北京大学
PEKING UNIVERSITY

区块链课程

孙惠平
sunhp@ss.pku.edu.cn

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

北京大学
PEKING UNIVERSITY

PART 第九章

区块链挑战

目 录

CONTENTS

第一节

隐私

01 区块链中的隐私问题

02 基本要素隐私防护

03 基于密码学原语的隐私防护

04 基于后量子密码学的隐私防护

01 区块链中的隐私问题

北京大学 PEKING UNIVERSITY

账本隐私

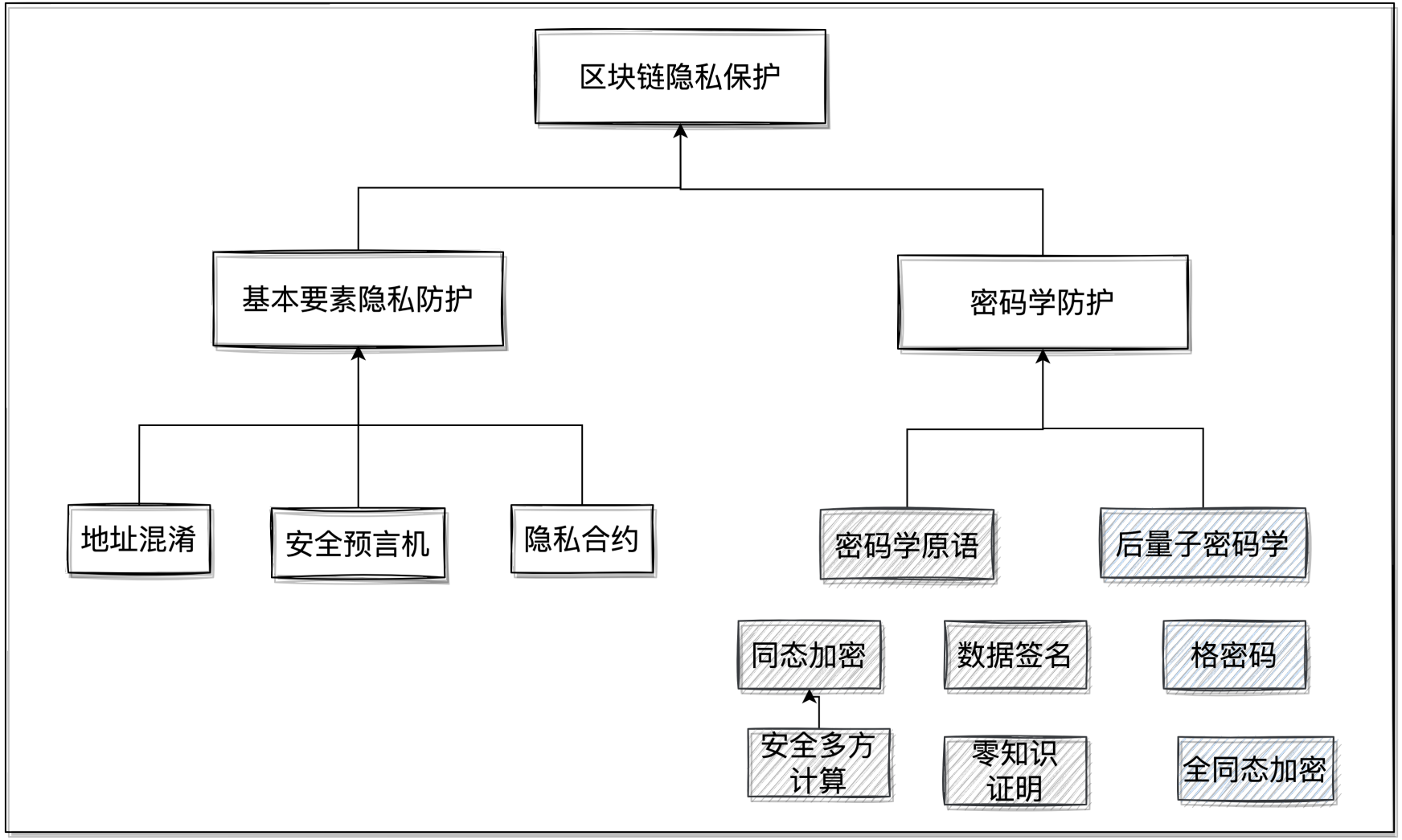
- 交易内容隐私：账本记录的单笔交易内容，包含交易发起方、交易接受方、交易金额以及附带数据等隐私信息。
- 账户地址隐私：区块链地址与交易的关联关系，包含账户地址的交易记录、账户余额以及不同账户地址间交易关联等隐私信息。
- 用户身份隐私：用户和区块链地址、交易的关联关系，含同一用户的交易记录、资金余额等隐私信息。

网络隐私

- 节点隐私：节点自身的隐私内容，包含节点网络IP、软件版本、服务器系统等隐私信息。
- 通信隐私：节点间通信隐私内容，包含节点间通信的数据内容以及通信流量情况。

01 区块链中的隐私问题

- 区块链隐私保护技术图

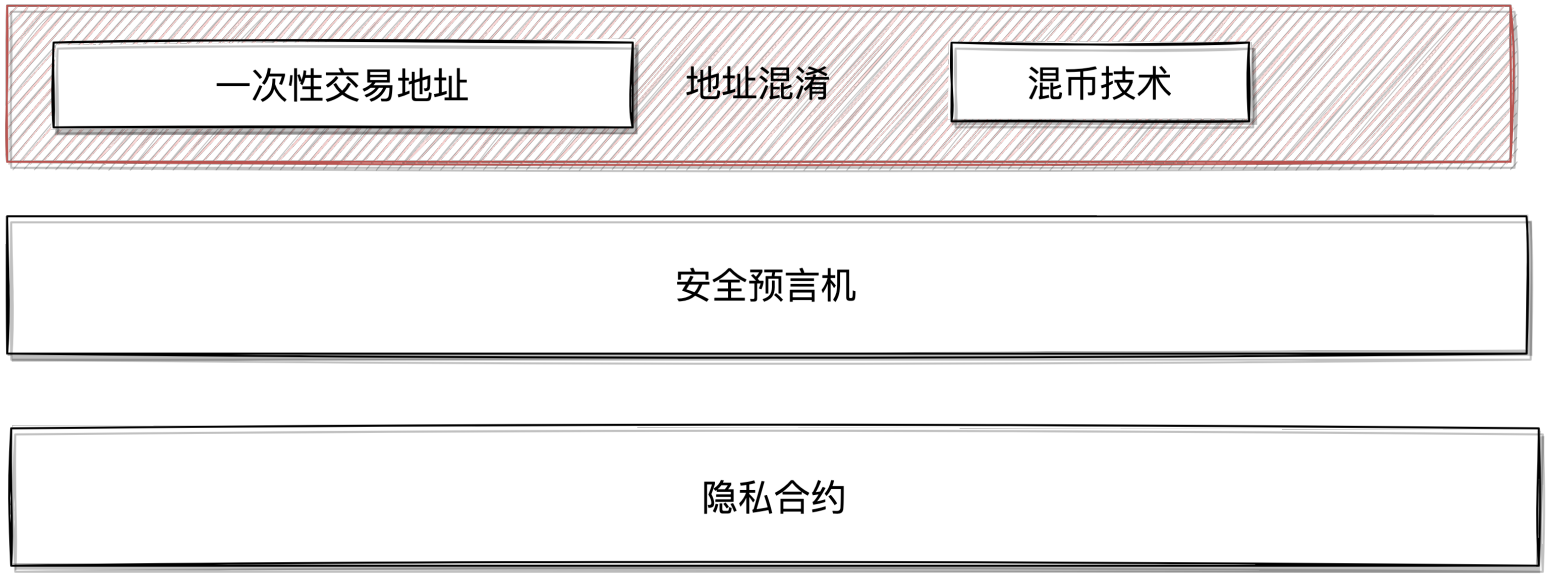


02 基本要素隐私防护

- 介绍基本要素隐私防护的定义和类别

要素防护

区块链基本要素的隐私安全，通常会从**交易地址、链上与链下数据交互的接口以及智能合约** 3 个方面进行考虑。从隐私视角率先切入与区块 链应用设计安全密切相关的基本内容，有助于理解区块链隐私加密技术方式。主要分类如下：



02 基本要素隐私防护

- **地址混淆**

技术定义

地址混淆技术在交易地址隐私保护中应用**最为广泛**，它是指将进行交易的地址加密重组，使混淆处理过后的地址**无法被判别直接源头**，从而实现**交易隐私的目的**。地址混淆在区块链中主要分为两类:一类是**一次性交易地址**，另一类是**混币技术**。

一次性交易地址

在区块链中**持续使用同一个交易地址**会使交 易和用户身份容易被追踪，最直接的解决方法是**在进行不同交易时使用不同的交易地址**，给追踪 和分析增加难度，使混淆处理过后的地址**无法被判别直接源头**，从而实现**交易隐私的目的**。

混币技术

混币技术是指将**多个不相关输入进行混合后再输出**，使外界**无法分辨出数字货币的流向**一般地，混币主要利用**混淆器实现**地址隐私保护，在混淆服务通证池中将若干用户的交易通证进行混淆处理后，输出给匿名交易地址，从而减少敌手窃取资金的可能性。

北京大学 PEKING UNIVERSITY

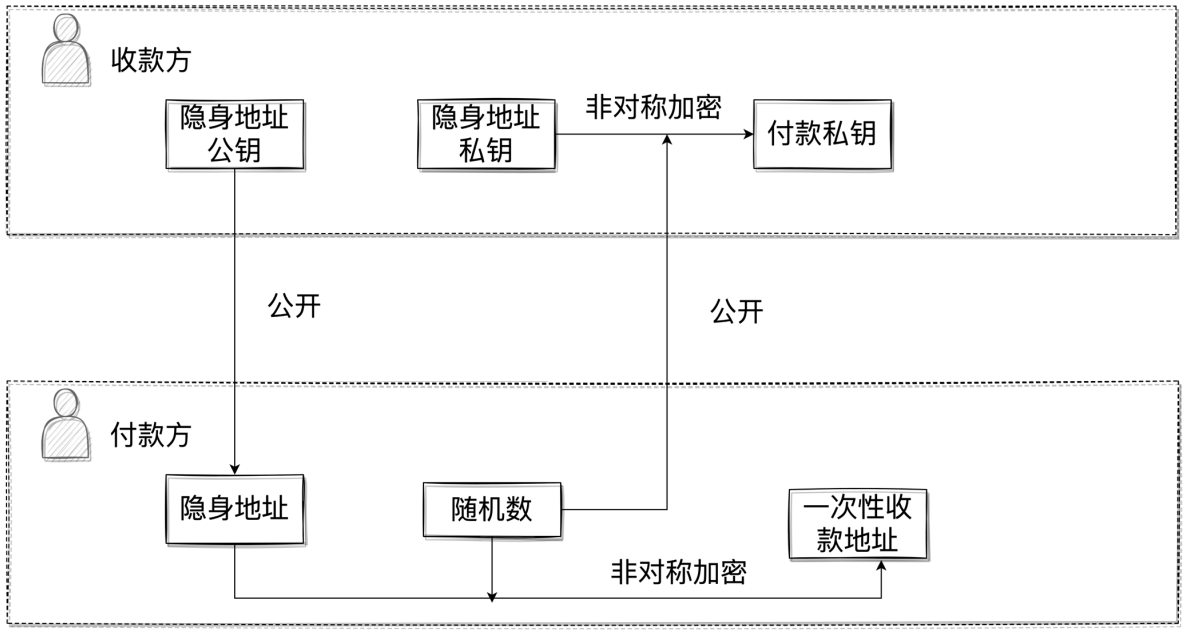
- **地址混淆：一次性交易地址**

隐身地址

一次性交易地址每次都需产生新地址进行交易，在交易场景中不断切换新地址反而会影响用户体验、降低交易效率。为了消除这种弊端， **隐身地址应运而生**。

地址流程

为了不暴露自己的交易地址，**收款方**把正常交易中使用的**公钥进行隐藏**，然后发送**隐身地址公钥给付款方**。**付款方**则利用该隐身地址和一个**随机数**进行非对称加密，生成一个临时存放交易资金的一次性收款地址。然后， 收款方可借助隐身地址私钥对该一次性收款地址进行解密，获取可以转出该笔资金的付款私钥。



02 基本要素隐私防护

- **地址混淆：混币技术**

中心化混币

早期中心化混币服务的部署方式， 典型如 **Mixcoin** 协议，虽然具备可审计性，但混淆服务器仍掌握着交易地址的关联信息，对**用户隐私威胁较大**。研究表明即使经过**多轮混淆处理**，如果交易支付的 Cookie 不及时清除，仍然可以通过**技术手段辨别出用户的钱包再窃取其敏感信息。**

去中心化混币

近些年，为进一步改进中心化混币协议， BlindCoin利用盲签名对**隐私泄露进行防范**，同时降低了交易的时间开销。此外，为解决中心化混币技术的信任问题，涌现出 CoinParty、Xim等**分布式混币技术**。然而，这些技术并不完美， 在**计算开销、通信复杂度以及交易隐私性等问题 上仍留有缺口。**

北京大学 PEKING UNIVERSITY

- 地址混淆：混币技术对比

类别	混币机制	性能开销	主要隐私安全问题
中心化混币	Mixcoin	交易时延高	混币服务商掌握用户隐私
	BlindCoin	计算开销与存储开销大	混币服务商掌握用户隐私
	TumbleBit	交易时延与交易费用高	易遭受中继节点窃取隐私
去中心化混币	CoinJoin	交易时延随参与用户增加而增加	混币服务商掌握用户隐私
	CoinShuffle	交易时延随参与用户增加而增加	易遭受中继节点窃取隐私
	CoinParty	交易时延随参与用户增加而增加	未经认证的恶意用户易盗取他人资产
	Xim	混币时间长且混币轮换次数多	混币期间易遭受攻击和查询

02 基本要素隐私防护

- 预言机隐私处理

预言机

考虑区块链预言机的隐私处理。预言机是**智能合约连接链下数据和系统的数字化代理**，能够将区块链与外部世界进行链接。在基础要素防护方面，隐私预言机的设计是区块链隐私保护的战略枢纽。**预言机隐私方面研究正不断向前推进**，并且更多地倾向于去中心化预言机可扩展运算中的隐私。

区块链预言机应用

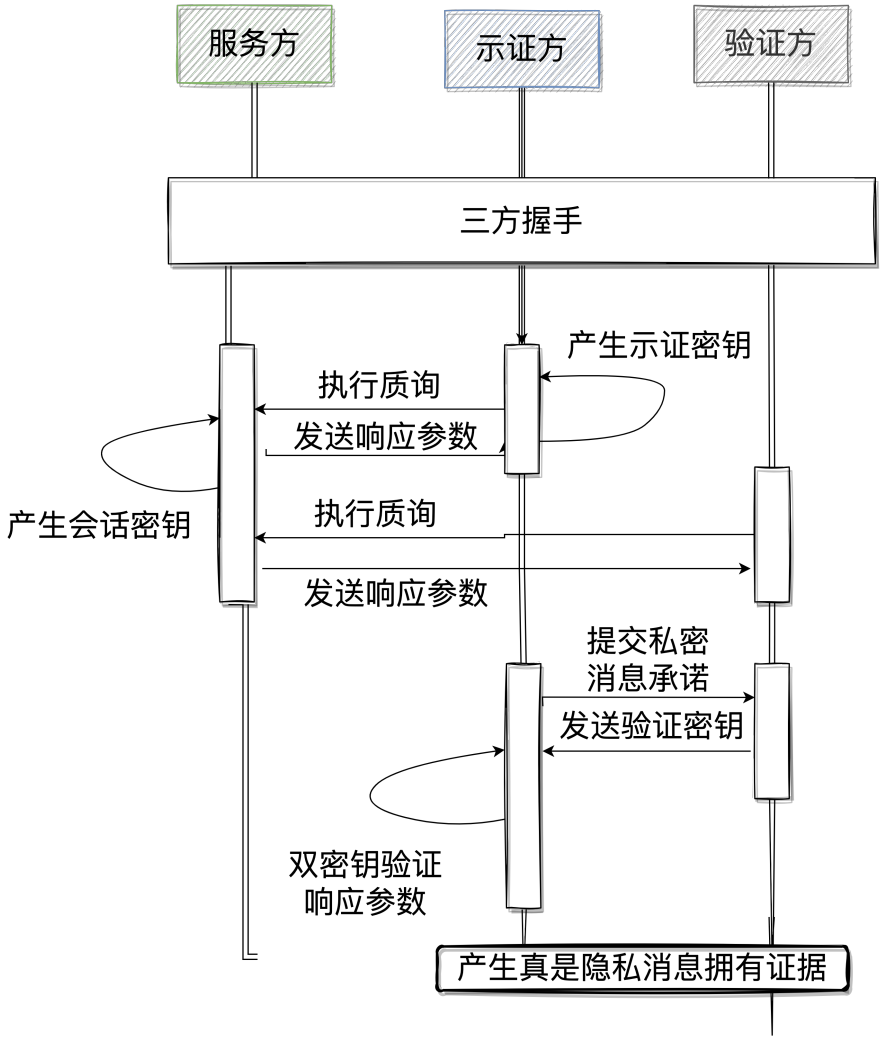
尽管在应用方面，区块链预言机项目的实施已经屡见不鲜，然而像 Chainlink、Oraclize 等预言机网络仍然只能基于各自机制**为区块链提供一些基本公开信息**，如**价格、交易量等**，在信息隐私，脱敏处理上很难满足真实商业需求。在**学术研究方面**，康奈尔大学**提出了隐私预言机协议 DECO。**保障了各类隐私和付费数据源传输数据时的隐私性和不易篡改性。

02 基本要素隐私防护

- **预言机隐私处理：DECO 协议工作流程**

流程说明

从右图的工作流程可以看出，DECO 在**使用 HTTP/TLS 协议**的服务器中实现了**传输层安全** (TLS，transport layer security)的短**时间握手和零知识性**，使数据在建立握手连接过程中不会被轻易泄露。DECO 协议通过提交私密消息承诺给验证方，使即使是最终使用数据的计算机也无法查看数据内容，借助预言机在无须公示私密信息的情况下可**进行脱链验证**。



北京大学 PEKING UNIVERSITY

- 智能合约安全治理

智能合约

智能合约是区块链 2.0 时代基本要素的重要组成部分，是解决区块链信任问题的突破性技术之一。合约具备图灵完备的编程语言，能够扩充区块链的使用场景和功能。随着区块链应用的不断开发，各式各样的智能合约在不断增多，**对合约隐私安全的治理显得尤为重要。**

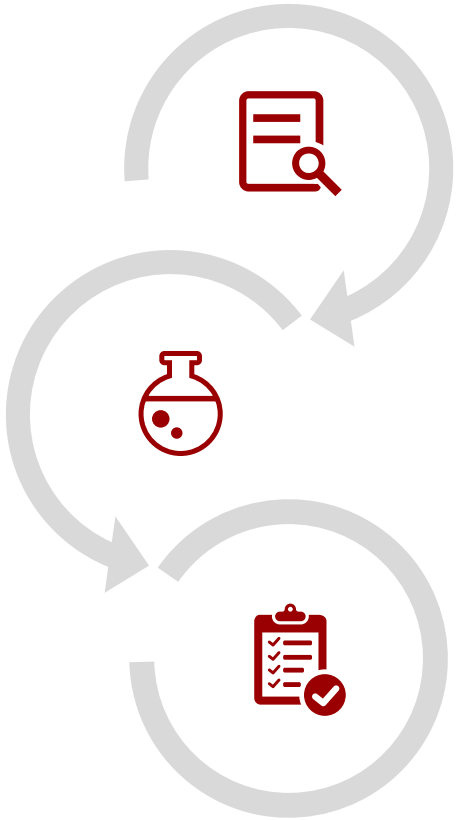
合约隐私治理

在诸多合约隐私研究中，有**支持预言机特殊形式的隐私智能合约** Mixcles，通过结合通证混淆技术为以太坊提供隐私保障。也有针对**以太坊智能合约设计的隐私协议** Zether，作为 ElGamal 公钥账户之间传输的载体，支持匿名的智能合约交互。此外，共识计算成本高，可被**委托链外的隐私计算能力**受人青睐。

02 基本要素隐私防护

- **合约隐私技术在不断突破，并且隐私研究与应用越来越受到关注，但合约上隐私安全问题的要因还需要注意以下几点：**

缺乏形式化证明：
大多数智能合约在编写之初并**没有考虑过形式化验证**，当部署在某一区块地址后，因为不能修改，如果存在 BUG，会很容易被**黑客利用进行恶意攻击**，造成不可弥补的**经济损失。**



缺少审查。合约逻辑的审计是必不可少的，**规范化合约能够助推合约的法理性研究**，如考虑匿名性检测、隐私威胁预警、脆弱性检 测、漏洞挖掘等。

智能合约编程语言内生性安全问题：
早些年合约常用语言 Solidity 因为**空指针等逻辑设计缺陷**饱受诟病。另外，相关的开发者社区并不健全，需要多方努力对**合约编程语言进行分析测试。**

03 基于密码学原语的隐私防护

- 介绍基于密码学原语的隐私防护的定义和类别

密码学原语隐私防护

有别于操作系统原语，密码学原语如**签名、密钥交换**等，主要侧重在解决问题的动机上。区块链本质上是一个**基于密码学**的技术，使用的密码学原语比较广泛，包括**椭圆曲线签名 ECDSA、 安全哈希**等。本小节归类面向区块链的**具备隐私效应的典型密码学原语**，分析它们各自的特点以及使用场景。

北京大学 PEKING UNIVERSITY

- **特殊数字签名隐私性简述与分析**

签名隐私

一般而言，区块链上交易信息是通过签名标定交易发起方的身份，然后由**区块链通过特定规则验证签名**以确保交易信息的正确性，这一切**得益于签名的不易篡改和校验性**。区块链主流平台 RSA、ECDSA 等交易签名方式已被普遍使用，但这些签名隐私保护效果不是十分理想，存在**参与方身份信息隐匿性弱、多方签名消息保密性差等弊端**。在一些区块链新兴应用场景中，能够实现身份匿名、交易内容隐藏等特殊隐私保护的聚合式数字签名技术极具价值。

签名分类

03 基于密码学原语的隐私防护

- **特殊数字签名隐私性简述与分析**

群签名

群签名首先由群管理者建立群资源，然后**向外界隐蔽群成员身份的隐私信息**， 让群成员在**群组内进行签名**。签名完成后只有群公钥被公开，交由区块链上验证节点或者逻辑合约进行验证。整个过程中，群管理者可以利用群私钥对群成员生成的群签名进行追踪以实现监管目的。

环签名

环签名会为一组交易成员提供各自的对外公钥，使区块链公开数据只能追踪到交易成员所在组，**无法解析出个人信息**。

聚合签名

签名过程中如何有效处理隐私也是亟须考虑的问题。在此现状下，能够**对多方签名消息进行合并签署的聚合签名逐步占据优势**，典型如 Schnorr 签名与 BLS 签名聚合方案。聚合签名的参与方无须提供与 自己直接相关的公钥给验证者 这就使在**减少用户隐私泄露的同时提高了签名的效率**。

盲签名

盲签名是数字签 名的变种，主要借助**盲因子对签名数据进行盲化签名**，验证时则需利用盲 化因子进行解盲实现隐私交易。

03 基于密码学原语的隐私防护

- 特殊数字签名隐私性能对比分析

签名类型	参与方隐私性	签名消息隐私性	地址隐私性
环签名	基于环密钥分发中心	基于环状签名结构	隐私性强
盲签名	盲化消息者隐私性能	基于盲化函数与因子	盲化消息者隐私性强
Schnorr 签名	签名时隐私性差	基于离散对数难解	签名后隐私性强
BLS 签名	签名时隐私性差	基于离散对数难解	签名后隐私性强

03 基于密码学原语的隐私防护

- **基于属性基加密的区块链访问控制**

定义

属性基加密(ABE，attribute-based encryption)源自**对身份信息属性的识别**，其安全性在于使不满足既定策略的攻击者所拥有的密钥无法解密密文。密文可在不安全的信道上进行传输， 也可上传至开放的网络存储设备中。

分类

属性基加密主要分为两种:**一种是密钥策略的属性基加密（KPABE**，key-policy attribute encryption)，另一种是**密文策略的属性基加密（CPABE**，ciphertext-policy attribute-based encryption)。其中，CPABE 方案能够有效处理区块链隐私，此方案中数据拥有者可以设定访问策略，只有满足访问策略的用户可以解密共享一份数据内容。

03 基于密码学原语的隐私防护

- 同态加密

定义

同态加密属于基于非噪声方法的安全计算，**可以使数据在密文状态下进行计算，解密后可获得与明文进行同样运算后的结果。**对于区块链应用同态加密的理论很多，如 Pedersen 承诺、ElGamal 承诺等密码学承诺，这些承诺或具备加法同态特性或具备乘法同态特性，可以将数据进行私密保存并通过公布数据的哈希值来承诺它的真实性。

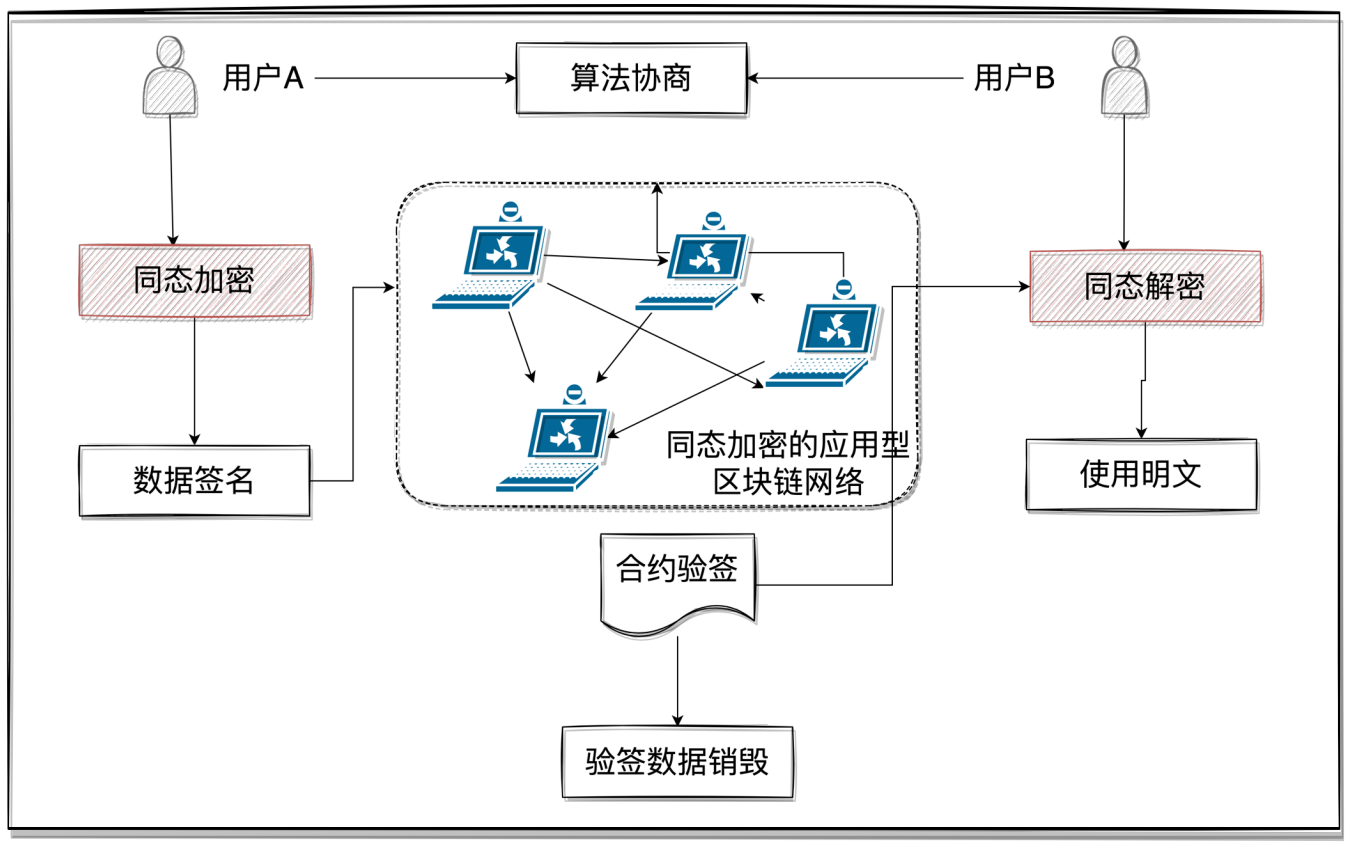
好处

在区块链中，不管是公有链、私有链还是联盟链，直接对明文信息进行处理并发布至智能合约将会**很大程度地泄露敏感数据。**应用同态加密**既能保证链上数据隐私，也能实现节点与节点之间数据的可计算性。**

- 同态加密

区块链同态加密理论模型

参与方首先**需要进行算法协商**，协 定公**共参数**;然后由加密方对交易信息进行**同态加密**，并将完成签名的数据传送上链。等到数据经智能合约验签后，使用方将在链**下解密数据**，获取明文信息;最后由合约**对验签数据进行销毁。**



03 基于密码学原语的隐私防护

北京大学 PEKING UNIVERSITY

- **安全多方计算**

定义

信息安全，包括数据安全、通信安全以及计算安全。计算安全在多方协作交易中尤为重要， 在密码学知识领域被称为**安全多方计算(SMPC**， secure multi-party computation)。SMPC 可以**解决协同计算隐私保护问题**，具有**输入隐私性、计算正确性以及去中心化特征**，能使数据既保持隐私又能被使用，从而释放隐私数据分享、隐私数据 分析以及隐私数据挖掘的巨大价值。

隐私保护

个人信息在共享和计算中容易出现安全问题和隐私问题，安全多方计算可以结合区块链特征使用户数据隐私得以保护，使不可信多方之间进行敏感数据联合计算、敏感数据求交集、敏感数据联合建模等。 例如，隐私计算平台 Enigma，通过 SMPC 以分布式形式计算数据，同时改进分布式哈希表进行数据存储，并分散到多个区块链节点上进行责任分摊。

03 基于密码学原语的隐私防护

- 安全多方计算

不可过度依赖

虽然对于计算本身，在区块链链外的数据计算隐蔽性较强，但某种程度上**会使区块链可信性降低**。如果过于依赖链外多方计算，则需要**额外的可信第三方参与验证和确认交易**，从而增加**交易开销和单点故障风险**。可信执行环境一定程度上可增强安全多方计算在区块链隐私保护上的安全效益，但高要求的硬件环境对于目前应用而言，仍然存在差距 。

低效问题

在区块链通用计算领域SMPC 的“**低效**”**是需要克服的问题**。一般地，多方计算中需要多轮交互，尤其在某些协作计算的场景下要求参与方保持在线，交易的效率偏低。此外，区块链中应用 SMPC，协作计算方的身份往往无法确定， 身份识别**不可避免地需要揭露参与方的部分隐私**，单靠安全多方计算可能无法处理这方面的隐私问题。在大规模商业部署中，SMPC 仍存在不小阻力。

03 基于密码学原语的隐私防护

- **零知识证明**

定义

零知识证明是一种**不泄露敏感数据**信息即能**向他人证明信息归属权的密码学技术**，善于平衡隐私和透明的需求。**ZKP** 作用于区块链上不仅可以解决数据**上链隐私泄露**，也可以在**性能提优、 数据量大无法上链方面**做出改善。本小节介绍零知识证明技术的含义、算法和影响力

优缺点

虽然零知识证明在区块链**隐私保护**上效果显著，用户可以借助其离线计算数据达到在区块链上的**交易信息隐藏**，但在实现上仍存在一些问题亟须解决。首先是**电路设计**，因为区块链公开透明在零知识电路设计上需要大量密码封装实现，不可避免地依赖了很多约束和参数调优。其次是**侧信道攻击**。

03 基于密码学原语的隐私防护

- 零知识证明：常见零知识证明算法对比

算法	算数复杂度	通信复杂度	以太坊gas费用	密码学假设性强度	可信设置	后量子安全
SNARA	$O(nlog(N))$	$O(1)$	600kB	强	是	否
STARK	$O(n\text{poly}log(N))$	$O(\text{poly}log(N)$	2.5MB	抗强哈希碰撞	否	是
BulletProof	$O(nlog(N))$	$O(N)$	N/A	离散对数安全	否	否

04 基于后量子密码学的隐私保护技术

- **区块链隐私加密技术发展需考虑未来挑战及如何实现加密技术的升级与替换。量子计算是当前区块链面临的最具挑战性的前沿技术 。**

量子密码学

量子计算机攻破当前的区块链隐私加密技术可能只是时间问题。因此，寻找**能够应用至区块链的抗量子计算密码学理论**已成为下一代隐私加密技术研究的**热点话题**，而抗量子计算的区块链隐私计算的研究重点在于**格密码与全同态加密。**

格密码尝试

格密码主要是**基于格困难问题**产生的一类噪 声加密密码。对于量子时代区块链隐私数据保护，格密码可**结合同态加密**， 建立**具备加同态的后量子安全承诺方案保护数据隐私。**

全同态加密

一个算法或协议**同时具备加法同态和乘法同态的特性即可视为全同态加密**(FHE，fully homomorphic encryption)。区块链隐私保护上寻求全同态加密，主流方法是**构造容错学习或环容错学习**的困难问题来实现全同态场景的近似替代。**现今仍以理论研究为主。**

隐私

北京大学 PEKING UNIVERSITY

- 区块链密码学隐私保护技术对比

名称	主要技术特点	主要使用场景
聚合签名	签名分片	多方参与
属性基加密	访问控制	身份验证
同态加密	密文计算	敏感数据处理
安全多方计算	多方计算	多方协作
零知识证明	零知识性	保密交易
格密码	抗量子计算	隐私技术融合
全同态加密	抗量子计算	隐私技术融合

第 二 节
安全

01 区块链安全事件

北京大学 PEKING UNIVERSITY

针对区块链的不同组件，发生了各类安全事件，存在各种攻击方式，也带来了各种威胁。

对等网络威胁	共识机制威胁	智能合约威胁
BlackWallet，EtherDelta，MyEther-Wallet等基于以太坊智能合约的交易系统在2017和2018年多次遭受DNS劫持攻击，造成经济损失逾82万美元。	Eligius矿池在2014年遭受区块截留攻击而损失300余枚比特币（价值约16万美元），以太经典在2020年8月先后遭受三次51%攻击。	针对智能合约的恶意攻击所引发的安全事件约占区块链安全事件总数的三分之一。

01 区块链安全事件

2021年区块链安全事件

事件	损失
Yearn Finance 被攻击，黑客利用闪电贷操控 3pool 代币平衡，并通过y Dai保险库放大差异。	黑客获利 280 万美元，而保险库损失超1100 万美元。
以太坊协议组合工具 Furucombo 智能合约被爆出存在请求授权权限过高问题，黑客可通过向 Furucombo 代理添加攻击合约，从而获得影响用户账户的权限	该漏洞影响超 1400 万美元。
去中心化交易所DODO因未对init进行权限控制，导致黑客在进行闪电贷归还操作时通过init函数将需要归还的代币修改为自己提前加入pool的垃圾代币，从而规避校验以次充好	损失超 200 万美元。
Paid Network铸币功能存在漏洞。	被利用铸造超6000 万枚PAID代币。
Filecoin 由于节点特性出现“双花交易”漏洞。	-

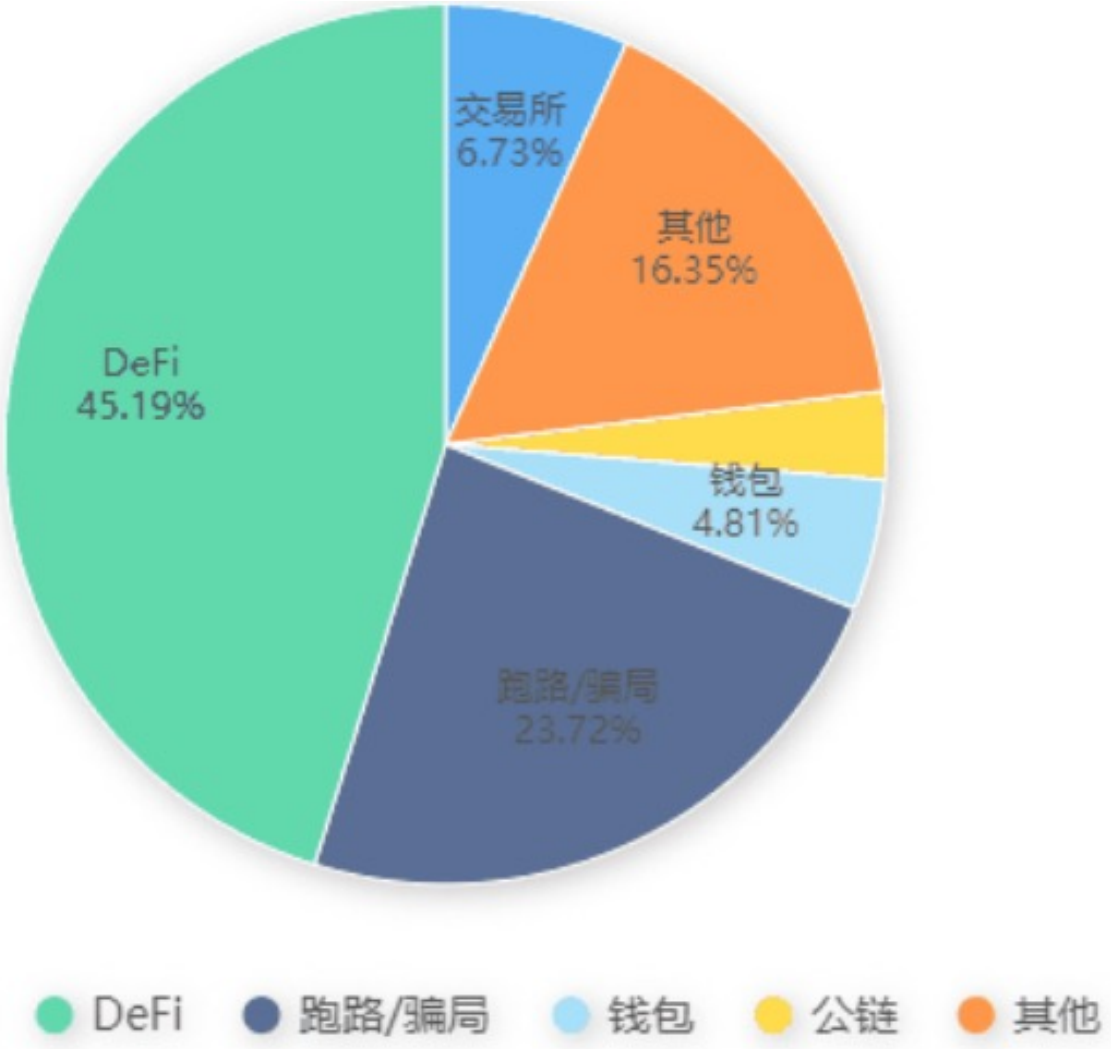
01 区块链安全事件

2021年区块链安全事件

事件	损失
Uniswap 上的 imBTC 池遭到黑客攻击，漏洞原因是 Uniswap 与 ERC777 协议出现兼容性问题，当交易产生时，ERC777 中的迭代调用tokensToSend可以被用来实现重入攻击。	损失超 30 万美元。
以太坊上DeFi 协议 Popsicle Finance 遭遇闪电贷袭击，漏洞原因在于 PLP 池合约对手续费奖励的计算存在缺陷。	损失 2,070 万美元。
跨链协议 Poly Network 遭到攻击，由于函数缺陷导致keeper可被修改，这次攻击被称为年度最大黑客事件。	损失约 6.1 亿美元。
以太坊上被动收益协议 Indexed Finance 遭到攻击，其漏洞产生的原因在于协议通过一种代币来描述整个矿池价值。	损失约1600万美元。
……	……

01 区块链安全事件

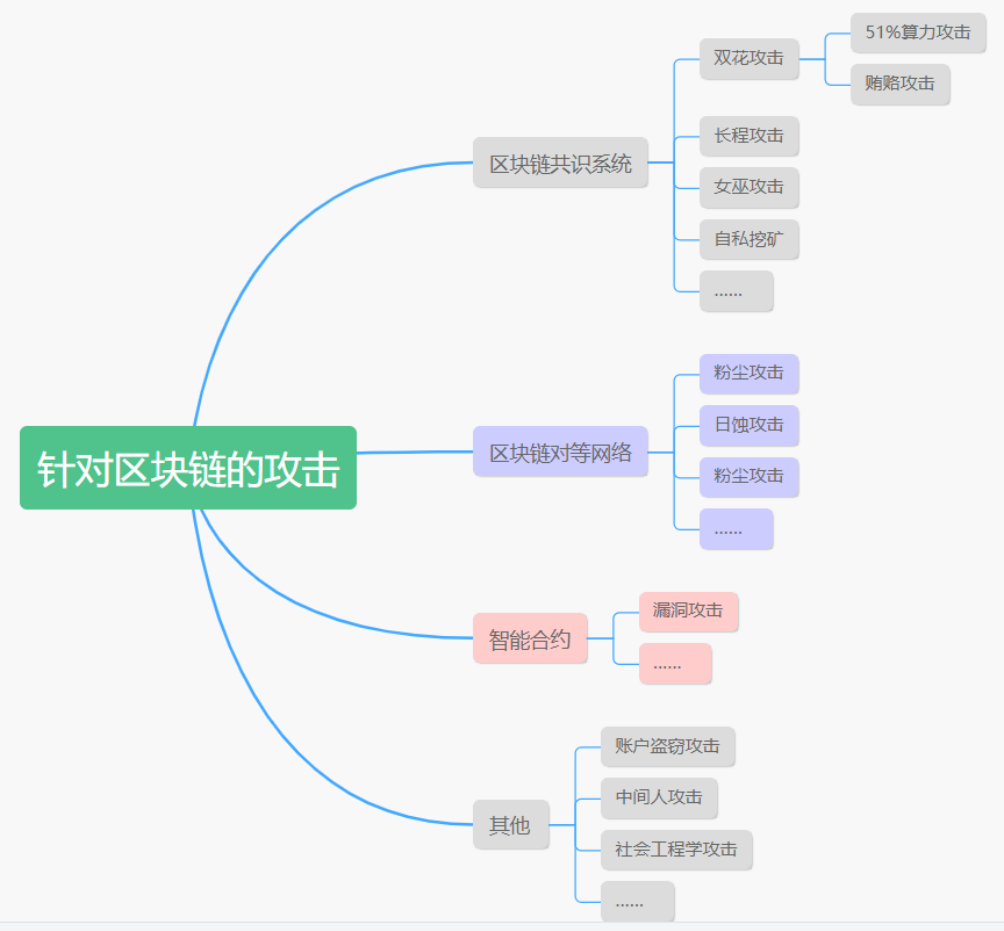
2021年区块链安全事件



02 针对区块链的攻击

北京大学 PEKING UNIVERSITY

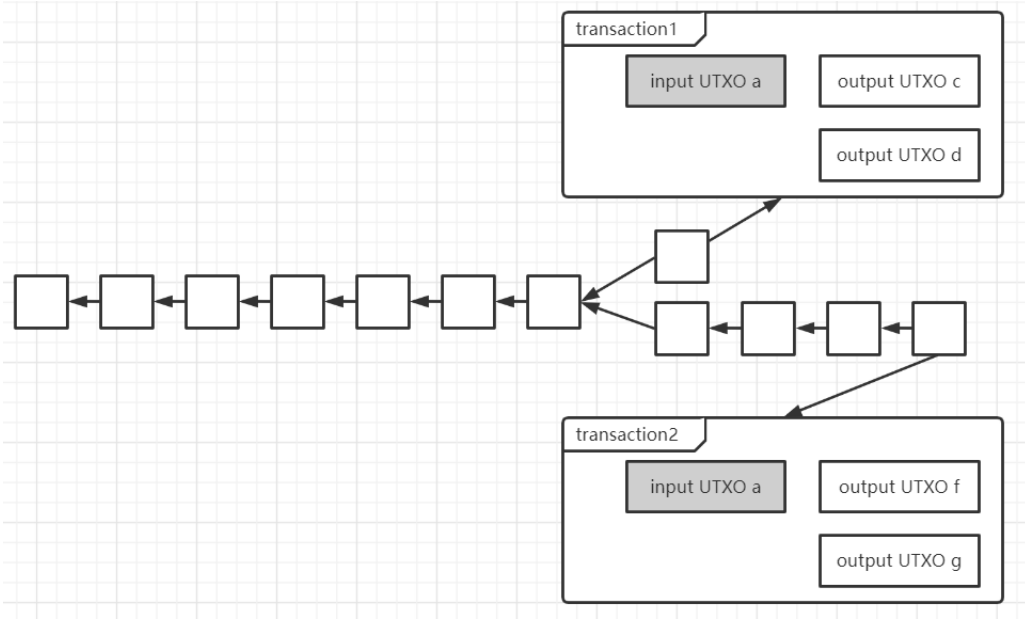
针对区块链的攻击可以来自各个方面，并且发生在各个环节。



03 针对区块链共识的攻击

双花攻击

- 双花攻击, 顾名思义就是将同一笔数字货币花费多次的攻击。
- 双花攻击包含以下 4 个步骤：
- ① 攻击者的地址 1 发起一笔向受害者转账数字货币的交易 A;
- ② 受害者在交易 A 收到足够多的确认后, 认可交易 A, 并向攻击者转账现金或是发送商品;
- ③ 攻击者的地址 1 发起一笔向其地址 2 转账数字货币的交易 B, 该交易的交易金额为攻击者地址 1 中的数字货币总数, 由于交易 A 与交易 B 冲突, 因此区块链产生分叉;
- ④ 攻击者运用各种手段, 使包含交易 B 的链的长度超过包含交易 A 的链, 根据最长链原则, 交易 B 被认为有效, 而交易 A 被认为无效, 攻击者攻击成功。



03 针对区块链共识的攻击

51% 攻击

- 51% 攻击是一种在掌握绝对算力优势的情况下, 把已经花出的数字货币重新收回或多次利用的攻击方式, 主要针对基于工作量证明 (PoW) 共识机制的区块链。攻击者在拿到财物后, 从支付交易 之前区块开始制造分叉, 利用>51% 的算力优势在该分叉链上进行挖矿; 当分叉链长度超过原主链时, 根据最长链原则成为新主链, 原主链上的交易无效, 攻击成功。

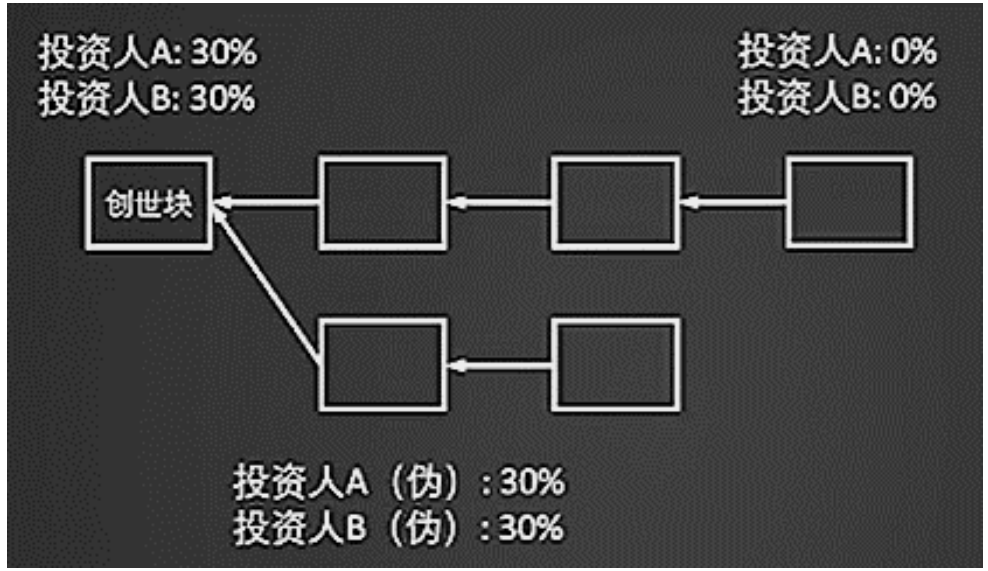
贿赂攻击

- 贿赂攻击是一种在非协作选择模型上 (比如无信任基础区块链) 的攻击, 攻击者通过额外经济奖励收购挖矿算力, 使得自己所掌握的算力短期内超过 51%, 从而对区块链进行 51% 攻击。攻击者在网络中宣称将提供额外奖励给在目前相对较长但不包含交易 A 的次主链上工作的矿工, 以鼓动其他矿工违背共识, 在非主链上进行工作， 当次主链足够长时, 攻击者通过加大奖励力度, 促使次主链的长度在短时间内超过原主链的长度。

03 针对区块链共识的攻击

长程攻击

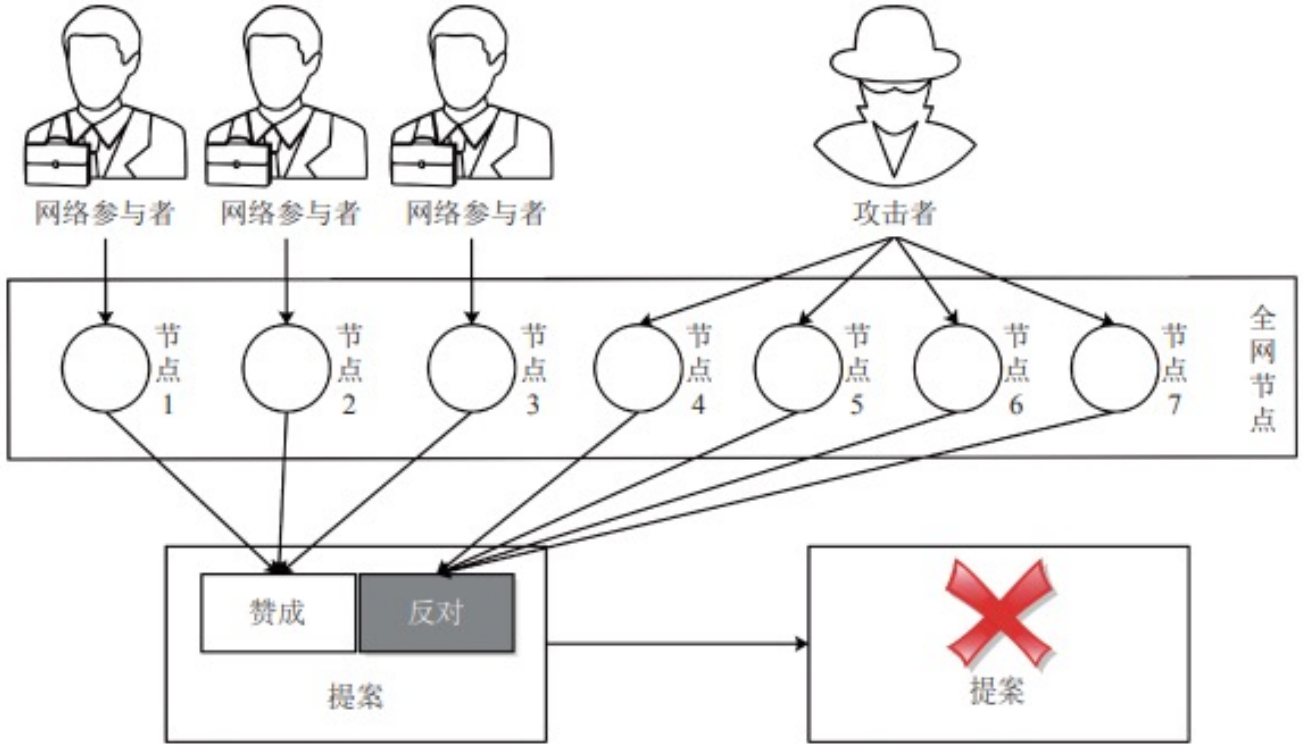
- 在 PoW 共识中, 如果攻击者要篡改某区块的历史, 需要在这个区块前制造一条分叉链, 并且让其长度超过主链长度。但由于 PoW 共识的特性, 攻击者制造一条超过主链的分叉链需要大量的算力, 且分叉链长度越长, 分叉链超过主链的难度越高, 这就在导致了在 PoW 共识下, 攻击者只能对短程的区块进行修改; 而在 PoS 共识下, 延长分叉链只需要权益, 即币的数量和币龄, 因此, 攻击者可以较为轻松的篡改成百上千个区块之前的历史区块, 实现长程攻击。



03 针对区块链共识的攻击

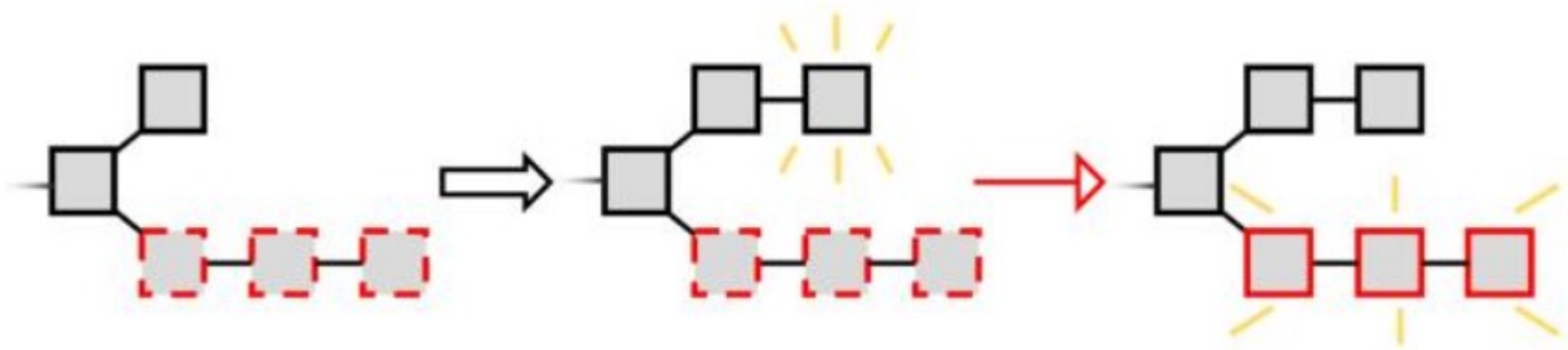
女巫攻击

- 女巫攻击主要针对的是采用拜占庭容错 (BFT) 协议而非 PoW 机制的区块链.。攻击者通过创建多个身份节点破坏区块链网络的信任基础和冗余策略, 操控区块链选举投票。



自私挖矿攻击

- 自私挖矿攻击是一种针对基于 PoW 共识的区块链的恶意挖矿策略。实施自私挖矿攻击的恶意矿池在挖到新区块时，不会立即发布新区块，而是根据自私挖矿策略决定是发布该块还是继续在自私分叉上挖矿。当自私分叉长度超过公共链长度时，若恶意矿池公开分叉链，则原公共链包含的所有数据将会回滚，区块链用户将损失回滚部分的数字货币收入，诚实矿池也将损失原主链上的出块奖励。自私挖矿攻击同时会导致在诚实矿池中工作的矿工为了获得“超额”的挖矿奖励，转而加入恶意矿池进行工作，诚实矿池的算力逐步被蚕食。



04 针对区块链网络的攻击

粉尘攻击

- 粉尘攻击是指用大量交易额极小、毫无价值的垃圾交易占据区块空间，从而导致正常的交易无法被处理，造成区块堵塞的攻击。攻击者通过发起很多交易额极小但手续费较高的交易，使得矿工优先处理这些交易，从而达到堵塞区块链的目的；攻击者也可以利用矿池，打包无意义的交易，使得区块链拥堵，阻碍正常交易被打包。

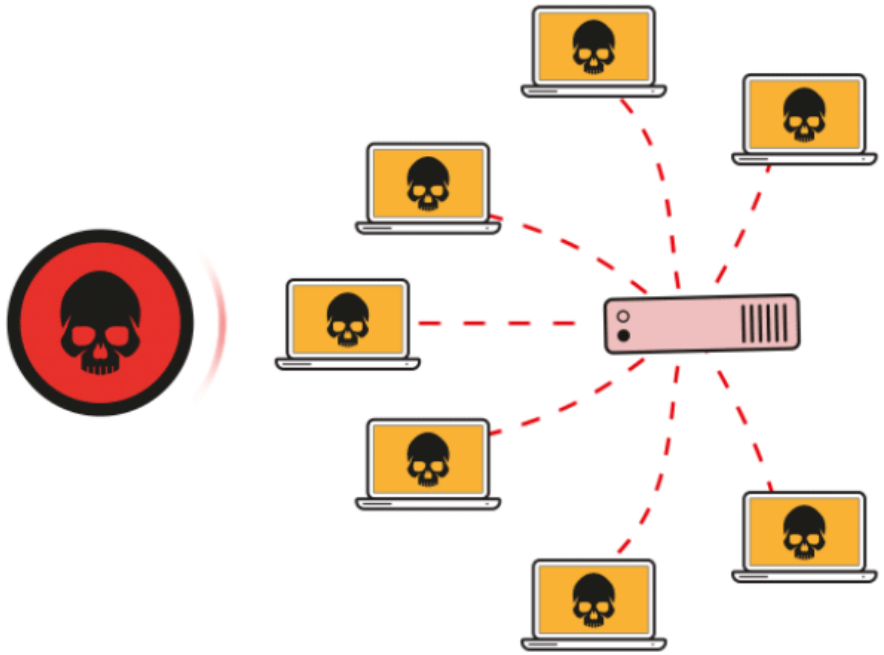
日蚀攻击

- 日蚀攻击是一种由多个傀儡节点发起的针对区块链网络层面的攻击，攻击者利用傀儡节点修改受害者节点节点表并阻止受害者节点接收和发送消息，从而达到隔离受害者节点的目的。攻击者通过隔离受害者节点，征用受害者的挖矿能力进行双花攻击或私自挖矿，也可以诱使受害者在交易完成前将现金或货物发给攻击者。

04 针对区块链网络的攻击

分布式拒绝服务攻击

- 交易所遭遇的拒绝服务攻击多数是分布式拒绝服务 (DDoS) 攻击。攻击者通过大量傀儡机向目标发送合法的请求以占用大量网络资源, 从而瘫痪目标网络, 使合法用户无法获得服务的响应。



05 针对智能合约的攻击

漏洞攻击

- 漏洞攻击是以太坊智能合约最主要的安全风险. 以太坊智能合约威胁较高的漏洞有整数溢出漏洞、可重入漏洞、交易顺序依赖问题、时间戳依赖问题、深度调用问题等。
- 其中包括：
- 整数溢出攻击
- 可重入攻击
- 交易顺序依赖攻击
- 时间戳依赖攻击
- 调用深度攻击

北京大学 PEKING UNIVERSITY

安全攻防

双花攻击、51%攻击、贿赂攻击

- 51%攻击：保持算力分散。51% 攻击能够成功实施的根本原因是算力过分集中, 在 PoW 共识机制下只要存在算力中心化, 所有区块链都无法完全避免 51% 攻击。

- 贿赂攻击：可以在区块链挖矿机制设计中引入保证金和惩罚措施。当矿工做出不利于区块链的决策时, 会受到处罚并失去抵押在链上的保证金。这种惩罚措施变相提高了攻击者的贿赂成本, 使得贿赂攻击更难发生。

北京大学 PEKING UNIVERSITY

安全攻防

长程攻击

- 区块链设计者需要在共识中加入时间戳验证机制, 可以防止攻击者伪造时间戳从而提前生成区块完成攻击。也可以设置移动检查点 (moving checkpoint), 即仅允许区块链尾端的 X 个区块被重组, 来缩小攻击者可修改历史的区块数目。

女巫攻击

- 区块链设计者可以在区块链系统中加入身份认证机制。只有获得可信的第三方节点或是获得当前网络中大多数可靠节点的认证后, 新的节点才能加入区块链。

自私挖矿攻击

- 改进挖矿规则。当矿工收到两个及以上的相同长度的分支时, 他必须传播所有分支并随机选择一个分支, 在其后继续挖矿, 从而增大恶意矿池进行自私挖矿的成本。

共识机制安全攻防总结

减缓网络中心化

- 降低节点间的收益差距，避免形成大矿池。
- 通过利用博弈论和机器学习，通过实时监测节点间潜在的合作行为，并及时采取应对措施以减小形成矿池的可能性；
- 矿池“关闭“（拒绝更多节点加入）策略，以防范区块截留攻击和避免形成大矿池。

改进共识

- Ouroboros共识机制在权益证明共识机制基础上引入新的奖励机制使得诚实节点的行为构成一个近似纳什均衡，可有效抵御自私挖矿等策略攻击。
- Flux、FruitChains、Bobtail等通过改变区块结构设计和奖励机制来减小节点间的收益差距，使得借由策略攻击获取利益的方式失去意义。

北京大学 PEKING UNIVERSITY

安全攻防

粉尘攻击

- 区块链设计者指定规则使矿工们达成共识, 不打包交易额极小的交易。从经济学角度看, 打包更多有意义的交易能够使区块链本身更有价值, 币值也会相应提升, 每个矿工都能从中获利。

日蚀攻击

- 区块链设计者修改节点连接规则。利用随机性或是加入噪声的方法使攻击者无法轻松的通过控制受害者节点的节点表发起日蚀攻击; 或是在删除较旧 IP 之前, 先测试该 IP 能否连接上, 只有在连接失败时, 才将此地址从表中删除。

DDoS攻击

- 交易所应做好预警工作, 开启防火墙并实时监控网络中的流量状况; 被 DDoS 攻击时关闭不必要服务的端口并对所有流量进行流量识别, 从而清洗攻击流量。

对等网络安全攻防总结

- 限制节点创建
- 合理设置节点间的连接（连接数目、时长和更新频率）
- 增加连接选择和异常检测机制
- 中继网络
- 网络入侵检测系统: 入侵检测系统常通过自动识别并过滤异常活动, 来保护网络和系统免受意外攻击, 以增强网络的安全性。

北京大学 PEKING UNIVERSITY

安全攻防

不安全的合约编程

- 使用通用编程语言开发安全的智能合约
- 提出新的安全的领域专用语言

不可靠的合约执行

- 使用符号执行技术、模糊测试技术、形式化验证技术等检测合约漏洞
- 对非确定性智能合约，提供可信的外部数据源

安全攻防

- 当前智能合约安全的研究重点主要为智能合约漏洞检测与修复。现有的漏洞检测方案可以针对智能合约中的简单漏洞进行检测并提供审计报告，部分降低了智能合约开发者出错的可能和人工审计成本。

- 但由于智能合约版本更新换代较快，各个平台采用的智能合约底层框架不尽相同，现有方案很难为所有平台所有版本的智能合约提供漏洞检测服务，因此设计一种通用性强的智能合约漏洞检测工具是未来研究方向之一。

安全攻防

- 除了漏洞检测，未来还可以通过研究标准化的智能合约编写工具以及智能合约漏洞自动修复工具来减少智能合约的安全风险。另外，站在智能合约设计者的角度，为预防在复杂合约的编程过程中可能出现的安全漏洞以及因此而带来的风险，设计一种“图灵完备”的安全脚本智能合约语言也是可以考虑的方案之一。

09 区块链安全总结

对等网络安全

对等网络安全攻防方案主要通过修改节点网络连接的设置、增加网络异常检测机制以及在原有网络基础之上为节点提供额外连接等措施来解决节点间网络通信所面临的安全威胁。然而，这些方案多是针对比特币和以太坊网络的理论研究，缺乏在更多区块链网络的研究和实践。

共识机制安全

在共识机制层面上，相关安全研究一方面关注 PoW、PoS、PBFT 等共识机制的安全性分析，尤其是针对PoW和PoS的中心化安全威胁和各种挖矿策略攻击的分析；另一方面尝试提出新的共识机制以克服共识机制层的安全挑战。然而，现有研究很少有对各种挖矿策略有效检测和应对措施的讨论，且缺乏对新共识机制的安全性分析。

智能合约安全

智能合约的安全开发和可靠执行仍是智能合约未来研究的热点与重点方向，而且在产生错误时能够停止执行并自我恢复的容错合约也将是未来研究的热点方向之一。此外，在性能提升和隐私保护方案中，应更加关注智能合约运行所需数据的可用性及可信性问题，以及如何通过密码学技术和可信硬件等措施为智能合约提供更加安全可信的执行环境。

第三节
监管

01 区块链潜在的问题

02 区块链监管技术的发展

03 我国区块链的监管政策

04 国际区块链的监管政策

05 国际数字资产监管分析

01 区块链潜在的问题

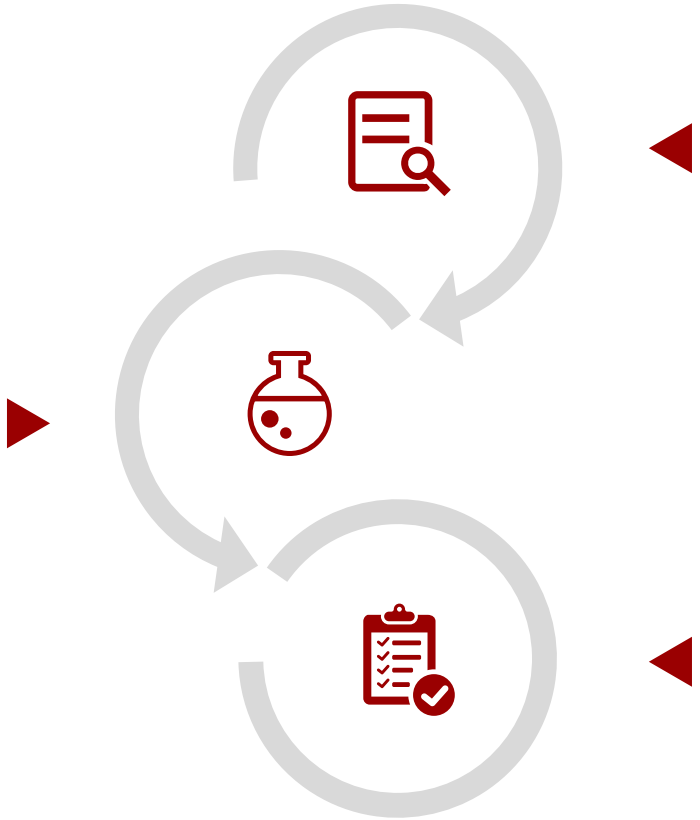
- 现在，区块链还存在很多潜在的风险，因此需要对区块链严加监管。

安全漏洞

区块链技术虽然在近年来飞速发展，但在技术上仍然存在安全问题等待被解决。

金融安全挑战

全球涌现了很多基于区块链技术跨境的金融基础设施，如果缺乏好的监管政策应对，任由这种技术涌入国内，国内的反洗钱、地下钱庄的管制、外汇的管制政策都会面临挑战。



意识形态的挑战

由于区块链上的内容难以被删除，而且所有人都可以访问历史数据，这违背很多领域的管理模式，因此很多传统应对手段受到了根本性的挑战。

02 区块链监管技术的发展

- 区块链的监管技术近年来也在蓬勃发展中，例如以下几个方面：

区块链节点的追踪与可视化

区块链节点的追踪和可视化即用动态的可视化方法展现一个区块链中的各类节点的网络地址、账户地址和交易等情况，这样可以方便管理者对若干个区块链的参与者进行有效的管理。

公链主动发现与探测技术

该技术的实质是如何在网络中发现一个在运行的公有链。该技术的主要任务是针对拥有服务功能的公有链，一般这类公链是由开发组织或是社区在互联网上运行和维护的。

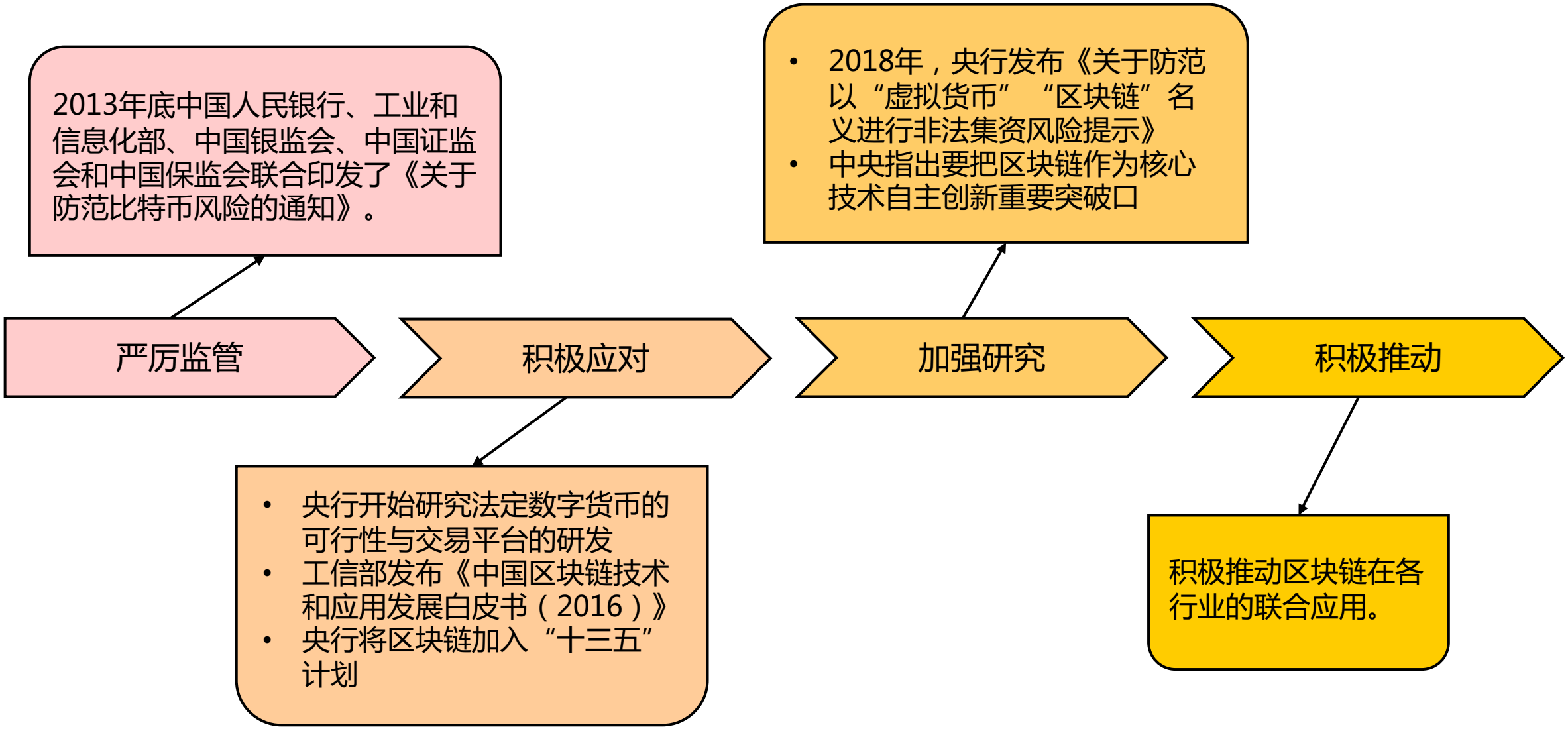
联盟链穿透式监管技术

联盟链“穿透式监管”是借用金融领域“穿透式监管”的概念，它表示对联盟链中参与节点的各种行为进行监管，以保证数据的真实性、准确性和甄别业务性质等方面的要求。

以链治链的体系结构

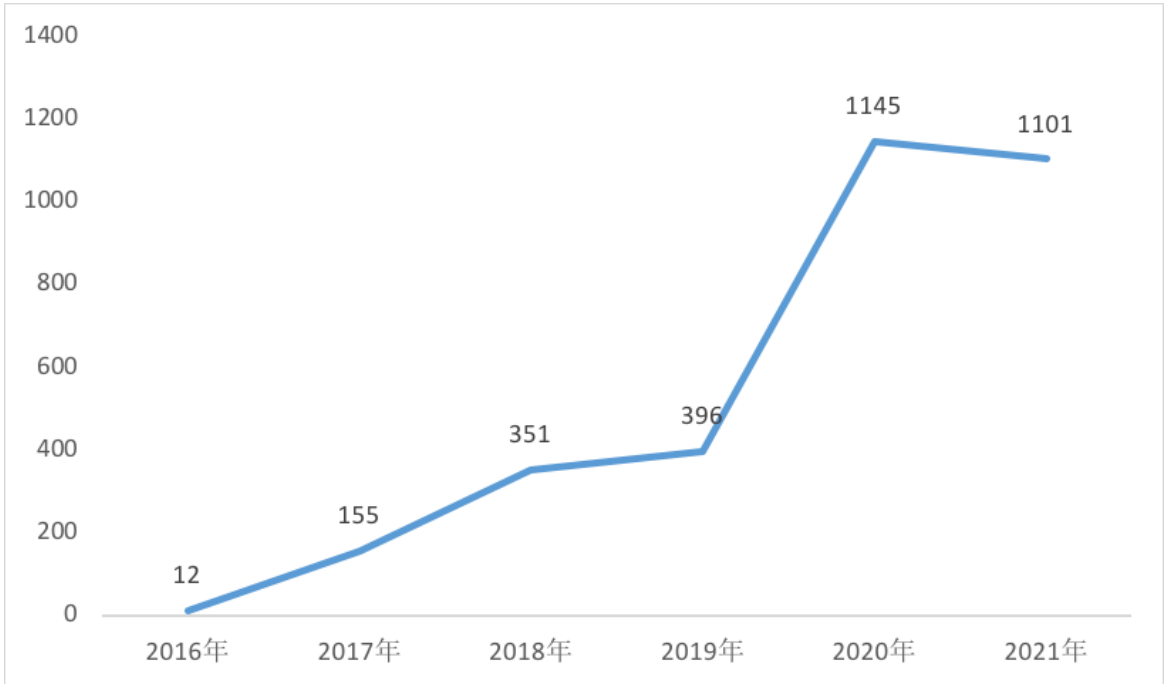
“以链治链”技术就是用区块链的技术治理区块链及其应用。在现实中，以链治链可分为链上治理和链下治理。

03 我国区块链的监管政策



03 我国区块链的监管政策

- 我国近几年来对区块链相关政策以扶持和鼓励产业为主，但同时也延续了对虚拟货币的监管和打压的高压政策：



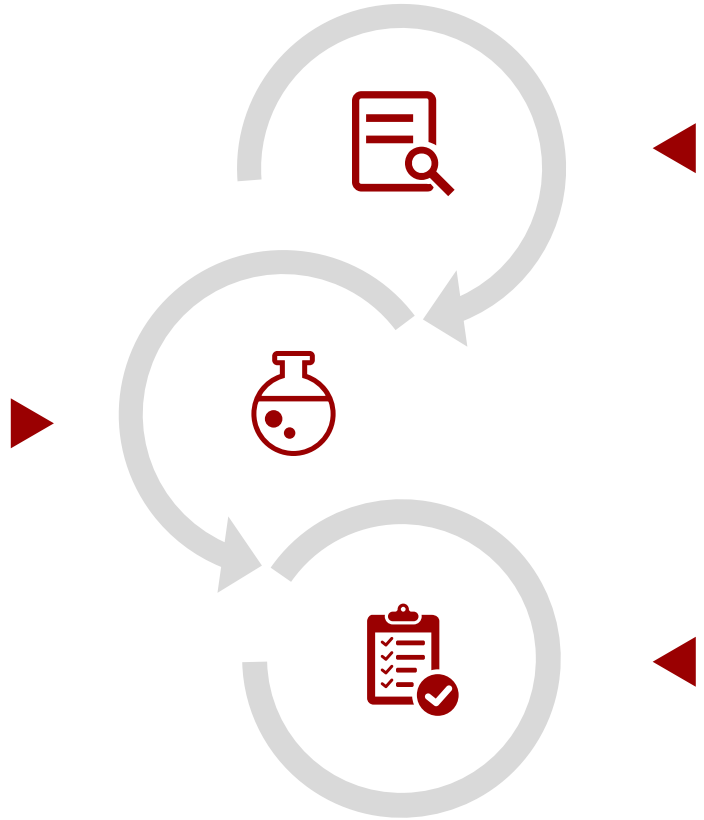
2016-2021年中国区块链相关政策数量变化趋势

04 国际区块链的监管政策

- 大多数国家近几年来对区块链技术持审慎态度。

标准制定机构及行业自律组织发挥重要作用

国际上的标准化组织均已开展对区块链或分布式账本技术的标准制定工作，以规范和引领技术发展。行业自律组织主要关注投资者保护、反洗钱反恐怖组织融资、金融稳定性等，他们在技术应用分析、监管经验分享等方面积极开展工作，并通过制定加密资产行业行为准则，发布监管指导意见等来促进行业自律。



区块链技术中立论

在国际上，大多数国家的政策和对区块链技术监管步调一致，他们对相关领域的创新研发和在实体经济领域的应用采取积极探索和支持的态度，并通过立法、制定政策或发展规划来支持技术研发和应用。

监管重点在数字货币

世界上多数国家对数字货币的发行、交易等尚未提出明确的监管框架和监管要求。部分国家允许数字资产发行使用，交易流通，这些国家出于对风险防范、反洗钱反恐怖组织融资的顾虑，他们对数字货币普遍采取较为审慎的监管态度，少数持较为开放的态度。

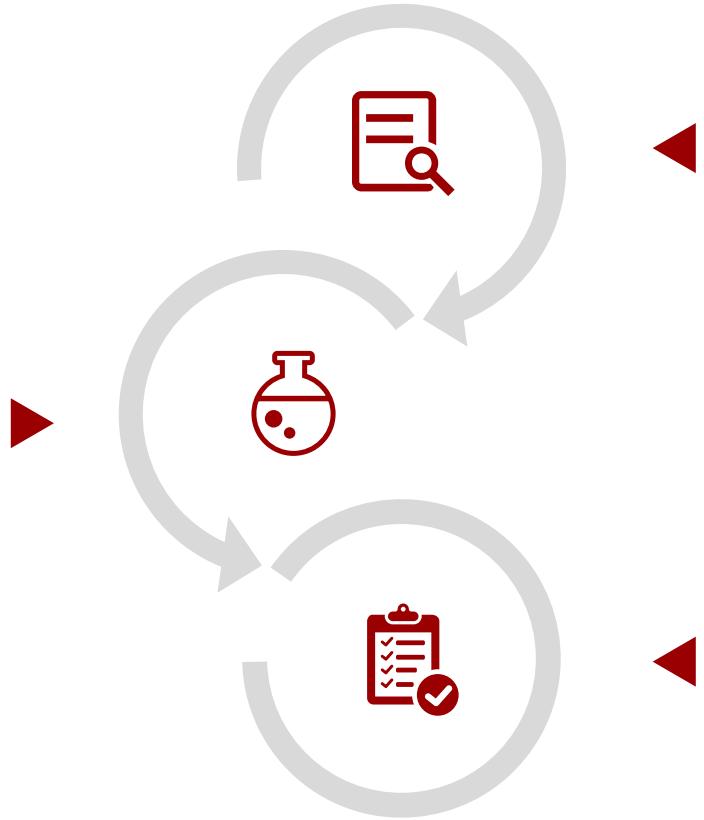
04 国际区块链的监管政策

对区块链的监管趋向成熟

除了英国、新加坡、香港、加拿大、日本等以外，更多的国家和地区开始推行沙盒制度。部分对区块链持谨慎和观望态度的国家和地区也开始尝试创建沙盒进行试点。

联合监管进程加快

联合监管主要体现在两方面：一方面是应对全球稳定币的发行，促成监管的协同和一致性；另一方面是联合反洗钱、反恐怖组织进行联合监管。



监管框架逐渐形成

2020年2月，欧盟委员会广泛收集欧盟公民、企业、监管机构和其他有关方面的反馈意见，以建立针对欧洲范围内加密资产和市场的监管框架。

05 国际数字资产监管分析

北京大学 PEKING UNIVERSITY

对数字资产的定义

目前国际上还没有对数字资产进行统一的定义，对其定性也存在多种看法。但主要的两种定位是将数字资产定位为资产或工具，这是监管机构出于监管的需要而对数字资产进行的分类。

对数字货币交易及服务的监管

部分国家允许交易数字货币和从事数字资产服务活动，并对市场设置准入门槛。从事相关活动需持有许可，并满足风控以及反洗钱、反恐怖组织等监管要求。

对数字货币发行和使用的监管

目前世界范围内大概有二十个国家或经济体允许发行或使用数字货币，大多数国家针对数字资产及相关服务没有提出明确的监管框架和要求，少部分国家禁止发行或使用私人数字货币和从事相关服务。

数字货币相关业务的税收政策

对加密货币的定义决定着相应的税收法规，随着各国对加密货币的态度变化，相应的征税态度和方案也发生着变化。整体上看，尽管存在障碍和难度，针对加密货币持有者个人征税制度被逐渐提上日程。

本章小结

本章主要围绕区块链挑战展开。

- 第一节对**区块链隐私**进行论述，主要从区块链中的隐私问题、基本要素隐私防护、基于密码学原语的隐私防护、基于后量子密码学的隐私防护这四个方面讨论区块链隐私。

- 第二节对**区块链安全问题**展开分析，主要介绍了区块链安全事件、针对区块链的攻击、针对区块链共识的攻击、针对区块链网络的攻击、针对智能合约的攻击、共识机制安全、对等网络安全、智能合约安全以及区块链安全总结这九个方面。

- 第三节对**区块链监管情况**进行概述，从区块链潜在的问题、区块链监管技术的发展、我国区块链的监管政策、国际区块链的监管政策、国际数字资产监管分析这5个方面讨论监管问题。

北京大学
PEKING UNIVERSITY

感 谢 观 看