



# 算丰AI芯片的产品设计与安全设计

芯之安全磐石 若广厦之地基

比特大陆 汤炜伟

2020.12.17



# 目录

01 比特大陆简介

02 算丰AI芯片的设计初心

03 算丰AI芯片的安全六盾

04 他山之石：区块链

01

# 比特大陆简介

# 01 比特大陆公司历程

经过七年成长的高性能计算芯片设计企业：  
掌握7纳米和5纳米芯片设计能力的全球几家公司之一

## 区块链业务-蚂蚁矿机

全球市场占有率第一



## 人工智能业务——算丰

AI芯片和产品 / 深度学习专用TPU



2013

公司成立

推出55nm芯片

2014

推出28nm芯片

ANTPOOL矿池上线

2015

AI业务算丰启动

BTC.com矿池上线

2016

推出16nm芯片



2017

第一代AI芯片

年营收突破

25亿美元

2018

首款7nm芯片

第二代AI芯片



2019

第二款7nm芯片

第三代AI芯片

# 01 比特大陆算丰AI芯片

## 高算力，大带宽

- 8核A53，主控能力提高2~3倍
- INT8算力17.6T / 35.2T



BM1684

## 强劲的视频编解码能力

- 最高支持38路1080P解码，提升4倍
- 视频前后处理能力提升4倍

## 接口丰富，超低功耗

- 支持双千兆以太网口
- 功耗较上代产品降低50%以上

## 安全可靠，完美保障

- 新增安全引擎，保证数据安全、算法模型安全、设备安全



BM1682

第二代面向云端与边缘应用的AI推理芯片



BM1880

第一代面向终端应用的AI推理芯片

## 组建AI芯片团队

2021

BM1686

2019

BM1684

工艺制程 峰值性能  
12nm 17.6T/16W  
视频解码  
32路1080P硬解码

2018

BM1682

工艺制程 峰值性能  
28nm 3T FP32  
视频解码  
8路1080P硬解码

BM1880

工艺制程 峰值性能  
28nm 1TOPS@INT8  
视频解码  
H.264解码

2017

BM1680

工艺制程 峰值性能  
28nm 2T FP32

2016

# 02

## AI芯片的设计初心

## 02 AI芯片的设计初心

Performance &  
Power

算力强、功耗适合  
场景全覆盖  
云端和边缘

Application  
& Easy use

机器视觉全算法支持  
GPU迁移代价低  
客户研发投入小

Lower cost  
& Safe

产品性价比优  
客户数据安全  
算法安全

# 02 全产品矩阵：云和边缘全覆盖

PeaceNet  
算力云管理平台

算力资源池  
算力调度 / 弹性伸缩

算法资源池  
算法适配 / 算法仓库

应用网关  
运营管理

BMNNSDK  
一站式开发工具链

Compiler 编译器  
BMNetC / BMNetT / BMNetP / BMNetM / Paddle-Lite

Runtime 运行时部署工具  
BMRuntime Engine / BMCV / OpenCV / FFMpeg / BMLib

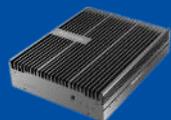
边缘



AI计算模组 SM5  
算力 17.6TOPS@INT8



AI单芯加速卡 SC5H  
算力 17.6TOPS@INT8



AI计算盒 SE5  
算力 17.6TOPS@INT8



AI计算盒 SE3  
算力 3TFLOPS@FP32

云



AI三芯加速卡 SC5+  
算力 52.8TOPS@INT8



SC5+ AI服务器系列  
X86平台, 国产飞腾FT平台  
一机多卡



AI超级算力中心  
AI推理服务器集群  
P级超强算力



BM1684  
12nm 17.6TOPS@INT8



BM1682  
28nm 3TFLOPS@FP32

# 02 AI芯片的设计：ASIC专用架构，算力、功耗、解码优于GPU

## 高算力，大带宽

- 8核A53，主控能力提高2~3倍
- INT8算力17.6T / 35.2T

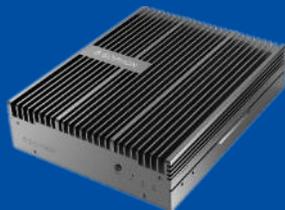
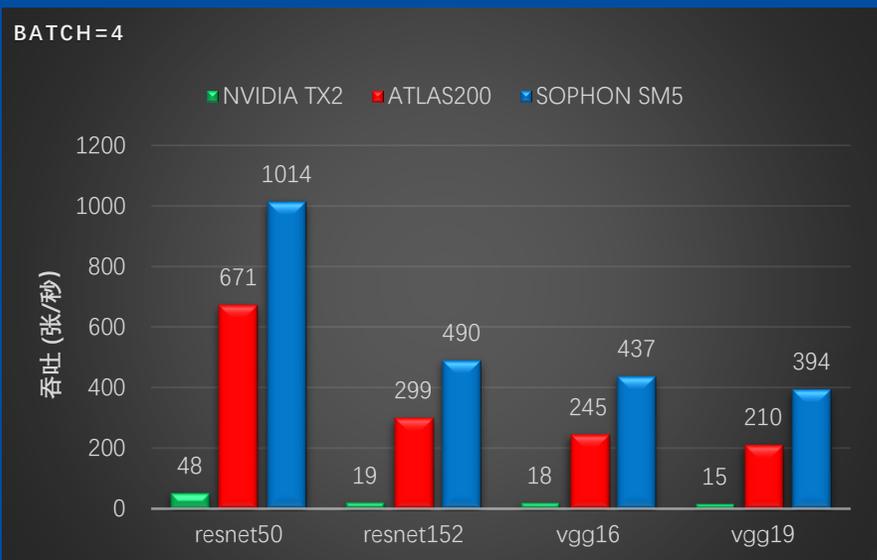
## 强劲的视频编解码能力

- 最高支持38路1080P解码，提升4倍
- 视频前后处理能力提升4倍



- ResNet超过GPU **20倍**
- VggNet超过GPU **25倍**
- 能量效率超过旗舰 GPU **20倍**

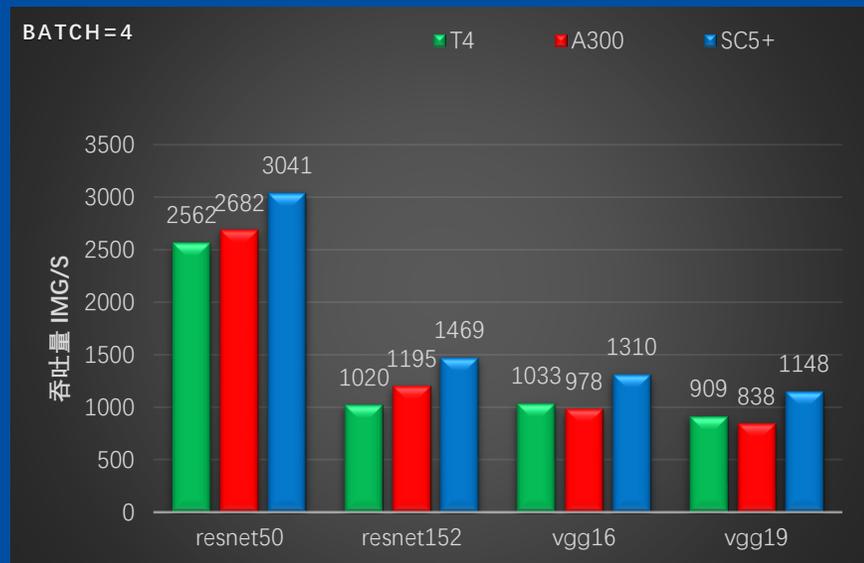
- ResNet超过旗舰 GPU **10%-32%**
- VggNet超过旗舰 GPU **8%-41%**
- 能量效率超过旗舰 GPU **70%**



同等的被动散热  
边缘盒/模组  
( $<20W$ )

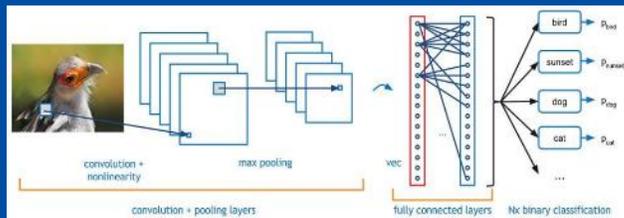


同等的半高半长板卡  
( $\leq 75W$ )



# 02 AI芯片的设计初心：机器视觉类AI算法全覆盖

## 图像分类



### 典型模型

- AlexNet、GoogLeNet、VGGNet、RESNET、DenseNet、mobilenet .....

## 目标检测



### 典型模型

- YOLO、SSD、Fast R-CNN .....

## 语义分割

语义分割：在语义上理解每个像素的角色



### 典型模型

- Deeplab, FCN、SegNet .....

## 实例分割

语义分割的基础上，实例分割将不同类型的实

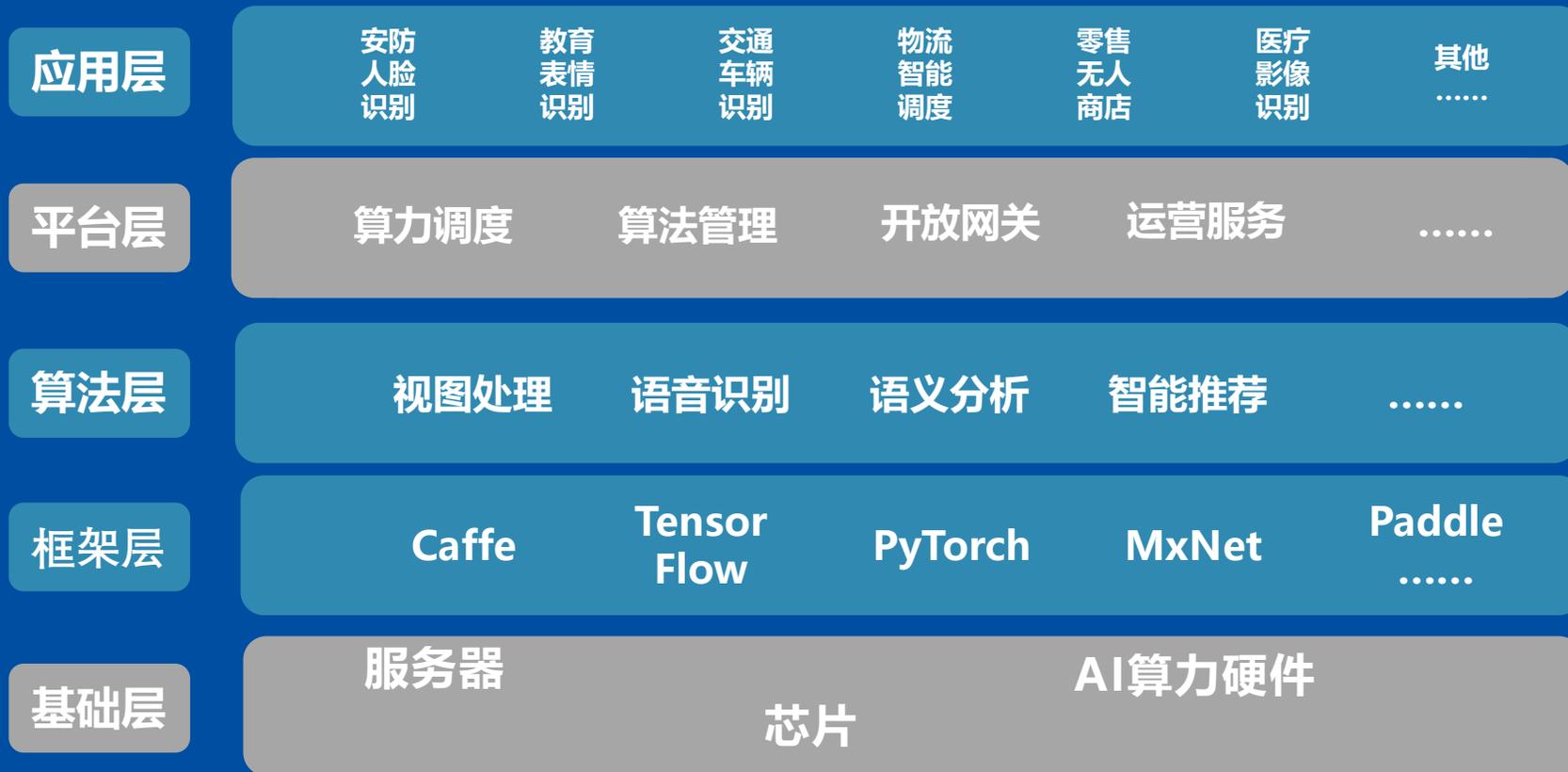


### 典型模型

- Mask R-CNN、Deeplab .....

行业/技术	图像分类	目标检测	语义分割	实例分割
安防	人体车辆属性分类	人脸检测、目标检测	行为姿态检测	行为姿态检测
互联网	电商图像识别、OCR	内容审查	视频广告	视频广告
消费电子	手机相册分类	手机相册分类	手机美颜	抠图、电影效果
汽车	人车分类、红绿灯	人车检测	可行驶区域感知	可行驶区域感知
医疗	病灶标注	病灶识别与标注	CT、X光辅助诊断	CT、X光辅助诊断

## 02 AI芯片的设计初心：框架完善支持、易开发易迁移



03

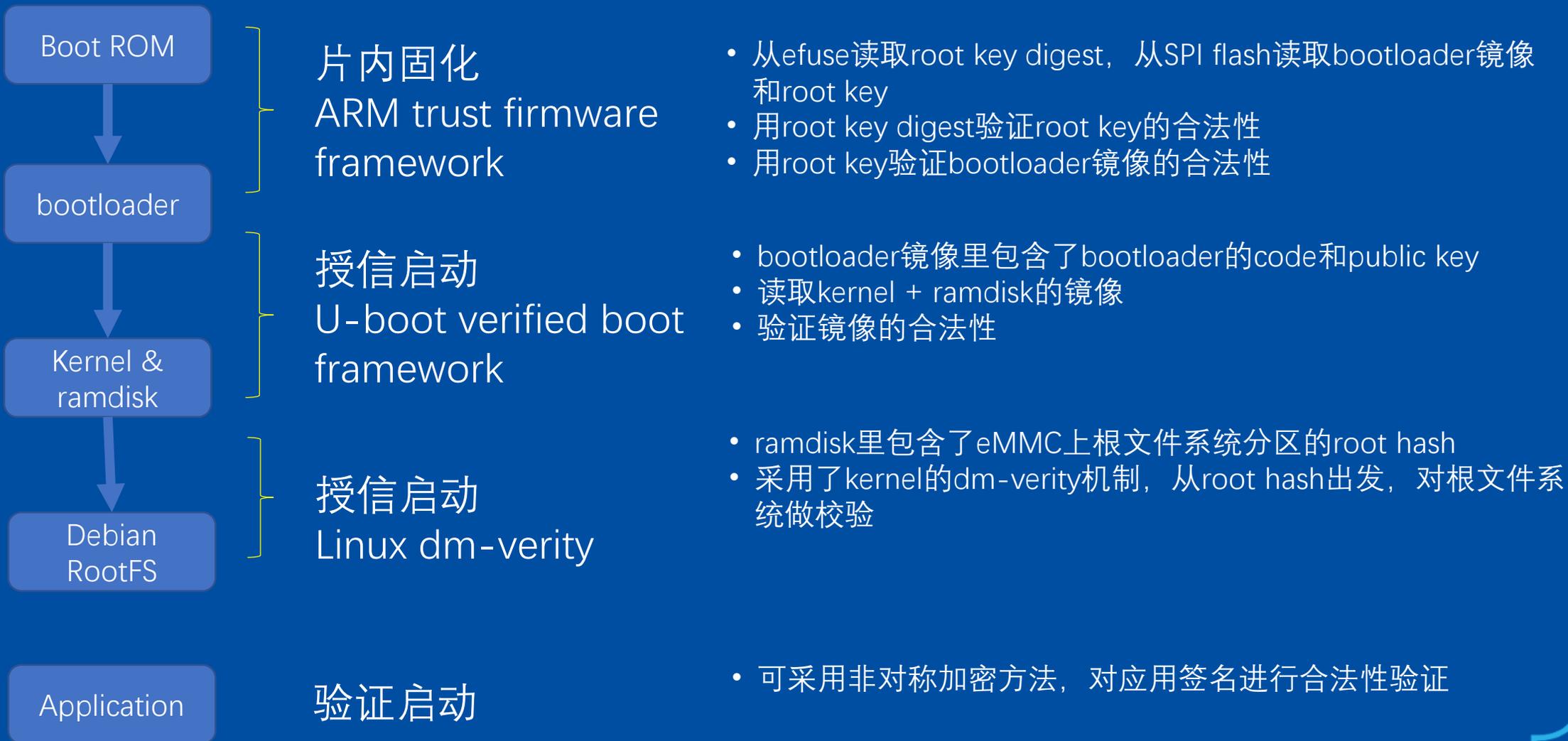
## 算丰AI芯片的安全六盾

## 03 最新一代AI芯片：BM1684的安全六盾

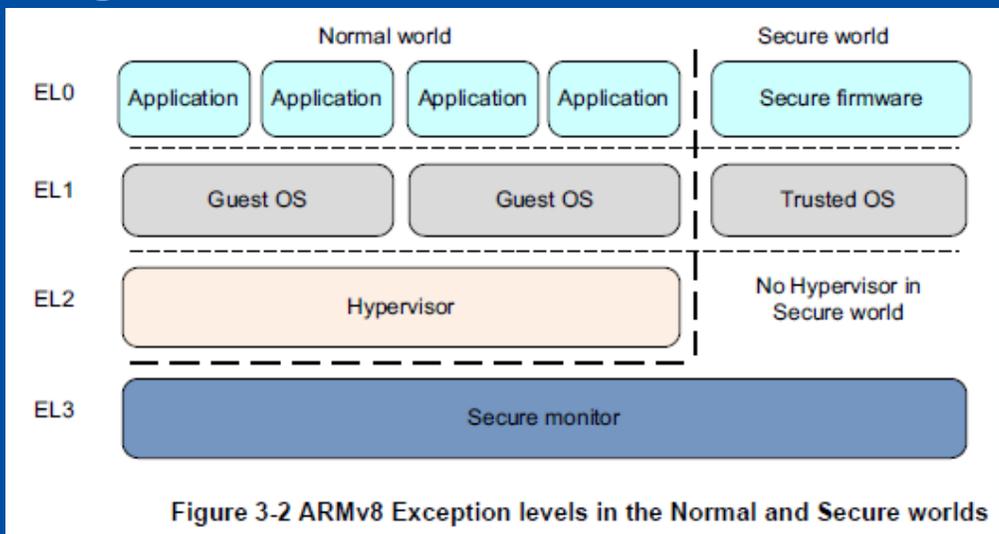


- Secure boot
- Crypto engines
- Secure key for customer
- Trust zone
- Secure firewall
- Chip unique ID

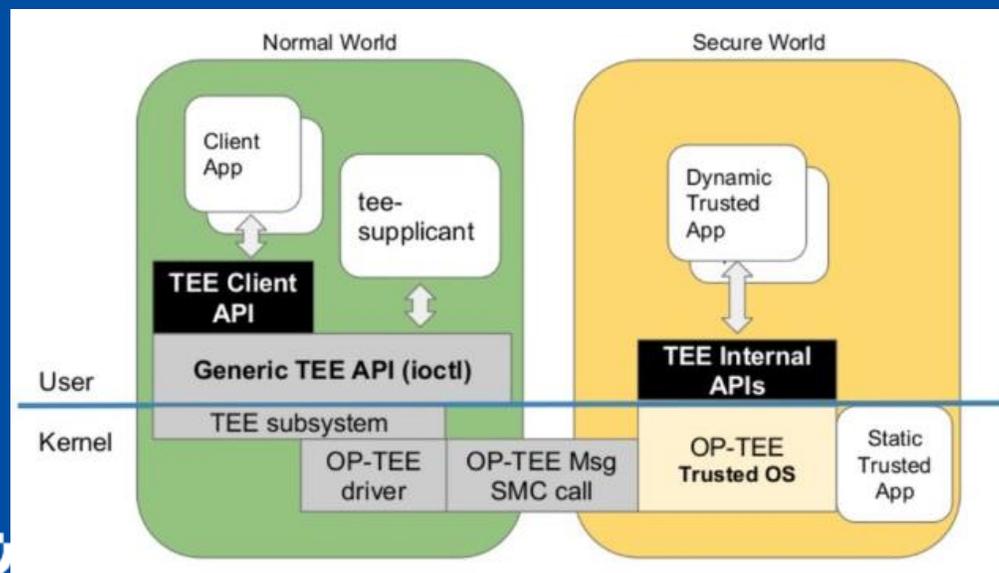
# 03 构建可信的系统：Secure boot 验证启动



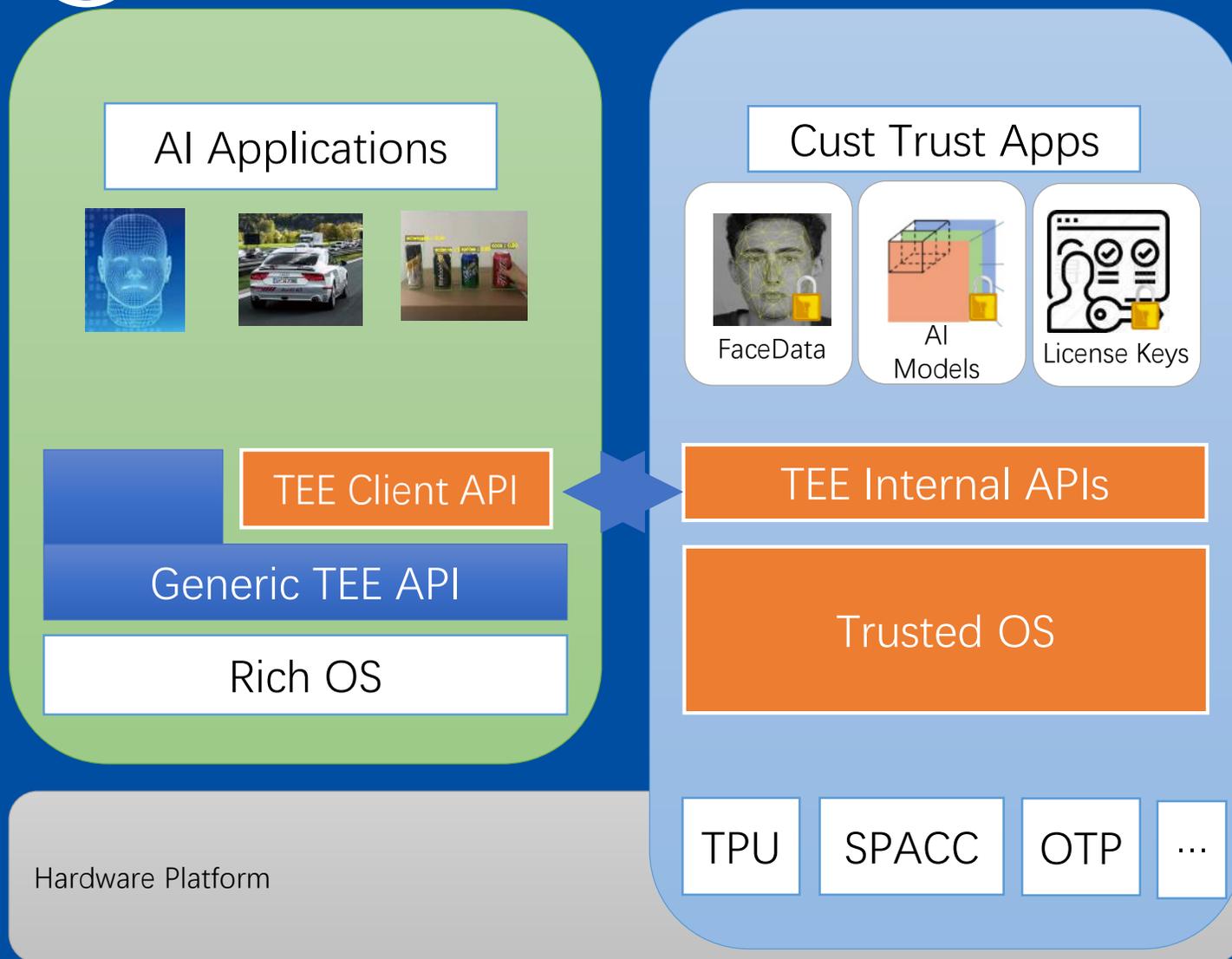
# 01 构建可信的系统：Trust zone 可信区



- TrustZone提供一套高效系统安全保护硬件架构，可以有效的抵御各种可能的攻击
- 它将SOC的资源划分为安全(security world)和非安全(normal world)两个世界，关键的高敏感数据在安全世界执行，其它操作在正常世界执行
- 从芯片ROM开始，逐级建立信任链，每一步启动都需要最高特权级别执行和密钥验证，防止软件篡改替换
- BM1684遵循TrustZone设计规范进行了完整的实现



# 01 构建可信的系统: Secure Firewall & Secure key & Chip unique ID



- 应用密钥
  - 客户根钥烧写至OTP区域, 采用 secure mode保护, 仅供硬件加解密引擎读取
  - 加密后应用密钥由normal world传入 secure world解密, 用于相应数据的解密
- 数据:
  - 加密存储在非易失设备中 (eMMC/SDD/HDD)
  - 使用时加载至secure world解密后使用
- 算法模型:
  - 加密存储在非易失设备中或由网络下发
  - 通过TA加载至secure world解密运行

# 01 构建可信的系统: Crypto Engines

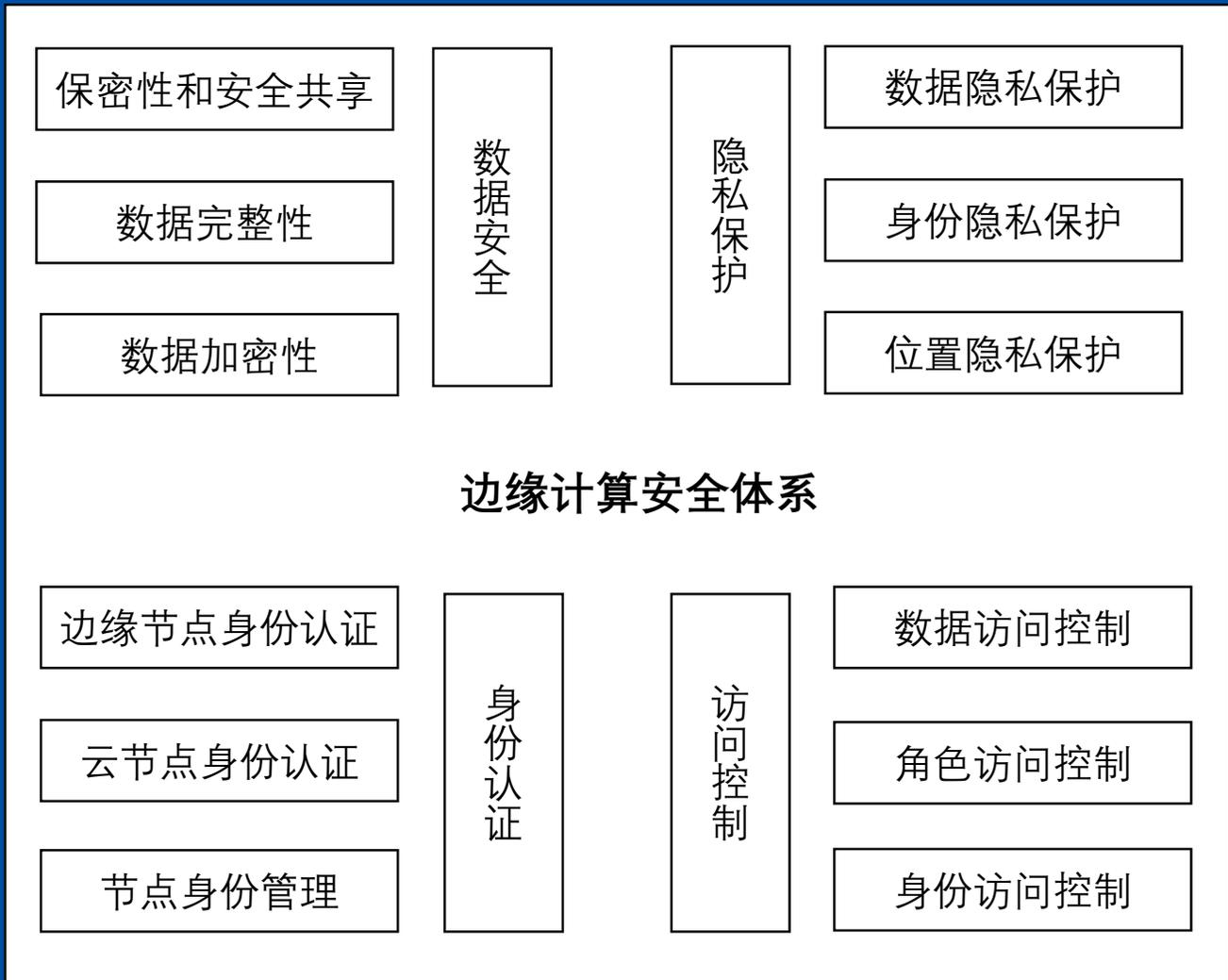


- Support crypto engines:
  - AES/DES;
  - SM4/SHA;
  - RSA/ECC;
- All above hardware accelerator
  - SPACC enabled one way read
  - Software (cpu) accelerator can read both ways not secure
- Secure key storage scheme support

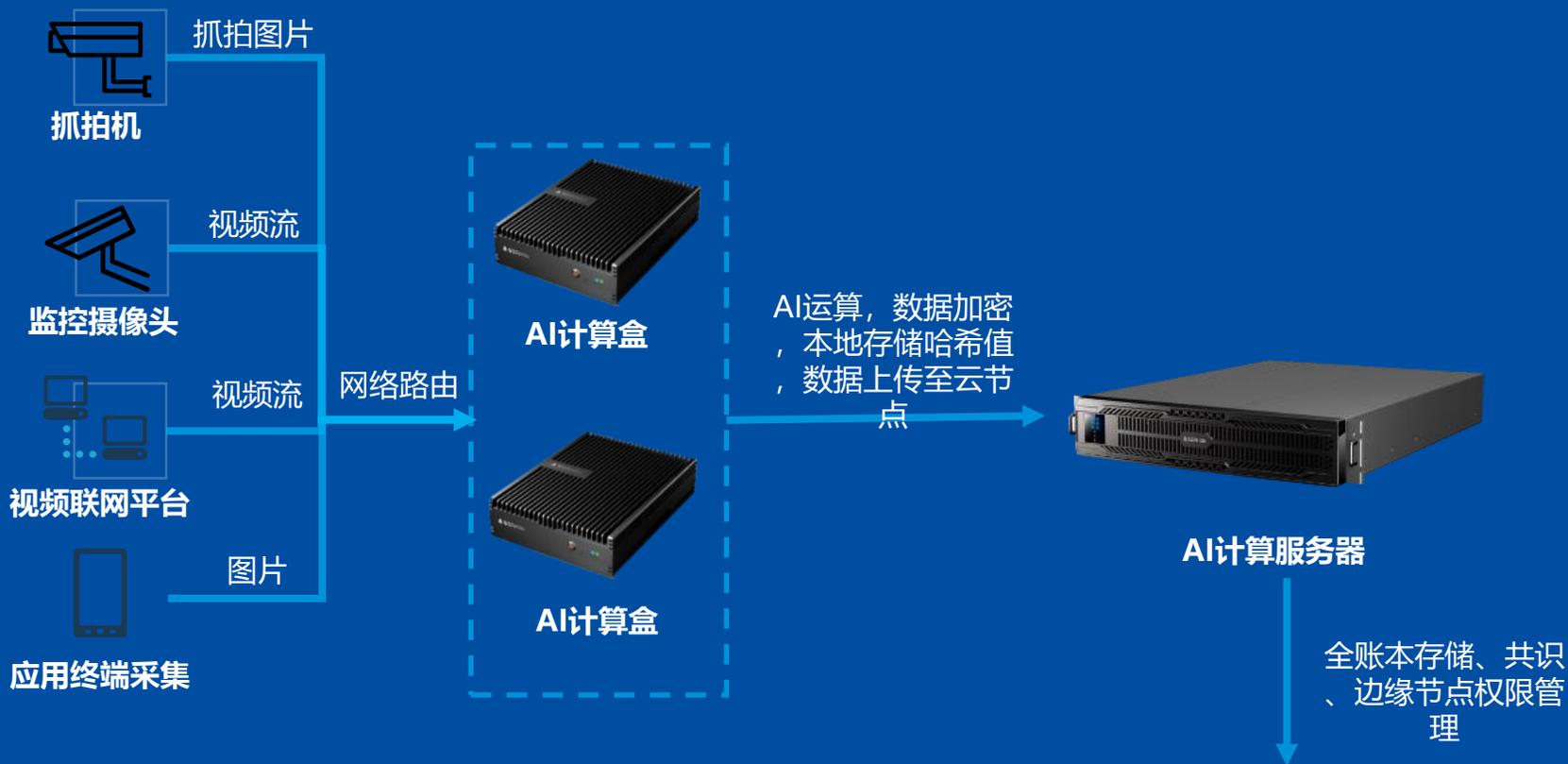
# 04

## 区块链设想

# 01 边缘计算安全体系

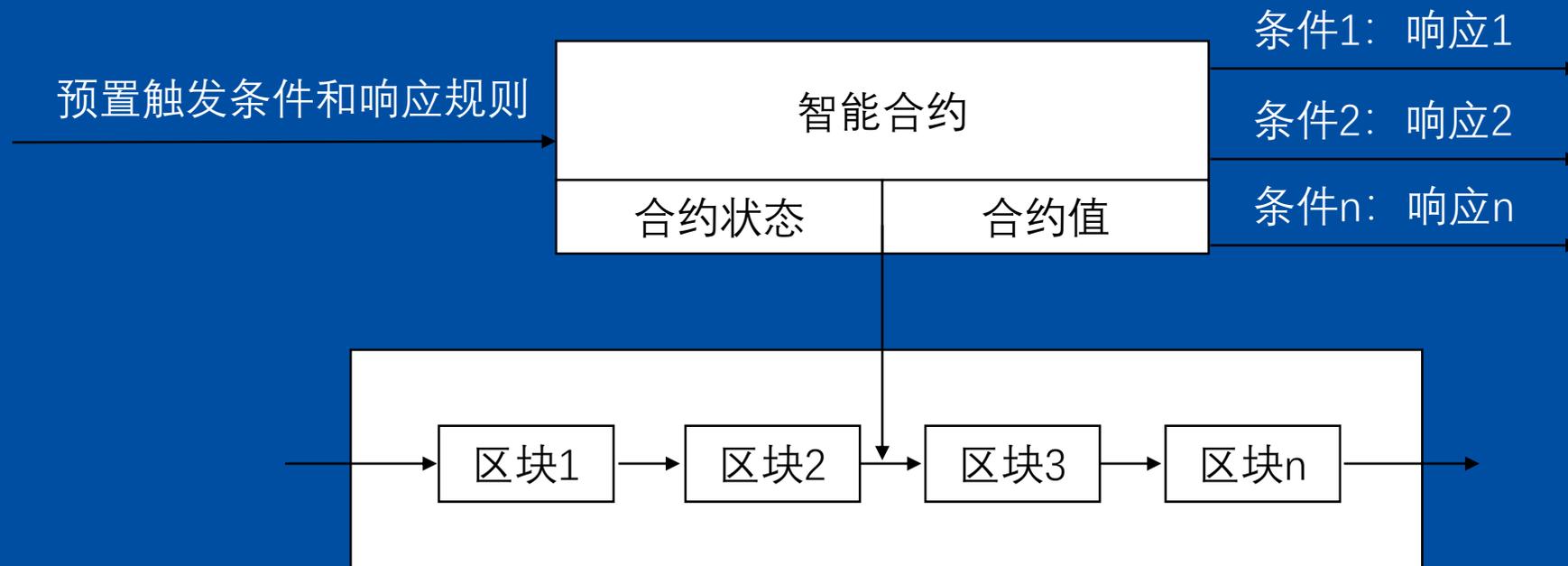


## 04 边缘计算典型网络节点和结构图



抓拍机、摄像头以及应用终端等终端节点负责采集数据，将数据通过网络路由上传到AI计算盒，边缘计算节点对终端采集的数据进行AI运算和处理，然后存储各个区块的哈希值。云节点负责账本存储、共识、路由和应用等任务，云节点是云平台上划分的多个虚拟机，虚拟机负责共识出块和全账本存储，并可以通过开发区块链应用来管理和监控整个网络。

## 04 边缘计算和云：基于区块链的智能合约



智能合约封装了预定义的触发条件及响应规则、触发合约执行的场景（如达到特定时间或发生特定事件等）、特定情境下的应对动作等。在边缘计算场景中，可以采用智能合约来操作数据，实现区块链数据的生成、修改、删除等权限管理功能，智能合约在区块链部署到AI硬件产品上提供了灵活可编程的机制和算法。

## 结语

- 比特大陆作为最早的AI芯片厂家之一，芯片设计和软件设计健全；
- 从最底层的芯片和硬件层，提供多种安全框架的产品解决方案；而芯片级别的安全保护、隐私保护等是最基础的磐石；
- 以AI芯片构建的边缘计算方案，未来有机会通过区块链智能合约，构建安全认证和访问体系；
- 5G+AI时代来临，千亿级的物联网设备，安全问题会更加突出。我们愿与滴滴和各界朋友合作，打造一个具有算力之美的、安全的智能世界；





谢谢观看  
THANK YOU