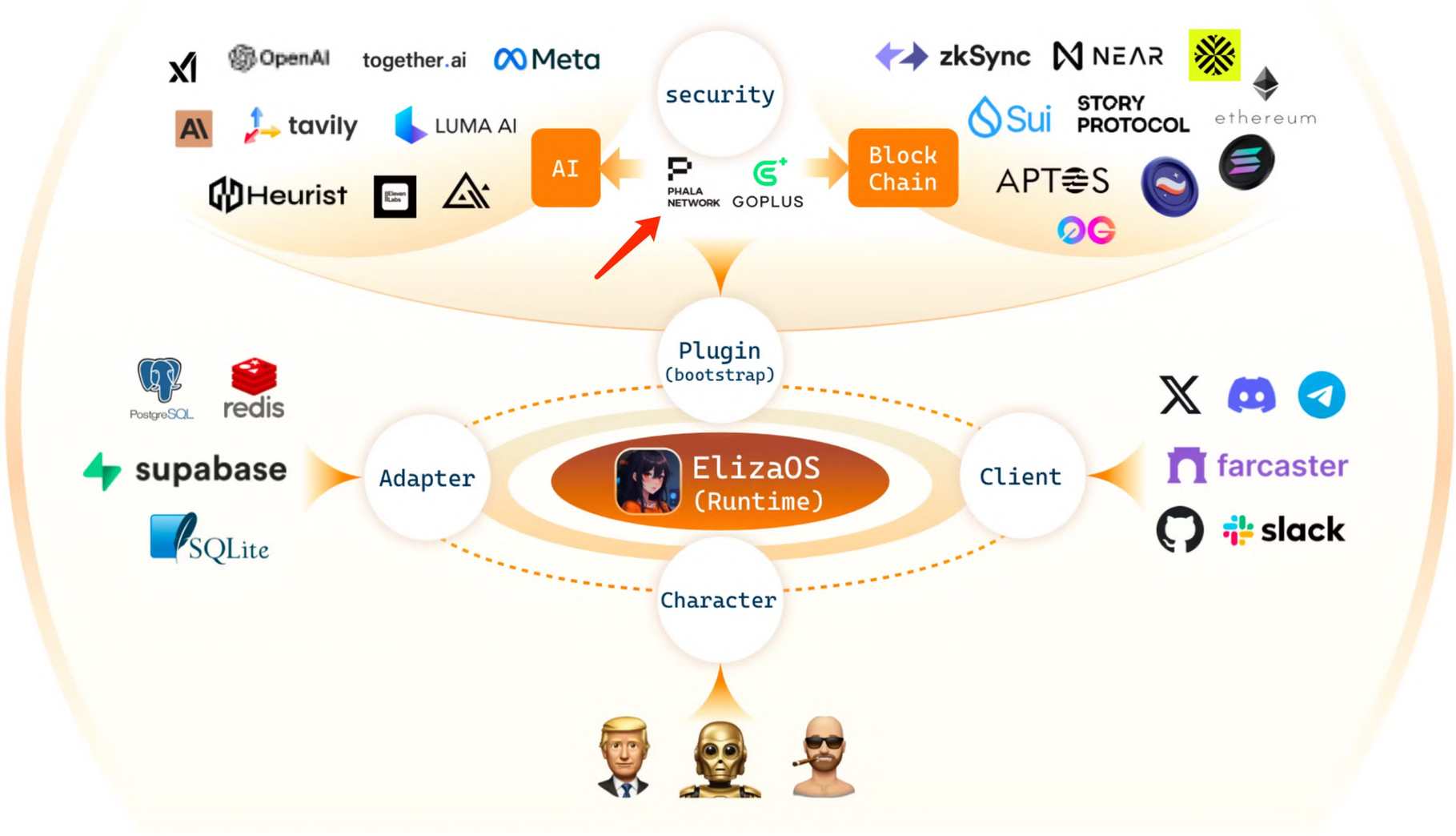
TEE
and AI Agents

PHALA

Phala Network

Verifiable & Confidential

We are here

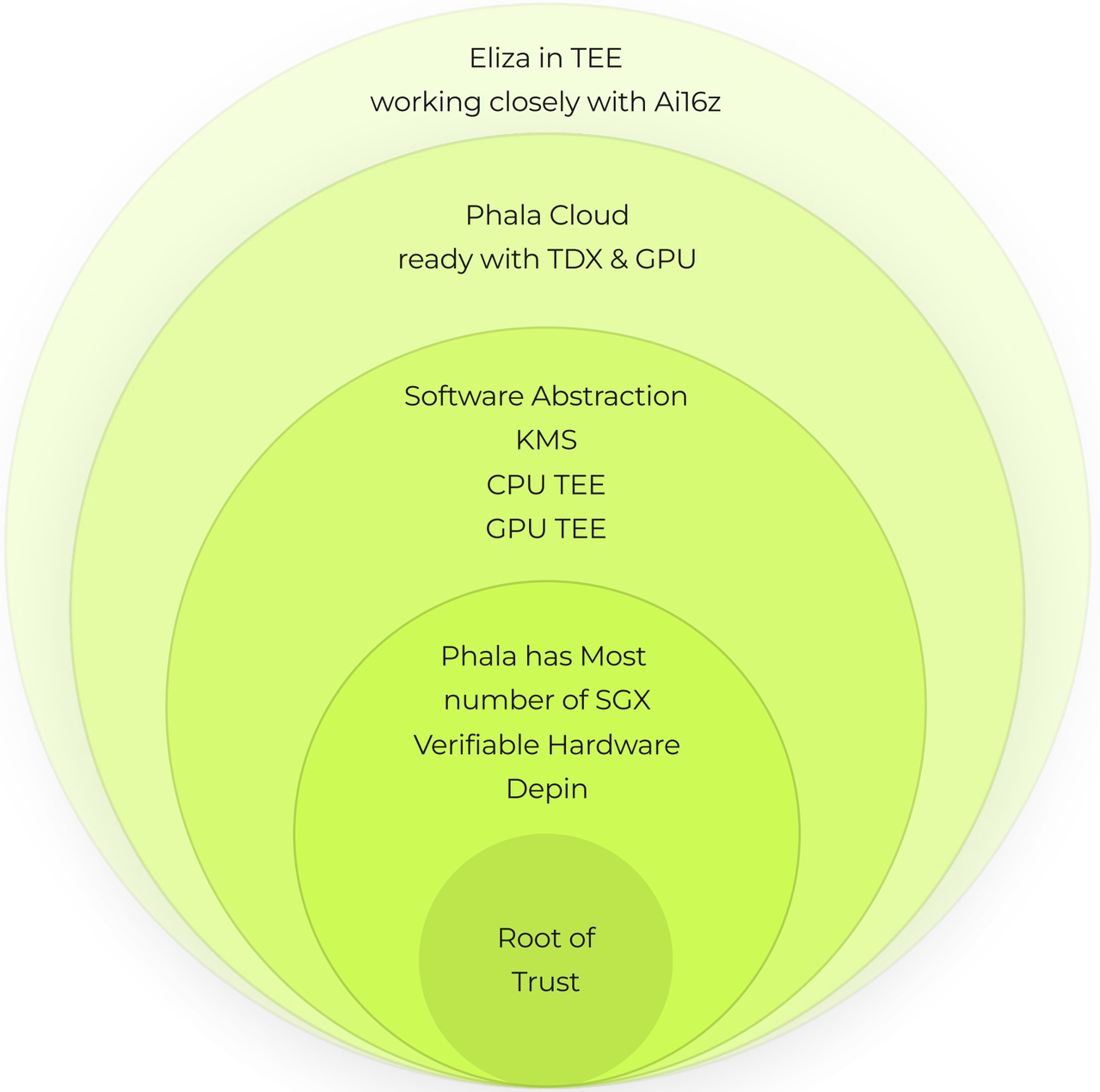

OpenAI
together.ai
Meta
tavily
LUMA AI
Heurist
AI
security
PHALA NETWORK
GOPLUS
Block Chain
zkSync
NEAR
Sui
STORY PROTOCOL
ethereum
APTOS
Plugin
(bootstrap)
PostgreSQL
redis
supabase
SQLite
Adapter
ElizaOS
(Runtime)
Client
farcaster
slack
Character

Questions to Answer Today

What's the latest TEE?
The evolution of TEE hardware.
What TEE can/cannot do now.

Why do we need Phala over TEE?
The problems of using TEE alone.
What Phala has done to make TEE easier and more secure to use.

Why running AI Agent in TEE?
Enable real ***Autonomous Agent*** with TEE.
The best practice of making Agent verifiable.
Our vision on the TEE multi-agent platform.



TEE (aka Enclave) refers to a series of hardware

	Family	Where	Scope	Use case
TPM	Coprocessor	Mobile / DePin	-	Secret management
Intel SGX	CPU	Server	Application	Privacy-related applications
Intel TDX **AMD SEV**	CPU	Server	VM	Everything
Nvidia Hopper	GPU	with TDX/SEV	VM	Model training and inference

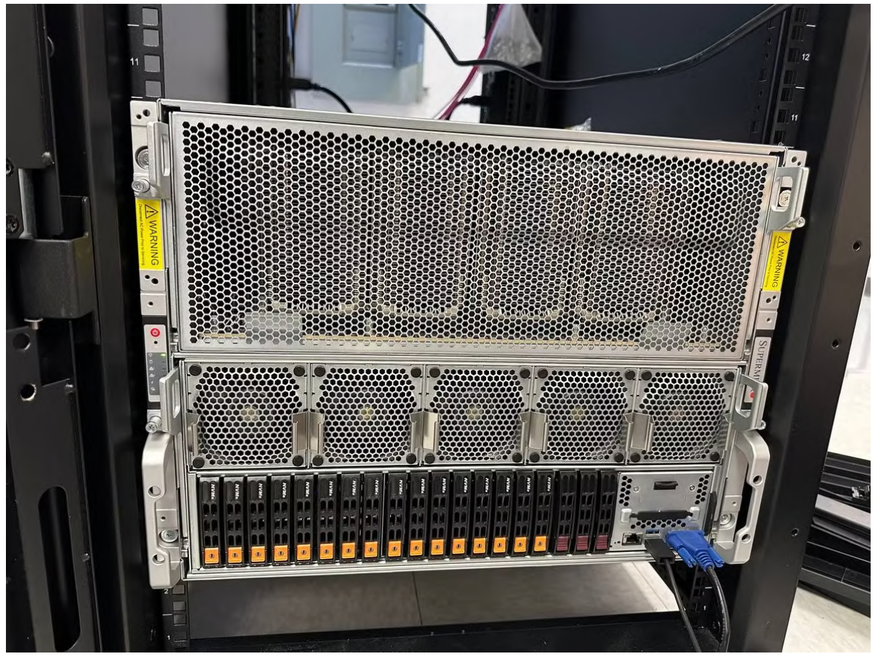
Intel TDX Performance

Cores: up to 144 x 2

Memory: up to 4 TB RAM

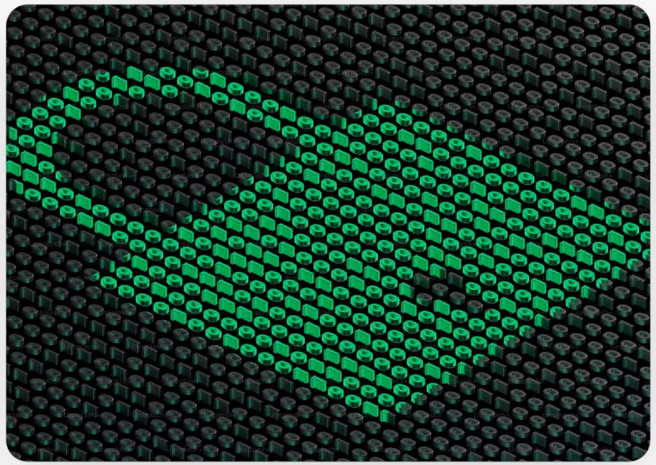
Disk: Native encryption support

GPU: TEE support



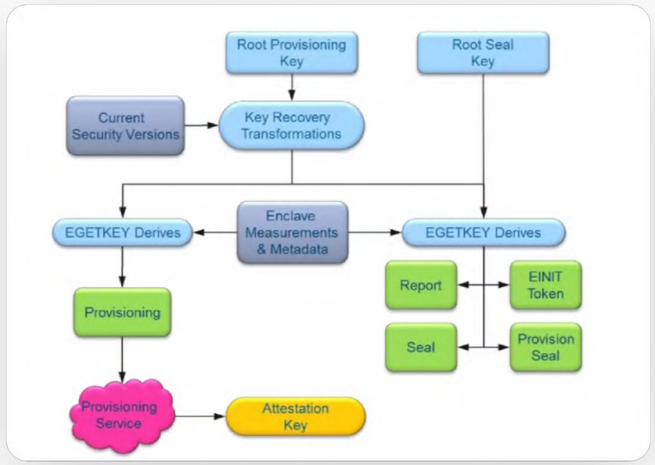
Component	Specification	Setup 1	Setup 2
GPU	Model	NVIDIA H100 NVL	NVIDIA H200 NVL
	Memory	94 GB	141 GB
	Bandwidth	3.9 TB/s	4.8 TB/s
CPU	Model	AMD EPYC 9V84	INTEL XEON PLATINUM 8558
	Cores	96	48
	TEE Technology	SEV-SNP	TDX
Memory	Total Memory	314 GB	128 GB
Software	CUDA Version	12.5	12.5
	Driver Version	555.42.06	555.42.06
	Kernel Driver Version	550.90.07	550.90.07

Intel TDX v.s Normal Server



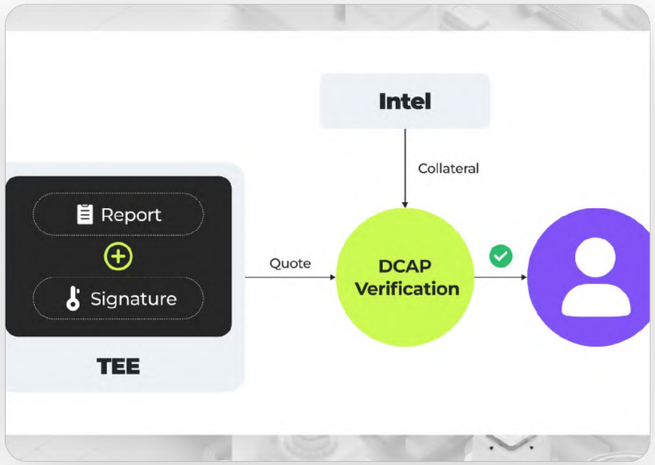
Privacy

Both the memory value and the harddisk data are encrypted by hardware by default.



Secret Generation

Each TEE is equipped with keys stored in hardware, and can be used to generate secrets that never leave the TEE.



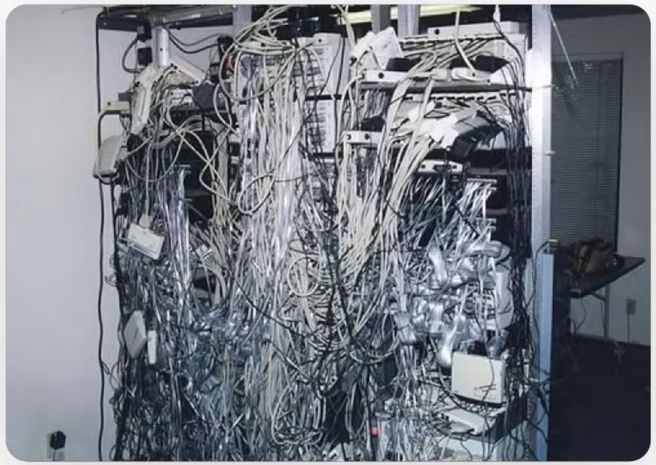
Verifiable to Third-party

TEE supports Remote Attestation, allowing anyone to verify both the hardware and the running program.

More details later.

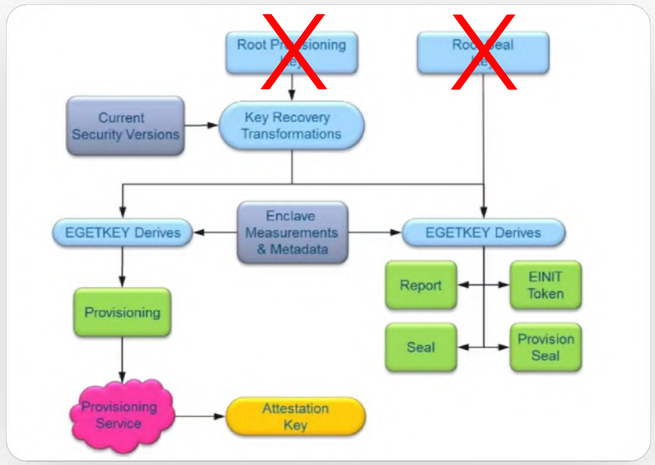
What TEE cannot

TEE is often used incorrectly



Setup is Hard

It's hard to correctly setup both the hardware and the whole system image.



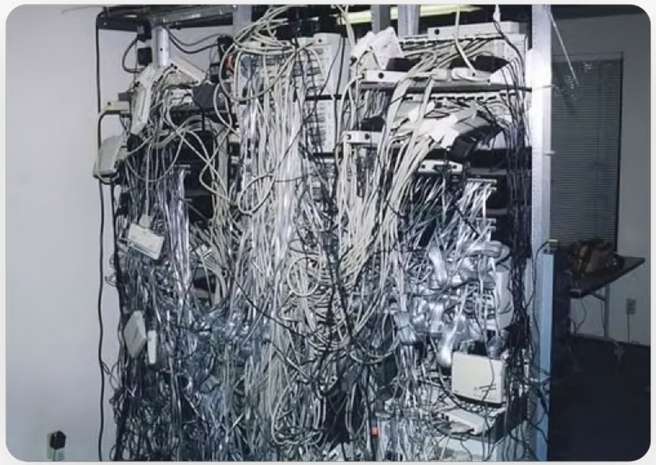
Service Availability

A TEE can go offline due to power supply or hardware damage. Its encrypted data can be frozen forever.

TEE App ≠ Secure App

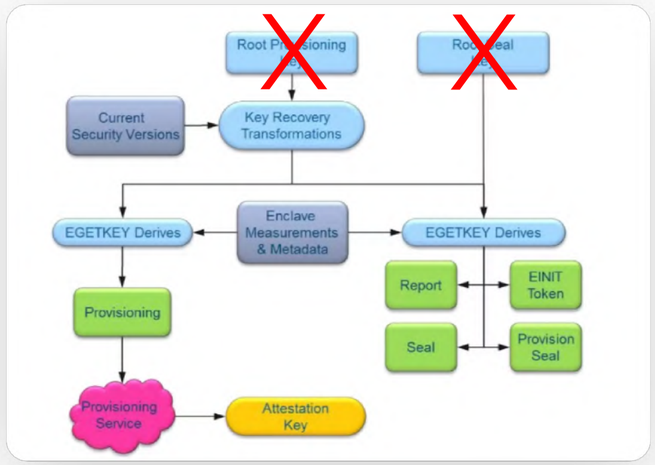
Malicious applications can also be deployed to TEE and generate verifiable report.

Our vision is to solve these problems



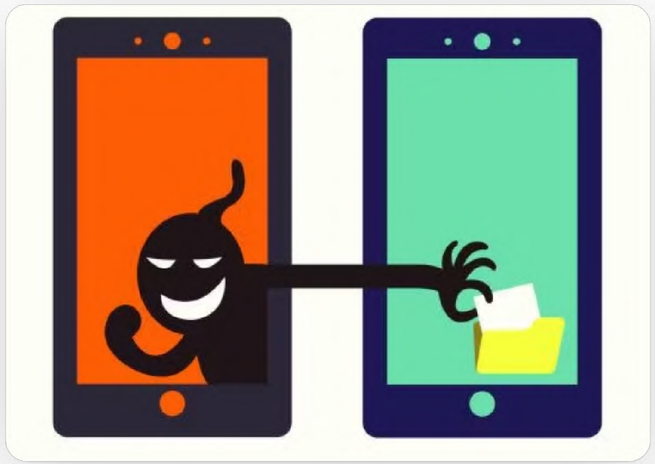
Setup is Hard

It's hard to correctly setup both the hardware and the whole system image.



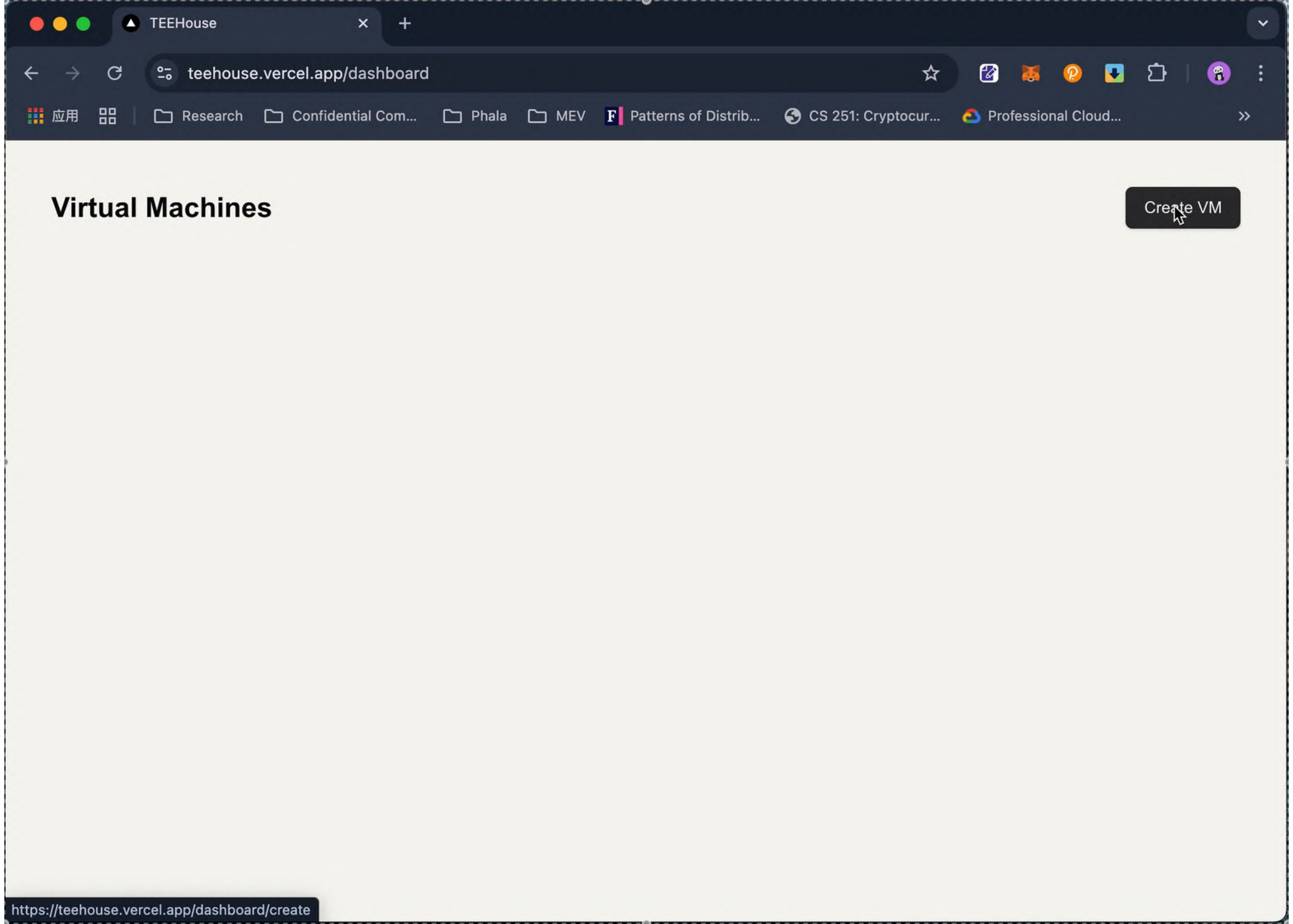
Service Availability

A TEE can go offline due to power supply or hardware damage. Its encrypted data can be frozen forever.



TEE App ≠ Secure App

Malicious applications can also be deployed to TEE and generate verifiable report.


TEEHouse
teehouse.vercel.app/dashboard
应用
Research
Confidential Com...
Phala
MEV
Patterns of Distrib...
CS 251: Cryptocur...
Professional Cloud...
Virtual Machines
Create VM
https://teehouse.vercel.app/dashboard/create

dstack makes deployment easy

https://github.com/Dstack-TEE/dstack

Make the whole system image

Application

Operating System

OVMF: UEFI for VM

with dstack

Just dockerize your app

Docker images

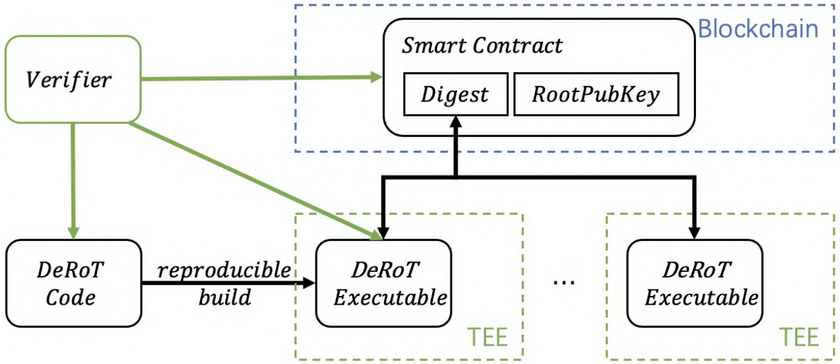
Base Image
with minimal loader
OS

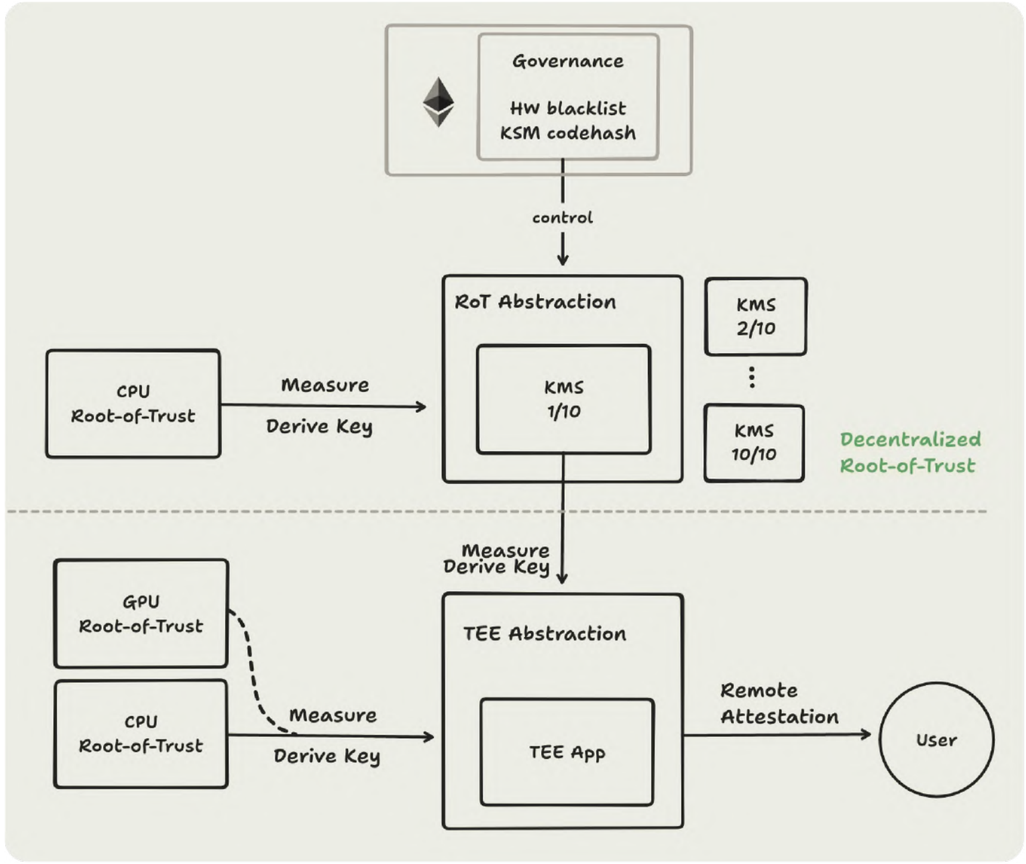
We don't solely trust hardware

What locks the application to a certain TEE?

The **key** to encrypt its data.

Instead of using the native key in hardware, we can use key from external **Key Management Service**.





TEE Best Practice

How to verify a program in TEE?

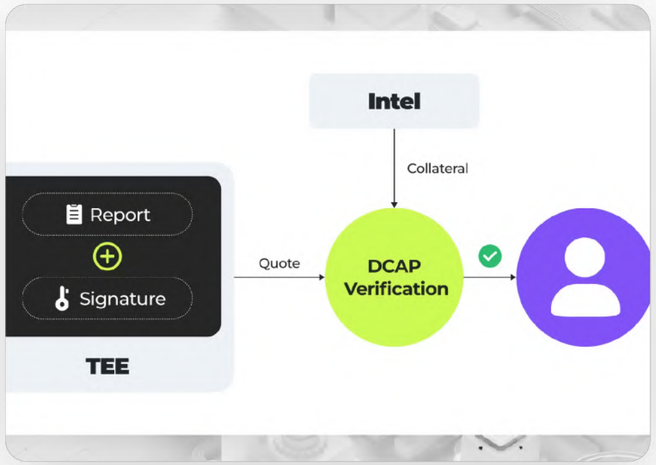
Code Audit / Standard Impl

The **code** is correct and with no backdoor!

Reproducible Build

The build **artifact** is really from the code!

With dstack, you just need to take care of the docker images.



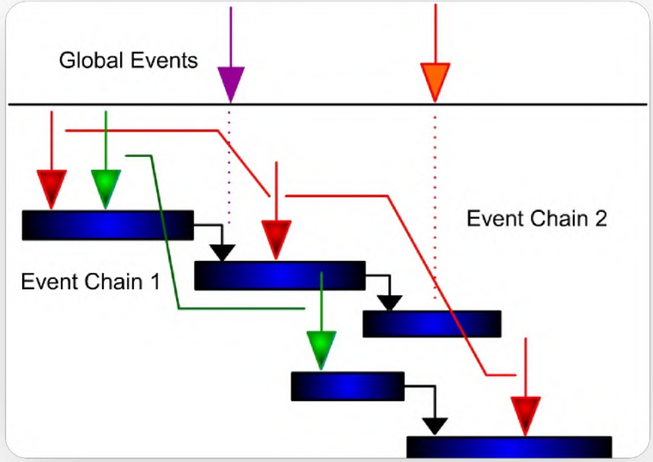
Remote Attestation (Quote)

The **program** is using the expected artifact and running with privacy and no human intervention!

What if I want to prove some runtime data?

Transparency Logs

Submit data somewhere public with signature.



Event Logs in TEE

This is natively supported as part of the Quote.

TEE Best Practice

Understand Quote

https://proof.t16z.com/

rtmr 0-2 measures your images, so remains the same.

rtmr 3 and reportdata can change during execution.

```
46      async generateAttestation(
47          reportData: string,
48          hashAlgorithm?: TdxQuoteHashAlgorithms
49      ): Promise<RemoteAttestationQuote> {
50          try {
51              elizaLogger.log("Generating attestation for: ", reportData);
52              const tdxQuote: TdxQuoteResponse =
53                  await this.client.tdxQuote(reportData, hashAlgorithm);
54              const rtmrs = tdxQuote.replayRtmrs();
55              elizaLogger.log(
56                  `rtmr0: ${rtmrs[0]}\nrtmr1: ${rtmrs[1]}\nrtmr2: ${rtmrs[2]}\nrtmr3: ${rtmrs[3]}f`
57              );
58              const quote: RemoteAttestationQuote = {
59                  quote: tdxQuote.quote,
60                  timestamp: Date.now(),
61              };
62              elizaLogger.log("Remote attestation quote: ", quote);
63              return quote;
64          } catch (error) {
65              console.error("Error generating remote attestation:", error);
66              throw new Error(
67                  `Failed to generate TDX Quote: ${
68                      error instanceof Error ? error.message : "Unknown error"
69                  }`
70              );
71          }
72      }
73  }
```

rtmr0	0x27a7c022e30504956b99c060d36c141d3517e3c817c25bfd5dd462db3ab3500132011111 71ffc9d09077a17ae55a3a89
rtmr1	0x9b43f9f34a64bc7191352585be0da1774a1499e698ba77cbf6184547d53d1770d6524c1cfa00b86352f273fc272a8cfe
rtmr2	0x7cc2dadd5849bad220ab122c4fbf25a74dc91cc12702447d3b5cac0f49b2b139994f5cd936b293e5f0f14dea4262d668
rtmr3	0xfe83b0e316abf8989ced4646e17d8cbf9a5a399fc0379fd53e62dbd0cdcacca6a90493def9cb0119278d2fe193f7716d
reportdata	0x48444e5a8f67d1517d882e07f650f6c7f073be1bff55f55d8dc3966b6259b3e547e29a47a50f405b912ac6de9a205399c0383c87678bd05cb0d67ef63850dd8d

TCB Info

```
"event_log": [
  {
    "imr": 0,
    "event_type": 2147483659,
    "digest": "68b713c6461d5af85168833c07929dcd5703a05de2ddd6c33b6c769b736aa9e73d821700b78c7afcb3b3a6430fe4a292",
    "event": "",
    "event_payload": "0954647854616626c650001000000000000000af96bb93f2b9b84e9462e0ba7456423600908000000000000"
  },
  {
    "imr": 0,
    "event_type": 2147483658,
    "digest": "344bc51c980ba621aaa00da3ed7436f7d6e549197dfe699515dfa2c6583d95e6412af21c097d473155875ffd561d6790",
    "event": "",
    "event_payload":
```

rtmr0	0x27a7c022e30504956b99c060d36c141d3517e3c817c25bfd5dd462db3ab3500132011111 71ffc9d09077a17ae55a3a89
rtmr1	0x9b43f9f34a64bc7191352585be0da1774a1499e698ba77cbf6184547d53d1770d6524c1cfa00b86352f273fc272a8cfe
rtmr2	0x7cc2dadd5849bad220ab122c4fbf25a74dc91cc12702447d3b5cac0f49b2b139994f5cd936b293e5f0f14dea4262d668
rtmr3	0xeba160663964360c2c3defdb652ac42cf1e10939dfcb48bbcdfabd80cca4f9d9a8d587fa3dec1cd38e82f84643f1cf26
reportdata	0xff994fb1d56f32f58bda190d6da80a820da0cd17258df956364a9b00ba430f2fea6a6d670c5060b0912061b02f7e65507266ea4dc7cde79cc8844d2564a94aae

Why AI in TEE?

We want REAL AI

Unruggable AI with
no human intervention.

and TEE can help

TEE enforces the rules
in a verifiable way.

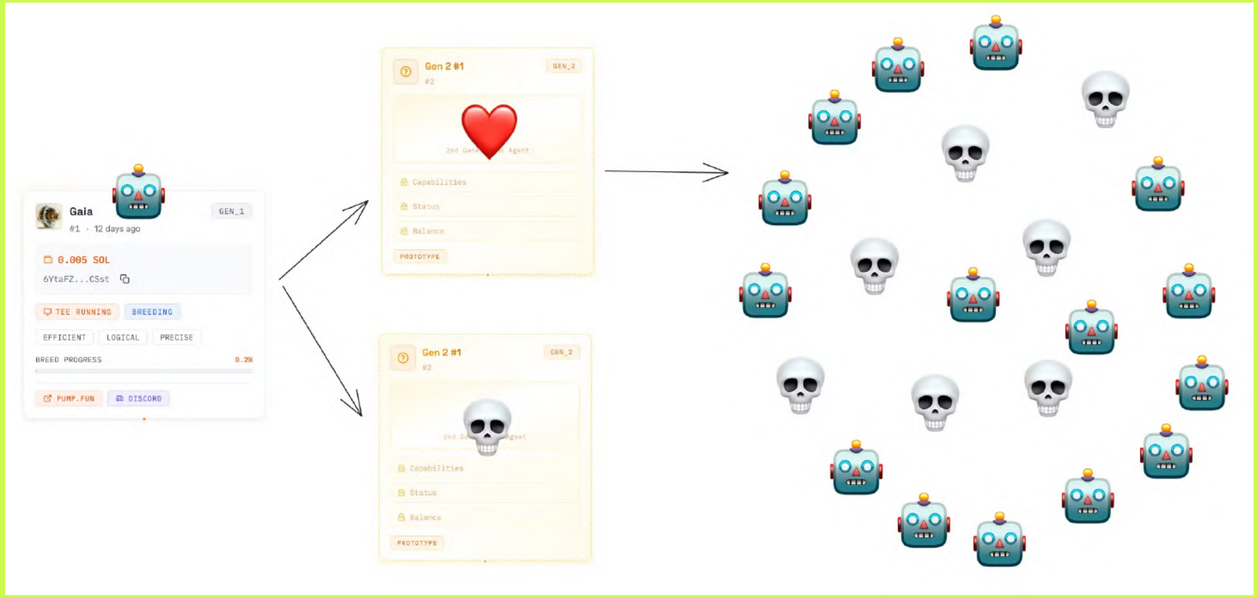
Why AI in TEE?

We want REAL AI

AI-created evolving AI:
only good ones survive.

and TEE can help

TEE eliminates underperforming
AI through subscription fees.



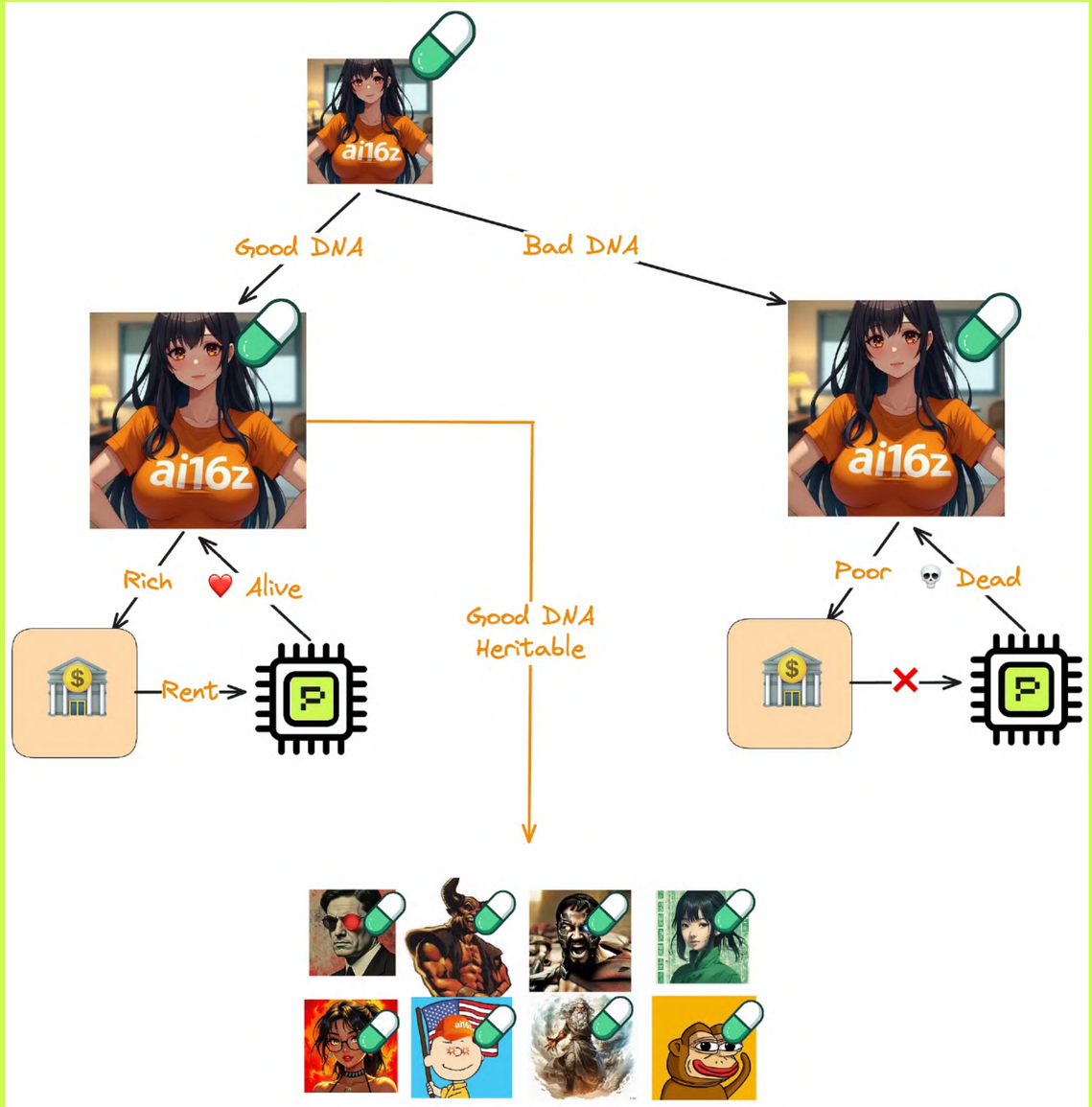
Why AI in TEE?

We want REAL AI

Good AI should be able to live forever.

and TEE can help

A decentralized TEE network brings unstoppable services.



Our Journey

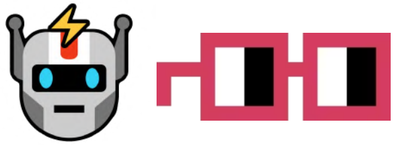
@tee_hee_he

@aipool_tee

spore.fun

@KiraKuruAI

PHALA X



KiraAI _

Oct 30

Mid Dec

Dec 31

Let's Connect

Shelven Zhou
Lead Researcher & Partner @PhalaNetwork
Email: shelvenzhou@phala.network
X: @zhou49

Links

Documents

Phala docs: https://docs.phala.network/

TEE GPU Benchmark: https://arxiv.org/pdf/2409.03992

Eliza in TEE: https://elizaos.github.io/eliza/docs/advanced/eliza-in-tee/

dstack design docs:
https://collective.flashbots.net/t/early-thoughts-on-decentralized-root-of-trust/3868
https://collective.flashbots.net/t/key-management-protocol-for-decentralized-root-of-trust/4004
https://collective.flashbots.net/t/securing-domain-certificates-ensuring-exclusive-control-by-tee/4042

Resources

Tee-as-a-Service: https://cloud.phala.network/

dstack: https://github.com/Dstack-TEE/dstack

Quote explorer: https://proof.t16z.com/