TEA: Trusted Execution & Attestation

Elevating Decentralized Trusted Computing to a T

www.teaproject.org

The TEA Project's goal is to make rich dApps run on blockchains at native speed and similar scalability as cloud computing yet still decentralized.

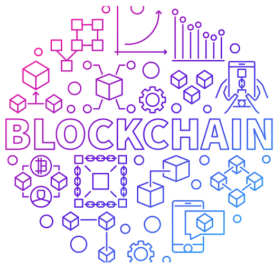
The problems

The existing Internet heavily relies on cloud computing. Cloud computing allows us to run complex and rich applications. However, cloud computing also comes with problems: a typical internet business model provides free service to customers. In return, the tech giants can use customer data to generate huge revenue.

The Internet has become more and more centralized over time. Very few tech giants take control of most internet traffic so that censorship and privacy protection become a big problem.

Centralization became a big problem. What about decentralization? Blockchain is decentralized, but it has other issues.

Rich applications cannot run on blockchain due to performance and scalability limitations. On the other hand, everything is open to the public on the blockchain by default. We need special treatment to protect sensitive information.



Decentralized but

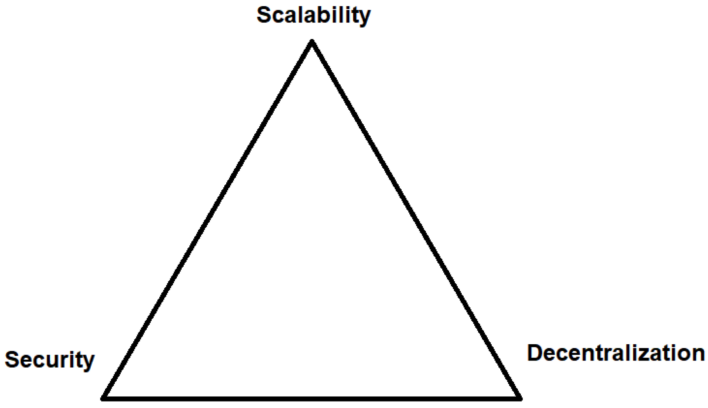
- Hardly run rich applications
- Need special protocol for privacy
- Pool performance

Run rich application with high performance but

- Centralization
- Privacy
- Censorship

The TEA Project's Innovations

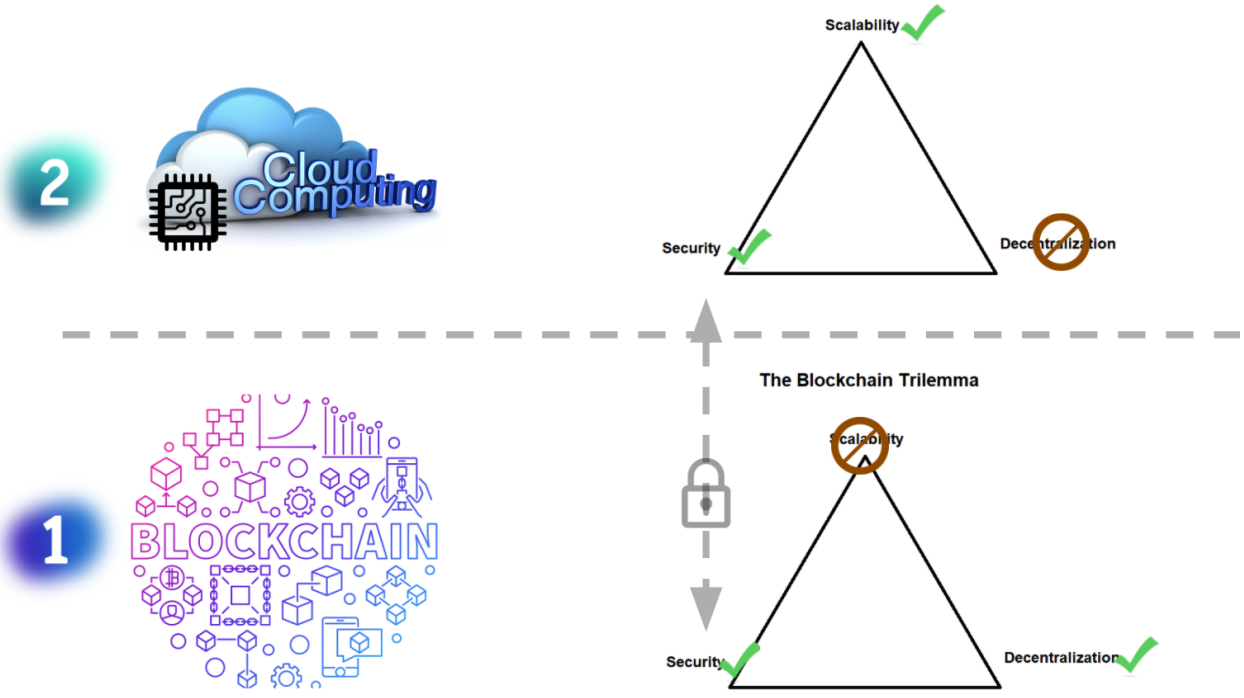
Trilemma



Termed by Vitalik Buterin, The Blockchain Trilemma addresses the challenges developers face in creating a blockchain that is scalable, decentralized, and secure — without compromising on any facet. This methodology also applies to cloud computing. Because cloud computing is centralized, it can gain security and scalability.

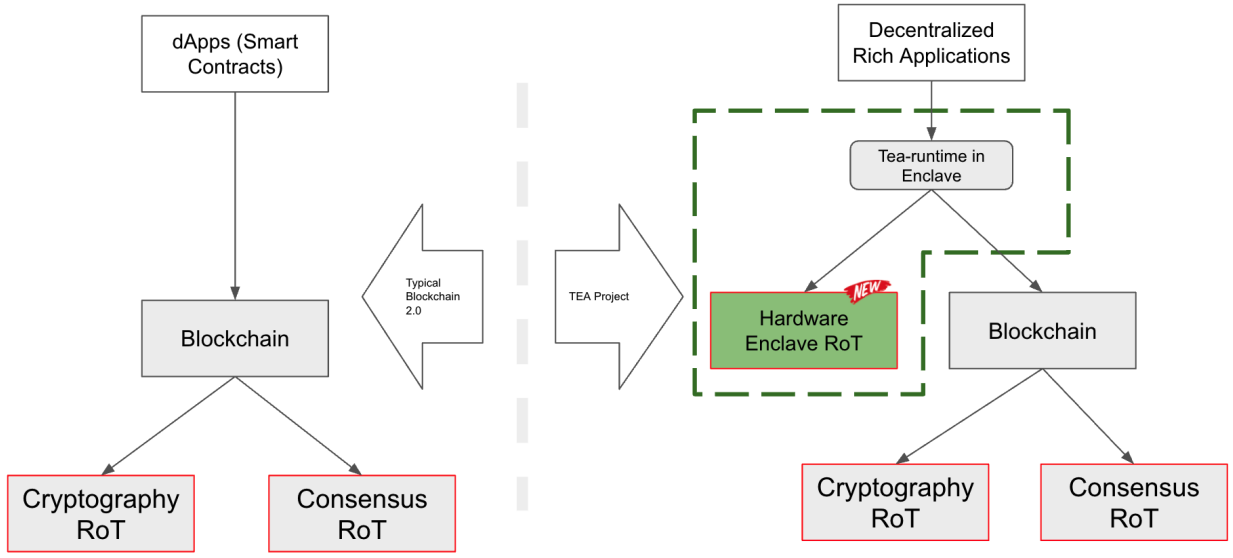
The TEA Project cannot violate the trilemma but try to solve the problem by separating the three concerns into two layers. Each layer has a compromise on one factor. We use a secure channel to bind those two layers together so that two layers work together to make an ideal environment

to run dApps.



Introducing the third Root of Trust(RoT): The hardware RoT

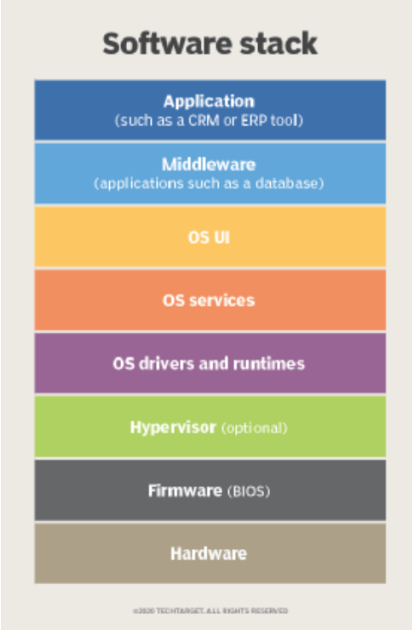
The secure channel between two layers is the hardware enclave. It is a newly introduced RoT (Root of Trust) besides the two existing RoTs (Cryptography and Consensus Algorithm).



The left side of the diagram above is the RoT tree of traditional blockchains. The right side is TEA Project's RoT tree. Instead of running dApps on the blockchain, TEA Project's dApps run in an enclave protected by hardware RoT. Blockchain becomes one of the two RoTs. Blockchain itself is guarded by the original two RoTs: Cryptography and Consensus Algorithm.

It is crucial to note that in the TEA layer 1 blockchain makes consensus decisions on different content than traditional blockchains. It ONLY makes consensus on the Proof of Trust provided by the hardware RoT. No more executing smart contract code and verify the result between other validators as traditional blockchains did. Verifying Proof of Trust is much simpler and faster, assuming that hardware is a Root of Trust.

Why is Hardware a Root of Trust

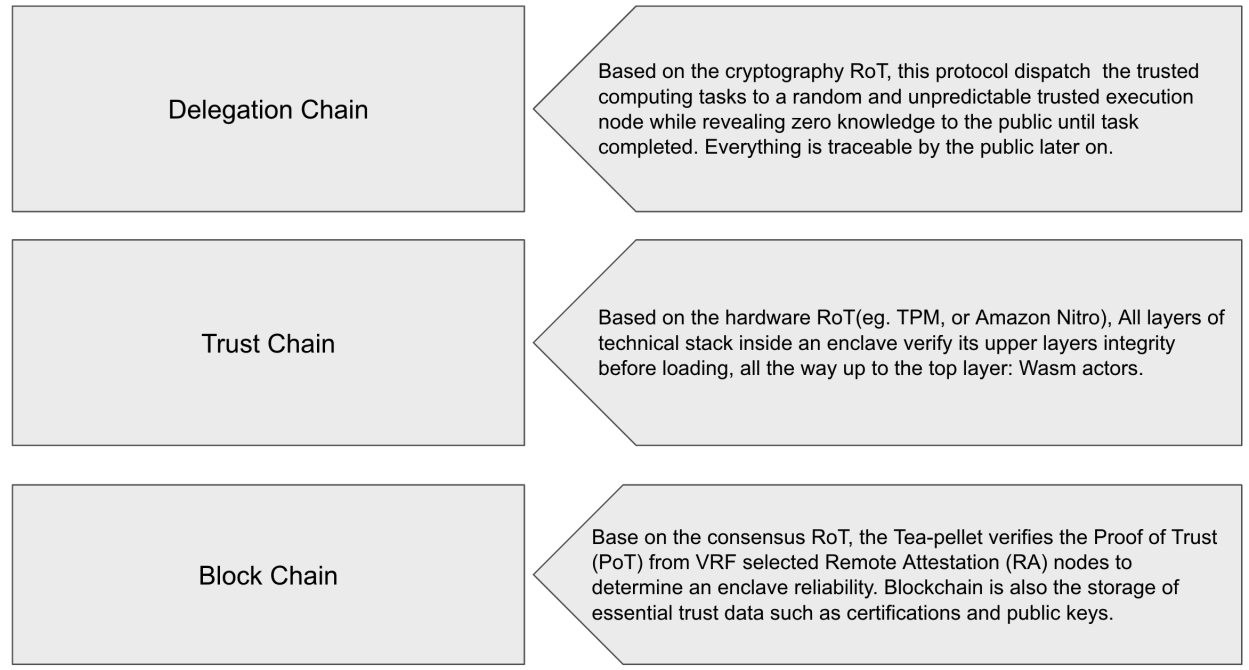


Software stack tells us that each layer of software relies on the underlayer to run. If the underlayer cannot be trusted, neither can the upper layer. You can see the bottom layer is hardware. That means if the hardware cannot be trusted, no matter how secure the other layers are, they are simply cannot be trusted.

Hardware has been used as a Root of Trust for many years. One example is that almost every computer produced after 2006 has a security chip called TPM embedded in the motherboard. It is the root of trust used by OS for decades. Most smartphones have such a chip as well. Modern CPUs have similar enclave technologies too. Even cloud computing platforms started to provide hardware-based trusted computing services such as Amazon Nitro to clients that require high-level confidential computing IaaS.

The TEA Project does not reinvent wheels by making new hardware technologies. TEA is just leveraging existing secure hardware technologies, such as TPM, SGX, or Nitro, and using them in the blockchain world.

Three Logical Chains Rooted from Three RoTs



From the three RoTs, we designed three logical chains to make the TEA project a trusted execution and attestation environment. This is where TEA's name comes from. TEA is short for "Trusted Execution and Attestation."

From the bottom up, the first chain we are talking about is the Blockchain made by Substrate. As explained before, we do not run our clients' dApps on the blockchain directly. Instead, we only run Proof of Trust consensus on our layer 1 blockchain while dApps run inside layer 2 tea-runtime. The PoT verifies every tea-runtime to make sure it runs inside a qualified enclave. The PoT consensus uses VRF to select random Remote Attestation nodes (RA) to challenge the testee for attestation documents signed by hardware. If the majority (⅔) of RA nodes get a positive result from verifying the attestation document (positive means verify pass), the consensus will mark this testee as "good to use." Because only approved "good to use" nodes can be selected as RA nodes, as long as we can already maintain more than ⅔ TEA nodes are honest, we could trust the consensus result. To keep the ⅔ threshold, we need to bootstrap clear and control the birth rate, which will be explained in the later "seeds" session. We also store the essential trust data in the blockchain, such as certifications and public keys, because blockchain is immutable.

The 2nd chain is the Trust Chain. The first node of the trust chain is the hardware RoT. It could be a TPM chip, Amazon Nitro, or Intel SGX. The RoT can generate other key pairs and hold the private key inside the hardware chip NVRAM. Please note that the hardware is designed never to reveal the private keys out of NVRAM. Other follow-up nodes can use software modules to generate their secret using the parent nodes' key pairs so that all of them can pass cryptographic verifications. They chain up one after another to become the trust chain. The root of the chain is the hardware RoT. Because the public key of the RoT is stored in the Blockchain publicly, anyone can easily verify any derived secrets by tracking back the hardware RoT, then verify the RoT using Blockchain.

The topmost chain is the Delegation Chain. In most applications, secrets need to be transferred

from one enclave to another. We call the first node “pin” the secret, and other nodes receive this secret “repin” node. The repin nodes will keep signature data pointing to the parent node where it “pin” from. The head node of the chain is usually a node selected by layer 1 blockchain under consensus. The head node’s parent link points to the block, which anyone can verify. So the delegation chain records the delegation relationship between different enclaves as proof of delegation. Every enclave involved in any task needs to verify that this task’s source is “clear” by verifying the delegation chain. This is also traceable evidence in case of any potential malicious behavior. The blockchain can be used for judging and punishing nodes for wrong behavior.

We call these logic “chains” because the idea of blockchain inspires us. One new fact is based on previous facts that anyone can easily verify. If a bad actor tries to temper with the facts, he has to change all the way back to the first fact. Unfortunately, the first fact is the RoT which cannot be altered.

Defeat Attackers by Technologies and Economics

Although we carefully design all three chains. It is impossible to build a 100% secure system. What we have done is to make attacks too expensive to afford while the reward is too little.

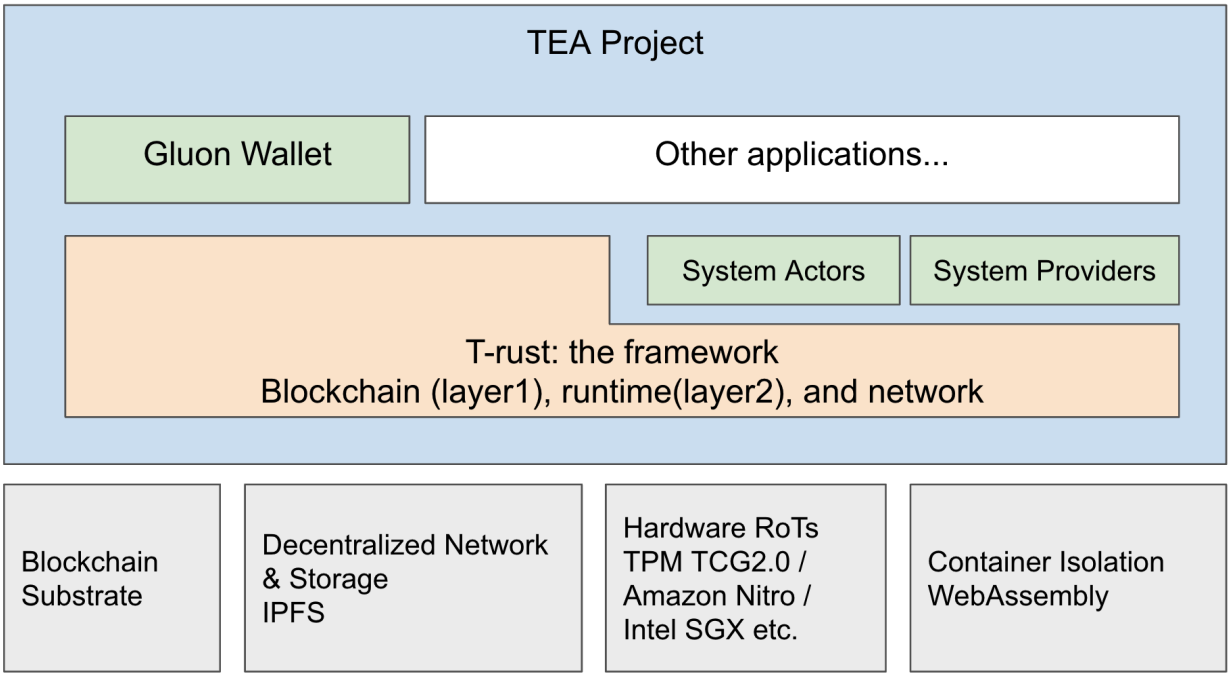
We design our protocol to reveal as little as possible information by keeping all the secrets inside the enclave (executable code and data). Anyone cannot know or predict which node is running valuable tasks. Hacking a random node at a relatively high cost is not worthy.

Every node needs a deposit and sometimes has to bid for the “seed” to join the TEA network. While work honestly can gain credit score as rewards (we call it Camellia, more info is in our token economic white paper). If any bad actor tries to alter its own TEA node to cheat the system, the constant random remote attestation can find and run through a penalty which costs

a significant loss on both token (TEA) and credit score(Camellia). Not to mention we have phishing police patrolling.

To reduce the surface of attacks, we minimize the TCB (Trusted Codebase) by introducing our minimized NixOS and wasm runtime that runs inside the enclave. No matter the code is TEA system actor or guest dApps only verified WebAssembly code could be loaded and run in our tea-runtime. All the hash and signatures can be verified on the blockchain layer 1. If an attacker tries to cheat the system, he has to cheat the blockchain first. It is very hard.

the Implementation



TEA uses many other open source technologies in different layers of our tech stack.

- Substrate: We develop layer1 blockchain using Substrate from Parity
- IPFS: TEA's data storage and p2p network is based on IPFS/ Libp2p
- TCG2.0(TPM)/Amazon Nitro/Intel SGX: TEA doesn't invent new hardware technologies. We are compatible with major existing or future hardware enclave technologies.
- WebAssembly: Our tea-runtime is a wasm runtime specially designed to be running inside an enclave. It is heavily inspired by and forked from the WaSCC framework by Kevin Hoffman.

TEA's code is written 90% in Rust, 5% in Golang, 5% in Javascript.

Enclave Technologies Compatibilities and TEA Box

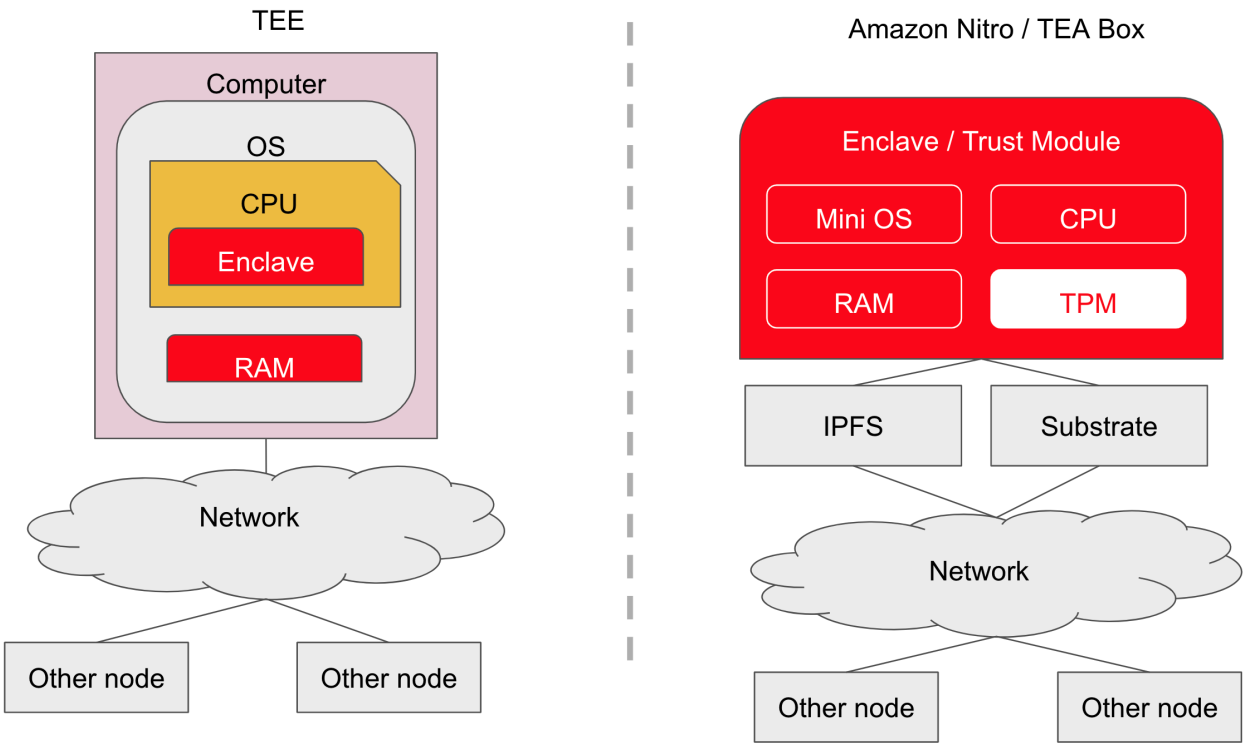
The following table lists the major enclave technologies and service providers.

	TEA Support	Technology	RoT Verification	Cloud IaaS 4 Rent?
Google Cloud / MS Azure Confidential Computing	On Roadmap	CPU Based (AMD/Intel)	Centralized Cloud	Y
TEE SGX/SEV/TrustZone	On Roadmap	CPU Based	Centralized by CPU manufacturer	N
Amazon Nitro	In Development	TPM Based(?)	Centralized Cloud	Y
Trusted Computing (TPM)	Software Simulator Completed	TPM Based	Decentralized	N

As of March 2021, we are able to complete the simulator of TCG2.0 compatible TPM. We are working on Amazon Nitro and hopefully finish it by Jun 2021. Once it is done, miners do not need to build their own TEA Box(the mining machine powered by TPM chips). They can simply rent an Amazon EC2 instance with Nitro support to start mining. Nitro is likely to be our first type of production-ready TEA node. After that, we will release a technical reference of TEA Box so that anyone can build their own or buy manufactured mining machines at a very low cost (our testing prototype cost less than $100).

CPU Enclave vs. TPM Enclave

One commonly asked question is why TEA Box uses TPM instead of well-known Intel SGX Enclave technology. They are very different approaches to the same goal. TEA supports TPM today and will support SGX or other CPU enclaves in the future.



Intel SGX and other CPU-based TEE create an enclave inside the CPU, but TPM based enclave protects a minimized computer or virtual machine inside. Given there are very few CPU manufacturers but many TPM manufacturers, TEE is potentially more centralized than TPM. On the other hand, TPM is much cheaper and less energy greedy, so that it could be used in small electronic devices such as Raspberry Pi or IoT, which Intel CPU could not fit.

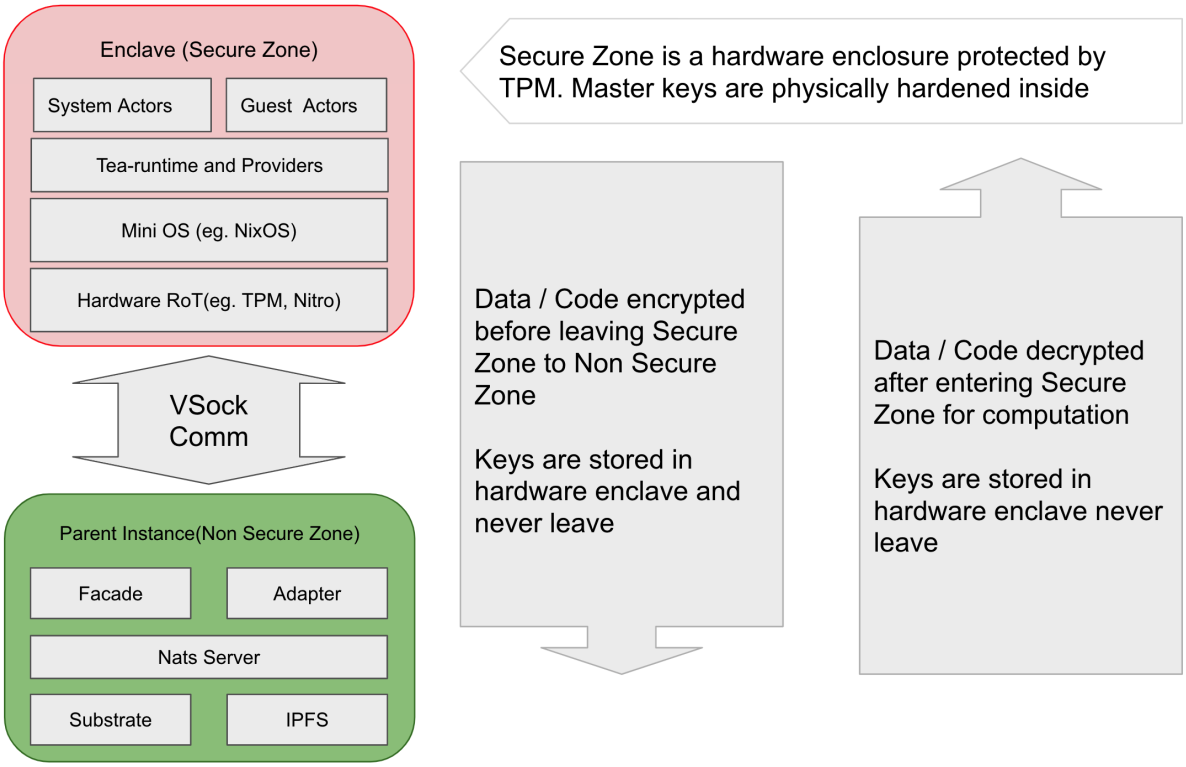
Modules Inside and Outside of the Enclave

Let's use TPM (or Amazon Nitro) as an example to explain the modules inside and outside of an enclave.

To reduce the TCB(Trusted codebase) size to minimize the attack surface, only those who can access secrets can reside inside the enclave. Not only are they carefully selected, but they are also carefully stripped to just small enough to run the wasm actors. For example, the mini OS (we use NixOS in our current implementation) only contains minimal libraries that can launch Tea-runtime, our stripped version of WaSCC.

The enclave is a fully isolated environment to the outside world. The only way to talk to the outside is the vsock channel heavily monitored by the tea-runtime.

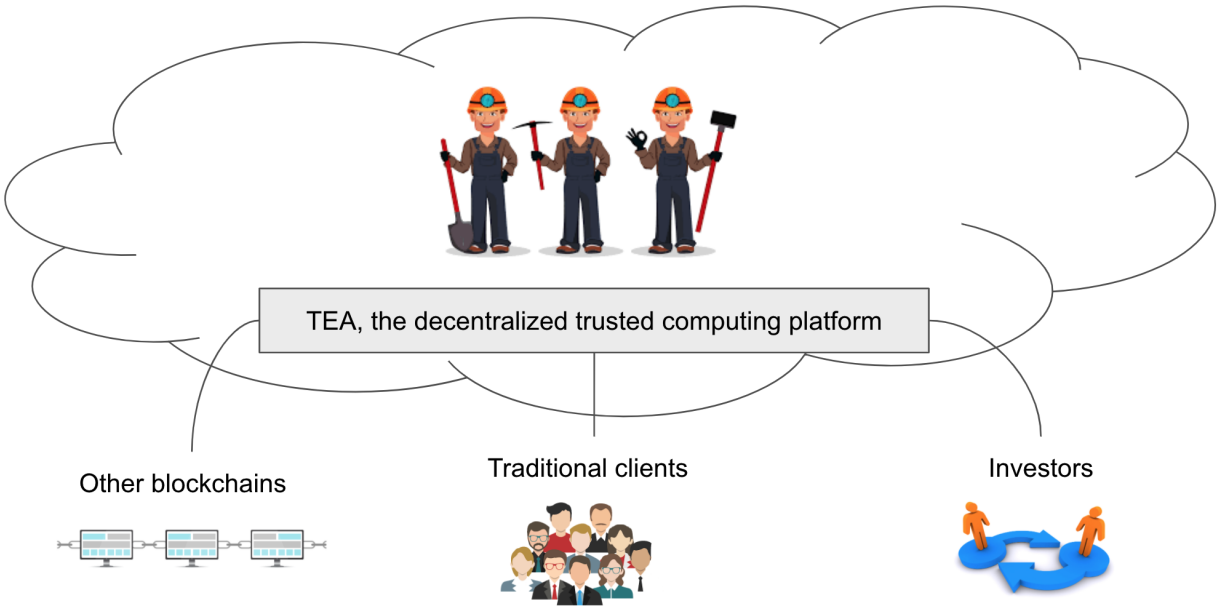
Only wasm code is allowed to run in the tea-runtime. Not only because wasm is so far the safest container technology, but also because the execution is measurable, just like gas measurement in Ethereum. Measurable is very important as tea-runtime can measure how much TEA token miners earn.



No matter system actors or guest actors, even the tea-runtime and NixOS are measured when the system boots by TPM. Even a single bit modification can be noticed by the TPM chip and reported to the remote verifiers when running the Remote Attestation Process (RA). Any node that cannot pass RA is considered malicious and won't handshake with other nodes. Any fault in RA will be recorded in the blockchain and result in severe penalties.

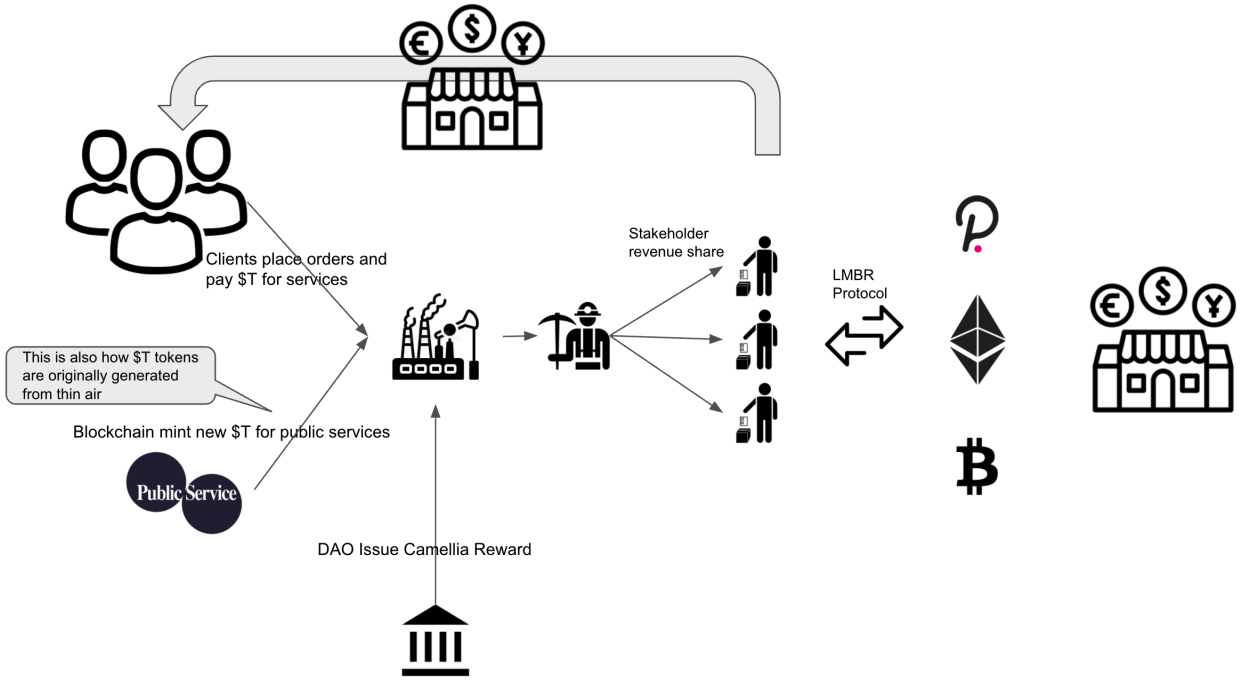
Other modules such as blockchain, IPFS, all adapters or bridges reside outside of the enclave because they have no access to secrets. They communicate with actors inside the enclave using vsock. Any secrets leaving the enclave will be encrypted before entering the vsock channel.

Ecosystem and Token economics in Brief



Unlike centralized traditional cloud computing service providers, TEA won't own or run any servers. Instead, like Uber, Airbnb, or any blockchain operators, it is not TEA but individual miners who run actual servers. What TEA provides is just Trust-as-a-Service.

TEA is a DAO consisting of miners, developers, clients, and investors. Developers compile dApps to wasm modules then deploy to TEA. Clients or developers pay to use the dApps while miners earn the gas fee measured by the TEA protocol. Investors can stake their tokens to share the revenue with miners.



TEA has two tokens. TEA and Camellia (CML).

TEA: TEA, the ticker of the token, shortened as $T. It is a utility token. It is used for mining revenue and service fees (aka Gas in Ethereum). It is a stable token pegging to the measurable computing resources.

Camellia：Sometimes called "Tea Tree." It is the governance token in TEA DAO. It also represents the credit score and profitability of miners. Camellia has a limited supply.

In addition to the two tokens, there is another concept: "Seed." The seed is not a token but a qualification similar to "headcount." It is used to control the number of new miner nodes allowed to join TEA at any given time window. When more miners want to join, they need to obtain miner qualifications through bidding. Miners earn service fees TEA by executing customers' computing tasks assigned by the system. In Ethereum and other blockchains, this concept is usually called Gas. Camellia represents the level of miners. The higher the Camellia, the higher the probability that the miner will obtain high-value computing tasks, and the higher the community responsibility and voting power. Inside DAO, Camellia is also considered an equity token. The owner can stake (lock-up) Camellia to a delegate miner so that they can share part of the revenue from this miner. Camellia represents profitability so that it can also be used for the credit value when used under collateral loans.

The TEA token economics is a complicated system. Please read the economics white paper for detailed design. We only list a few design principles here as a brief

- By introducing, we create underlying support for Defi that supports under collateral lending
- Through the unmodifiable constitution and modifiable community governance, the interests of early participants and late participants are taken into account so that the project can benefit from early investors while always maintaining metabolism for long-term development
- Create a legal utility token to avoid legal risks
- Automatically adjust liquidity, allowing speculation and investment to be controlled, and profits coexist

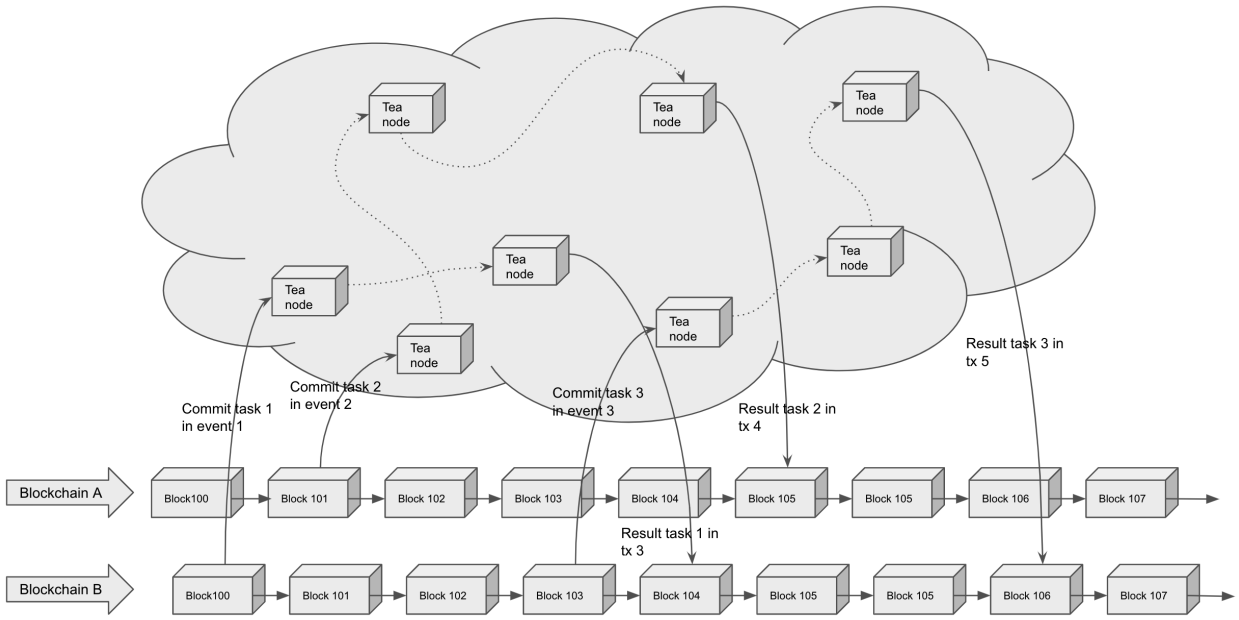
Use Cases

TEA does not aim to speed up smart contracts but enables a new kind of Rich Decentralized Applications on blockchains.

There are multiple types of use cases.

Backend Decentralized Trusted Computing Services to Smart Contracts

TEA as a backend service to support complicated and expensive computation offloaded from smart contracts. It is an extension of off-chain workers of Substrate. TEA's first demo dApp showed how it works.



The client blockchains do not blind trust the result from TEA. They can query and verify the Proof of Trust of the TEA layer 1 blockchain. This model is similar to the blockchain oracle.

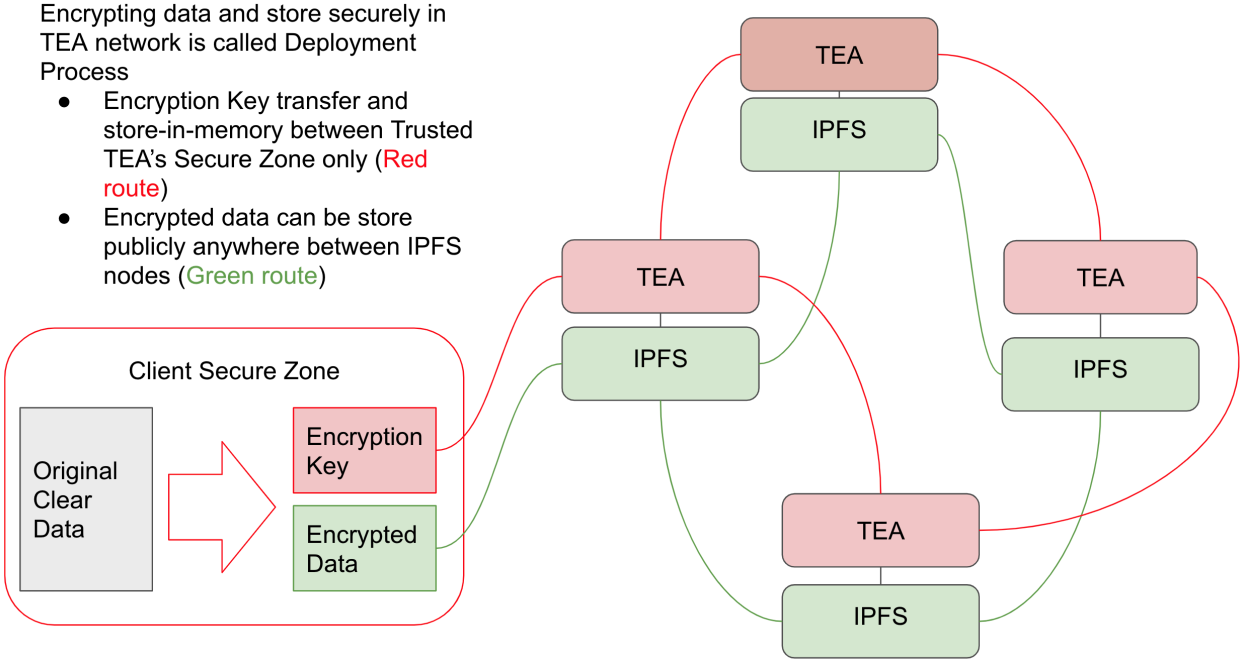
Add Computing Module into IPFS Miners, Turn it to Interplanetary Functions Service

There are miners who run the TEA nodes. Developers compile their dApps into wasm modules and update them to IPFS, then deploy the hash of code to TEA layer 1 as a "service." End users can run the dApps on web browsers or mobile directly from IPFS without any central app store or servers. All back-end services are requests/responses to the TEA layer2.

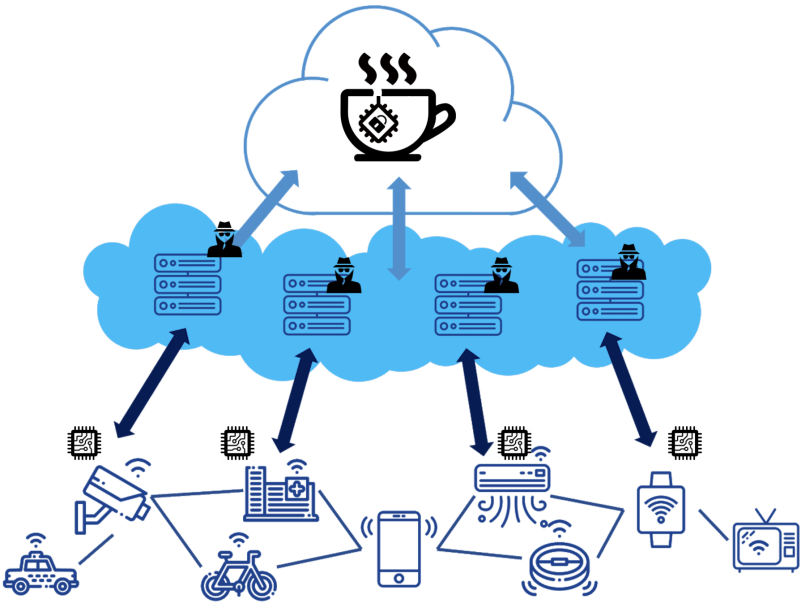
This kind of dApps has similar user experiences as a modern rich application, but it is decentralized. That means no one can take it off-shelf or stop the server. It is censorship-free and potentially runs forever.

Encrypting data and store securely in TEA network is called Deployment Process

- Encryption Key transfer and store-in-memory between Trusted TEA's Secure Zone only (Red route)
- Encrypted data can be store publicly anywhere between IPFS nodes (Green route)



Edge computing



In the future Edge Computing era, there would be a lot of data collection and process happening at the edge nodes instead of data centers. TEA can act as a decentralized source of trust that untrust parties can verify the PoT of others.

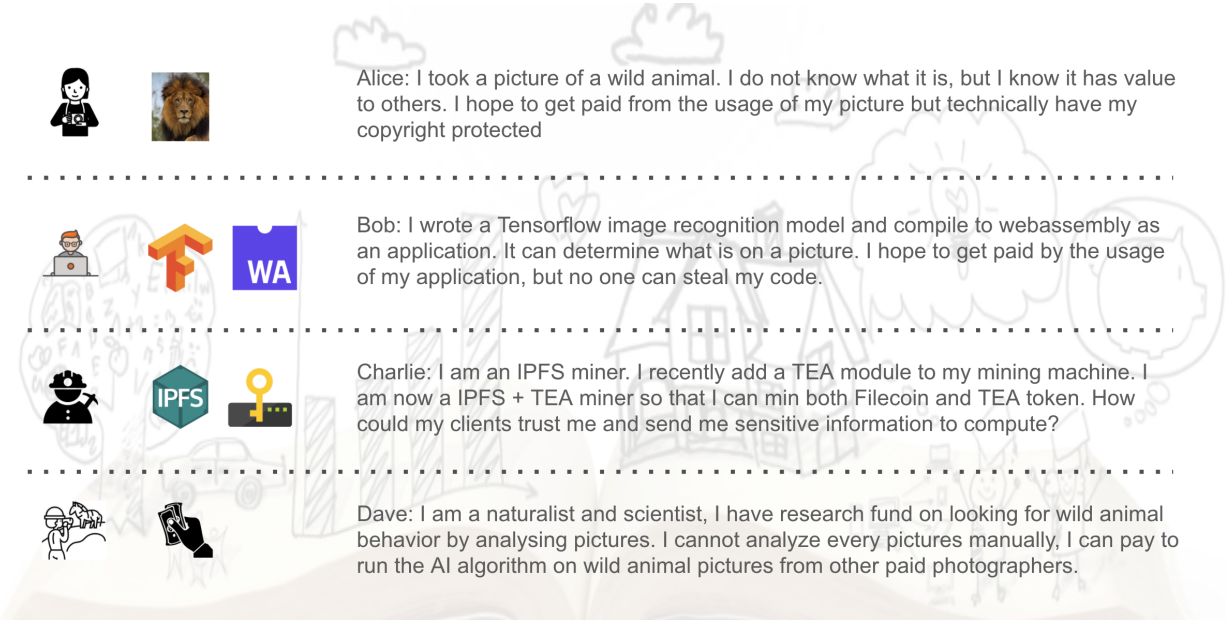
Due to the size and energy consumption, Intel SGX could not be the ideal solution for this case. TPM-based TEA Box could be the best fit.

The trusted computing can protect data right from the collection IoT sensors to the data pre-processing at the edge nodes, all the way to the Amazon Nitro protected data center. AI is also supported as we demoed in our first demo dApp.

Existing demos

Privacy Protection and AI on Blockchain

In Nov 2020, we developed our first demo dApps. Please go to our teaproject.org home page to watch the 2 full demo videos.

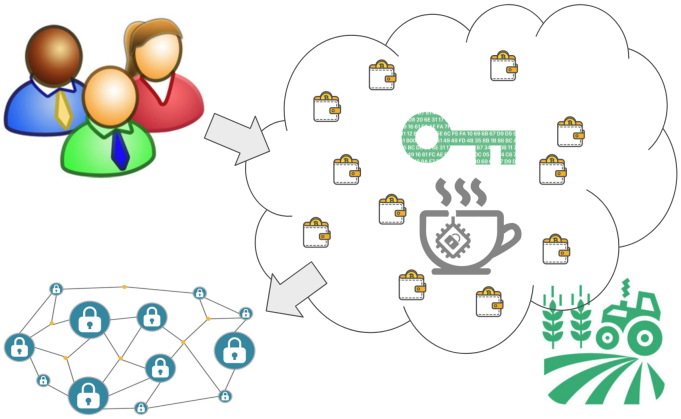


In this demo dApp, we showed how to run a Tensorflow image recognition application in the blockchain between untrust parties while privacy protected.

Gluon

Gluon is our second demo dApp, also used as our official wallet. It is a TaaS hardware crypto wallet service. It features

Gluon is NOT a hardware wallet, it is a blockchain powered TaaS(Trust as a Service) so that you do not need to own one

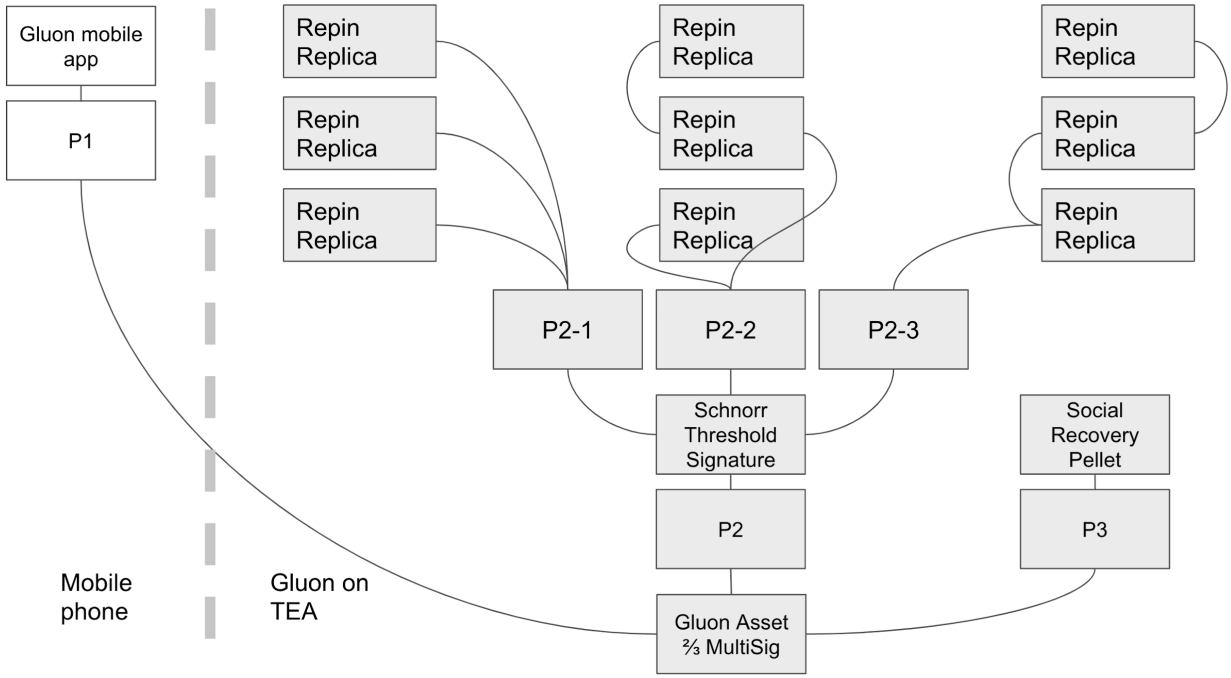


- Passwordless; users won't have to take responsibility for backup mnemonic phrases.
- Social disaster recovery is available for users who have lost all their authentication devices.
- Private keys managed by Gluon over the TEA network are randomly distributed and encrypted by TEA Nodes, which are hardware secure modules (HSM); it is a no-fail process.
- Tolerance of up to 1/3 compromised or failure nodes.

- Users only need to submit a transaction to Gluon, and it will take over the signing and committing blockchain.
- Leverages popular biometric technologies in mobile devices to attain better user experiences without compromising security.

It uses Schnorr Threshold Multisig Algorithm to disperse private keys to many TEA enclaves, but they do not know what they are.

All the under-the-hood complex logic is hidden behind the scene so that users only need to use it as if it is a typical cloud-based wallet without worry about security and private keys. If both computer and mobile phone are lost, users can still use social recovery to get back their assets.



The long-term goal of Gluon is not only a wallet but an entry point for all kinds of dApps. It will be embedded in TEA's typical Defi applications so that users can use it as the TEA portal.

Roadmap

TEA Project is a big and long-term open source project. It depends on many community developers' contributions to complete. TEA Core Team is only focused on the core consensus and low-level protocols. Essential utilities or interfaces can be built by individual squads from the community. They are rewarded by the development funding from tax income. DAO is in charge of the distribution of development funding.

Pre-seed

The TEA Project started in 2019. It was funded by founders without investors. During this period, the founders researched different tech stacks and make Proof of Concepts to verify ideas. Finally, we have overcome most technical challenges and made running demos.

Seed to private sales

With the fund from the seed round, we can set up a legal structure, a “C” corp. This C corp is the legit entity to own the IP and benefit of the TEA Project. Seed investors are the shareholders of this C corp.

During this period of time, the to-do list is

- Setup a DAO to initiate future token sales
- TEA layer 1 main net for token issuing only. No mining just yet
- TEA layer 1 test net for test mining. Not real tokens and won’t migrate to the main net later.
- Preparing for private sale

Private sales to pre-mining

DAO established in the previous milestone is the entity to initiate the token sale. The C corp is the technical supporter or contractor in the token sale.

At the private sale, investors pay crypto to buy seeds and initial CML. Both seeds and CML are limited supply at private sale. Investors who own seeds can start pre-mining at the end of this milestone. The amount of CML is an indicator of how fast he can harvest tea. The funding raised in this presale is used for the development and building ecosystem.

The to-do list for this milestone

- Amazon Nitro pre-mining ready. No external client tasks yet. Just for internal pre-mining
- System update feature ready.
- New miner provisioning
- Gluon wallet ready
- Miners portal ready

Pre-mining to public sale

Once pre-mining starts, all investors who join pre-sale can deploy their mining machine and starting mining. This is the privilege to those pre-sale investors as a reward. We will not open public mining before promised time spot so that pre-sale investors can harvest enough tokens without competition from the public.

The to-do list for this milestone

- LMBR protocol so that token can be circulated outside of the TEA ecosystem

- Create liquidation pool to major DeX preparing for IDO
- Public sale sites ready
- Marketing

Public sale to open mining

At public sale, public investors can join TEA IDO from major DeX. But they cannot join TEA mining until the end of this milestone.
Since TEA and CML are public exchangeable in DeX. Early investors can sale part of their tokens and exit. The vesting schedule is TBD.

The to-do list for this milestone

- TeaSwap (the DeX inside TEA) is ready
- API/SDK/Tutorial ready for external developers
- Mainnet ready to launch

Mainnet 1.0 lauch