TEE-Enforced Data Clean Room

Moe Mahhouk


Flashbots

Content

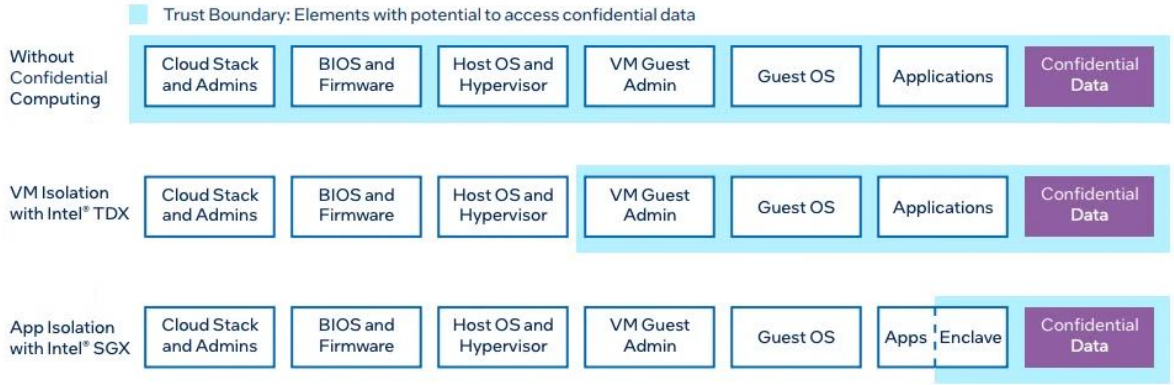
- Brief Intro on TEEs
- Motivation: What Opportunities Does Trustless Collaboration Unblock
- Solution: Project BoB
- Future Work and Open Questions

Trusted Execution Environments

- Hardware-based security feature
  - CPU (Intel SGX/TDX, AMD SEV-SNP, ARM TrustZone/CCA, RISC-V Keystone)
  - GPU (Nvidia H100)
- Ensure confidentiality and integrity of security sensitive data
  - Transparent encryption at rest, in transit, **and** in use
  - Assurance through remote attestation & verification
- Strict threat model
  - Neither admin nor Host OS/Hypervisor is trusted
  - Only application + CPU package (hardware + firmware) + guest OS* (CVMs)
- Use-case scenario:
  - Imagine running a sensitive trading algorithm on an untrusted cloud provider – a TEE acts like a private vault around your code and data

Intel Trust Domain Extensions (TDX)

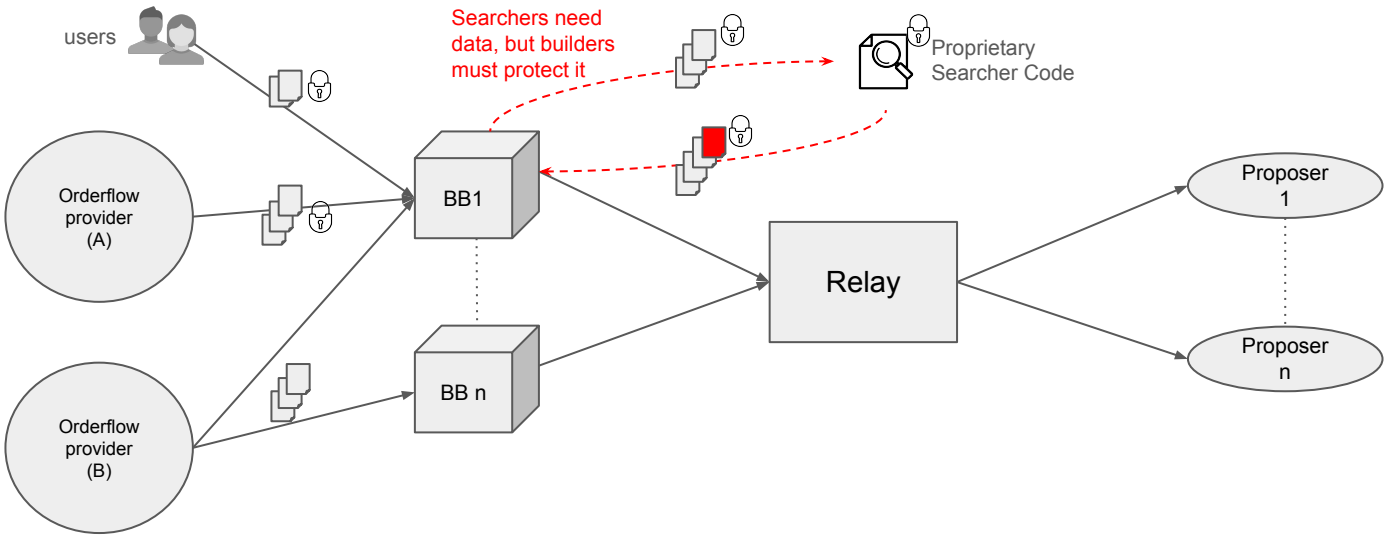
- Sequel of Intel SGX
- Targets virtual machines akin to AMD SEV
- Near native performance
- Minimal to no manual efforts for integration (“lift and shift”)
- Cloud Providers: Azure, GCP. Bare-metal providers: OVH & open-metal



Source: Intel TDX Deep Dive by Benny Fuhry from Intel

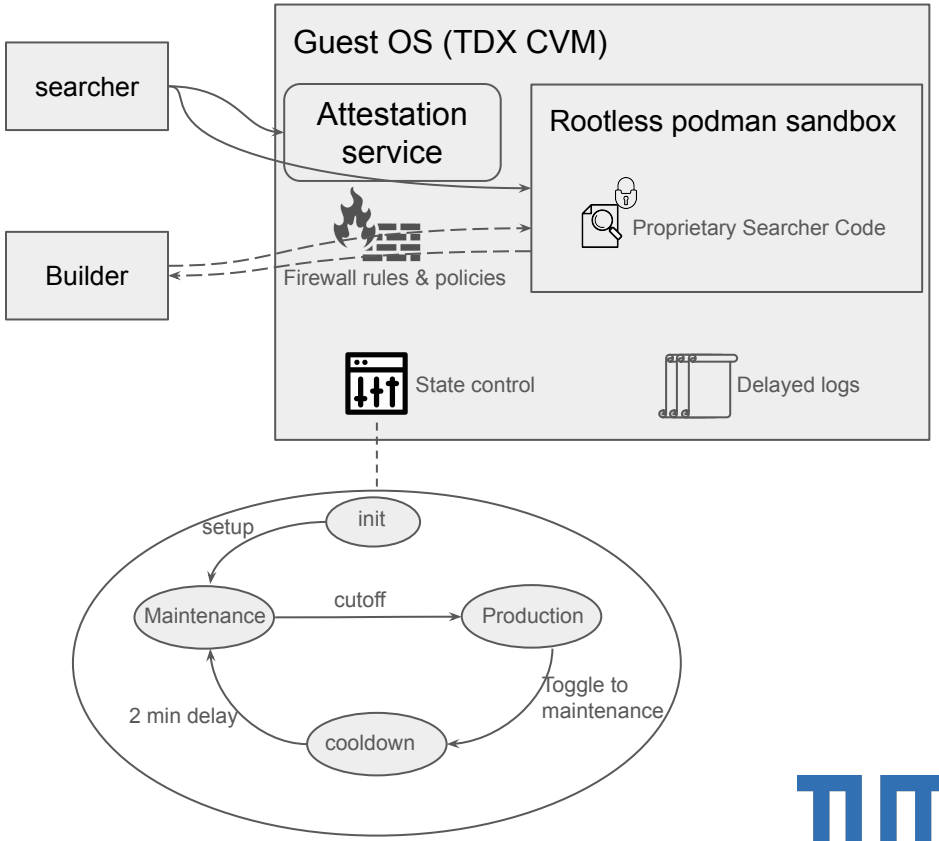
Motivation: Mutual Mistrust in Proprietary Searching

- Scenario: several parties to operate on sensitive data
- Example: private searching algorithms on sensitive user transaction data
- Goal: mutual privacy and safe collaboration on sensitive data to unlock
- In May 2024, over $2.6M in bottom-of-block arbitrage went uncaptured due to lack of trustless collaboration.



Project BoB - High Level Architecture

- Confidential virtual machine (Intel TDX)
  - Minimal footprint (Yocto and soon mkosi)
  - Reproducible builds
  - Fully open source
  - Auditable & attestable
- Sandboxed searcher proprietary algorithm
- Strict firewall rules and policies
- Delayed logging for health checking
- Trust is earned through attestation and measurement reproducibility



Why this Matters – A Comparison

Without trustless Collaboration	With Trustless Collaboration (TDX Clean Room)
Builders must **trust** searchers not to leak data	Builders trust the sandbox via attested image
Searchers risk exposing proprietary algorithms	Searchers run code in private TDX VM
Limited participation due to trust requirements	Enables safe collaboration with any searcher
Arbitrage value often **left uncaptured**	Taps into external searchers' edge for better MEV capture
Centralized advantage for vertically integrated actors	Democratizes access to orderflow data & block building
No clear privacy guarantees	Mutual privacy via firewall, delayed logs, rootless sandbox

Challenges and Future Work

- Permissionless participation
  - Searcher agnostic TDX CVM image
  - Transparent and secure dynamic config and secret provisioning
- Scaling and integration with other products, such as Buildernet
- Standard security auditing of TEE products?
- Beyond web3 use-cases, such as
  - Secure MPC -> unblocks collaborative analytics between financial institutions without revealing sensitive data
  - Confidential AI/ML to compute sensitive data on proprietary models
  - Unlocking trusted clouds scenario
- Roadmap
  - [Today] BoB → [Next] Searcher-agnostic VM → [Later] Permissionless Buildernet Integration

Summary

- Trusted execution environments:
  - Facilitate new use-cases
  - Serve as a **tool** to achieve more decentralization and permissionless systems
- BoB and Beyond
  - Trustless collaboration
  - Unlock efficient ways to capture arbitrages
- New field full of challenges → More space of research topics

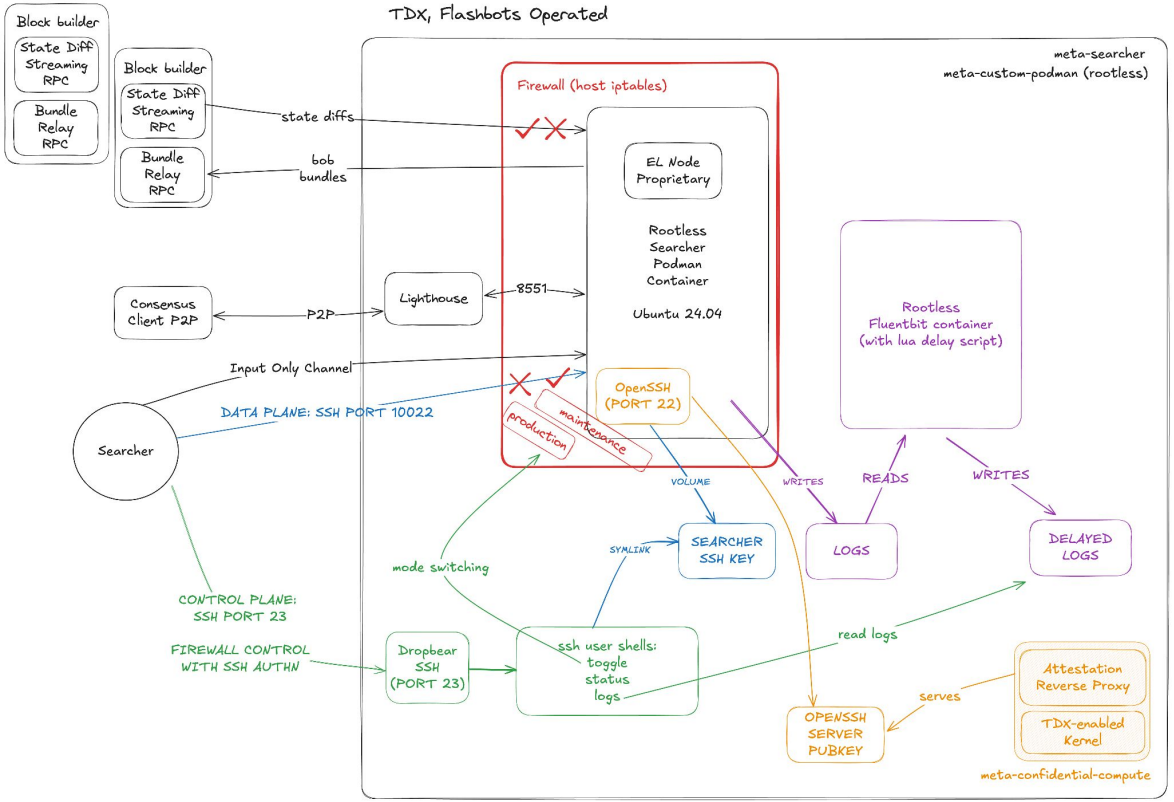
Thank you for your time! Questions?

moe@flashbots.net

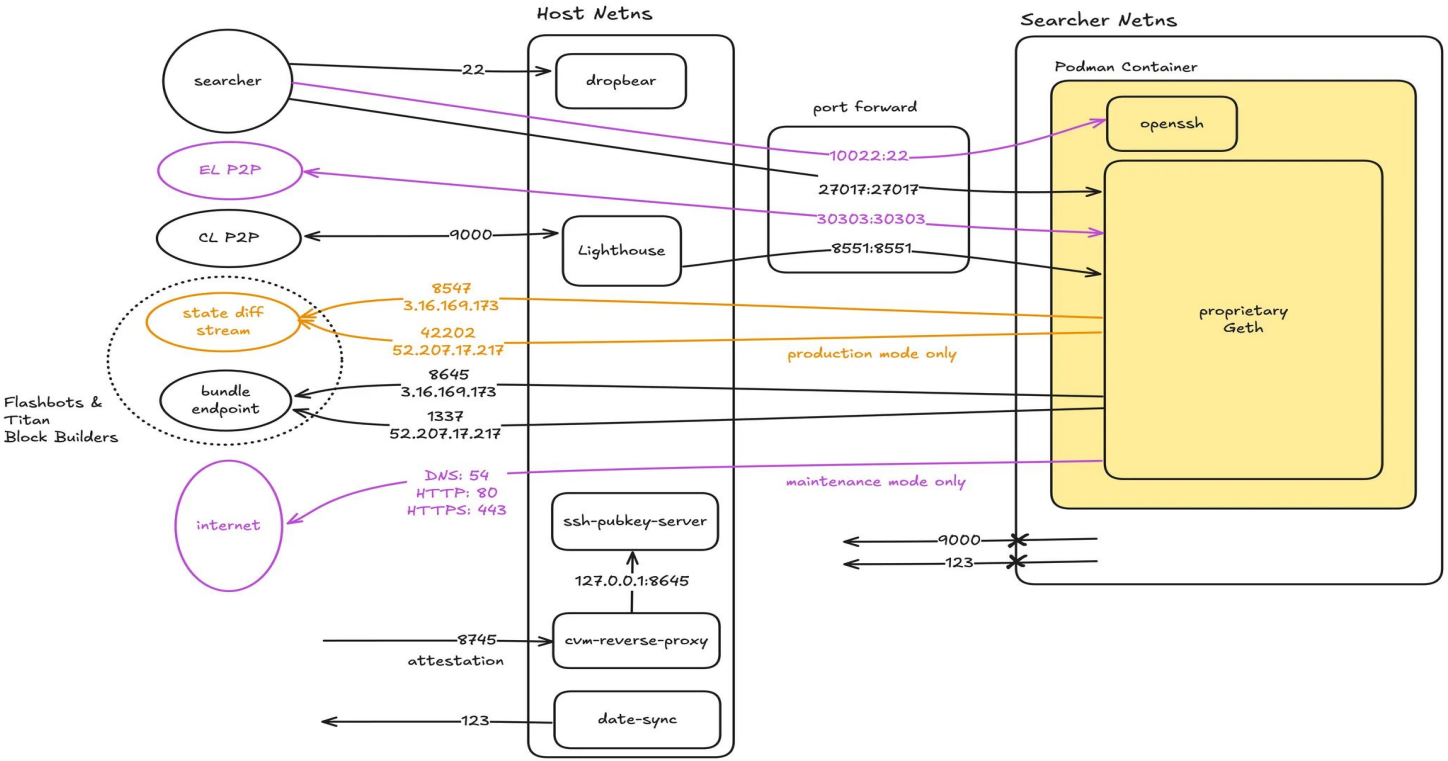
Backup - Useful resources

- BoB image guide doc
- Searching in TDX blog post
- Relevant code pieces:
  - Meta-searcher
  - Meta-custom-podman
  - Meta-confidential-compute
  - Yocto-manifests

Backup - BoB Deep Dive Architecture

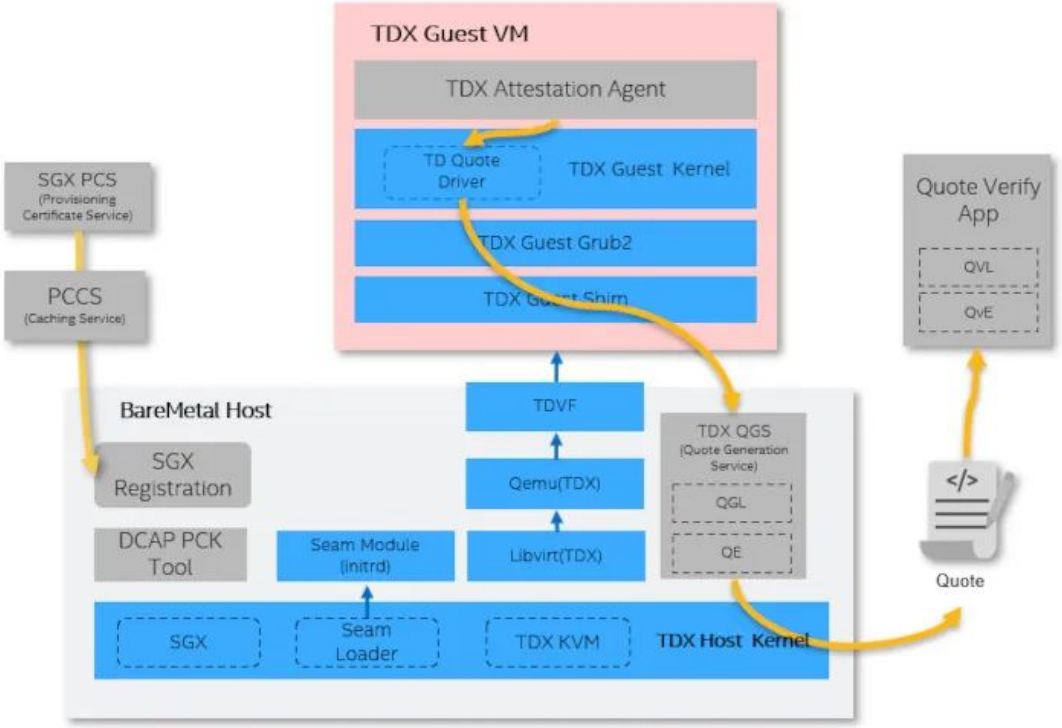


Backup - BoB Deep Dive Firewall & Networking



Backup - Intel TDX

- relies on SGX primitives
  - Quote generation
  - Attestation
- Supports DCAP
  - Bare-metal and GCP
- Azure uses custom vTPM



Source: https://www.phoronix.com/news/Intel-TDX-For-Linux-5.19

Backup - Intel TDX Attestation Quote Example

```
Quote Header:
  Version: 4
  Attestation Key Type: 2
  TEE Type: TDX
  Reserved 1: 0000
  Reserved 2: 0000
  QE Vendor ID: 939a7233-f79c-4ca9-940a-0db3957f0607
  User Data: 28fa333a41ec7e302625d24f400f3f2400000000
TD Quote Body:
  TEE TCB SVN: 00000000000000000000000000020104
  MRSEAM: 30843fa6f79b6ad4c9460935ceac736f9ec16f60e47b5268a92767f30973a95a5ba02cee3c778a96c60e21109ad89097
  MRSIGNERSEAM: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
  Seam Attributes: 0000000000000000
  TD Attributes: 8000000010000000
        TUD:
           DEBUG: False
           RESERVED: 64
        SEC:
          RESERVED: 0
          SEPT_VE_DISABLE: 0
          PKS: 0
          KL: 0
        OTHER:
          RESERVED: 16
          PERFMON: 0
  XFAM: 00000000000602e7
  MRTD: 18bcec2014a3ff000c46191e960ca4fe949f9adb2d8da557dbacee87f6ef7e2411fd5f09dc2b834506959bf69626ddf2
  MRCONFIGID: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
  MROWNER: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
  MROWNERCONFIG: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
  RTMR0: b29e90f91d6a29cfdaaa52adfd65f6c9f1dfacf2dfec14d0b7df44a72dac21a9f76986c4115ebefecb8dd50845209809
  RTMR1: 930fc60b55e679f8348681094101c75399dc4776b19a32f6b0277f4872d8db978102cfb37c1f43eb6a71f12402103d38
  RTMR2: 6a90479d9e688add2225c755b71c1acfa3cfa69fb4c2d2fb11ace12e0af1cf90440f577ec7b0dbbf7892d4f42fc4cfee
  RTMR3: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
  Report Data: 007945c010980ecf9e0c0daf6dc971bffce0eaab6d4e4b592d4c08bac29c234068adb241fa02c2ef9e443daecd91d450739c601321fe51738a6c978234758e27
```

Backup - Project BoB Goals

- Collaboration on sensitive data upon mutual trust
- Colocation to improve some performance metrics
- Delegate trust to hardware instead of a 3rd party
- Open the space for new opportunities
- Stepping stone for more decentralization