区块链的发展与前沿热点

汇报人：仲崇鹏

1

PART 01

发展概述

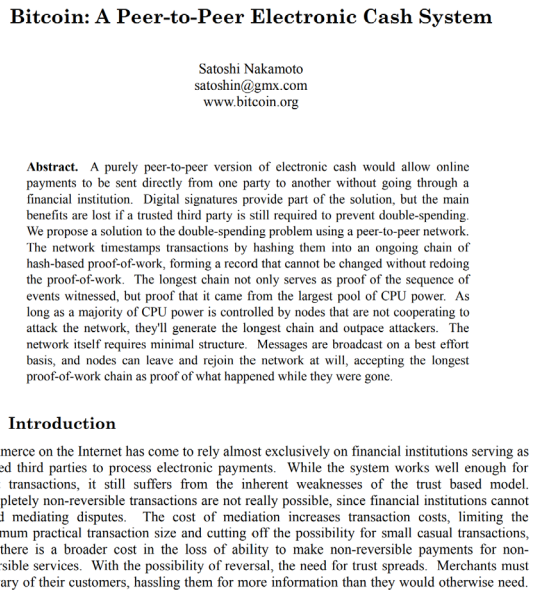
区块链的诞生

比特币

2008年，中本聪在 bitcoin.org 发布比特币白皮书：《Bitcoin: A Peer-to-Peer Electronic Cash System》

区块链

2015年，《The Economist》发表名为《The Trust Machine》的封面文章。



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.

区块链的定义

区块链技术是以数据库作为数据存储载体，以**P2P网络**作为通信载体，依赖**密码学**确定所有权和保障隐私，依赖分布式系统**共识框架**保障一致性，旨在构建价值交换系统的技术。

哈希函数
Merkle树
数字签名
椭圆曲线
环签名
零知识证明

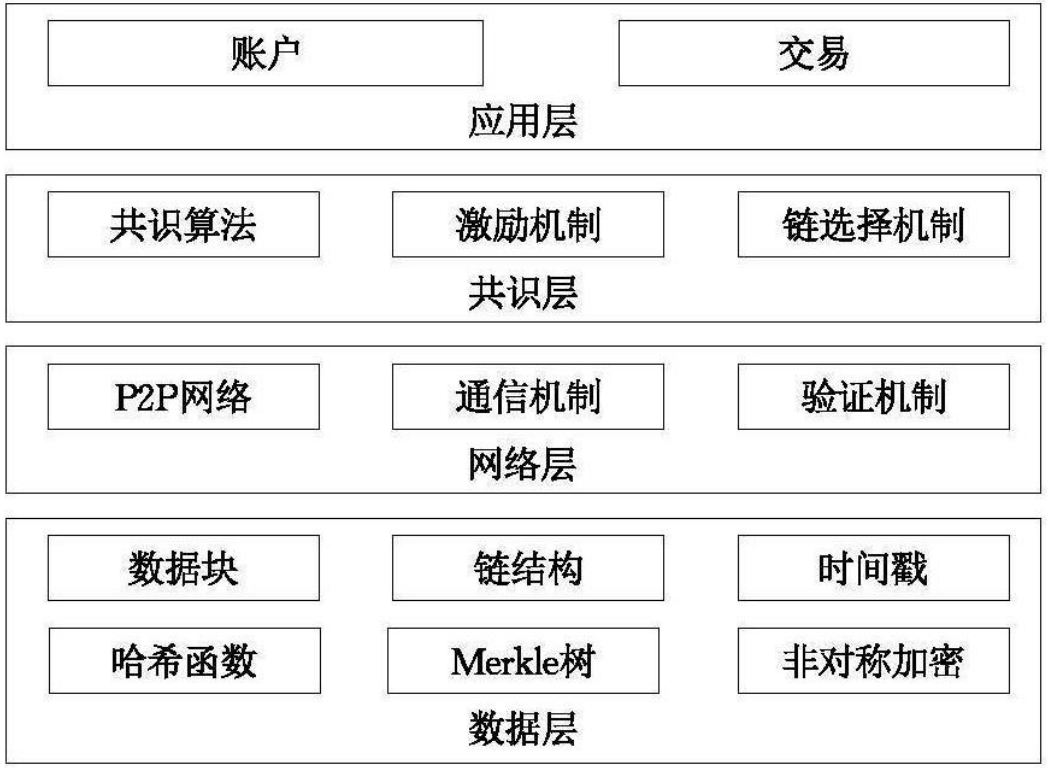
记账节点选取算法
区块生成算法
区块选取算法
激励机制

Proof of Work
Proof of Stake
Proof of Space
……

区块链1.0——数字货币

在区块链1.0时代，主要的应用对象是以比特币为代表的虚拟货币，实现的常用功能为货币转移、汇兑和支付等。

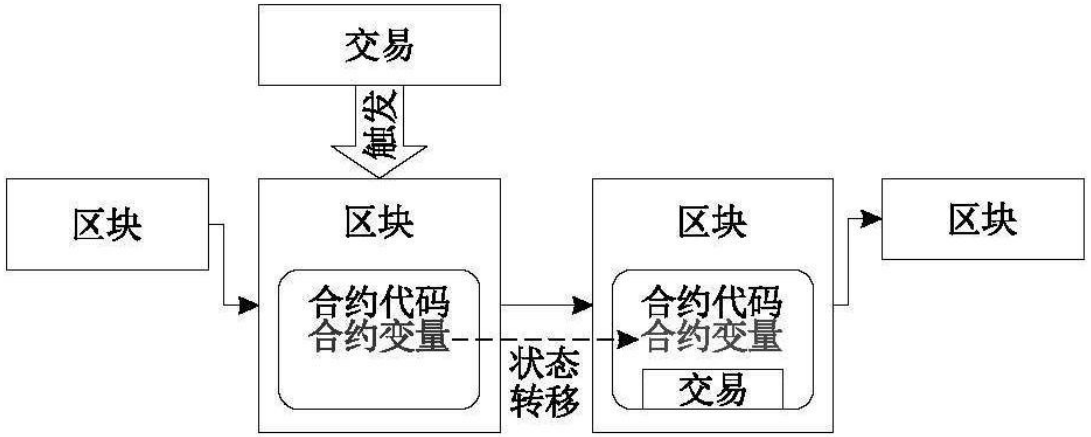
比特币、莱特币、瑞波币、达世币、未来币



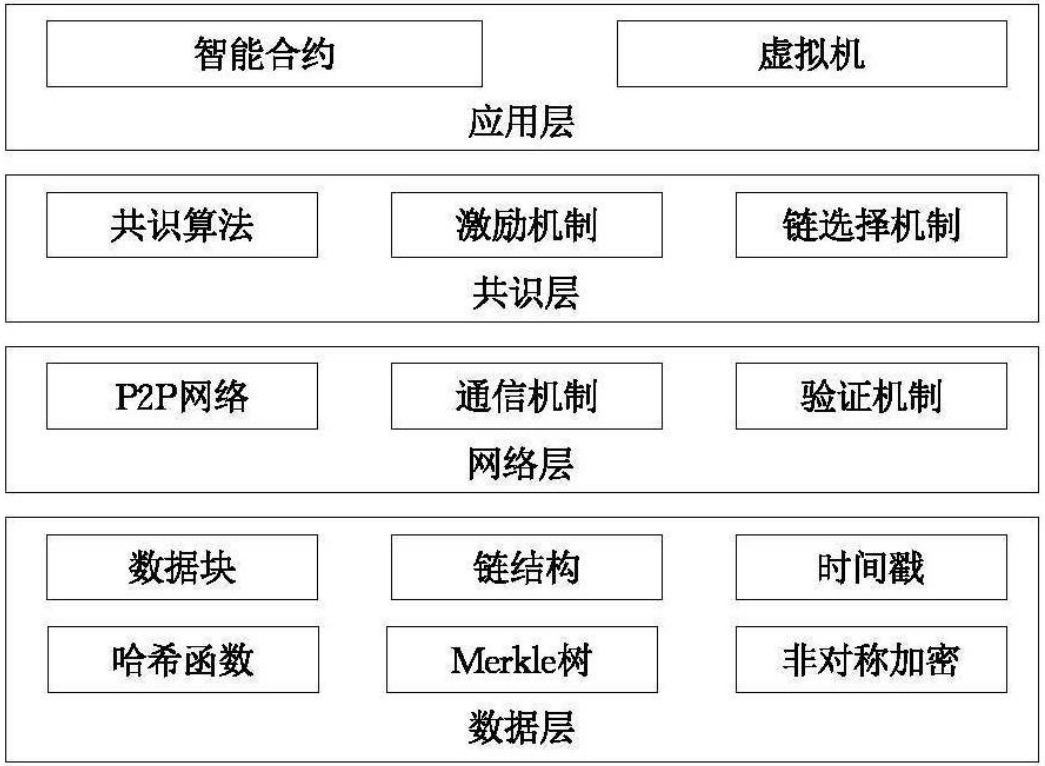
区块链1.0架构

区块链2.0——智能合约

区块链2.0以以太坊为代表实现了更复杂的分布式合约记录——智能合约。



智能合约区块链架构



区块链2.0架构

区块链3.0——扩展的发展领域

区块链3.0将区块链应用的领域扩展到现实场景中，与物联网等其他技术相结合，覆盖人类社会生活的各个方面，在各类社会活动中实现信息的价值证明与保障，不再依靠某个第三方或机构获得信任或建立信用，实现信息的共享，例如医疗健康、知识产权、物联网、社会管理、慈善公益等。

2

PART 02

前沿热点

共识算法

共识机制作为区块链的核心特征，解决了各个独立节点之间互相信任的问题，是保证区块链系统在分布式架构下的一致性方案。

POS 权益证明
Proof of Stake

PoW 工作量证明
Proof of Work

BFT 拜占庭容错算法
Byzantine Fault Tolerance

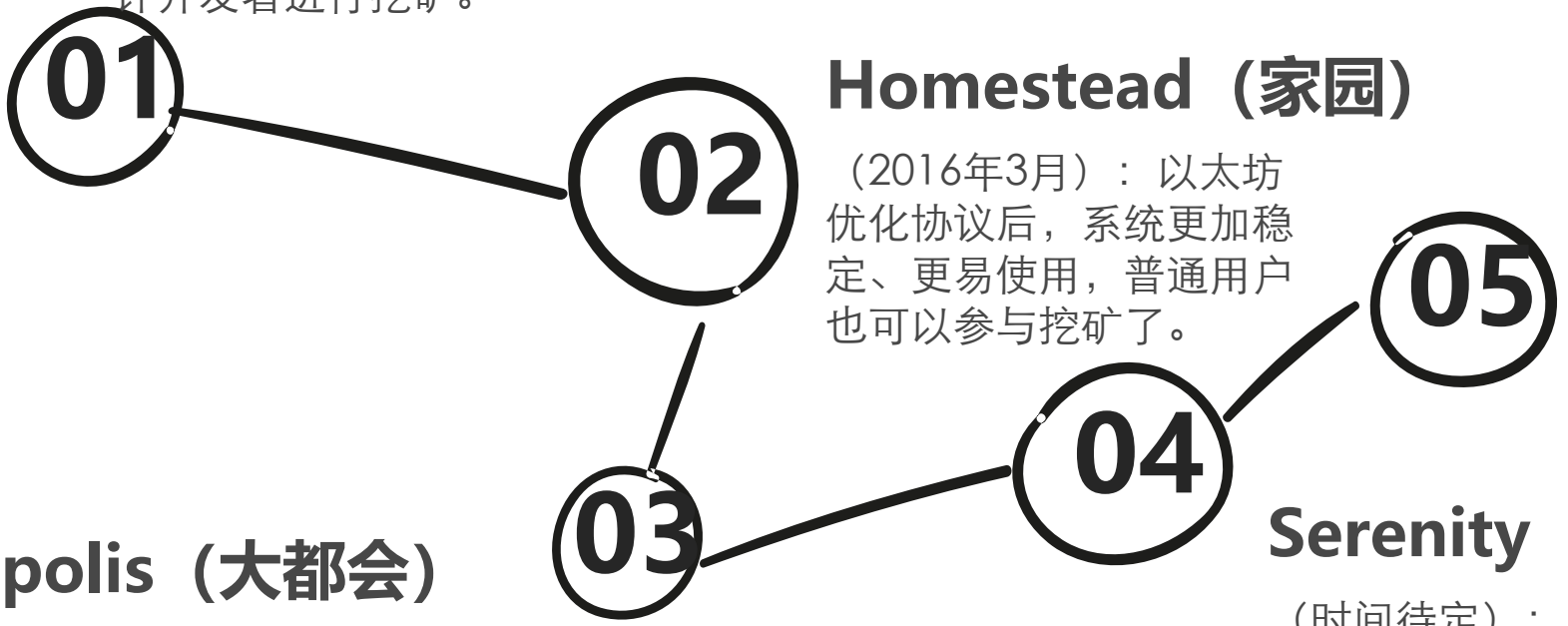
SPoS 委任权益证明
Delegated Proof of Stake

PBFT 实用拜占庭容错
Practical Byzantine Fault Tolerance

ETH 2.0

Frontier（前沿）

（2015年7月）：以太坊的最初版本，非常复杂，只适用于开发者测试，并允许开发者进行挖矿。



Homestead（家园）

（2016年3月）：以太坊优化协议后，系统更加稳定、更易使用，普通用户也可以参与挖矿了。

Future……

Metropolis（大都会）

（2017年10月）：这个阶段被认为是从PoW机制到PoS机制的过渡阶段，以太坊的底层协议发生了重要改变，也就是产生了硬分叉。

Serenity（宁静）

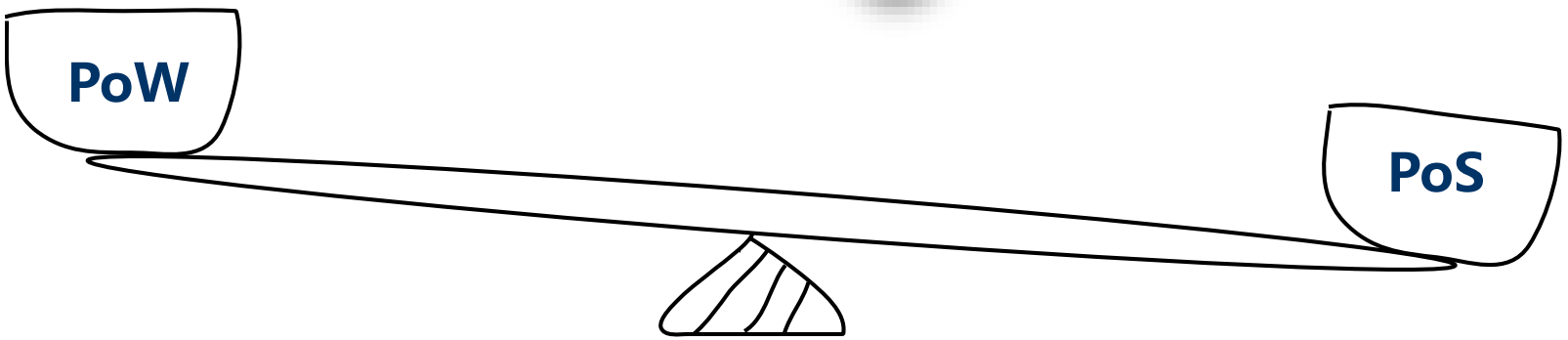
（时间待定）：完全使用PoS机制。

也即 ETH 2.0

PoW or PoS ?

- 算法简单，容易实现，安全性高。
- 资源消耗大，可监管性弱，性能效率低，容易产生分叉。

- 资源消耗较少，性能较高，出块速度较快。
- 可监管性弱。

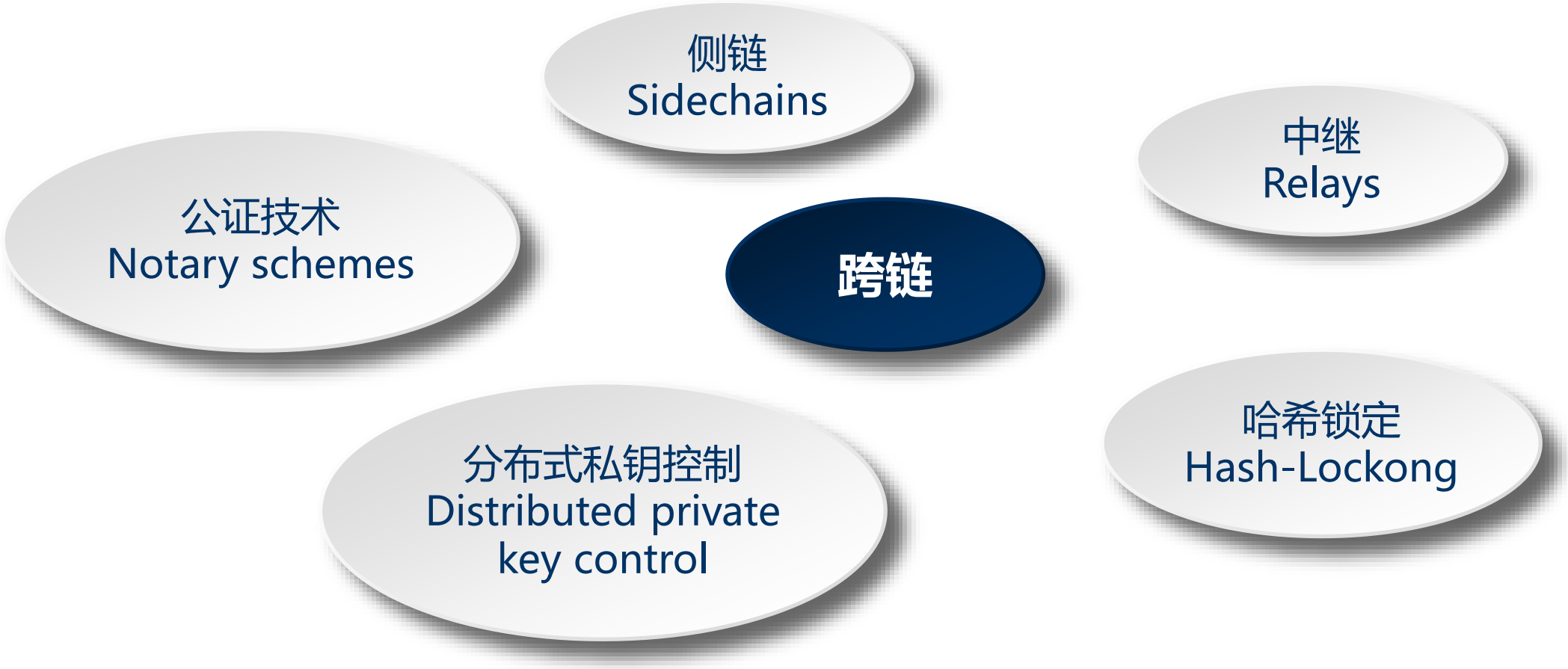


ETH 1.0 和 ETH 2.0 的对比

	以太坊1.0	以太坊2.0
架构	单链	多链（分片）
后端开发	Solidity/Vyper	Solidity/Vyper
执行环境	单VM	多同质分片
可组合性	智能合约可互相同步调用	智能合约可在同一个分片中互相同步调用， 也可在分片之间互相异步调用
治理	off chain	off chain
共识机制	Ethash (PoW)	Casper (PoS)
项目执行费	每次调用以gas进行计价	每次调用以gas进行计价

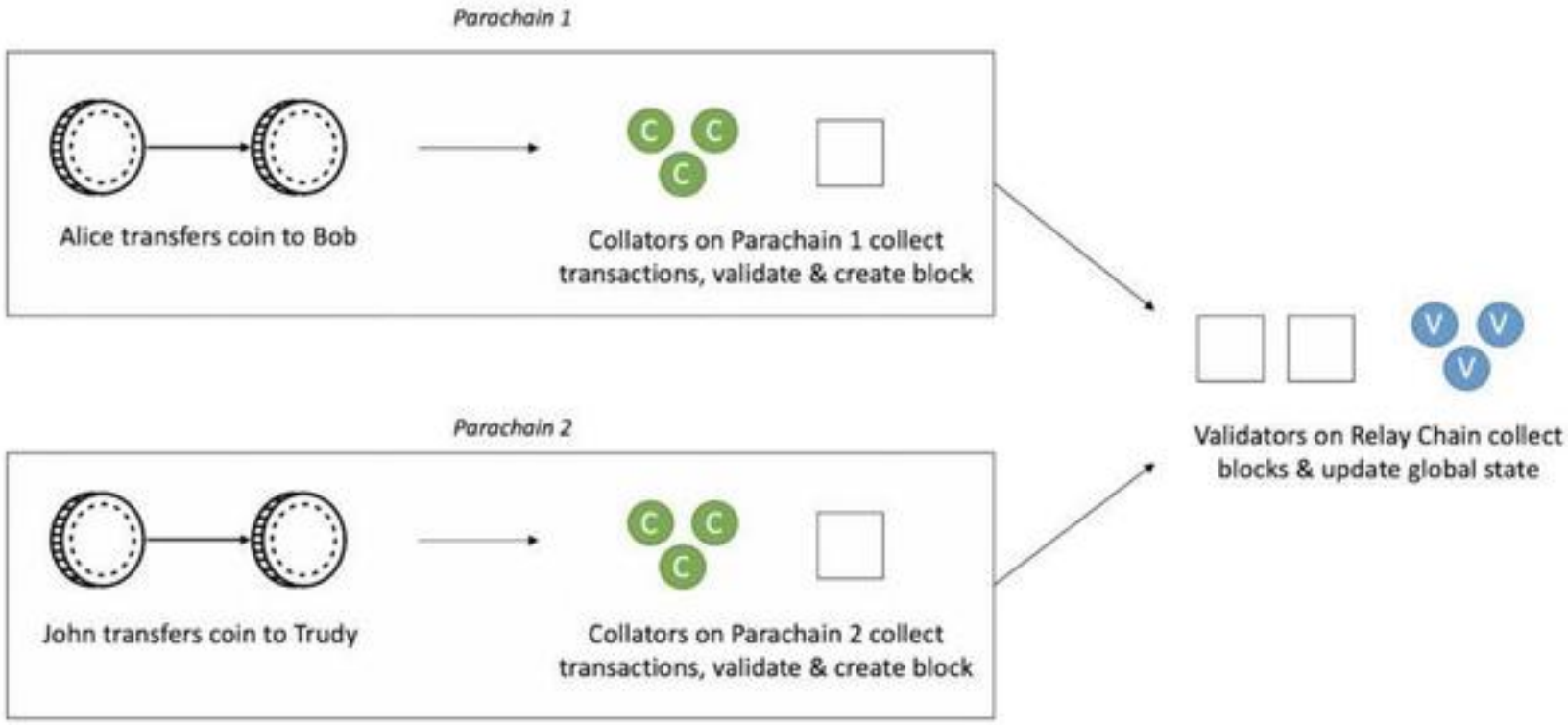
跨链拓展

区块链技术发展至今，公链、联盟链和私有链纷纷涌现，发展的背后是链与链之间高度异构化，形成孤立的价值体系。伴随着落地应用的逐步实现，链间互通互联的重要性日益凸显。



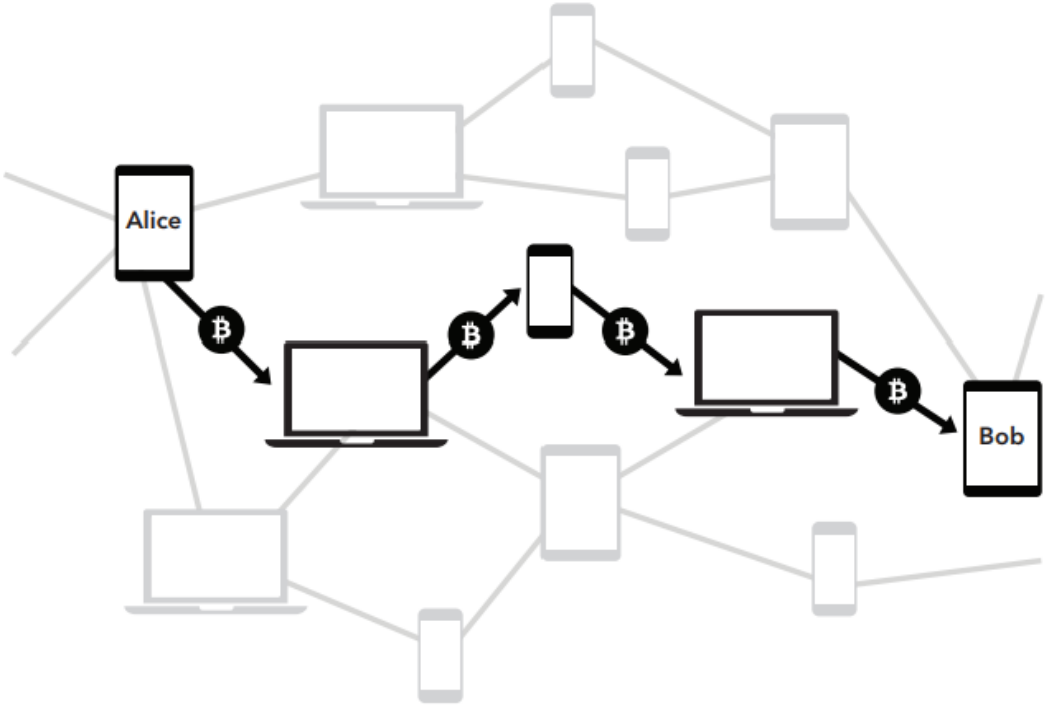
跨链项目：波卡

Polkadot 旨在解决跨链问题，并创建一个可扩展（可随需求增长）的区块链架构。Polkadot定义了一套平行链（Parachain）和中继链（Relaychain），来分别解决扩展性和伸缩性问题。



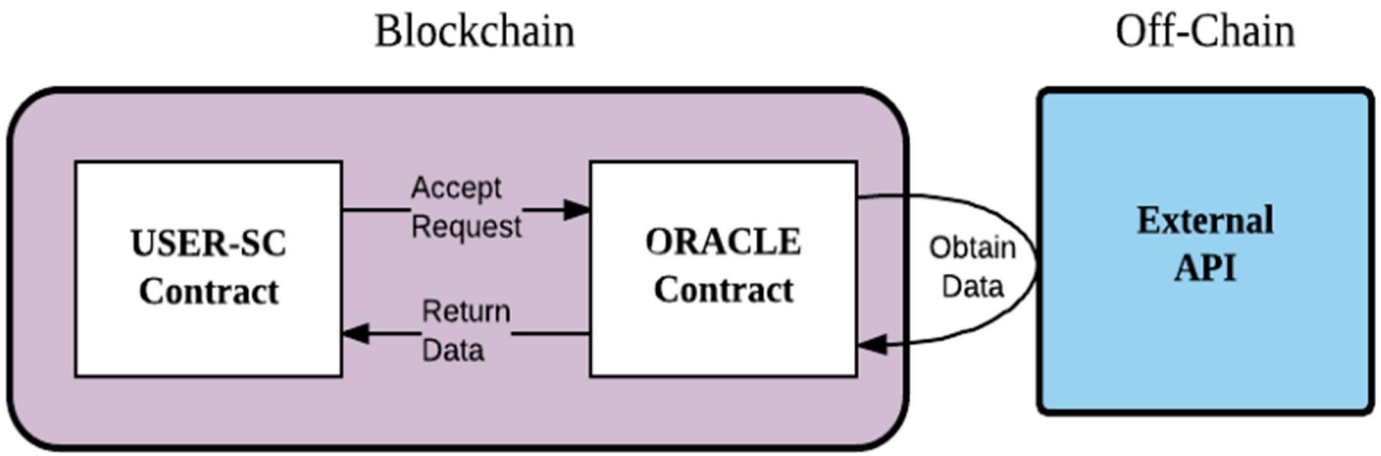
跨链项目：闪电网络

闪电网络 (Lightning Network）的目的是实现安全的链下交易，本质上是使用了哈希时间锁定智能合约来安全地进行0确认交易的一种机制，通过设置巧妙的“智能合约”，使得用户在闪电网络上进行未确认的交易和黄金一样安全（或者和比特币一样安全）。



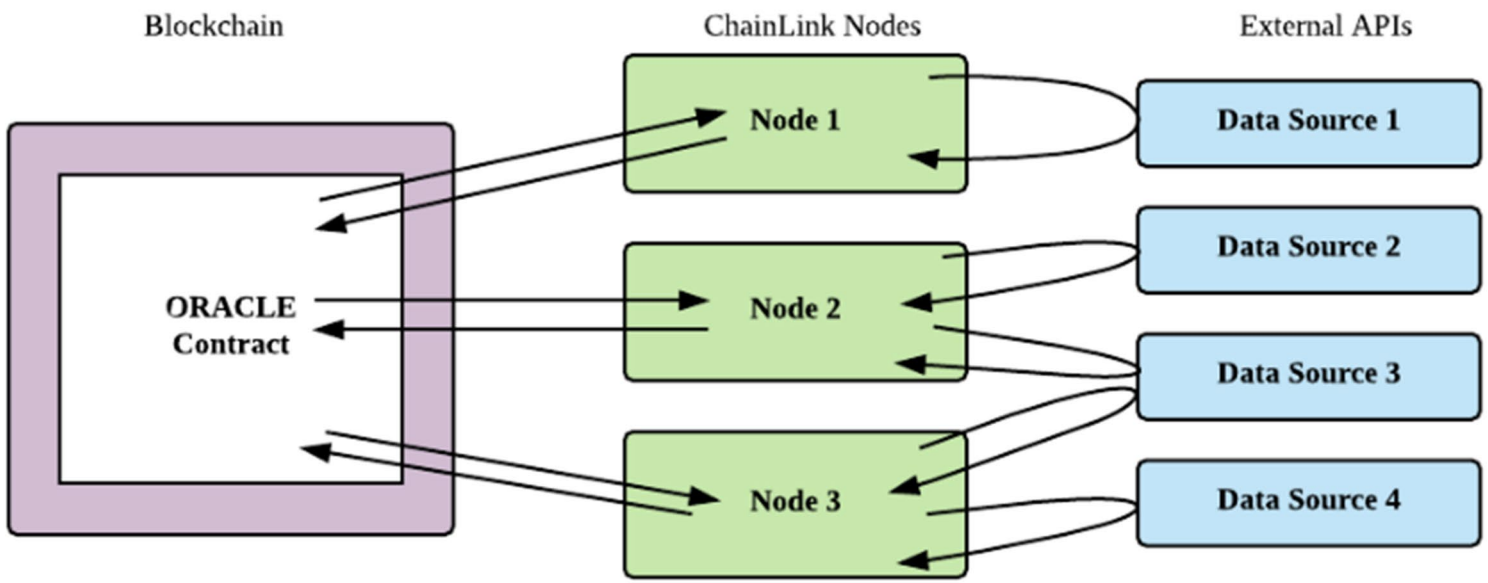
预言机

预言机（Oracle）提供了一种无信任的方式来获取链外的信息，用于以太坊平台上的智能合约。可以将预言机视为弥合链外世界与智能合约之间差距的机制，允许智能合约基于真实世界的事件和数据来强制执行合约关系。



为了提高预言机的准确性，产生了以Chainlink为代表的分布式预言机。

分布式预言机的链外聚合是由门限签名（BLS）算法完成的。



网络安全与隐私保护

双花攻击

自私攻击

扣块攻击

日蚀攻击

平衡攻击

女巫攻击

重放攻击

……

匿名性分析

混币技术

环签名

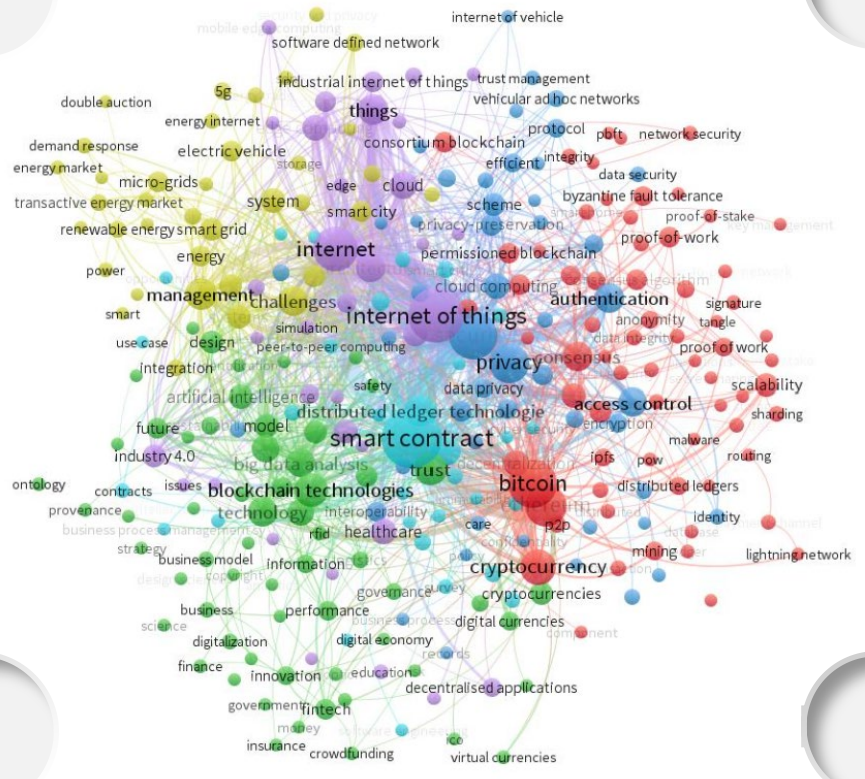
零知识证明

学术领域

区块链技术体系

智能合约

比特币、加密货币



物联网、云计算

数据安全、隐私保护

智能电网、智慧城市

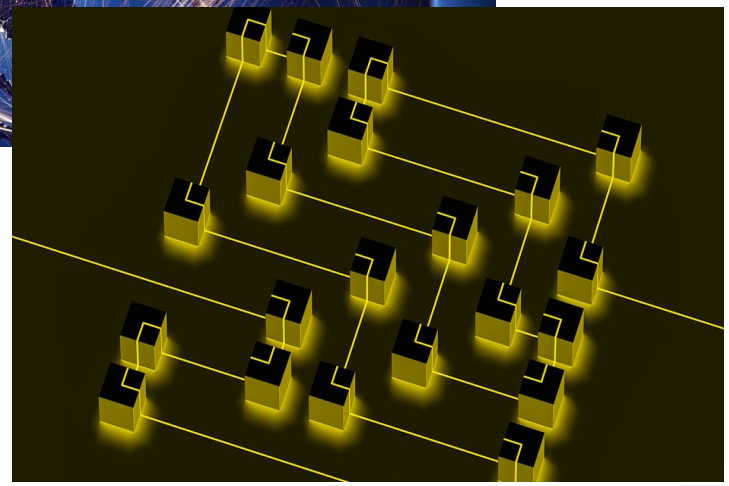
应用领域

重点领域发明专利数量（按简单同族合并）

少 多

领域	细分领域	2013	2014	2015	2016	2017	2018	2019
能源	源网荷储协调			1	6	39	186	178
	智能充放电				5	23	122	104
	能源交易			1	4	22	103	77
	综合能源服务				4	8	52	51
司法	侵权保护	1	10	10	42	124	396	503
	存证确权		1		11	38	162	211
互联网	社交媒体		8	12	41	79	284	346
	电子商务		3	4	22	59	195	182
	O2O			1	5	16	90	111
金融	清算	1	21	65	213	398	1306	1464
	资产管理		7	21	101	236	1199	1324
	银行业		13	30	115	303	875	933
	投融资	1	2	9	55	160	584	721
	交易		8	9	37	103	321	408

未来?



谢谢！