1. **请在开头注明文献调研的会议范围，时间跨度**
2. **一级类别应该主要是整个区块链生态的一些重要组成部分，问题，大体包括但不限于：Blockchain，Mining挖矿，Blockchain网络/PCN网络，加密货币，智能合约，共识机制，Blockchain应用。在这些主题下面，再细分更具体的安全、隐私、激励、性能问题。**

**1、跨链操作**

（19 USENIX）Tracing Transactions Across Cryptocurrency Ledgers：研究跨货币交易的追踪

（19 CCS）HyperService:Interoperability and Programmability Across Heterogeneous Blockchain：在异构区块链间提供互操作性和可编程性

（19 S&P）Proof-of-Stake Sidechains 本文提出了一个适合于权益证明（PoS）的侧链系统【侧链：为方便数字资产在不同区块链间互相转移，侧链（Sidechain）技术应运而生。简单地说，侧链就像是一条条通路，将不同的区块链互相连接在一起，以实现区块链的扩展。侧链完全独立于比特币区块链，但是这两个账本之间能够“互相操作”，实现交互。】

[（19 S&P）XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets 本文实现了无信任和高效的跨链交换的第一个通用框架（例如Bitcoin-backed tokens on Ethereum）

**2、BlockChain**

**① 安全**

（19 Usenix）Inadvertently Making Cyber Criminals Rich: A Comprehensive Study of Cryptojacking Campaigns at Internet Scale 本文研究了Cryptojacking现象：当用户在访问Web站点时在用户的Web浏览器中秘密的挖矿。例如，犯罪分子入侵易受攻击的网站，安装挖掘脚本或使用加密劫持代码创建恶意广告。这篇也不算blockchain本身的安全，而是偷偷让普通网络用户帮忙挖矿。可以忽略或者放到MISC类（杂类）里。

**② 隐私**

（19 CCS）MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol：介绍一种基于计算格问题（特别是M-SIS和M-LWE）的高效、后量子的RingCT协议，并给出完整的实现。

**③ 性能**

（19 CCS）Prism: Deconstructing the Blockchain to Approach Physical Limits：Prism是一种新的工作量证明区块链协议，设计该协议的方法是将区块链解构成其原子功能（提议块、交易块和投票者块），并系统地扩展这些功能以达到其物理极限。

（18 CCS）RapidChain: Scaling Blockchain via Full Sharding：第一个基于分片的公共区块链协议

（19 NDSS）Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based区块链中细粒度和控制下的重写：基于属性的变色龙哈希：一直以来不可篡改性都是区块链一个很重要的特性，但在某些特定应用场景下需要对区块链的数据进行更改（以受控方式或者用户有足够权限时），有时甚至基于法律要求需要打破这种不变性；本文提出了一种基于变色龙哈希的解决方法实现对区块链的重写，并且相比于之前的方案更加细粒度 这篇和下一篇研究的都是区块链的重写机制，建议单独开一个小类。

（19 S&P）Redactable Blockchain in the Permissionless Setting本文提出了一个可重写的区块链，该协议使用了基于共识的投票（voting），如果收集到足够的投票，则在链上执行重写操作。它易于在比特币中实现，且不依赖于繁杂的加密工具或信任假设。

（19 NDSS）YODA: Enabling computationally intensive contracts on blockchains with Byzantine and Selfish nodes 比特币和以太坊等无权限区块链的一个主要缺点是，它们不适合运行计算密集型智能合约（CICs）。这样的区块链不能高效的运行机器学习算法、零知识证明等可能需要繁杂计算的算法。本文提出了第一个有效计算区块链中CICs的解决方案，大概的思想是仅通过部分节点在链下（off-chain）执行智能合约，来降低交易费用并避免验证者两难困境。这篇应该也是属于智能合约类，重点考虑如何执行计算密集的合约

（18 CCS）FairSwap: How to fairly exchange digital goods：最小化在区块链上运行智能合约的成本/避免使用昂贵的密码工具。这篇信息量太少，更像是区块链技术的一种应用，利用区块链去实现公平交换。

（19 NDSS）A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence  本文提出的“Treasury System”是一个由集体控制的和去中心化的协作决策机制，用于为区块链开发和维护提供可持续资金，它与大多数现有的区块链兼容（如比特币、以太坊） 这篇也应该是考虑加密货币的系统。放入加密货币类比较好。

**3、加密货币**

**① 安全**

（19 CCS）Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware：安全的实时加密货币交换服务Tesseract，依赖SGX、支持跨链交易。这里的Exchange应该是特指“**交易所**”，用户可以在交易所里自由兑换不同类型的加密货币。

（19 CCS）Power Adjusting and Bribery Racing: Novel Mining Attacks in the Bitcoin System：提出新的矿工挖掘攻击策略，权力调整预扣（PAW）和贿赂自私挖掘（BSM）这篇主要考虑的是“**挖矿**”，而不是加密货币本身。

（19 CCS）Erlay:Efficient Transaction Relay for Bitcoin：让比特币更安全，Erlay协议如何节省节点84%的带宽？比特币网络的安全性取决于节点的连接性，Erlay结合了快速低扇出（fanout）洪泛法（flooding）和高效集对账，以较小的成本允许更多的连接，带宽利用率高。这篇考虑的是比特币的“**区块链网络**”，也不是加密货币本身。

（19 Usenix）The Anatomy of a Cryptocurrency Pump-and-Dump Scheme本文对加密货币市场中的pump-and-dump方案进行了详细的实证研究【Pump-and-Dump Scheme：通常指一种低市值的低价加密货币，通过精心策划的市场营销它的价值被人为地夸大了，让人们以为，这是投资者不想错过的热门币种，从而使人们以高价购入的欺诈方案】

**② 隐私**

（19 USENIX）BITE: Bitcoin Lightweight Client Privacy using Trusted Execution：利用SGX保护比特币中轻量级客户的隐私

（19 CCS）Privacy Aspects and Subliminal Channels in Zcash（Zcash中的隐私权和潜意识渠道）：zcash中屏蔽交易和潜意识通道的研究及对策

**③ 性能**

（19 USENIX）FASTKITTEN: Practical Smart Contractson Bitcoin：利用可信计算环境TEE，在分布式加密货币上低成本实现复杂智能合约 这篇应该是讲**智能合约**的。

（19 NDSS）Vault: Fast Bootstrapping for the Algorand Cryptocurrency加密货币需要参与者跟踪系统的状态，以便验证新的交易。随着用户和事务数量的增长，这一需求成为一个巨大的负担，需要用户下载、验证和存储大量数据。本文提出的Vault是一种基于Algorand的权益证明（PoS）共识协议的新加密货币系统，它可以最小化参与者的存储和成本。【Algorand是图灵奖获得者Silvio Micali主导研发的一种加密货币方案。该方案通过密码学抽签算法实现了拜占庭共识算法的大规模扩展，从而适用于公链数字货币体系。】

**4、Payment Channel**

（19 CCS）Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks :第一个应用原子多通道更新和简化抵押品的协议

（19 CCS）Balance: Dynamic Adjustment of Cryptocurrency Deposits：不损害协议安全的情况下减少过度抵押

（18 CCS）General State Channel Networks：支付网络的进一步扩展——状态通道网络，允许执行任意复杂的智能合约

（19 NDSS）Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability 用于区块链可扩展性和互操作性的匿名多跳锁：①提出了针对现有Payment Channel Network的虫洞攻击（*wormhole attack*）②构建了一种叫匿名多跳锁的结构来抵抗虫洞攻击，其实是对哈希时间锁协议（*Hash TimeLock Contract*）的改进

（19 S&P）Perun: Virtual Payment Hubs over Cryptocurrencies 本文提出的Perun系统，是一个链下通道（off-chain channel）系统，它提供了一种新的连接多个通道的方法，比现有的在多个通道中寻找交易路径的技术（payment channel network）更有效率。为此，Perun引入了一种称为“虚拟支付渠道”（virtual payment channels）的技术，它避免了中间节点参与每个支付。”Payment hub”指的是在多个交易中存在一个中间节点，这个中间节点可以被视为一个“支付中心”，与多个交易方有直接通道。

**5、Consensus（PoW / PoS）**

（19 USENIX）StrongChain: Transparent and Collaborative Proof-of-Work Consensus：对比特币共识机制进行修改，引入了透明度并激励参与者进行协作而不是竞争

（18 CCS）A Better Method to Analyze Blockchain Consistency：基于简单马尔可夫链的分析区块链协议一致性属性

 （19 S&P）Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols’ Security本文提出了一个多度量评估框架来定量分析PoW协议的质量和抗攻击性；结论是，到目前为止，没有一个PoW协议能够达到理想的链质量或抵抗三种攻击：自私挖矿（selfish mining）攻击、双花（double-spending）攻击以及羽量级分叉（feather-forking）。基于分析，作者提出了更安全的PoW协议的未来方向，并指出了PoW安全分析中的几个常见陷阱。

（19 NDSS）Constructing an Adversary Solver for Equihash： 区块链网络很大程度上依赖于工作证明（PoW）系统，这些系统需要解决特定的难题，近年来出现了ASIC（特定于应用程序的集成电路）的专用设备（即专用挖矿设备），以提高加密货币挖矿行业的效率，但这些设备可能损害区块链网络。Equihash是由卢森堡大学开发的一种以内存为导向的PoW算法，它被开发用来抵抗ASIC设备。本文在两个方面为安全界做出了贡献：（1）揭示Equihash的局限性，提高对其算法的认识；（2）提出了检测工作量证明系统的方法，证明了这种检测在PoW系统上是实用的和有用的，作为未来研究和开发的起点

（18 CCS）Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic

Availability：采用一种新颖的链选择规则来适应基于PoS的区块链协议

 （19 S&P）Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake 本文提出了第一个具有隐私保护的权益证明（PoS）区块链协议

**6、Smart Contracts**

**① 安全**

（19 Usenix）The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts最近攻击者不再关注易受攻击的智能合约，而是试图通过发布包含隐藏陷阱的智能合约来引诱受害者进入陷阱，这种新型合同通常被称为蜜罐（honeypots）。本文通过调查蜜罐智能合约的普遍性、行为和对以太坊区块链的影响，对蜜罐智能合约进行了系统分析。

**② 隐私**

（19 CCS）Privacy Aspects and Subliminal Channels in Zcash（Zcash中的隐私权和潜意识渠道）：zcash中屏蔽交易和潜意识通道的研究及对策 这篇重复出现了。

**③ 系统**

（19 Esorics）PDFS: Practical Data Feed Service for Smart Contracts：实用的数据馈送服务（PDFS）系统，包含数据透明性和一致性验证的新功能

**7、Incentives Incentives单独做一大类也不好，还是一样的愿意，incentive激励问题是一类问题，就像安全、隐私、扩展性，它不适合做一级的类别，可以出现在一些一级类别里的子类。**

（19 Esorics）Incentives for Harvesting Attack in Proof of Work Mining Pools：在由PPS和PPLNS池组成的系统中，管理这两个池的管理者可能会激发一种新型的“池收获”攻击

（18 CCS）The Gap Game：在现实环境中分析了加密货币的安全性，同时考虑了费用和报酬的所有要素。“采矿缺口”——避免激励失调，为加密货币设计提供方案。

**8、Applications of BlockChain**

**① MPC**

（19 Esorics）Towards a Marketplace for Secure Outsourced Computation：介绍了kosto框架，意在为安全外包计算提供市场；使用可信硬件/实现fair exchange

（19 CCS）Efficient Publicly Verifiable 2PC over a Blockchain with Applications to Financially-Secure Computations：提出了一种更简单的judge算法，提出“财务安全计算”的概念

（19 NDSS）Giving State to the Stateless: Augmenting Trustworthy Computation with Ledgers 本文研究了无状态可信设备（stateless trusted devices）与公共账本相结合实现安全计算的问题