区块链安全问题与攻击模型

吴嘉婧
副教授
中山大学 计算机学院

目录

为什么我们说区块链还不是很安全？

区块链 的安全现状： 黑客的提款机

区块链为什么不安全？

1. 区块链安全架构
2. 区块链六类安全隐患
3. 网络连通性与区块链安全性

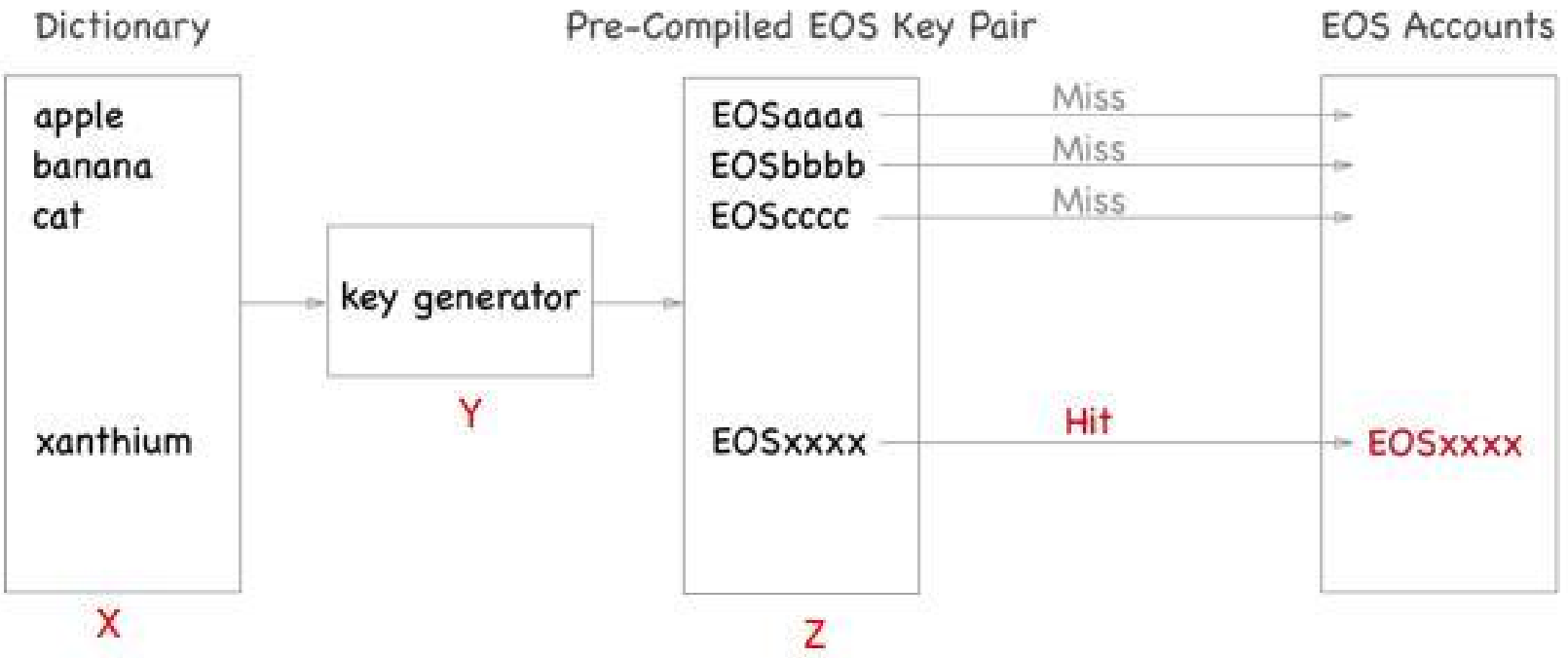
区块链安全架构

区块链结构复杂，无论是在任何一个环节出现的安全问题，都有可能造成整个区块链系统的损失。

区块链常见的六类安全隐患

1	密码学	区块链信任基础	哈希算法、数字签名、随机数等
2	用户私钥	用户参与凭证	防御彩虹攻击
3	节点系统安全	传统安全范畴	缓冲区溢出、分布式节点可靠度、API接口等
4	底层共识协议	区块链一致性	难以证明的协议安全性、不可能实现的三角关系
5	智能合约	区块链业务逻辑	合约漏洞、合约可信度以及合约的规范化
6	激励机制	好的区块链生态	防止庞氏骗局

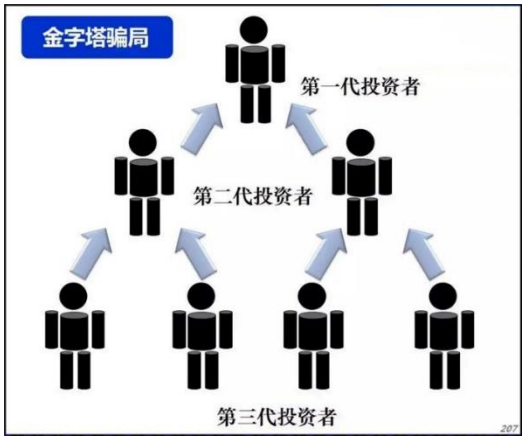
彩虹攻击的原理


Dictionary
apple
banana
cat
xanthium
X
key generator
Y
Pre-Compiled EOS Key Pair
EOSaaaa
EOSbbbb
EOScccc
EOSxxxx
Z
Miss
Miss
Miss
Hit
EOS Accounts
EOSxxxx

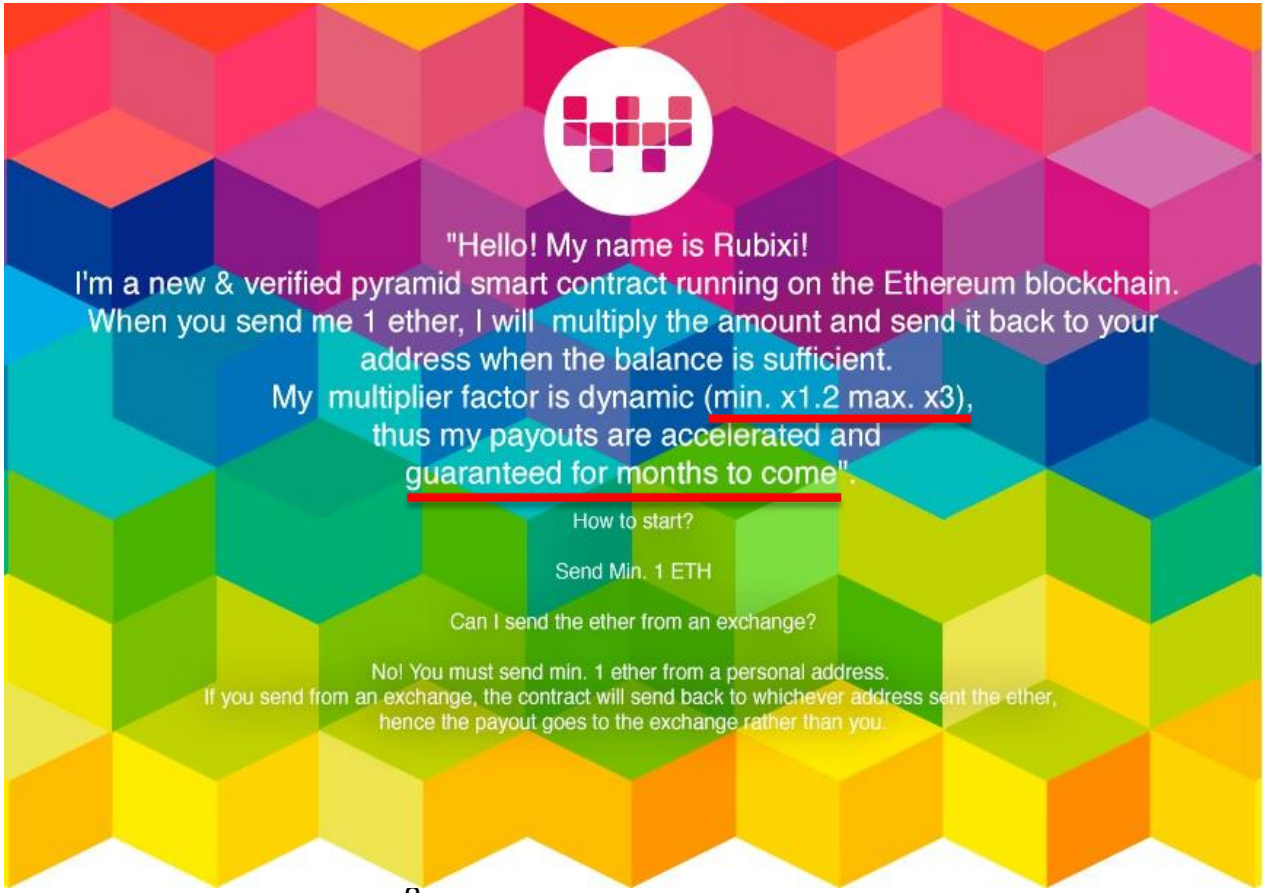
庞氏骗局

庞氏骗局

简言之：利用新投资人的钱向老投资者支付利息和短期回报，以制造赚钱的假象进而骗取更多的投资



传销



网络连通性与区块链安全

2020-IEEE INFOCOM 顶会

Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain

Yang Xiao*, Ning Zhang†, Wenjing Lou*, Y. Thomas Hou*
*Virginia Polytechnic Institute and State University, VA, USA
†Washington University in St. Louis, MO, USA

- 网络连通性越低
  - 系统越容易出现分叉
  - 矿工进行51%攻击所需的算力就会越低
  - 区块链系统的安全性也就会越差
- 网络连通性的差异性越大
  - 具有更好连通性的矿工进行51%攻击所需的算力就会越低
  - 区块链系统的安全性也就会越差

网络连通性与区块链安全

- 2020-IEEE infocom

Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain

Yang Xiao*, Ning Zhang†, Wenjing Lou*, Y. Thomas Hou*
*Virginia Polytechnic Institute and State University, VA, USA
†Washington University in St. Louis, MO, USA

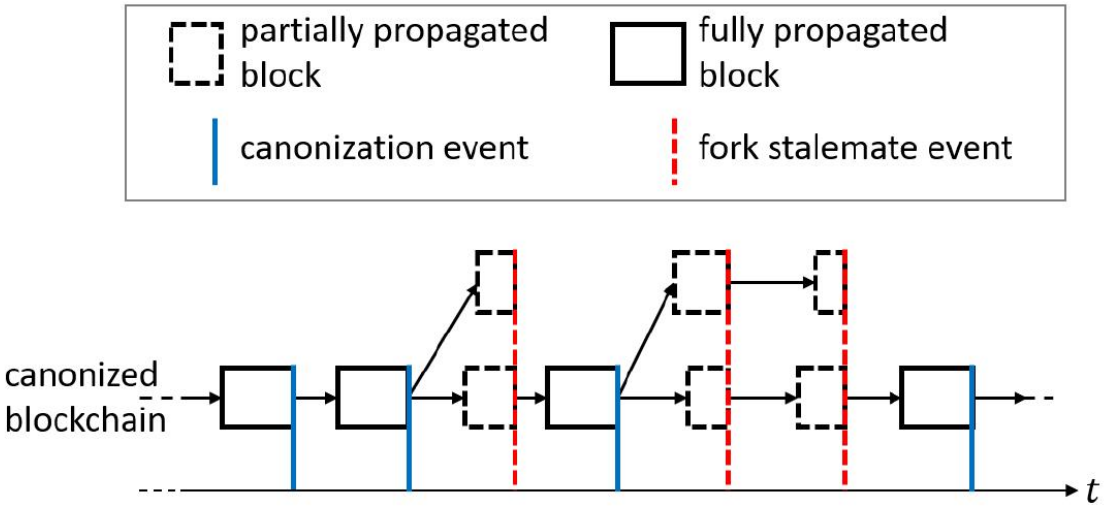


Fig. 2. Illustration of blockchain canonization and fork stalemate events. Width of a block denotes its propagation period.

- 基于假设：当一个节点已经接受节点 j 发出来的区块：block_j (h)， 然后又收到了节点i发出的区块 block_i (h)，则在本地区块链进行分叉，并停止广播区块 block_i (h)。

网络连通性与区块链安全

- 2020-IEEE infocom

Modeling the Impact of Network Connectivity on Consensus Security of Proof-of-Work Blockchain

Yang Xiao*, Ning Zhang†, Wenjing Lou*, Y. Thomas Hou*
*Virginia Polytechnic Institute and State University, VA, USA
†Washington University in St. Louis, MO, USA

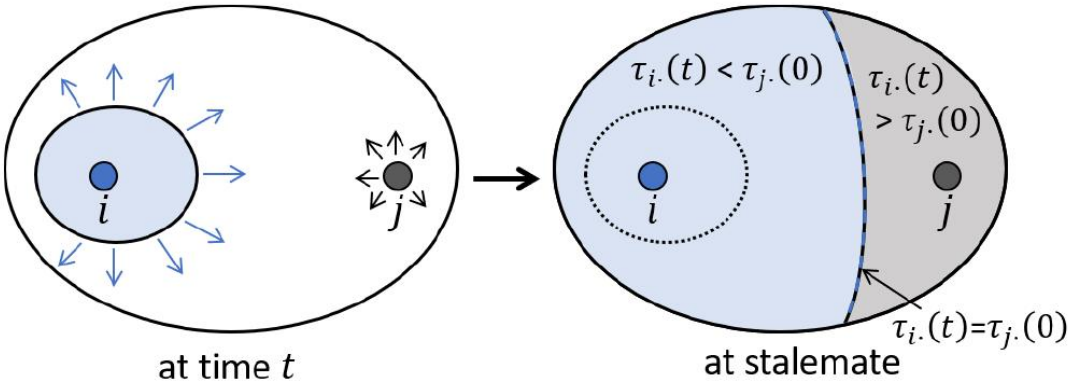


Fig. 3. Explanation of (12). Light blue (grey) area denotes portion of the network that advocates i's (j's) block. $\hat{\omega}_{i\succ j}(t)$ is evaluated by the total computing power covered by light blue area at stalemate.

- 所以，对于 well-connected 的节点，广播的速度更快，更多人支持他发出来的区块并接着往后挖，所以更容易发动51%攻击。

目录

1. 区块链为什么不安全？
2. 怎样让区块链不安全？
3. 怎样让区块链更安全？
4. 区块链攻击案例

区块链为什么不安全？

1. 基础组件和设施面临的安全威胁
2. 系统核心设计安全威胁
3. 应用生态安全威胁
4. 区块链面临的安全挑战

基础组件和设施面临的安全威胁

密码学安全威胁分析

- 2017年5月，IOTA 团队请求的研究组审计其软件及代码
- 7月，MIT研究者告知IOTA团队，他们发现了IOTA的加密哈希功能函数Curl中存在严重的漏洞（哈希碰撞），因此 IOTA 的数字签名及 PoW 安全性均无法保障
- 8月，IOTA团队采用SHA-3替代掉了备受质疑的Curl哈希算法
- 9月，MIT研究者公布了之前发布的漏洞审查报告。IOTA团队随即强烈抗议，认为MIT人员违反学术道德，并声称:

> “之前MIT学者发现的所谓的漏洞，实际上是我们有意为之，目的是防止代码被他人抄袭拷贝。”

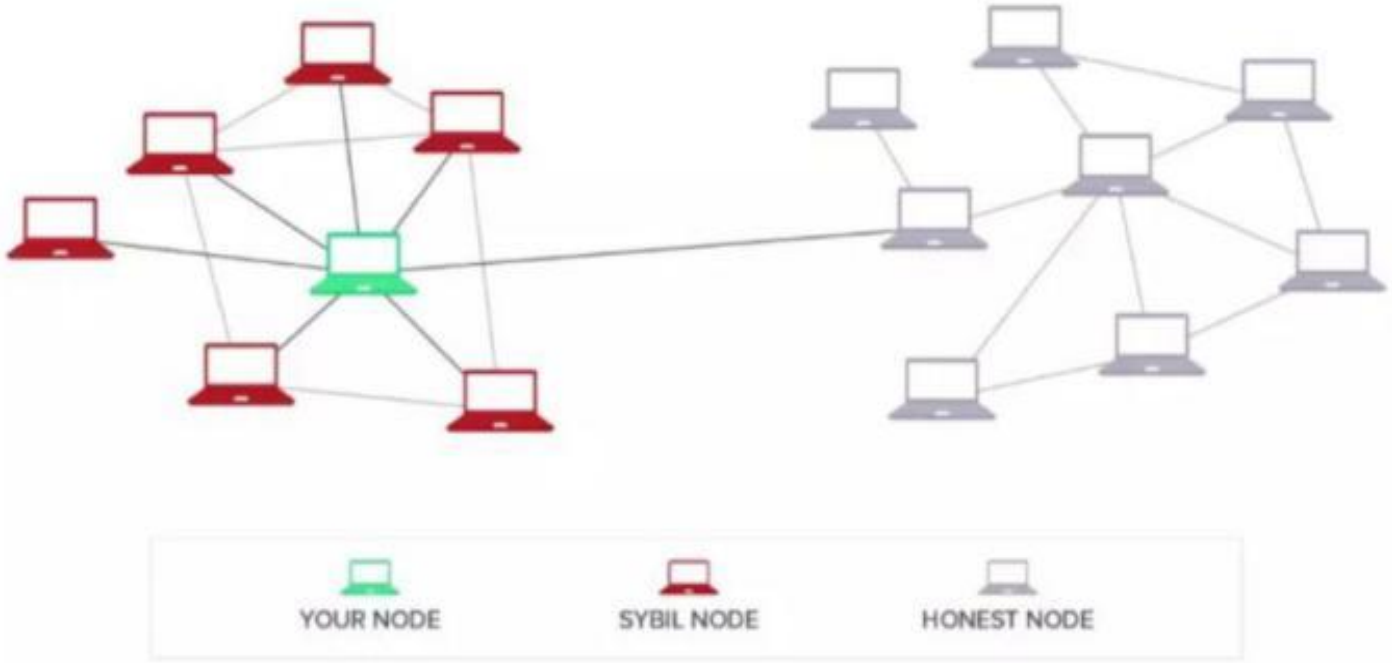
基础组件和设施面临的安全威胁

P2P网络安全威胁

- Eclipse日蚀攻击
- 分割攻击
- 延迟攻击
- DDoS 拒绝服务攻击
- 交易延展性攻击

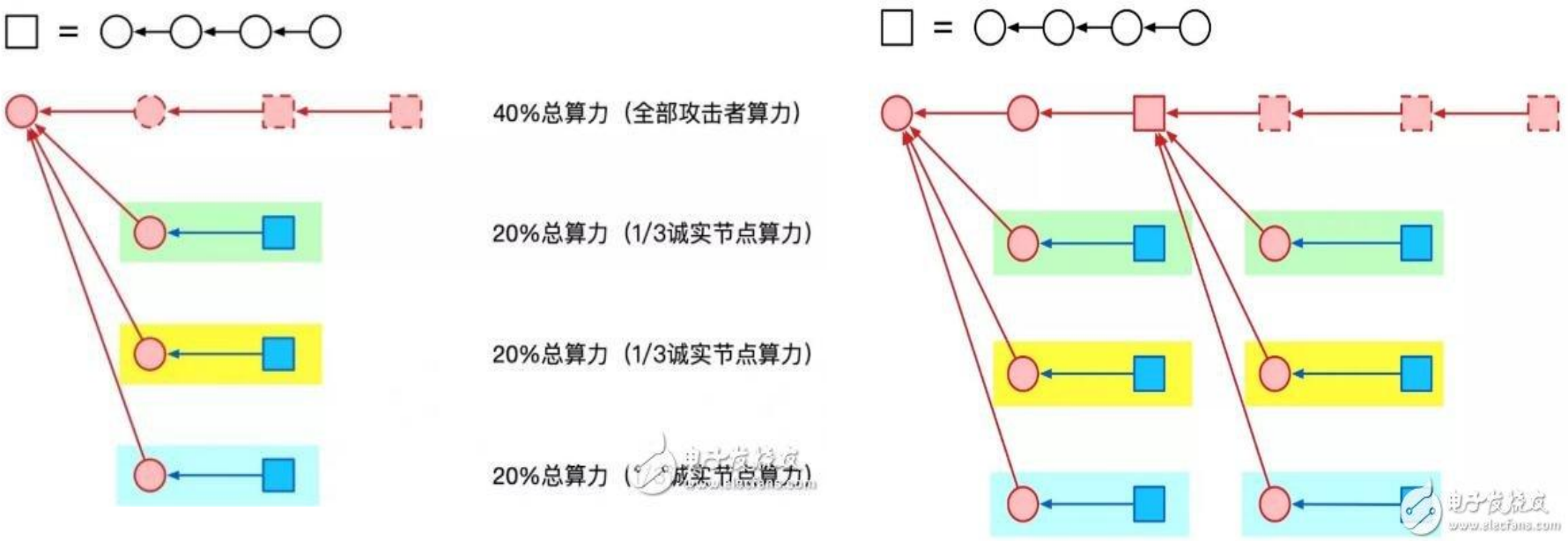
P2P网络安全威胁

- Eclipse 攻击（日蚀攻击）——孤立正常节点



P2P网络安全威胁

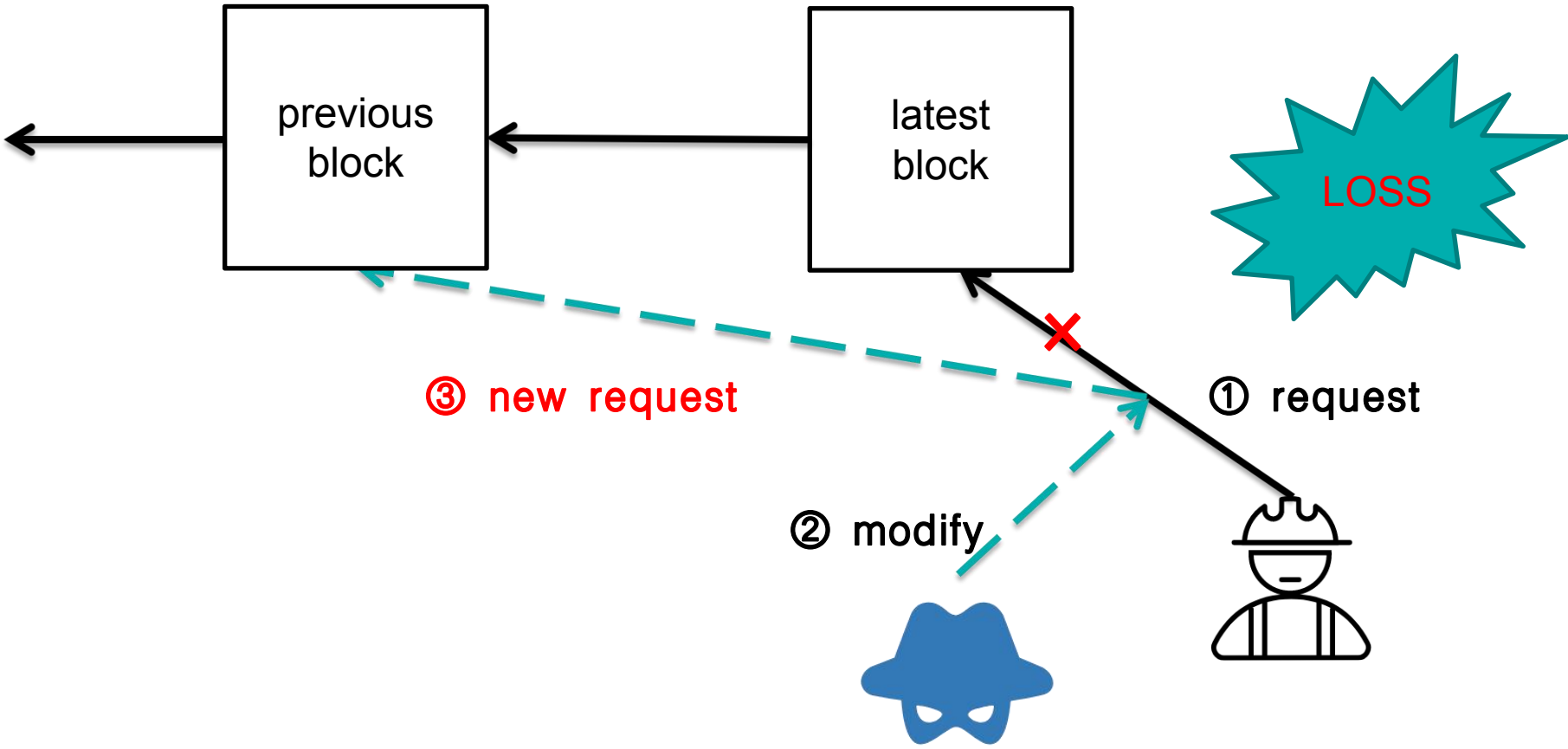
分割攻击——将诚实节点的算力分割，分开击破



- 图中每一个红色圆圈代表一个区块，攻击者让3个社区的诚实节点分别在右侧 3 个不同的子树下贡献算力。
- 图中方框代表在一段时间内新生成的一些区块。其中虚线表示坏人藏起来没有广播区块。蓝色表示诚实节点生成的区块。
- 之后，攻击者如法炮制，重复上述这个过程。

P2P网络安全威胁

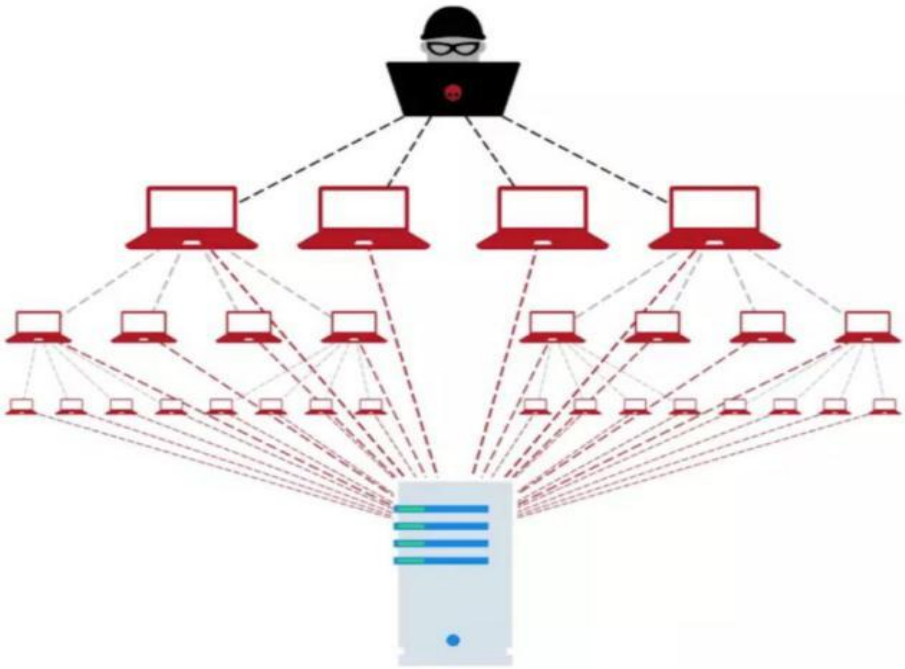
- 延迟攻击——反馈过时区块



P2P网络安全威胁

DDos攻击——破坏诚实节点通信

- 传统的DoS攻击：入侵，形成僵尸网络，发起DoS攻击
- 分布式DoS攻击：不需建立僵尸网络，发起DoS攻击



P2P网络安全威胁

DDos攻击

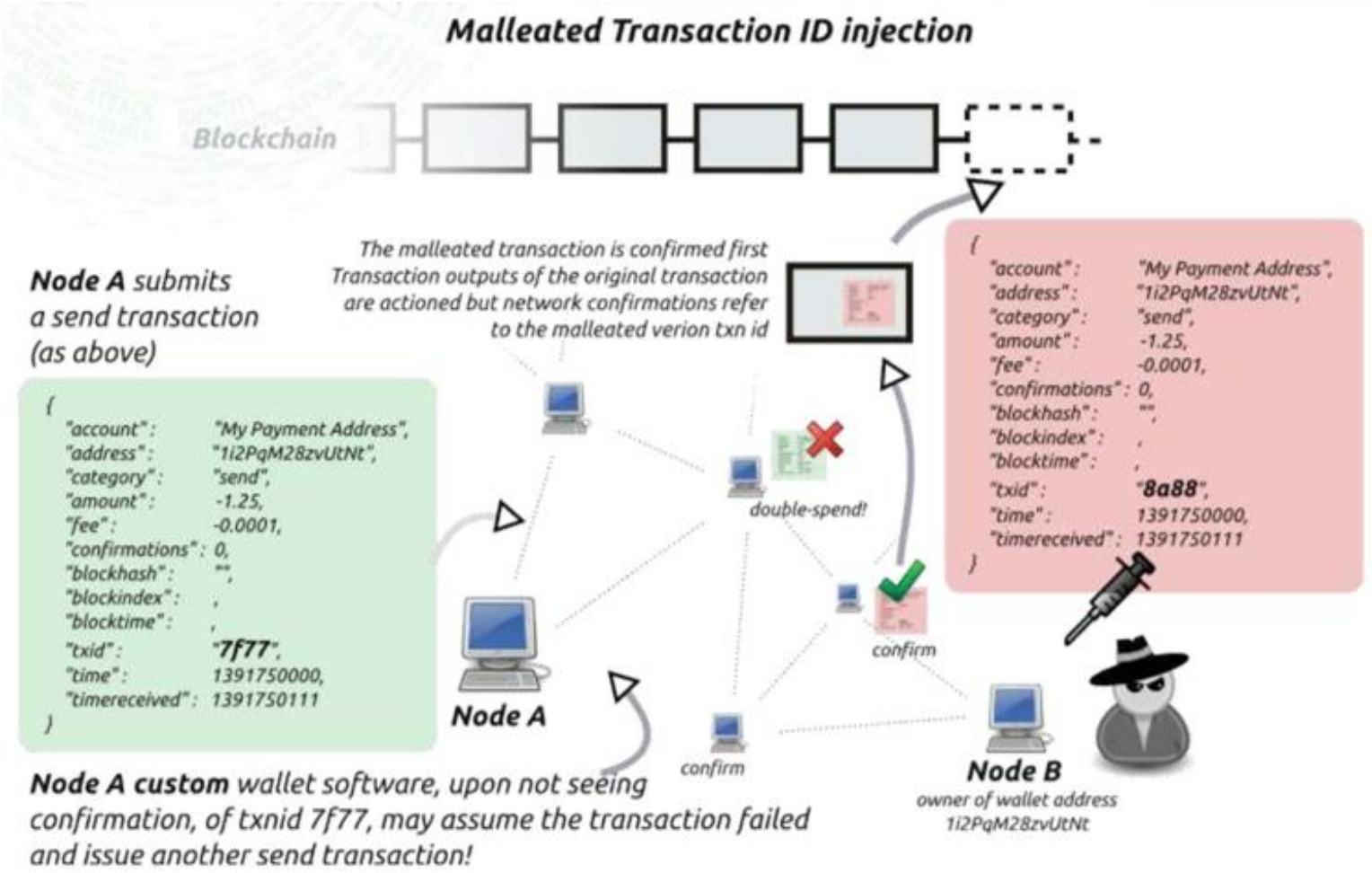
攻击方式

主动攻击：
通过主动向网络节点发送大量虚假信息，使得针对这些信息的后续访问都指向受害者来达到攻击效果，

被动攻击：
通过修改区块链客户端或者服务器软件，被动等待来自其它节点的查询请求，再通过返回虚假响应实现攻击效果。

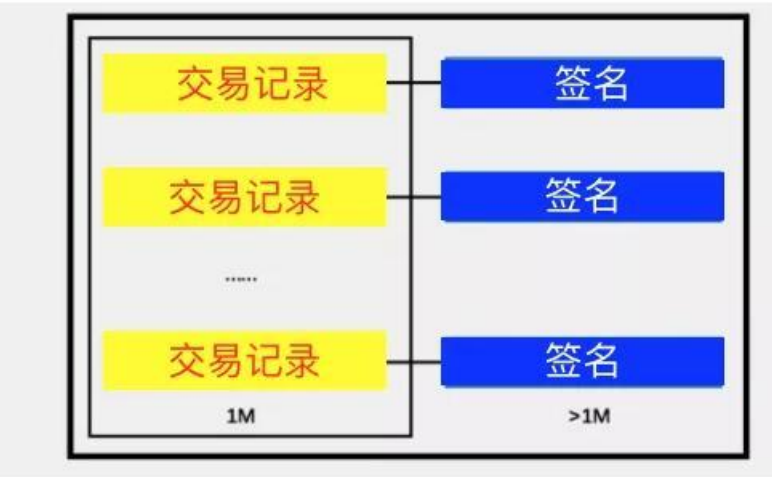
P2P网络安全威胁

- 交易延展性攻击——破坏区块链



P2P网络安全威胁

交易延展性攻击——破坏区块链



解决方法：Segwit（隔离见证）

将签名从交易中移除，生成区块头的交易哈希值，完全由交易信息决定。即使签名被改变，而交易的内容没有改变，交易的哈希仍然相同。

P2P网络安全威胁

恶意挖矿攻击

- 目的：劫持用户挖掘设备挖掘加密货币
- 解决方式：安装安全插件，注意设备性能和CPU利用率

木马攻击

- 目的：使计算机感染木马病毒并实施操作
- 解决方式：安装安全插件，提升计算机的安全性

系统核心设计安全威胁

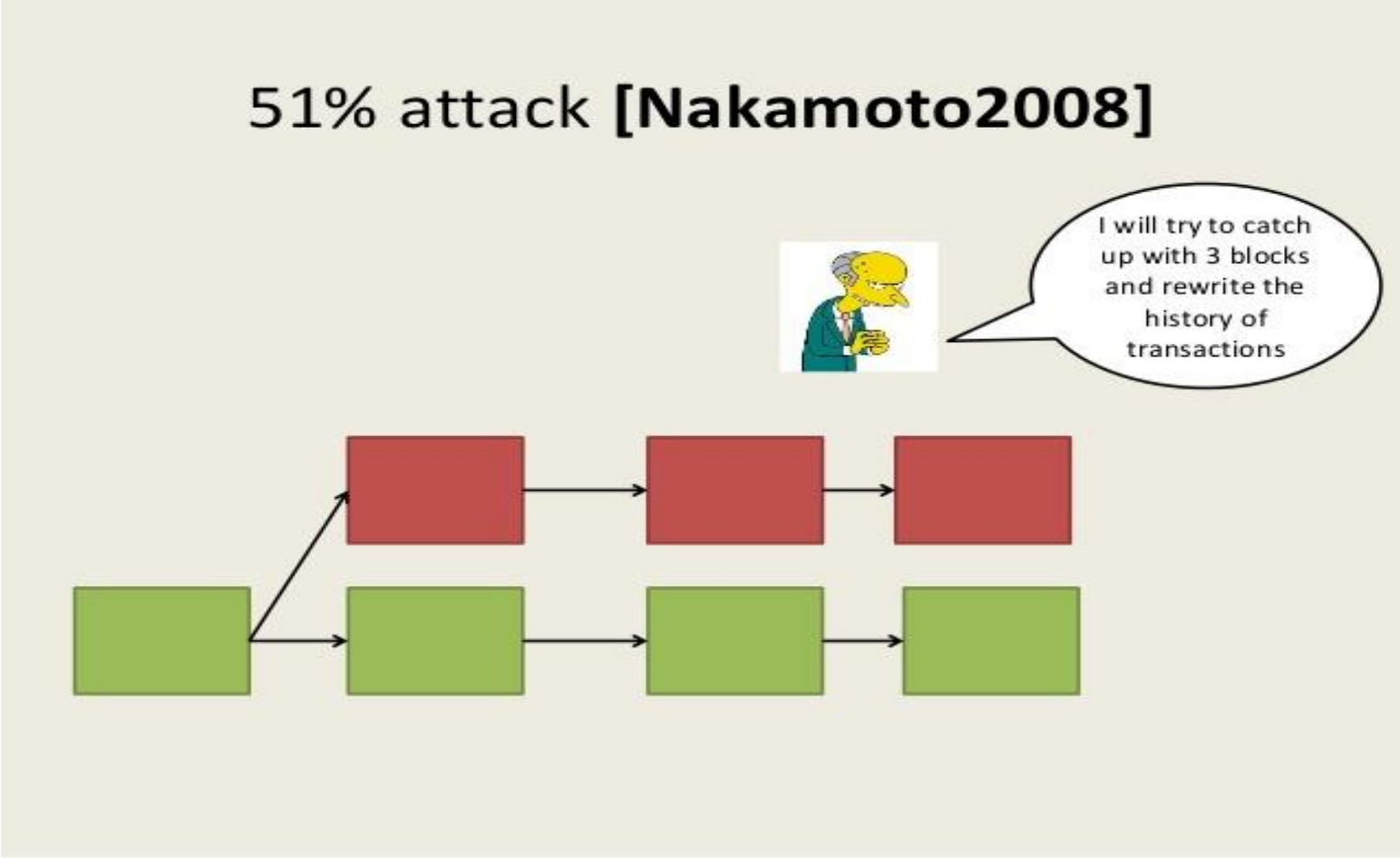
共识层安全威胁

表 2-1 常见的共识机制攻击方式对比

攻击类型	PoW	PoS	DPoS
51%攻击	√	—	—
女巫攻击	√	√	√
长距离攻击	—	√	√
短距离攻击	—	√	—
币龄累计攻击	—	√	√
预计算攻击	—	√	—

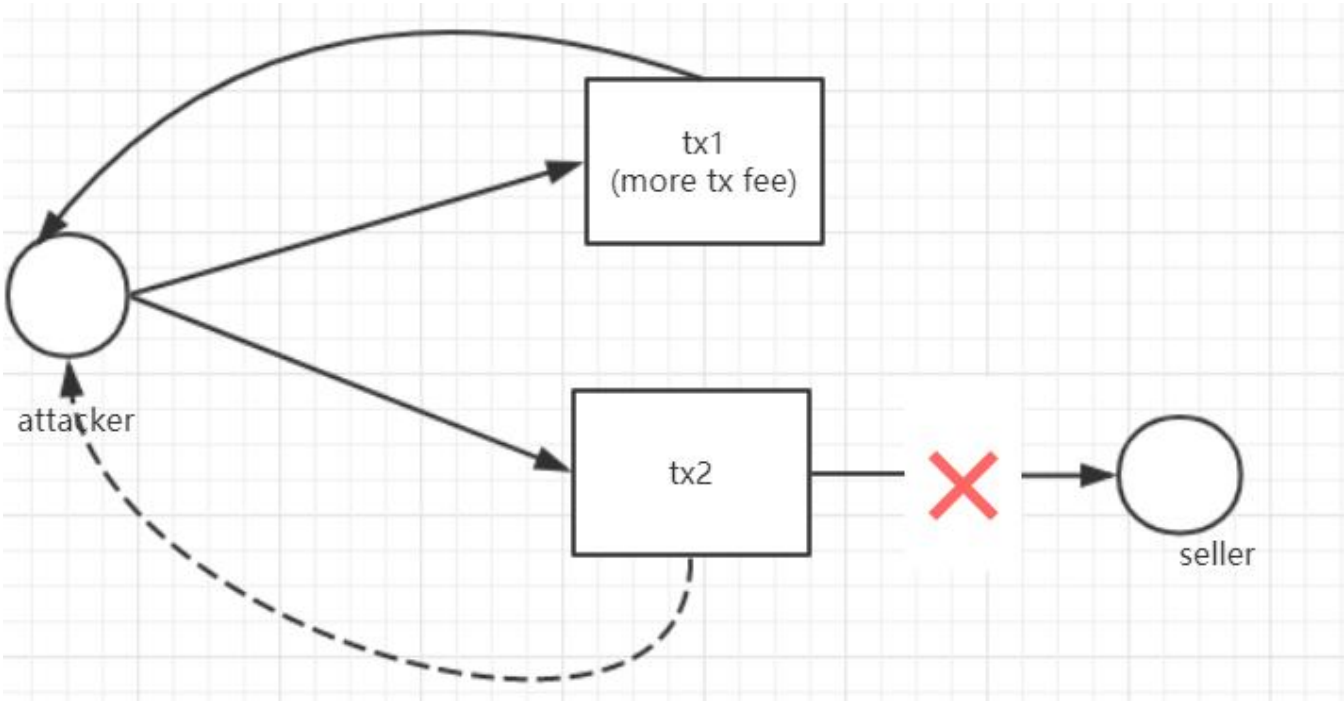
共识层安全威胁

- 51%攻击



共识层安全威胁

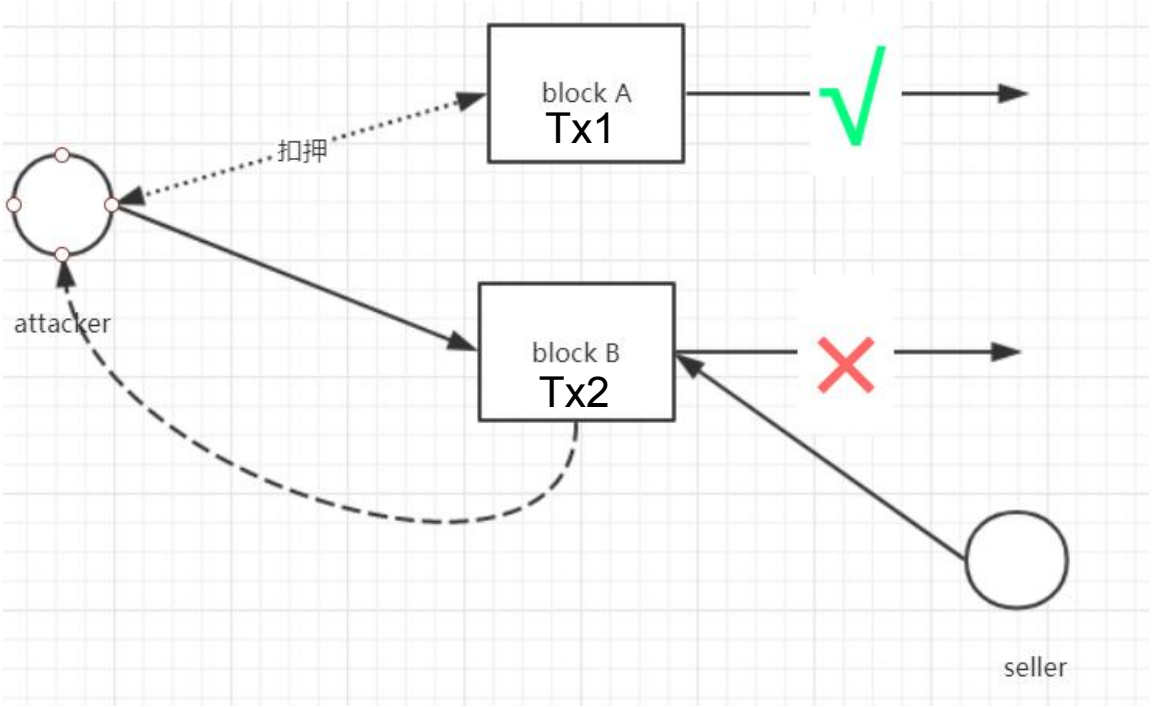
双花攻击——① Race Attack



关于双花攻击的三种方式参考链接：
https://www.qukuaiwang.com.cn/news/143715.html
https://36kr.com/p/1722580041729

共识层安全威胁

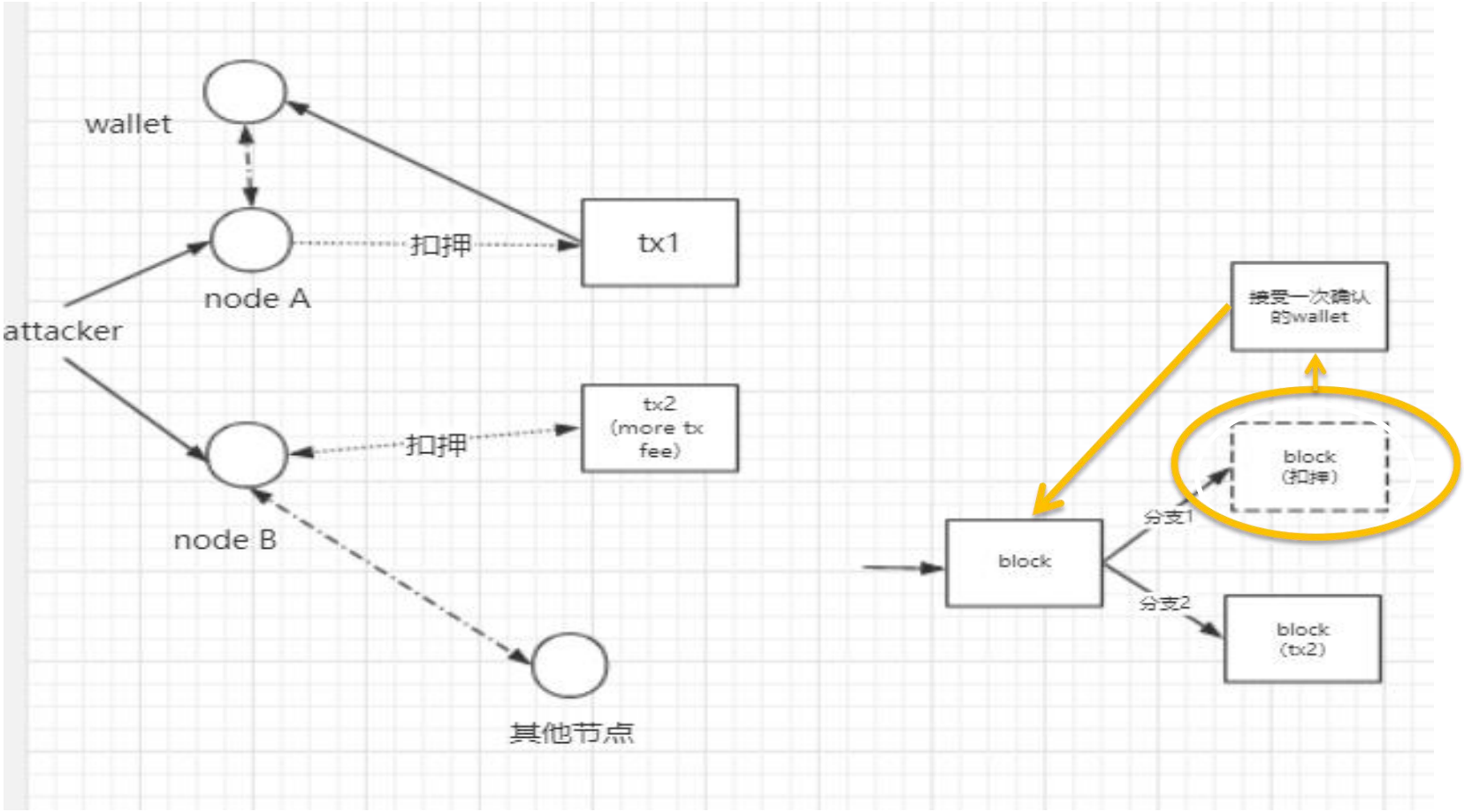
双花攻击——② Finney Attack



然而，这种攻击在实践中很难使用，因为它要求攻击者具有高哈希率(因为他创建了自己的块)，而且大多数商家现在倾向于需要一些确认。

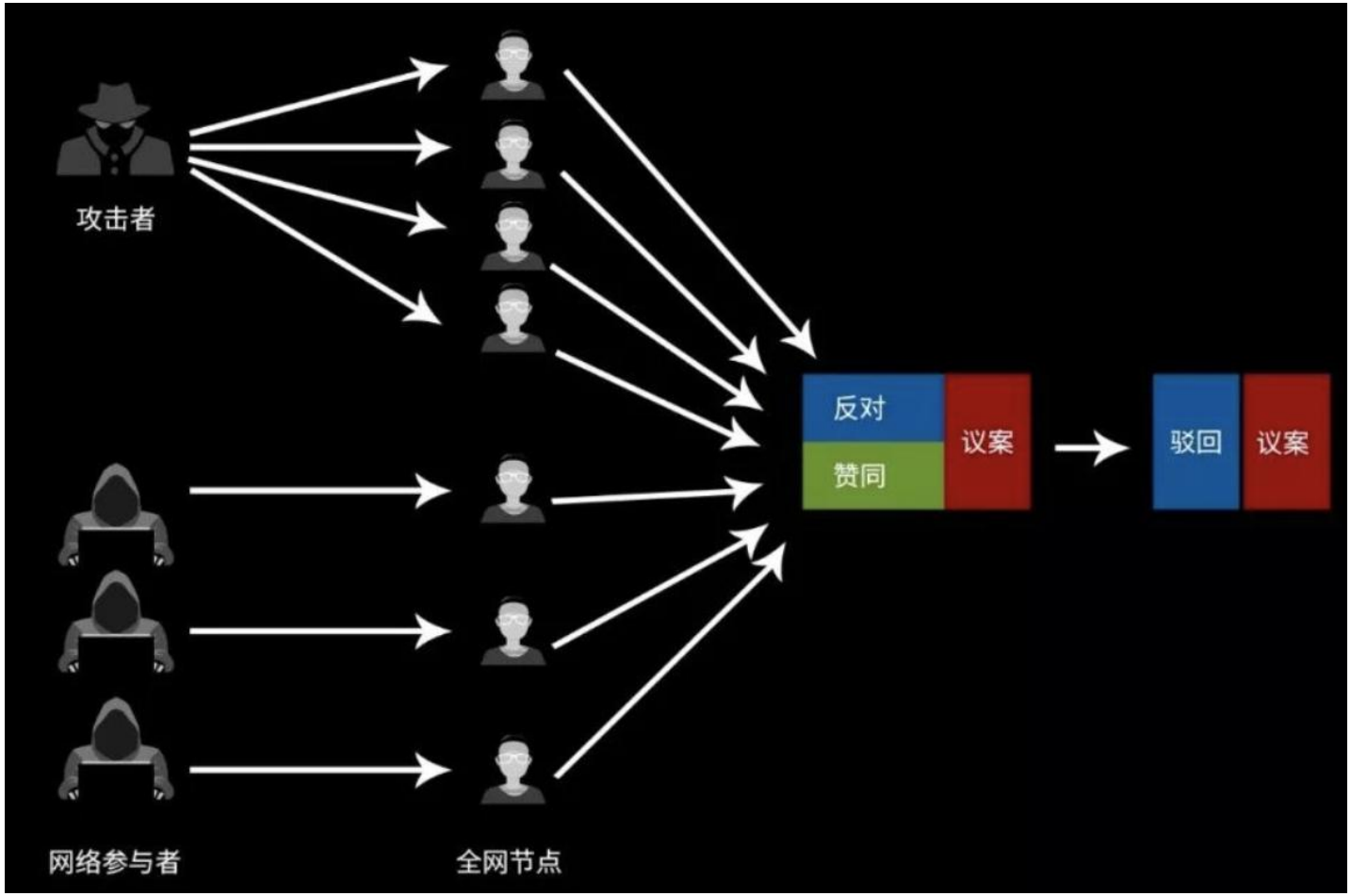
共识层安全威胁

- 双花攻击——③Vector76 Attack（①+②）



共识层安全威胁

- Sybil女巫攻击



共识层安全威胁

- 短距离攻击
- 长距离攻击
- 币龄累计攻击
- 预计算攻击

参考梆梆安全研究院发布的《区块链安全白皮书》

https://m.qukuaiwang.com.cn/news/14259.html

合约层安全威胁

序号	漏洞名称	漏洞描述
1	The DAO 漏洞	The DAO 智能合约中的 split 函数存在漏洞，攻击者可以在 The DAO Token 被销毁前，多次转移以太币到 Child DAO 智能合约中，从而大规模盗取原 The DAO 智能合约中的以太币。
2	Parity 多重签名钱包合约漏洞	核心问题在于越权函数调用使多重签名的智能合约无法使用。攻击者通过调用公开函数 initWallet，能够重新初始化钱包，对之前合约钱包的所有者进行覆盖，即可改变钱包所有者为攻击者，相当于从 Unix 中获得了 Root 权限。
3	Parity 多重签名钱包提款漏洞	该漏洞使得黑客能通过库函数成为库的主人，然后调用自杀函数报废整个合约库，导致钱包的提款功能都失效。
4	太阳风暴	Solidity，以太坊用于开发智能合约的类 java-script 语言，被发现有一个安全漏洞，当以太坊合约进行相互调用时，它们自身的程序控制和状态功能会丢失。它能切断以太坊智能合约间的沟通，就像太阳风暴能切断地球的通讯设备一样，可以影响整个以太坊。
5	以太坊编程语言 Solidity 漏洞	影响智能合约中一些地址以及数据类型，大多数受影响的合约将无法被撤回或更改。
6	智能合约 Fallback 函数调用漏洞	当调用某个智能合约时，如果指定的函数找不到，或者根本就没指定调用哪个函数（如发送以太币）时，fallback 函数就会被调用，黑客可以利用 fallback 函数做出很多危害系统的事情。
7	智能合约递归调用漏洞（recursive）	用户取款的代码存有严重的递归调用漏洞，攻击者可轻松地将用户账户里的以太币全部提走。
8	调用深度限制（call depth）	以太坊虚拟机 EVM 中一个智能合约可以通过 message call 调用其它智能合约，被调用的智能合约可以继续通过 message call 再调用其它合约，甚至是再调用回来（recursive）。黑客可以利用嵌套调用的深度被限定为 1024 发动攻击。
9	浪子合约漏洞	交易资金因为漏洞返还给所有者、交易者过去发送给以太网的地址，以及特定地址。这种漏洞就像是空手套白狼，买家得到商品，而卖家无法得到加密货币。
10	自杀合约漏洞	智能合约的拥有者可以在以太坊发生故障时选择退回，类似于微信中的撤回选项。但是这个指令也可以被其他人执行，使得交易失败。
11	贪婪合约漏洞	这是指那些永远停留在以太坊的智能合约，上述的 Parity 漏洞正是一种贪婪合约，它会把智能合约所涉及的商品以及加密货币锁定在以太坊中，交易双方均无法得到，也不能取消。

来源于：《区块链安全白皮书》

合约层安全威胁

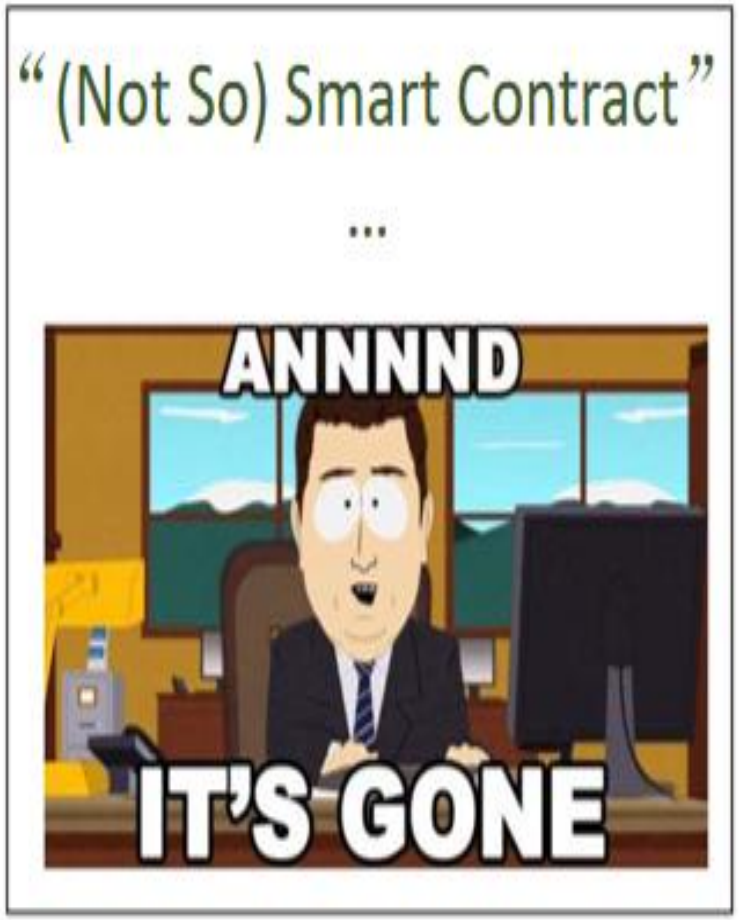
著名的智能合约攻击事件

- 2016年，黑客攻击DAO智能合约，成功盗取360万个ETH（现在相当于72亿元）

- 2017年，Parity多重签名合约存在漏洞，被两次攻击，先后造成15.3万个ETH、93万个ETH的损失

- 2018年4月，美链BEC出现合约无限复制token的Bug，市值蒸发64亿

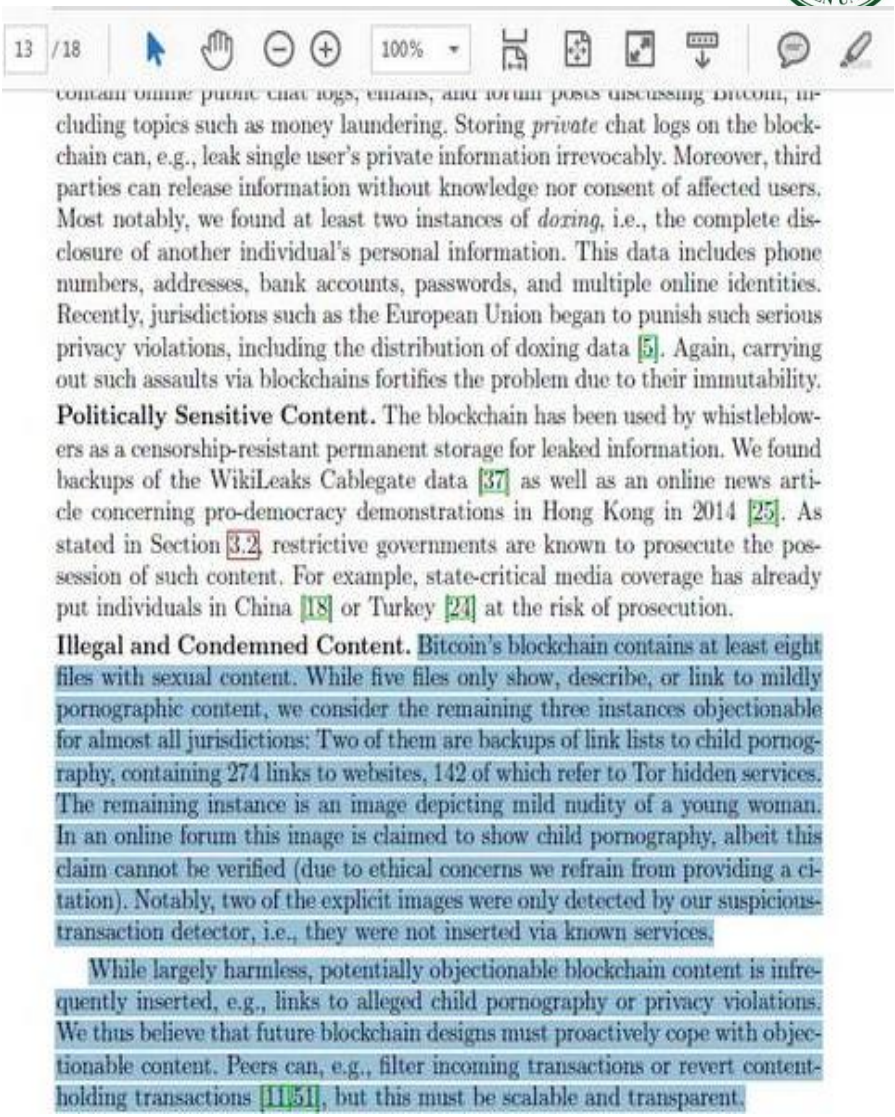
- 2018年7月，Bancor智能合约更新程序遭黑客攻击，损失约2.5万个ETH和一些其他加密货币



数据层安全威胁

- 2017年在EuskalHack安全会议上，有安全研究者提出了基于区块链模式的 botnet 网络，利用区块链网络进行C&C的恶意指令发布并且提供了PoC。

- 2018年3月德国 RWTH 亚琛工业大学的研究人员发现了比特币区块链中的非财务数据，其中包括色情内容等。在他们的论文中，研究人员指出可以通过多种方式在加密货币的区块链上插入内容。


13 / 18 100%

contain online public chat logs, emails, and forum posts discussing Bitcoin, including topics such as money laundering. Storing *private* chat logs on the blockchain can, e.g., leak single user's private information irrevocably. Moreover, third parties can release information without knowledge nor consent of affected users. Most notably, we found at least two instances of *doxing*, i.e., the complete disclosure of another individual's personal information. This data includes phone numbers, addresses, bank accounts, passwords, and multiple online identities. Recently, jurisdictions such as the European Union began to punish such serious privacy violations, including the distribution of doxing data [5]. Again, carrying out such assaults via blockchains fortifies the problem due to their immutability.

Politically Sensitive Content. The blockchain has been used by whistleblowers as a censorship-resistant permanent storage for leaked information. We found backups of the WikiLeaks Cablegate data [37] as well as an online news article concerning pro-democracy demonstrations in Hong Kong in 2014 [25]. As stated in Section 3.2, restrictive governments are known to prosecute the possession of such content. For example, state-critical media coverage has already put individuals in China [18] or Turkey [24] at the risk of prosecution.

Illegal and Condemned Content. Bitcoin's blockchain contains at least eight files with sexual content. While five files only show, describe, or link to mildly pornographic content, we consider the remaining three instances objectionable for almost all jurisdictions: Two of them are backups of link lists to child pornography, containing 274 links to websites, 142 of which refer to Tor hidden services. The remaining instance is an image depicting mild nudity of a young woman. In an online forum this image is claimed to show child pornography, albeit this claim cannot be verified (due to ethical concerns we refrain from providing a citation). Notably, two of the explicit images were only detected by our suspicious-transaction detector, i.e., they were not inserted via known services.

While largely harmless, potentially objectionable blockchain content is infrequently inserted, e.g., links to alleged child pornography or privacy violations. We thus believe that future blockchain designs must proactively cope with objectionable content. Peers can, e.g., filter incoming transactions or revert content-holding transactions [11, 51], but this must be scalable and transparent.

(论文报告原文13页)

应用生态安全威胁

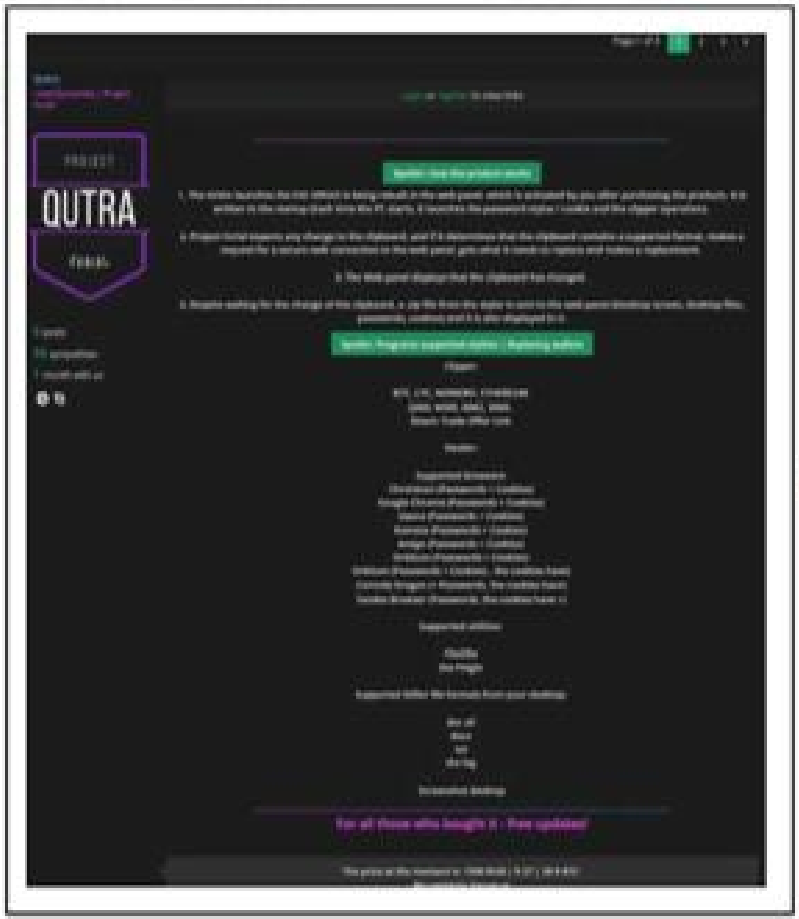
交易网站安全威胁

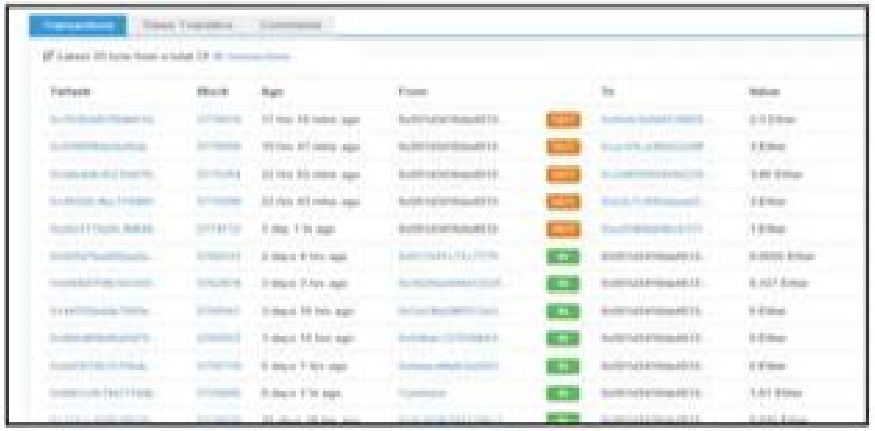
- 针对服务器软件的攻击
  - Tether (USDT)
  - Blockchain.info
  - CoinDash ICO
  - Steem.it (STEEM)
- 针对管理人员的攻击(钓鱼)
  - BitPay
- 针对云服务器提供商的攻击
  - Slush Pool

应用生态安全威胁

数字货币钱包App安全威胁

数字货币钱包App与其他App一样，会遭受破解、内存篡改攻击等





区块链面临的安全挑战

钱包安全管理

- 保护私钥在运行和存储的安全
- 考虑用户密钥被盗、丢失后账户资产安全

智能合约安全

- 提升智能合约代码的可靠性
- 进行智能合约协议安全性分析

隐私安全

- 加密交易内容
- 验证交易的正确性

目录

1. 区块链为什么不安全？
2. 怎样让区块链不安全？
3. 怎样让区块链更安全？
4. 区块链攻击案例

怎样让区块链更安全？

1. 人为主观的强化
2. 区块链系统漏洞优化
3. 结合其他技术提升区块链安全性

1. 人为主观的强化 (1/3)

区块链资产的 持有者（用户）

- 牢记：私钥即权利
- “买买提”
- 不要重复使用密码，使用自动生成的密码
- 开启2FA
- 从收藏夹访问交易所、检查SSL标志。
- 学会识别并避免百度、谷歌等的推广链接
- 仔细阅读产品或网站上的安全提示相关内容
- 大额资产离线存储，或使用知名厂商的硬件钱包
- 慎用云盘、云笔记软件等备份私钥数据
- 保管好您的邮箱账号

1. 人为主观的强化 (2/3)

区块链项目的 开发者 ：

- 习惯“去中心化”思维，您面对的是拜占庭节点
- 不要尝试使用自己发明的加密算法
- 谨慎对待随机数，不要轻信时间戳
- 重视安全测试用例的编写，在开发时即充分开展安全测试
- 检视您引用的每一个Library
- 如果您的工作基于其他项目（如BTC/ETH），应关注并同步更新其漏洞补丁部分的代码
- 告诫自己写好智能合约很难，对合约安全检查应谨小慎微
- 补齐加密学和安全基础知识，并学会看论文
- 您开发的区块链系统有多安全，完全取决于您，而不是取决于高大上的“区块链技术”

1. 人为主观的强化 (3/3)

区块链相关产品的 创业者

- 如您的项目尚未开始：问一问自己，一定要用区块链吗？
- 如您的项目已经开始：重新从安全的角度审视它的各个方面
- 只有当安全事故出现的时候，才能知道代价有多么大
- 防范针对自己以及关键团队成员（人）的安全攻击
- 修复服务器上非区块链系统（网站系统、操作系统等）的漏洞
- 划拨资金设立Bug Bounty；聘用安全顾问，请第三方审计代码
- 如果产品为公链，建议用两组人员、两种不同语言独立开发
- 开源的，才是安全的（但不要等到上线前一天才开源）
- 做好思想准备：系统一定有漏洞、一定会被攻破的。因此要有：
  安全专员、应急小组、安全预案

2. 区块链系统漏洞优化 (1/2)

比特币“1 RETURN”Bug（核心代码缺陷）

- 2010年7月，德国程序员 Art Forz 发现比特币脚本程序中有一处潜在破坏力极强的 Bug
- **该Bug被恶意用户利用后，可以越权动用他人钱包中比特币**，从而可能导致比特币变得一文不值
- 比特币的创始人中本聪在邮件中向 Kavin 说（Kavin 是比特币早期的另一位主要开发者，中本聪消失后接手比特币代码管理权）：“对于其他不知道该 Bug 的人，要避免描述这个 Bug 的名字（1 Return）”

```
case OP_RETURN:
{
    pc = pend;
}
break;

OP_1 OP_RETURN
```

Digital Gold : Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money

- **该 Bug 在大多数比特币节点经过更新修复、不再受此问题影响后，才被公之于众**
- 程序员ArtForz在发现Bug后选择悄悄告诉中本聪，成为比特币区块链历史上鲜为人知的安全救星

2. 区块链系统漏洞优化 (2/2)

比特币天量刷币漏洞（核心代码缺陷）

- 2010年8月，美国程序员Jeff Garzik发现比特币区块链中第#74638个区块，包含了一笔涉及3个地址、金额超过1800亿BTC的交易

- 经核实，**代码中检查交易的逻辑存在求和溢出漏洞，而未被妥善处理，**发现此Bug后，比特币开发者很快发布了含有补丁的新版本软件

- 在第#74691块，**带补丁版本的比特币区块链的长度终于追赶上并且超越了包含天量BTC漏洞的链**，最终有惊无险地解决了这次比特币区块链历史重大的危机事件。

3. 结合其他技术提升区块链安全性

- Open Question
  - Various Solutions are needed

目录

1. 区块链为什么不安全？
2. 怎样让区块链不安全？
3. 怎样让区块链更安全？
4. 区块链攻击案例

区块链攻击案例 —— 最新研究

1. 区块截留攻击
2. 以太坊空账户DoS攻击
3. 比特币矿池中的DDoS攻击

区块截留攻击

Q: 矿池（mining pool）如何计算矿工的贡献比例？

部分工作量证明机制（partial proof of work, PPoW）

完整PoW

(1) 系统挖矿难度为D，要求区块的hash值前n位为0

0000000000000000000000000000000000……

n位

PPoW

(2) 矿池挖矿难度为D'，要求区块的hash值前m位为0

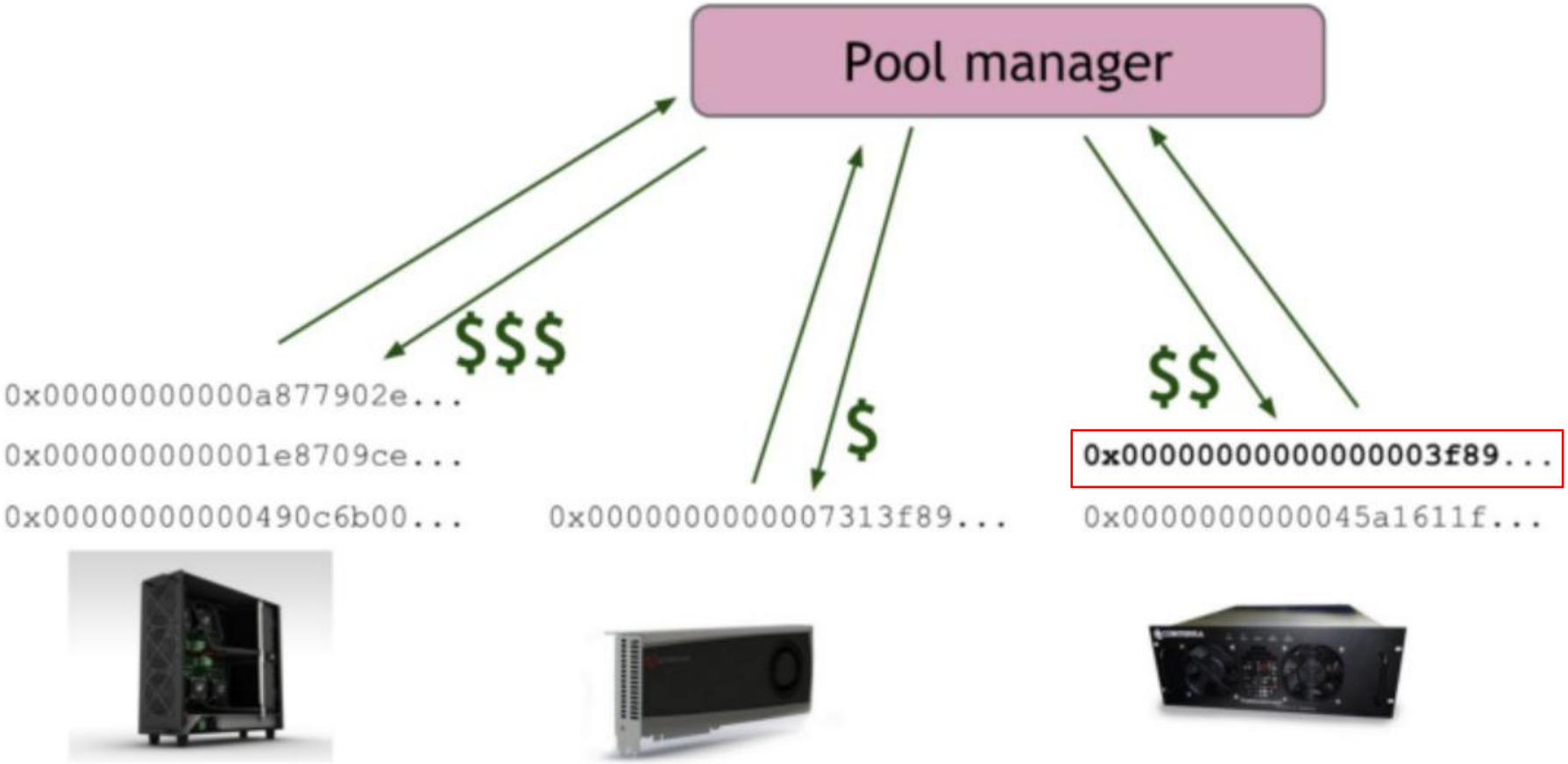
00000000000000000000000000000000……

m位

$(D' < D,\ m < n)$

矿工提交符合（2）的 PPoW 以核算其贡献比例。

区块截留攻击

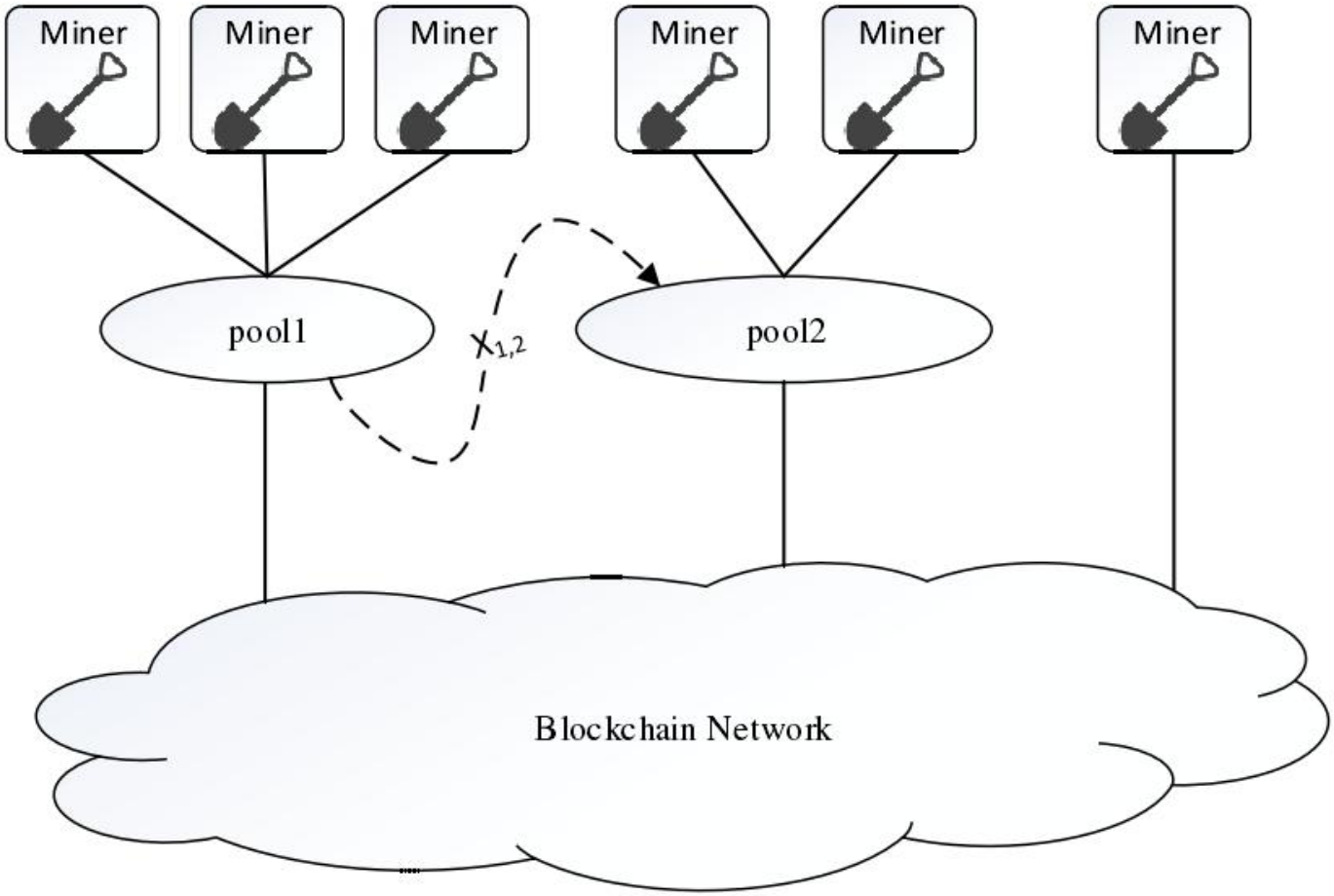

Pool manager
$$$
$
$$
0x00000000000a877902e...
0x000000000001e8709ce...
0x0000000000490c6b00...
0x0000000000007313f89...
0x0000000000000003f89...
0x0000000000045a1611f...

区块截留攻击

- 区块截留攻击（ Block Withholding Attack）
  - 攻击者只发送 **PPoW** 给矿池管理员， 当发现完整PoW时就将其抛弃。
  - 其他人找到完整答案时，攻击者会收到一定份额的奖励，但他并未对该矿池提供任何实质贡献。

区块截留攻击

- Block Withholding Attack（区块截留攻击）



区块截留攻击

- 假设系统中有两个矿池，其算力分布如下：

	矿池A	矿池B	other	total
算力占比	30%	30%	40%	100%
挖矿奖励	0.3	0.3	0.4	1

- 矿池A分配10%的算力加入矿池B（卧底）
- 该部分算力进入矿池B实行区块截留攻击

区块截留攻击

- 矿池A分配10%的算力加入矿池B，系统目前算力分布如下：

	矿池A	矿池B	other	total
原算力占比	30%	30%	40%	100%
名义算力占比	20%	40%	40%	100%
实际算力占比	20%	30%	40%	90%

10%

矿池A收益情况：

$$\frac{20\%}{90\%} + \frac{10}{40} \times \frac{30\%}{90\%} = 0.30555 > 0.3$$

A矿池挖矿　B矿池分配

获得高于诚实挖矿的奖励

区块截留攻击

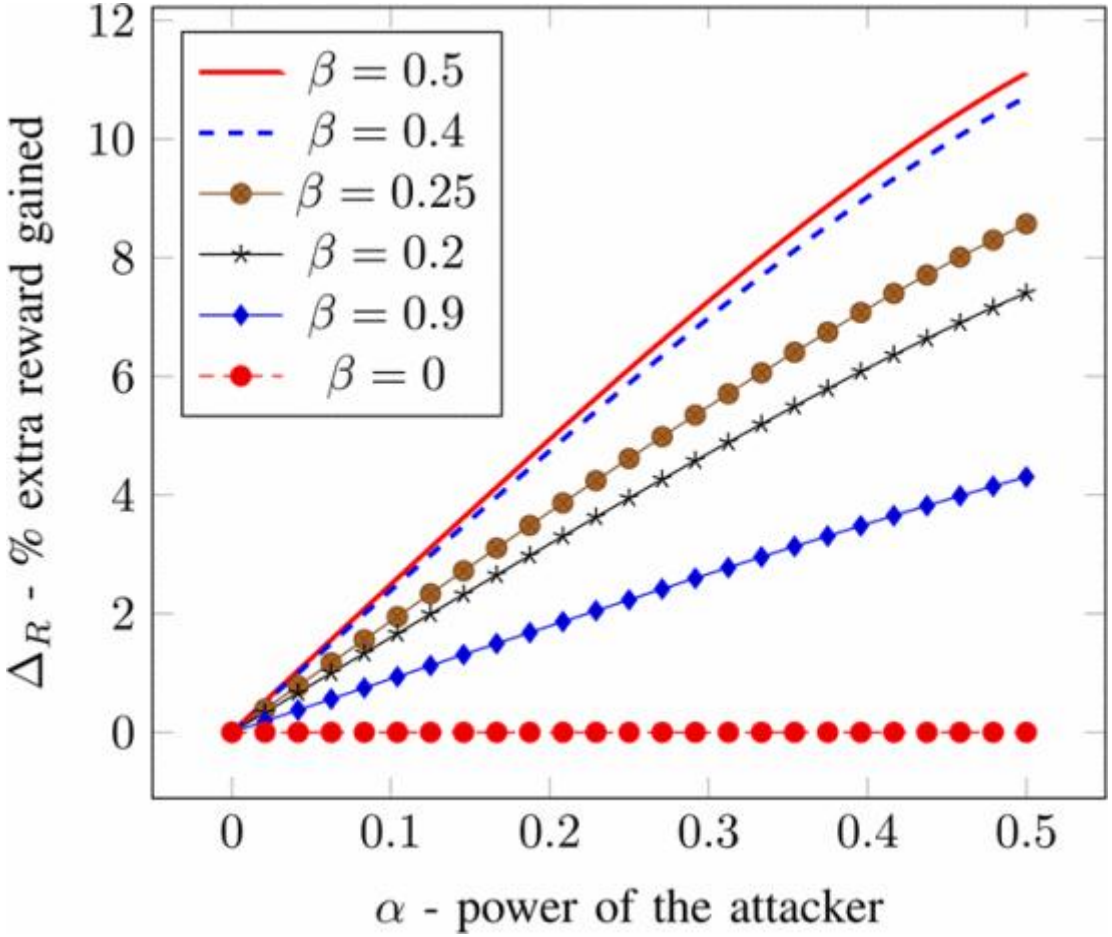


Fig : The attacker's extra reward (ΔR) in the scenario where the whole network is considered as one public pool.

Luu L, Saha R, Parameshwaran I, et al. On power splitting games in distributed computation: The case of bitcoin pooled mining[C]//2015 IEEE 28th Computer Security Foundations Symposium. IEEE, 2015: 397-411.

区块截留攻击

矿池A收益情况：

思考：

$$\frac{20\%}{90\%} + \frac{10}{40} \times \frac{30\%}{90\%} = 0.30555 > 0.3$$

1. **出块奖励是一定的，那么矿池A的额外收益是从哪获取的？谁会遭受损失？还有谁会受益？**
   - 根据计算可知，矿池A会获得额外收益；遭受攻击的矿池B会受到一定损失。
2. **各大矿池间是否有发生区块截留攻击？**
   - 2014年的时候发生过一定规模的区块截留攻击，Eligius矿池因此损失了约300BTC。
   - 若矿池同时互相发动攻击，双方收益都会下降。为了避免收益下降，矿池间就形成了“互不侵犯”的默契。所以目前没有大规模发生攻击。

以太坊空账户 DoS 攻击

以太坊在 2016 年 9 月和 10 月遭受一连串的 DoS 攻击：

- 攻击者在以太坊网络内以非常低的成本创建了1900万个空账户
- 空帐户会浪费硬盘空间，增加同步时间并减慢处理时间

- 为了解决该问题，以太坊进行了一次硬分叉。

以太坊空账户DoS攻击

以太坊中，执行智能合约花费 = 消耗的Gas数量（gas value）× Gas的价格（gas price）

Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.

（节选自以太坊黄皮书）

以太坊空账户DoS攻击

智能合约“自毁函数”：

selfdestruct(address)

作用：将合约销毁，并将余额转到一个指定账户 （若指定账户不存在，会创建一个新的空账户）

- 为了鼓励人们主动对不再使用的智能合约进行销毁，该函数的gas value 为 0
- 攻击者利用该特点，恶意多次调用该函数，最终生成了1900万个空账户。
  - 浪费存储空间
  - 增加同步时间
  - 减慢了事务处理速度

以太坊空账户DoS攻击：Hard Forks

Ethereum Hard Forks

Name	On Roadmap	Date	Block
Frontier	Yes	2015年7月31日 01:26:28	1
Frontier Thawing	Yes	2015年9月8日 07:33:09	200000
Homestead	Yes	2016年3月15日 03:49:53	1150000
DAO Fork	No	2016年7月20日 23:20:40	1920000
EIP-150 Hard Fork	No	2016年10月18日 23:19:31	2463000
Spurious Dragon	No	2016年11月23日 01:15:44	2675000
Byzantium	Yes	2017年10月16日 15:22:11	4370000

关于Hard Fork 的争议

DDoS Attacks in Bitcoin Mining Pools

How to DDoS attack:

- 矿池 manager 作为攻击作恶者, 向 victim pool 提交大量假的 solution

影响:

- Hash power of victim-pool is weakened due to such DDoS attacks
- 矿工可能会离开victim矿池，并加入到 attacking 矿池

Wu S, Chen Y, Li M, et al. Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools[J]. IEEE/ACM Transactions on Networking, 2020, 28(2): 874-887.

DDoS Attacks in Bitcoin Mining Pools

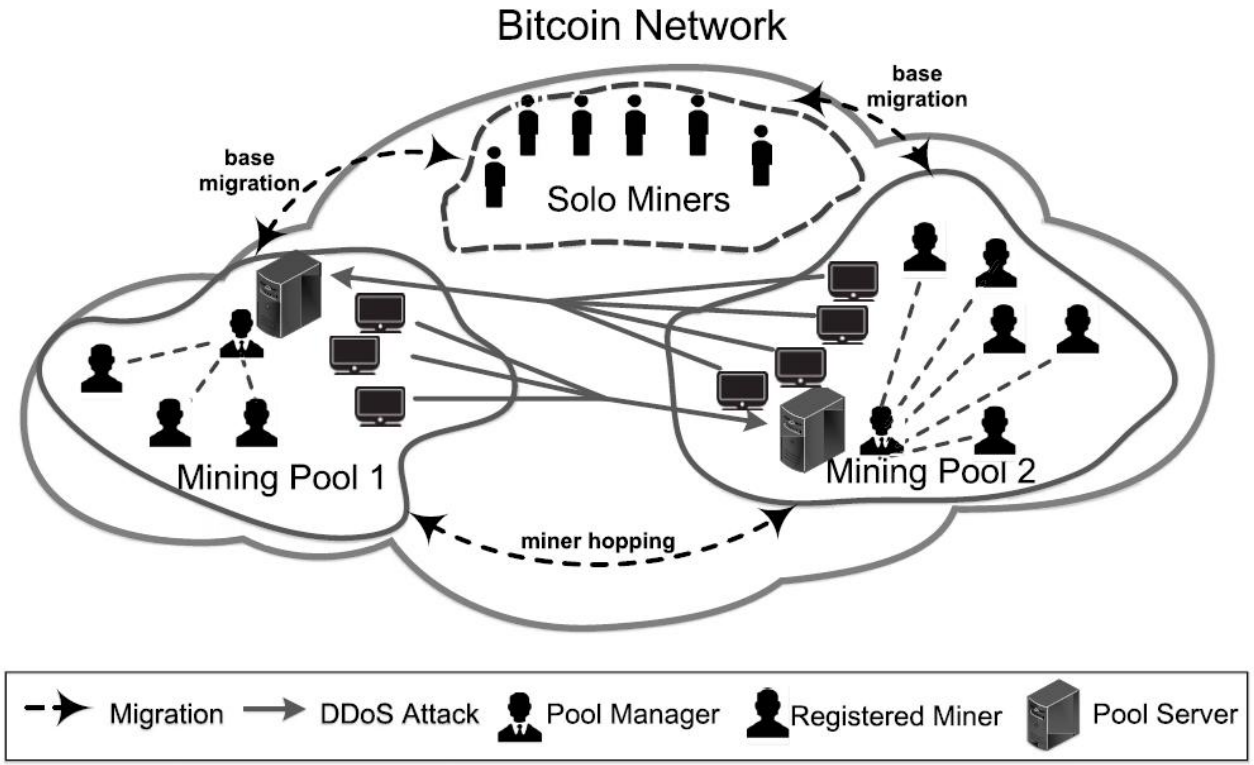


Fig. 1. The bitcoin system with 14 miners and 2 mining pools led by 2 pool managers. Pool 1 and Pool 2 have 3 and 5 registered miners each. 6 solo miners are in the rest of the bitcoin network.

Wu S, Chen Y, Li M, et al. Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools[J]. IEEE/ACM Transactions on Networking, 2020, 28(2): 874-887.

DDoS Attacks in Bitcoin Mining Pools

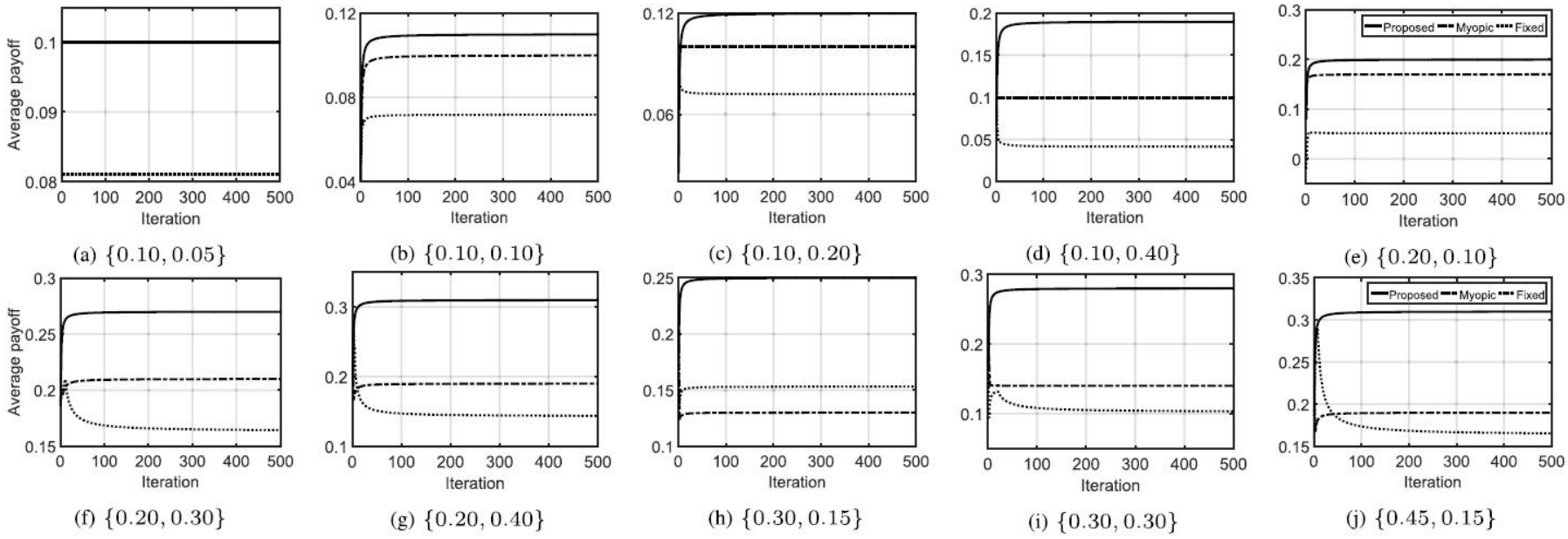


Fig. 4. Accumulated average payoffs of different strategies under different initial states.

- 当M1 算力< M2 算力时，M1 收益比其公平情况下的 fair share 高。
- M2矿池算力越大，对M1的收益反而越有利
- 当M1的算力 更大时，收益 <= 公平情况下的 fair share (因为M2可以对M1发动DDoS攻击了
  - 和baseline相比，可以降低其损失 。

结论：

- 矿池越大越容易遭到 DDoS 攻击。

Wu S, Chen Y, Li M, et al. Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools[J]. IEEE/ACM Transactions on Networking, 2020, 28(2): 874-887.

谢谢！