

1. 数据层

关注区块链上数据的表达方式，包括区块头数据，签名数据，加密数据类型，交易数据的格式（UTXO），交易数据的组织形式(Merkle树)，地址数据格式（SHA256），区块的组织形式（链式数据结构）。

1. ECDSA私钥。比特币区块链使用公私钥对保护钱包的安全，目前有团队针对私钥的破解进行研究，主要办法是从硬件中得到额外信息的侧信道方法。
2. 时间戳。用于对每个数据的独立性标记，以抗伪造和重放。比特币网络有专门的时间戳服务器，存在中心化现象和安全瓶颈，目前暂无研究。
3. 各类区块链1.2点类似，而其他数据的表达格式依区块链平台不同而各有不同。
4. 网络层

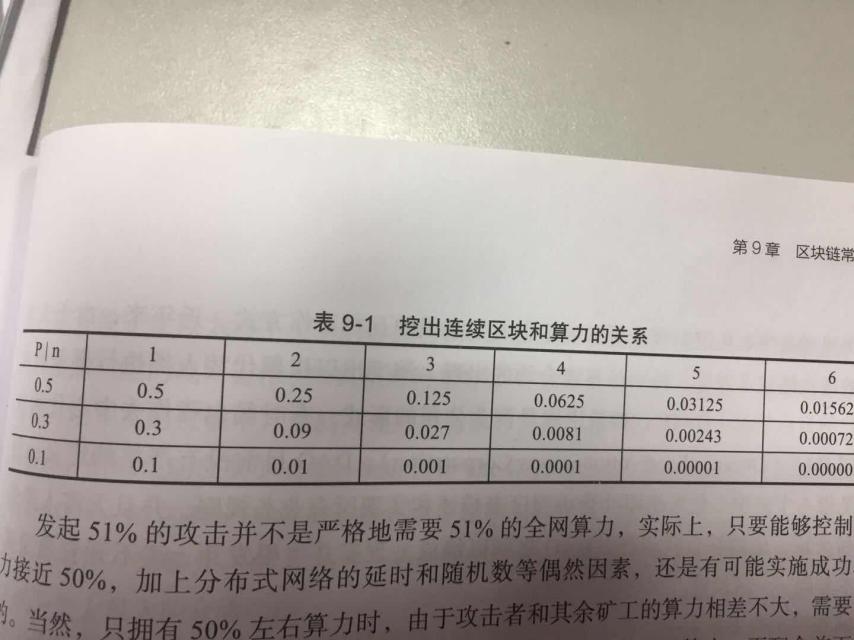
关注区块链上数据的传播方式。

1. P2P网络。p2p网络的开放性自由性可能导致女巫攻击，指在区块链网络中引入大量新的恶意节点误导节点路由表，消耗连接资源，传输非法数据等行为，区块链的开放性导致参与成本少、门槛低，攻击者可以制造虚假节点发布虚假信息降低网络可信任度。
2. 网络寻径方式。区块链内挖矿节点和路由分布的中心化，导致网络级的攻击者能通过劫持控制少量（小于100）BGP网段来实现对约50%的挖矿算力的隔离，隔离攻击的目标是将一组节点集合完全从区块链网络中隔离，无法连通，降低区块链的可信任度。
3. 传播机制（交易信息的传播和区块数据的传播）。在比特币网络中，每个比特币节点维护一个IP地址列表，IP地址列表保存所有可达节点的地址，此列表由DNS服务器初始化，之后在与其他节点交换消息时添加地址，每个比特币节点最多保持125个与其他节点的连接。每当节点接收到一个新区块，它就通过INV消息对外广播新区块的生成，INV消息包含了新区块的区块头部、hash值等必要信息。监听INV消息的节点如果验证此区块未被记录过，它将向一个邻近节点发送GETDATA消息，后者通过BLOCK消息向它返回所请求的区块数据。若20分钟后没有收到此区块，它将会向另一个邻近节点发起请求。比特币协议中节点间以对称的方式使用INV，GETDATA，BLOCK消息交换区块数据，这些消息未做加密和完整性检查；比特币节点请求20分钟未获得区块数据才会转向其他节点重新请求数据。篡改中间消息，注入恶意信息，可能导致延时攻击和DOS攻击。延时攻击的目标则是减缓来自于一组节点集合或是通往一组节点集合的区块的传播速度。
4. 验证机制。验证包括对交易信息的验证（与已有数据链比对），对新区块区块头的验证（验证各字段和hash值是否合法），对新区块区块内容的验证（验证是否是诚实节点产生的诚实区块）。目前暂无研究。
5. 共识层

关注区块链上数据副本达成一致的方法。

1. 公有区块链的安全性衡量标准（非准入，开放性）。区块链的性能指标有：共同前缀性质（诚实节点共有的最长的链，最长共同前缀）、链质量性质（诚实节点算力贡献的区块的数量称为质量）、链增长性质。安全属性有persistence（一个区块内的数据经过k个区块长度的确认，将最终被所有诚实节点记录）、liveness（确保诚实地产生的交易一旦提供给网络节点足够长的u个时间之后，就说这个交易是稳定的。）存活性和持久性相结合提供了一个强大稳健的交易账本，即被诚实地产生的交易会被采纳并且会变得不可改变。
2. 私有区块链的安全体系构建（准入，封闭性）。(1)物理安全。区块链终究是运行在网络和主机上的，传统的安全防护方法能够有效增强网络和主机安全，如VPN、防护墙、入侵检测和物理隔离。(2)数据安全。区块链各个节点之间的数据应该是加密传输的，并对发送到区块链中的数据实施严格的访问权限控制，以规避不必要的数据泄露。(3)应用安全。应用的安全需要保证认证、授权、交易规则等方面的安全，任何参与到区块链计算中的用户和计算节点都应该是被监控的。(4)密钥安全。私钥安全是区块链放伪造的核心，要建立合理的安全机制对密钥进行保管。当密钥泄露时，应当对密钥进行及时的修改。
3. 激励层

关注驱动共识算法顺利执行的机制。私有链的激励层可以专门设定，主要讨论公有链的激励层。这一层的安全属性是可用性：保障共识过程顺利进行；公平性：奖励与贡献相一致；可持续性：可长期运行。

1. 挖矿算力中心化。影响区块链公正并不需要百分之51算力，下图反映了全网算力比例与挖出连续区块的关系。在挖出连续三个区块时已经可以获得较大优势。
2. 自私挖矿行为。挖到连续两个区块隐藏起来，在他人公布一个区块时再广播自己的两个区块以获得竞争优势的行为成为自私挖矿。文献研究了自私挖矿行为的实际收益。
3. 虚标挖矿行为。以矿池为单位进行挖矿时，矿池内的一个矿工挖出区块，所有矿工按工作量平均获利。pow本质需要正确衡量工作量（即hash的尝试），然而亲自验算数百亿次的尝试不可行，唯结果论只认同成功挖出区块的办法不公平，折中方案以统计数据衡量工作量，导致造假牟利的攻击。
4. 应用层

关注区块链上各种应用的对接。

1. 在区块链的编码中，不可避免会存在很多的安全漏洞，针对这些漏洞展开的攻击层出不穷。The DAO是基于以太坊区块链平台的智能合约去中心化自治项目，2016年 6月 17 日由于其智能合约中存在的漏洞而被黑客攻击The DAO作为搭载在以太坊平台的去中心化应用，本次攻击是通过代码递归调利合约的去中心化应用，本次攻击是通过代码递归调用合约的既有漏洞实现的。
2. 2010年8月15日，比特币区块链的第74638块上被发现了一条包含有92233720368.54277039 BTC的交易记录，而且这些比特币仅被发送到两个比特币地址。而导致这次攻击的原因，是由于比特币代码中的大整数溢出漏洞。为使这笔交易失效，比特币核心开发人员开发了比特币补丁版本，并启动了硬分叉。在33个区块的竞争之后，带补丁版本的区块链才成为主链，消除了原有漏洞的影响。
3. 区块链的管理问题。作为去中心化的公有链，不应该存在一个管理机构，然而，当发生代码漏洞时需要管理机构回滚旧链开启新链，当区块链软件需要升级时，需要考虑不同版本软件的兼容问题，新旧协议的切换问题。目前区块链的管理，还是采取社区建议，矿工认可的方式进行。当社区和矿工存在分歧时，会产生硬分叉，新旧两条链同时延伸。如以太坊分叉为ETH和ETC，两链的代码相同，分叉前历史账本一样，地址私钥也一样，交易广播到连个网上都是合法的，可能会导致重放攻击。