

# 隐私计算研究分享

节点资本 朱子川



# 节点资本项目分类







NODE CAPITAL

- 更多请查询网站：[www.nodecap.com](http://www.nodecap.com)
- 在推特上关注我们: [@Node\\_Capital](https://twitter.com/Node_Capital)
- 关注我们的微信公众号[nodecapital](#)，了解最新的节点动向
- 如果你有好的区块链项目，请发送邮件至  
[Dream@nodecap.com](mailto:Dream@nodecap.com)
- 商务合作，请联系[partner@nodecap.com](mailto:partner@nodecap.com)
- 我们也欢迎您对报告翻译的一般反馈



# 目录


---

- 1、什么是隐私计算
- 2、隐私计算技术分类
- 3、隐私计算项目对比
- 4、隐私计算投资逻辑



# 加密货币隐私领域概览

Richard Chen (2018) 在他的文章An Overview of Privacy in Cryptocurrencies提出了一个比较全面的关于加密货币隐私性题材领域的一个全面性概述，把加密货币隐私领域分成四个方面：1) 隐私性代币 (Privacy Coins)，2) 智能合约的隐私(Smart Contract Privacy)，3) 隐私性基础设施(Privacy Infrastructure)，以及4) 隐私性研究(Privacy Research)。

<u>Privacy Coins</u>	<u>Smart Contract Privacy</u>
 CASH  MONERO  Grin  BEAM  MobileCoin	Zether  ORIGO <b>KEEP</b>   enigma <b>OASIS</b> LABS
<u>Privacy Infrastructure</u>	<u>Privacy Research</u>
 CoinJoin  KOVRI <b>BOLT</b>  ORCHID <b>NUCYPHER</b>  STARKWARE	Zero-Knowledge Multiparty Computation Fully Homomorphic Encryption



# 什么是隐私计算



隐私交易是最早发展的一个分支，其代表技术包括**密钥混合**、**环签名**、**零知识证明**。

隐私存储不仅在区块链领域，在云计算领域也是较热门的领域，其代表技术有**数字签名**、**密钥分发**、**密钥管理**等。

隐私计算是技术难度最高的一个分支。其代表技术有**同态加密**、**可信执行环境**、**多方计算**，不可区分混淆和**零知识证明**。

# 隐私计算技术的分类与比较

技术方向	技术细分	描述	目前问题
同态加密		用符合完全同态条件的函数对明文进行加密后发送给计算节点，返回计算结果后用反函数解密	加密过程耗时较长，生成的公钥很大
可信执行环境	Intel SGX	由硬件厂商经由CPU划分内存区域，构造远程执行沙盒	已经被提出很多可攻击的方法，需要硬件厂商进行验证，有中心化风险
安全多方计算	秘密共享	所有参与者通过分享密文参与，需要计算的函数转化为有限域上的“电路”	需要所有参与者同步进行，不易在有延迟的网络环境进行
	混淆电路	将需要计算的函数解析成布灵电路并进行混淆，再通过不经意传输协议进行密文交换	小型电路表现好，大型电路较慢
	不经意传输协议	一种发送者无法预知是否将正确的信息传送给接收者的协议	
	ORAM	将访问数据时调取的内存地址随机化，使得调取者不能从访问的地址获取任何信息	需要占用客户端存储空间较大
不可区分混淆		将程序代码搅乱成无法理解的形式，但是保留原来的所有功能	尚未有大量实际应用方面的研究
零知识证明	zkSNARK/zkSTAR	基于IOP(交互预言证明)模型的零知识证明方法，证明生成和验证时间有良好可扩展性。	zkSNARK需要信任建立过程，两者生成的证明仍较大
	Bulletproofs	基于离散对数问题的零知识证明方法，生成的交易证明非常小。	验证证明速度较慢



# 隐私计算重点项目比较

项目名称	Enigma	Taxa	Origo	Hawk	Starkware	Wanchain
技术分类	可信执行环境	可信执行环境	零知识证明	零知识证明	零知识证明	多方计算
开始时间	2015年Q1	2018年7月	2018年5月	2016年5月	2017年9月	2017年8月
描述	白皮书中采用多方计算-秘密共享，后改为Intel SGX；实现隐私Dapp平台	基于pBFT共识的通用跨链Layer 2架构，有高性能、可靠性和隐私保护	用不同的零知技术搭配实现隐私Dapp平台	使用zkSNARK，通过一个被信任的合约管理者实现隐私智能合约	使用zkSTARK在以以太坊等不同公链上实现隐私保护功能	使用安全多方计算以及门限密钥共享进行隐私保护，支持跨链交易
团队	MIT	美国团队	硅谷工程师	康奈尔/马里兰大学团队	以色列团队	原Factom创始人
开发进度	数据市场测试网上线	未释放白皮书	有白皮书，Github为空	有白皮书，不开源	有白皮书，不开源	2.0测试网即将上线



# 隐私计算投资逻辑

1、代码隐私

2、和隐私存储结合







# THANKS