隐私计算-信任机器-赛博星球：人类信任体系的全面重构

北京大数据研究院区块链与隐私计算中心 莫晓康

2021-10-24

1. 数字世界的信任重构
2. 信任机器的基本概念
3. 信任机器的技术突破
4. 赛博星球基建四部曲

21世纪人类大迁移：物理空间→赛博空间

150亿年前：宇宙大爆炸→物理宇宙

飞速奔向数字经济

1994年：互联网革命→赛博宇宙

Cyberspace：赛博空间、信息空间、网络空间、数字世界

商业大迁移，2021（Q1）上市公司，TOP 10：

信息技术7家， 石油1家， 汽车1家， 巴菲特1家。

清华大学李稻葵教授：第四产业概念

第一产业：农业

第二产业：工业

第三产业：服务业

第四产业：信息服务业(未来的)

李稻葵：我坚信第四产业一定会来到，第四产业一定是未来中国经济……最重要的一个产业，而第四产业的“高速公路”与网络，第四产业的“电”、“水”来自于区块链。

世界区块链大会·杭州，2021-07-24

人类信任体系重构：物理信任→赛博信任

商业生态迁移

信任体系迁移

数字世界

信任重构

信任体系：商业社会的核心基础设施。

什么是信任体系？

信任体系：

- 在多边合作中，确保所有参与方遵循事先约定的规范。
- 对违反规范的情况，系统有知晓、制止、惩罚的机制。

信任之两翼：

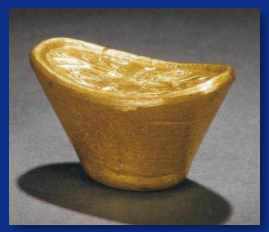
A. 信息规范：能知道什么。

B. 行为规范：能做些什么。

物理世界信任体系：两大要素(人与物)

A. 物理实体及操作

- 自然属性：黄金，稳定性、可度量、匿名性，等等。
- 观察操控：钻石，鉴定、存储、运输、交付，等等。
- 信任要素：身份、道德、商务、财产、法律，等等。







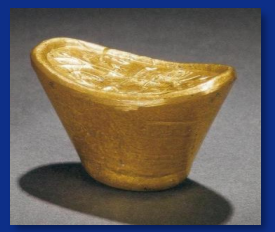

B. 可信第三方(TTP)

- 美元体系、金融机构、担保机构、电商平台、社交平台、证券市场、拍卖市场、中介机构等等。
- 学历证明、在职证明、收入证明、存款证明、房产证明、股权证明、无犯罪证明、公正机构等。
- 在一个理想社会，所有人之间都有绝对信任，上述TTP成为多余，90%传统商业模式都将消失。

赛博世界信任体系：两大要素→数学算法

A. 物理实体及操作→赛博替代（算法模拟）

- 自然属性：黄金匿名性(所有权，交付)，2016年Zcash用零知识证明首次实现。
- 观察操控：隐私计算精准规范，能看什么，能做什么，数学算法替代物理规律。
- 信任要素：身份、道德、商务、财产、法律，用数学算法构建替代物。







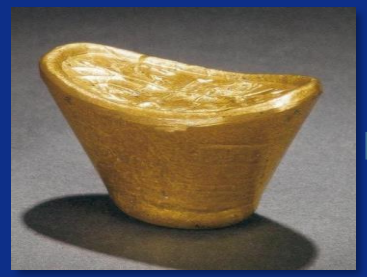
B. 可信第三方(TTP)→信任机器（算法模拟）

- 分布式计算程序+精妙的数学算法→信任机器→替代TTP。
- 间接信任→直接信任，TTP成为多余，TTP商业模式的柯达时刻。
- 人类信任体系全面重构，全新商业模式替代，第二次互联网革命。

数字世界的信任重构：小结

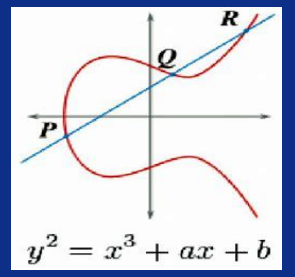
物理空间→赛博空间

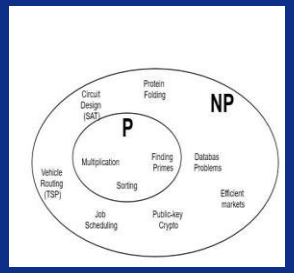
经济活动迁移

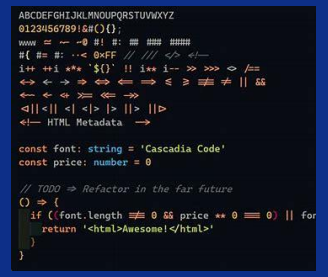


人与物→算法代码

信任重心转移







认知误区：以上变革正是区块链技术的主要使命。

不同视角：区块链≈开胃菜，隐私计算≈真命天子。

1. 数字世界的信任重构
2. 信任机器的基本概念
3. 信任机器的技术突破
4. 赛博星球基建四部曲

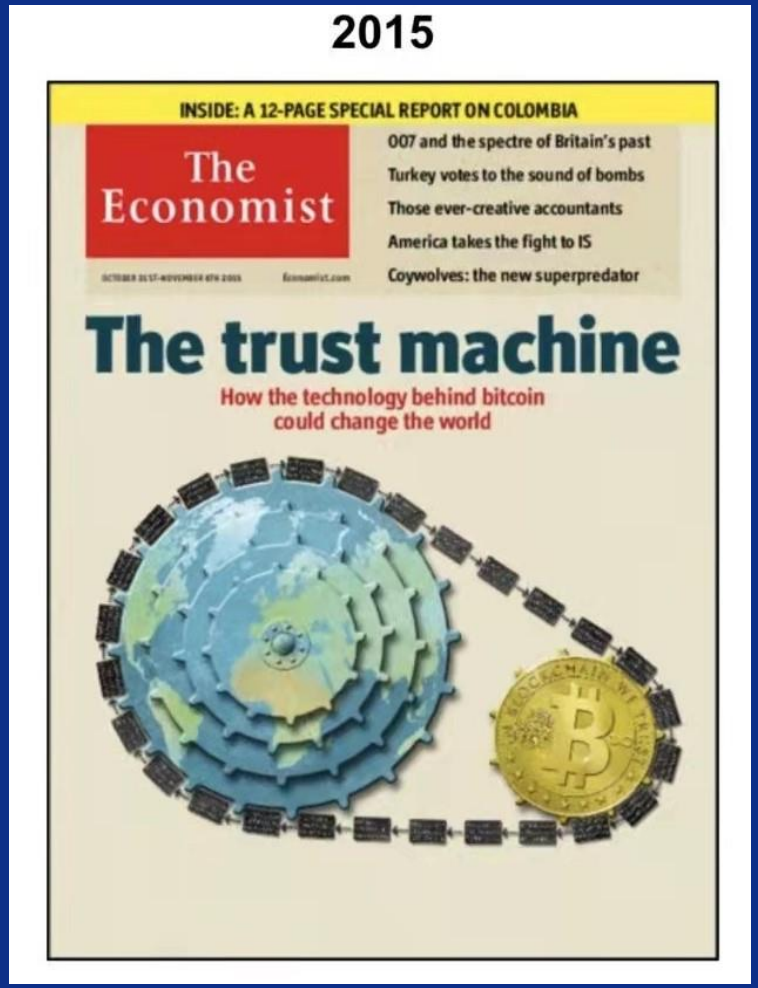
什么是信任机器?

A. 信任重构的核心技术

- 2015年10月《经济学人》封面文章
- 技术演进：区块链→隐私计算→信任机器
- 未来30年大工程，21世纪IT人的重大机会

B. 三个相关的数学难题

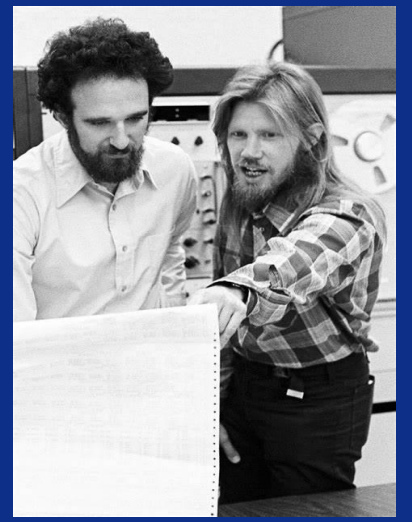
- 电话密谈：a）允许窃听；b）无密码本。
- 电话下棋：a）没有棋盘；b）没有TTP。
- 电话打牌：a）没有纸牌；b）没有TTP。
- 共同目标：脱胎物理世界，进入赛博世界。



电话密谈问题

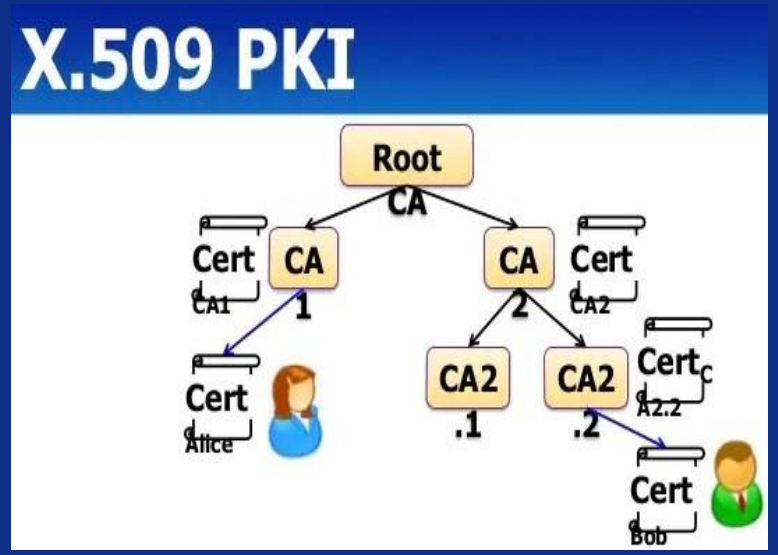
限制条件：① 有窃听者 ② 事先没有密码本（密钥）

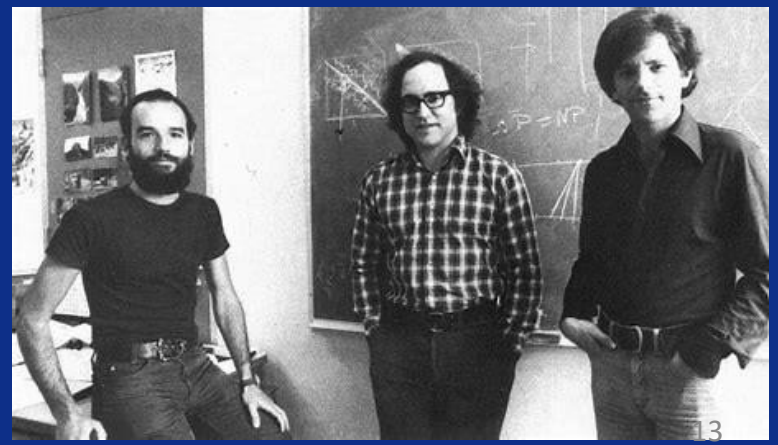
- 秘密通信问题，可用加密解决，但是需要双方事先交换密钥。
- 密钥交换作为物理操作，成本极高。冷战时期苏美红线电话。
- 1974年，Diffie-Hellman提出，能否用公开通信办法解决？
- 1976年，找到数论算法解决此问题，启动了公钥密码革命。



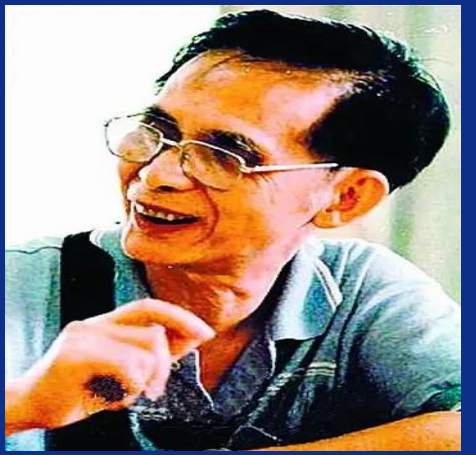
公钥密码革命(1976)

- 1978年，基于数论的RSA算法，首次构建了公钥密码。
- 1995年，Netscape，SSL/TLS/HTTPS，安全浏览器。
- 基于PKI/CA的身份认证体系，电子签名，能安全上网。
- 第一个赛博信任体系，20年电子商务爆发的技术基础。
- 还没有摆脱“物理操作+TTP”模式，但已迈出一步。





电话下棋问题



胡荣华，在上海

杨官麟，在广东

限制条件：① 没有物理棋盘 ② 没有TTP协助

技术问题：要让双方无法犯规，无法抵赖等等。

区块链革命(2009)

- 2009年，区块链诞生，棋局≈账本，一步棋≈一笔交易。
- 第一个赛博空间内在信任体系，摆脱“物理操作+TTP”。
- 赛博空间的内在商业生态，高度脱离物理世界的商业闭环。
- 重大缺陷：没有隐私保护能力，所以是“半信任机器”。

=

电话打牌问题

扑克大师A，在纽约　　双方均不完全知晓的牌局　　扑克大师B，在旧金山

限制条件：① 没有物理纸牌　② 没有TTP协助　③ 只能说话

洗牌过程：双方通过对话，构建一个双方都不知道，但却客观存在的牌序信息。如何做到?

三种数据：① 桌上的牌，对双方保密　② 手上的牌，对一方保密　③ 已出的牌，公开数据。

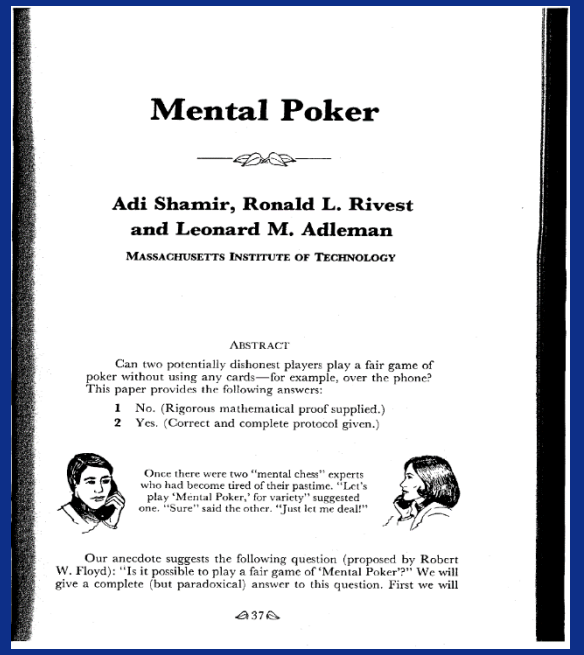
隐私计算革命：算法突破(1979)

Abstract

Can two potentially dishonest players play a fair game of poker without using any cards (e.g. over the phone)?

两个有可能不诚实的玩家，能否不使用任何纸牌(例如说在电话上)，完成一局公正的扑克游戏?

- 1979年，RSA三位作者的MIT论文，Mental Poker。
- 1982年，华人科学家姚期智先生论文，百万富翁问题。
- 早于区块链30年，完全解决了它“遗留”的隐私问题。
- 完成了“全信任机器”的构建，隐私计算科学的诞生。
- 遗留问题：计算成本过高，达不到工程实需要的标准。



Mental Poker

Adi Shamir, Ronald L. Rivest and Leonard M. Adleman

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

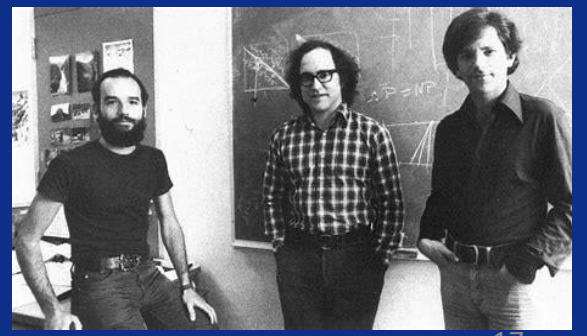
ABSTRACT

Can two potentially dishonest players play a fair game of poker without using any cards—for example, over the phone? This paper provides the following answers:

1 No. (Rigorous mathematical proof supplied.)
2 Yes. (Correct and complete protocol given.)

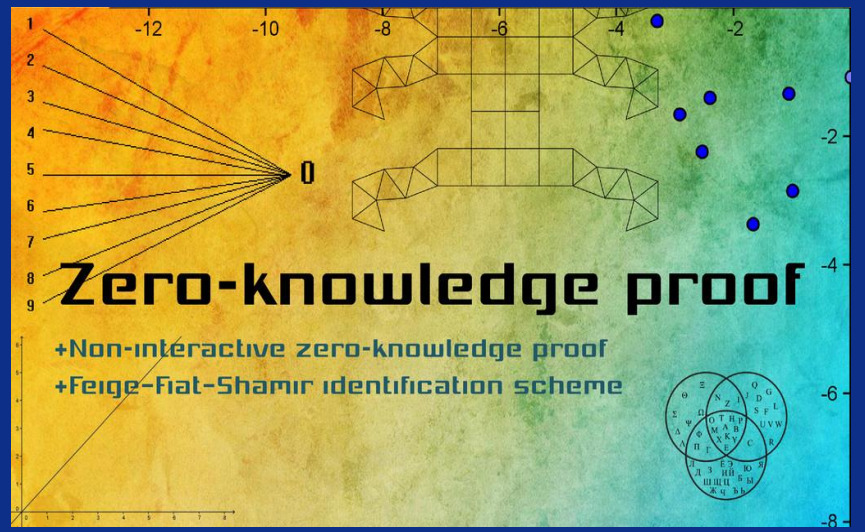
Once there were two "mental chess" experts who had become tired of their pastime. "Let's play 'Mental Poker,' for variety" suggested one. "Sure" said the other. "Just let me deal!"

Our anecdote suggests the following question (proposed by Robert W. Floyd): "Is it possible to play a fair game of 'Mental Poker'?" We will give a complete (but paradoxical) answer to this question. First we will



隐私计算革命：工程突破(2016)

- 2013年，零知识证明第一个工程化算法Pinocchio出现。
- 2016年，Zcash以此首次实现匿名数字货币(赛博黄金)。
- 隐私计算（全信任机器）的第一个大规模工程实用案例。
- 隐私计算革命的第二个里程碑：实验室→产业化落地。
- 2016-至今，零知识证明+区块链技术一系列重大突破。



半信任机器 vs. 全信任机器

A. 信任体系

- 多方合作中，确保各方遵循规范的机制。
- 信息规范：能知道什么。
- 行为规范：能做些什么。

B. 信任机器

- 分布式算法程序，确保各方遵循规范。
- 信任转移：对人与物→对算法与程序。

		半信任机器	全信任机器
代表技术		区 块 链	隐私计算
信任	信息规范	✕	√
	行为规范	√	√
游戏对比		电话下棋	电话打牌
账本对比		公开账本	保密账本
商业应用		有天花板	未来方向

C. 商业应用

- 对真实商业应用，隐私问题是绝对刚需，而不是选项。
- 没有隐私计算的区块链，无法与商业逻辑深度融合，5-10年后是否会淘汰？

不用隐私计算，能解决隐私问题吗？

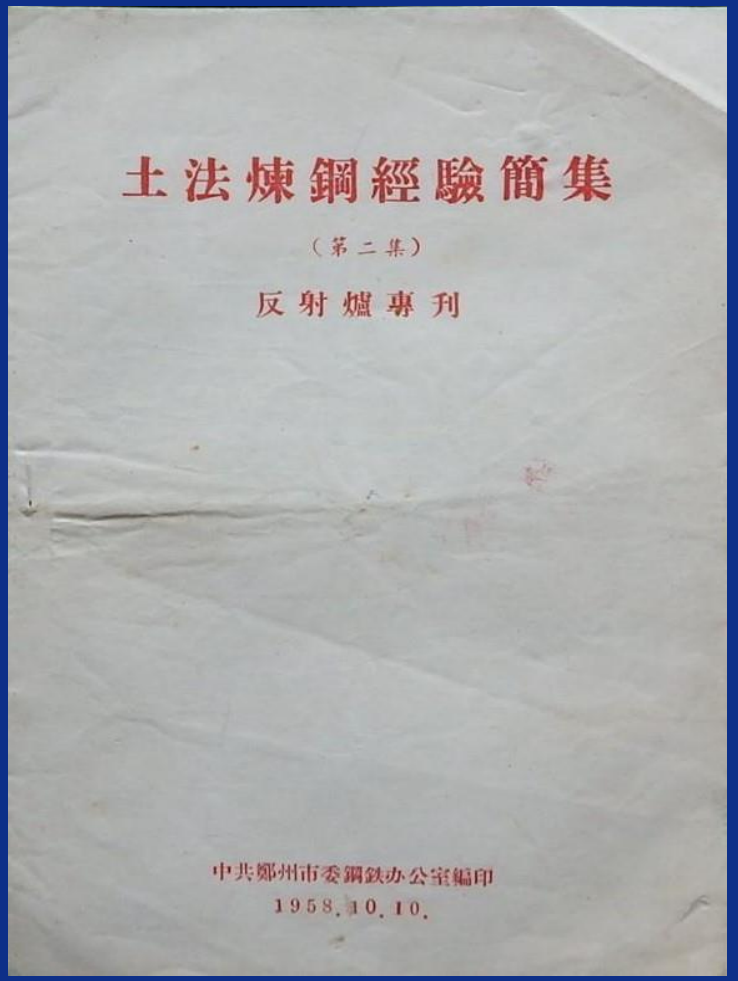
保护隐私之权宜法门：

① 中 本 聪：频繁更换密钥，土法炼钢，无奈之举。

② 哈希上链：数据化石，杀敌1000，自损800之法。

③ 访问控制：传统IT思想复辟，“不可见则不可用”。

试金石：① 能打牌吗？② 不能打牌的区块链，能做深度商业应用吗？



信任机器的基本概念：小结

公钥密码技术：前信任机器
区块链技术：半信任机器
隐私计算技术：全信任机器
未来更强技术：……

哈希值上链、访问控制，主流之外的技术补丁

信任机器技术主流

信任体系重构
商业生态颠覆

50年后，没有银行的世界？…

认知误区：哈希上链与访问控制技术路线，构成产业化区块链的主流。
不同视角：传统IT的技术补丁，临时治标的权宜之计，或非未来所在。

1. 数字世界的信任重构
2. 信任机器的基本概念
3. 信任机器的技术突破
4. 赛博星球基建四部曲

Vitalik Buterin不可能三角形（三难问题）

A. 信任机器实用化的瓶颈问题

- 通用MPC理论1990前完成，实用化瓶颈在于性能。
- 区块链虽然是“半信任机器”，但性能初步可接受。
- 性能仍不够，集中表现为Vitalik Buterin的三难问题。
- 另一个表述：计算能力、存储能力、隐私能力问题。
- 解决上述问题，成为区块链技术创新的核心议题。

B. 零知识证明：破解的核心技术之一

- 区块链+零知识证明，构建各种高效全信任机器。
- 最近五年来：令人震撼的成果，不可思议的妙用。
- 未来10-20年区块链产业化应用落地的关键技术。

零知识证明→区块链技术若干重大突破

1. PoW →PoS，分布式抽签，废除挖矿

- 完全解决了挖矿浪费电的问题，以及相关的算力高度集中化问题（矿池等等）。
- VRF（可验证随机函数，其中有零知识证明），实现分布式抽签，选出产生区块的委员会，替代PoW挖矿机制。
- ①随机性：抽签结果不可预测；②可验证性：抽签结果不可伪造；③零知识性：验证过程不泄露抽签者隐私。
- 具体方法：每个节点用私钥进行VRF计算，如中签将结果及证明文件广播出去，其它节点用其公钥进行验证。
- 实现区块链无分叉性，从而达到交易瞬间确认（例如几秒）。

Silvio Micali：2021 PERFORMANCE GOAL

Block proposal time will remain 0.5 seconds.

Block size will grow from 5,000 to 25,000 transactions.

Block finalization time will shrink from 4.5 to 2.5 seconds.

Finalized TPS will grow from 1,000 to 46,000.

零知识证明→区块链技术若干重大突破

2. 区块链扩容的zk-rollup方案

- 将大量计算与存储挪到主链以外做，结果上传主链并附正确性证明，由主链进行检验后确认上链。
- 核心技术：零知识证明，同时解决扩展性与隐私性；TPS从几十提高到几千（预计加分片技术可达10万）。
- 以下是Vitalik Buterin的估算：

Application	Bytes in rollup	Gas cost on layer 1	Max scalability gain
ETH transfer	12	21,000	105x
ERC20 transfer	16 (4 more bytes to specify which token)	~50,000	187x
Uniswap trade	~14 (4 bytes sender + 4 bytes recipient + 3 bytes value + 1 byte max price + 1 byte misc)	~100,000	428x
Privacy-preserving withdrawal (Optimistic rollup)	296 (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient + 256 bytes ZK-SNARK proof)	~380,000	77x
Privacy-preserving withdrawal (ZK rollup)	40 (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient)	~380,000	570x

零知识证明→区块链技术若干重大突破

3. IPFS分布式存储

- 把互联网上分散的存储资源，整合成一个统一可用资源，与中心化的云存储形成对照。
- 基于存储证明（proof of storage，零知识证明的应用），确保存储服务方不能造假。
- 防范三种攻击：① Sybil Attacks ② Outsourcing Attacks ③ Generation Attacks。
- 挑战-响应的互动式证明→非互式动式，运用VDF（随机延迟函数），防止证明方提前生成证明。

4. 互联网计算机

- 把互联网上分散的计算资源，整合成一个统一可用资源，与中心化的云计算形成对照。
- 基于一系列密码学算法，形成ICP协议，协调分散各处的计算中心，形成统一计算能力。
- 作为互联网上公共服务，试图彻底改变互联网高度依赖“Big Tech”的开发与服务生态。
- CanCan ≈ Decentralized TikTok；Endorphin ≈ Decentralized Android。
- Badlands：Data Centers vs. every person is a node, inexpensive hardware。

零知识证明→区块链技术若干重大突破

5. 分布式证券交易系统

- SBA：借鉴Algorand的相关技术，实现区块链无分叉，交易迅速确认。
- Proof-of-Blind Bid：隐私PoS（权益证明），保证系统维护者的隐私性。
- Phoenix：将Zcash单资产隐私技术，拓展到多资产，支持传统证券交易。
- Zedger：提供专门技术工具，以满足监管部门的合规性要求。
- Rust VM：内置零知识证明功能的虚拟机，基于PLONK/Plookup等方案。
- 区块链技术从加密币圈子走向真实经济领域的一个尝试。

6. 极轻量级区块链

- 运用隐私计算中最精妙的技术之一，递归零知识证证明，将任意区块链压缩到几十KB，手机即可运行。
- 极大提高信任效率，降低信任成本，原则上可实现几十亿人共同维护区块链，构建全球一体互信体系。

零知识证明→区块链技术若干重大突破

7. 零知识证明+HTTPS

- 通过HTTPS获得经过机构签名的可靠数据来源，以隐私方式使用，形成真实世界与加密世界的桥梁。
- 用户通过自己的权限，查询私有数据，用零知识证明向第三方证明。
- 可以通过区块链，引入时间的概念，对特定时间、特定网站的特定信息，进行有效存证。
- 案例：某日在社交网站的发帖，获得多少点赞；在某杂志发表了什么文章。

8. 零知识证明与机器学习

- 机器学习模型，向社会提供公共服务。模型方需求：模型参数保密，甚至模型结构保密。
- 使用方需求：保证所提供服务的真实性，即所给结果确系按某个模型计算所得。
- 零知识证明：可以同时满足以上两项需求。

信任机器其它技术：MPC/FHE/TEE

	技术路径	信任来源	信任机器	速度
0	中心化 IT	人类自律	不是	快
1	区块链（中本聪版）	数学算法	半信任机器	可用
2	零知识证明（或+区块链）	数学算法	全信任机器，特定	可用
3	MPC/FHE（或+区块链）	数学算法	全信任机器，全能	很慢
4	TEE（或+区块链）	硬件厂商(+算法)	全信任机器，全能	足够快
5	混合方案	混合	–	–

小结：春秋战国时代，八仙过海，各显神通，未来走向融合的可能性。

1. 数字世界的信任重构
2. 信任机器的基本概念
3. 信任机器的技术突破
4. 赛博星球基建四部曲

赛博星球：为何需要基础设施建设？

人类迁移

物理世界的生存条件，几千年构建的基础设施：

- 空气、水、食物、温度
- 服装、房子、烹饪食物、交通运输（路、桥、车、船）
- 通讯、能源、生产能力、仓库
- 组织形态、政府、公司、协会、司法
- 货币、银行、金融体系、中介机构

赛比星球需要构建替代物，也许几十年：

- 信任：身份、信息、财产、规则
- 经济：货币、交易、合作贡献价值认定、财富分配
- 组织：决策机制、人类自我管理
- 信任是其它的基础，这里的重点

赛博星球-基建四部曲：荒漠→绿洲

	Cyber 1.0	Cyber 2.0	Cyber 3.0	Cyber 4.0
	1994	2009	2016	today-2050
标志技术	安全浏览器	区 块 链	隐私计算	跨链一体化
	前信任机器	半信任机器	全信任机器	全球信任基础设施
科学理论	公钥密码	公钥密码	隐私计算	隐私计算
信任模式	间接信任-依赖TTP	直接信任-不依赖TTP（颠覆传统商业模式）		
商业影响	电子商务	虚拟经济演练	回归实体经济	演绎柯达故事

赛博星球-基建四部曲：荒漠→绿洲

	Cyber 1.0	Cyber 2.0	Cyber 1.5/2.5	Cyber 3.0	Cyber 4.0
	1994	2009	2016	2016	today-2050
标志技术	安全浏览器	区 块 链	哈希上链 +访问控制	隐私计算	跨链一体化
	前信任机器	半信任机器	信任机器+传统IT	全信任机器	全球信任基础设施
科学理论	公钥密码	公钥密码	公钥密码+IT思维	隐私计算	隐私计算
信任模式	间接信任	直接信任	混合模式	直接信任	直接信任
商业影响	电子商务	虚拟经济演练	企业试验+天花板	回归实体经济	演绎柯达故事

赛博星球 4.0：全球信任基础设施

开始时间：现在-2050

所用技术：所有信任机器技术，跨平台整合

总体目标：

- 全球计算与存储资源，整合成为一台计算机
- 全球数据资源，全部隐私共享，可用不可见
- 互联网→互信网，间接信任 →直接信任（做恶成本）
- 物理与数字世界打通，人类信任体系全面重构
- 颠覆几千年商业生态，大范围演绎柯达故事

感谢您的参与！