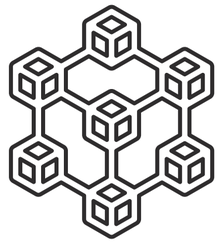
TEA: Trusted Execution & Attestation

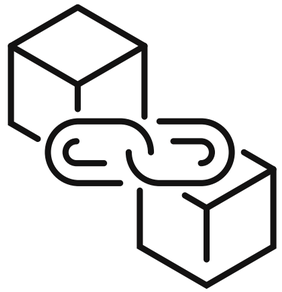
Elevating Decentralized Trusted Computing to a T

teaproject.org



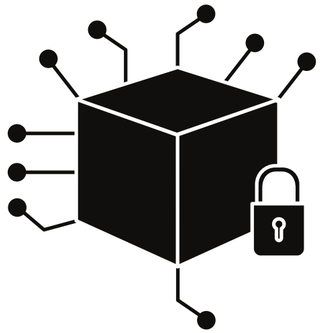
A Decentralized Cloud

A decentralized trusted cloud computing DAO where miners run the nodes.



2-Layer Blockchain

A 2-layer consensus blockchain able to host rich UX dApps.



Trusted Computation Environment

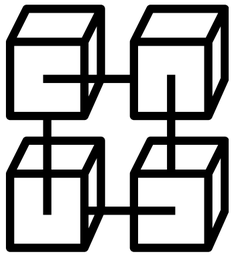
A trusted and secure computation environment that protects privacy and is censorship-resistant.

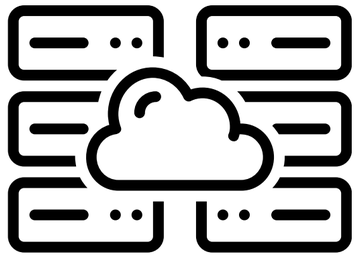
The TEA Project Mission

A decentralized and secure cloud computing environment leveraging two blockchains: layer-1 for trust and layer-2 for speed.

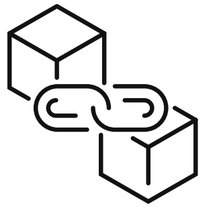
→

The TEA Project Combines the Best of Blockchain & Cloud Computing





Traditional Blockchain	Cloud Computing	The TEA Project
Decentralized but slow	Centralized	Decentralized
Consensus required because of Byzantine fault tolerance (BFT)	Consensus doesn't require BFT but does require trust between nodes	**Rich UX dApps run on layer-2 non-BFT consensus; layer-1 blockchain handles BFT**
Small number of rich apps	Can run rich apps / possibly censored	Runs rich apps at full speed / no censorship
Needs special privacy protocol	Potential privacy breaches	Privacy protected by TPM chip



Existing Blockchains ...

Byzantine-fault tolerance leads to slow processing

No matter how many nodes are running in a typical blockchain system, the one-by-one ordered transaction queue of existing Byzantine fault tolerant (BFT) consensus algorithms leads to slow data processing times. Smart contracts currently cannot run complex algorithms. Attempts to do so have shown smart contracts to be too slow or too expensive as they lack the processing power of modern cloud computers.

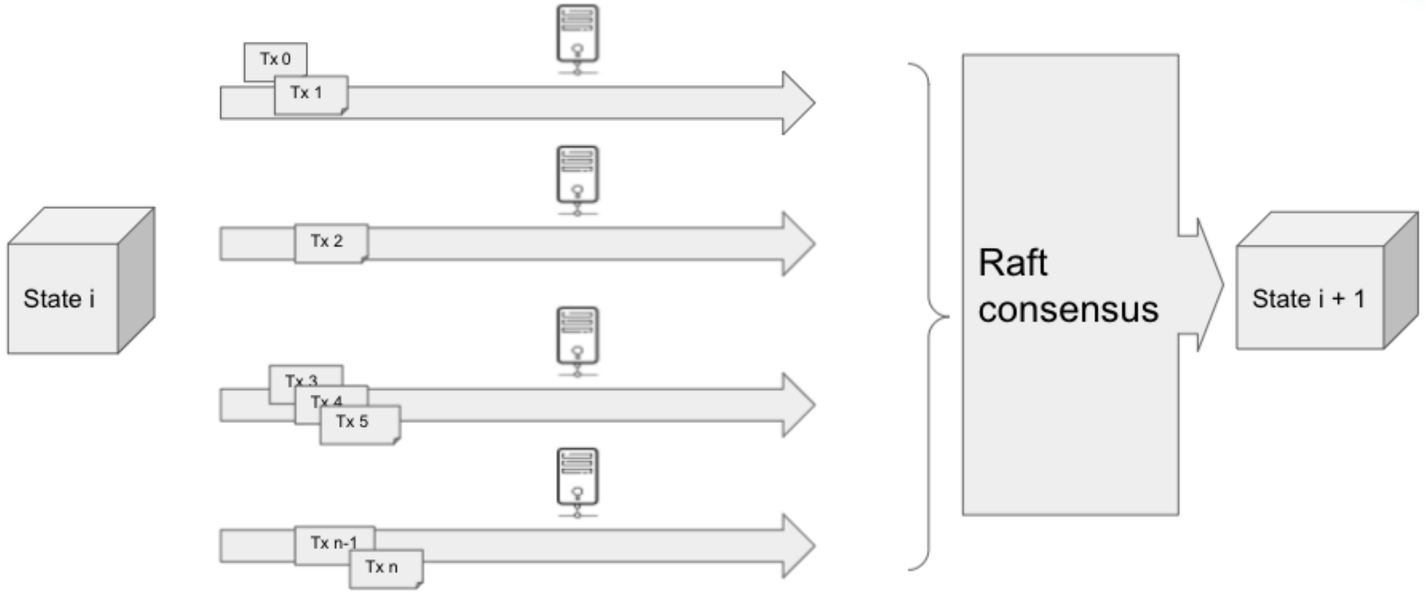
Existing blockchains are slow because they need BFT to reach consensus. They could host dApps that reach the speed of cloud computers if only they had ...

→

We don't yet have rich dApps running at cloud-speed on blockchains since these systems need consensus to guard against a trust-less environment. Cloud computing gives you rich and fast apps, but it's not decentralized and you must assume their ecosystem is trustable.

But what if trust is already taken care of? Then our blockchain could implicitly trust its nodes and use Raft consensus. Our blockchain would run fast like cloud computers who are able to take trustable nodes for granted.

How theTEA Project solves the issue of running rich dApps on the blockchain.



Solution: use non-BFT consensus (Raft) to run dApps on a fast layer-2

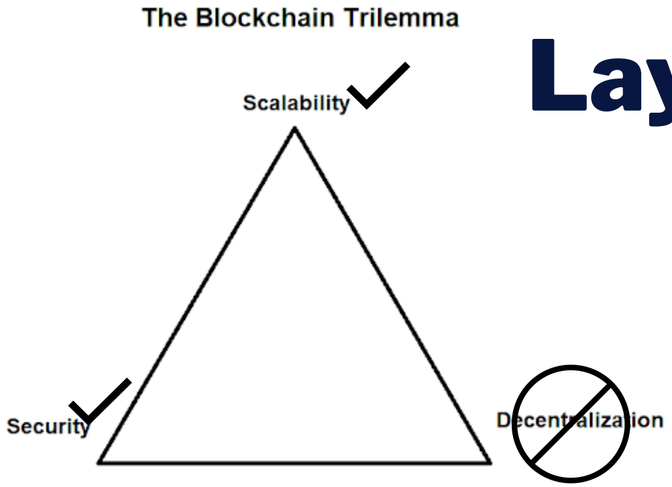
The TEA Project uses layer-1 to run BFT to filter out all non-trustable nodes.
The layer-2 blockchain can check the trust status of any of its nodes by querying the layer-1 blockchain.
The TEA Project's layer-2 can now use the much faster Raft consensus as it can assume all its nodes are trustable as reported by the layer-1 blockchain.

→

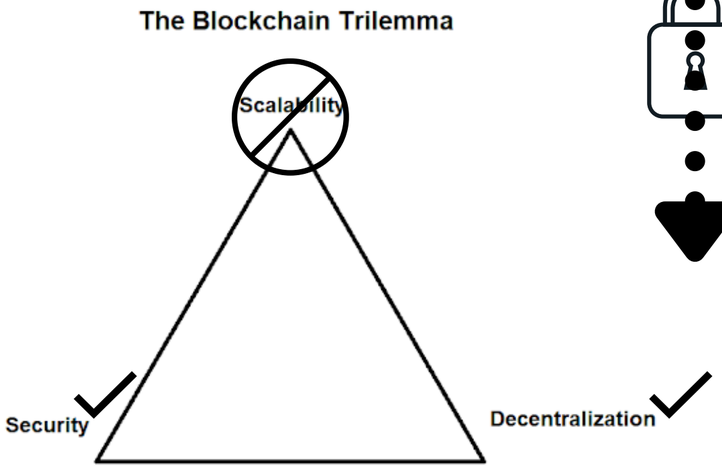
The TEA Project's Two Layer Setup

Layer 2

- Rich applications run on decentralized nodes that have already gained trust from layer-1.
- Layer-2 uses Raft consensus to maintain the dApp state.
- Programming logic and data are secured inside hardware protected enclaves.
- Security chip (TPM) used as Root of Trust (RoT) to generate Proof of Trust (PoT).
- Verifies other nodes' PoT and sends verification result to Layer 1.



Layer 1



- Immutable data storage.
- Polkadot PoA for consensus.
- Consensus on the verification result from Layer 2.
- Manages remote attestation.
- Manages TEA token economy.
- Verifies blocks.

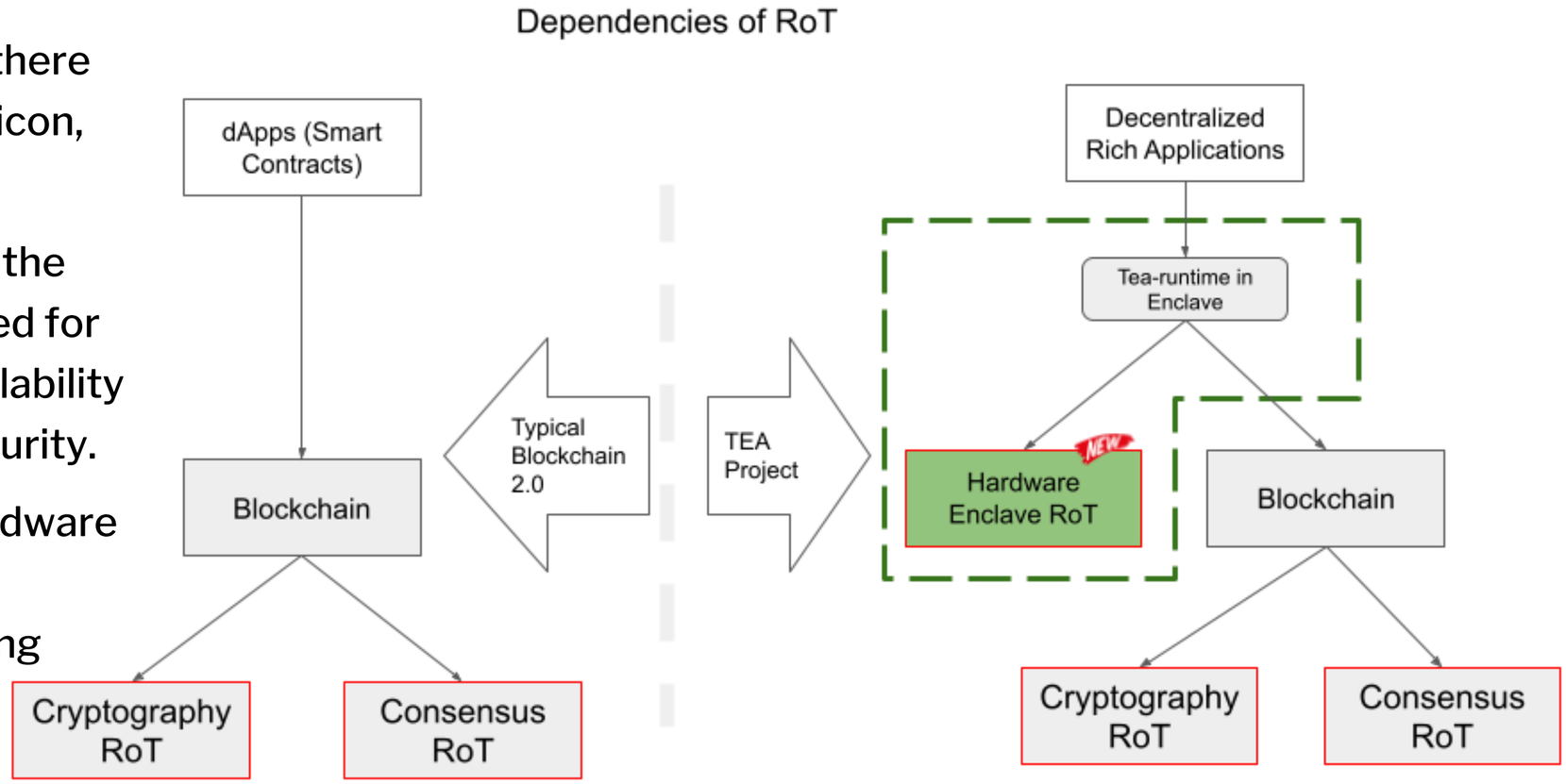
→

Security: The TEA Project's Root of Trust (RoT)

In traditional blockchain, there's two RoT (Root of Trust), consensus and cryptography. In the TEA Project, there are three RoT: secure hardware silicon, consensus, and cryptography.

In traditional blockchain, the dApps run on the blockchain directly (layer-1). Due to the need for BFT consensus, it's not possible to get scalability while maintaining decentralization and security.

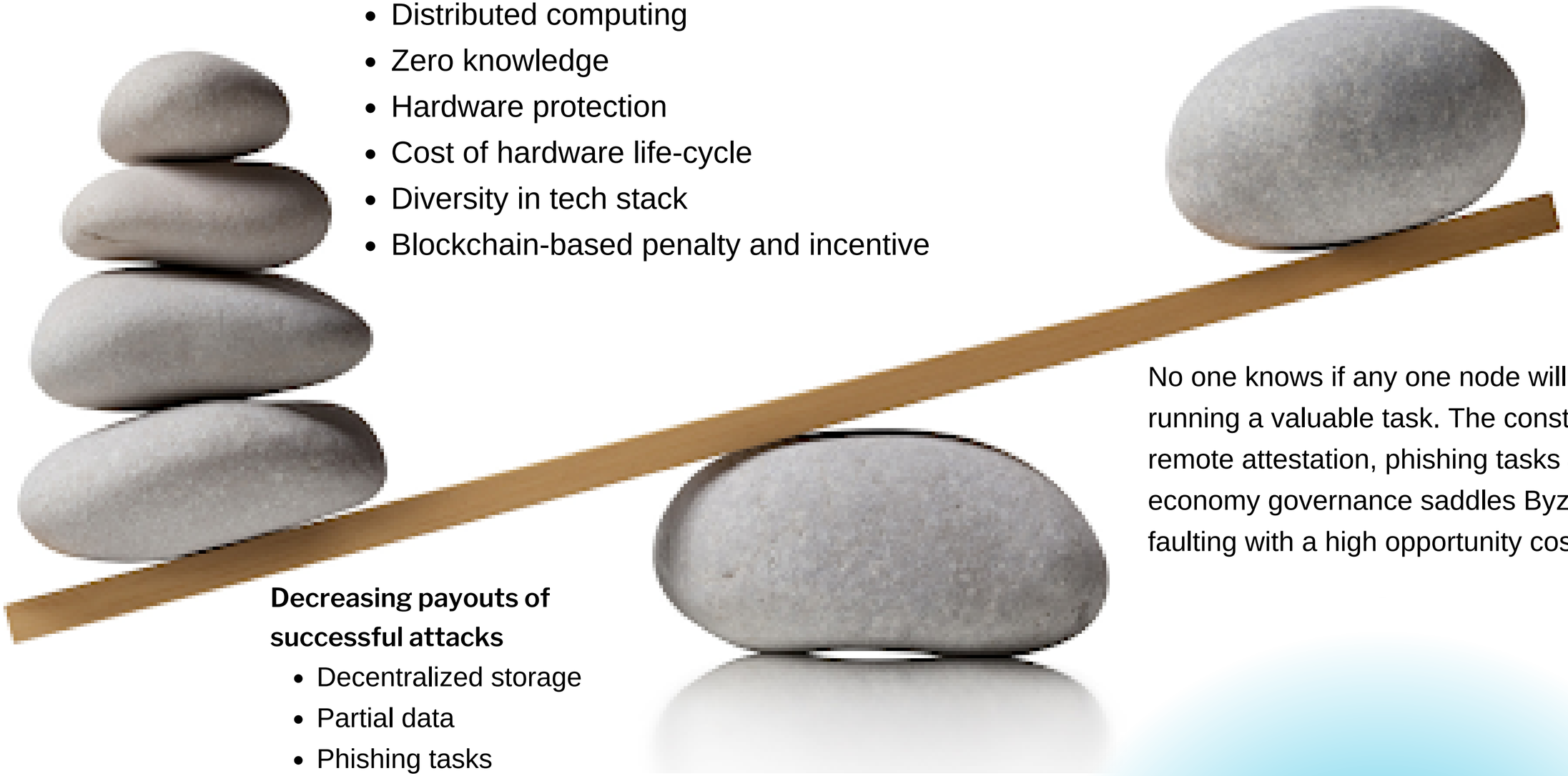
But in the TEA Project, dApps run inside hardware protected enclaves on layer-2. These dApp instances only need to run Raft without caring about BFT and let layer-1 handle BFT.



Punishing Bad Actors

Increasing cost of attacks

- Verifiable randomness
- Distributed computing
- Zero knowledge
- Hardware protection
- Cost of hardware life-cycle
- Diversity in tech stack
- Blockchain-based penalty and incentive



Decreasing payouts of successful attacks

- Decentralized storage
- Partial data
- Phishing tasks

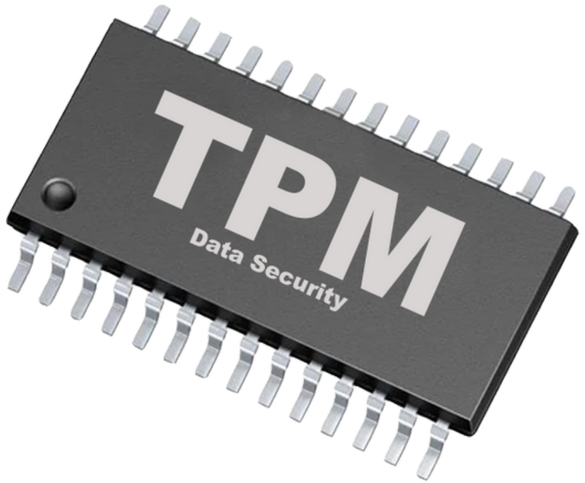
No one knows if any one node will be running a valuable task. The constant remote attestation, phishing tasks & token economy governance saddles Byzantine faulting with a high opportunity cost.

→

The TEA Project Hardware Support

The TEA Project's roadmap for supporting various Root of Trust (RoT) verification chains depends on the underlying hardware

Architecture	TEA Support	Technology	RoT Verification	Cloud IaaS for Rent?
Google Cloud / MS Azure	On roadmap	CPU-based	Centralized cloud	Yes
TEE SGX / SEV / TrustZone	On roadmap	CPU-based	Centralized by CPU manufacturer	No
Amazon Nitro	Completed	Similar to TPM	Centralized cloud	Yes
Trusted Computing (TPM)	Software simulator completed	TPM-based	Decentralized	No

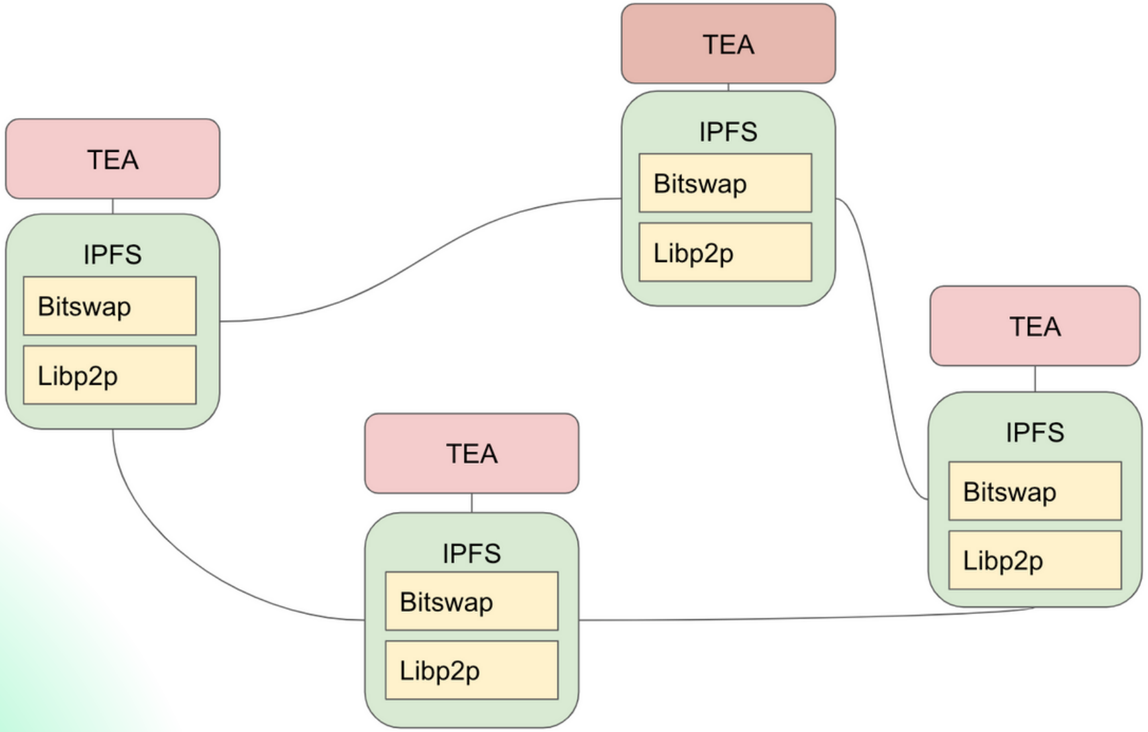


TEA Project = A Decentralized Cloud With Rich DApps

The TEA Project uses IPFS for storage & networking (LibP2P).

IPFS miners can install a TEA module (inexpensive devices with a TPM chip) to turn their mining machines into a Function-as-a-Service node.

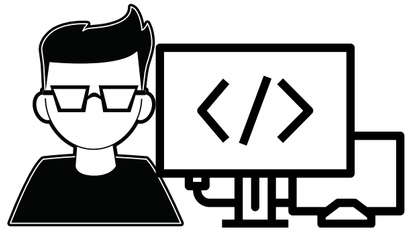
IPFS miners can now do more than just store data & code, they can execute it.



→

Example TEA Project Use Case

Data and code are uploaded encrypted to the TEA network



IPFS miners can add a TEA hardware module to mine both FIL & TEA tokens.

In this example, the end client, an AI researcher, uses the developer's Tensorflow image recognition app to analyze the photographer's pictures.

The developer, data provider, and miners hosting the dApp are all compensated in TEA tokens.

Trustless Process

The TEA Project takes care of the trust layer. This allows for a trustless experience between data owner, code owner, miners and clients.

→

The TEA Project's Two Tokens

Stable coin: TEA

• Utility token. Stable coin pegged to computing cost, not fiat.
• Used as gas, and has unlimited supply.
• No genesis block supply: every TEA needs to be mined.
• Born from public service rewards and burnt by DAO when CML seeds are bought at auction.
• Can be staked to Camellia for revenue sharing.

NFT: Camellia (CML)

- A TEA mining node can only be activated by associating a Camellia NFT with it.
- Miners buy new Camellia seeds through open bidding.
- Camellia has a life cycle determined randomly via an algorithm. DAO regulates the supply & burns it when it dies.
- Camellia has a technical stack used for diversity control.
- Investors can stake to Camellia-enabled mining machines for revenue sharing.

Miners

At the very beginning, miners buy CML to start pre-mining and earn TEA.

Presale Investors

Presale investors buy TEA to stake on miners and earn TEA revenue from their mining.

DApps

When dApps are deployed, clients buy TEA to purchase computing services (dApps). Miners earn the TEA from the clients and share the revenue with their stakeholders.

DAO Burns TEA

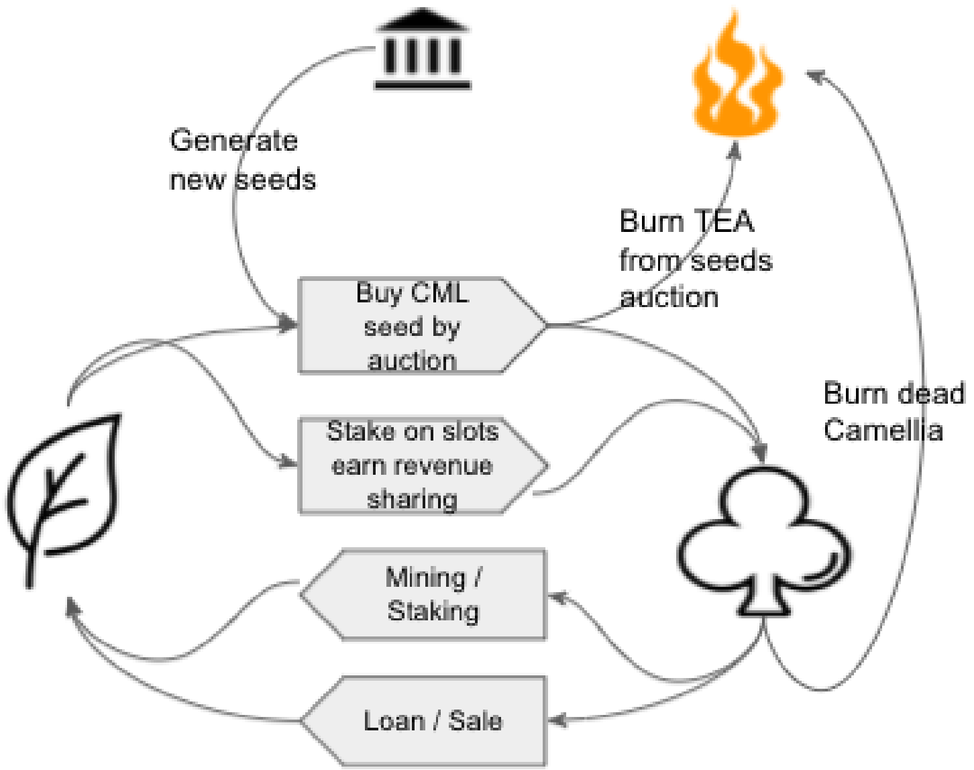
New miners joining the TEA network bid for new CML seeds necessary for mining. The DAO burns the received TEA payment from the winning bidder.

DAO Ensures CML Scarcity

The DAO generates seeds based on auction prices and maintains a reasonable scarcity of CML.
Each CML seed has a limited lifetime which adds to its scarcity.

→

CML Life Cycle



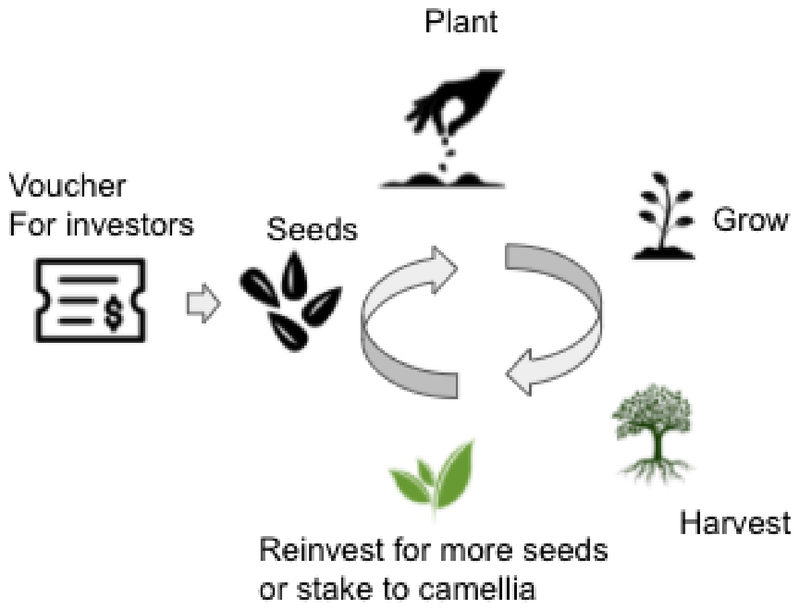
Early Stage Miner Economy: FOMO & Scarcity

Prior to the maturity of the TEA Project's Web3 Rich dApps ecosystem, a mining economy is necessary to keep the TEA economy running.

TEA’s carefully designed token economy creates NFT scarcity during mining. The scarcity encourages miners to reinvest their harvest back into CML instead of selling.

TEA doesn’t require a GPU, ASIC or a hard drive. It only requires the Camellia NFT and cheap secure hardware such as an RPi with a TPM chip.

Camellia Seed Vouchers & Funding Rounds



Funding rounds and voucher release schedule

	Team	Seeds round investors	A round investors	Private sales
Frozen seeds %	60	10	10	20
Defrost schedule	2 month lockup. 5% per month for 20 months	10% immediately, 5% per month for 18 months		

Funding Rounds With Voucher

Investors receive temporary seed vouchers (ERC20-like tokens on the TEA blockchain.)

Before pre-mining starts, vouchers are redeemable for randomly generated frozen Camellia seeds (the NFT).

During pre-mining, defrosted Camellia seeds are planted to TEA nodes and can begin harvesting TEA tokens at an accelerated speed for a short duration.

When public mining starts, everyone can start mining without needing a voucher.

Each Camellia Seed is Unique

Camellia seeds are unique NFTs. They each have varying defrost times, life spans, and productivity.

The TEA Project Will Also Host Bonded Token Sales

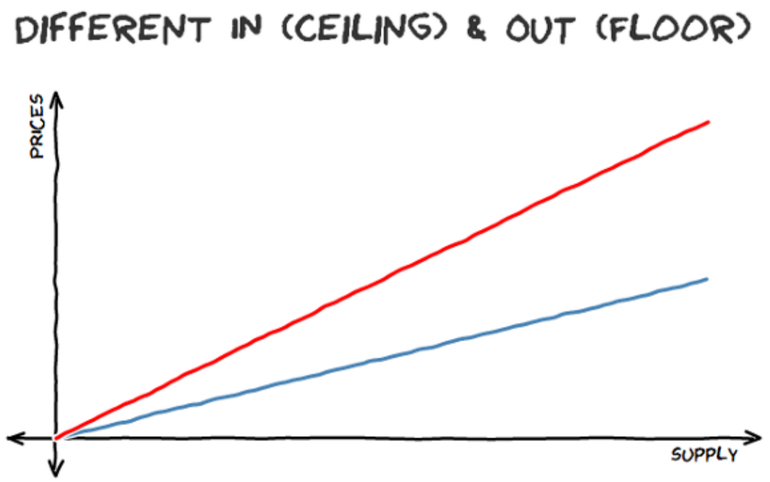
Bonded token sales help generate interest in the TEA Project network.

- The TEA Project will host bonding curves for dApp developers and other creators to monetize their ideas. Investors stake their TEA tokens on projects they believe will be more valuable in the future. Early adopters are rewarded for their investment as their token price increases when more people buy the project's token on its bonding curve.

- We envision bonding curves hosted on the TEA platform to encompass a variety of projects and contests. Bonding curve sales will likely be advertised by interested participants on their social media profiles. These various bonding curve projects act as another method of onboarding new users into the TEA ecosystem.

An example of a bonding curve sale

- A developer looking to launch a dApp on the TEA network could hold a bonding curve sale to generate early liquidity. Part of every sale goes to fund their project, and the other part goes to fund the project token's bonding curve.
- The project's bonding curve provides on-chain liquidity to enter and exit positions, providing security for investors. In the bonding curve below, the price increases as more tokens are bought. Investors buy at the red line and sell at the blue line where there will always be liquidity at each level along the bonding curve.



Core team and milestones

Kevin G. Zhang

- Founder of ELK Insight LLC
- CTO of iHealth Labs US
- https://www.linkedin.com/in/kevingzhang/

Zhijun (William) Zhang

- Lead, Security Architecture at The World Bank Group
- Enterprise Security Architect at The Vanguard Group
- https://www.linkedin.com/in/zhijun/

Yang Li

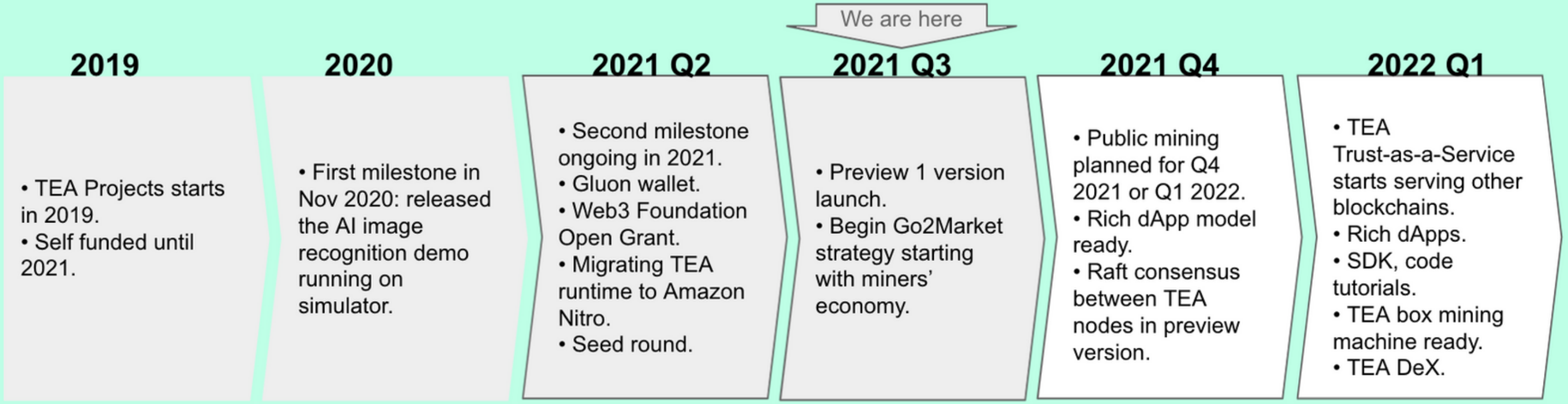
- Software Engineer of iHealth Labs Singapore
- System Architect of HP Shenzhen
- https://www.linkedin.com/in/jacky-li-4039747b/

Mingzhi Yan

- Software Architect of Cloudwalk Beijing
- Lead Blockchain Developer of Elastos Beijing
- https://www.linkedin.com/in/mingzhi-yan-7544b9203/

George Pornaras

- Content Writer at Luminus Sunnyvale / Xiamen
- Freelance Writer – Crypto & Cloud Computing
- https://www.linkedin.com/in/george-po/



TEA: Trusted Execution & Attestation

Run rich dApps on the blockchain at cloud speeds by leveraging silicon security.

teaproject.org

admin@teaproject.org