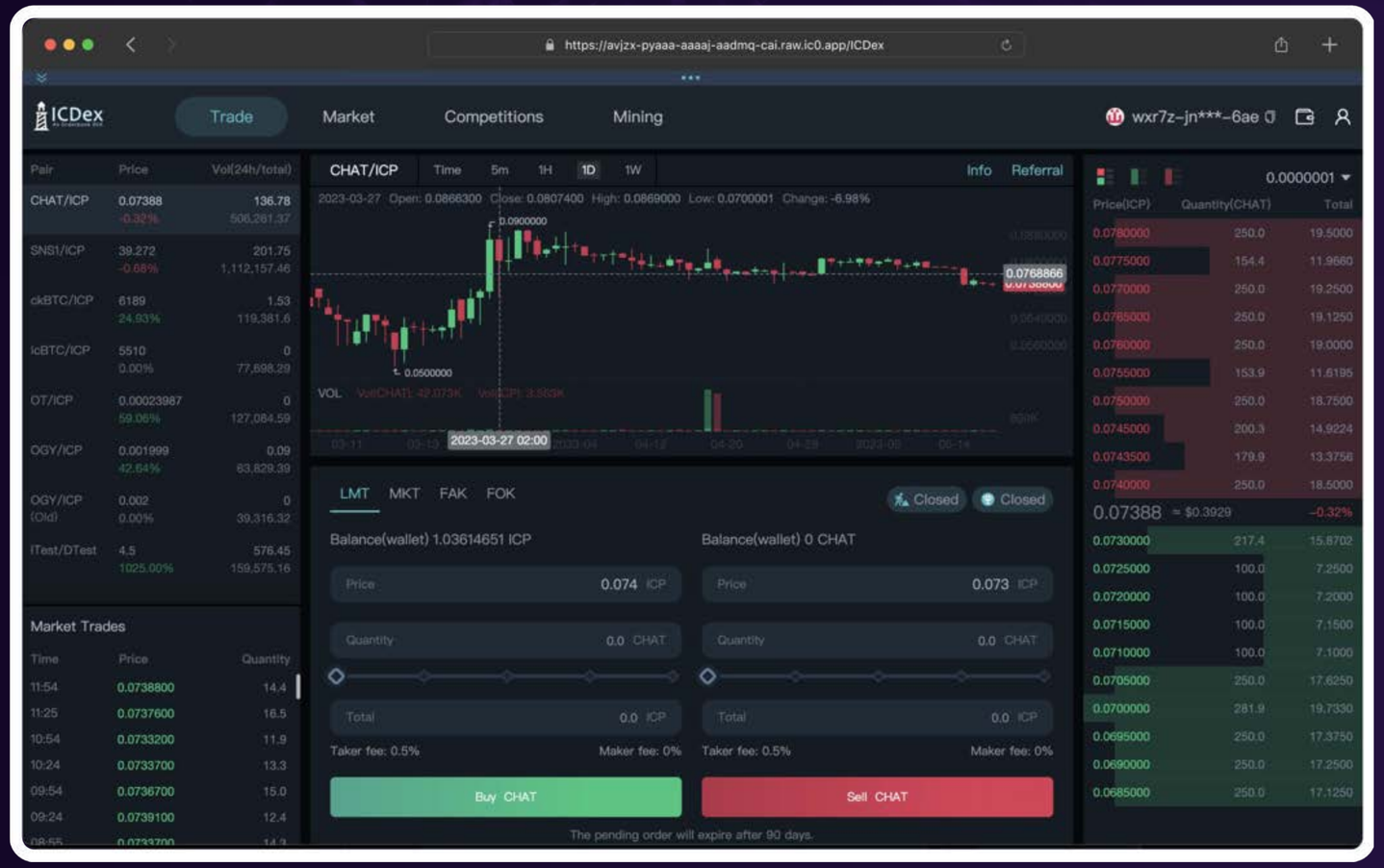
- messaging service runs 100% on network
- chat accounts also crypto wallets i.e. full SocialFi
- *seamlessly* send satoshis using chat messages
- users hold governance tokens for SNS DAO
- bounties for users promoting OpenChat
- rewards for those creating viral content
- updates pass transparently through governance
- runs as protocol with an SNS in full control

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 OSI inverts centralized business models…
- video creators, users, are founderized team members
- 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

a grass roots army is now building 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

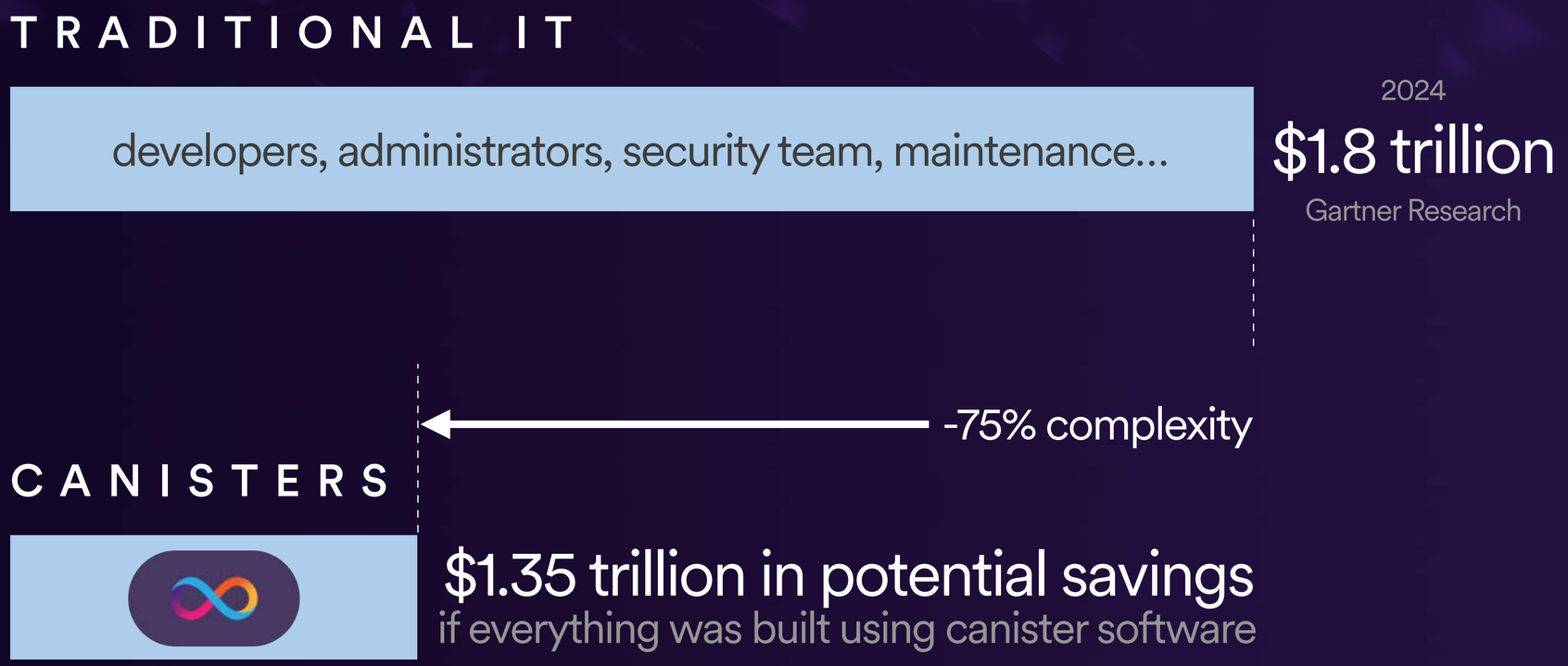
cool services. tiny tech teams.

web3 services are sophisticated and scale to large numbers of users, but:
far fewer engineers are required to create them

enterprise

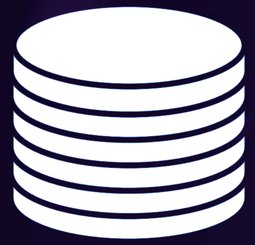
going beyond web3, the Internet Computer can deliver
tremendous advantages to the enterprise sector

building with canister software addresses spend on IT personnel



REDUCE

the Internet Computer stack addresses numerous core IT costs



Gartner Research

Software (e.g. databases)

2023

$912 billion

REDUCE

Gartner Research

Cloud services

2023

$600 billion

REDUCE

Gartner Research

Data Center Systems

2023

$224 billion

REDUCE

tamperproof systems and services address security costs

Gartner Research

Cybersecurity

2022

$172 billion

REDUCE

Gartner Research

CPS incident costs

2023

$50 billion

REDUCE

sovereign

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

the future of global identity?

=

“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

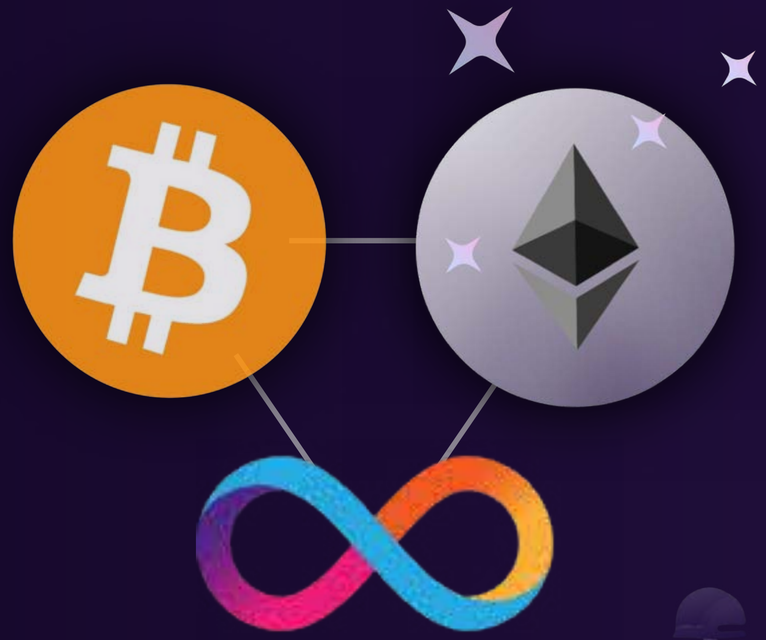
the Internet Computer network will create geographically-local specialized sovereign subnets for nations

no bridges, just trustless cryptography

multi-chain

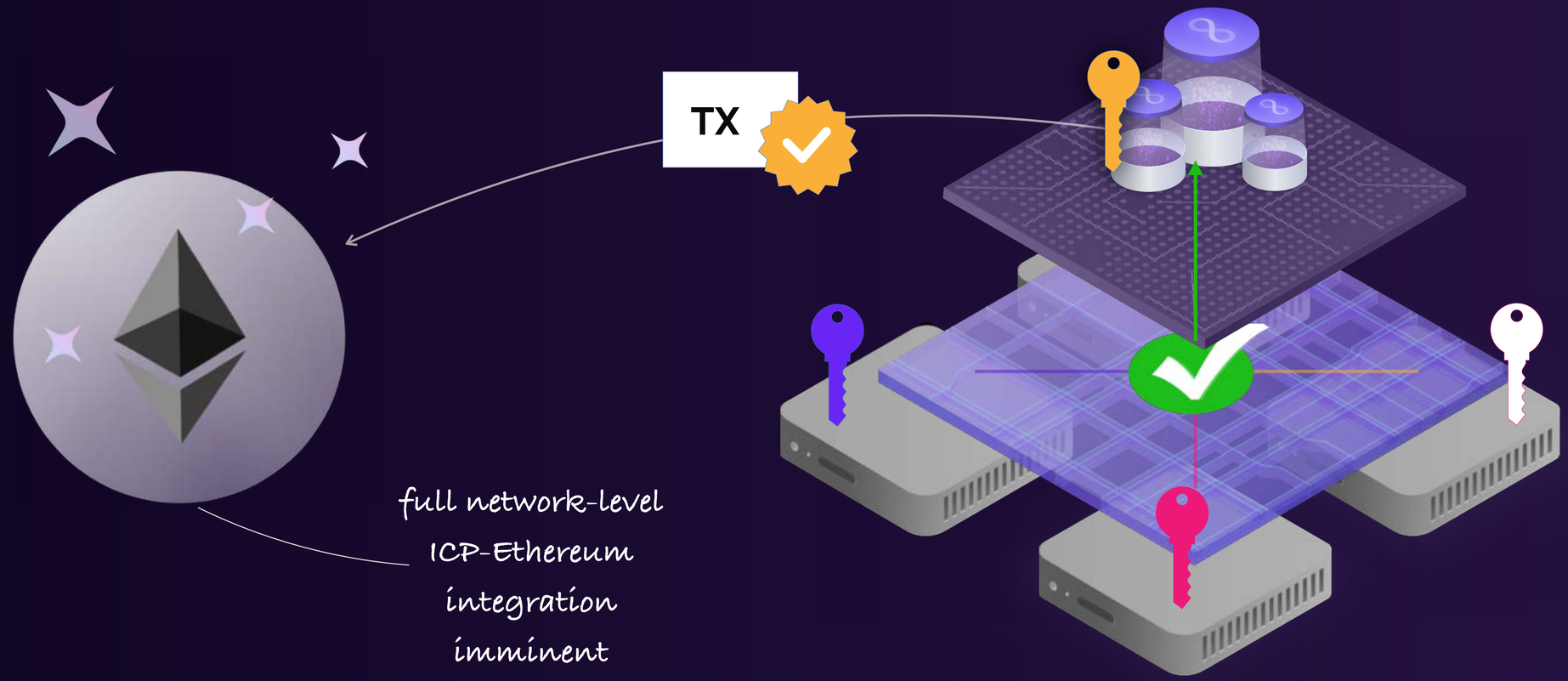
“chain key cryptography” creates transactions on other chains.
network-level integrations with Bitcoin and Ethereum

Internet Computer enables the World Computer vision from 2014



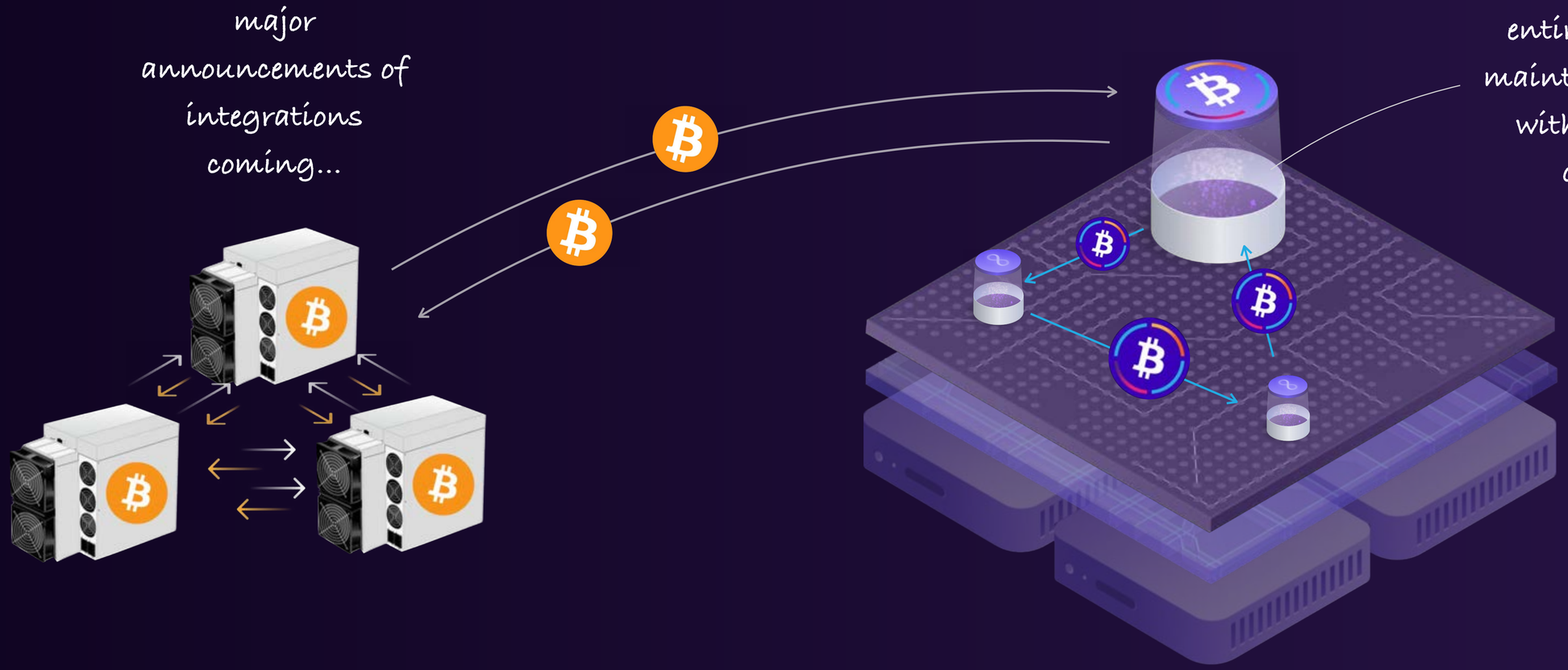
NEW

canisters create accounts and sign TXs on other blockchains



chain key cryptography does the signing – without need for traditional private keys

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

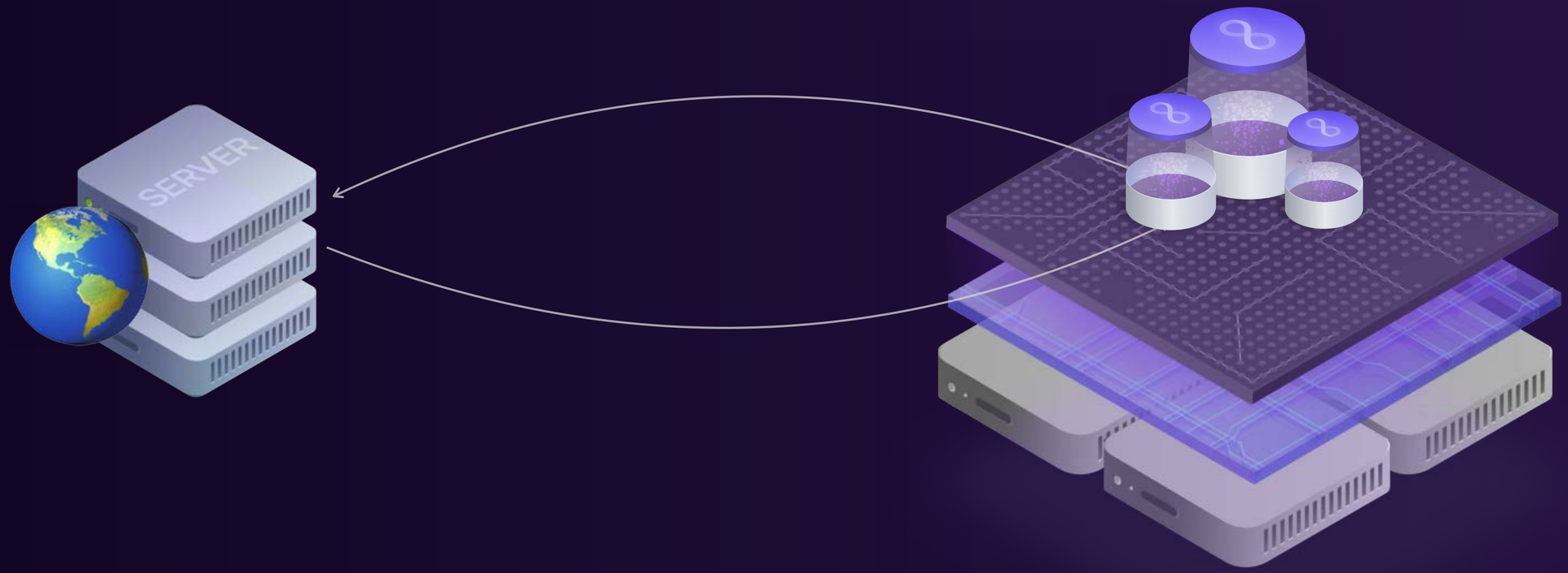


“chain-key bitcoin” supports usage of bitcoin in DeFi, social media, games, the metaverse with 1s finality

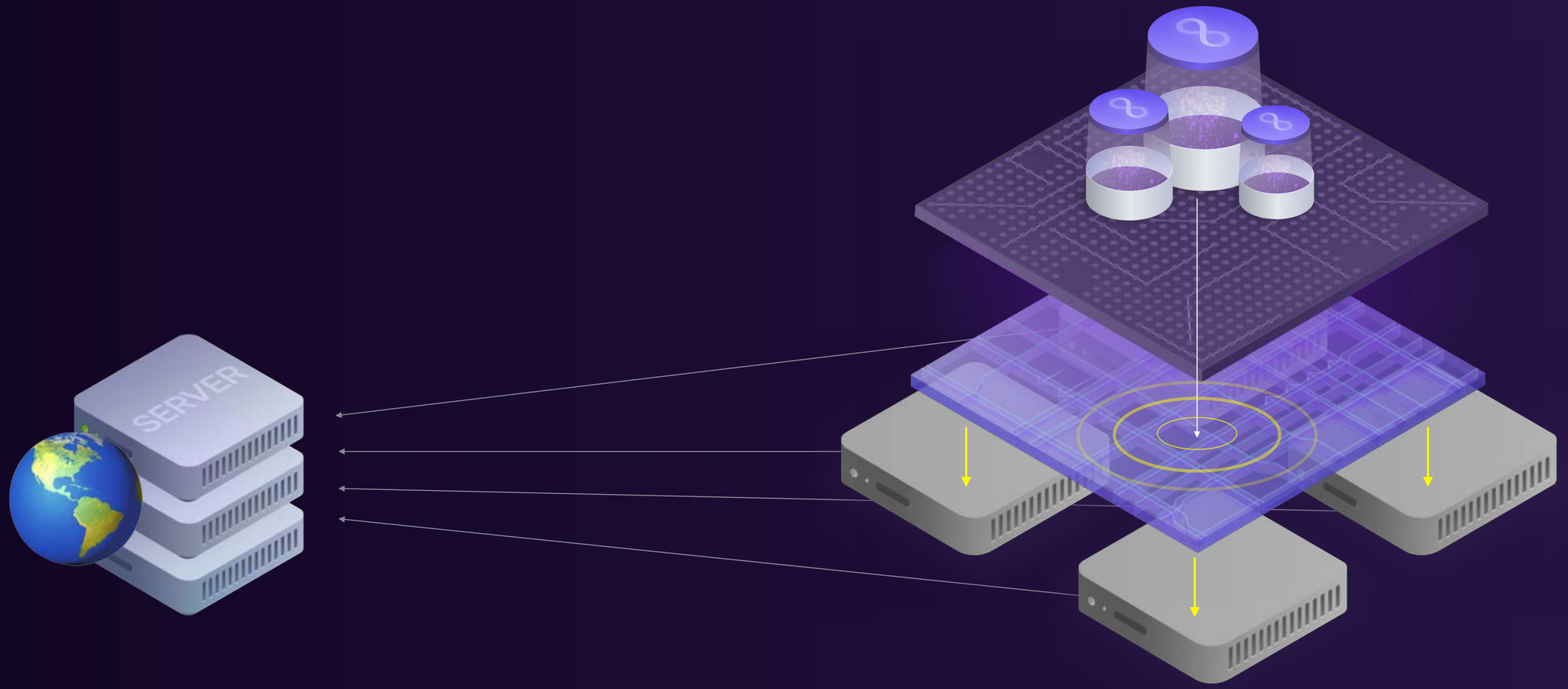
web2+3

canister smart contracts can trustlessly calls into external web2 systems – the network passes results through consensus

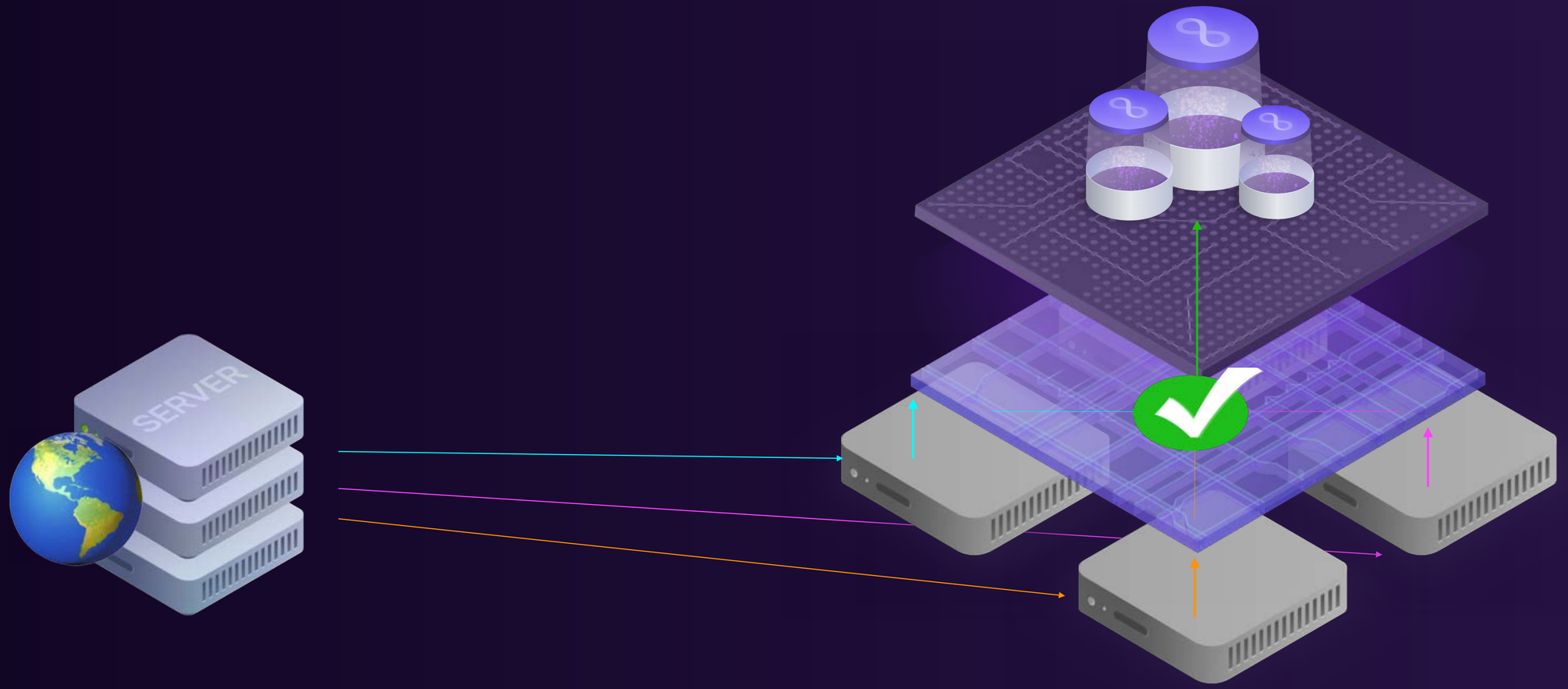
1. a canister initiates a call to a web2 service



2. multiple nodes make call, consensus normalizes result



3. enables decentralized oracles, web2 integrations, etc



ai

ICP ai compute units under development with a pathway to support for ai models that runs as smart contracts

data security model security 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

see the majority of the world's systems and services
reimagined on a public World Computer

growing canister compute tells a story

2 011 578 950

Blocks processed

36 parallel subnets

37.1 MB/s block throughput capacity

Throughput

Capacity horizontally scales as subnet blockchains are seamlessly combined into one unified blockchain. Blocks and transactions per second are unbounded.

259 954

ETH equivalent TX/s

4 754 Transactions/s

Comparing transactions

Transactions invoke "actor" canister smart contract computations, which subnet blockchains can run concurrently (yet deterministically).

DFINITY Foundation 🇨🇭

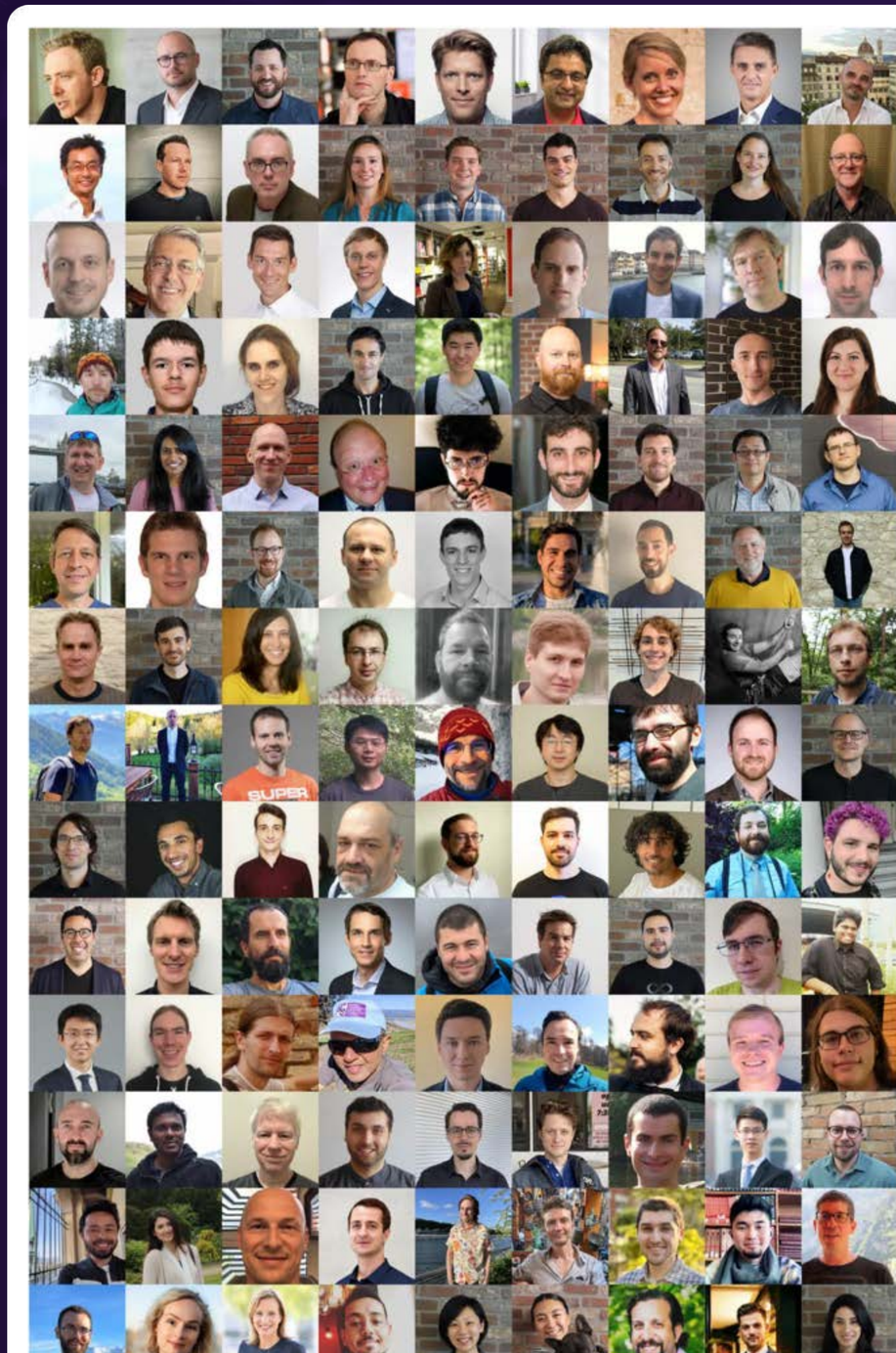
- Emerged from early Ethereum community in 2015
- DFINITY Foundation established October 2016
- Swiss not-for-profit foundation not a corporation
- World’s largest team of cryptographers
- Over 140 people in Zürich HQ
- 270+ people globally

1600+
research papers

100 000+
academic citations

250+
technical patents

Crypto People + Google IBM facebook



build on the network

https://internetcomputer.org

make
everything
web3

PARTNERSHIPS

partnerships@dfinity.org

COMMUNITY

community@dfinity.org

GRANTS

grants@dfinity.org

PRESS

comms@dfinity.org