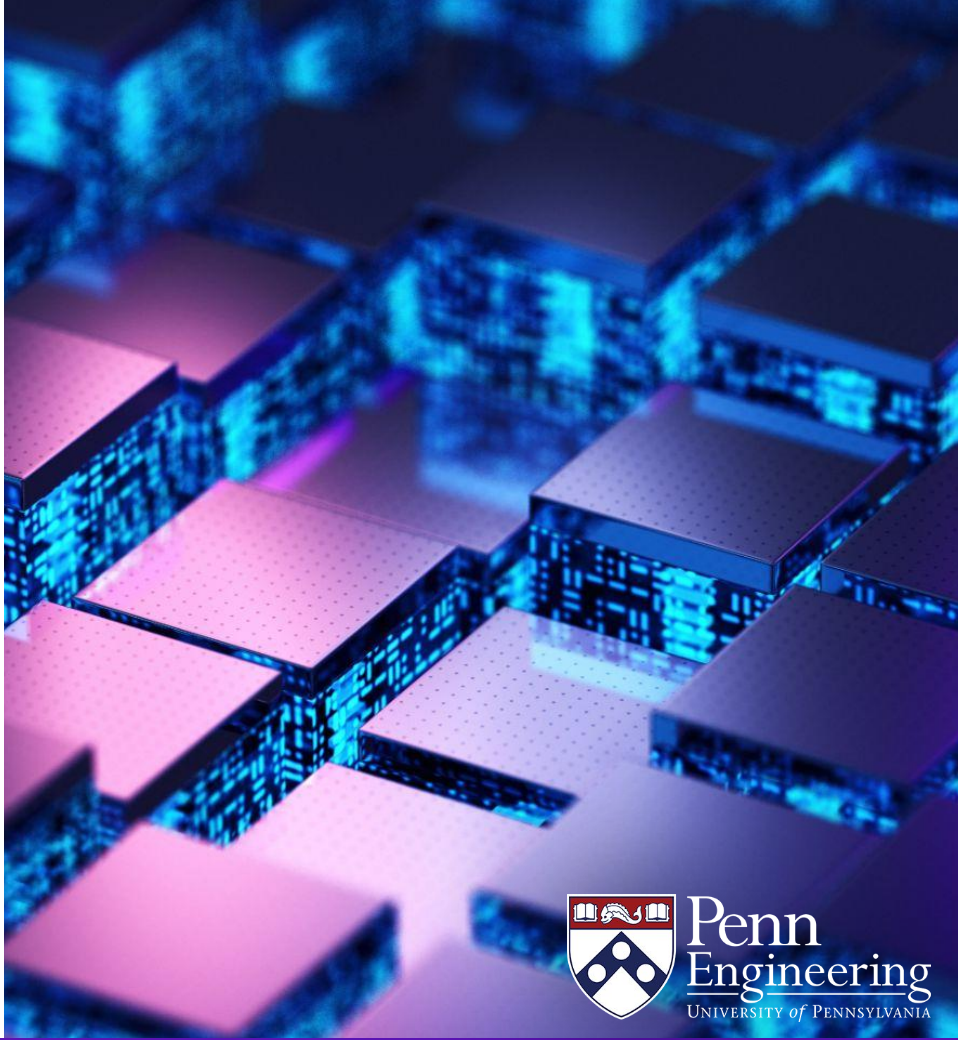
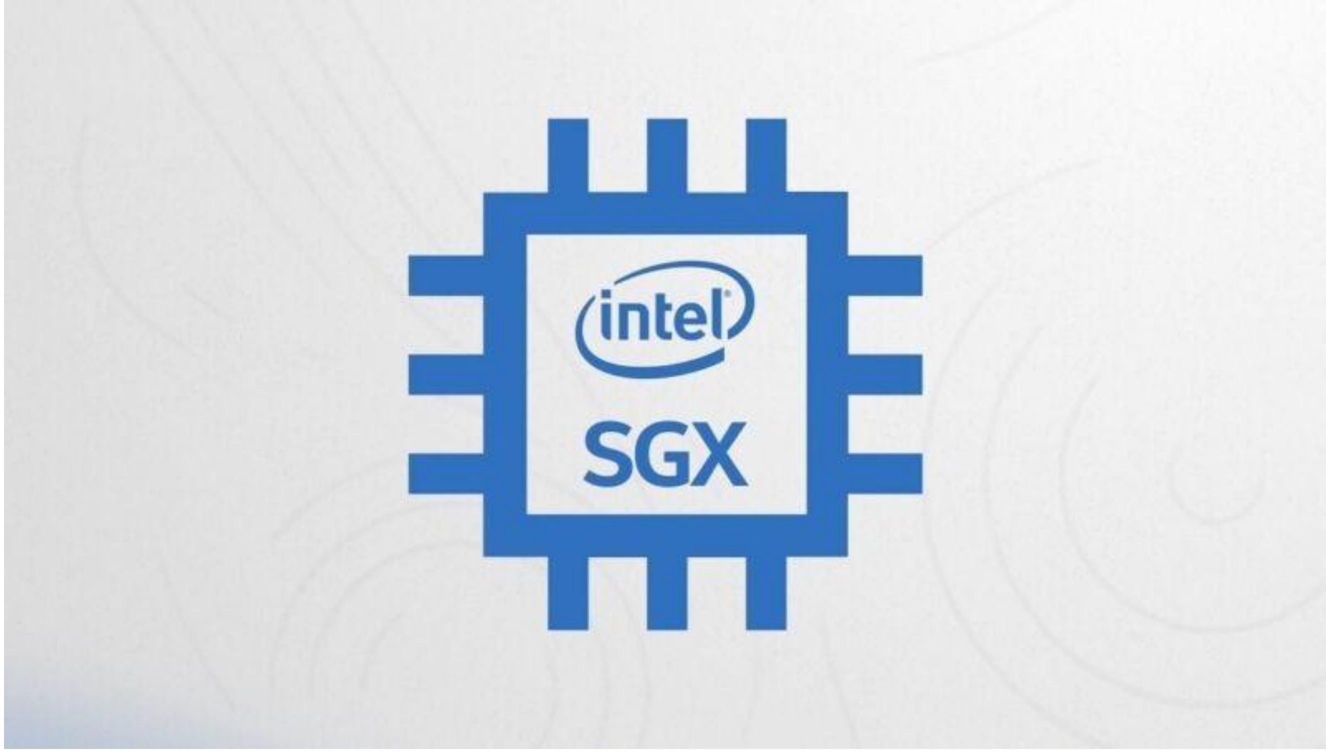
EAS 5830: BLOCKCHAINS

TEEs

Professor Brett Hemenway Falk

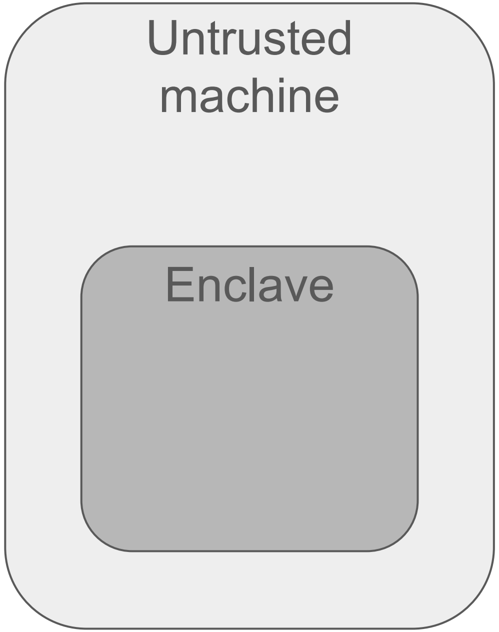


Penn Engineering
UNIVERSITY of PENNSYLVANIA

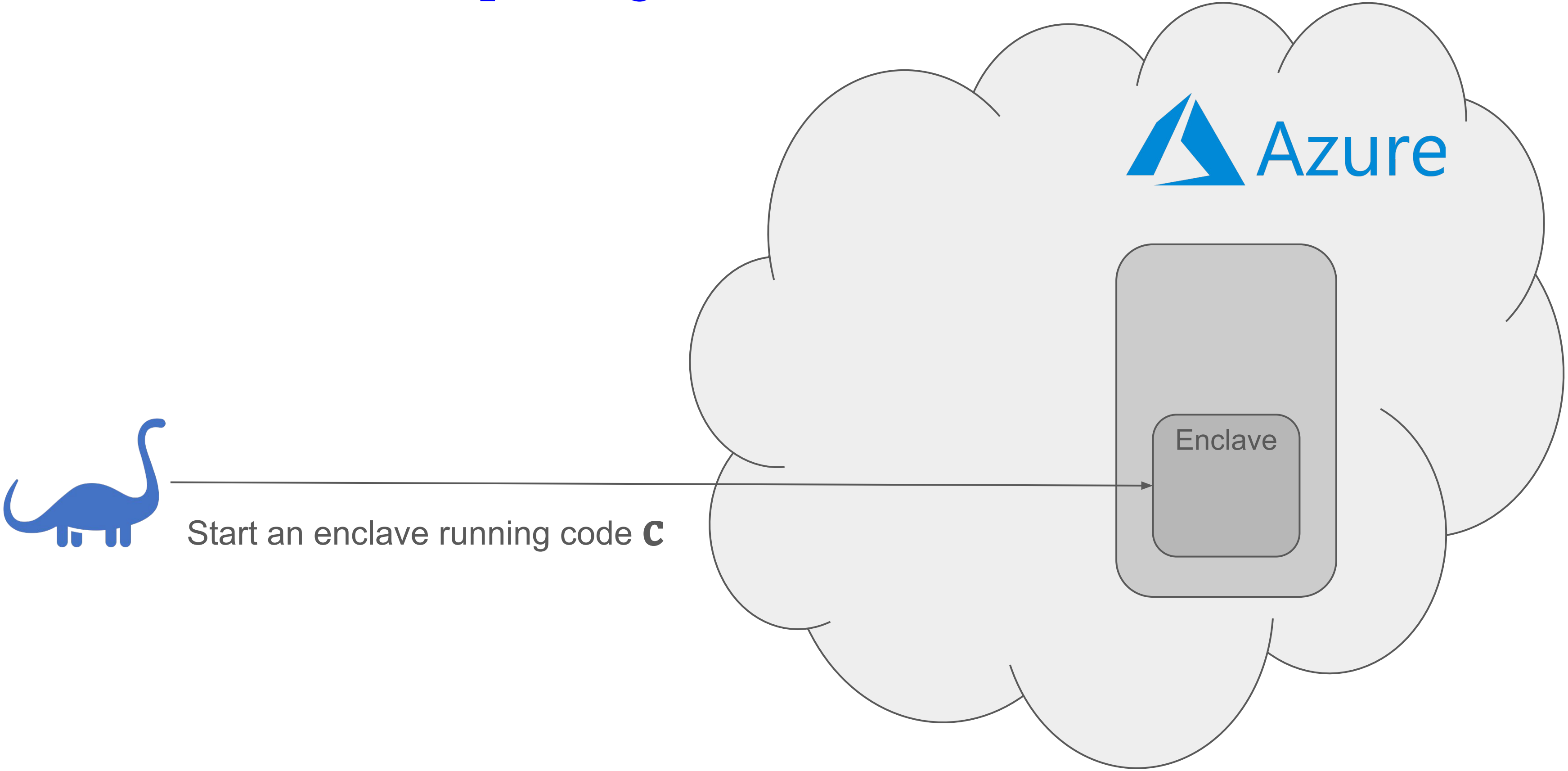

intel
SGX

SGX “Enclaves”

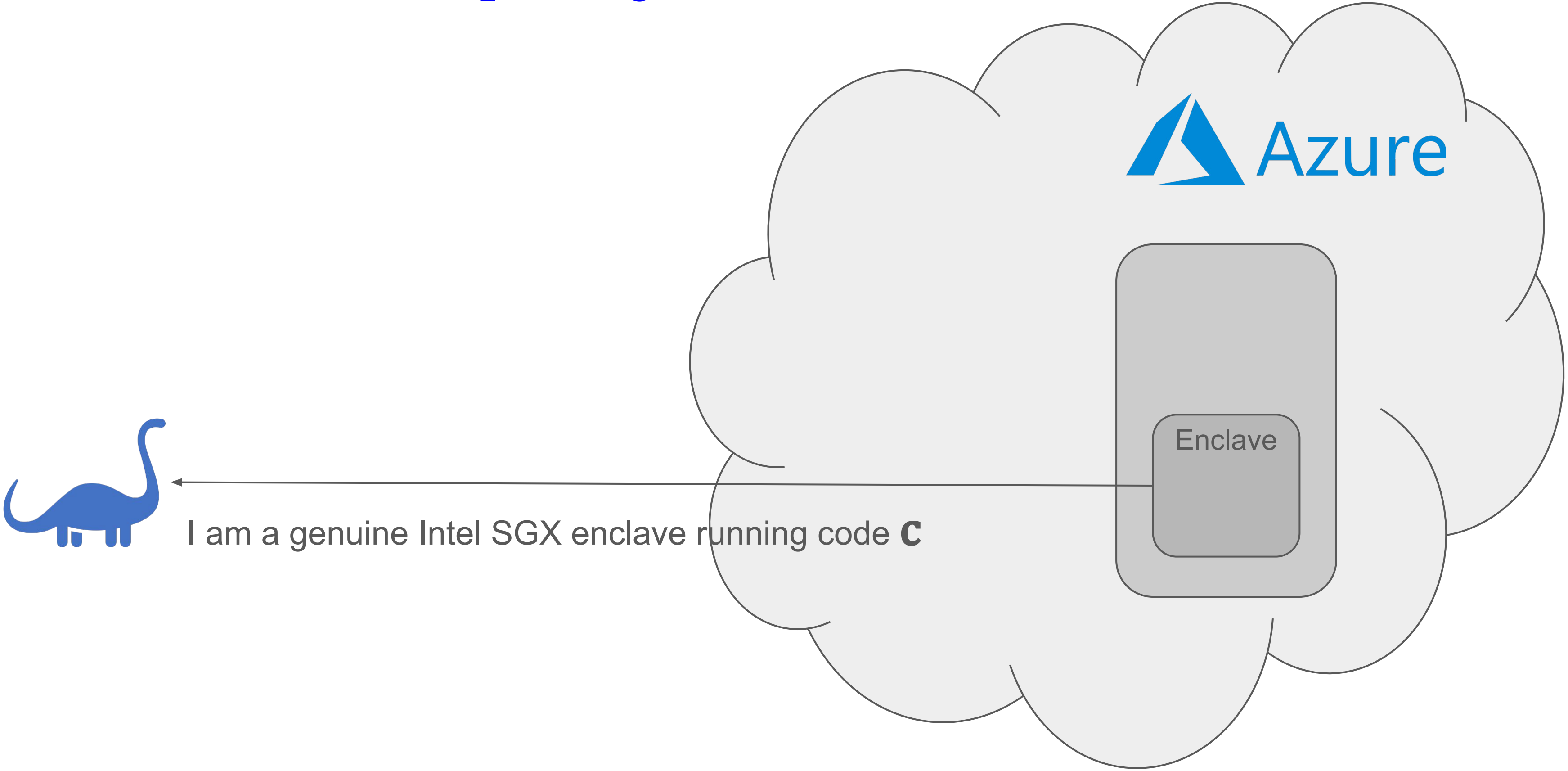
- You can run any code inside the enclave
- Your code defines I/O behavior
- Machine owner can only read state through predefined I/O
- Enclave can “attest” to the code it’s running
- Enclave can “prove” it’s an enclave



Trusted Cloud Computing

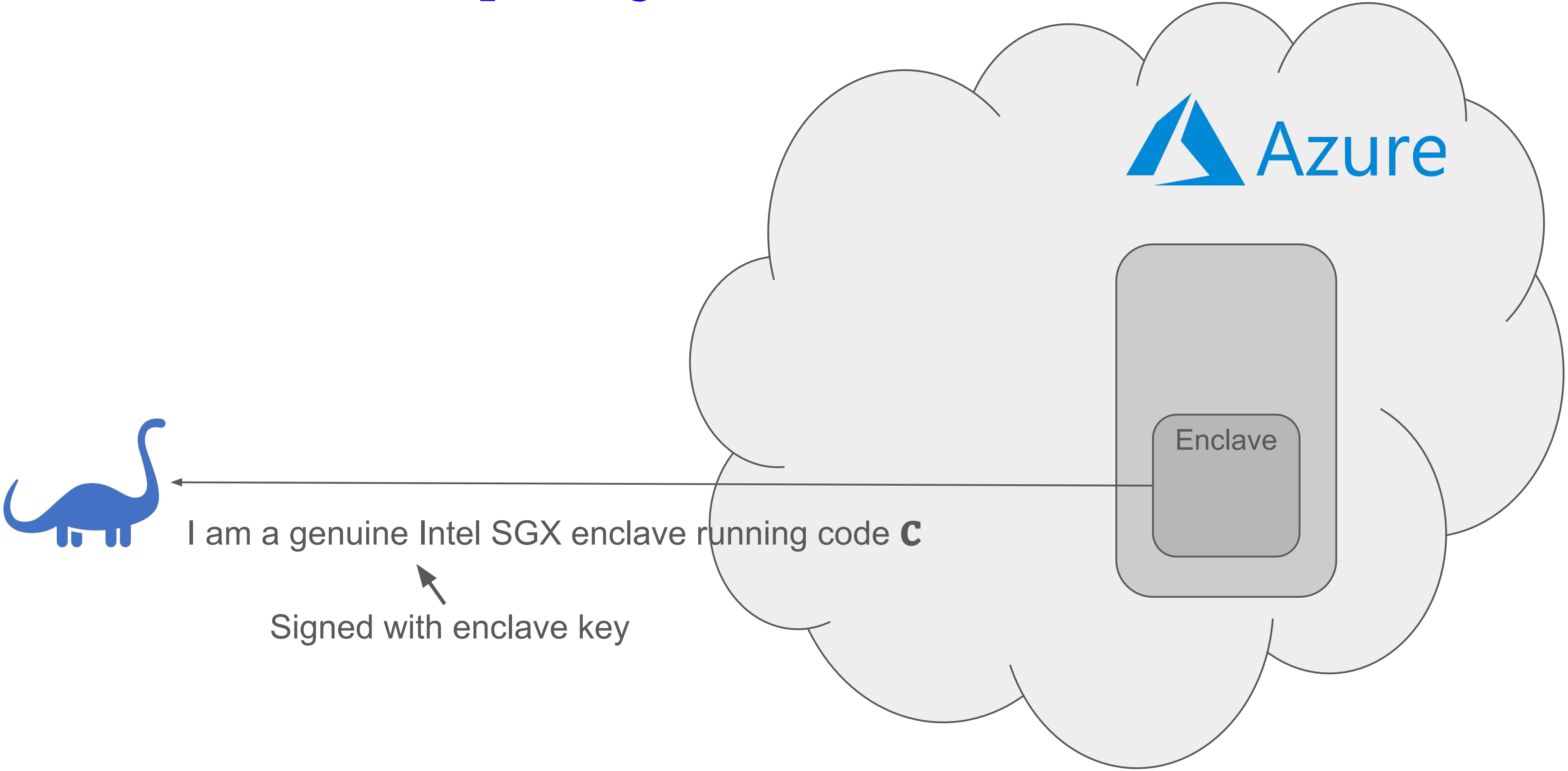


Trusted Cloud Computing

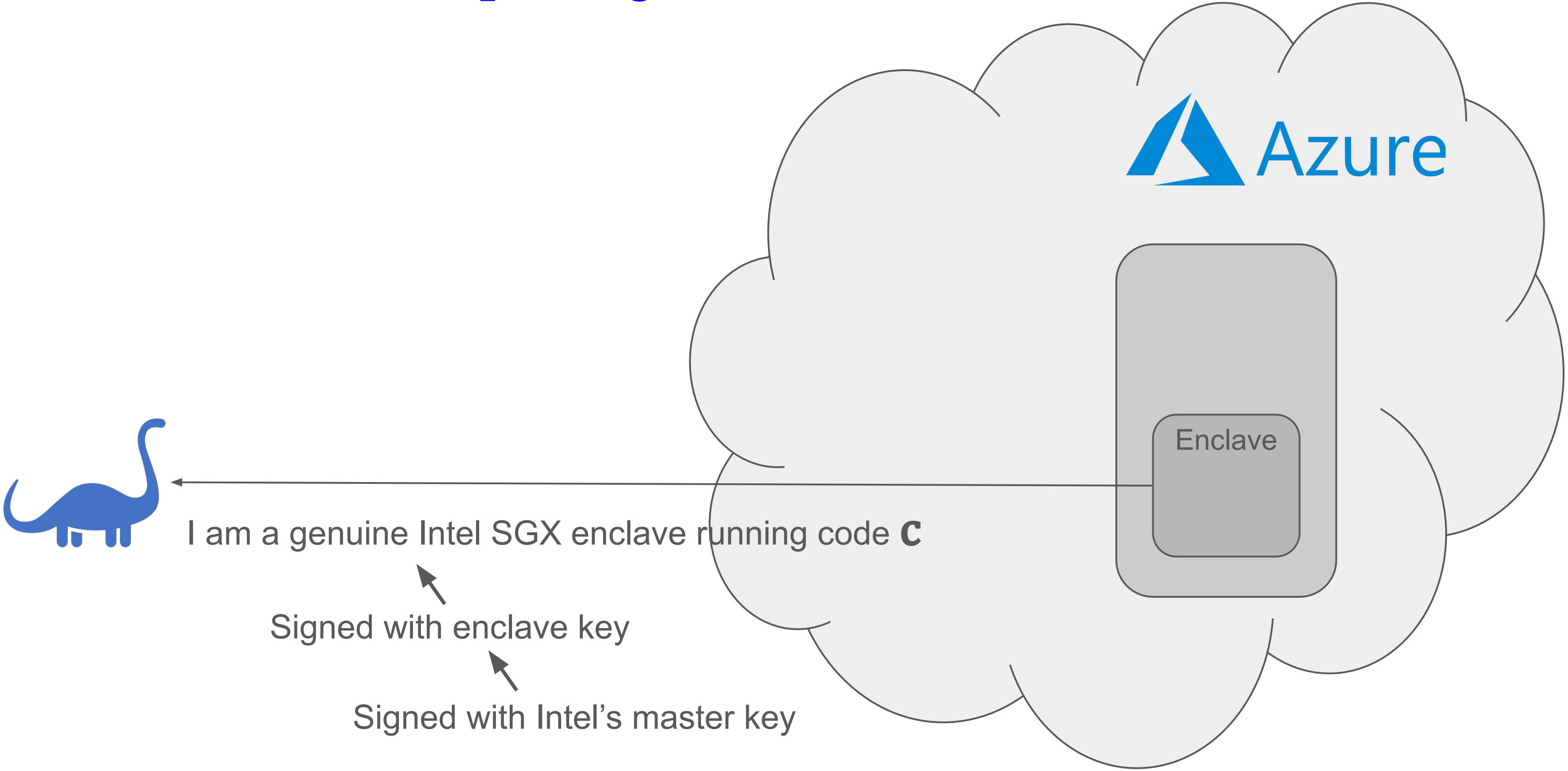


I am a genuine Intel SGX enclave running code **C**

Trusted Cloud Computing



Trusted Cloud Computing

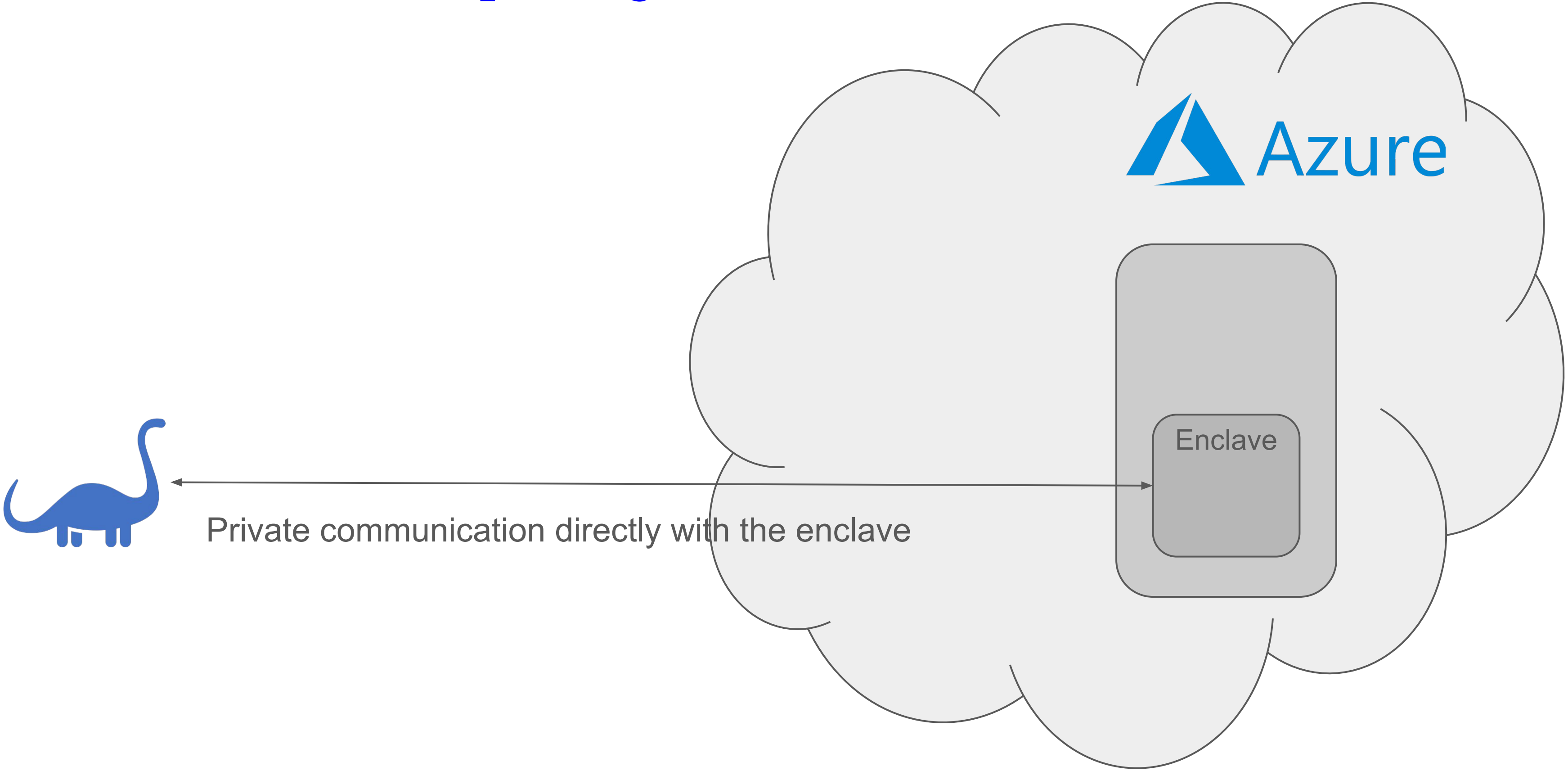


I am a genuine Intel SGX enclave running code **C**

Signed with enclave key

Signed with Intel’s master key

Trusted Cloud Computing

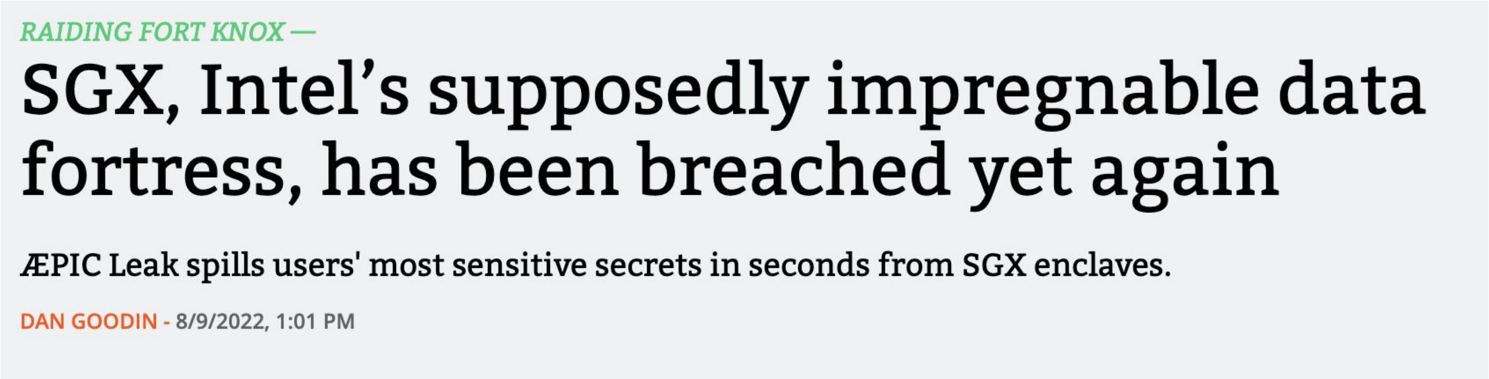


Using SGX in Blockchains

- **Idea**: Run a blockchain validator inside an SGX Enclave
- Nodes only peer with validators running SGX with the same code
- All transactions are encrypted under key held by the enclaves
- Entire state of the blockchain is private

secret
network

Sapphire
OASIS NETWORK

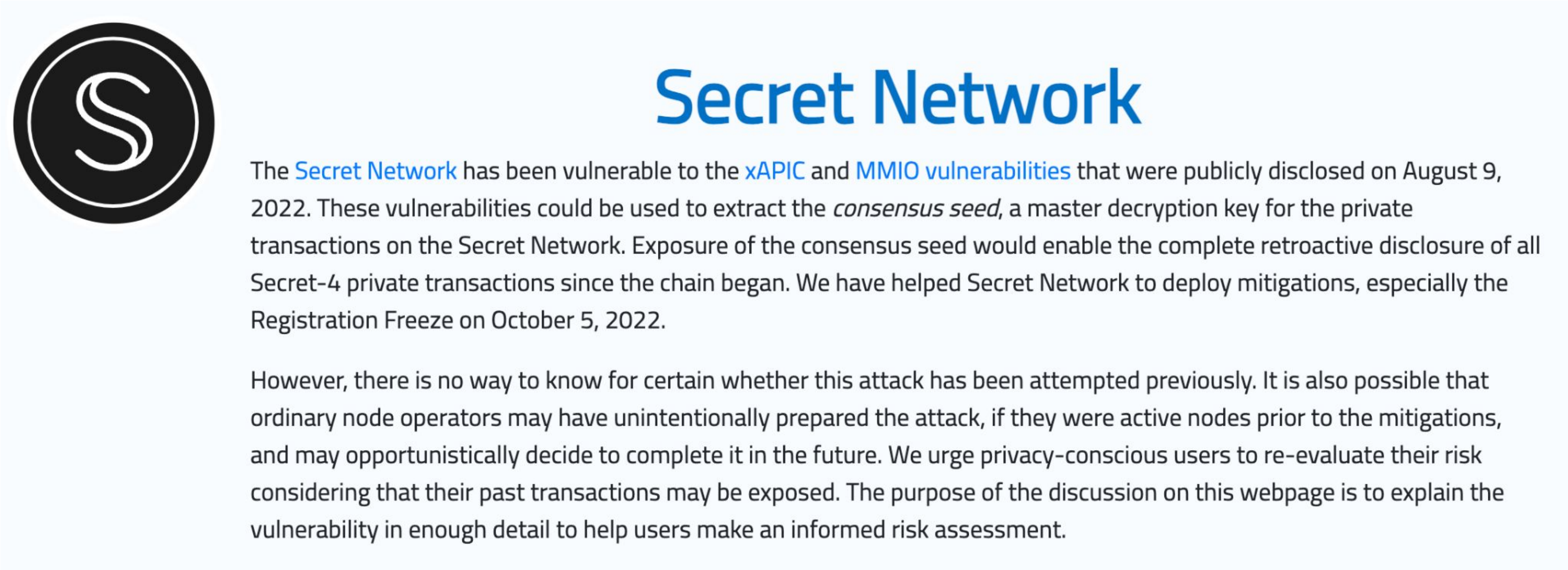


RAIDING FORT KNOX —

SGX, Intel’s supposedly impregnable data fortress, has been breached yet again

ÆPIC Leak spills users' most sensitive secrets in seconds from SGX enclaves.

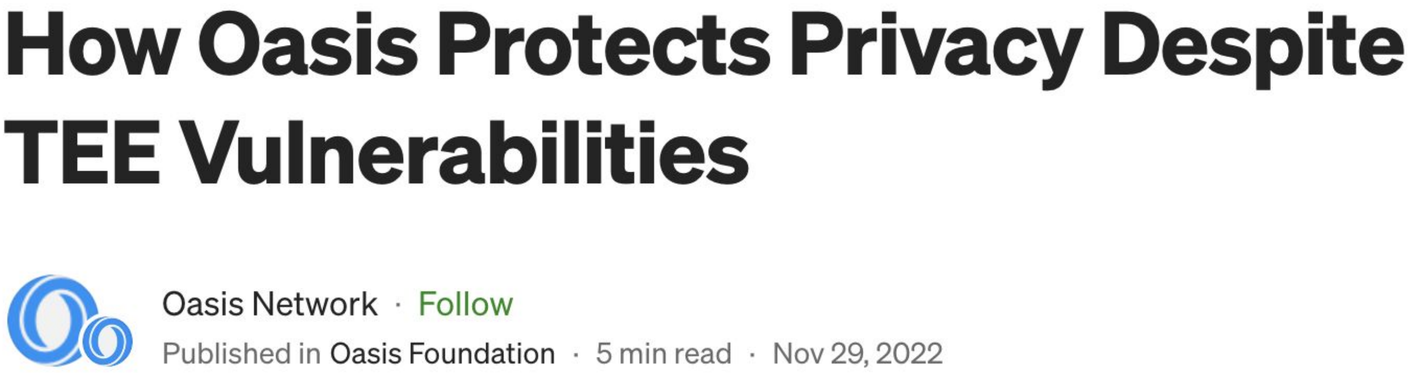
DAN GOODIN - 8/9/2022, 1:01 PM



Secret Network

The Secret Network has been vulnerable to the xAPIC and MMIO vulnerabilities that were publicly disclosed on August 9, 2022. These vulnerabilities could be used to extract the *consensus seed*, a master decryption key for the private transactions on the Secret Network. Exposure of the consensus seed would enable the complete retroactive disclosure of all Secret-4 private transactions since the chain began. We have helped Secret Network to deploy mitigations, especially the Registration Freeze on October 5, 2022.

However, there is no way to know for certain whether this attack has been attempted previously. It is also possible that ordinary node operators may have unintentionally prepared the attack, if they were active nodes prior to the mitigations, and may opportunistically decide to complete it in the future. We urge privacy-conscious users to re-evaluate their risk considering that their past transactions may be exposed. The purpose of the discussion on this webpage is to explain the vulnerability in enough detail to help users make an informed risk assessment.



How Oasis Protects Privacy Despite TEE Vulnerabilities

Oasis Network · Follow

Published in Oasis Foundation · 5 min read · Nov 29, 2022

Point

“Secret is the only chain shipping computational privacy on mainnet trying to solve the privacy problem 99.9% of all blockchains have. In that research it has chosen a pragmatic approach which works wonders for countless of usecases.

If you want full anonimity for TXs, use monero. If you want cool usecases like private comms, frontrunning resistance, liquidation protection and streaming private content than you HAVE to be in the secret ecosystem.”

Counterpoint

“The thing that people like you just don't understand is that Secret does not solve the privacy problem at all. Transactions are not private at all, the system is broken. It has always been obviously broken and was basically blown to pieces today.

And you are wrong, broken and invalid privacy is worse than no privacy. It gives a false sense of security which is absolutely detrimental.”