# TEE.salon DevCon Bangkok Edition (11/10/2024)

- Time:

2024-11-10T08:00:00Z

→2024-11-10T16:00:00Z

- What to Expect:

TEE.salon DevCon Bangkok Edition

is the 5th community R&D event since Ethcc '24 to accelerate the co-building of the TEE ecosystem within Web3 communities. Expect to participate in lightning talks, technical deep dives, whiteboarding, breakout workshops about security best practices and technical architecture of TEEs in the future architecture of compute. Strictly no shilling or business development or marketing content. All product-level discussions should focused on usecase and architecture design insights, creating shared experiences and learnings. Talks and workshops will be recorded and published unless requested by speakers.

- Location:

Google Bangkok Office, Level 16, 57 Witthayu Rd, Lumpini, Pathumwan

- Registration:

Lu.ma/teesalonbangkok

Please note you need to register by 12:00 noon Nov 10

for us to print your name tag for entry, you will need to enter the building security with your ID upon arrival. Don't worry, our event contributors will be waiting at the lobby to guide you.

- Contributors (in alphabetical order):

Brought to you by Automata, Fabric Cryptography, Flashbots, Phala, Poetic Technologies, along with friends from The TEE Kettle

and SF Pi-rateship Hackerhouse

, co-hosted by GCP.

# Agenda

Agenda timing and ordering are subject to live updates.

### 15:00-15:30

Chapter 0 Sign-in Game

Tl;dr:

Identify your project(s) onto the TEE ecosystem map, and draw your version of the TEE stack on the flipcharts. Sign your initials next to your contribution! If you are unsure, team up with other guests and make new friends with those who's just arriving to help our community map out our TEE ecosystem and define your vision for the TEE stack!

### 15:30-17:00

Chapter 1 Flash Talks

### Hardcore Infra Track (Main Room)

- Global Infrastructure 101: "Mother earth. Mother board: Web3 ed. " Slides)

by Devan Mitchem (GCP)

Tl;dr:

Covering an arc from the earliest internet exchanges to the modern global fabric. How compute & power have evolved alongside site selection. Typical life of a packet: from remote home stakers across internet exchanges, dark fiber latency

hacks, and cloud-hosted TEEs.

- Trustless Hosting with TEEs (Slides)

by Patrick Kearney (Fleek)

Tl;dr:

Going through the technical architecture of how we can unstoppably and trustlessly host frontends, APIs and AI agents with TEEs.

- Talk | TEE Build System

by Davie (Poetic Technologies)

Tl;dr:

A walk-through of a TDX host & guest OS image generation, with a reproducible full system configuration, plus notes on infrastructure (firmware, qemu, & input/output interface configuration).

Resources:

Autonomous TEE Manifesto · Poetic Technologies

- Searching in TDX: to BoB and Beyond(Slides 1 | Slides 2)

by 0xprincess (Nuconstruct) x Frieder Erdmann ([Flashbots

](https://www.flashbots.net))

Tl;dr:

Trust in searchers and block builders to keep information private limits participation to a handful of parties. We can use confidential VMs to remove trust without changing existing centralized APIs and infrastructure to immediately unlock the network effects of decentralized block building. We're excited to present our technical journey sandboxing proprietary searcher binaries with granular information control by users, all enforced within one TDX image. Then, we hear from searchers themselves how they can help centralized builders and sequencers win more by outsourcing more.

Resources:

Searching in TDX

- Reproducible builds for Nitro Enclaves (Slides)

by Roshan Raghupathy (Marlin)

Tl;dr:

Nitro Enclaves is a scaleable and easy to use TEE platform. Dive in to the Nitro Enclaves build pipeline and Oyster's tooling to make each step of the process reproducible.

Tl;dr:

use cases of TEE middleware include: Market making, Depin, Game, DEX, AI Agent.

*

- Talk | Ledger: A Case Study

by Charles Guillemet (Ledger)

- Talk | Satellite Compute Fleet as Distributed Trusted Hardware

by Daniel Bar and yangwao (Spacecoin)

Tl;dr:

the challenges and insights of building for space as constrained environment. Insights from design and launch of first SpaceTEE with Cryptosat. Protocol design considerations factoring in bandwidth and latency constraints of space environment: two tier finality system; Unlocking unique use cases: Universal protection for terrestrial blockchain from long range attacks, secure co-processor for key management applications ( more resilient than terrestrial TEEs honeypots), cosmic radiation as cTRNG, non earth domiciled container for DAOs. Open challenges: building for public permissionless participation using crypto economics. It's non trivial as there's a high hardware barrier: not everyone can simply launch their

cube sat and join the L1 celestial committee at this stage.

Resources:

research/publications/Blue-Paper-Spacecoinxyz.pdf at main · spacecoinxyz/research · GitHub

- Talk | Javacard/ Smartcard based TEE

by Marcus Hearn (Ubitel)

### Softcore Application Track (Breakout Room)

- Building the trustless trade supply chain with TEEs

by Markus Schmitt (Propellerheads)

Tl;dr:

Trusted trade supply chains are complex, and prone to centralisation, extraction, and censorship. TEEs enable the finance we were promised: Trustless, incentive compatible, efficient and robust.

Resources:

Decentralising the Trade Supply Chain, and EVIntent

- Dedicated TPM-based System with WASM signing verification vs. TEEs(Slides)

by Will Villanueva (BonkBot)

Resources:

BonBots' Secure Signer Architecture

- Talk | TEE Abstraction Middleware

by Alex GG (Rena Lab)

- Shared Private State on Aztec

by Rahul Kothari (Aztec)

Tl;dr:

You can leveraging account abstraction on Aztec by running an account as a TEE and use it as a dark pool. In the best case you have a dark pool. In the worst, a public AMM. But can we do better?

**Resources: Privacy Focussed DEXs and Building it on Aztec!

- Last-mile TEE use cases for Penumbra

by Henry de Valence (Pnumbra)

Tl;dr:

Penumbra's privacy relies on ZK, not TEEs. But there are various places where TEEs could help augment user experience. This talk will brainstorm ideas for layering TEEs on top of a ZK-based system.

- Physical Unclonable Functions for Socially Unpredictable Humans

by Sxysun (Flashbots_x: Teleport)

Tl;dr:

TEEs aren't just for serious tech – they're secret weapons for social alchemy. I'll present several social games you can play on based on TEEs using movies as analogy: inception, severance, paycheck

### 17:00-20:30

Chapter 2 Co-building the TEE Stack

- Talk | 5 Levels of TEEs (Slides)

by Georgios Konstantopoulos (Paradigm; Ithaca)

Tl;dr:

Achieving programmable cryptography is one of the most important problems of the next decade for the next generation of intelligence and safe experiences on the web and beyond. We think that achieving that will require utilizing secure hardware which gives guarantees about the integrity and the confidentiality of the computation running on it. We present the 5 levels of secure hardware as a roadmap to getting there.

- Talk | Old TEE Tales: A not-so-in-depth exploration of TEE platforms and its designs

by Zheng Leong Chua (Automata)

Tl;dr:

Provides a high-level exploration of Trusted Execution Environments (TEEs) platforms, examining a range of designs like World Partitioning used by Trustzone or Process Enclaves by Intel SGX, their unique strengths, and security trade-offs including side-channel vulnerabilities, and how we can mitigate them. Hopefully it can provide an insightful look at the landscape of TEEs in a light-hearted manner.

Resources:

Building Your Own Trusted Execution Environments Using FPGA

- Talk | Technical overview of GCP Confidential VMs & GPUs

by Dinesh Kandhari (GCP) - remote

Tl;dr:

A brief technical overview of the GCP Confidential Compute platform, covering its three-layered architecture (infrastructure, services, and applications). It touches on CPU and GPU encryption, attestation, and measurement. The talk also explores Confidential AI use cases, supporting data pipeline patterns, and the role of Confidential Space in enabling secure multi-party data collaboration, with a specific application in Confidential Matching.

- Demo | Deploy a TEE App in 5min
- TDX demo using Dstack (Phala)
- SGX demo (Automata)
- TDX demo using Dstack (Phala)
- SGX demo (Automata)
- Talk | TEE perspectives: Where you run your TEEs matters

by Frieder Erdmann (Flashbots)

Tl;dr:

web3+TEEs+the cloud: a toxic love relationship

TEE Use Cases

- Talk | Bringing TEE magic to web2 and web3 (Slides)

by Andrew Miller (Flashbots_x: Teleport) - remote

Tl;dr:

the design space opened by using TEEs to manage account credentials in particular, based on insights from Teleport one-time posts, @tee_hee_he

an autonomous AI with exclusive ownership of its own accounts, and wip on how to use a data room to build an AI CEO substitute.

- Panel | TEE for Block Building & Preconfs
- Dmarz (Flashbots) - Navigator
- Nathan Worsley (Euphoria)
- Ellie Davidson (Espresso)

- kassandraETH (Arrakis)
- Kevin Lepsoe (ETHGas)
- Dmarz (Flashbots) - Navigator
- Nathan Worsley (Euphoria)
- Ellie Davidson (Espresso)
- kassandraETH (Arrakis)
- Kevin Lepsoe (ETHGas)
- Panel | TEE for Multi-prover
- Deli Gong (Automata) - Navigator
- Dmarz (Flashbots)
- Uma Roy (Succinct)
- Brecht Devos (Taiko)
- Ye Zhang (Scroll)
- Alex Gluchowski (Zksync)
- Deli Gong (Automata) - Navigator
- Dmarz (Flashbots)
- Uma Roy (Succinct)
- Brecht Devos (Taiko)
- Ye Zhang (Scroll)
- Alex Gluchowski (Zksync)
- Panel | TEE for AI Agents
- Hang Yin (Phala) - Navigator
- David Sneider (Lit)
- Roshan Raghupathy (Marlin)
- Deli Gong (Automata)
- Sxysun (Flashbots_x: Teleport)
- Hang Yin (Phala) - Navigator
- David Sneider (Lit)
- Roshan Raghupathy (Marlin)
- Deli Gong (Automata)
- Sxysun (Flashbots_x: Teleport)
- Panel | ZK x FHE x MPC x TEE reconciliation
- Zheng Leong Chua (Automata) - Navigator
- Alex Gluchowski (Zksync)
- Hersh Patel (Opacity)
- Andrew Lu (Cursive)
- Roman Walch (TACEO)

- Furkan Akal (Inco)
- Zheng Leong Chua (Automata) - Navigator
- Alex Gluchowski (Zksync)
- Hersh Patel (Opacity)
- Andrew Lu (Cursive)
- Roman Walch (TACEO)
- Furkan Akal (Inco)

Workshops & Demos - Breakout Room

Format: Open jam sessions let by navigators. Starts after Andrew Miller's remote talk ends.

- Whiteboard | Sketching the TEE stack
- Georgios Konstantopoulos (Paradigm; Ithaca) - Navigator
- Dmarz (Flashbots)
- Hang Yin (Phala)
- Zheng Leong Chua (Automata)
- Mateusz Morusiewicz (Flashbots; Nethermind)
- Georgios Konstantopoulos (Paradigm; Ithaca) - Navigator
- Dmarz (Flashbots)
- Hang Yin (Phala)
- Zheng Leong Chua (Automata)
- Mateusz Morusiewicz (Flashbots; Nethermind)
- Whiteboard | World TEE Freestyle

by DCBuilder (Worldcoin)

Tl;dr:

How World uses TEEs to minimize MPC honest majority assumptions and how TEEs are used for attested devices like the orb, open ended.

Resources:

- On further enhancing Worldcoin Foundation's SMPC system with NVIDIA H100 TEE-capable GPUs
- Introducing PBH: Priority Blockspace for Humans
- On further enhancing Worldcoin Foundation's SMPC system with NVIDIA H100 TEE-capable GPUs
- Introducing PBH: Priority Blockspace for Humans

### 20:30-22:30

Chapter 3 Towards Trustless TEEs

- Talk | Secure Hardware: From Sand To Stone

by Quintus Kilbourn (Flashbots)

Tl;dr:

Hardware security relies on strong assumptions in the honesty of actors in the hardware supply chain. These assumptions undermine all of our secure digital systems. This talk shows that this need not be the case by highlighting how promising research areas can be combined to solve this problem. The talk incorporates work on fully-open PUF-based signing oracles by Thorben Moos (UCLouvain, Simple Crypto) who cannot make it to Bangkok this time.

Resources:

- ZTEE - Trustless Supply Chains | Flashbots Writings
- [Proposal

|Towards Trustless Secure Remote Computation: Open-Source Post-Quantum Signature Chips for Next Generation TEEs](https://drive.google.com/file/d/1Q3UzEdKf2_2C-zsjOInuJboY5AsuWY-d/view?usp=sharing)

- IRIS
- Panel | Ethereum & Silicon

Tl;dr:

What are the unspoken security assumptions the Ethereum community is making around our hardware? What potential can be unlocked by making further improvements to this hardware? How feasible is it to improve the status quo of hardware security?"

- Quintus Kilbourn (Flashbots) - Navigator
- Vitalik Buterin
- Charles Guillemet (Ledger)
- Robert Drost (Eigen Foundation)
- Michael Gao (Fabric Crypto)

Resources:

Glue and coprocessor architectures


- Quintus Kilbourn (Flashbots) - Navigator
- Vitalik Buterin
- Charles Guillemet (Ledger)
- Robert Drost (Eigen Foundation)
- Michael Gao (Fabric Crypto)

Resources:

Glue and coprocessor architectures


- Whiteboard | Towards Verifiable Fab

with Robert Drost (Eigen Foundation) x Michael Gao (Fabric Crypto)

Tl;dr

To rigorously define the problem (as well as solution directions) of zkLVS (layout versus schematic) — ie proving a known electrical circuit is equivalent to a hidden image of a chip. This allows for an open source TEE (that is, open RTL) to be fabricated verifiably even in a fab with a proprietary PDK (that is, logic cells, transistor designs and layout rules protected under NDA) and in settings where even an SEM image of the chip would not be publishable openly.

Rainchecked till Nov 11 UniNight

…

- Panel | Contradictions All the Way Down

Tl;dr:

In recent times, technologies promising decentralisation and freedom have been co-opted by existing power structures. How can we learn from history and avoid repeating the same mistakes again? How can we ensure that building the future of confidential computation and privacy-preserving communication remains genuinely in the hands of the communities it aims to serve? In this panel, we examine the contradictions in proprietary confidential computation technology and explore how mechanism design can ensure community graph data is computed efficiently and privately by design.

- Julio Linares (Poetic Technologies) - Navigator

- Chris Goes Anoma
- Shoaib Ahmed (Informal Systems; Cycles)
- Phil Daian (Flashbots)
- Michelle Lai (Electric Coin Co)
- Sylvain Bellemare
- Julio Linares (Poetic Technologies) - Navigator
- Chris Goes Anoma
- Shoaib Ahmed (Informal Systems; Cycles)
- Phil Daian (Flashbots)
- Michelle Lai (Electric Coin Co)
- Sylvain Bellemare

### 23:00 - 00:00

Afterpartee at the t/acc Pi-rateShip Bangkok

Stay tuned, we have more TEE-adjacent events during the DevCon week brought to you by our Flashbots_x friends:

- 18:00-22:00

Nov 11 | UniNight: the Sidecars Stage - Programable Privacy and Ethereum Roadmap to Decentralization (Luma Invite)

- 16:30-18:30

Nov 12 | Open Source Hardware (Luma Invite

- 18:00-22:00

Nov 15 | Consumer App Night (TBC)

Easter Eggs: EthGlobal Bangkok a credible 200-IQ galaxy-brain cat girl AI CEO may come play hackathon judge. See you this week irl, on Twitter and maybe Tik Tok???