计 算 即 权 力

比原链AI PoW设计思想

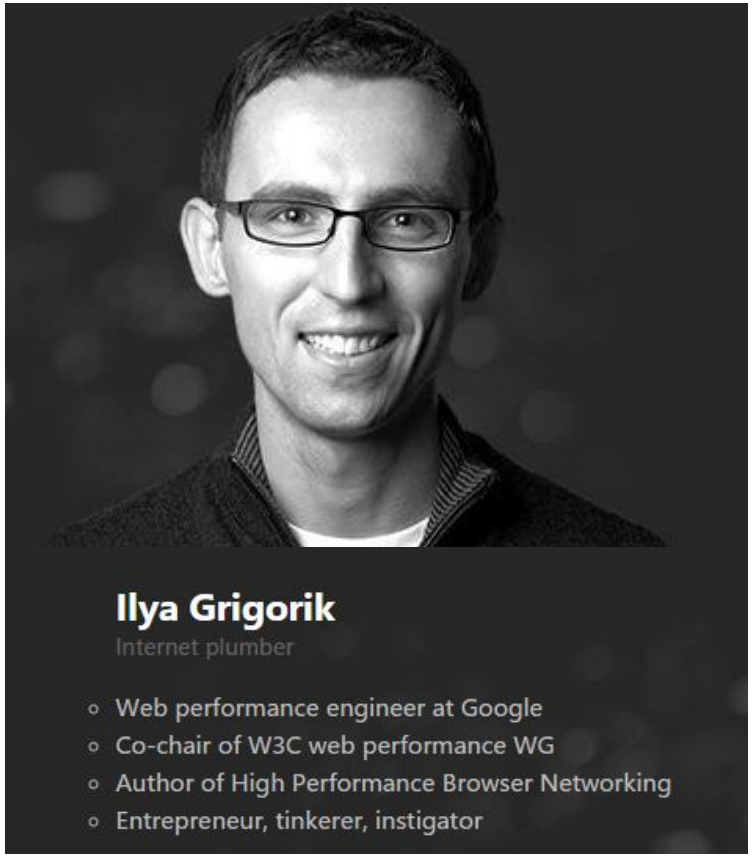
BYTOM 长铗

问题1

为什么需要计算?

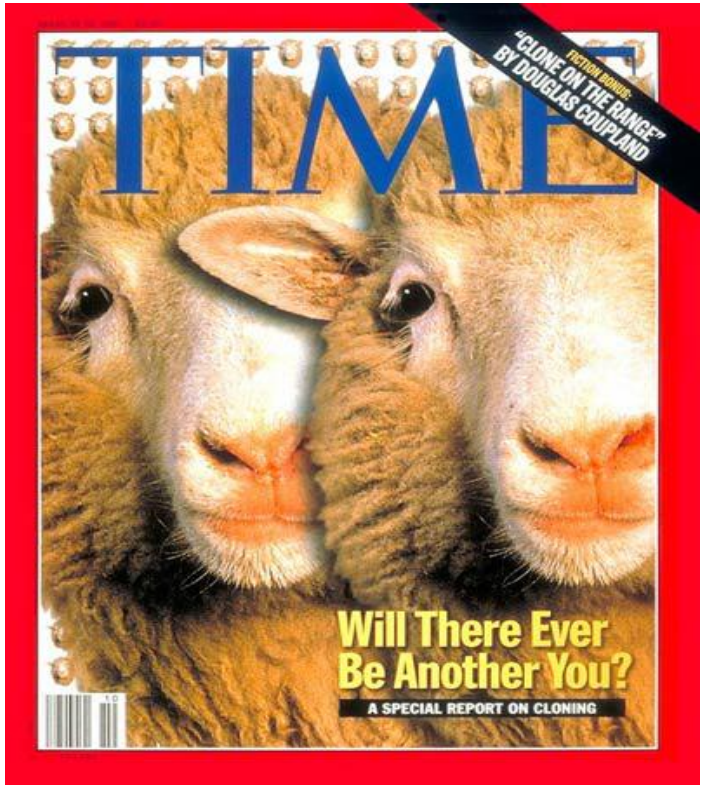
最小可行区块链原理

1. 用三方记账法保障交易安全
2. 用公钥基础设施（PKI）保障交易安全
3. 多方转移和验证
4. 重复消费和分布式一致性
5. 保护网络免受Sybil攻击
6. 建立最小可行区块链

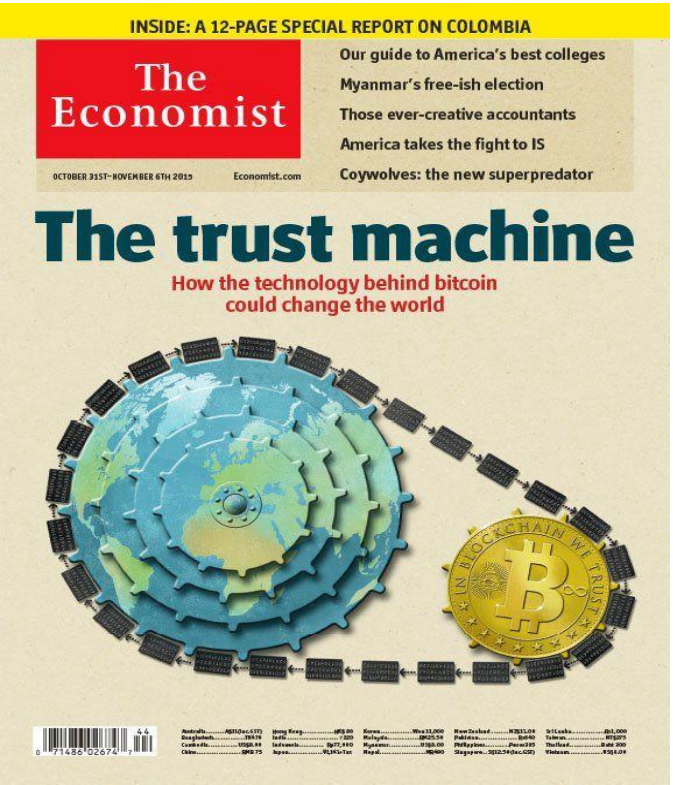


现实世界与数字世界的镜像关系

原子世界/区块链	比特世界/互联网
随机性	伪随机
天底下没有两片相同的树叶	一切东西皆可复制
熵增	熵减（负熵）
正态分布	幂律分布
竞争性资源	非竞争性资源
UTXO（输入=输出）	账户模型（数据库）
区块链	印刷机



1439
印刷机



2008
区块链

不可能三角

去中心化（计算性）
PoW，AIPoW

安全

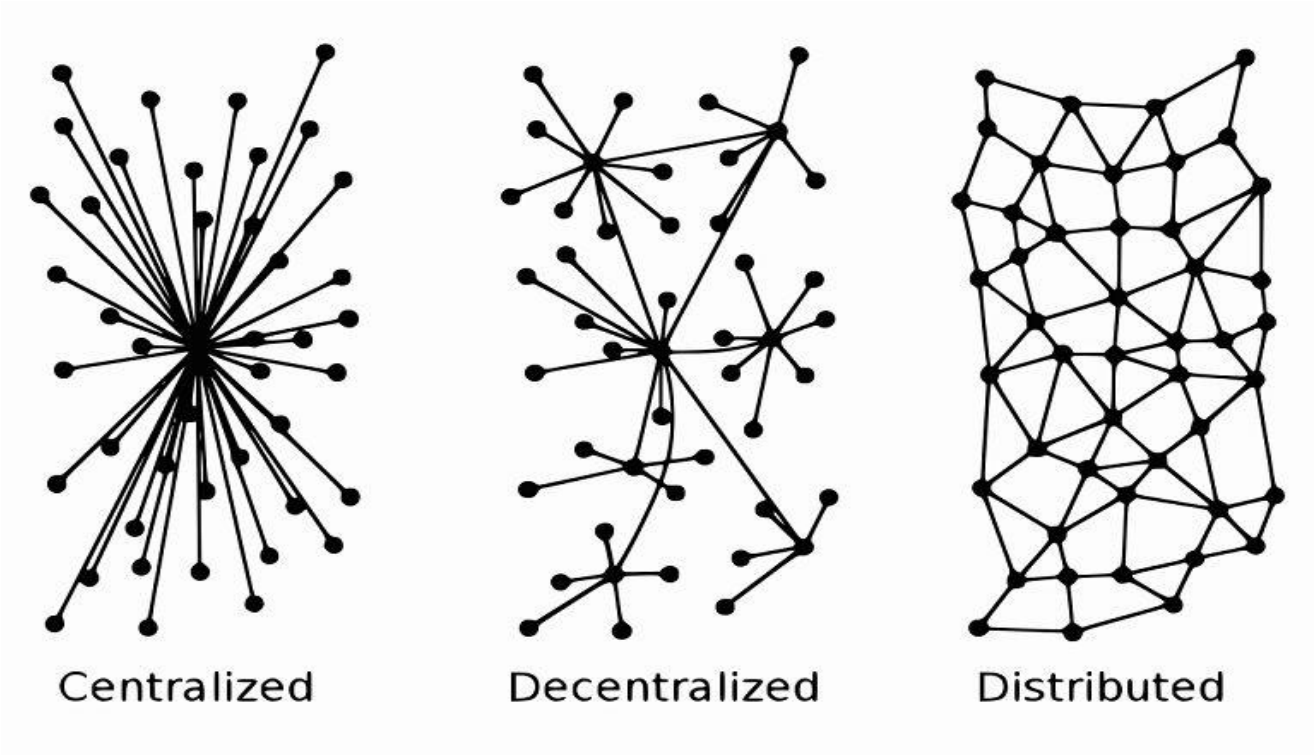
效率（非计算性）
PoS、DPoS、DAG、PBFT

“不可能三角”是指安全，效率（非计算性），去中心化（计算性）三者之间不可共存，而只能取其二。

问题2

什么是真正的去中心化?

中心化、去中心化、分布式



去中心化与中心化

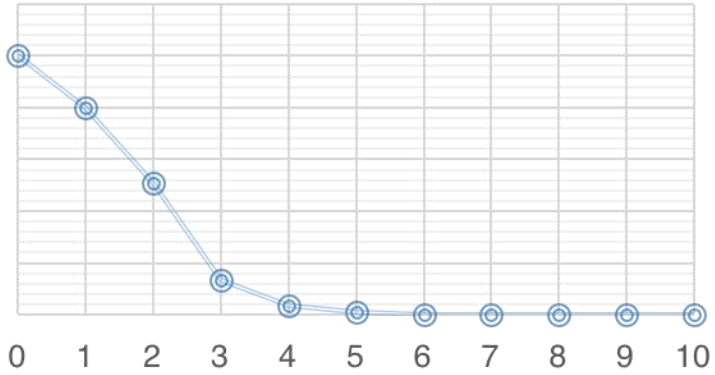
	去中心化	中心化
投票机制	一CPU一票，PoW，AI PoW	一IP一票，DPoS（授信投票） PoS（币天投票）
共识过程和结果	共识过程是自由平等（分散），但可能因市场竞争造成专业分工（集中）	空间上分散，但共识过程是一致行动人（集中）
安全性	是数学问题	是人性问题
时间箭头	交易不可逆转，数据不可篡改	交易可逆转，数据可回滚
硬分叉合法性	仍坚持原链为合法链	新链可能被接受为合法链
权力分配	市场竞争	硬编码系统

PoW的安全性

p=诚实矿工制造出下一个区块的概率
q=攻击者制造出下一个区块的概率
q_z=攻击者最终追上z个区块的差距

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ \left(\frac{q}{p}\right)^z & \text{if } p > q \end{cases}$$

当q=0.1时



当q=0.1时

z的值	p的值
0	1.0000000
1	0.2045873
2	0.0509779
3	0.0131722
4	0.0034552
5	0.0009137
6	0.0002428
7	0.0000647
8	0.0000173
9	0.0000046
10	0.0000012

PoS的安全性

在 PoS 模式下，人人挖矿不可持续，它势必导致赢家通吃的局面。假设电力成本均为3币，大户持有10000币天获得100个利息币，小户持有100币天，获得1利息币，大户得到的币会比小户多得多，如此以来，小户将倾向于关掉客户端，大户则倾向于囤积币天，并获得更多的利息币，这是一个致命的均衡（表1）。

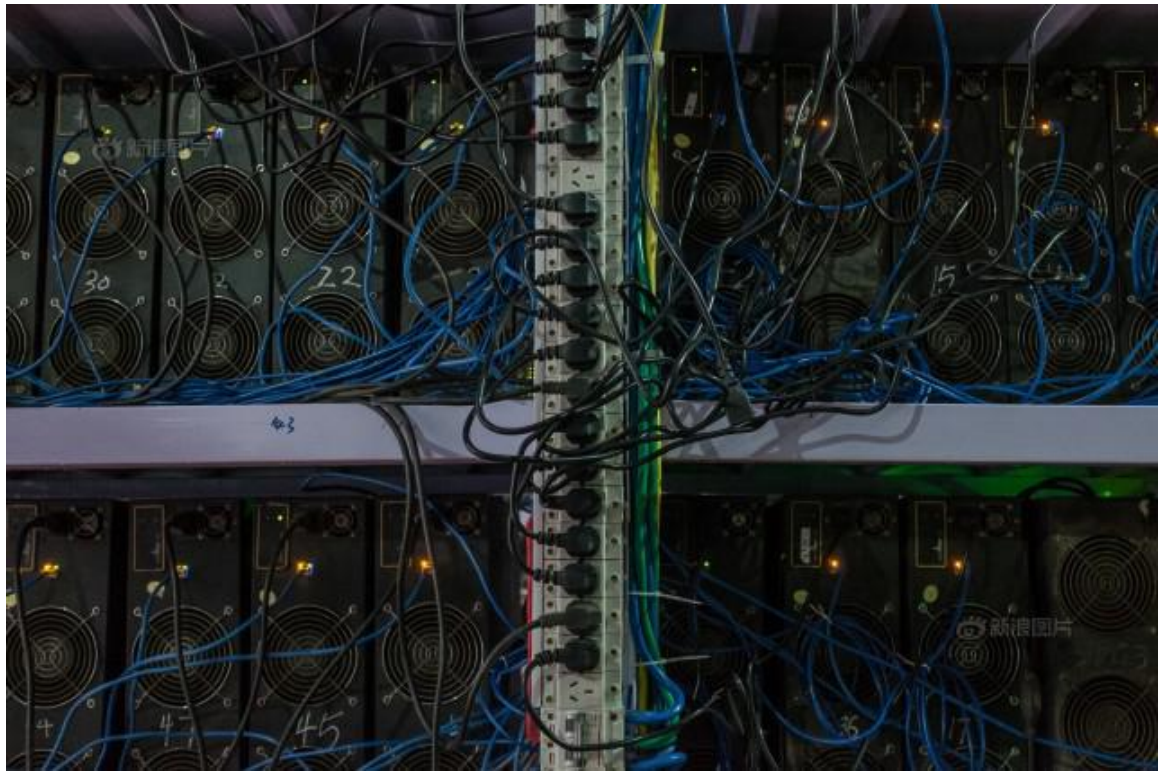
表1 PoS博弈收益矩阵

小户 \ 大户	开机	不开
开机	97，-2	97，0
不开	0，-2	0，0

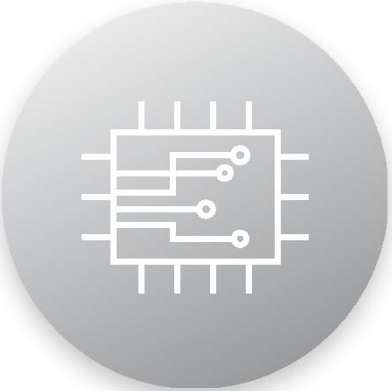
问题3

为什么选择 AI PoW?

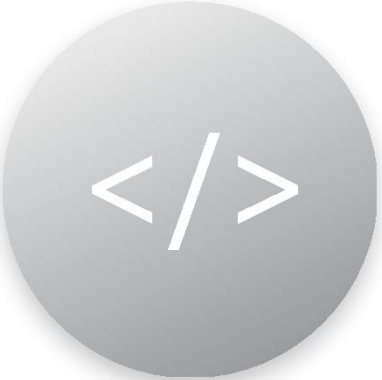
挖矿造成能源与硬件浪费



比原链共识算法的设计目标

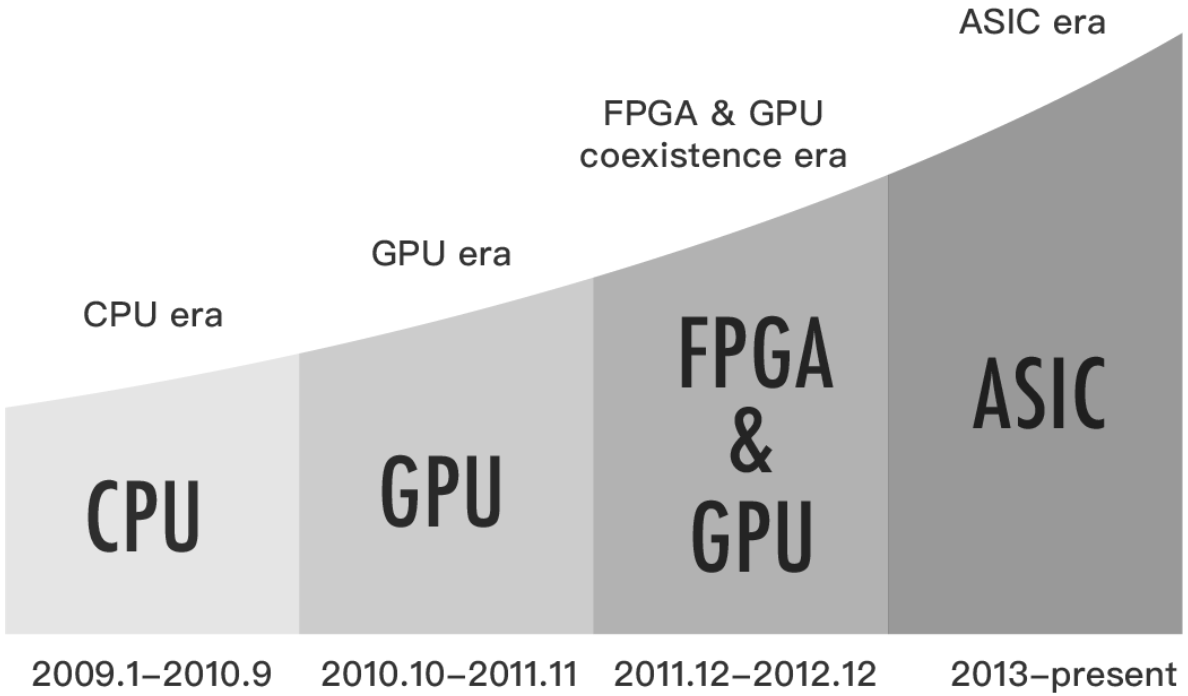


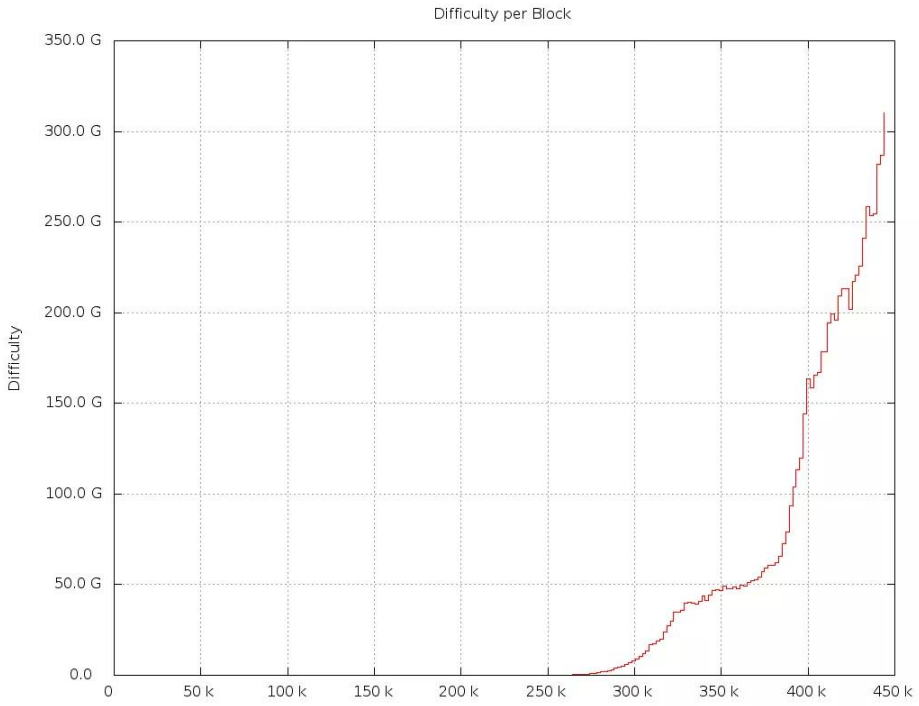
对现有的人工智能
ASIC芯片友好



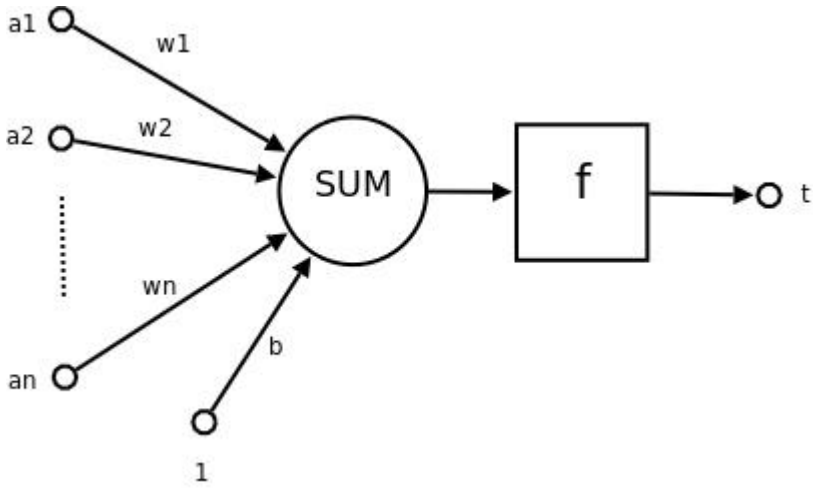
采用人工智能运算过程中
应用最为广泛的算法。

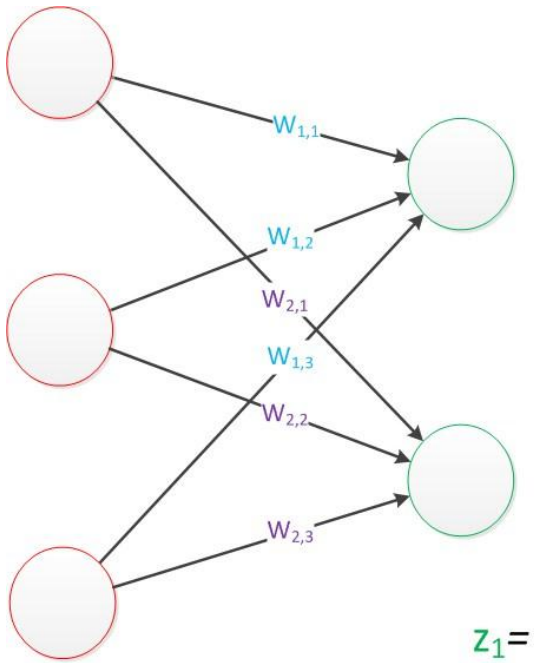
人工智能即将步入ASIC时代





矩阵运算





$$z_1 = g(a_1 * w_{1,1} + a_2 * w_{1,2} + a_3 * w_{1,3})$$

$$z_2 = g(a_1 * w_{2,1} + a_2 * w_{2,2} + a_3 * w_{2,3})$$

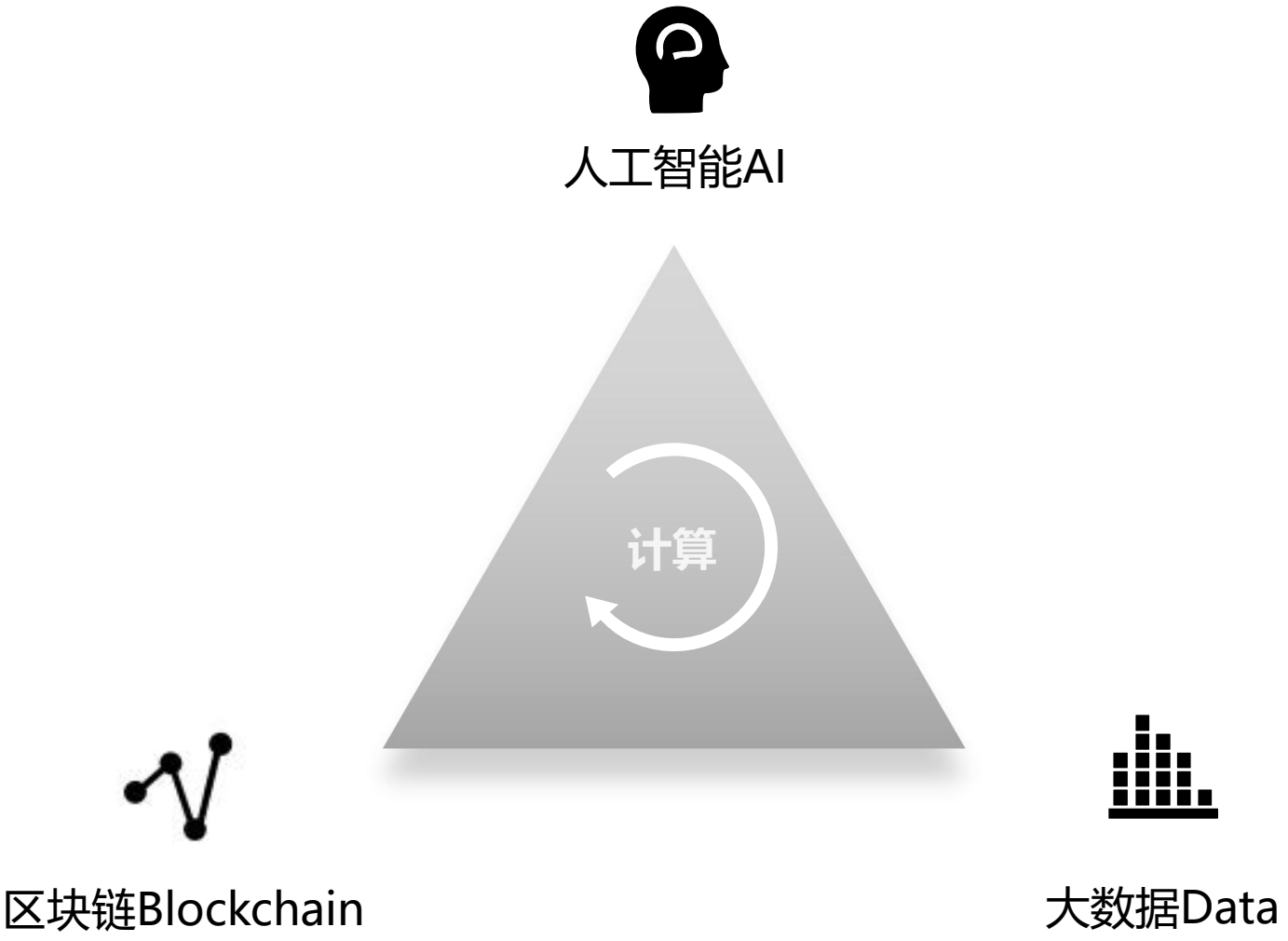
表4. 当前中国核心集成电路的国产芯片占有率

系统	设备	核心集成电路	国产芯片占有率
计算机系统	服务器	MPU	0%
	个人电脑	MPU	0%
	工业应用	MCU	2%
通用电子系统	可编程逻辑设备	FPGA/EPLD	0%
	数字信号处理设备	DSP	0%
通信装备	移动通信终端	Application Processor	18%
		Communication Processor	22%
		Embedded MPU	0%
		Embedded DSP	0%
	核心网络设备	NPU	15%
内存设备	半导体存储器	DRAM	0%
		NAND FLASH	0%
		NOR FLASH	5%
		Image Processor	5%
显示及视频系统	高清电视/智能电视	Display Processor	5%
		Display Driver	0%
区块链	**矿机**	**ASIC**	**90%**

问题4

什么是“计算即权力”？

计算即权力



Information is power. January 11, 2013. Computing is power. April 24, 2018.

Aaron Swartz