The Secret Network's reliance on Intel SGX for its privacy-preserving smart contracts is currently limited by using SMB (small medium sized business) grade hardware. With use cases emerging that necessitate higher performance such as Satoshis Palace, Silent Swap, and AI, the limitations of older-generation machines are becoming increasingly apparent. Even with the applications we have today such as Shadeprotocol, we find ourselves in a situation where a very small handful of transactions per block (less than 10 per block) or queries per block can cause many validator's to miss blocks and API nodes to crumble.

Technical Information

1. Memory Constraints on Older Machines
2. Older generation machines such as the E-21xx, E-22xx, and E-23xx have severe limitations in enclave memory, ranging from a minimum of 96 MB to a maximum of 512 MB. In stark contrast, enterprise servers equipped with scalable Xeon CPUs have a minimum of 8 GB and can reach up to 512 GB of enclave memory and memory comes from the systems RAM.
3. Secret Network's secretd

allocates 4 GB of memory at startup for enclave operations. On machines where the SGX memory is less than 4 GB, the system relies on disk paging, creating significant performance bottlenecks. This paging delay becomes a critical issue during high-load consensus operations on older nodes. (Validators missing blocks)

- The older machines are designed for small business applications, and the scalable cpu line is designed for enterprise applications.
- Older generation machines such as the E-21xx, E-22xx, and E-23xx have severe limitations in enclave memory, ranging from a minimum of 96 MB to a maximum of 512 MB. In stark contrast, enterprise servers equipped with scalable Xeon CPUs have a minimum of 8 GB and can reach up to 512 GB of enclave memory and memory comes from the systems RAM.
- Secret Network's secretd

allocates 4 GB of memory at startup for enclave operations. On machines where the SGX memory is less than 4 GB, the system relies on disk paging, creating significant performance bottlenecks. This paging delay becomes a critical issue during high-load consensus operations on older nodes. (Validators missing blocks)

1. The older machines are designed for small business applications, and the scalable cpu line is designed for enterprise applications.
2. Enclave Memory Utilization
3. Smart contract executions typically require around 12 MB of memory but can theoretically demand up to 128 MB or 256 MB. This further exacerbates the memory constraints on older machines, leading to increased paging operations and reduced performance.
4. Smart contract executions typically require around 12 MB of memory but can theoretically demand up to 128 MB or 256 MB. This further exacerbates the memory constraints on older machines, leading to increased paging operations and reduced performance.
5. Scaling improvements from roadmap
6. Even with scaling improvements or a more efficient engine, the constraints of older hardware interferes with significant performance gains. For example, concurrent executions is on the roadmap for an improvement this year, even if it's possible to add that and have it technically function with the old hardware it will likely exacerbate the performance issues given constrained memory.
7. Even with scaling improvements or a more efficient engine, the constraints of older hardware interferes with significant performance gains. For example, concurrent executions is on the roadmap for an improvement this year, even if it's possible to add that and have it technically function with the old hardware it will likely exacerbate the performance issues given constrained memory.

Proposed path forward

To prioritize the performance and scalability of the Secret Network, a discussion on phasing out older machines is essential. This transition would involve us formally upgrading the network's hardware requirements, validators provisioning newer machines, and rendering non-scalable CPUs non compatible via a network upgrade.

Proposed Timeline:

- Early 2025: I think this should happen early 2025. This provides ample lead time for node operators to upgrade their hardware and align with the new requirements.

- Communication from Leadership: Secret Labs and the Secret Network Foundation (SNF) should work closely with the community to ensure a smooth upgrade process, minimizing disruption.

Economic Implications

Transitioning to enterprise equipment comes with financial implications for APIs and validators:

- Cost of New Machines: Renting or purchasing next-generation enterprise servers will increase operational costs. While older machines can be rented for $80-$170 per month, the next-gen machines will at least start at $200-$350 per month.
- Long-Term Benefits: Without moving to the better hardware, we will continue to have current hardware based bottlenecks.

Final Thoughts

We really need to get this discussion going in the open, so I put some technical information out and a suggestion for how we can proceed. This topic has been lightly discussed in various channels, such as the Secret network validator room, Secret governance, and was touched upon in the validator reduction proposal. Though there is no formal communications from Secret Labs or SNF on the topic. If we don't start this discussion now, many will be surprised when the day comes where we need to do it swiftly, and participants surely would not be prepared to make this move in a timely manner.

Cc @LisaIsLoud @alexz

Source to back up claims :https://www.cse.iitd.ac.in/~srsarangi/files/papers/sgxgauge.pdf