Most solutions to provide privacy to smart contracts are based on SGX, which was a sensible choice years ago but recent attacks have proven it to be inadequate (see list of papers below breaking SGX). Moreover, the security model offered by SGX is much more useful for permissioned than permissionless blockchains.

Right now, the most adequate solution is to use state-of-the-art MPC protocols: 1000x faster than homomorphic encryption and backed by more than 30 years of research.

Note that there aren't many practical examples of blockchains running MPC: a system implementing MPC for Ethereum is described in the following paper: https://eprint.iacr.org/2017/878.

What practical uses cases in Ethereum would you use MPC for?

–

List of papers describing attacks on SGX:

- Ferdinand Brasser, Urs Muller, Alexandra Dmitrienko, Kari Kostiainen, Srdjan Capkun, and Ahmad-Reza Sadeghi. Software Grand Exposure: SGX Cache Attacks Are Practical, 2017.
- Michael Schwarz, Samuel Weiser, Daniel Gruss, Clementine Maurice, and Stefan Mangard. Malware Guard Extension: Using SGX to Conceal Cache Attacks, 2017.
- Ahmad Moghimi, Gorka Irazoqui, and Thomas Eisenbarth. CacheZoom: How SGX Amplifies The Power of Cache Attacks, 2017.
- Nico Weichbrodt, Anil Kurmus, Peter Pietzuch, and Rüdiger Kapitza. Async-Shock: Exploiting Synchronisation Bugs in Intel SGX Enclaves, 2016.
- Yuanzhong Xu, Weidong Cui, and Marcus Peinado. Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, SP '15, pages 640–656, Washington, DC, USA, 2015. IEEE Computer Society.
- Ming-Wei Shih, Sangho Lee, Taesoo Kim, and Marcus Peinado. T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs, 2017.
- Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado. Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing, 2016.
- Marcus Brandenburger, Christian Cachin, Matthias Lorenz, and Rüdiger Kapitza. Rollback and Forking Detection for Trusted Execution Environments using Lightweight Collective Memory, 2017.
- Yogesh Swami. SGX Remote Attestation is not Sufficient… Cryptology ePrint Archive, Report 2017/736, 2017.
- Jaehyuk Lee, Jinsoo Jang, Yeongjin Jang, Nohyun Kwak, Yeseul Choi, Changho Choi, Taesoo Kim, Marcus Peinado, and Brent ByungHoon Kang. Hacking in Darkness: Return-oriented Programming against Secure Enclaves. In 26th USENIX Security Symposium (USENIX Security 17), pages 523–539, Vancouver, BC, 2017. USENIX Association.
- Jo Van Bulck, Nico Weichbrodt, Rüdiger Kapitza, Frank Piessens, and Raoul Strackx. Telling Your Secrets without Page Faults: Stealthy Page Table-Based Attacks on Enclaved Execution. In 26th USENIX Security Symposium (USENIX Security 17), pages 1041–1056, Vancouver, BC, 2017. USENIX Association.
- Yuan Xiao, Mengyuan Li, Sanchuan Chen, and Yinqian Zhang. Stacco: Differentially Analyzing Side-Channel Traces for Detecting SSL/TLS Vulnerabilities in Secure Enclaves. CoRR, abs/1707.03473, 2017.
- Yuan Xiao, Mengyuan Li, Sanchuan Chen, and Yinqian Zhang. Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX. CoRR,abs/1705.07289, 2017.
- Frank Piessens Jo Van Bulck and Raoul Strackx. SGX-Step: A Practical Attack Framework for Precise Enclave Execution Control. In In Proceedings of the 2nd Workshop on System Software for Trusted Execution (SysTEX '17), 2017.