Decentralization

OPTIMUM

Prof. Muriel Medard

Co-Founder and CEO

MIT NEC Chair for Software Science and Engineering

EECS

Why decentralization?

Plus:

    No single control point
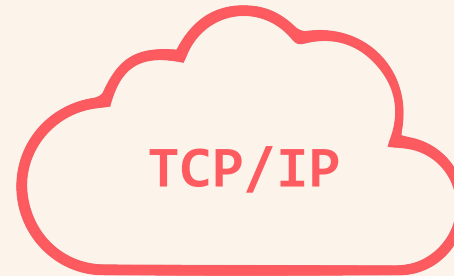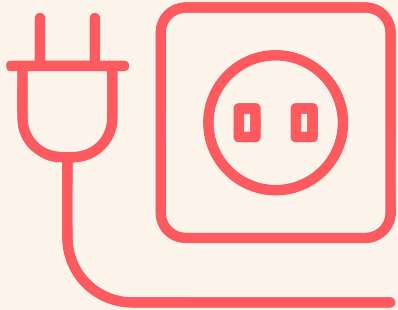
    Make use of all resources

Difficulty:

    Create a system that is reliable

    Create the consistency of a centralized system in the context of a decentralized one.

What makes a decentralized network successful?

Electric grid: **socket** for plugging in.   Web1 and Web2: transport TCP/IP or UDP **socket**
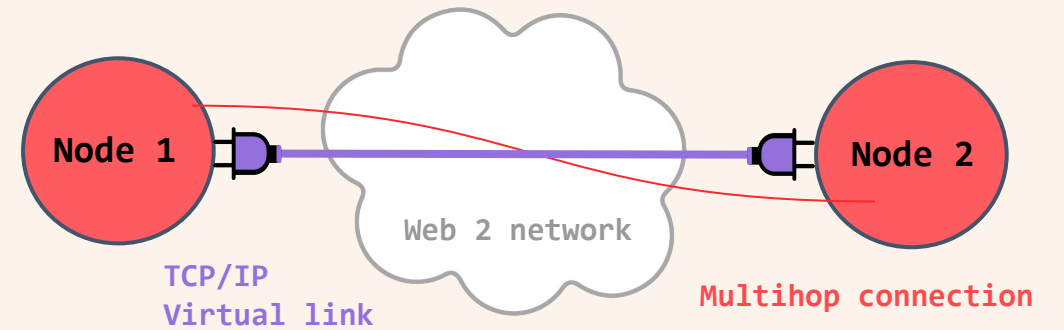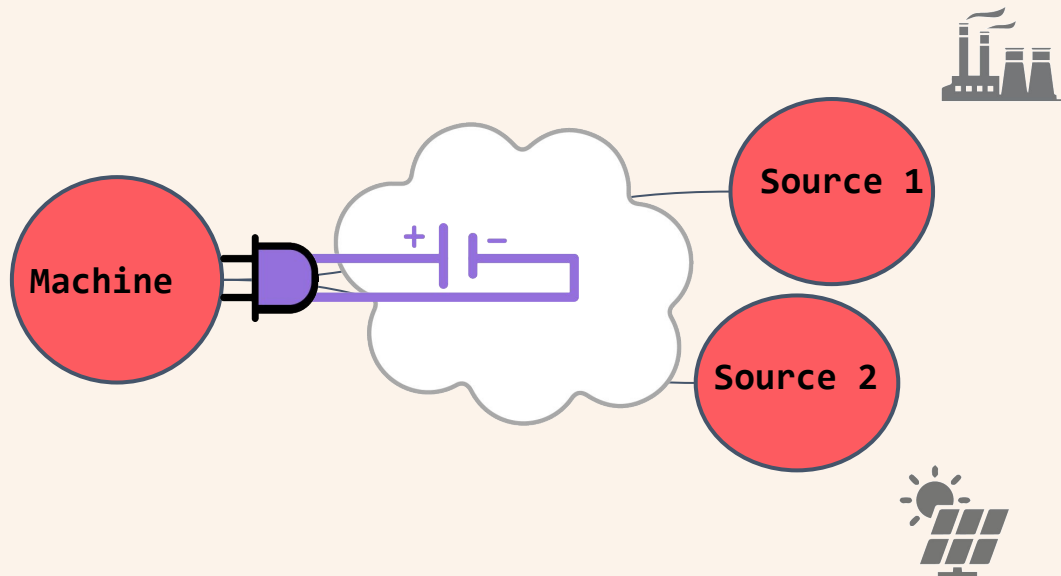
What is a socket?

An **abstraction** that makes a network look like a dedicated resource

Electric grid: **dedicated battery**

Web1 and Web2: **dedicated link**

Machine

Source 1

Source 2

Node 1

Node 2

Web 2 network

TCP/IP
Virtual link

Multihop connection
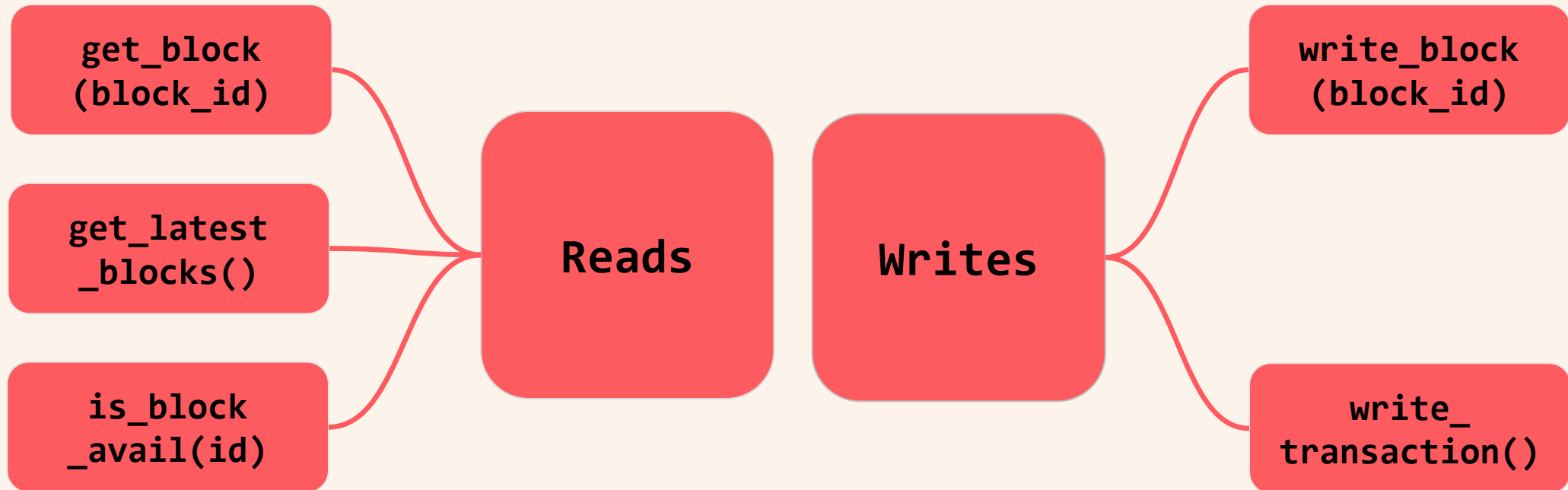
What abstraction for Web3?

The **Optimum Data Socket (ODS) emulates memory read/write access in a dedicated machine** in a permissionless, decentralized system.
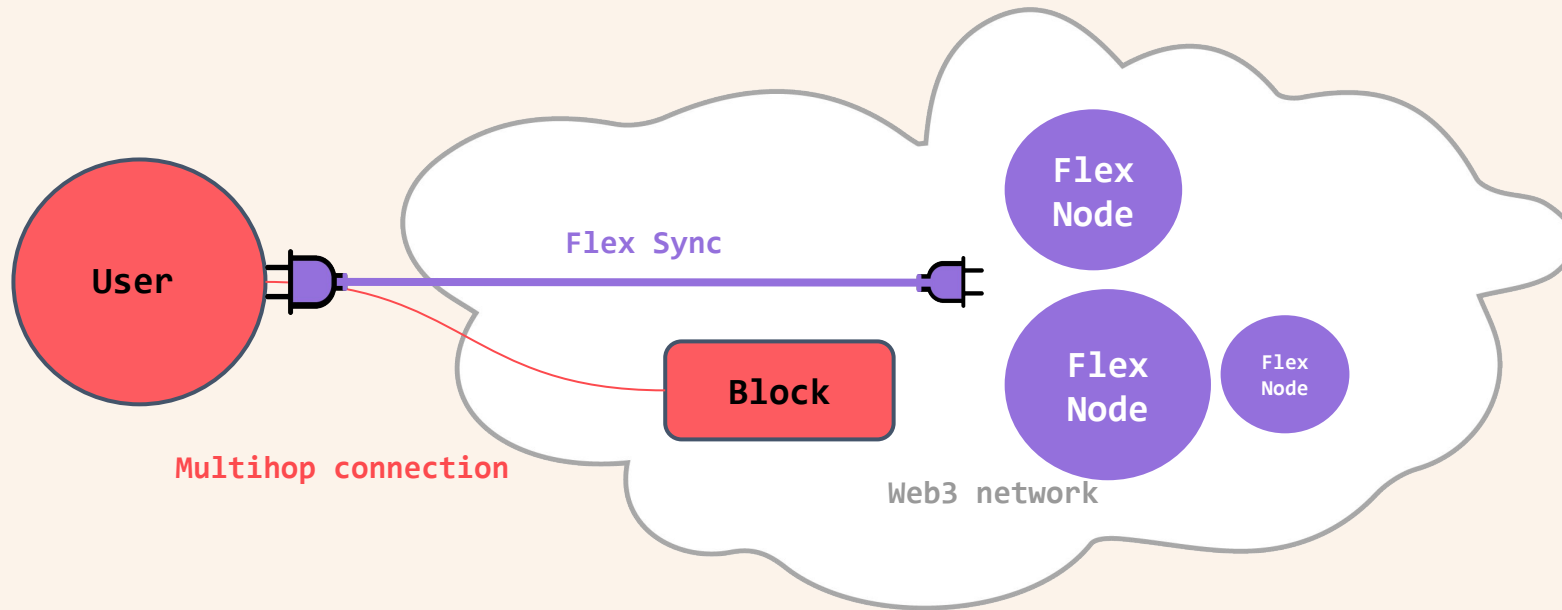
Optimum Data Socket Calls

Networking x Storage

Elementary calls to and from memory in a machine.

What is memory access in a dedicated computer?

- Data reads and writes as on a **single dedicated computer memory: Atomicity**
- **Dedicated data bus** in our computer, correct read/write ordering: **Consistency**
- **Data is reliably maintained** in our computer, despite crashes: **Durability**

This is the principle of Atomicity, Consistency, Durability (ACD)

https://en.wikipedia.org/wiki/ACID

Attiya, H., Bar-Noy, A., and Dolev, D. Sharing memory robustly in message passing systems. *Journal of the ACM 42(1)* (1996), 124–142

Cadambe, V. R., Lynch, N., Médard, M., and Musial, P. A coded shared atomic memory algorithm for message passing architectures. In *Network Computing and Applications (NCA), IEEE 13th International Symposium on* (2014), pp. 253–260

Dutta, P., Guerraoui, R., and Levy, R. R. Optimistic erasure-coded distributed storage. In *DISC '08: Proceedings of the 22nd international symposium on Distributed Computing* (Berlin, Heidelberg), Springer-Verlag, pp. 182–196.

RLNC

Sharding

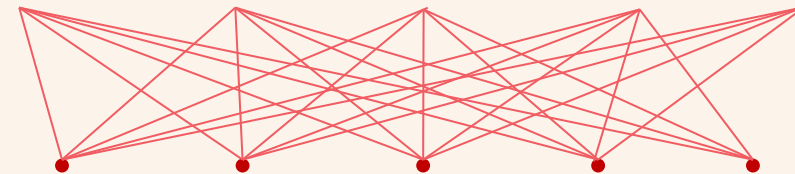**Coding**

Shards:
duplication/ missing pieces
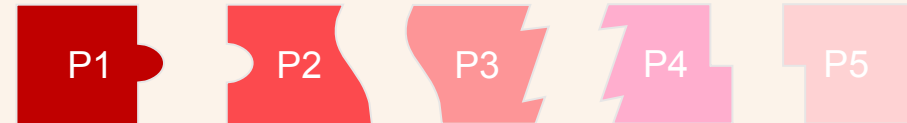
Albebraic mixtures from pieces

RLNC only: composability

Code: Any 5 mixtures will do

Ho, T., Medard, M., Koetter, R., Karger, D., Effros, M., Shi, J.,and Leong, B. A Random Linear Network Coding Approach to Multicast. In *IEEE Transactions on Information Theory*, 52:10 (2006), pp. 4413–4430

Durability

Blocks/
transactions

Blocks/
transactions

Stored in nodes →

**Nodes
randomly
down**

How durable?

ABDRASHITOV, V. and MEDARD, M., Durable Network Coded Distributed Storage, *Allerton 2015*
ABDRASHITOV, V. and MEDARD, M., Staying Alive - Network Coding for Data Persistence in Volatile Networks, *IEEE Asilomar 2016*

Current Infra

NO_CODING with POST_RECODING strategy_round_1

Optimum

NETWORK_CODING with POST_RECODING strategy_round_1

Reliability

Storage / Memory

Bandwidth

Resources (memory, bandwidth)

Fitzek, F., Toth, T., Szabados, A., Pedersen, M., Lucani, D., Sipos, M., Charaf, H., and Medard, M., Implementation and Performance Evaluation of Distributed Cloud Storage Solutions using Random Linear Network Coding, *IEEE CoCoNet (*2014)

Goal: keep data alive at low cost

	When reliability below 1, failure	Cost implication
Current Infra	Dies at round 27	Keep increasing
Optimum	Survive practically forever at low cost	Constant over time

Optimum

OPTIMUM

Turning Web3 into a truly decentralized machine built on top of network coding

- **ODS** ensures ACD

- **FlexNodes** ensure optimum use of memory and bandwidth

Creating ODS

Need to emulate abstraction while allowing permissionless operation

A few replication-based algorithms provide ACD and reconfiguration

Problem is **cost**:

- Replication cost
- Bandwidth cost
- Delay from keeping state

Use **random linear network coding (RLNC)** to:

- Make **Optimum** use of storage
- Make **Optimum** use of bandwidth
- **Remove** state dependency

Then instantiate an ACD algorithm using coding

AGUILERA, M. K., KEIDAR, I., MALKHI, D., AND SHRAER, A. Dynamic atomic storage without consensus. In *Proceedings of the 28th ACM symposium on Principles of distributed computing (PODC '09)* (New York, NY, USA), ACM, pp. 17–25
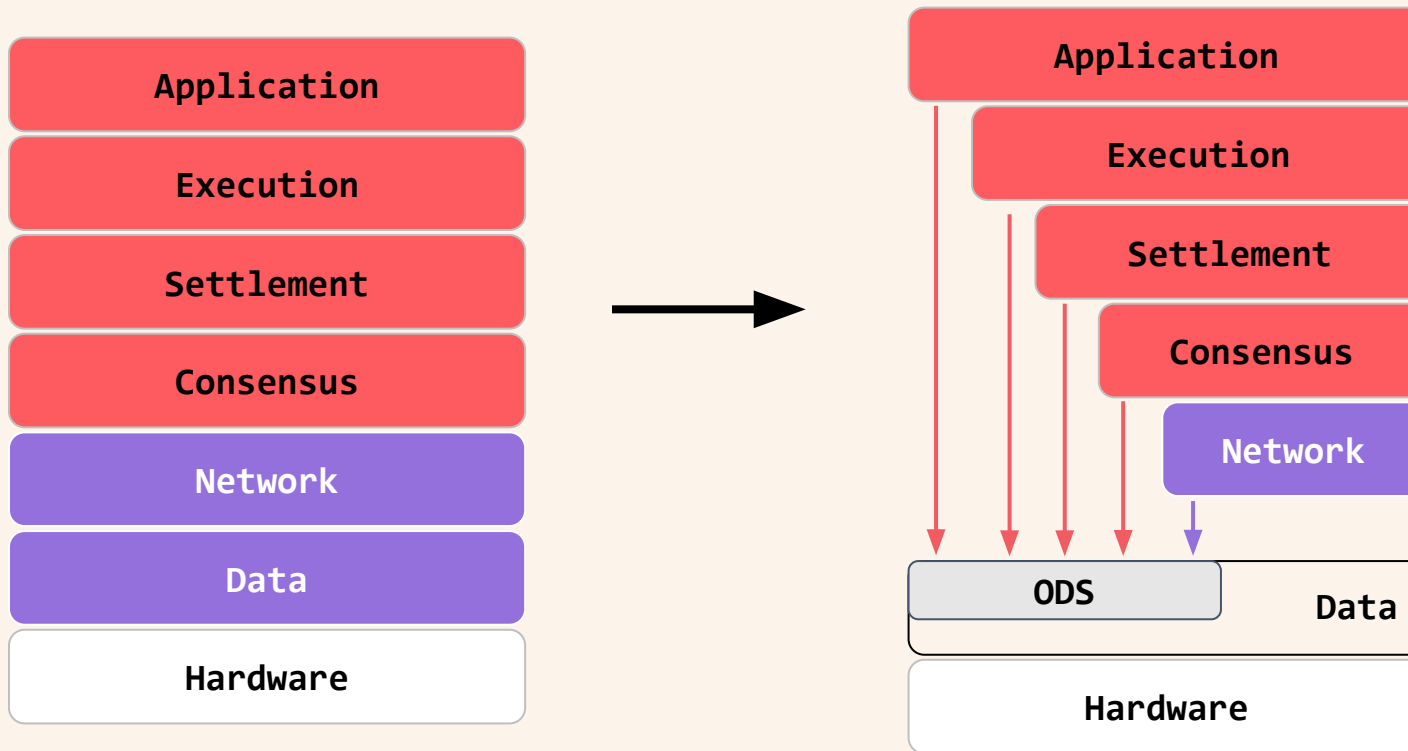
JEHL, L., VITENBERG, R., AND MELING, H. Smartmerge: A new approach to reconfiguration for atomic storage. In *International Symposium on Distributed Computing* (2015), Springer, pp. 154–169

GILBERT, S., LYNCH, N., AND SHVARTSMAN, A. RAMBO II: Rapidly reconfigurable atomic memory for dynamic networks. In *Proceedings of International Conference on Dependable Systems and Networks (DSN)* (2003), pp. 259–268
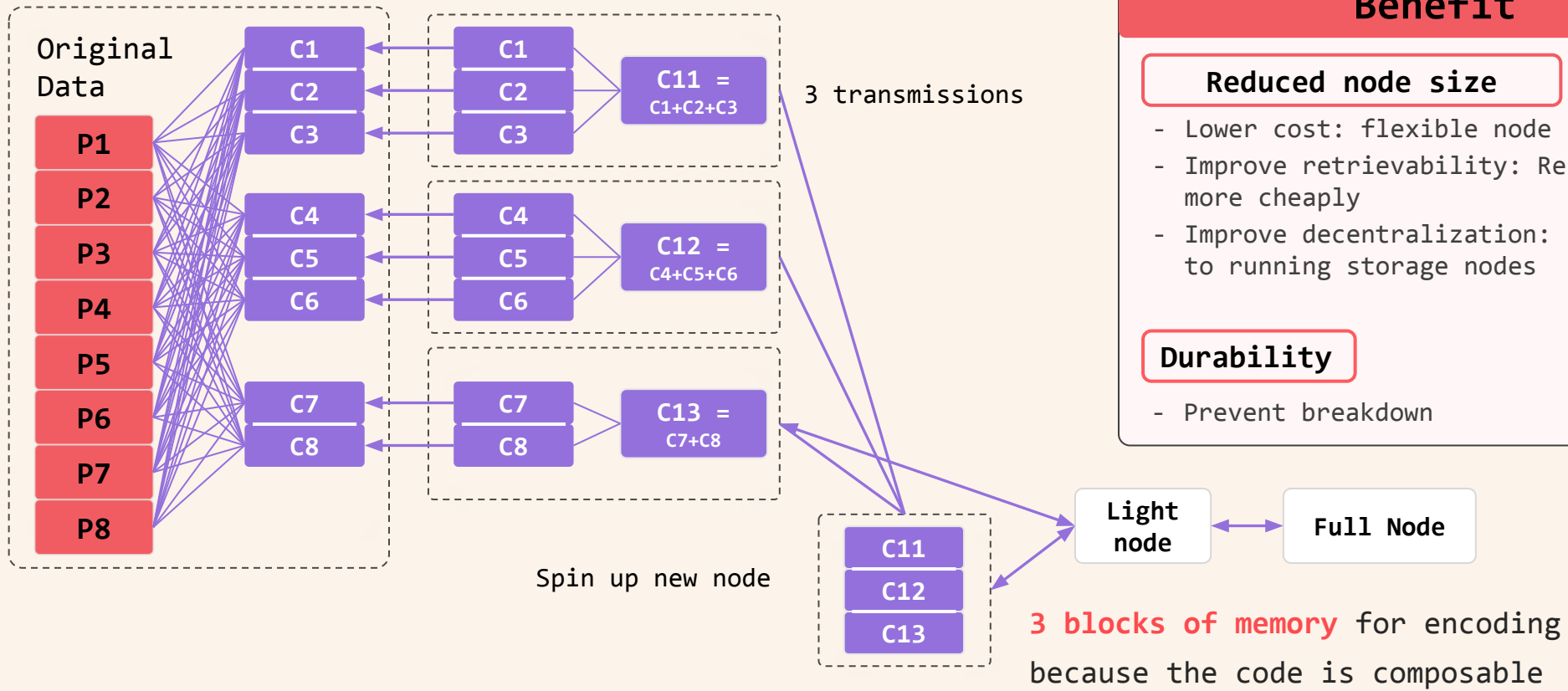
NICOLAOU, N., CADAMBE, V., PRAKASH, N., TRIGEORGI, A., KONWAR, K., MEDARD, M., AND LYNCH, N. ARES: Adaptive, Reconfigurable, Erasure coded Atomic Storage. *ACM Transactions on Storage* (2022).

Optimum Data Socket

Web3

OPTIMUM

$11M seed round led by 1k(x)

Institutional investors:

SPARTAN · CMT DIGITAL · Robot Ventures · Kraken VENTURES · LONG HASH VENTURES · CMS · SNZ CONNECT TO EMPOWER · CALADAN · MAPLEBLOCK · DEEP VENTURES

GSR · BIG BRAIN HOLDINGS · Finality CAPITAL PARTNERS · BLOCKDAEMON · OAK GROVE VENTURES · CHORUS ONE · NGC Ventures · Reforge · animoca VENTURES · M·H VENTURES · PANGA CAPITAL · RockX

Individual investors:

Name	Role	Affiliation
Saurabh Sharma	GP	jump_
Gracy Chen	CEO	Bitget
Yi Sun	Co-founder	AXIOM
Daniel Wang	Co-founder CEO	Aethir
Abhijeet Mahagaonkar	CTO	POLYCHAIN
Jayant Krishnamurthy	CTO	PYTH
Michael Cahill	CEO	PYTH
Sandeep Nailwal	Co-founder	polygon / Symbolic Capital
Bruno Faviero	Co-founder CEO	magna
Sankha Banerjee	Chief Economist	Babylon
Kevin Ding	GP	DHVC
Brecht Devos	Co-founder CTO	taiko
Tal Tchwella	Head of Product	SOLANA
Nabeel Qadri	Managing Partner	3·0 THREE POINT CAPITAL
Claire Arthurs Kart	CMO	Aztec

Name	Role	Affiliation
Michael Tong	Co-founder CEO	xterio
Eugene Ng	Founding Partner	DWF LABS
Tiancheng Xie	Co-founder CTO	Polyhedra
Rand Hindi	Co-founder CEO	ZAMA
Yaoqi Jia	Founder	AltLayer
Ismael Hishon-Rezaizadeh	Co-founder CEO	lagrange
Anuj Shankar	CEO	Luganodes
Zaki Manian	Co-founder	COSMOS
Arthur Cheong	Founder CEO	DeFiance Capital
Bochuan Du	Co-founder	Polymer
Richard Ma	CEO	Quantstamp / Zircuit
Benjamin Fisch	Co-founder CEO	Espresso
Robinson Burkey	Co-founder CCO	WORMHOLE
Gideon Daitz	Partner	3·0 THREE POINT CAPITAL

Why decentralization for Science?

Plus:

    Multiple data sets across the world, particularly for machine learning (ML)

    Make use of all resources for computation

Difficulty:

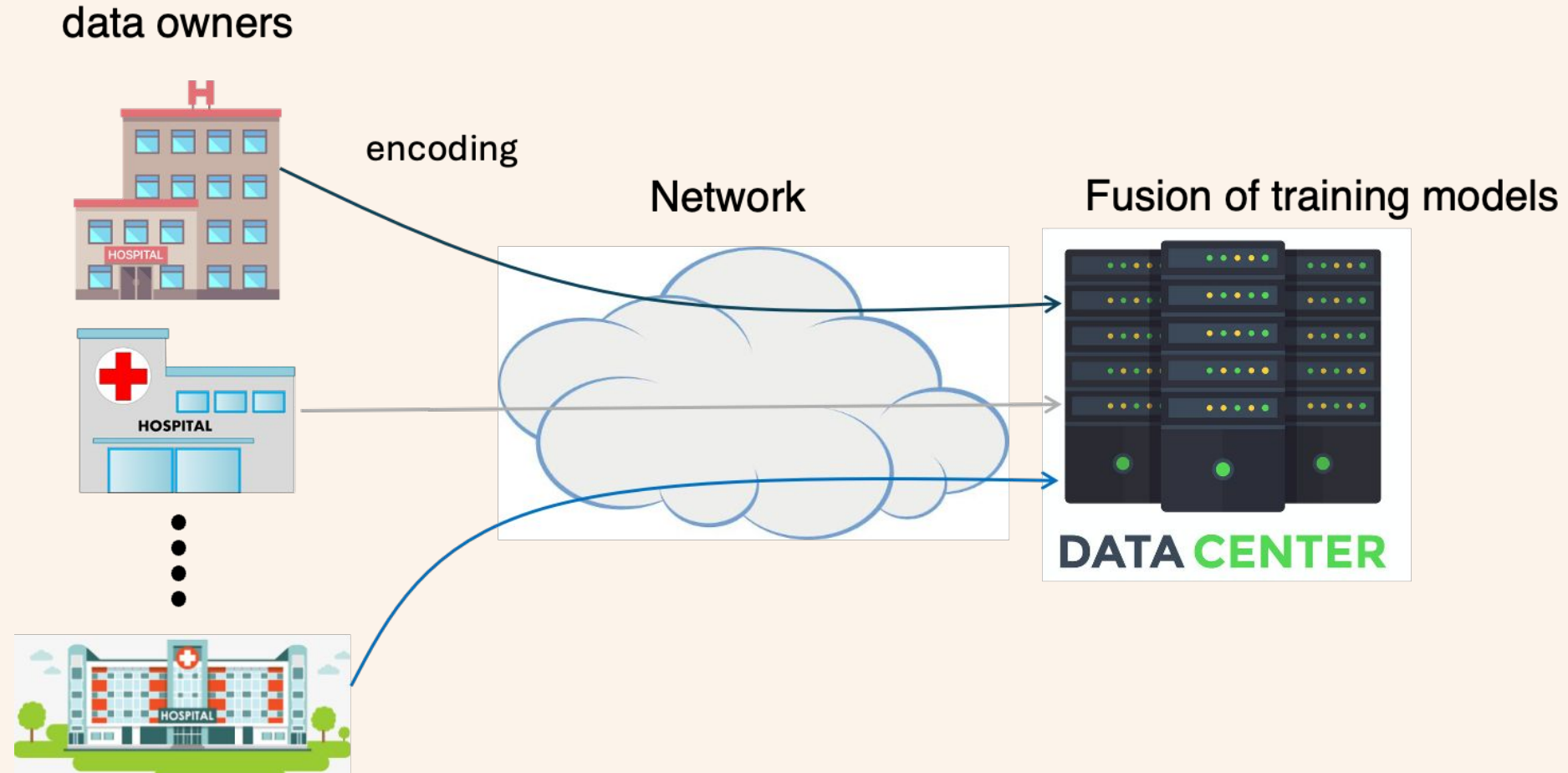   Create a system that is reliable

    Privacy concerns for data that is regulated or proprietary

    Ensuring accuracy of computation

    Create the consistency of a centralized system in the context of a decentralized one
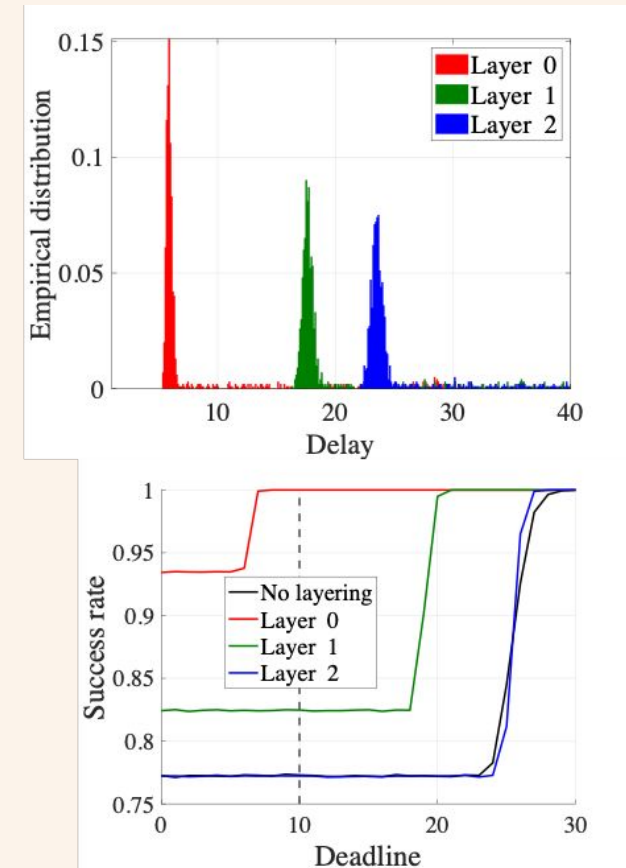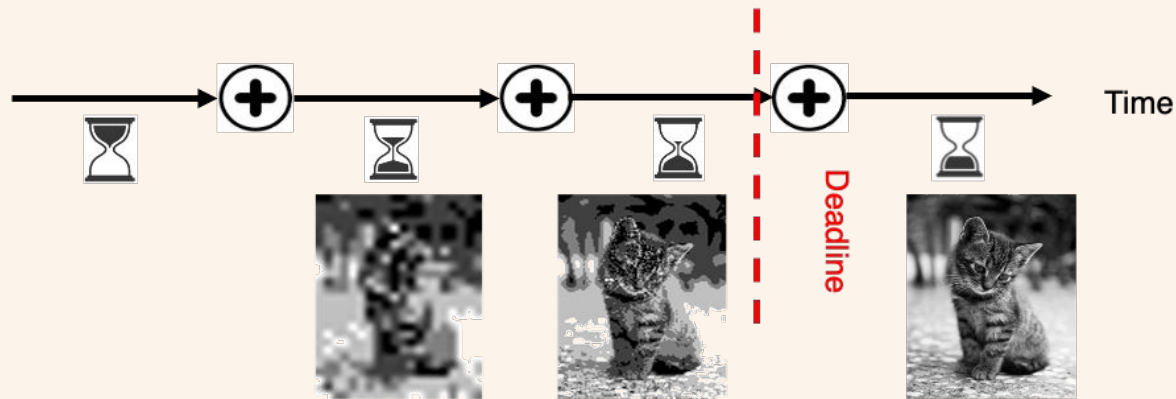
In computation often decentralization is difficult and the first step is distribution

Learning from decentralized data

data owners

encoding

Network

Fusion of training models

HOSPITAL
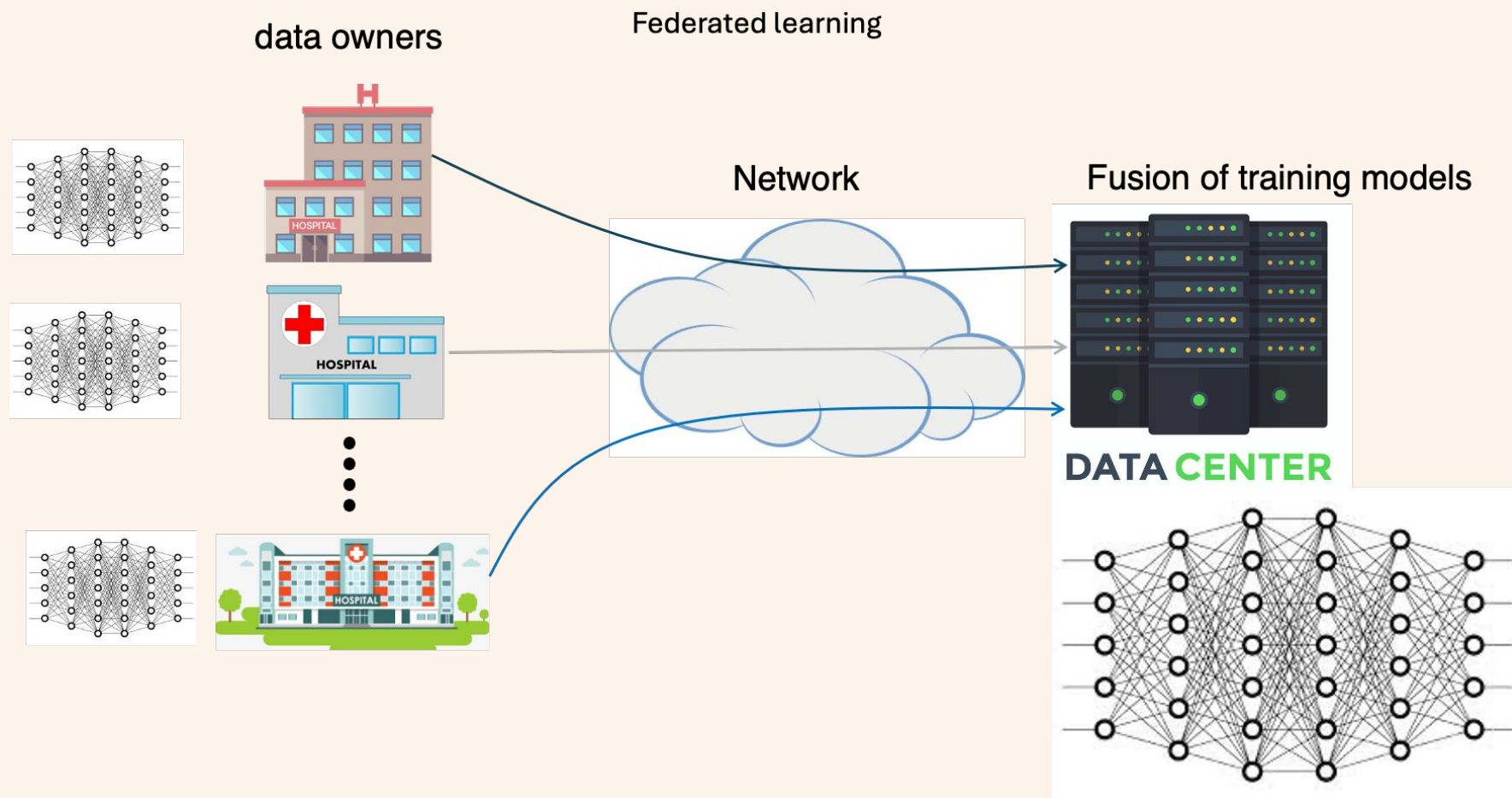
HOSPITAL

HOSPITAL

DATA CENTER

Theoretically not inefficient.

Learning from decentralized data - deadlines

Coarser approximations are released at earlier stages than the full resolution

H. Esfahanizadeh, A. Cohen, M. Médard, and S. Shamai, "Distributed computations with layered resolution," *IEEE Cloudnet* 2022.

Federated learning -distributed

data owners

Federated learning

Network

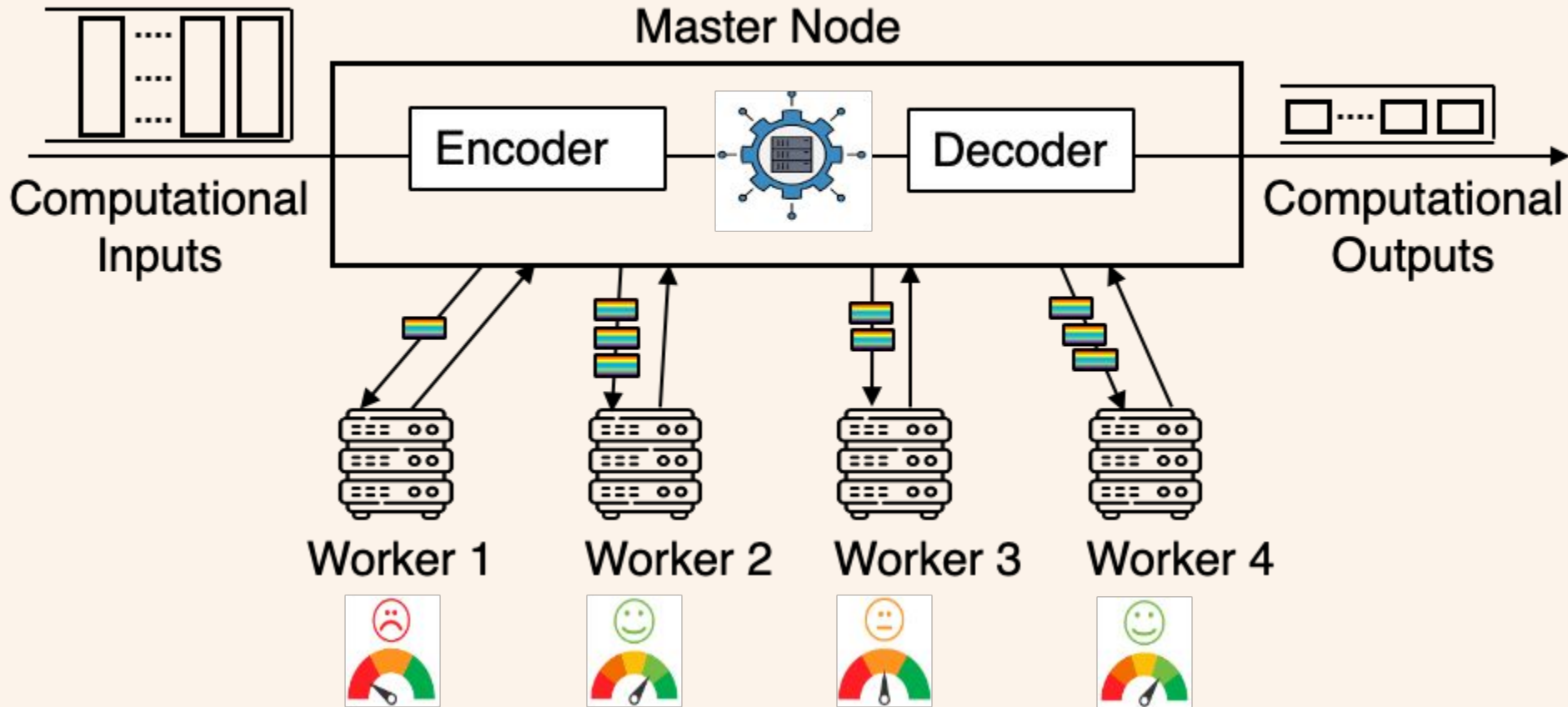Fusion of training models

DATA CENTER

Federated learning -distributed

Use underlying redundancy both in data and functions, and recover a sparse representation
Entropic surjectivity of a function is how well it can be compressed

(a) Physical topology of the network

(b) Function Manager

(c) Logical topology of workload distribution

D. Malak, A. Cohen and M. Médard, "How to Distribute Computation in Networks," *IEEE INFOCOM 2022*
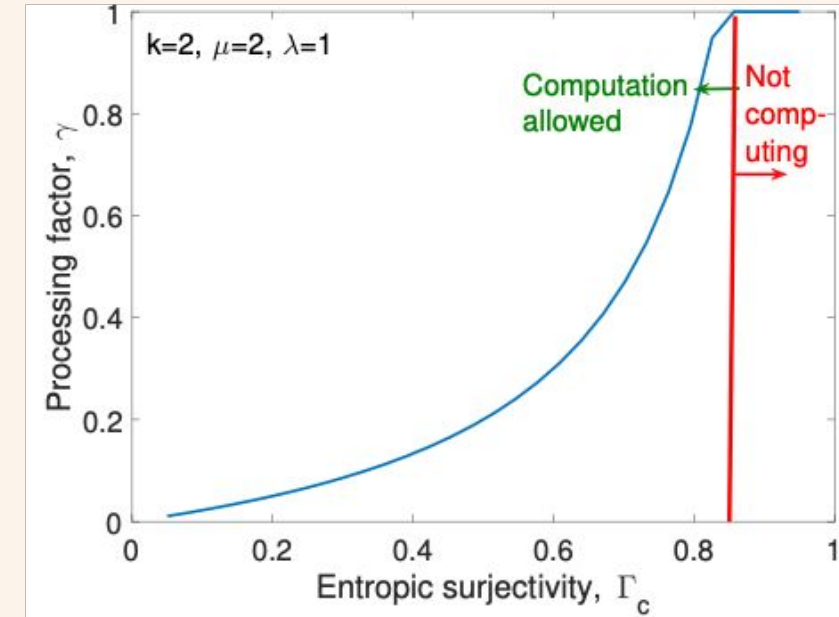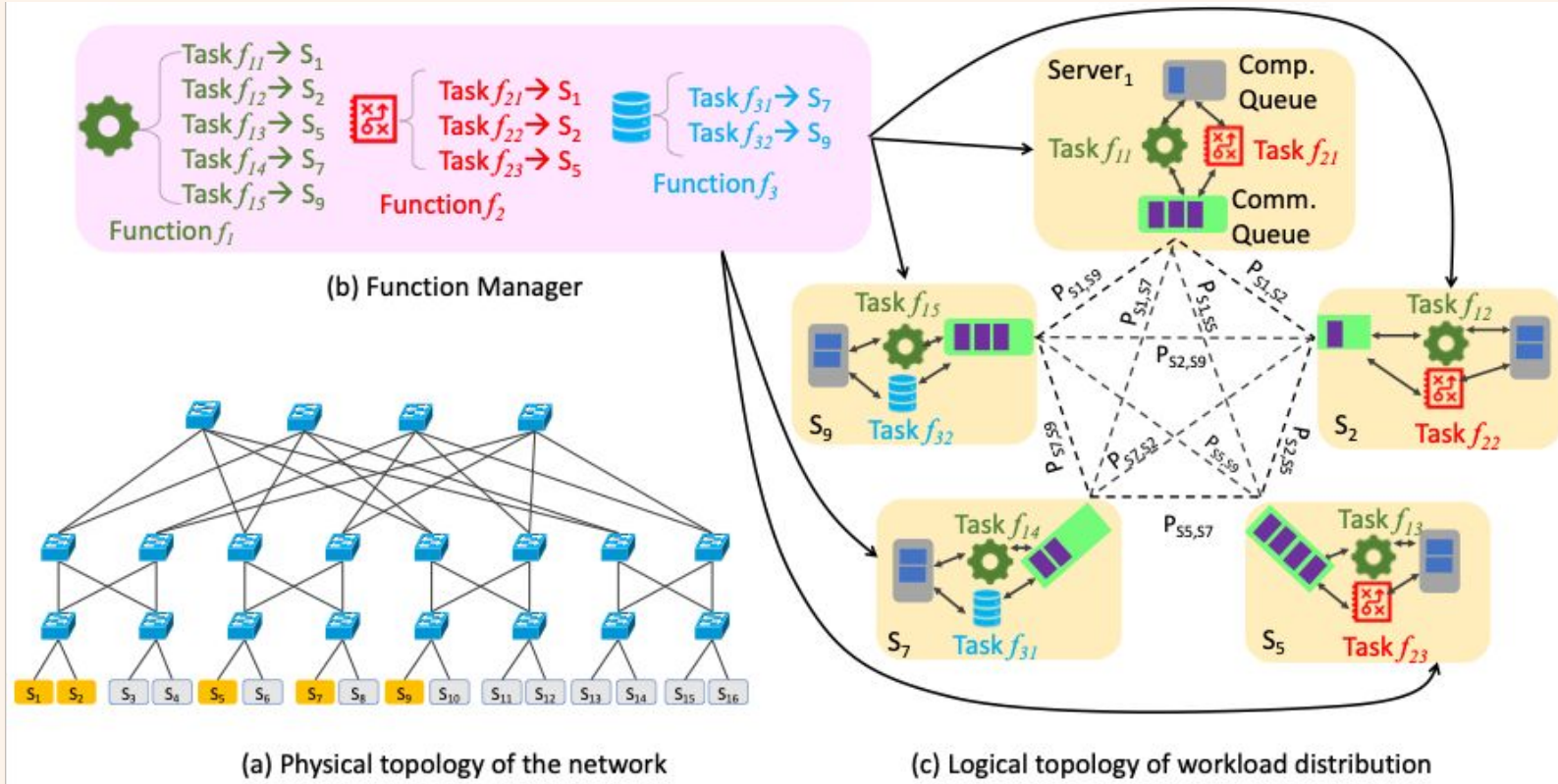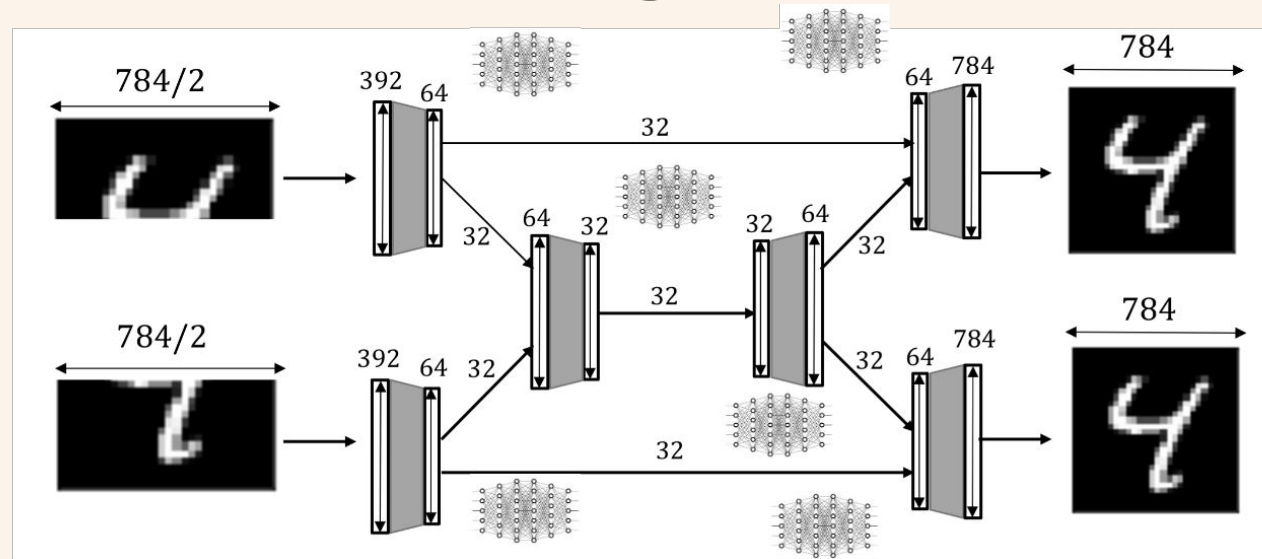
Federated learning - online coded distributed

Distribution Matching: Scheduling to match distribution of response time of workers to their coded assignment

H. Esfahanizadeh, A. Cohen, and M. Médard, "Stream iterative distributed coded computing for learning applications in heterogeneous systems," *IEEE Infocom* 2022.
A. Cohen, G. Thiran, H. Esfahanizadeh and M. Médard, "Stream distributed coded computing," *IEEE JSAIT* 2021
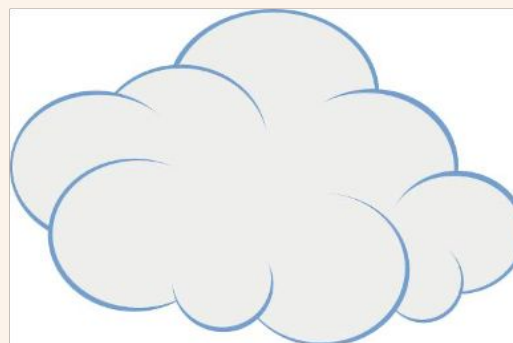
Decentralized learning
- neural network coding

L. Liu, A. Solomon, S. Salamatian and M. Médard, "Neural Network Coding," *in* Machine Learning and Wireless Communications 2022, also ICC 2022
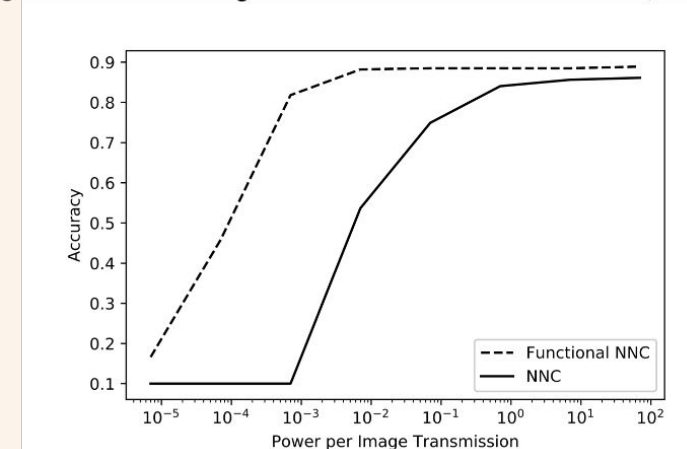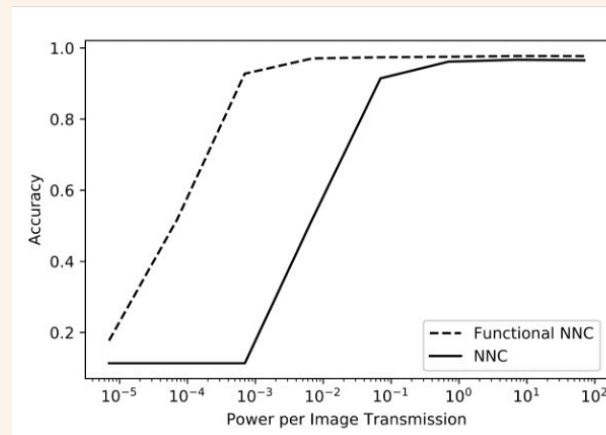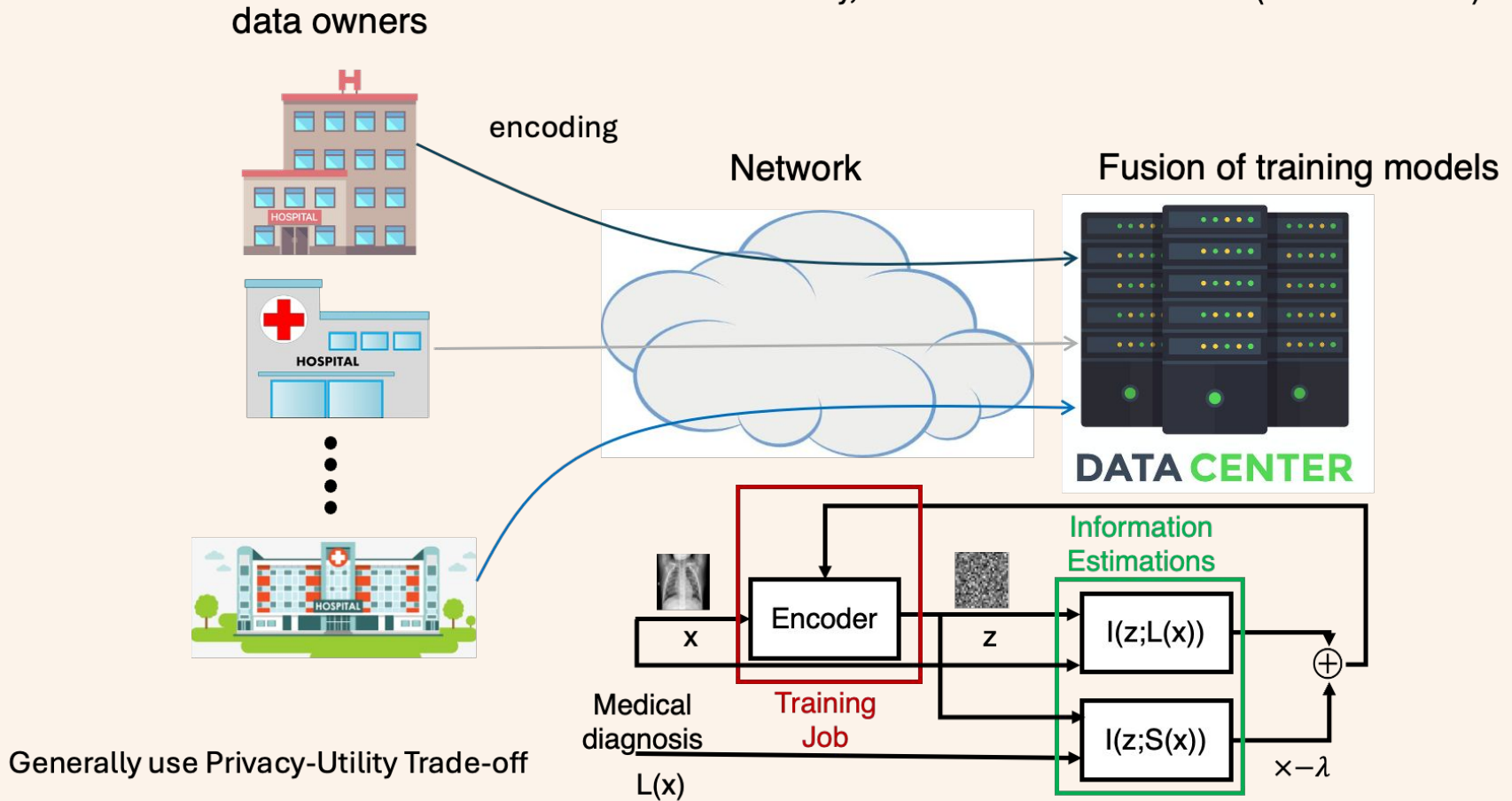
Privacy

Alice (Data-Owner)

Bob (ML Developer)

Eve (Adversary)

Privacy

Proposals for using Fully Homomorphic Encryption –

Costly, still leaks some information (see Salsa work)

data owners

encoding

Network

Fusion of training models

DATA CENTER

Information Estimations

Encoder

x

z

$I(z;L(x))$

$I(z;S(x))$

Medical diagnosis

Training Job

$L(x)$

$\times - \lambda$

Generally use Privacy-Utility Trade-off

H. Esfahanizadeh W. Wu, M. Ghobadi, R. Barzilay, M. Medard, "InfoShape: Task-based neural data shaping via mutual information," *IEEE ICASSP* 2023.

Privacy

Protection Against Re-Identification Attacks
To evaluate the privacy of an encoding scheme, we propose a guesswork-based framework, which identifies the number of attacker guesses required to re-identify a single image.
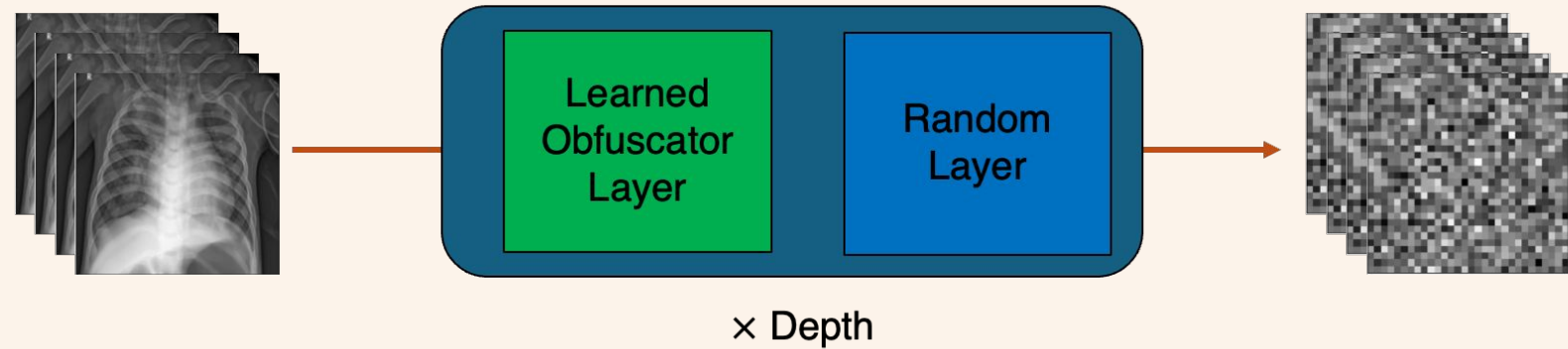
× Depth

H. Esfahanizadeh, W. Wu, M. Ghobadi, R. Barzilay, M. Medard, "InfoShape: Task-based neural data shaping via mutual information," *IEEE ICA*2023.

How Successful? How many guesses
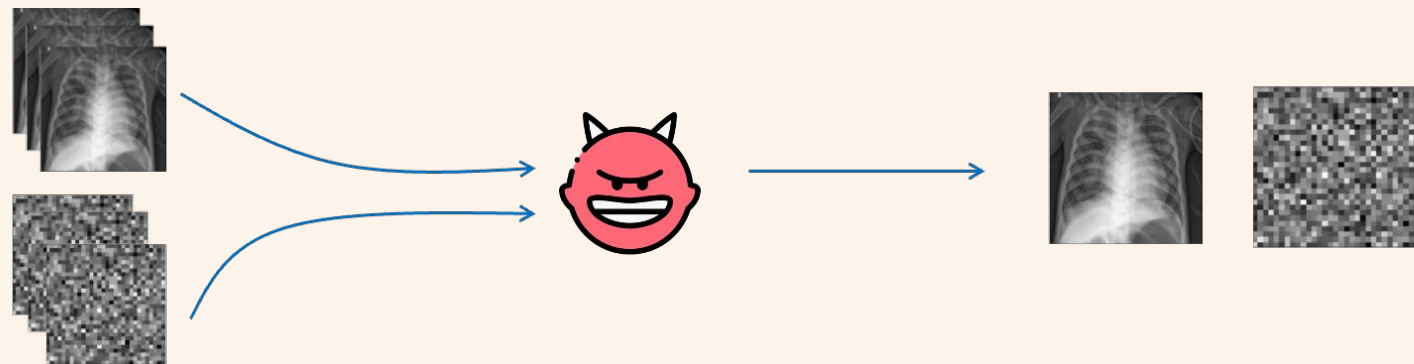
H. Esfahanizadeh W. Wu, M. Ghobadi, R. Barzilay, M. Medard, "InfoShape: Task-based neural data shaping via mutual information," *IEEE ICASSP* 2023.
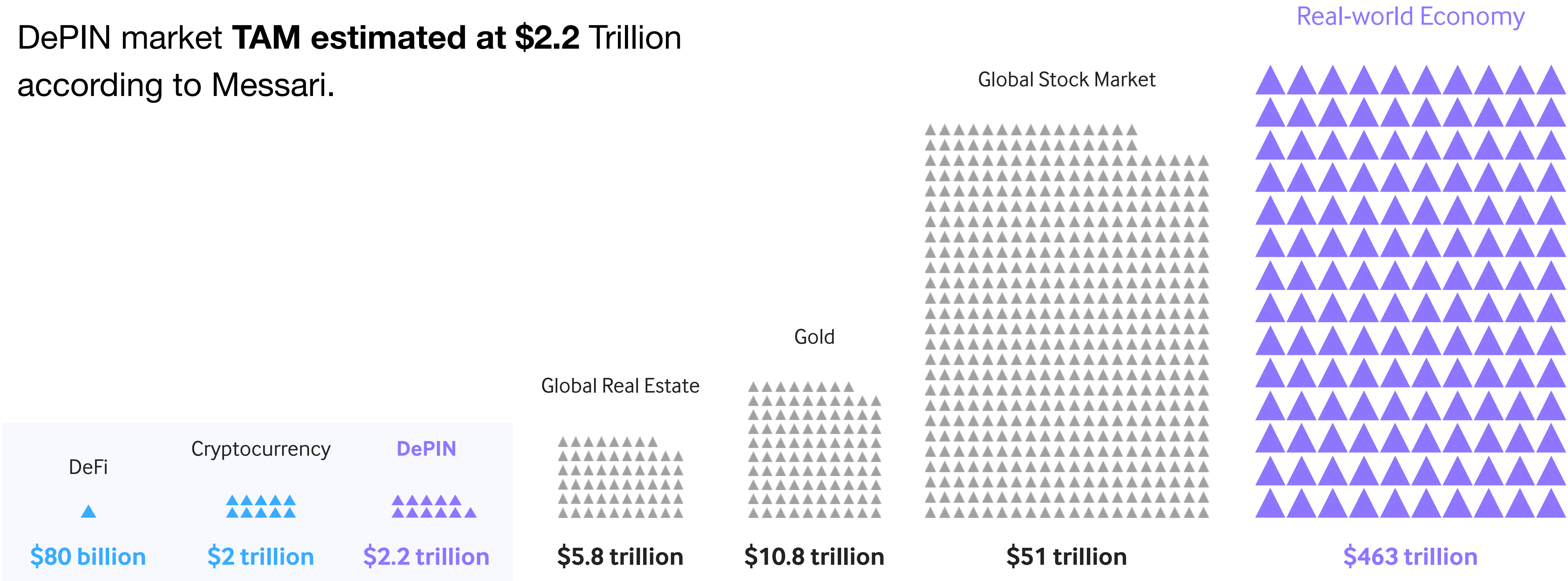
IoTeX 2.0

Modular Infra For DePIN

DePIN
Built on
IoTeX

IoTeX 2.0: Modular Infra Connecting DePIN to Web3

IoTeX L1

DePIN Infra Modules (DIM) Layer

DePIN Dapps & L2s
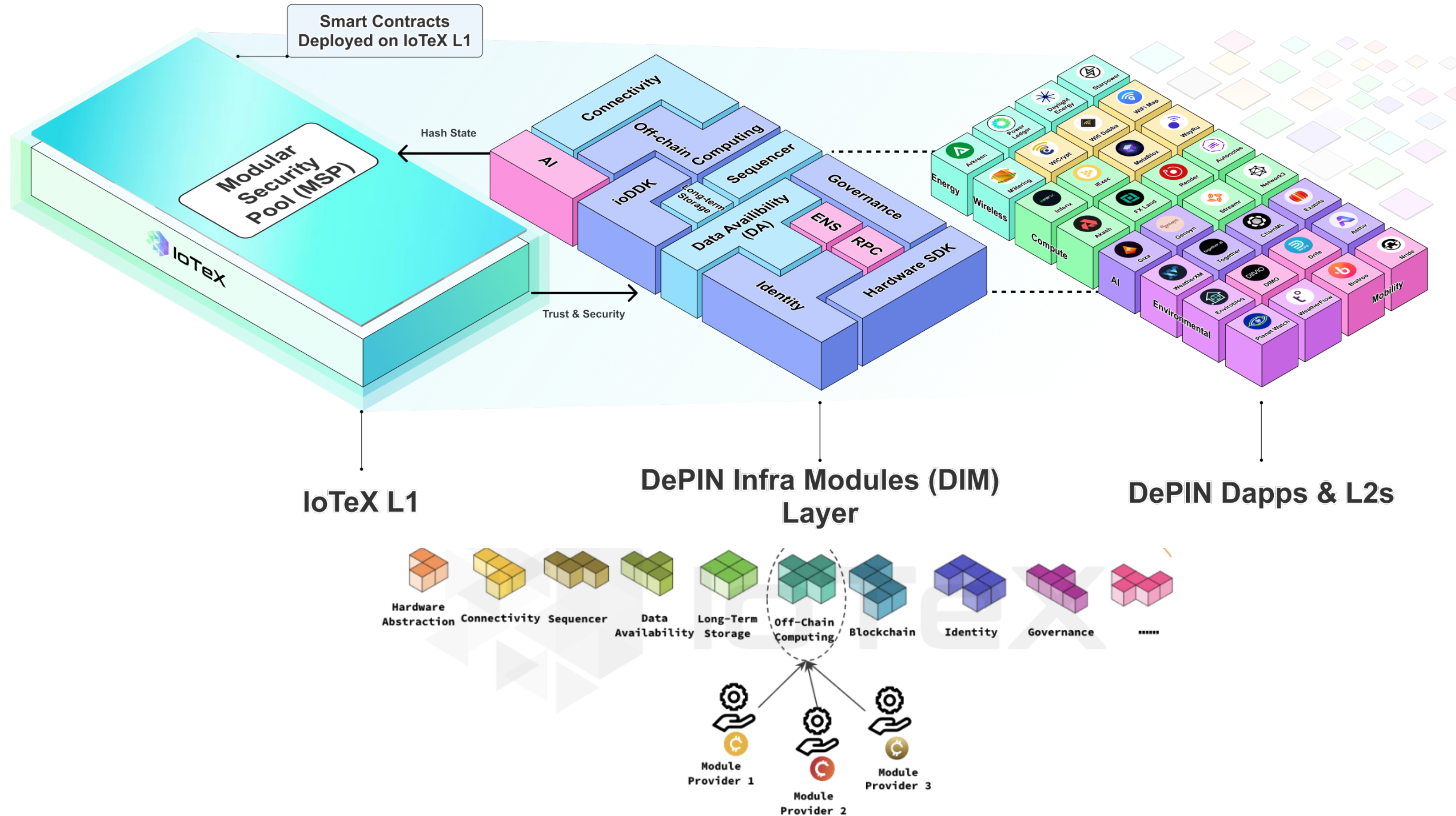
iotex.io | @iotex_io

The Blossoming DePIN Ecosystem on IoTeX

IoTeX is now the third-largest DePIN ecosystem with 50+ DePIN projects utilizing IoTeX's modular tech stack.

Where DePIN Projects are Building On
DePIN Projects by chain (2024)

Number of DePIN Projects

- Solana: 78
- Ethereum: 74
- IoTeX: 51
- Peaq: 31
- Polygon: 29
- Binance: 15
- Arbitrum: 14
- Cosmos: 12

Source: Messari, DePIN Ninja, DePIN Hub, DePIN Scanner

Messari | Data as of Aug 1, 2024
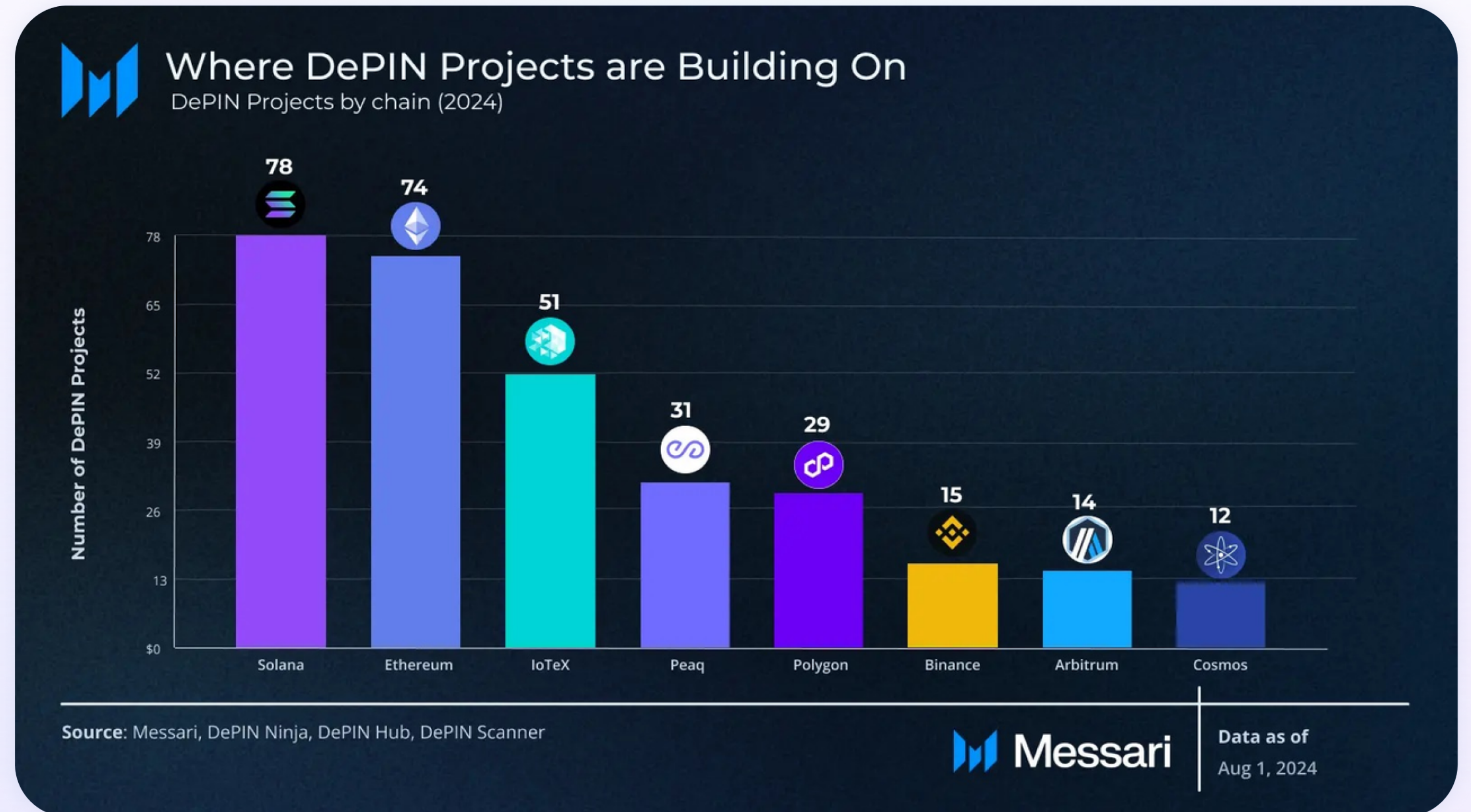
IoTeX DePIN Projects: Progress & Highlights

IoTeX

Network3
- Raised $5.5M from top VCs, incl. Borderless, EV3, SNZ
- V1 Node sale sold out in minutes
- Local LLM for AI on smart devices

Nubila
- Raised $2.5M from top VCs, incl. BCG, FMG, SNZ, OrangeDAO
- Pre-orders open for Marco device
- Acquired Bloomsky (weather HW)

Wayru
- Genesis hotspot sale sold out
- Pre-sale for next-gen WiFi miners coming in October
- Ongoing device minting on IoTeX

Inferix
- Public node sale is now live
- Proof of Rendering (PoR) demo released for verifiable compute
- New whitepaper released

Powerpod
- Launched RWA NFTs on IoTeX in partnership with Mamator
- 2,750 devices across 4 countries, live on DePINscan

EnviroBloq
- New smart home monitoring device launching soon via Seeed Studio
- Pebble Tracker sales opened to US customers with included SIM card

Scannit
- Raised $1.5M in private funding round
- Open beta of v1 Dapp released during Token2049 in Singapore

Qualoo
- New whitepaper released for global internet diagnostics via DePIN
- Waitlist opened for fixed nodes and mobile app access

WatchX
- Pre-orders of WatchX Founder and Fusion wearables are open
- Integration with ioID is ongoing
- 500 genesis NFTs sold on IoTeX

Innovex
- Node sale is now open with multiple tiers for miners of all levels
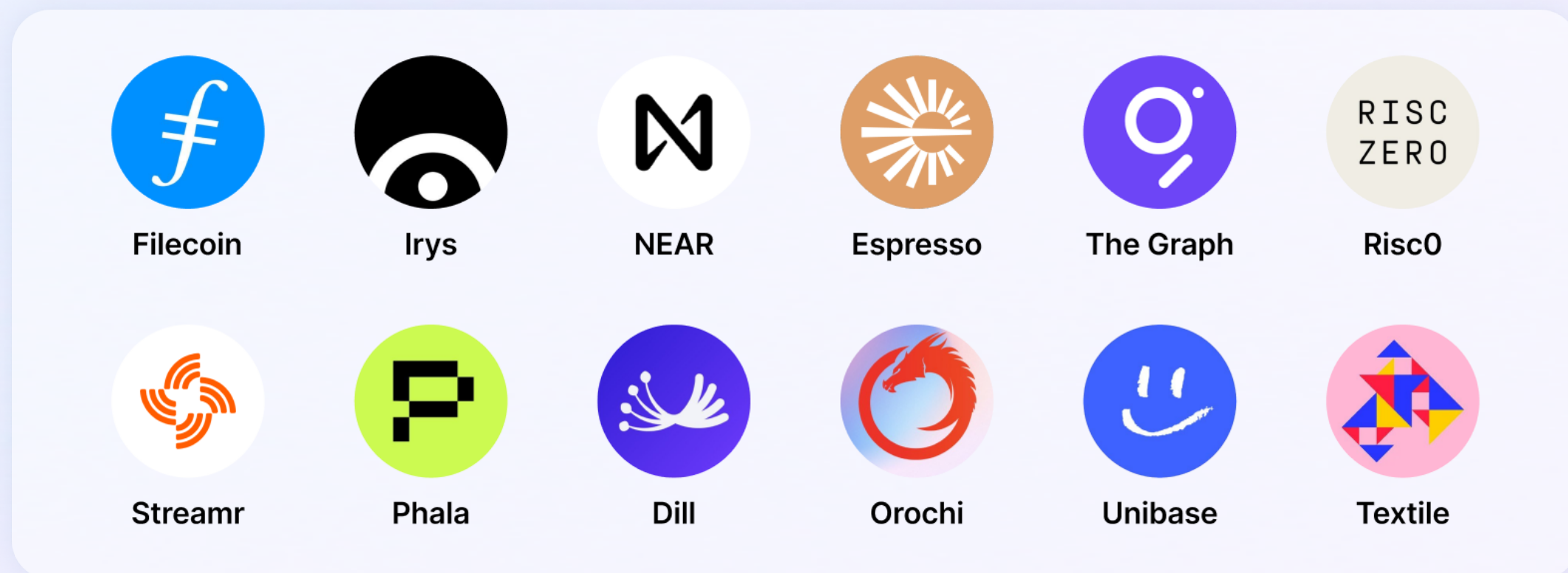- Vision paper for AI-powered computing network published

DePINscan
- Now tracking 18M+ devices and 281 DePINs with $25B+ market cap
- Welcoming new DePINs daily incl. Multiple, Coral, and CyberCharge
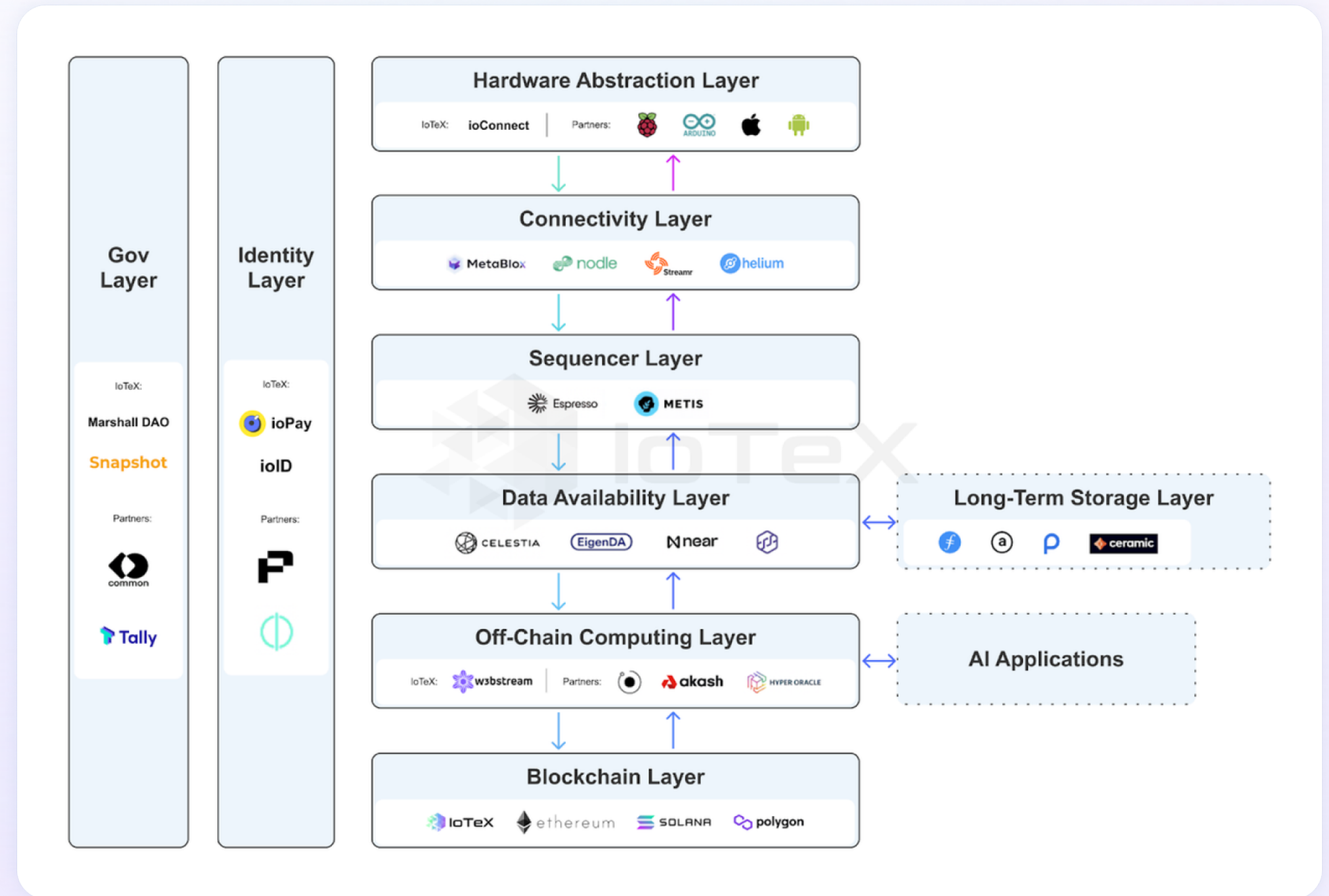
Other Partners
- DePIN X: $2M DePIN fund for IoTeX
- AiGO: geo-location for mobility
- PlayAI: real-time data for gaming
- Grafilab: GPU fractional ownership

DePIN Infrastructure Modules (DIMs)

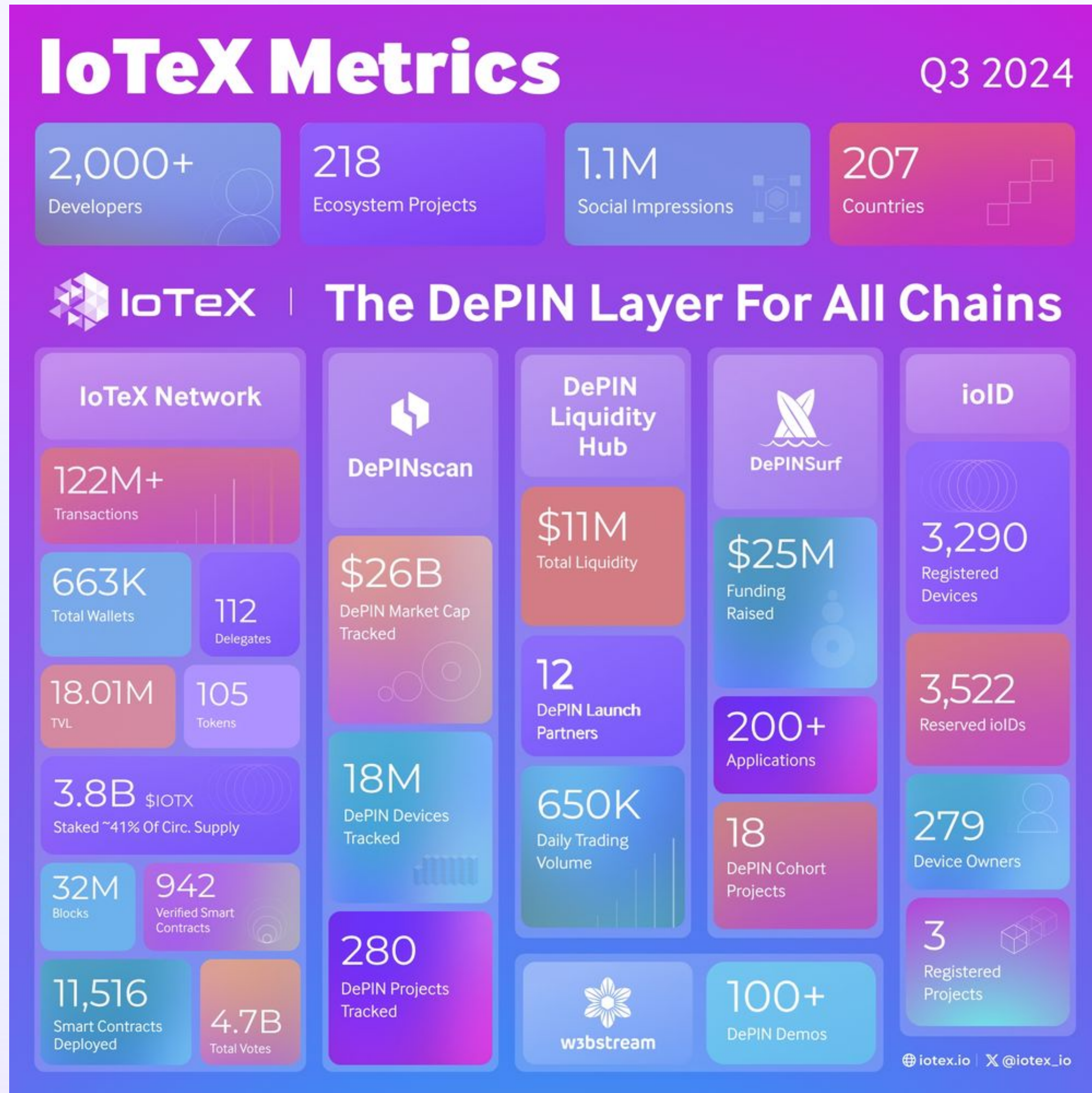IoTeX 2.0 brings top-tier infrastructure partners incl. Filecoin, Irys, NEAR, Risc0, and Espresso to the IoTeX ecosystem. Integrations with The Graph and Streamr are ongoing and new DIMs are joining every week.

Filecoin	Irys	NEAR	Espresso	The Graph	RiscO
Streamr	Phala	Dill	Orochi	Unibase	Textile

IoTeX 2.0 - Modular Infrastructure for Verifiable DePIN

The IoTeX Ecosystem

IoTeX Metrics — Q3 2024

- 2,000+ Developers
- 218 Ecosystem Projects
- 1.1M Social Impressions
- 207 Countries

IoTeX | The DePIN Layer For All Chains

IoTeX Network
- 122M+ Transactions
- 663K Total Wallets
- 112 Delegates
- 18.01M TVL
- 105 Tokens
- 3.8B $IOTX Staked ~41% Of Circ. Supply
- 32M Blocks
- 942 Verified Smart Contracts
- 11,516 Smart Contracts Deployed
- 4.7B Total Votes

DePINscan
- $26B DePIN Market Cap Tracked
- 18M DePIN Devices Tracked
- 280 DePIN Projects Tracked

DePIN Liquidity Hub
- $11M Total Liquidity
- 12 DePIN Launch Partners
- 650K Daily Trading Volume

DePINSurf
- $25M Funding Raised
- 200+ Applications
- 18 DePIN Cohort Projects
- 100+ DePIN Demos

ioID
- 3,290 Registered Devices
- 3,522 Reserved ioIDs
- 279 Device Owners
- 3 Registered Projects

w3bstream

iotex.io | X @iotex_io

Backed by Top Web3 & IoT Investors:
SAMSUNG NEXT, jump, DRAPER DRAGON, EV, Borderless, HASHKEY Capital, Goodwater

Leads of Industry Consortiums & Standards Bodies:
IEEE, Industry IoT Consortium, MOBI, CONFIDENTIAL COMPUTING CONSORTIUM

Team Background:
Google, facebook, Uber, BOSCH, intel

Advisors from:
ethereum foundation, SOLANA, UNIVERSITY OF WATERLOO, NUS National University of Singapore, Goldman Sachs, SoftBank, arm, OlympusDAO
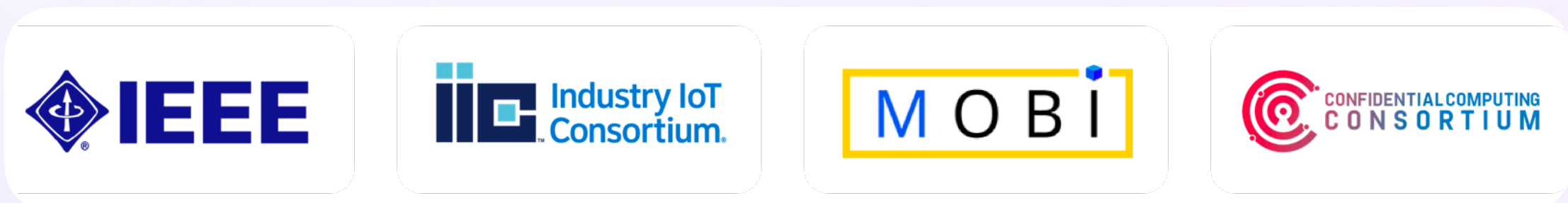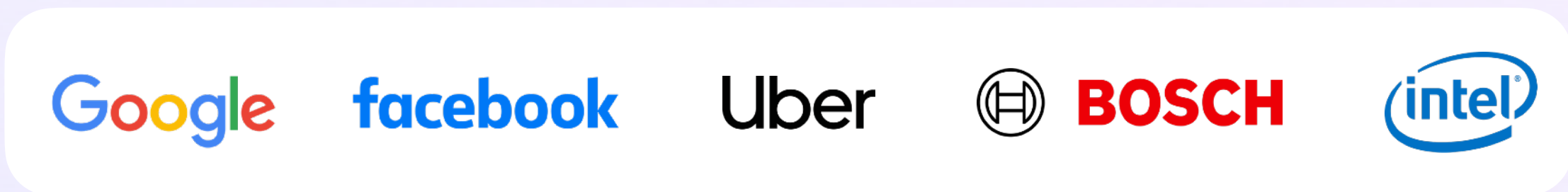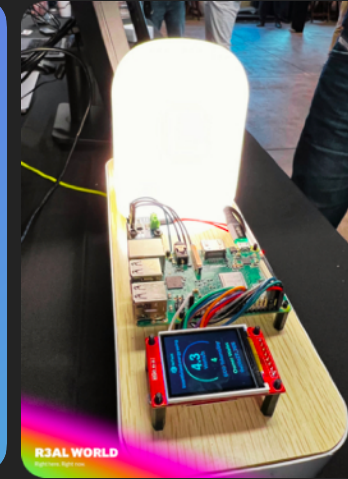
R3al World Previous Events Highlights

9+ Cities

1.1M Social Impressions

150+ Speakers

650+ Investors

100+ Demos & Pitches

7,000 Attendees
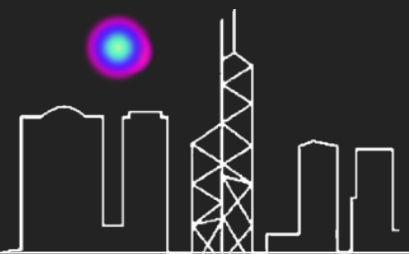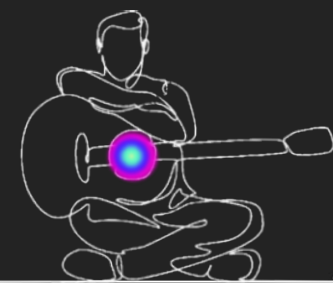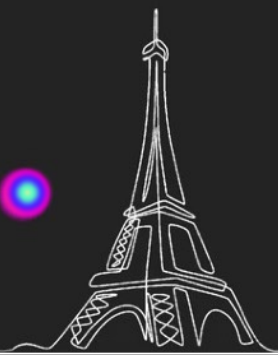
Denver	HongKong	Tokyo	Austin	Paris	Singapore	Denver	Dubai	Austin	Bruxelles	Singapore
Mar 3, 2023	Apr 12, 2023	Apr 15, 2023	Apr 26, 2023	Jul 16, 2023	Sep 13, 2023	Feb 28, 2024	Apr 18, 2024	May 29, 2024	Jul 8, 2024	Sep 17, 2024

UDC

iotex.io | @iotex_io
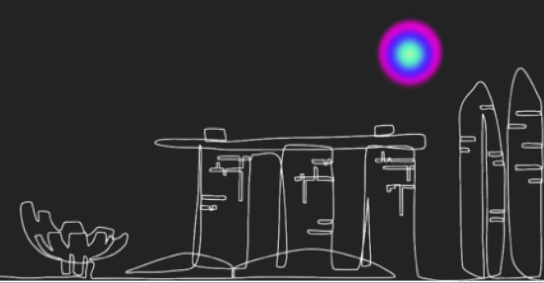
R3al World Previous Sponsors And Partners

IoTeX

EV · SAMSUNG NEXT · Future Money Group · DePHY · Roam · arm · DRAPER DRAGON · CryptoSlate · jump_ · WINTERMUTE · Foresight News

eclipse · HASHKEY Capital · Chainlink · SOLANA · polygon · helium · IOSG VENTURES · Borderless · longhash ventures · Celer · 1k(x)

Xoogler.co · SHIMA CAPITAL · Centrifuge · LATTICE · crypto.com · JDI · Hotspotty · TOPIA · 6MV · E-Money NETWORK · PHALA NETWORK

MXC · Dispersion Capital · Bitget · HYPER ORACLE · HUDDLE 01 · DIMO · SPHERE · exaBITS · STARPOWER · Streamr · a16z crypto

NGC Ventures · Alchemy Pay · COINTELEGRAPH The future of money · CELO · CIRCLE · hivemapper · TechFlow 深潮 · BLOCK TEMPO · BaaS.com · EDGE MATRIX · DMAIL

星球日报 ODAILY. NEWS · Partisia Blockchain · valora · CELESTIA · MANTA NETWORK · Layer Zero. · NETWORK3 · OpenEden · OMNI · ACURAST · CONFLUX

ATOR · SUPRA ORACLES · syntropy · CESS Cumulus Encrypted Storage System · TABLELAND · IO.NET · BEDROCK · ZKPASS · Apus Network · OpSec · MVL

AeroNyx · WAYRU · WEATHERXM · INFERIX · POWERPOD · NATIX Network · Republic

UDC

iotex.io | X @iotex_io

Launching Partners

IoTeX **GOAT** season 2

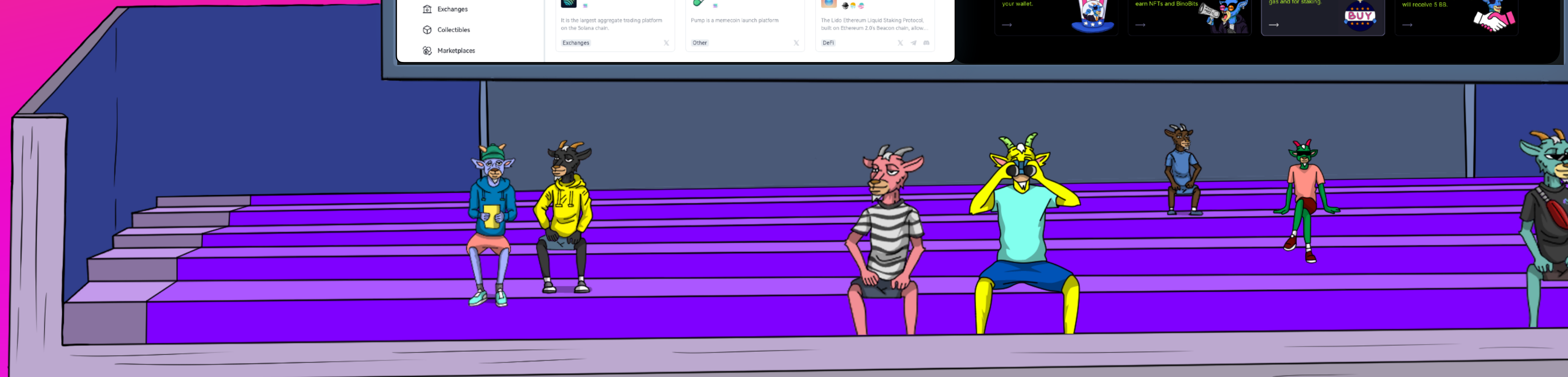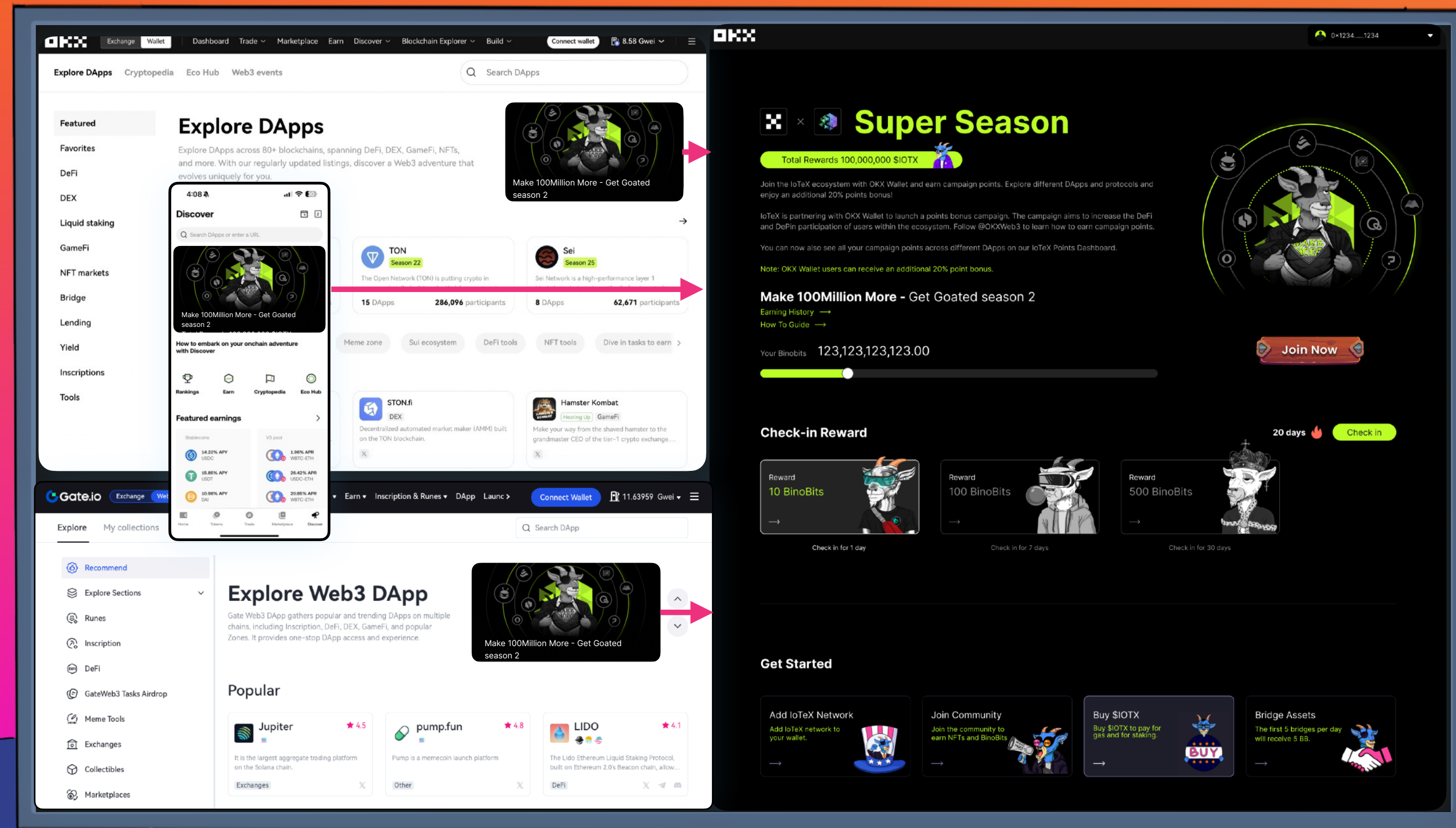# 50M+

User Reach in Partnership with OKX,
Bybit, more top-tier CEXs coming

OKX   **Gate.io**

COMING SOON

TON

BYBIT

UDC