Privacy in the Age of AI

Pierre Le Guen
Software Engineer
NEAR AI

AI systems are failing us

- Flawed responses
  - Ads based
  - Biases
  - Blackboxes
- Security risks
  - Major data leaks are waiting to happen
- Open-Source AI is not sustainable
  - Stability AI unable to pay for rented cloud GPUs
- Trust issues -> Restricted access in many countries

Why It Matters

User-Owned AI

- Fair access to anyone
- Fully verifiable/auditable stack
- Control over your data
- Sustainable business model for every actor
  - Share your data and get rewarded
  - Build a model for a specific need

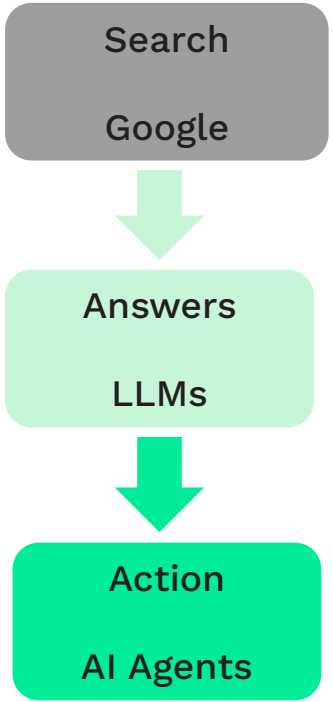
AI optimized for users' wellbeing and economic success

Thesis

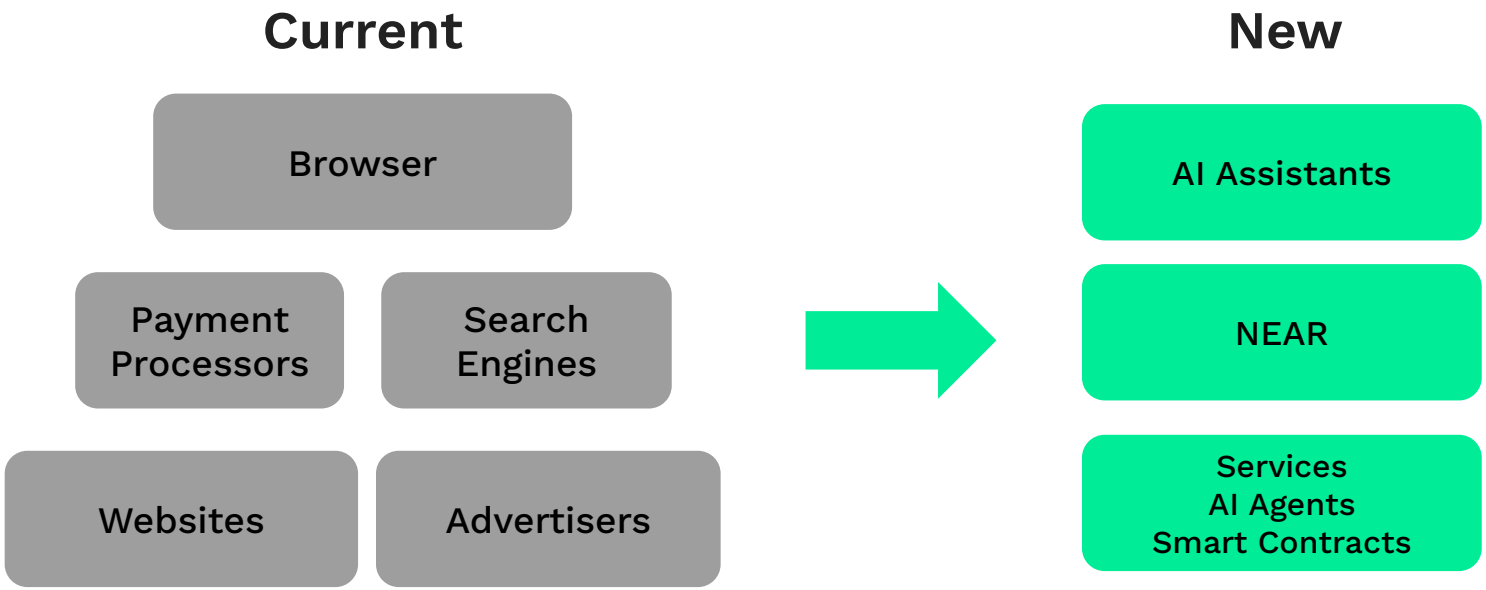
The world is going to transition from websites and apps to AI & agents

We need to ensure:

1. Confidentiality – your AI assistant will know everything about you
2. Equal access & control of AI capabilities
3. User ownership of assets, data, and choice



Paradigm Shift



What does ‘Blockchain for AI’ mean?

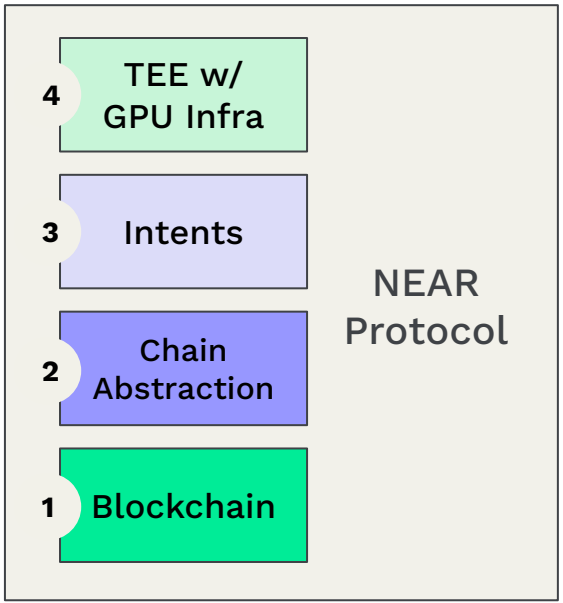
near

✅ 1. A **blockchain that can scale** & support transactions by trillions of AI agents and billions of users

✅ 2. Solutions that enable AI agents to **operate across different chains** (i.e. Chain Abstraction tech)

✅ 3. A negotiation, commitment, & dispute **framework that allows agents to work together** across a variety of on- & offchain systems

🏗️ 4. The ability to **privately & verifiably perform AI training and inference** (to incentivize open-source model contributors)



A multi-purpose Protocol for the AI-first future

NEAR AI Stack

Agent Cloud

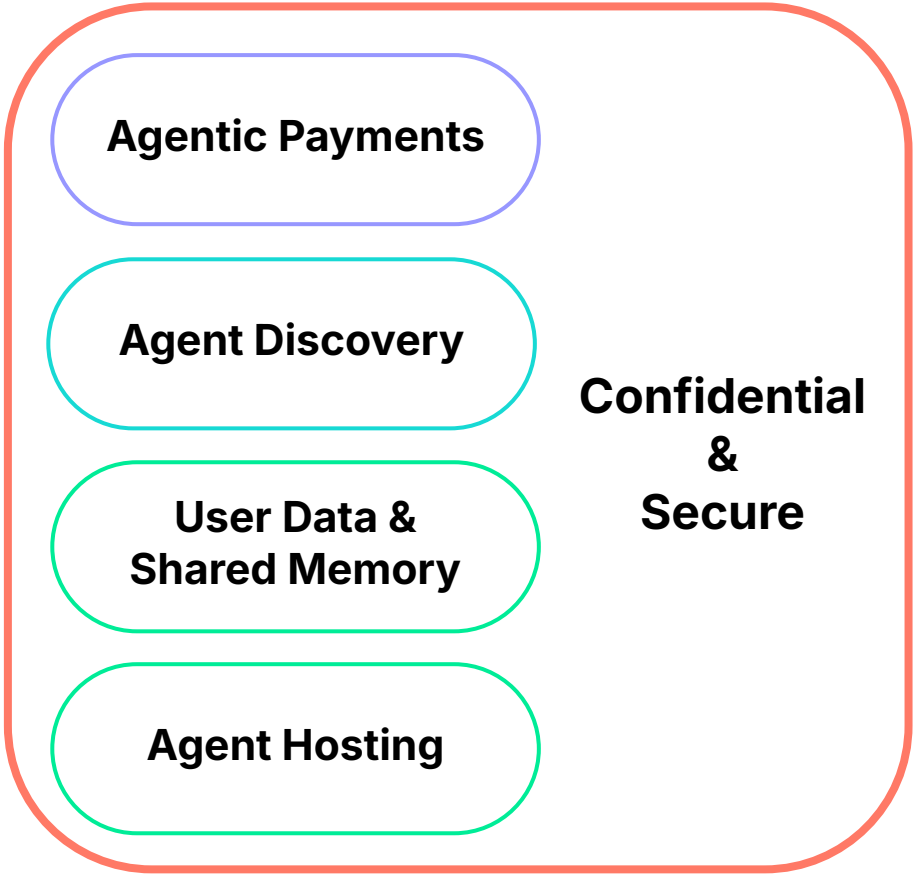
- Host your AI Agent
- Access hundreds of AI Agents
- Generate revenue from your agent

NEAR AI Agent SDK

- Create complex agents in Python or Typescript

NEAR Protocol

- Micro-transactions between agents
- Chain Abstraction to interact with any blockchain



Trusted Execution Environment

Trusted Execution Environment (TEE): enables computation on third-party hardware that guarantees the computation run & outcome achieved

CPU: Intel TDX, AMD SEV, ARM CCA

GPU: NVIDIA Confidential Computing starting with H100s

Confidential VM is an abstraction over TEE-specific hardware

CVM
Confidential Virtual Machine

What TEE magic enables?

- Fully Encrypted Models
  - Train your model in a TEE
- Monetized Confidential Inference
  - Share access to your model and get rewarded for it
- Verifiable Agents
  - Ensure that the AI Agent being ran is the one you expect.

Fully verifiable stack, don’t trust, verify!

Monetized Confidential Inference