INTERNET COMPUTER

Build on the network

ICP | Internet Computer

Main deck version: 11 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

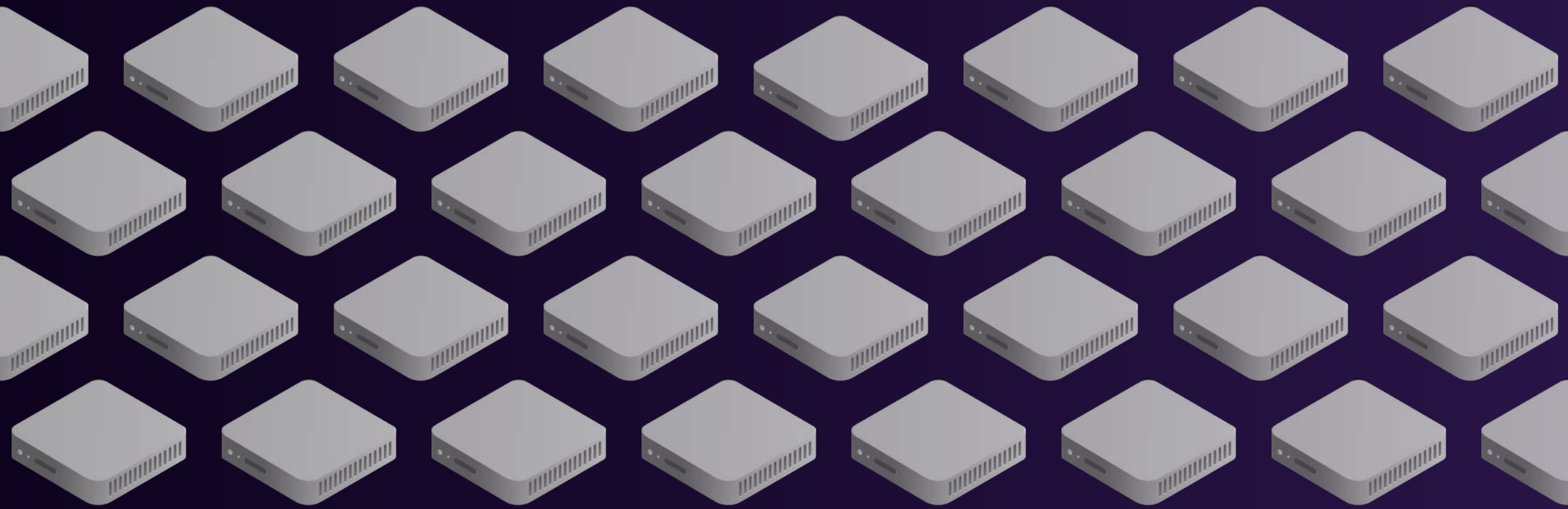
SOVEREIGN ENTERPRISES

build unstoppable infrastructures on an open network using tamperproof software w/o firewalls, and w/o the third party backdoors and kill switches of closed source and cloud

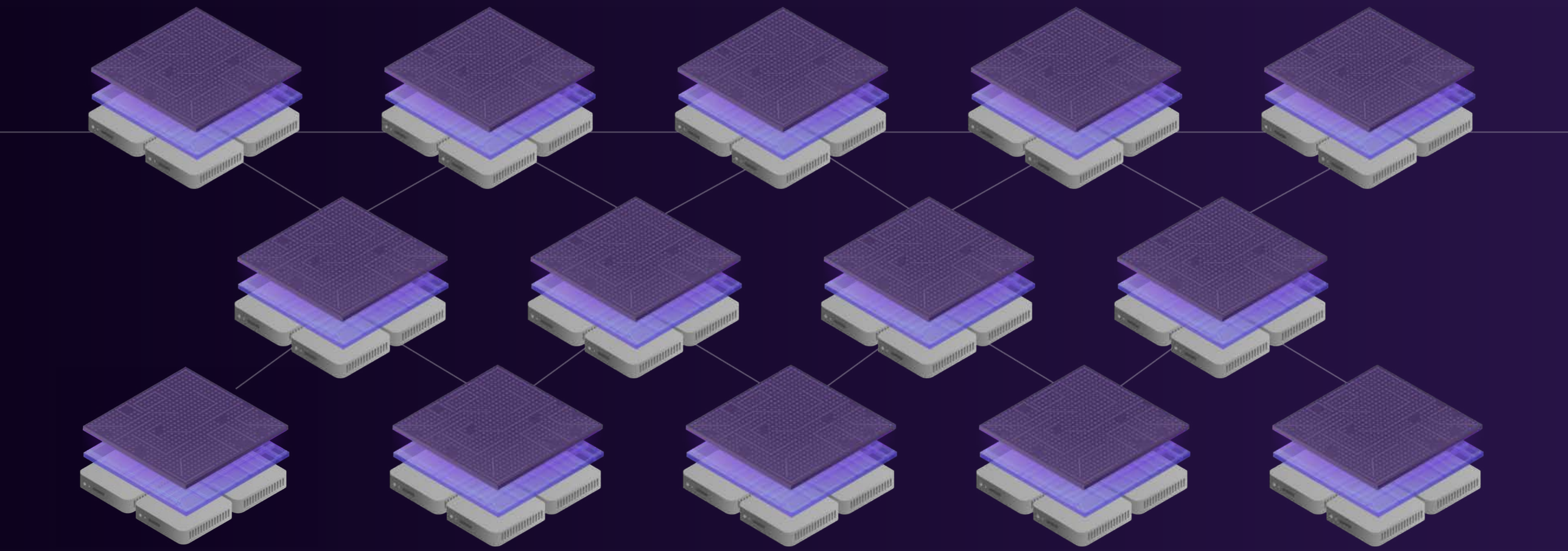
network

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

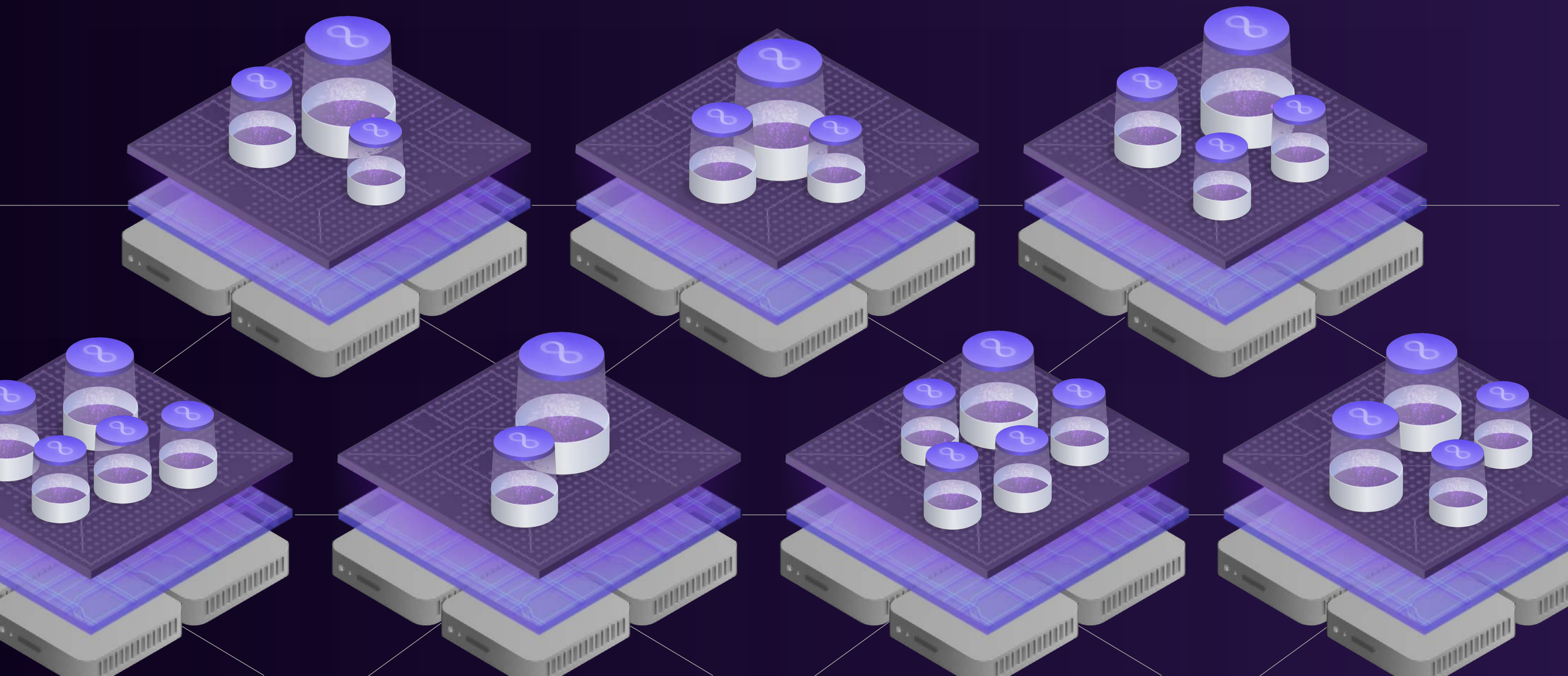
independent node providers own and operate node machines in data centers worldwide



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

smart contracts are a *new form of software*

ETHEREUM SMART CONTRACTS

tamperproof
no firewall or infrastructure security necessary

tokenization
hold, process & transmit value like data

unstoppable
nuke proof, no servers or failing over

composable
trustless dynamic collaborative building

autonomous
can remove human control & backdoors

borderless
code/services have no geography

canisters are a *new form of smart contracts*

CANISTER SOFTWARE

fast
web speed and canisters host web directly

efficient
reduces IT carbon footprints

scaling
scales services more easily than traditional IT

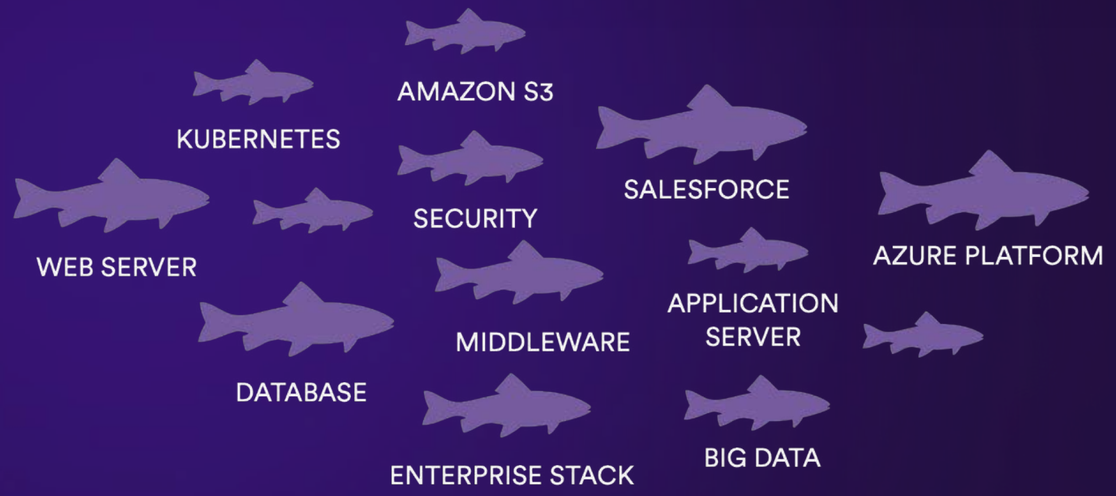
low cost
compute costs approach traditional IT

multi-chain
natively interacts with external blockchains

http (user experience)
canister code speaks web (http) directly

software will eat the world. smart contracts can eat software

SMART CONTRACTS



smart contract software's advantages will enable it to replace traditional software

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
it's not borderless
must trust developers

replace centralized IT using Internet Computer canister contracts

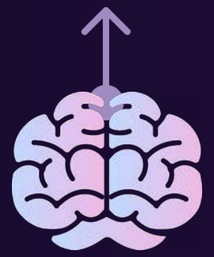
SMART CONTRACTS

ETHEREUM

CANISTERS

INTERNET COMPUTER

WEB3 EXPERIENCES



AUTONOMY

SERVICE NERVOUS SYSTEM

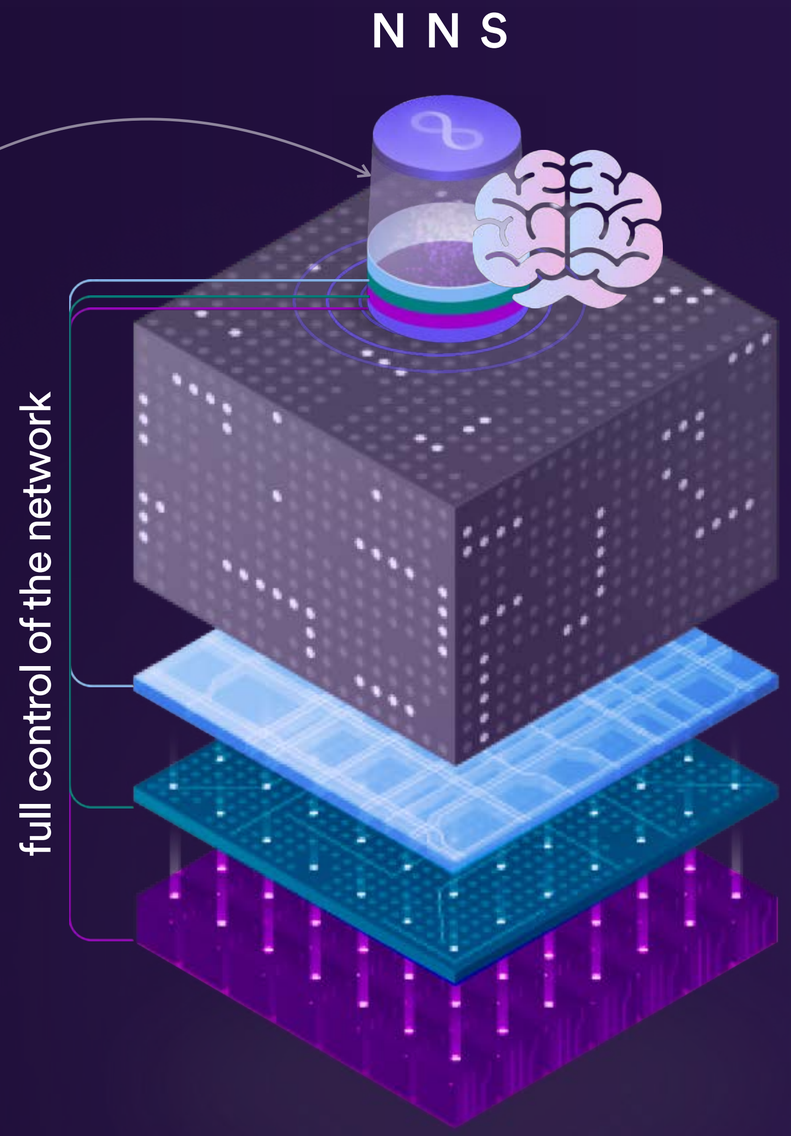
autonomy

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

the Network Nervous System DAO

the Internet Computer network adapts and evolves autonomously without backdoors using advanced protocol-integrated DAO governance:

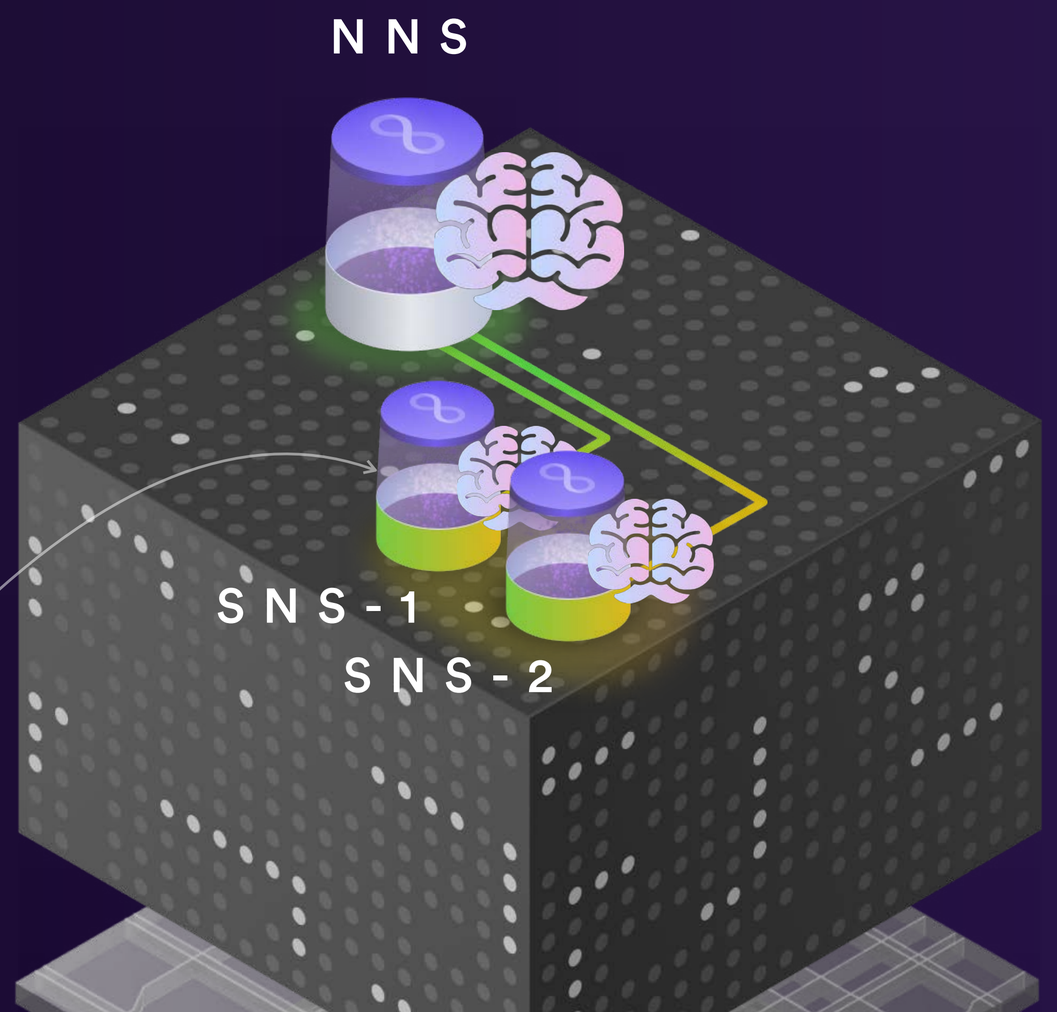
- public, open, transparent and permissionless
- proposals submitted and adopted or rejected
- adopted proposals are executed automatically
- on instruction, nodes update ICP protocol
- on instruction, nodes form into new subnets
- decisions made by algorithmic liquid democracy
- users lock ICP tokens 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



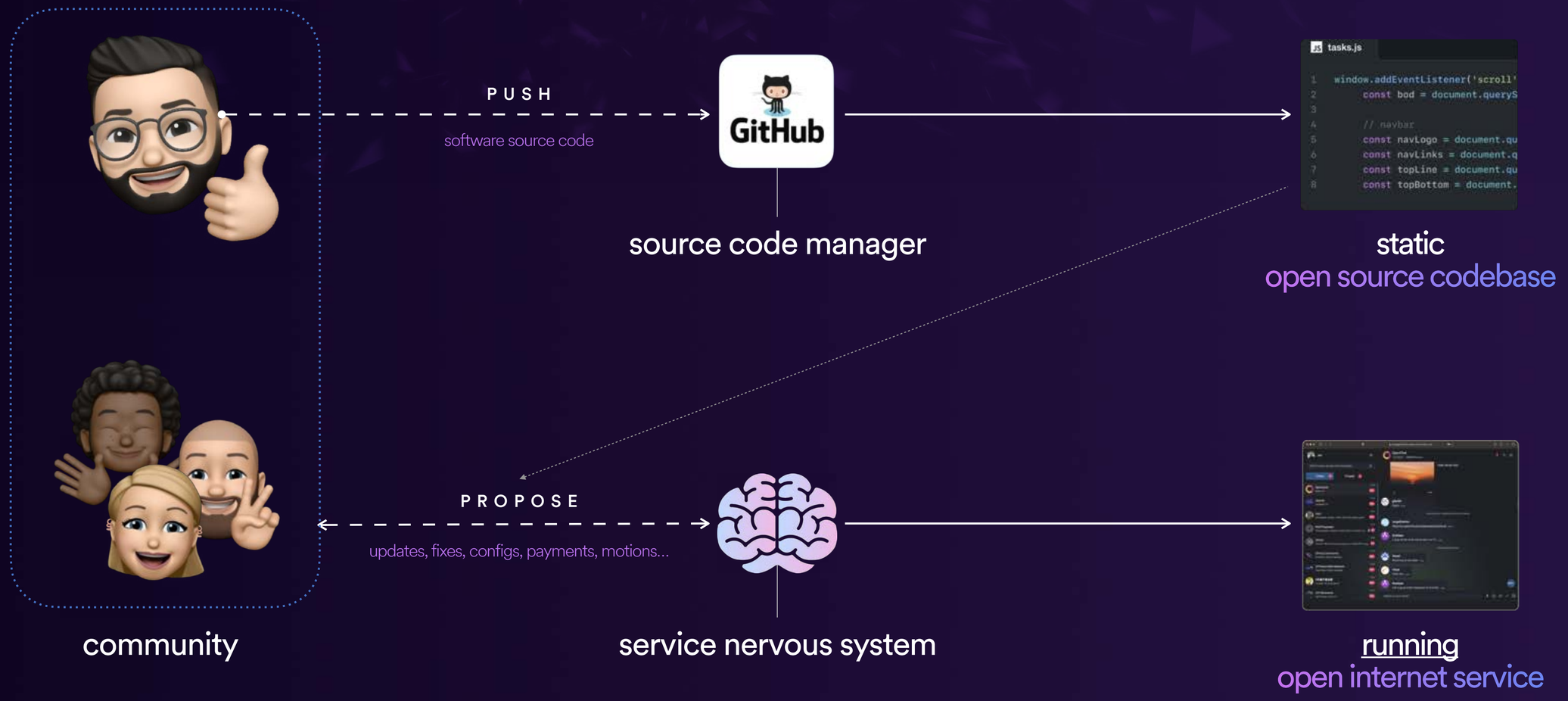
democratic web3 services use "service nervous systems" DAOs

an SNS DAO works similarly to the NNS, but is used to create a web3 "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



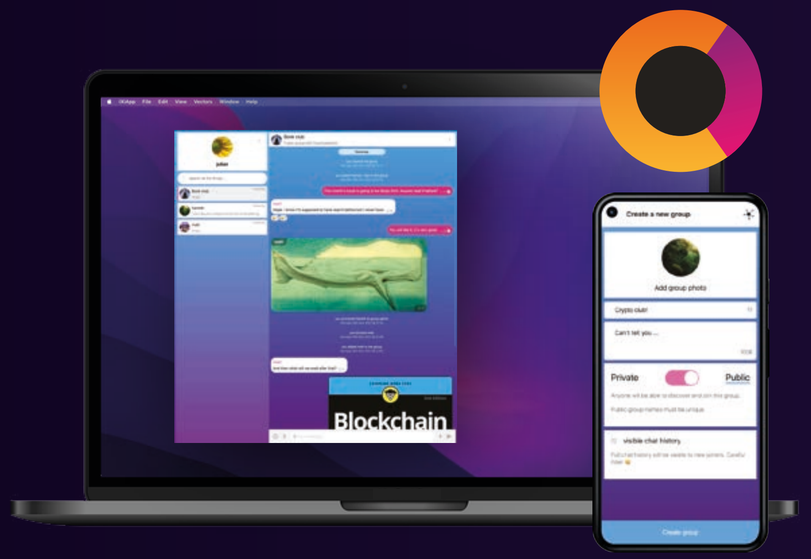
an open internet service (OIS) gives its community 100% control



pure web3

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

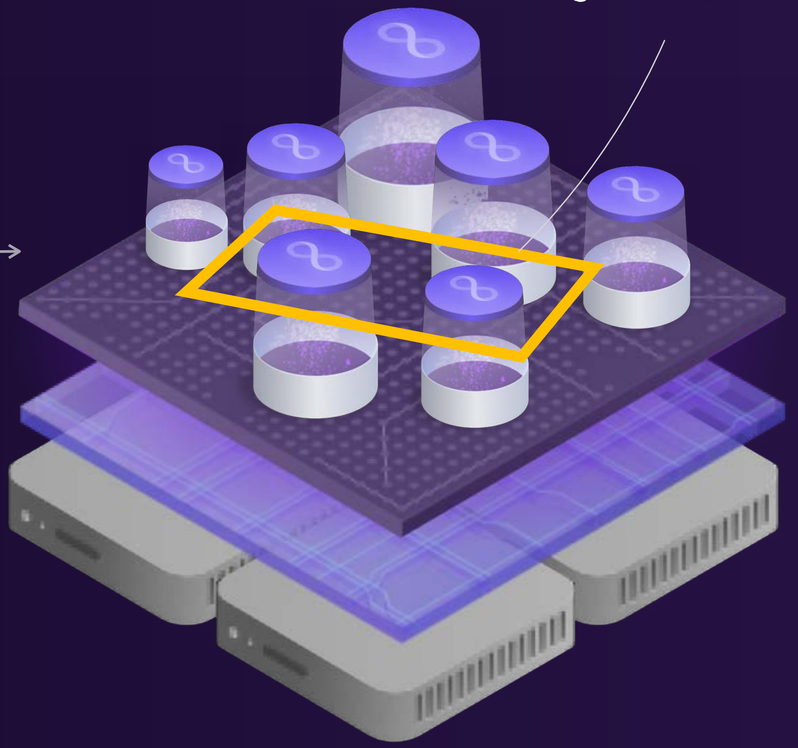
end-users interact with services over HTTP (the web)



WEB3 EXPERIENCE

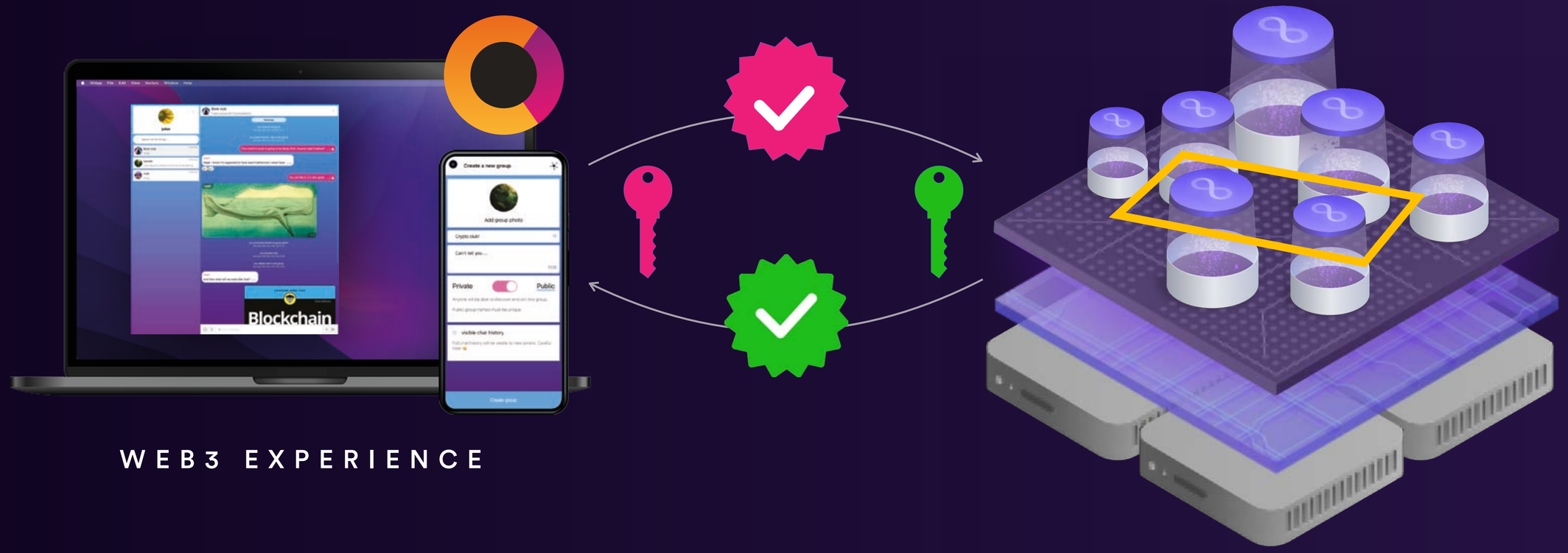
web browsers interact with canisters over HTTP

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



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

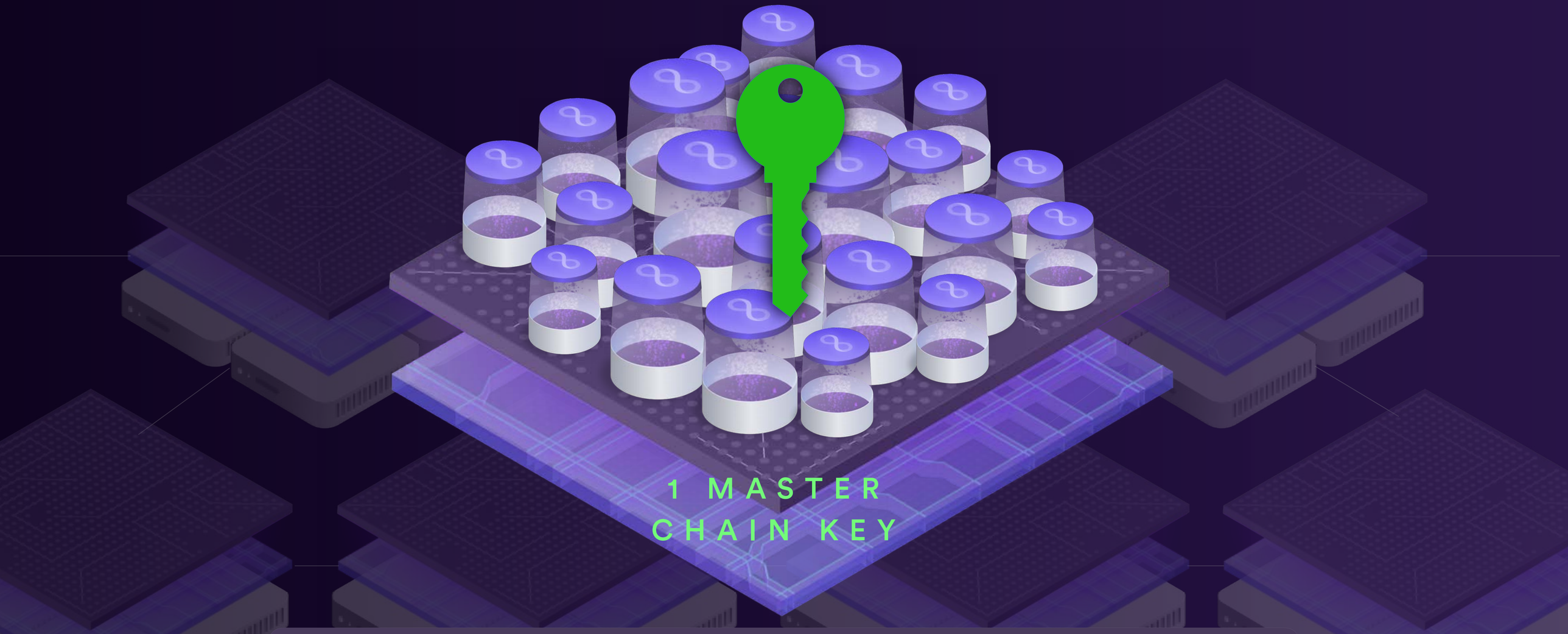
“Internet Identity” creates a session for user interaction



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 remember 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).

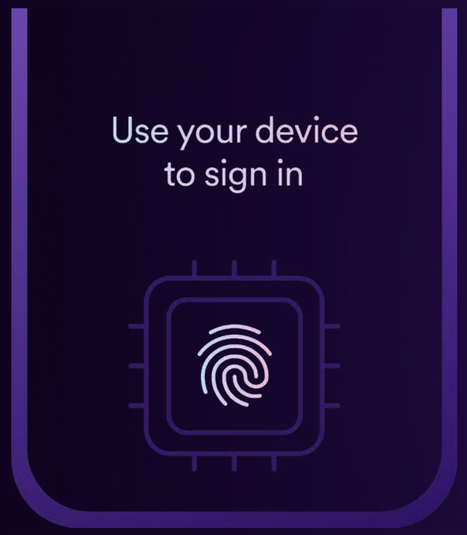
Open source

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 them being tracked between services used.

INTERNET IDENTITY



TPM

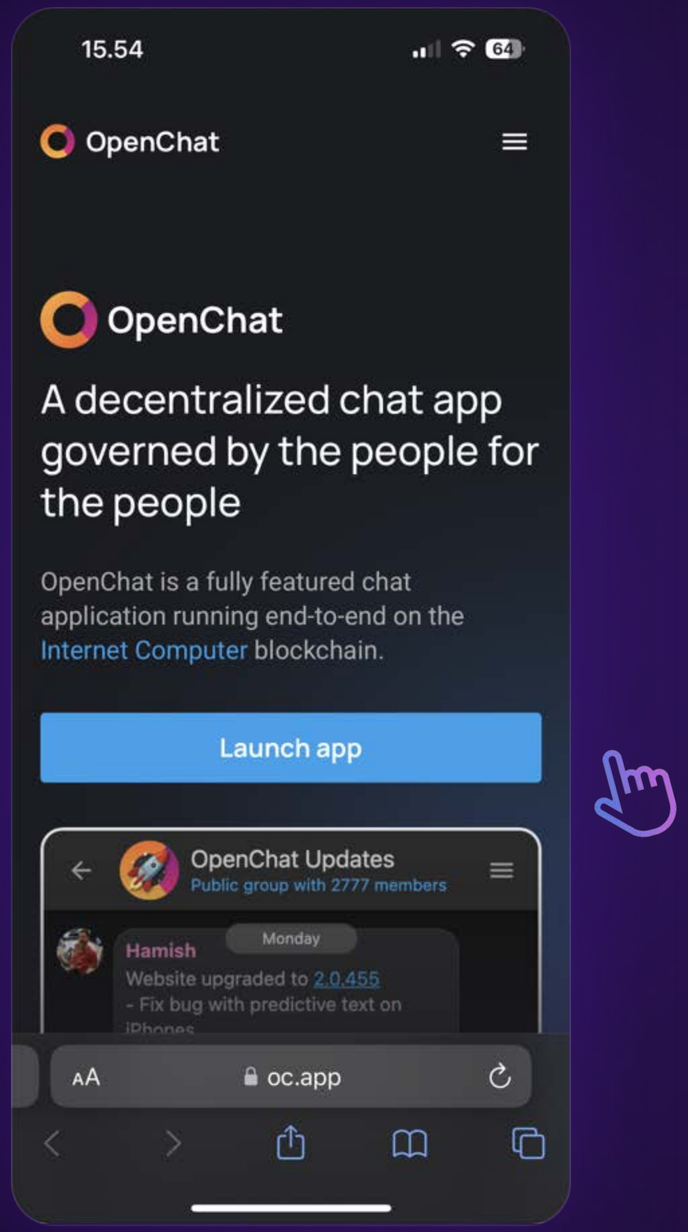
+

WebAuthn (+ FIDO)

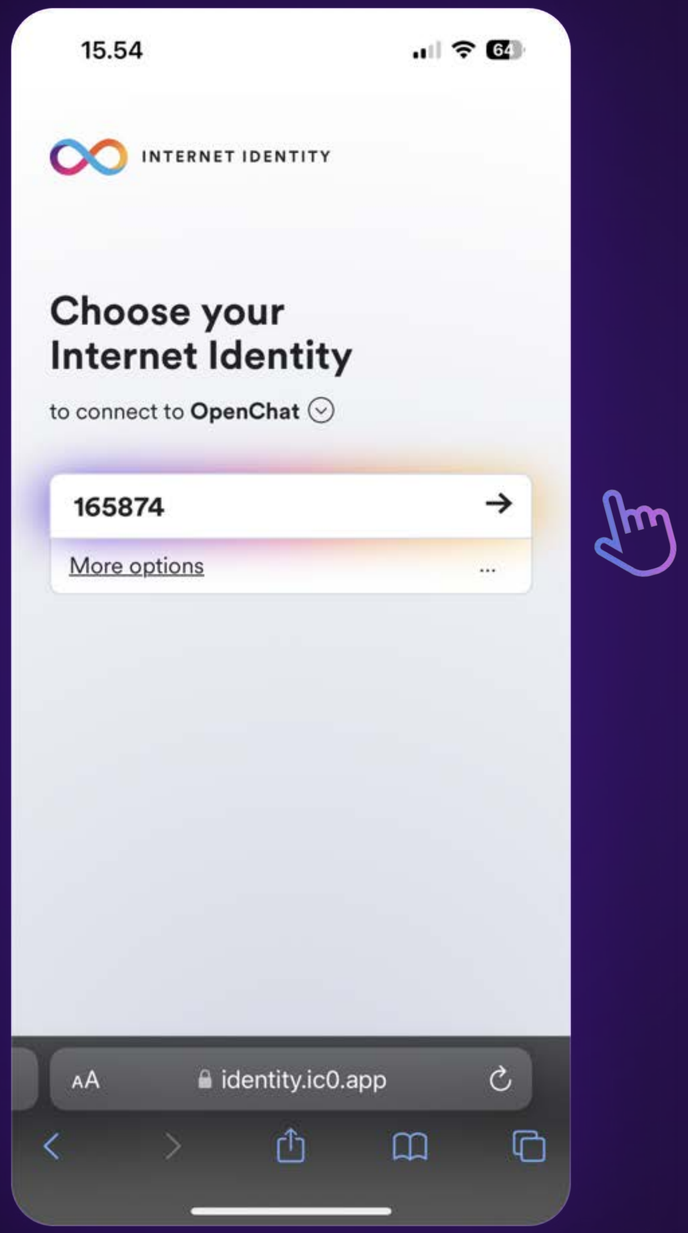
+

Internet Computer

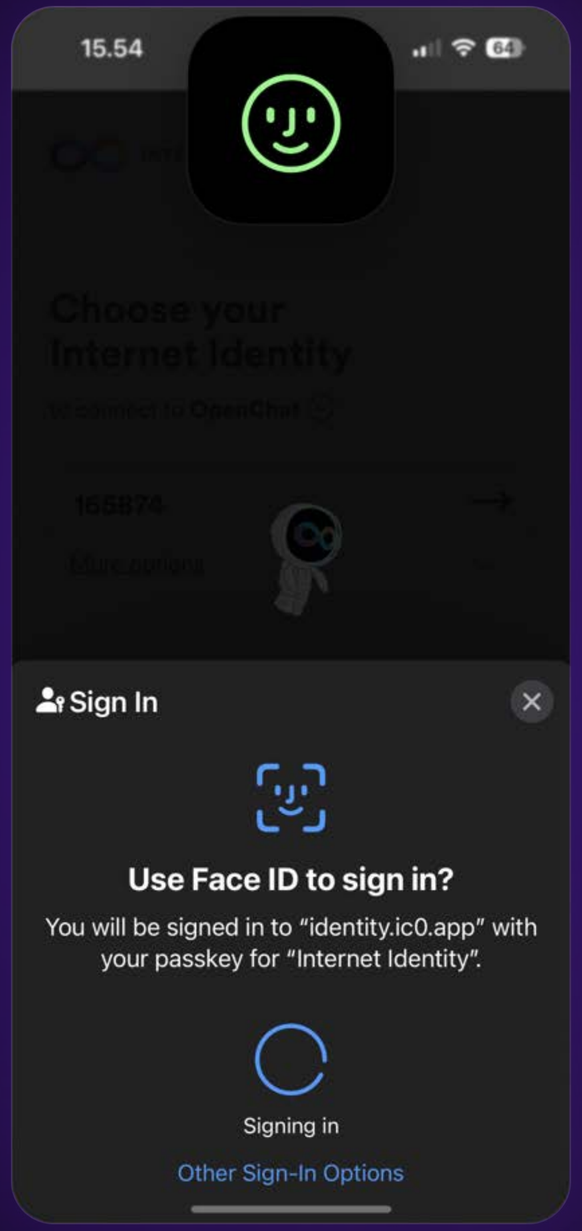
INTERNET IDENTITY



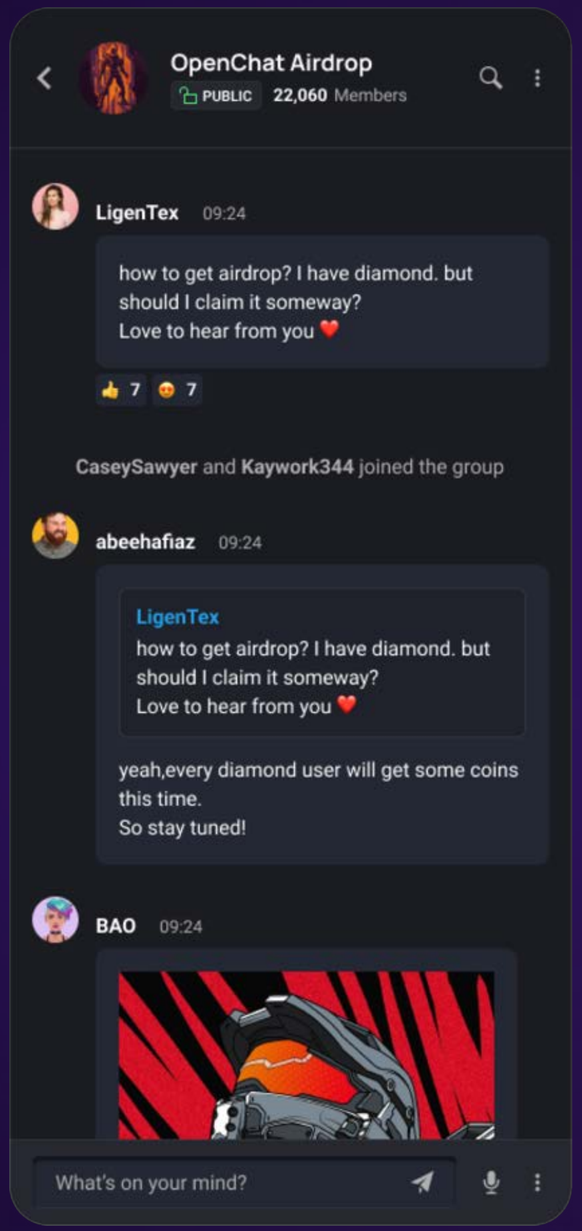
INTERNET IDENTITY



INTERNET IDENTITY



INTERNET IDENTITY



Where we are now

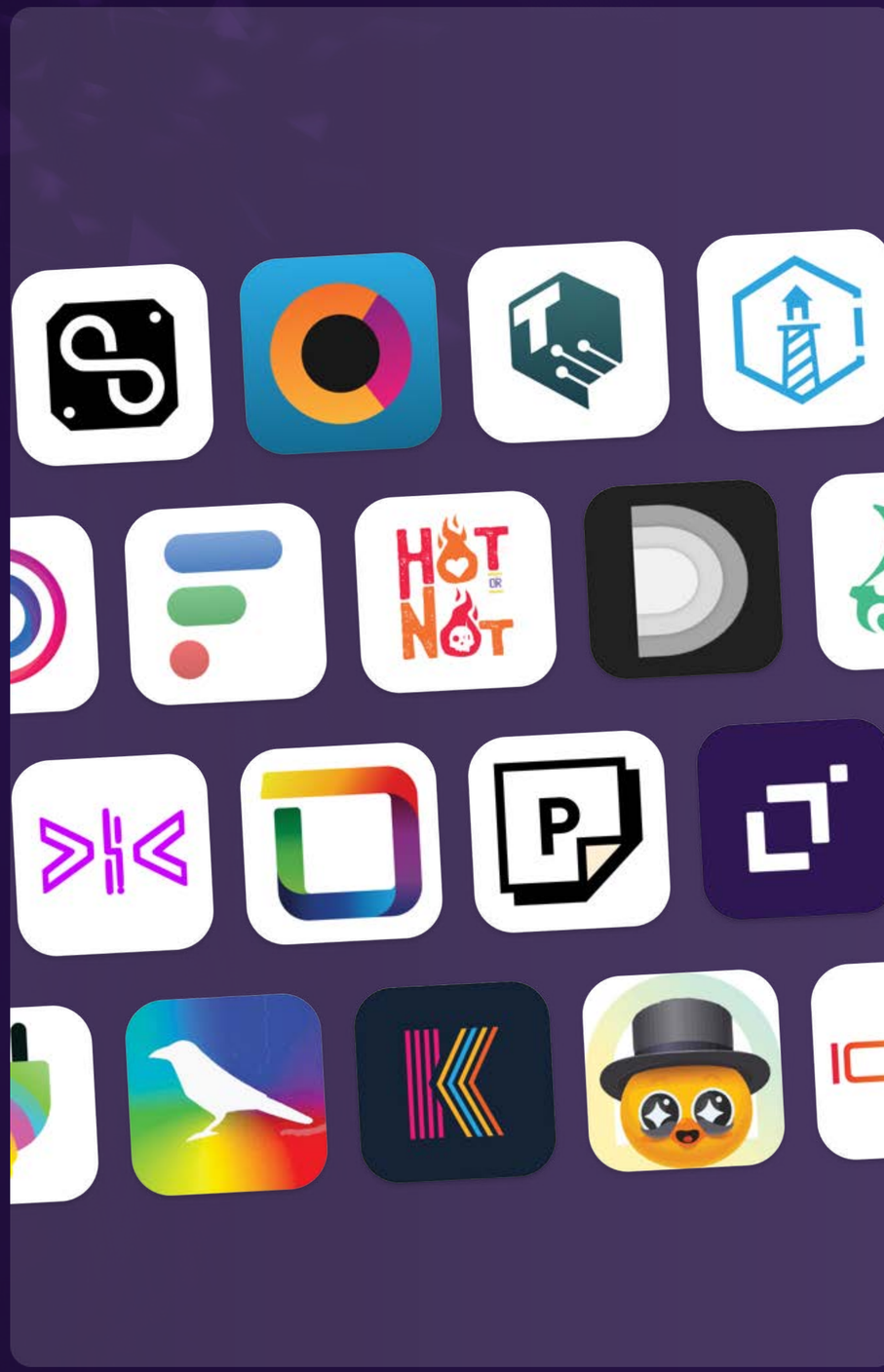
2.2M+

identities created

100+

dapps using II for authentication

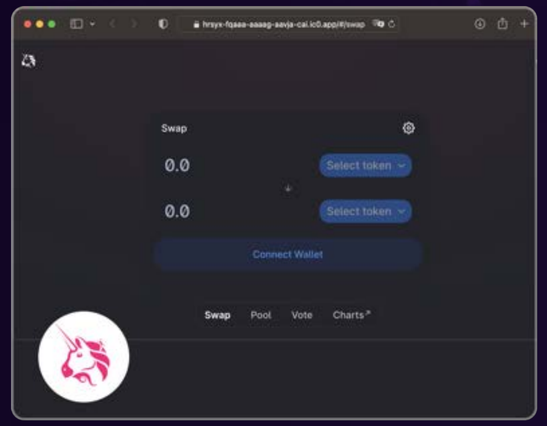
Support for relying parties and identity providers coming in 2023...

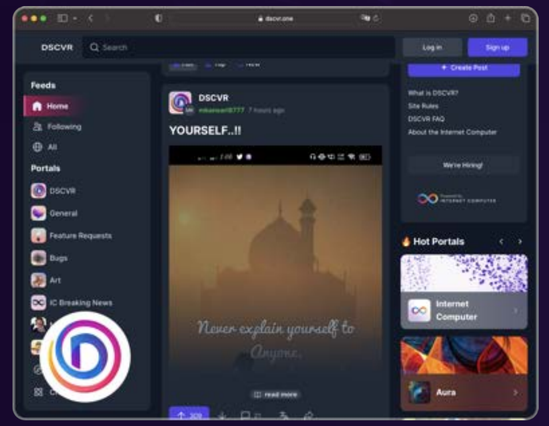


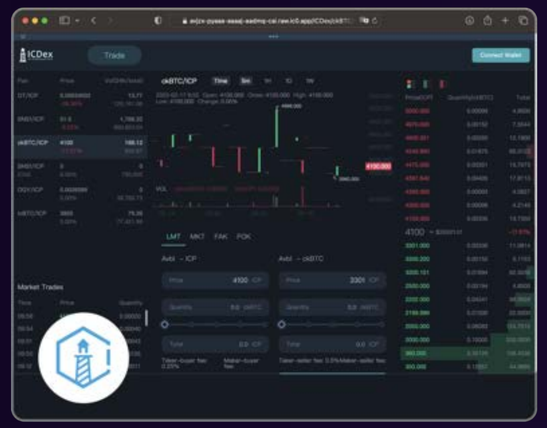
end-to-end software autonomy enables more compelling web3

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

full tokenization can transform user communities into giant industrious virtual workforces







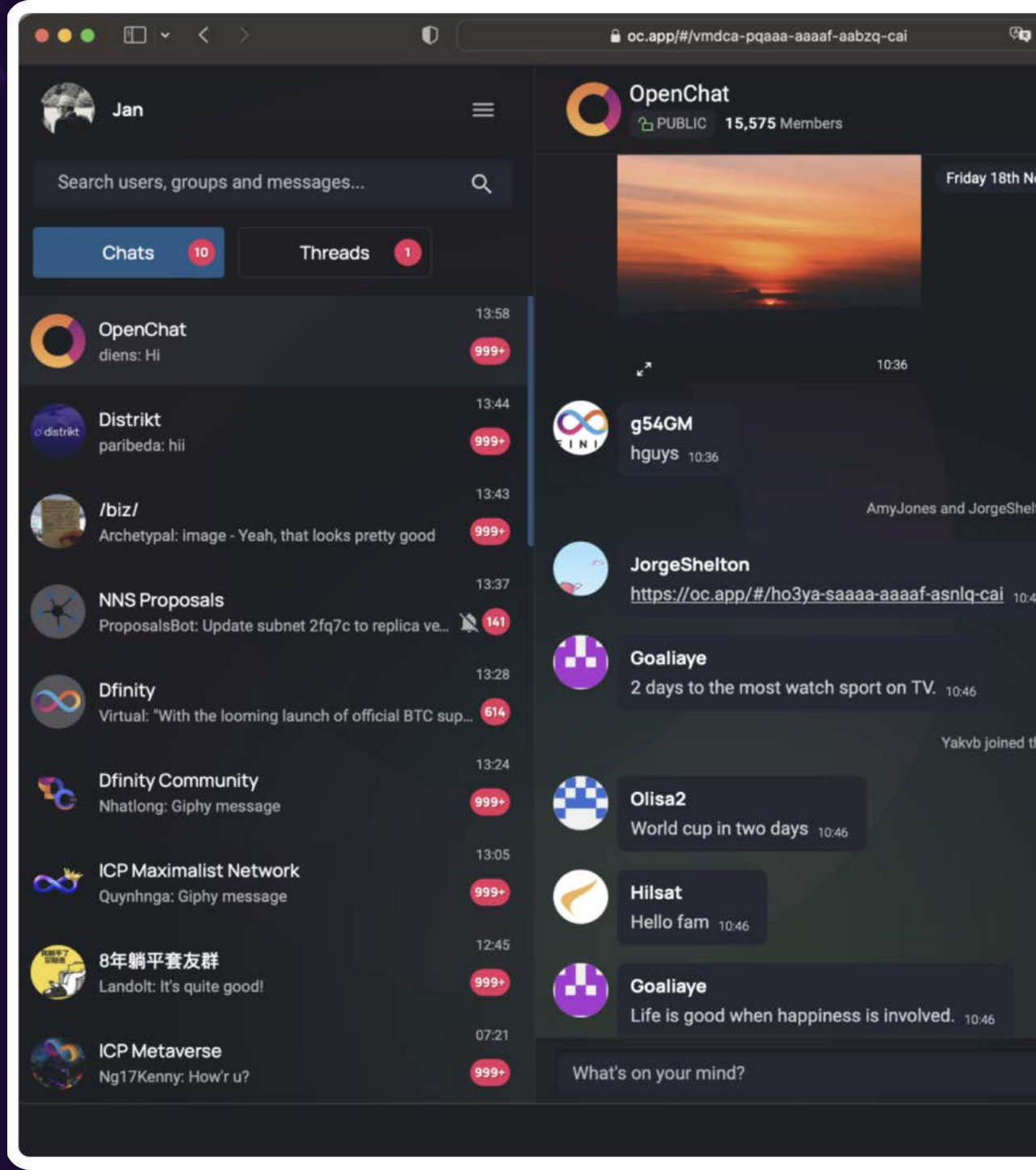
internetcomputer.org

build on the network

OC.app

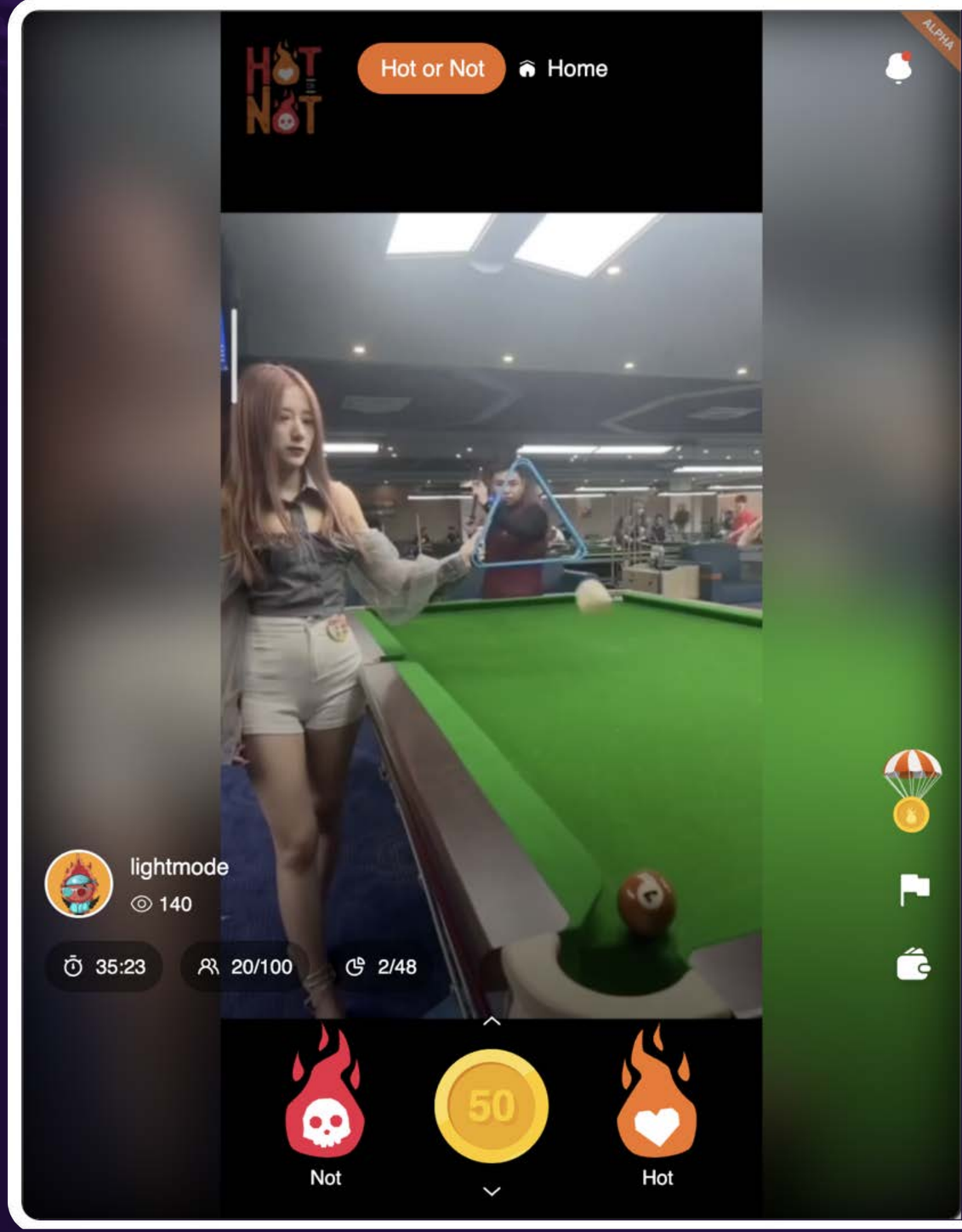
was the first
"open internet service"
on the Internet Computer

- ✓ 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
- ✓ OIS runs as an autonomous protocol...

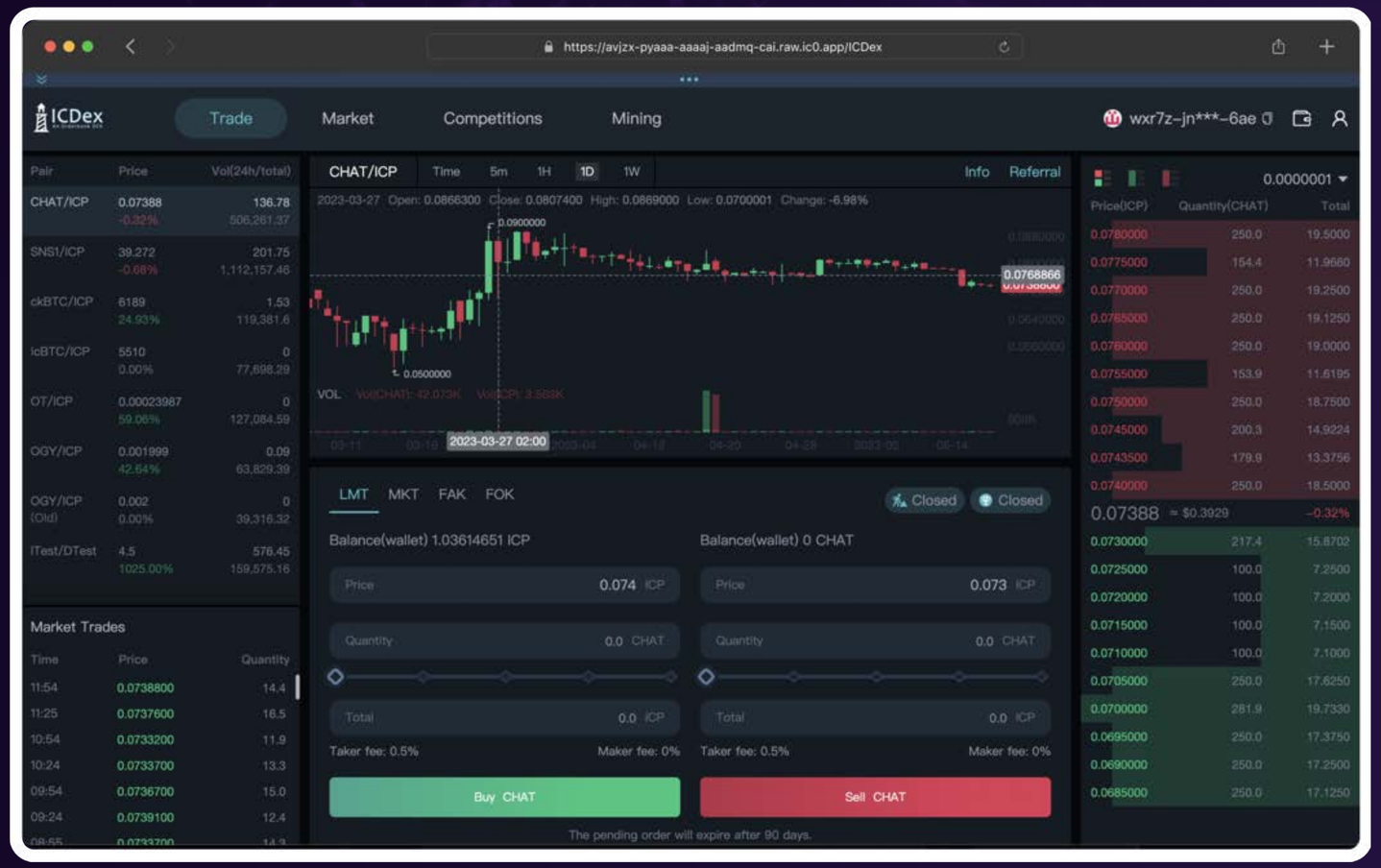


HotOrNot.wtf

- tokenized TikTok runs from 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 model....
- video creators, users, are founderized team members
- protocol exclusively controlled by SNS DAO



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



- All advantages of canister smart contract security
- SNS DAO can make fully transparent and remove backdoors

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

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

no cloud. no database servers.

web3 services can be built entirely from canister code:
the network is the entire tech stack

no firewalls. no security teams.

web3 services don’t need firewalls to protect them:

not necessary for tamperproof canister code

enterprise

web3 experience demonstrates canister smart contracts can deliver important advantages to enterprise

the world will spend $5 trillion on IT in 2024. 36% is personnel

TRADITIONAL IT

developers, security team, maintenance...

complexity

CANISTERS

$1.35 trillion
in potential savings

REDUCE

systems and services are tamperproof

Gartner Research

Cybersecurity spend

2022

$172 billion

R E D U C E

Gartner Research

CPS incident costs

2023

$50 billion

R E D U C E

serverless cloud model can deliver compute efficiencies

Gartner Research

Cloud services spend

2022

$482 billion

R E D U C E

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 US 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 hardware

sovereign subnets coming

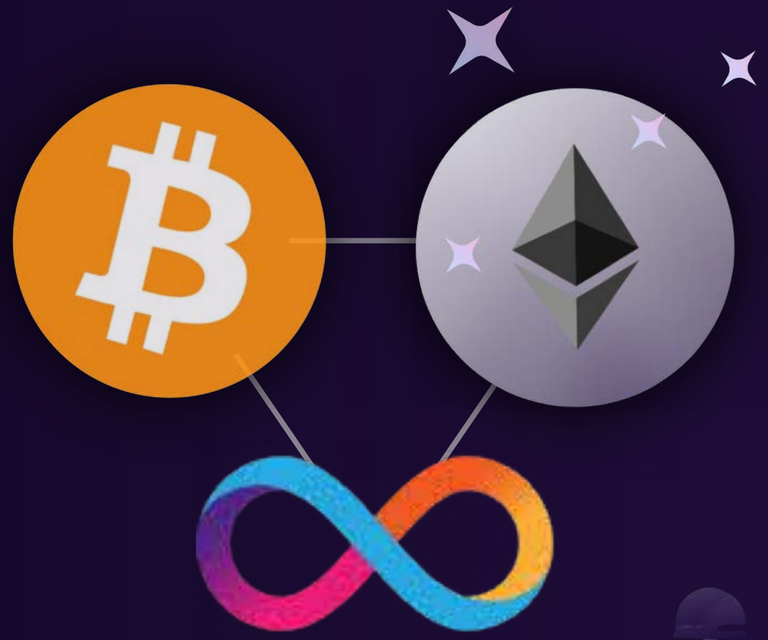
the Internet Computer network will create geographically-local specialized sovereign subnets for nations

yup, no bridges, just trustless cryptography

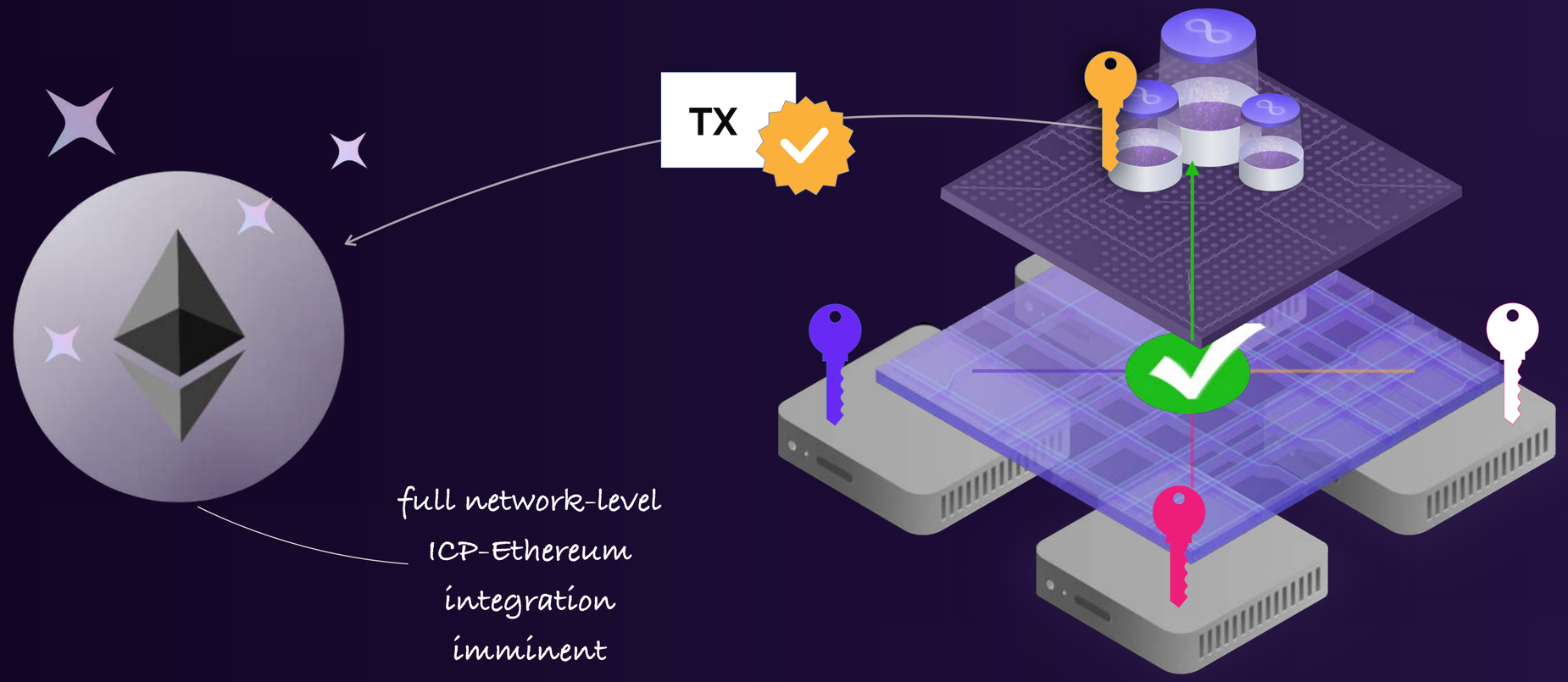
multi-chain

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

time to realize the World Computer vision from 2014

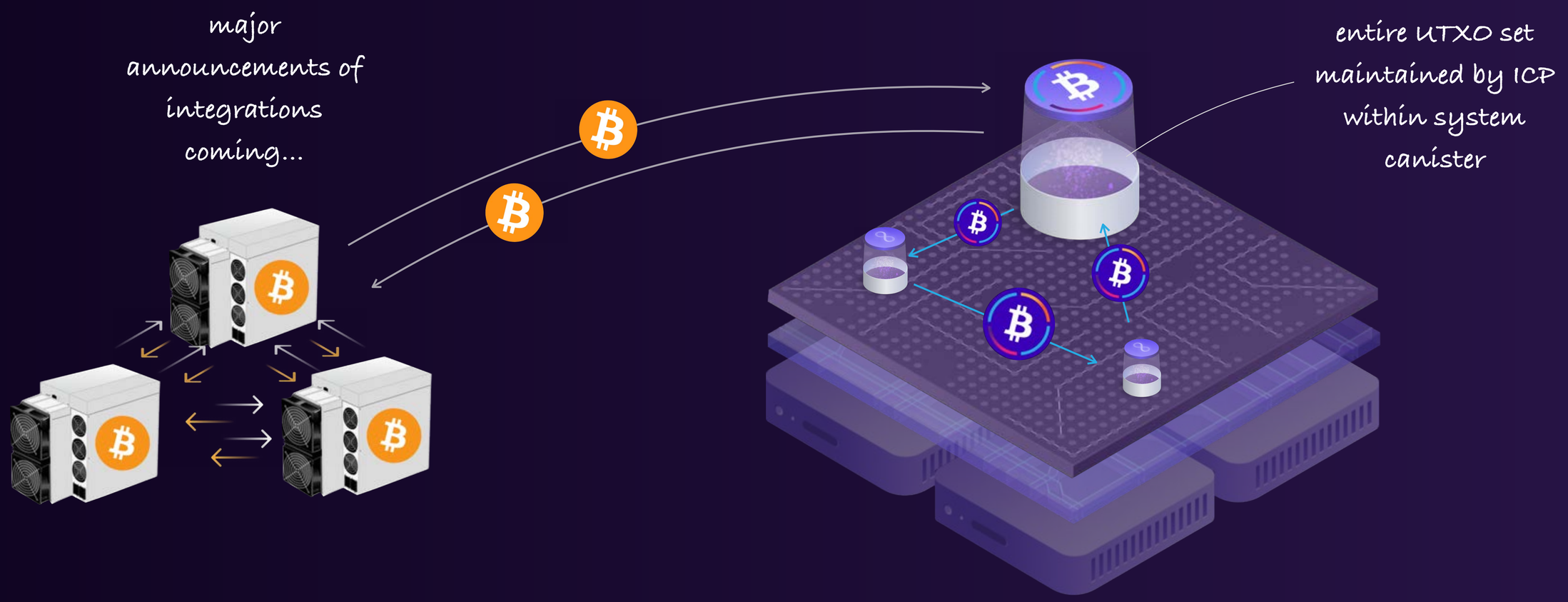


canisters create accounts and sign TXs on other blockchains



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

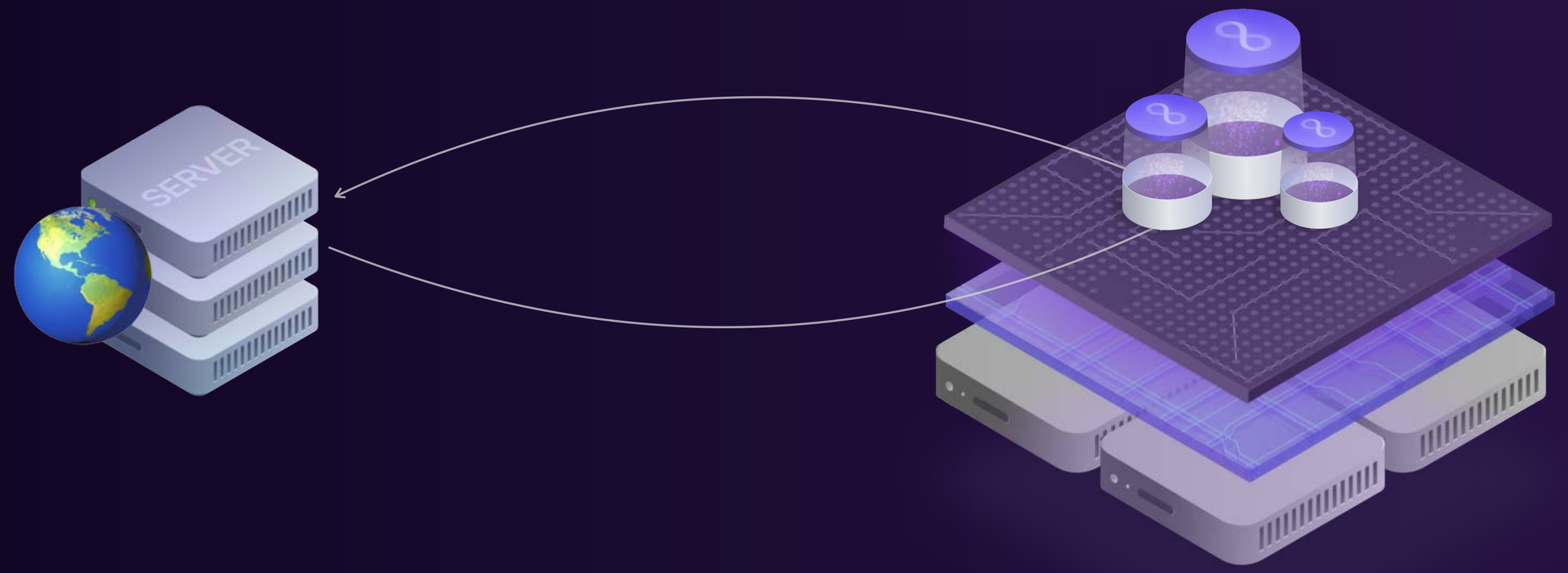


"chain-key bitcoin" supports usage of bitcoin in DeFi, social media, games, the metaverse with 1s finality

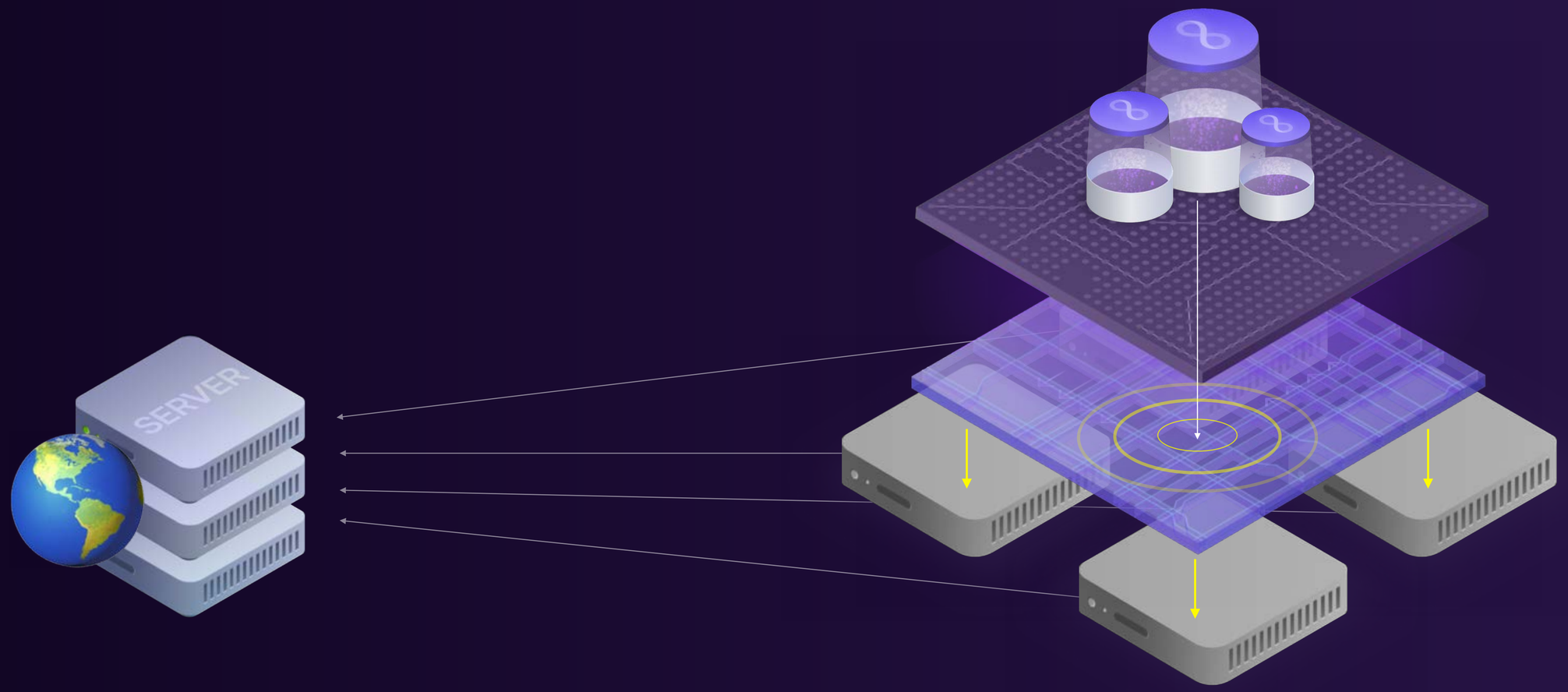
web2+3

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

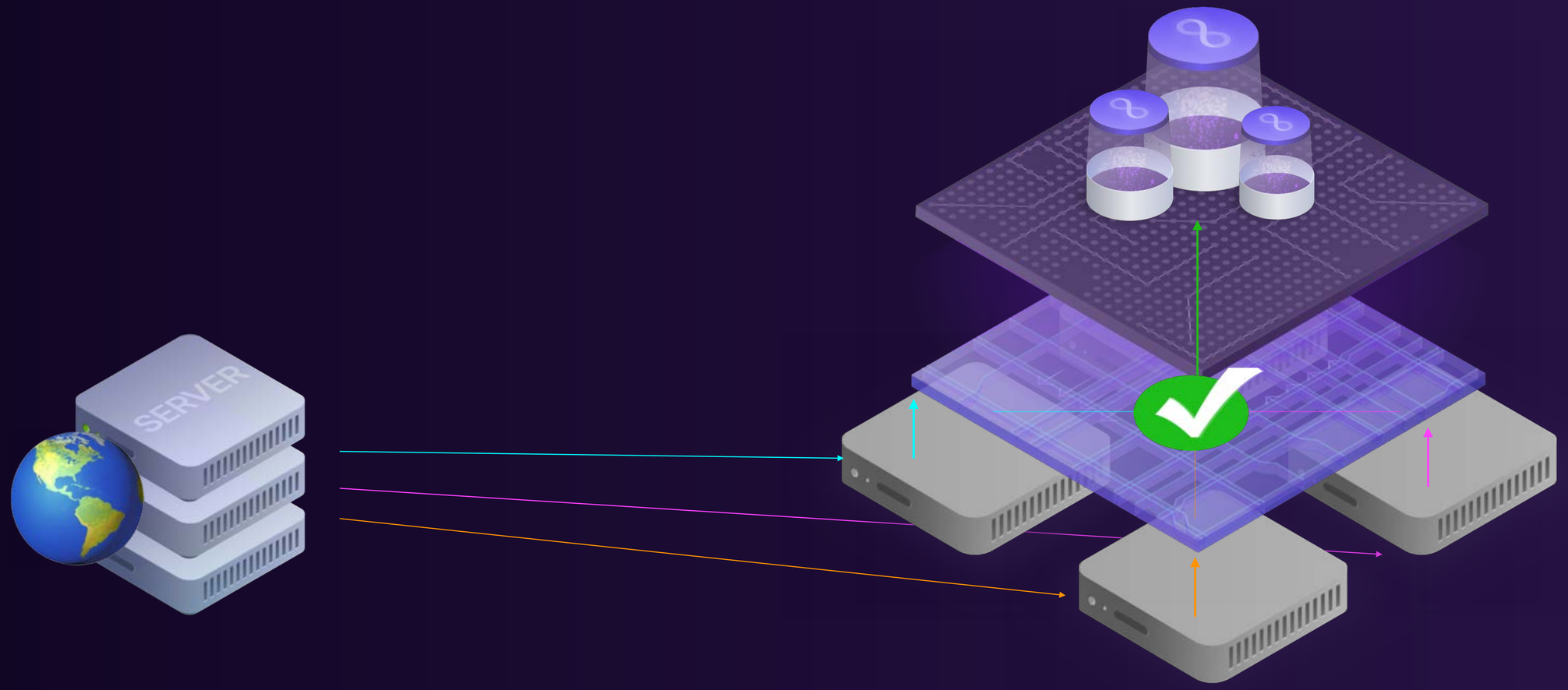
1. a canister initiates a call to a web2 service



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 🇨🇭

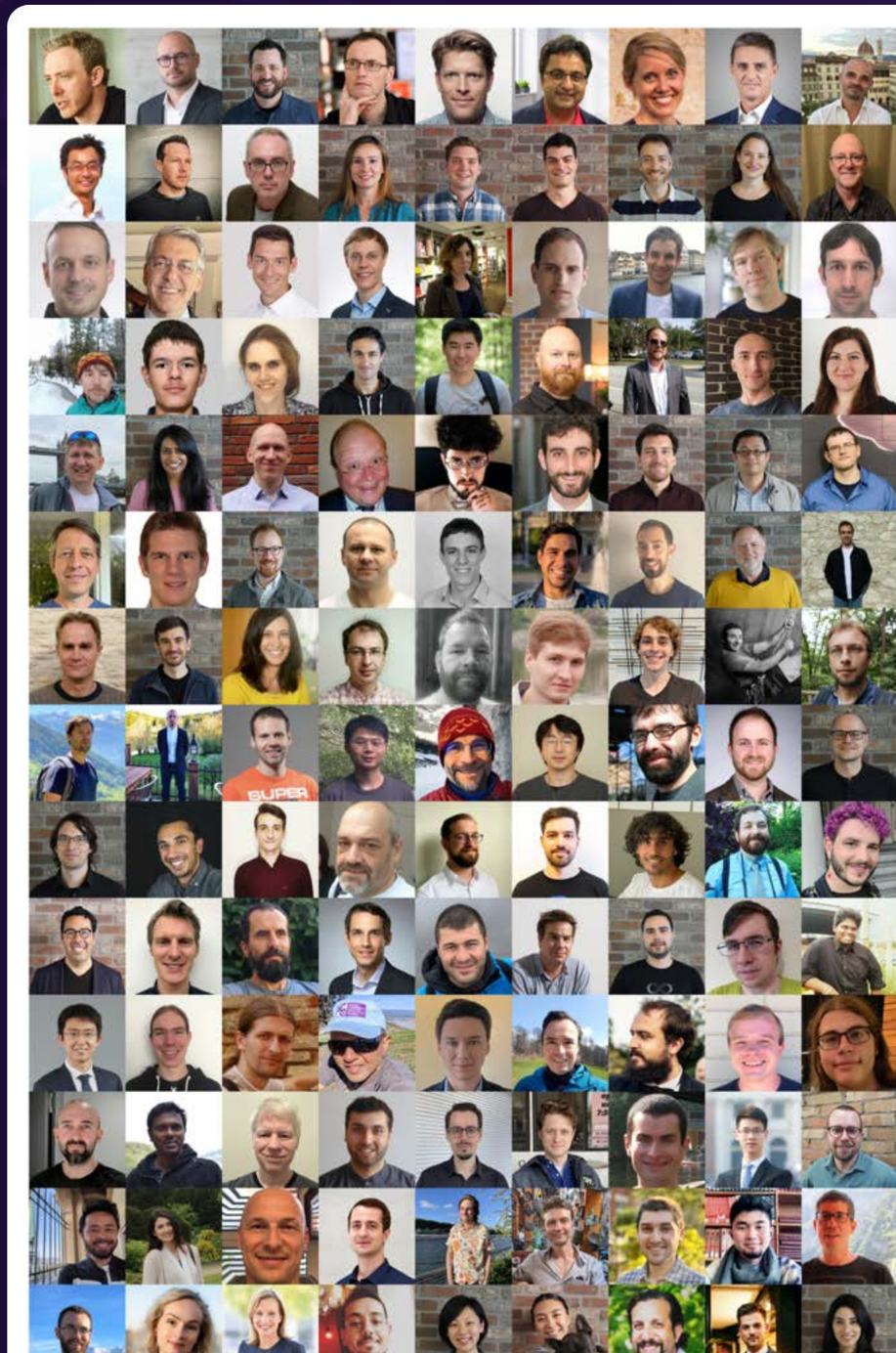
- Emerged from early Ethereum community in 2015
- DFINITY Foundation established October 2016
- Swiss not-for-profit foundation not a corporation
- World's largest team of cryptographers
- Over 140 people in Zürich HQ
- 270+ people globally

1600+
research papers

100 000+
academic citations

250+
technical patents

Crypto People + Google IBM facebook



build on the internet using the Internet Computer

decentralize everything

https://internetcomputer.org