# Trias in One Page

Trias is found by Dr Anbang Ruan, the former research associate in Trusted Cloud at the University of Oxford Dr Ruan got his PhD from Oxford and has more than 10 years of research experience in System Security, Trusted Computing, and Cryptography. Trias currently has a team of 22 scientists and engineers from Oxford, Gatech, Peking University and leading tech companies, including Alibaba, Microsoft and Intel. It has also established in-depth academic collaborations with Peking University, Tsinghua University and Oxford respectively. Trias's core designs are backed by its core team's academic research at Oxford since 2011. It will launch the testnet by the end of Q3 2018, and the mainnet in early Q1 2019.

Trias's vision is to build a trustworthy and reliable general-purpose computation infrastructure, where any system and software implement only expected behaviours. With Trias, we can root trust into machines with a firm assurance that the machines will deterministically "do what they are told to do". Trias is building an all-platform-supported native-application-compatible smart contract execution platform, development framework and collaborating ecosystem. Particularly, it builds three subsystems:

**Leviatom, an integration of Trusted Execution Environments (TEEs) and Graph to achieve correct execution of general-purpose software.** Leviatom implements a Heterogeneous Consensus Graph (HCGraph) algorithm, which combines heterogeneous TEE technologies (TPM, TXT, Intel SGX, ARM TrustZOne, etc.) and graph computing algorithms (similar to Hashgraph or DAGs). Heterogeneous TEEs allow Leviatom to identified misbehaving nodes rapidly while eliminating the dependency on any single technology's provider, e.g. Intel SGX-based consensus requires a strong dependency on Intel's centralised online verification service. Meanwhile, HCGraph's small-world-theory-based gossip protocol significantly reduces the redundant TEE verifications, while preserving a scalable and robust web-of-trust. With HCGraph, Leviatom easily achieves more 100,000 tps for a single shard, while defending near 90% malicious collaborative attacks.

**Prometh, a combination of formal verification and DevSecOps methodologies to achieve traceable and verifiable general-purpose software development.** Prometh genuinely records the critical information for a piece of software's entire lifecycle on blockchain. It further encourages the community to applies formal verification and DevSecOps methodologies to enforce automatic or manual examinations or verifications on the recorded information. This helps deducing the genuine properties of the software, which ensures any piece of software only implement intended behaviours.

**MagCarta, a consensus-oriented programming paradigm to achieve embed and self-defined consensus strategy for high-order enterprise DApps.** MagCarta schedules Prometh applications on Leviatom network to achieve high-order enterprise application logic. With the consensus-oriented programming paradigm, DApps can implement their embed consensus algorithm and ledger structure, and choose their strategy to reward the computing infrastructures (Leviatom) of software components (Prometh) contributors.

Trias enables a much wider range of usage scenarios, as it targets at bringing trust to general-purpose software platforms instead of only to the ledger-related applications: 1. Layer -1 enhancement for public blockchains. Leviatom enforces a trusted relationship among the consensus node of existing public chains. This will greatly reduce their consensus overheads and significantly increase their tps. 2. Consensus-Oriented Enterprise Programming. MagCarta allows DApps to implement their consensus logic and ledger format without confining to any predefined fixed strategies by the chosen public blockchain; 3. Trusted operating systems and application ecosystem. Trias eliminates easily malware and attacks, as Leviatom only allows the executions of white-listed applications and Prometh only allows the applications to implement white-listed behaviours; 4. Trustworthy Multi-Party Computation. Trias achieves multi-party computations by exchanging trustworthy applications instead of exchanging private data.