技术架构与产品矩阵

让能耗更轻一点

ZKP-SOC可编程芯片采用多标量乘法（MSM），优点在于高性能、低成本、高能效比的零知识证明矿机，为公链网络和隐私计算提供强大的基础设施支持。

ZKP-SOC矿机在算法上结合多标量乘法（MSM）与数论变换（NTT）的算法。
ZKP-SOC矿机加速MSM和NTT计算，将零知识证明生成时间从分钟级压缩至秒级，同时降低能耗。

MSM模块将标量分解为多基数表示（如二进制、4进制），减少点加法次数并且支持部署多个椭圆曲线点加法器，支持并行分桶计算。

NTT加速模块支持蝶形运算单元，在内存层优化了高带宽内存（HBM）和SRAM，减少数据搬运延迟，大大加速了数据同步。