INTERNET COMPUTER

Cypherspace as cloud 3.0

ICP | Internet Computer

Main deck version: 14 August 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?

THE INTERNET

could we use a public network as the foundations?

SOVEREIGN systems and services without big tech or government kill switches and backdoors

TAMPERPROOF systems and services where the logic and data cannot be subverted

COMMUNITY OWNED systems and services where a community has exclusive control

AUTONOMOUS systems and services that corporations cannot modify

EFFICIENT systems and services that need less IT personnel

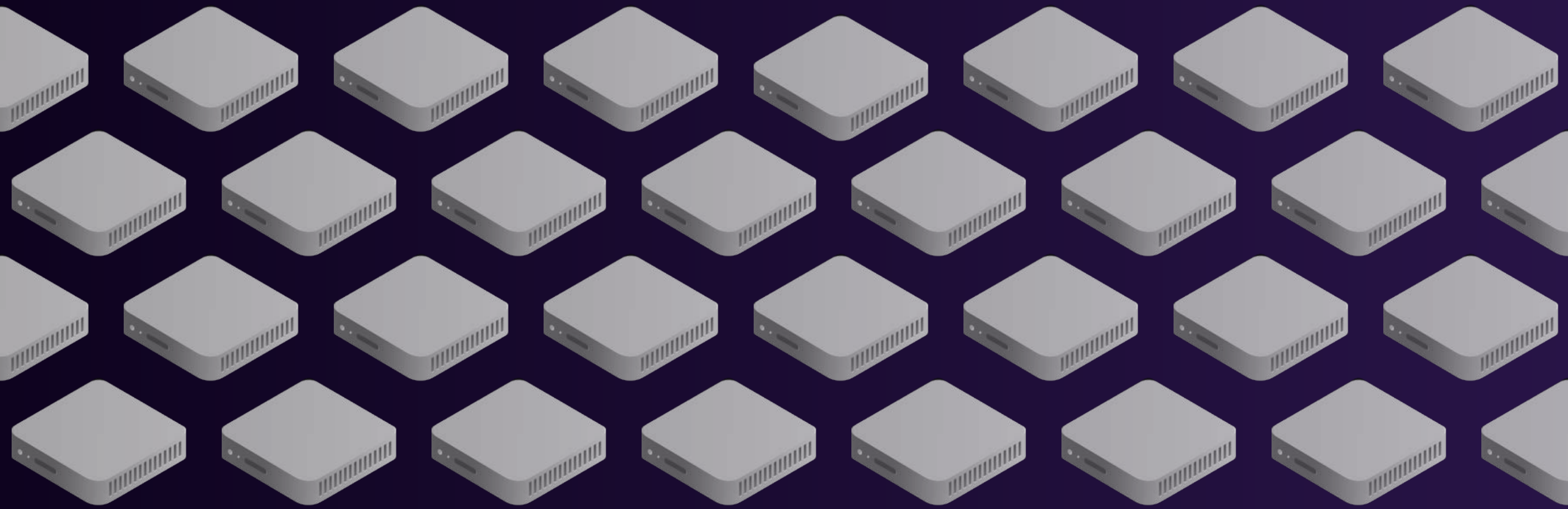
tech history arcs towards open networks

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

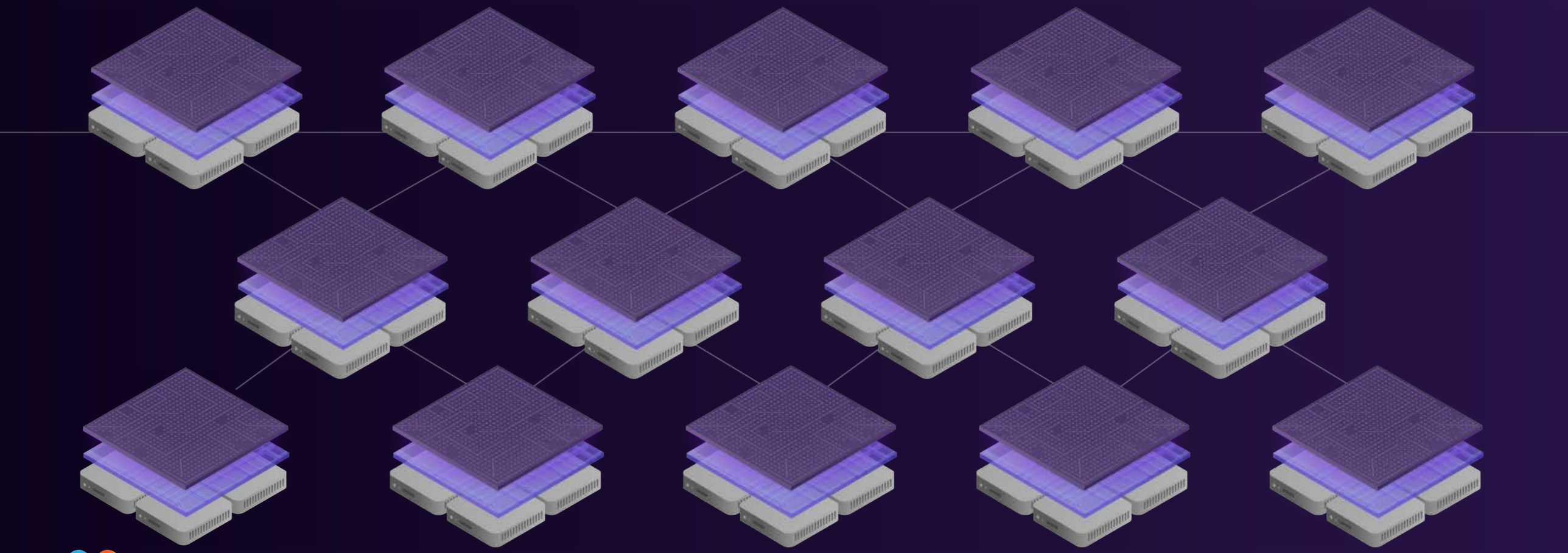
network

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

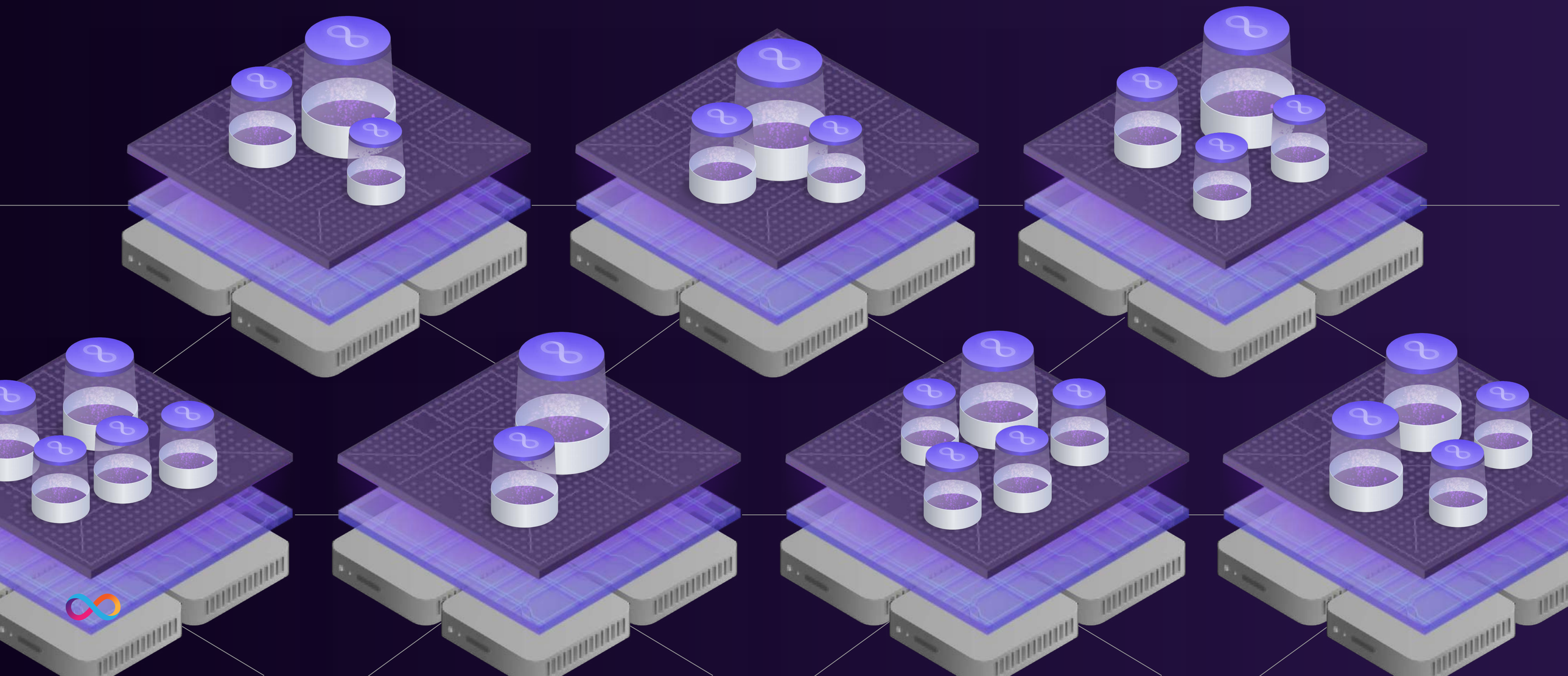
independent node providers own and operate node machines in data centers worldwide



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



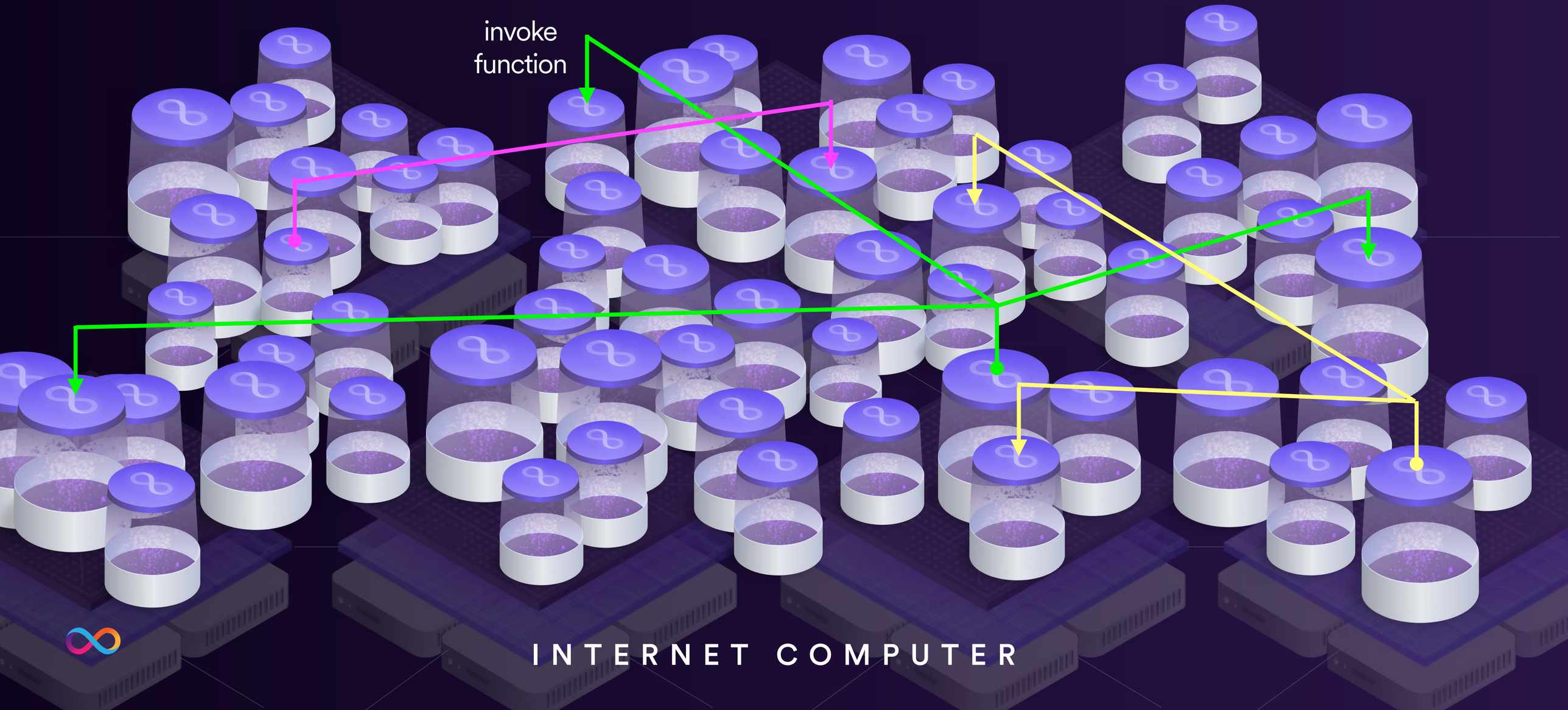
subnet blockchains add capacity for running *canister* smart contracts



subnets combine into ONE serverless *autonomous* cloud (that's stateful)

INTERNET COMPUTER

ONE seamless universe for tamperproof code units (no server instances)



INTERNET COMPUTER

created by a new form of blockchain network

blockchain speed, energy scalability and user experience challenges addressed allowing general application

Bitcoin

2009

digital gold

Ethereum

2015

smart contracts

Internet Computer

2021

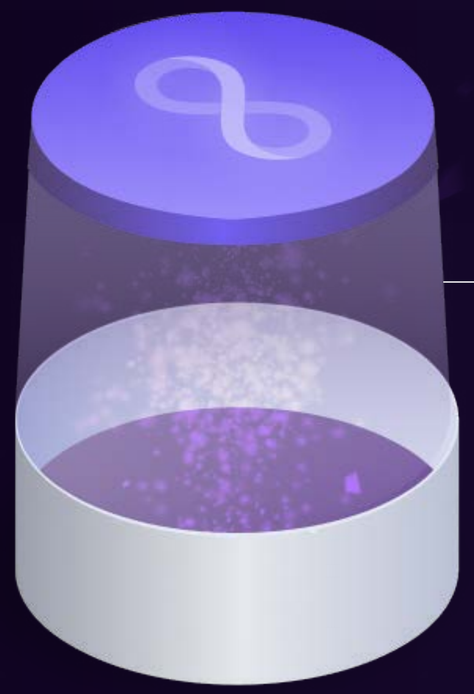
autonomous cloud

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.

smart contracts 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 fault tolerant and 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

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

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

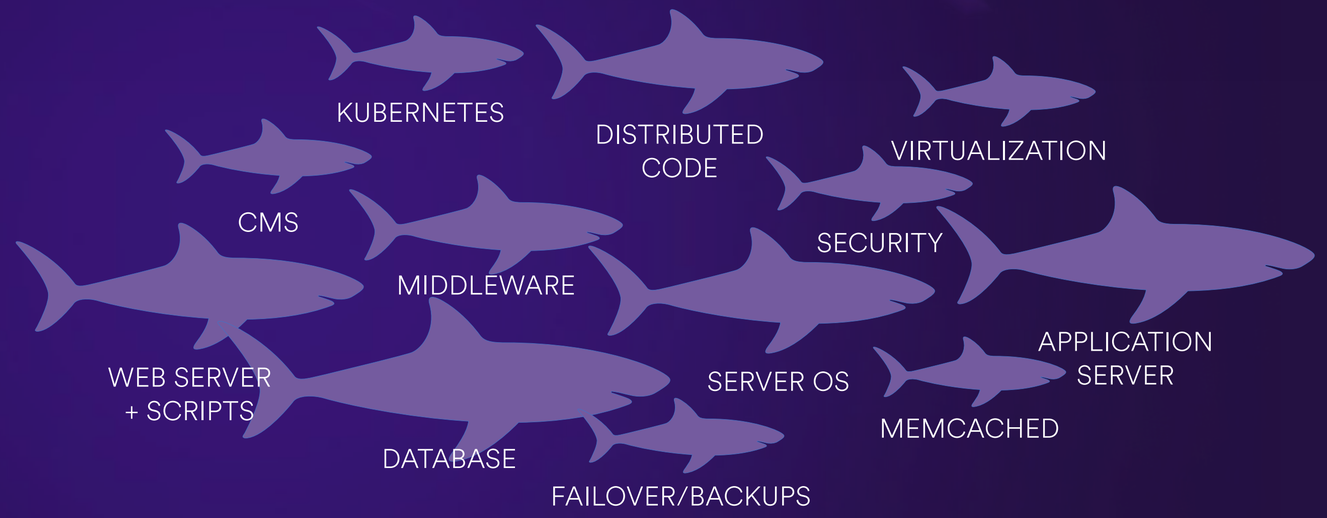
web interaction
directly process HTTP and serve user experiences

actor model
canisters keep data private and run in parallel

the network runs canisters in parallel deterministically

software will eat the world. smart contracts will eat software

SMART CONTRACTS



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

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 canisters

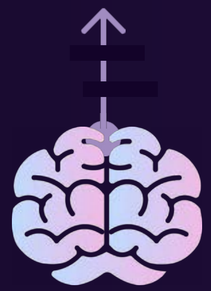
SMART CONTRACTS

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 autonomy on the Internet Computer

1.

fully autonomous network

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.

2.

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.

3.

unmodifiable canisters

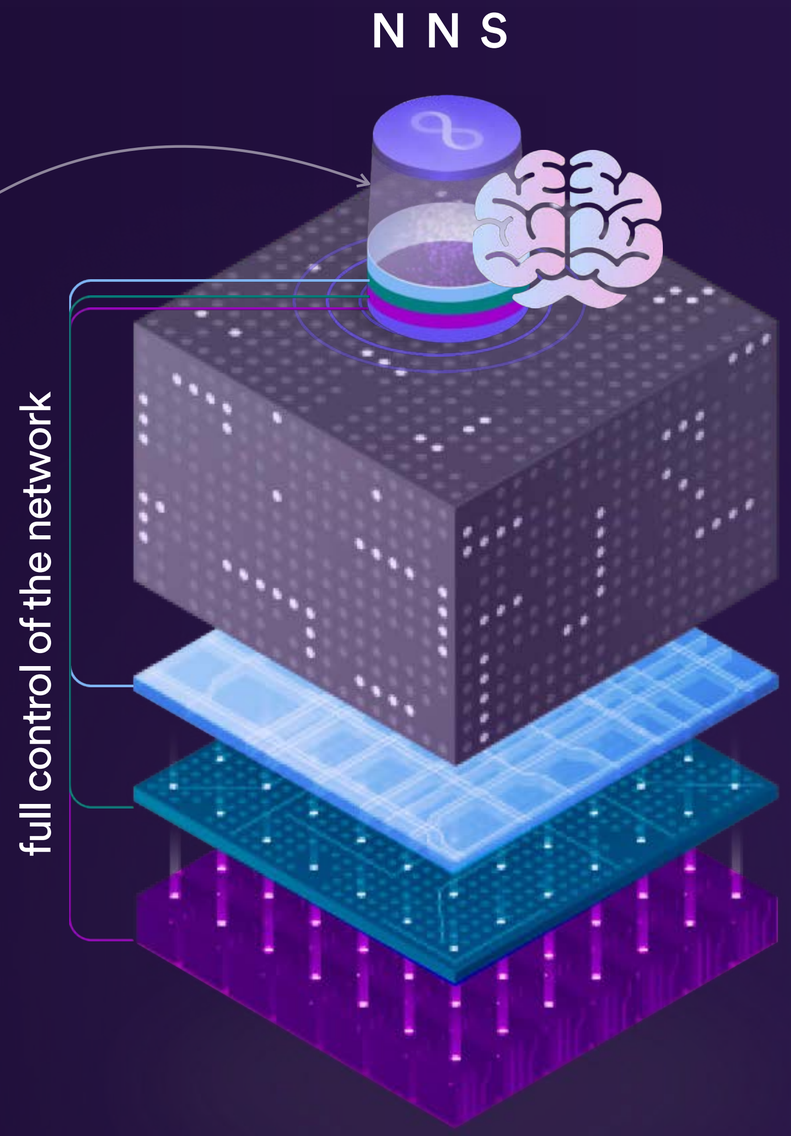
what if nothing should be able to modify canisters? For example, what about global financial rails that many other systems and services build on top of, or what about a wallet that must be absolutely secure? the Internet Computer network can host canisters that cannot be modified by anyone, which continue 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

Network Nervous System DAO

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

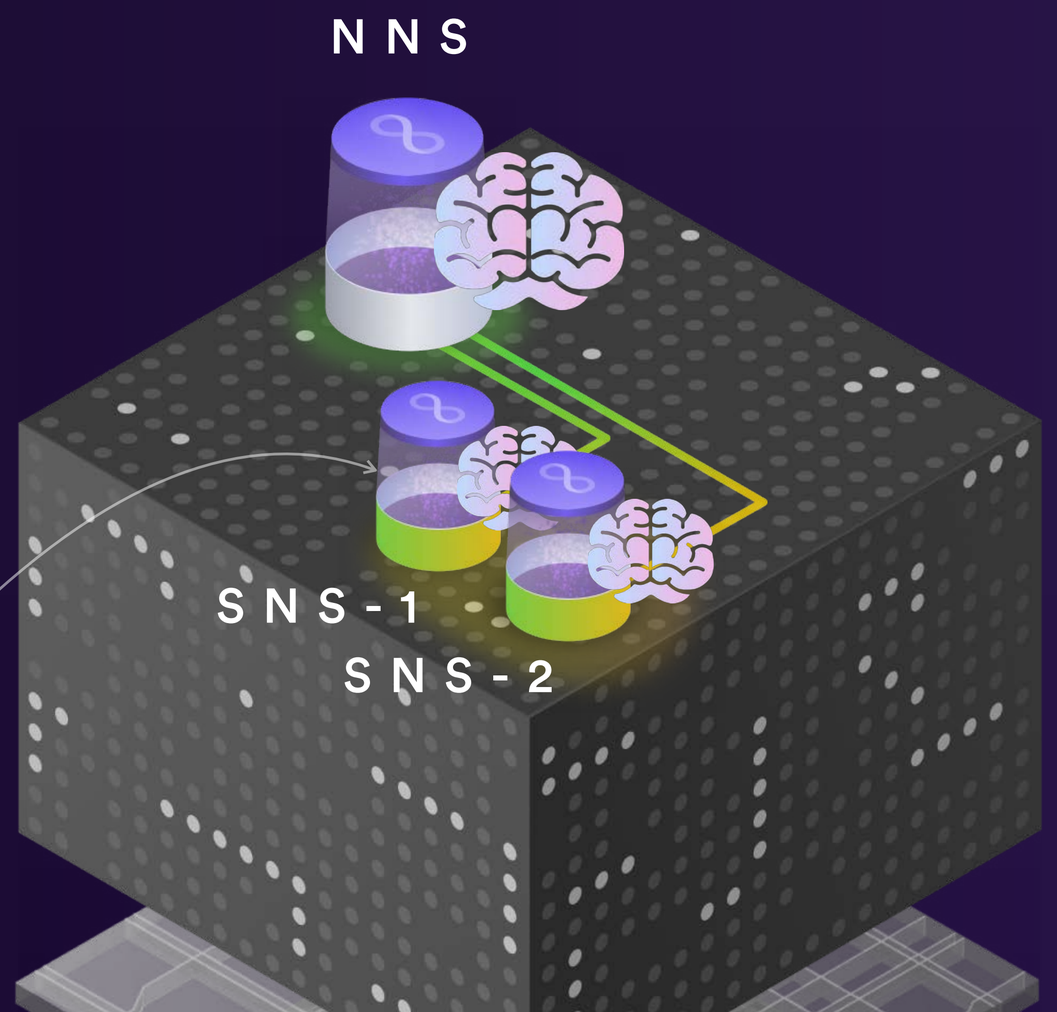
- public, open, transparent and permissionless
- users lock ICP tokens to create "voting neurons"
- neurons vote automatically by following other neurons
- tens of thousands of users have created neurons
- submitted proposals are adopted or rejected
- algorithmic liquid democracy decides on proposals
- 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



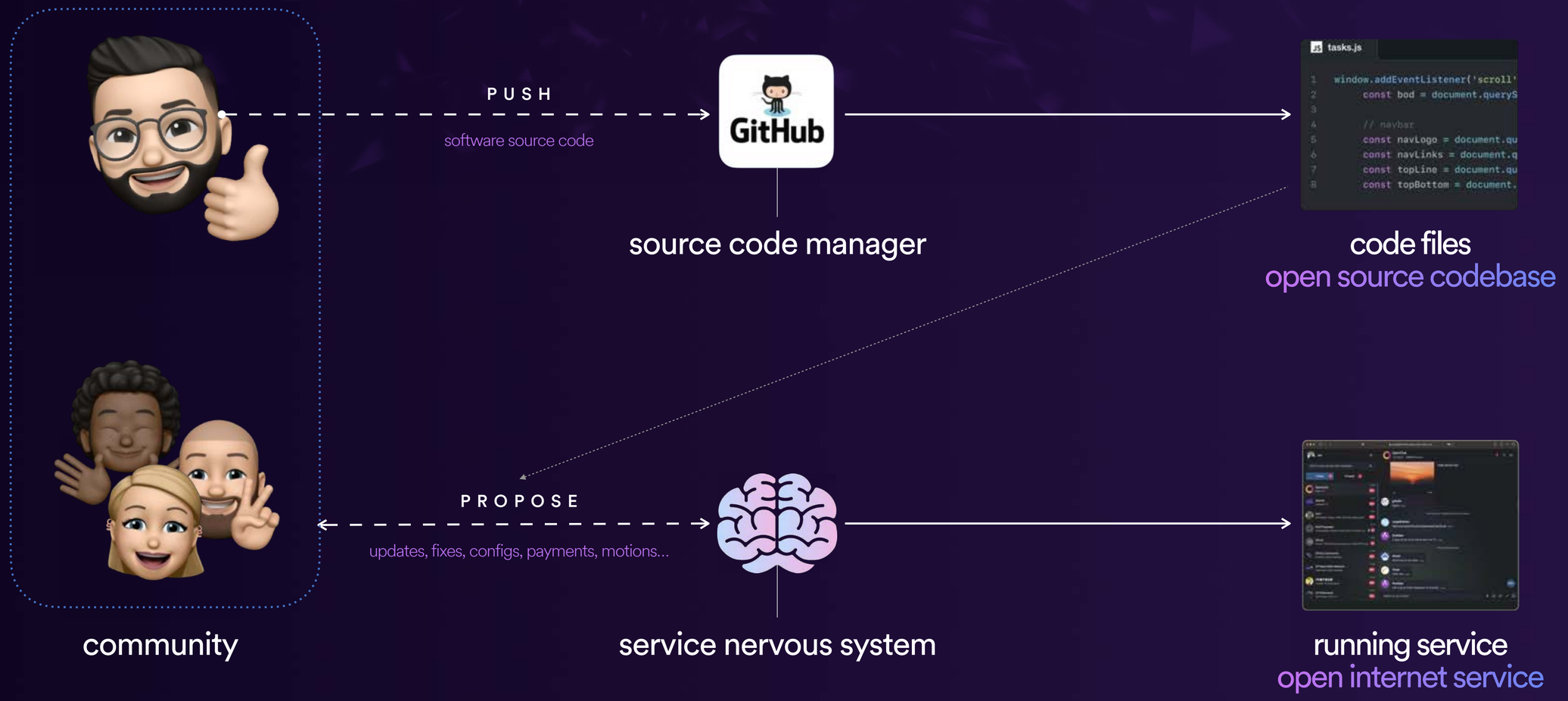
service nervous system DAOs

SNS DAOs use similar governance technology to the NNS. an SNS manages a democratic “open internet service” or a 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 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



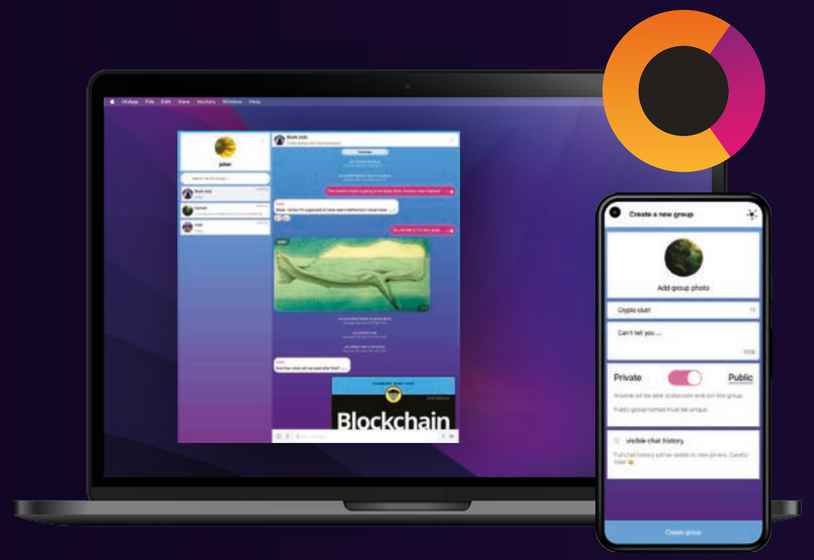
an open internet service (OIS) gives a community 100% control



pure web3

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

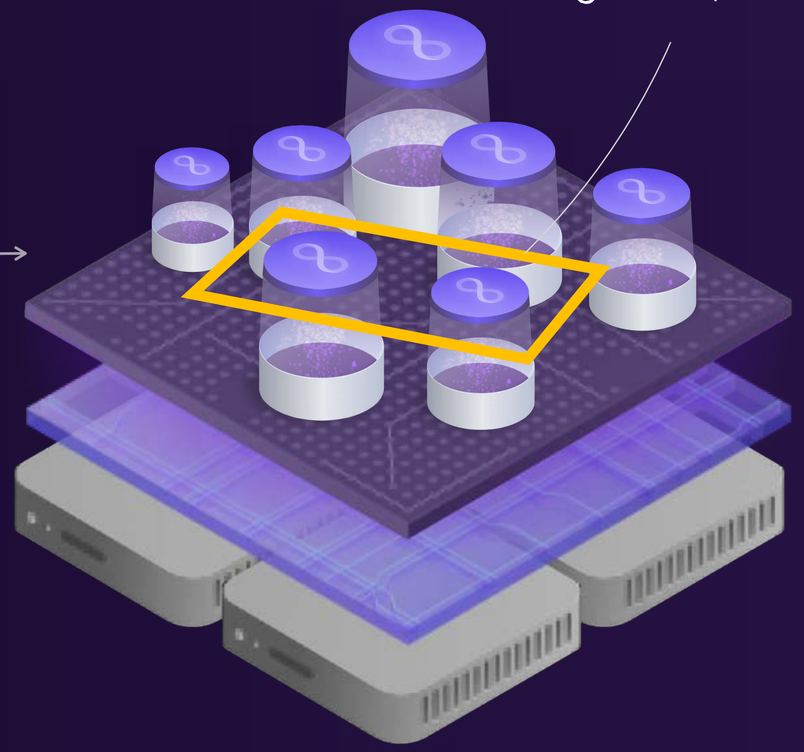
users interact with services over HTTP (the web)



WEB3 EXPERIENCE

web browsers interact with canisters over HTTP

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



crypto tip canisters pay for their own computation ("reverse gas") so users don't need wallets

Internet Identity frameworks create sessions for user interaction

the session allows the user experience to transparently submit 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

unique chain key cryptography is what makes the Internet Computer network possible

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).

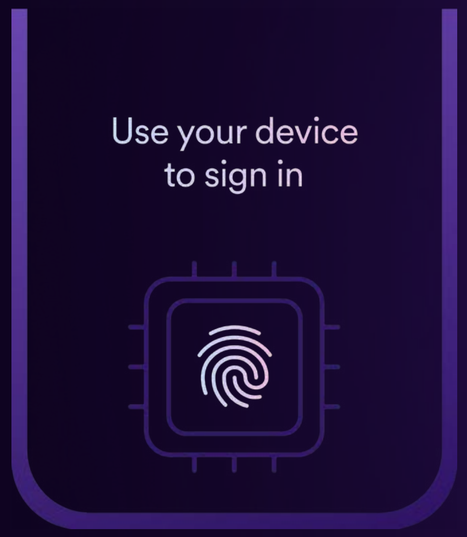
Open source

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

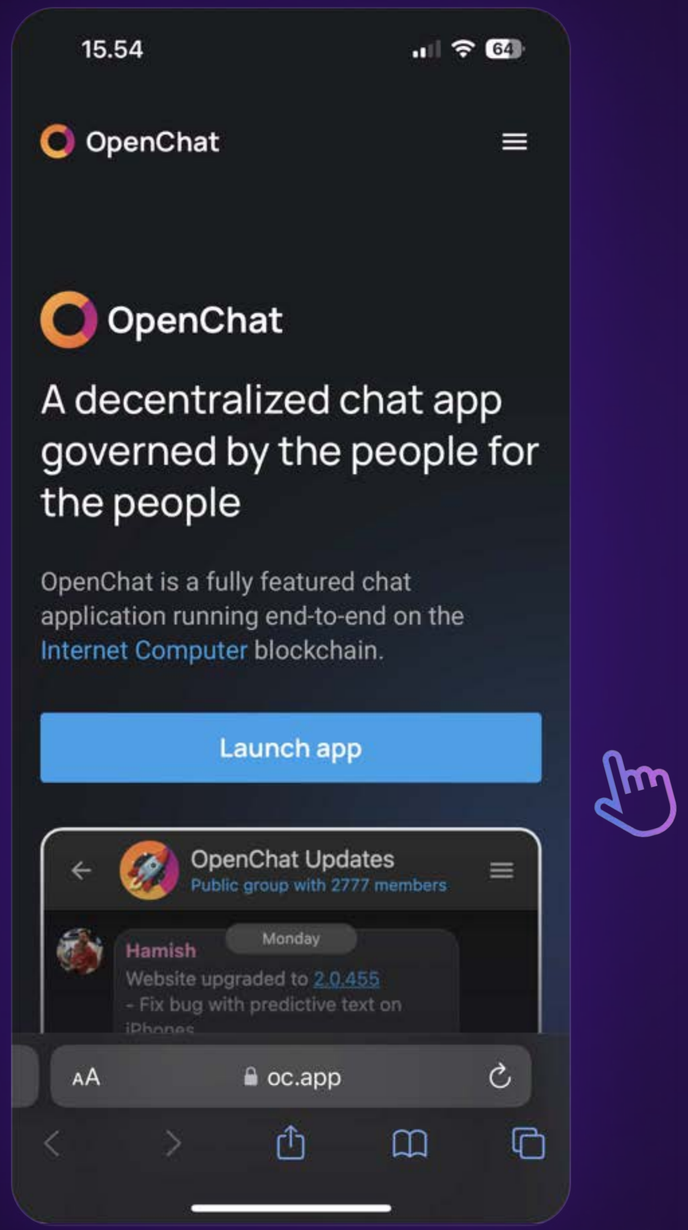
+

WebAuthn (+ FIDO)

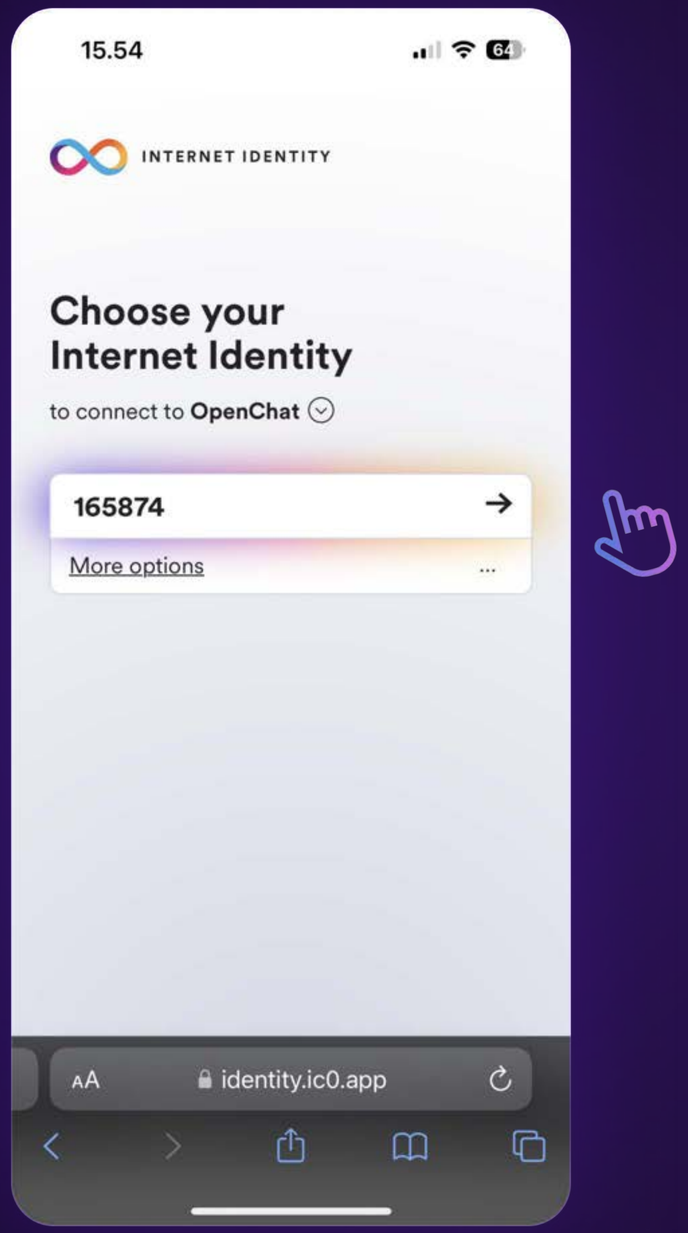
+

Internet Computer

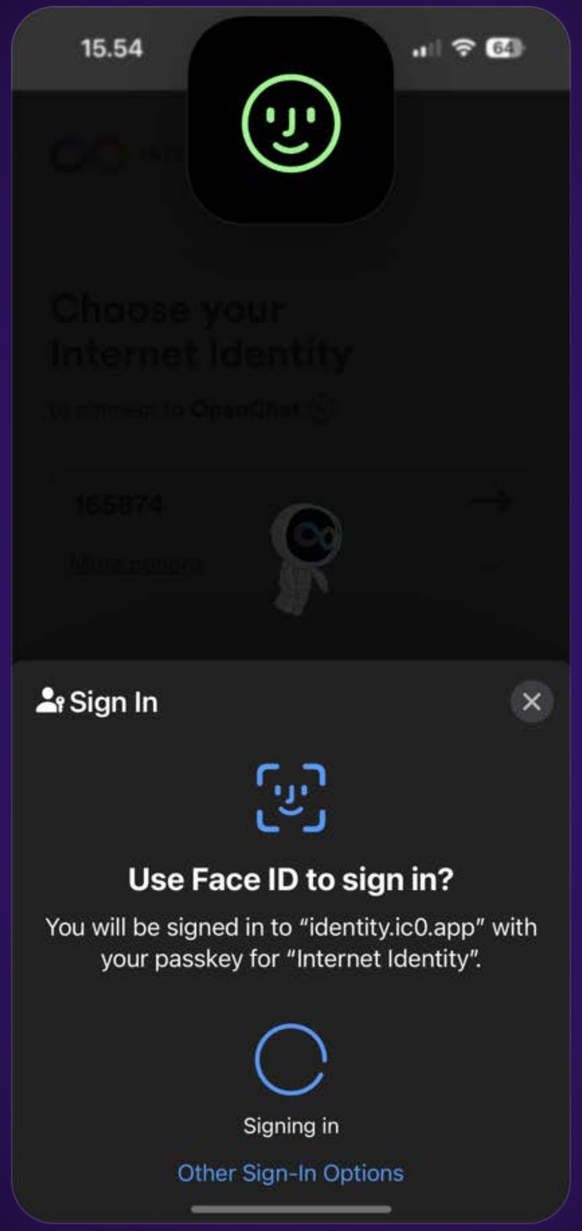
INTERNET IDENTITY



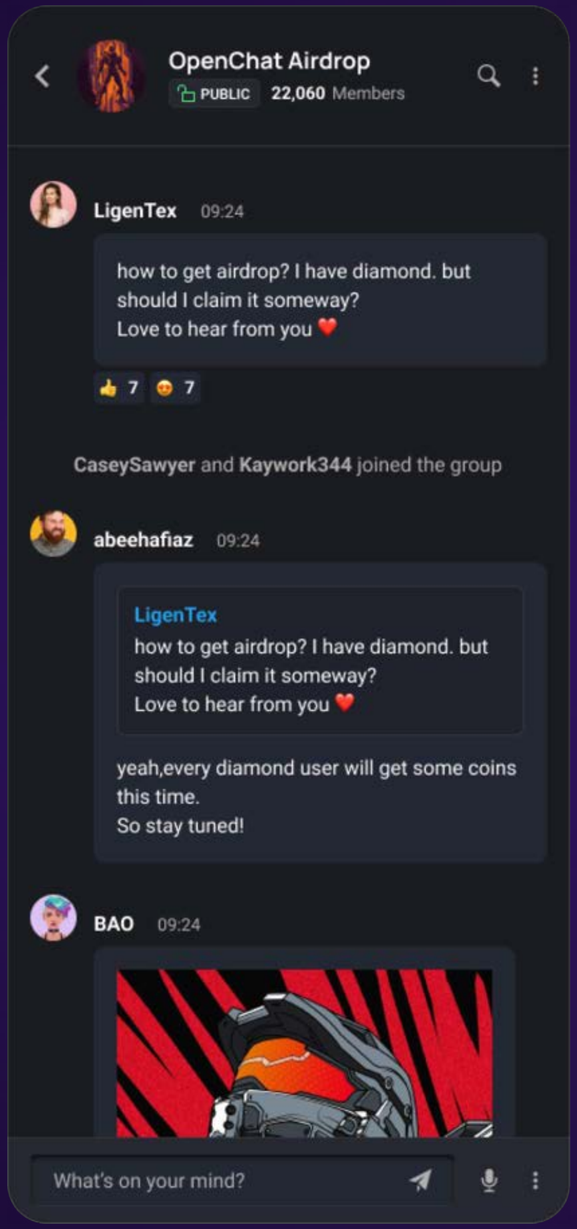
INTERNET IDENTITY



INTERNET IDENTITY



INTERNET IDENTITY



where we are now

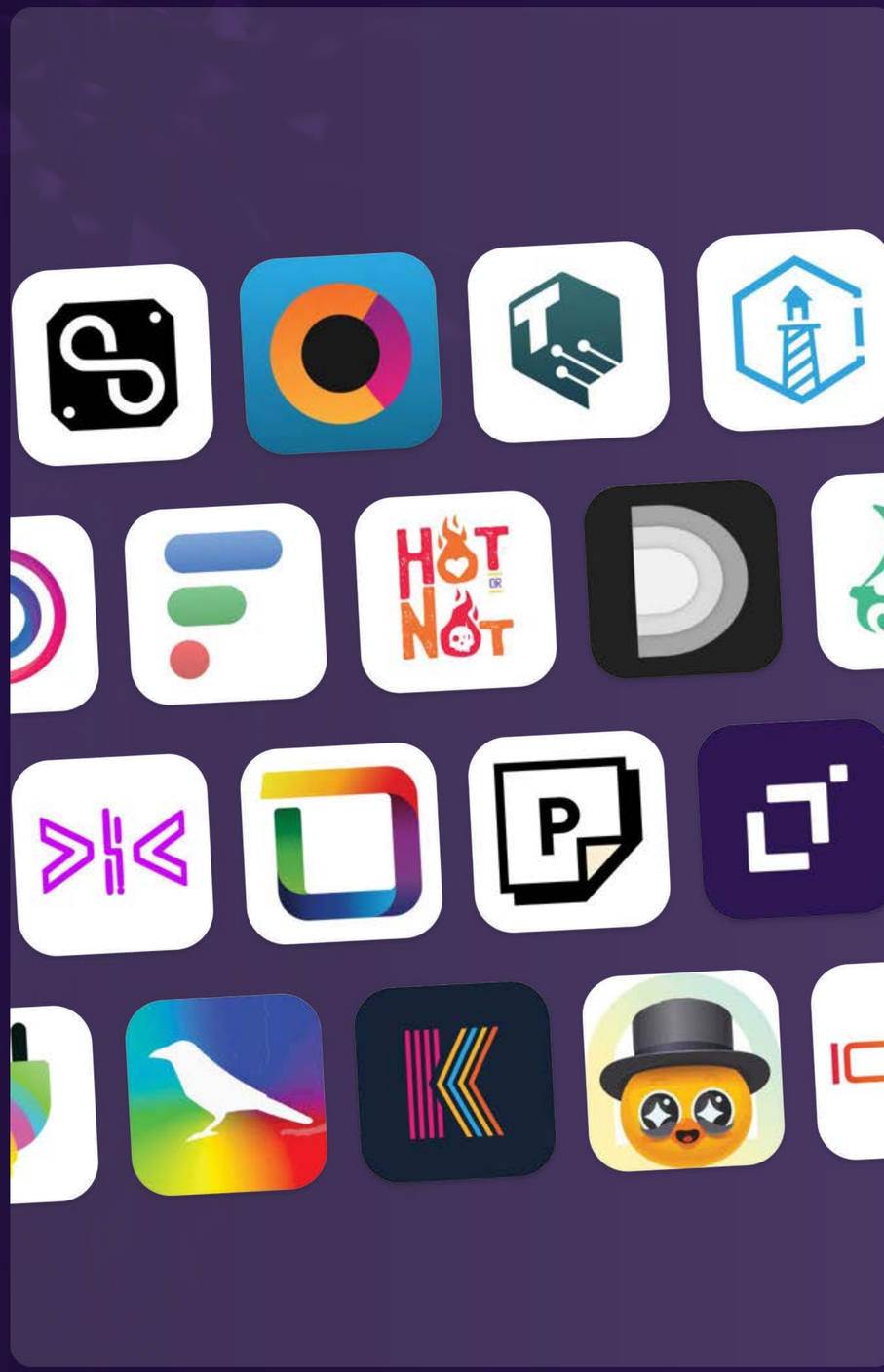
2.2M+

identities created

100+

dapps using II for authentication

support for zero knowledge identity attestation coming soon...



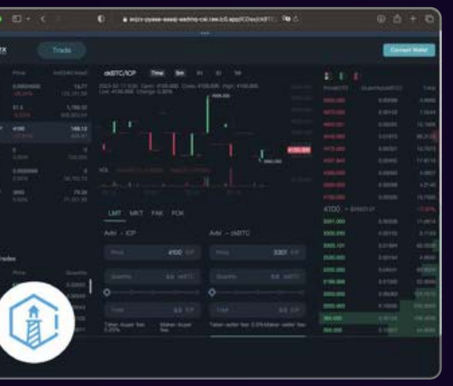
autonomous services can deliver more compelling web3

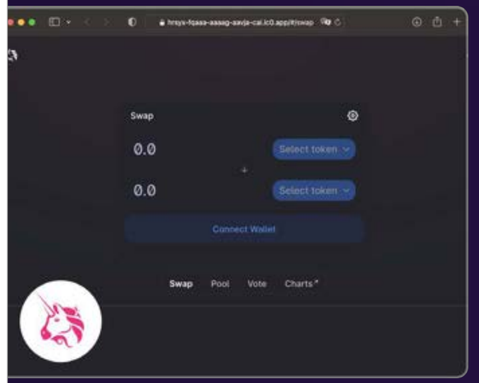
community DAOs have complete control · tokenization works without crypto wallets or friction

full tokenization can transform user communities into giant industrious virtual workforces

browse dapps in the ecosystem

internetcomputer.org





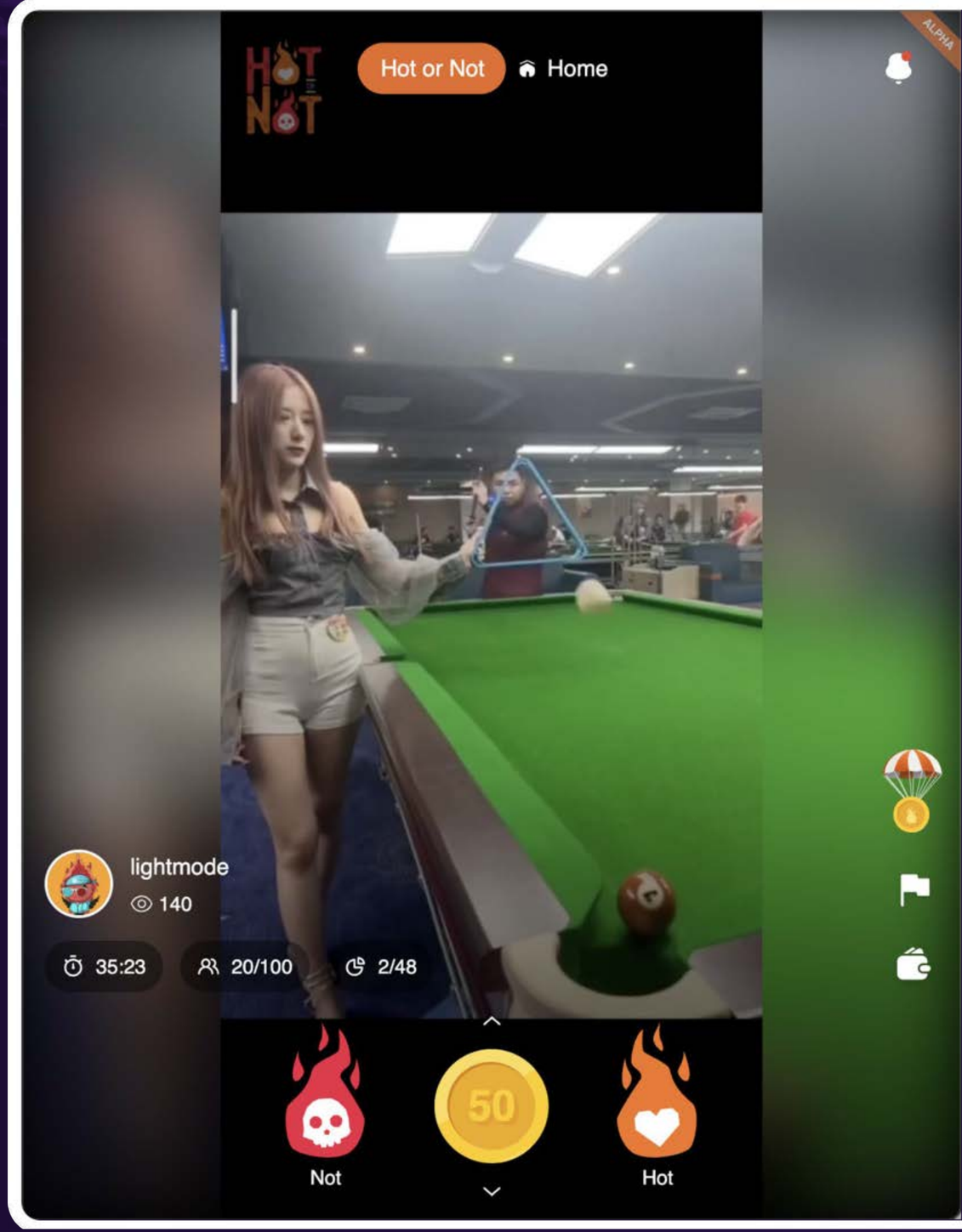
OC.app

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

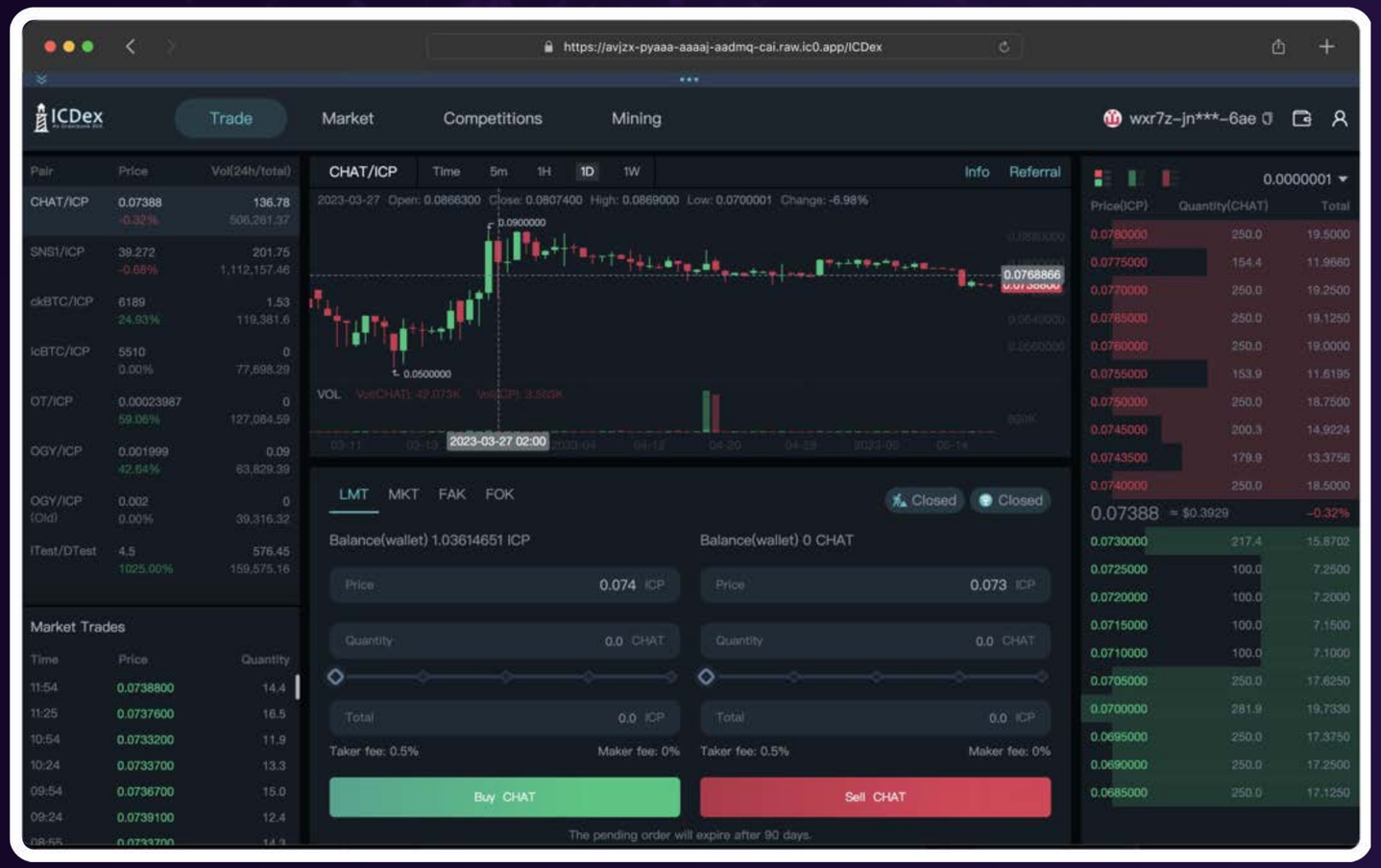
- ✓ messaging service runs 100% on network
- ✓ chat accounts are also crypto wallets i.e. full SocialFi
- ✓ seamlessly send satoshis using chat messages
- ✓ users hold governance tokens (called CHAT)
- ✓ bounties for users promoting OpenChat
- ✓ rewards for those creating viral content
- ✓ updates pass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

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

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

the Internet Computer can deliver tremendous advantages to the enterprise sector

building with canister software significantly reduces IT personnel spend

LEGACY IT STACK

developers, administrators, security team, maintenance...

2024

$1.8 trillion

Gartner Research

-75% complexity

CANISTERS

$1.35 trillion in potential savings

if everything was built using canister software

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 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

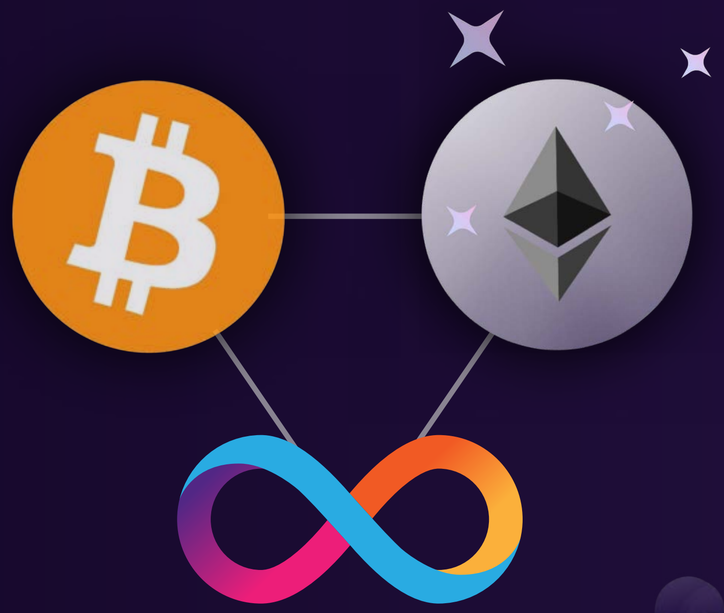
the Internet Computer network will create geographically-local specialized sovereign subnets for nations

no bridges, just trustless cryptography

multi-chain

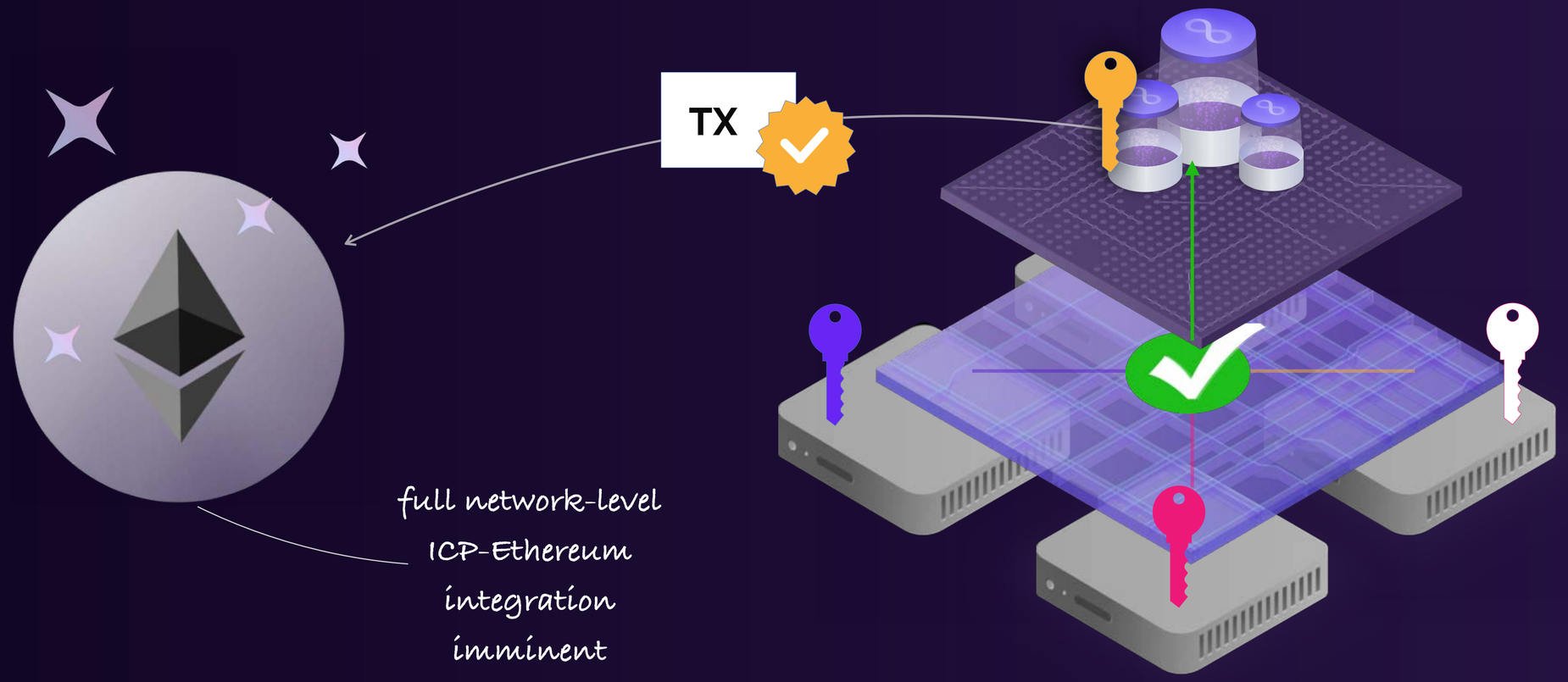
“chain key cryptography” creates transactions on other chains.
network-level integrations with Bitcoin and Ethereum

Internet Computer enables the World Computer vision from 2014



NEW

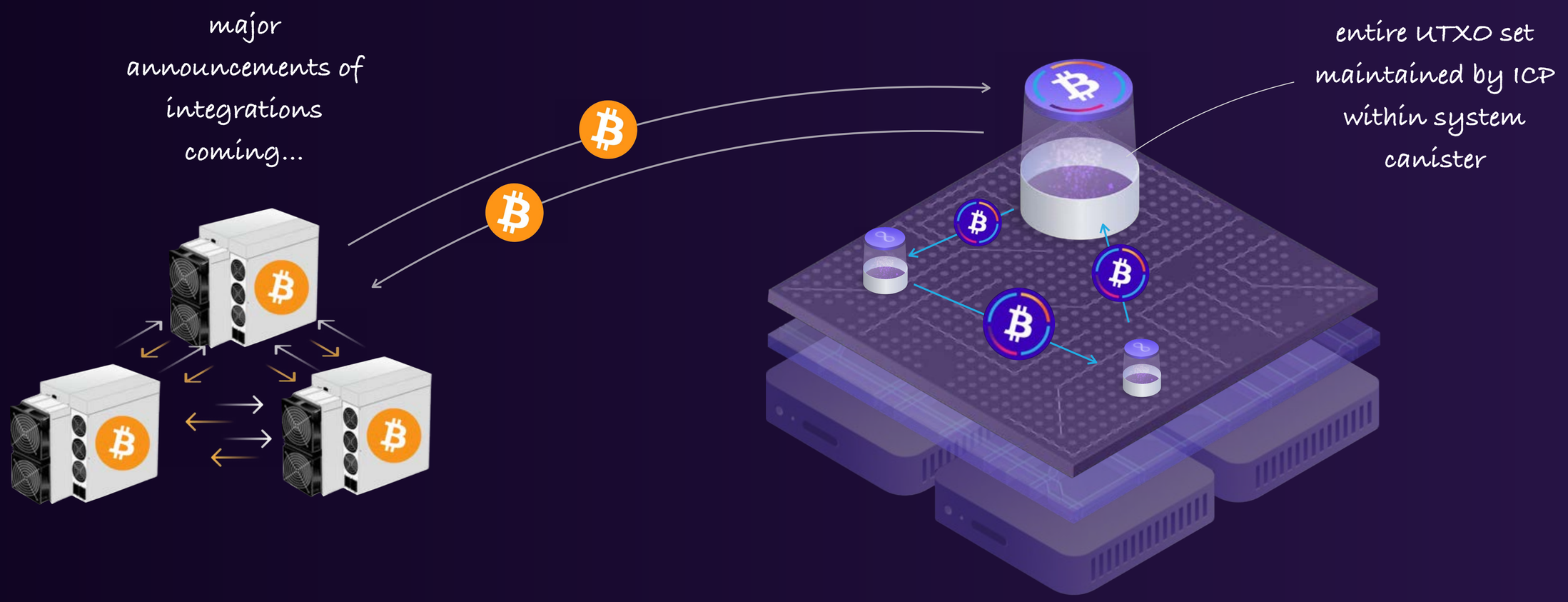
canisters create accounts and sign TXs on other blockchains



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

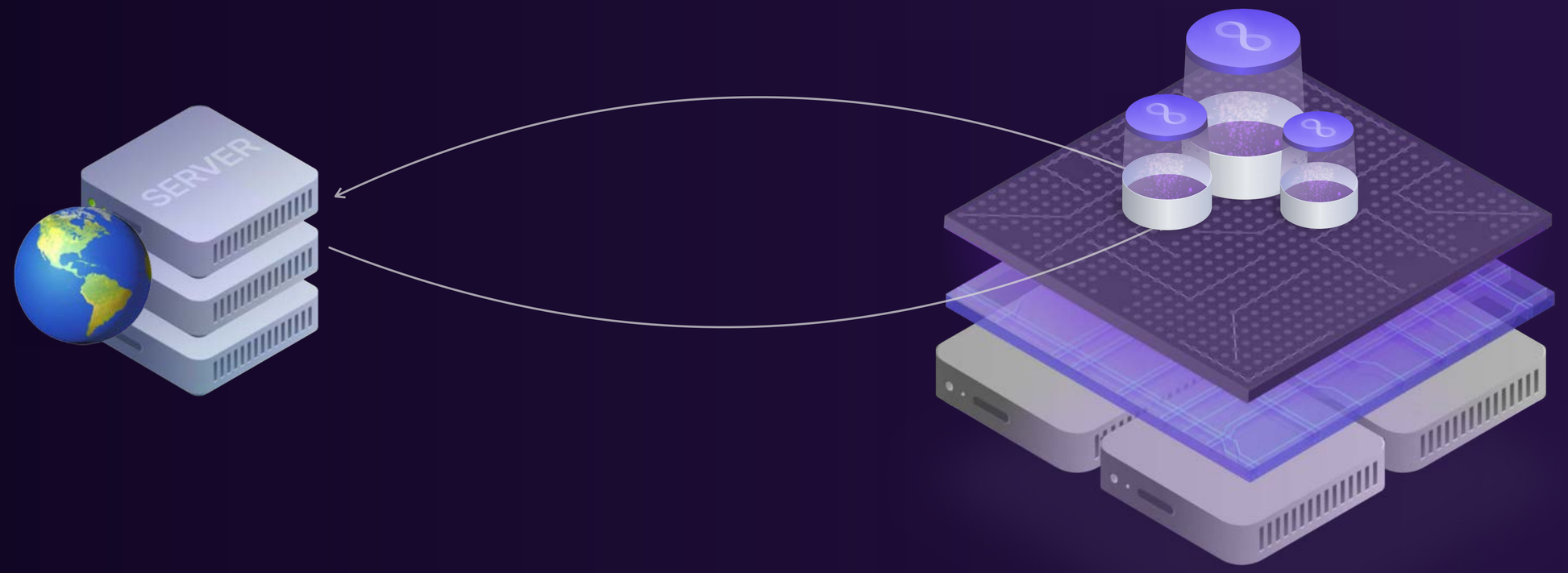


chain-key bitcoin supports usage of bitcoin in DeFi, social media, games, the metaverse with 1s finality

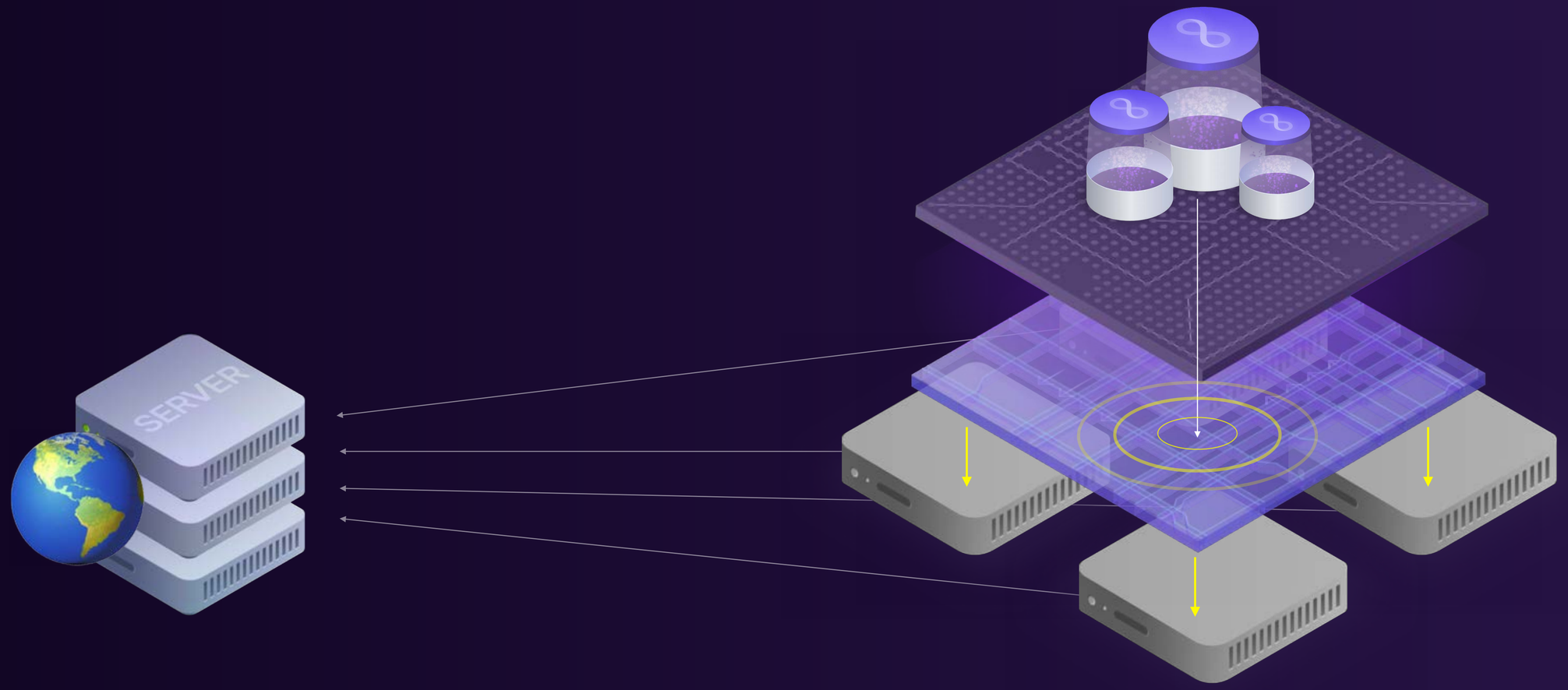
web2+3

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

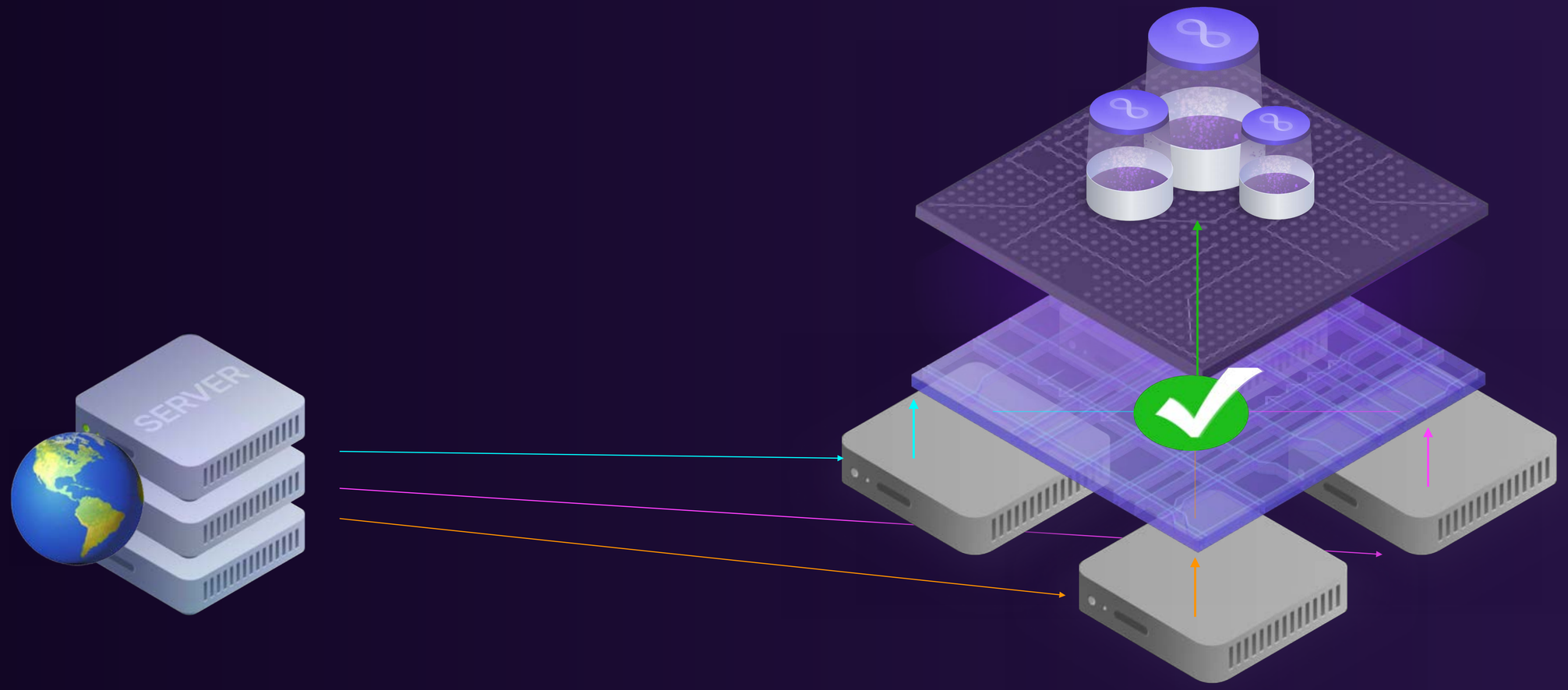
1. a canister initiates a call to a web2 service



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

organic Internet Computer network activity is substantial

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 🇨🇭

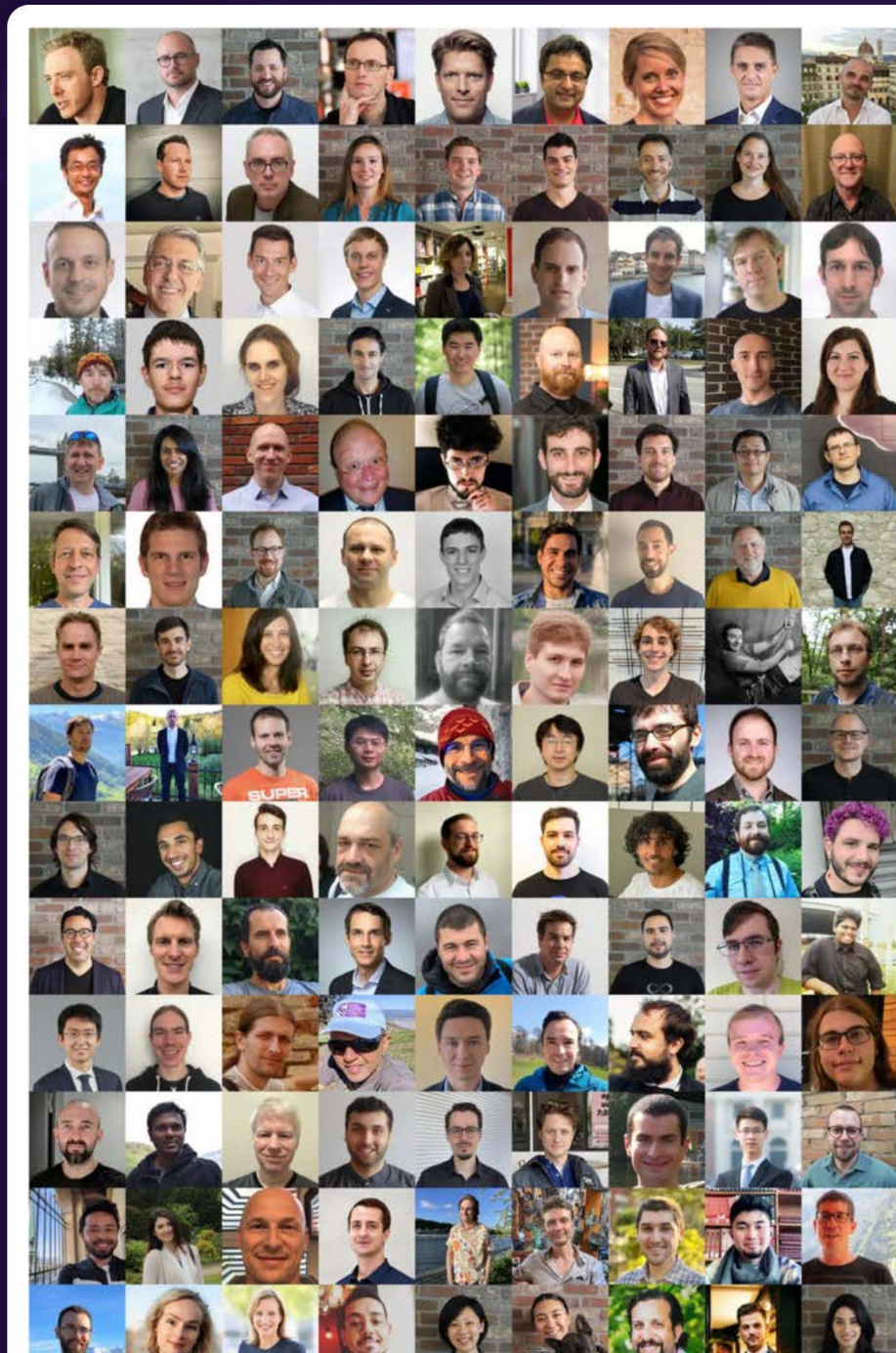
- emerged from early Ethereum community in 2015
- DFINITY Foundation established October 2016
- Swiss not-for-profit foundation, not a corporation
- world's largest team of cryptographers
- over 140 employees in Zürich HQ
- 270+ team members globally

1600+
research papers

100 000+
academic citations

250+
technical patents

Early Crypto Community + 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