A Self-Healing Mechanism for Internet of Things

物联网设备自愈机制

2001210186 毕廷竹

Blockchain Access Privacy: Challenges and Directions

报告人：刘鑫

2020年11月18日

密码学的拯救？

- 区块链的核心是大规模分布和可公开访问的数据库，应用广泛，但容易泄露隐私
- 研究者们提出改进，但都依赖外部匿名网络，如Tor网络
- 本文主要关注
  - 匿名发布交易
  - 私下获取交易

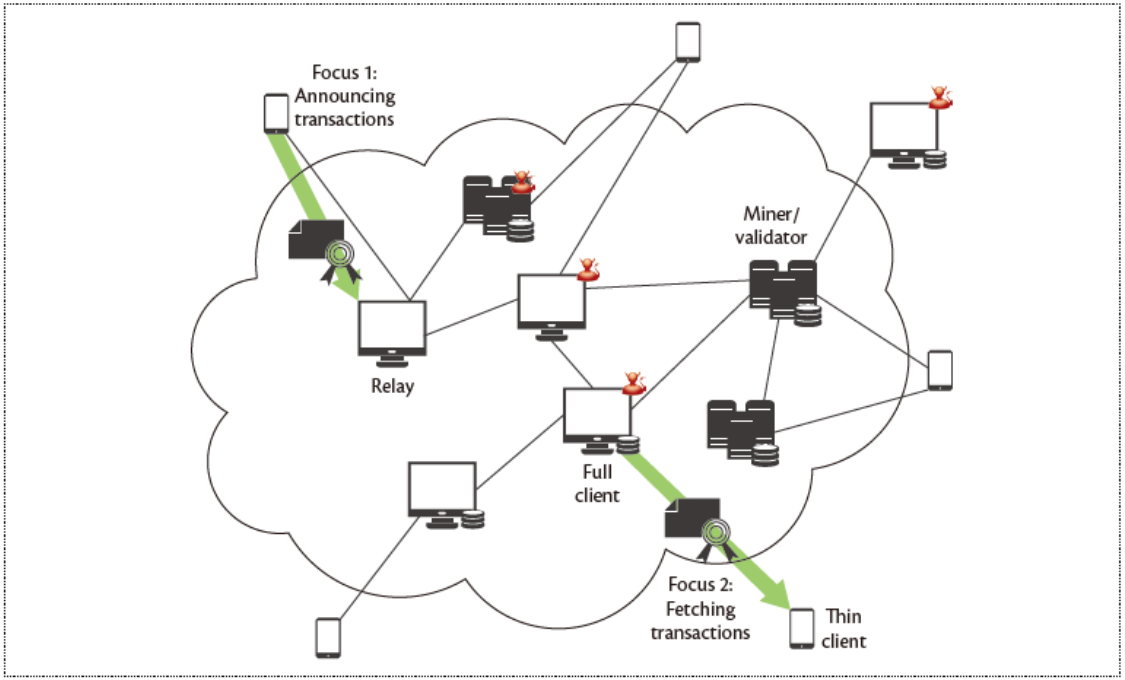


Figure 1. Topology of a typical blockchain system. The two bold arrows (highlighted in green) illustrate sensitive information flows that must be protected to prevent attackers from leveraging network-level information to compromise the privacy of blockchain users.

匿名发布交易

- 利用现有的覆盖网络结构实现，将用户网络级信息与其交易分离，而不是依赖Tor之类的外部服务

- 共识机制
  - 无许可
    - 比特币和以太坊底层
  - 有许可
    - Hyperledger底层

私下发布交易

- 使用加密技术避免集中化和可信赖的中间人，并确保抵制历史数据“篡改”
- 简化付款验证SPV
- 瘦客户端查询缺乏隐私性、匿名性
- 私有信息检索PIR

Thanks

- An Analogue
- General Architecture
- Remediation Process
- Evolutionary Process

IoT

Malfunction/Cyberattack

An Analogue

You feel sick

An Analogue

You feel sick

Physical examination

An Analogue

You feel sick

Physical examination

Get treatment

General Architecture

Host-Based Intrusion Detection System

Health-Monitoring Module

Auto-Remediation

General Architecture

Host-Based Intrusion Detection System

Health-Monitoring Module

Auto-Remediation

Remediation Process

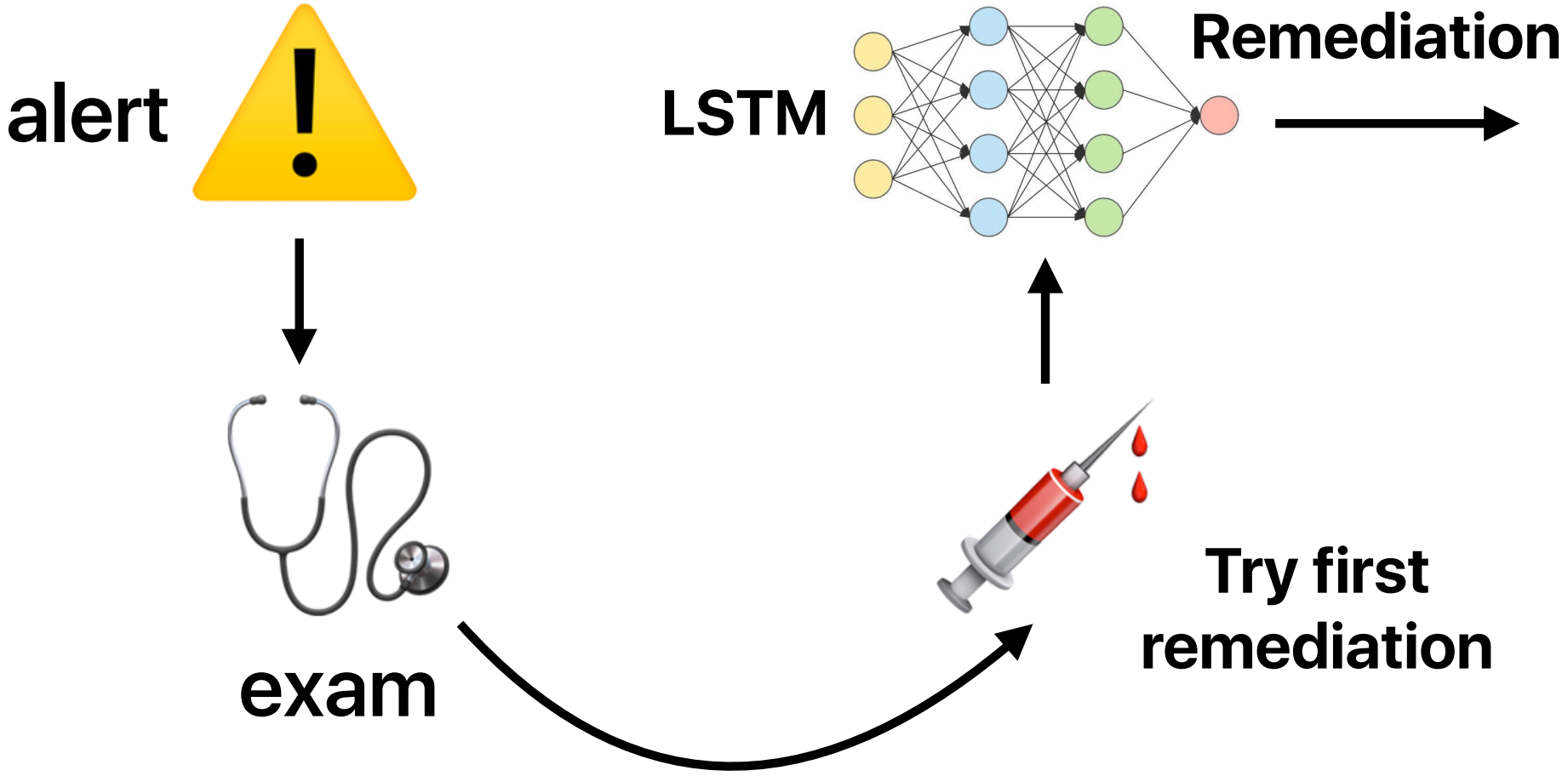
alert 

Remediation Process

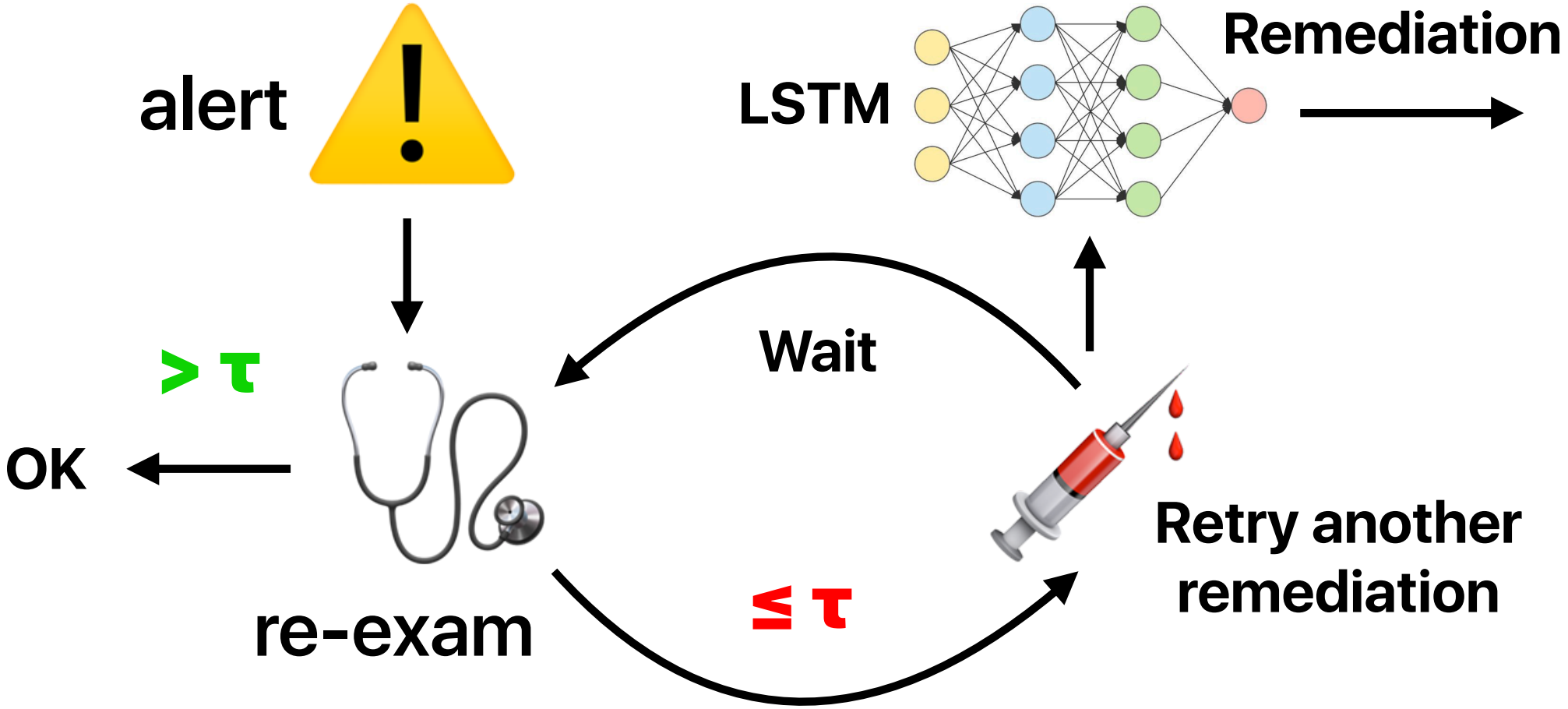
alert

exam

Remediation Process



Remediation Process

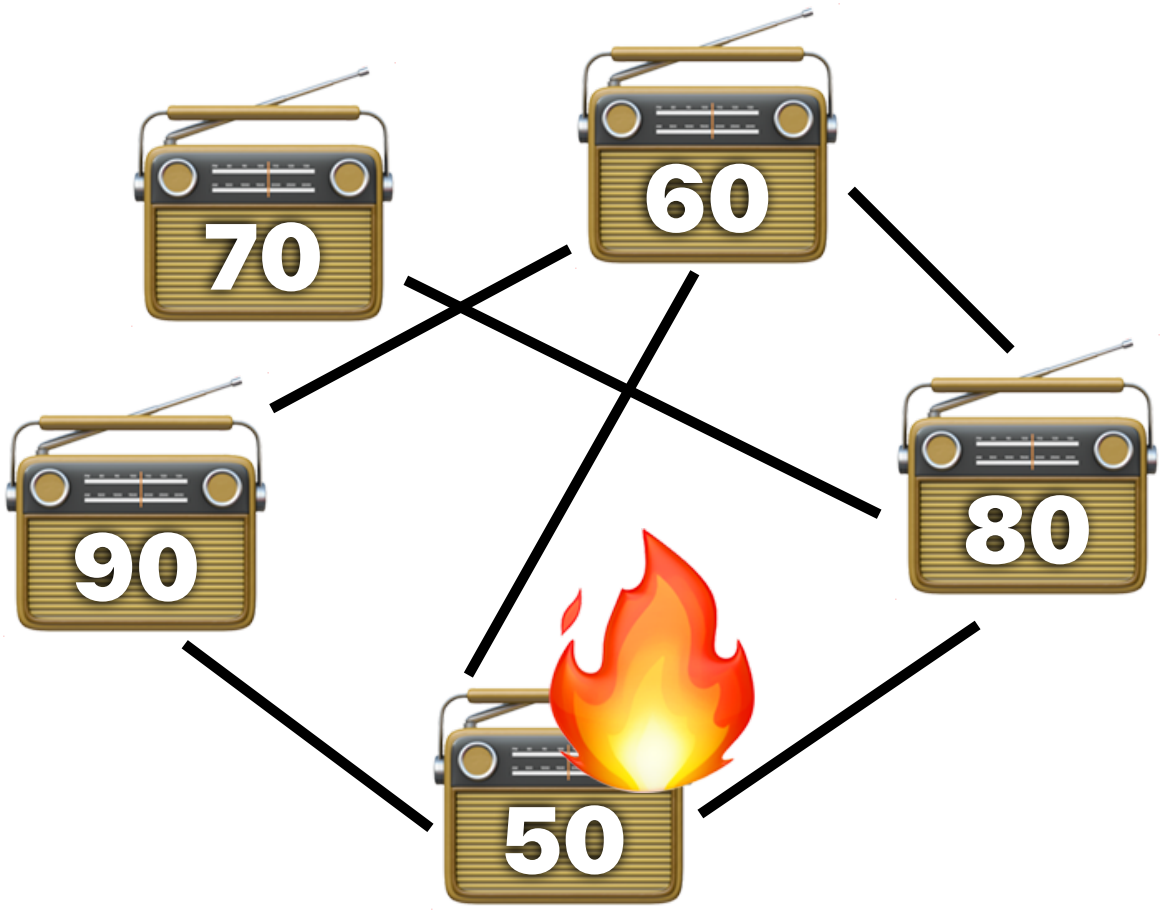


Remediation: Result

3.66

Attack	Trial 1	Trial 2	Trial 3	Average
DoS attack (CPU)	3	3	4	3.66
DoS attack (memory)	3	5	6	4.66
DoS attack (processes)	4	2	3	3
DoS attack (files)	5	7	7	6.33
DDoS (1)	5	6	7	6
DDoS (2)	7	5	5	5.66

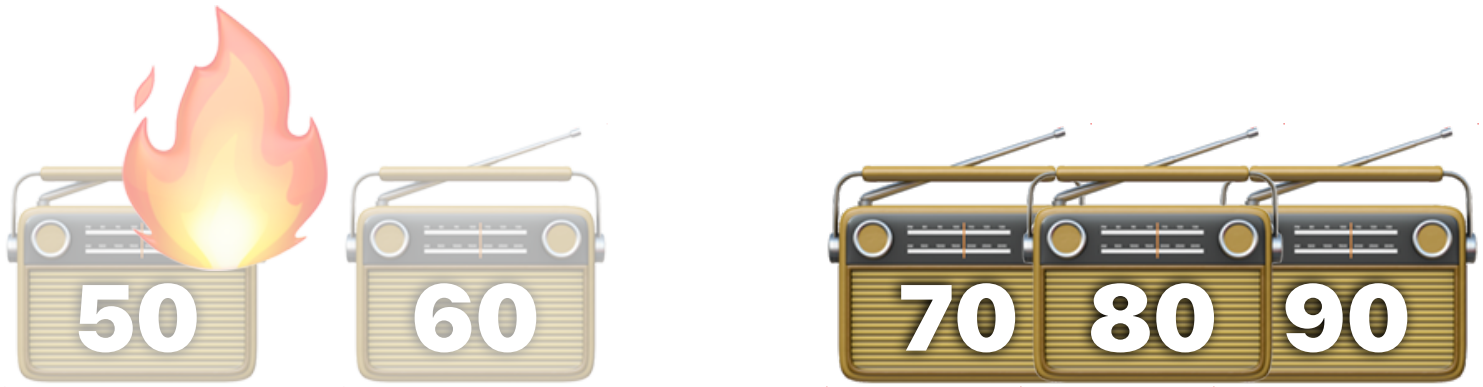
Evolutionary Process



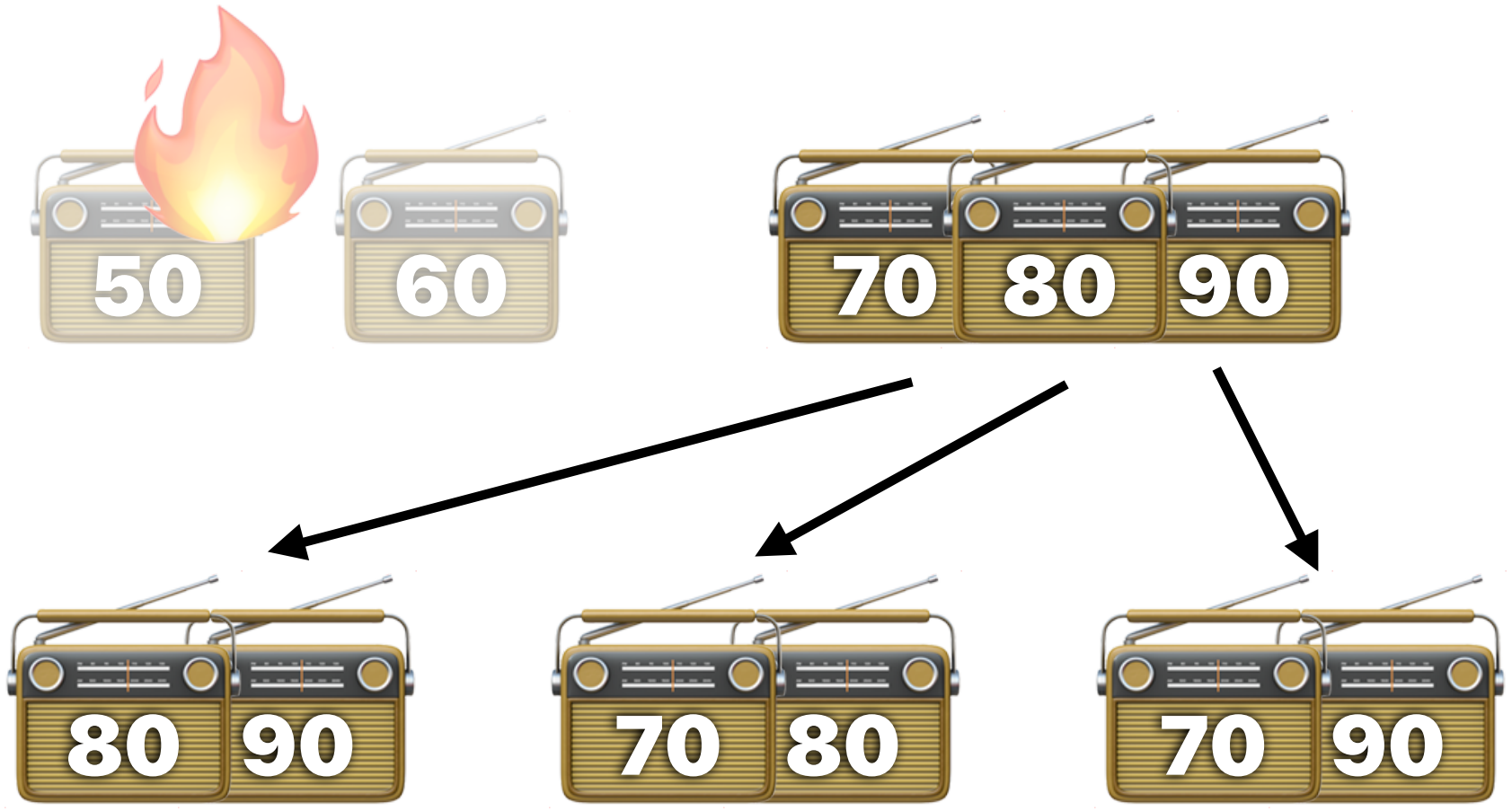
Evolutionary Process

Evolutionary: Selection

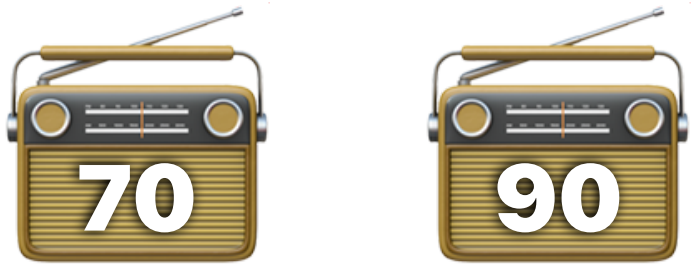
Evolutionary: Selection



Evolutionary: Selection

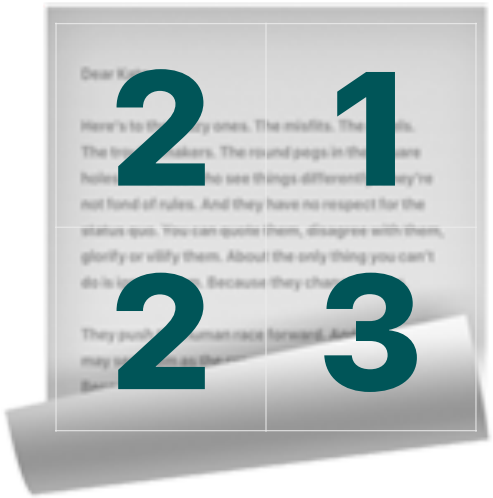


Evolutionary: Selection

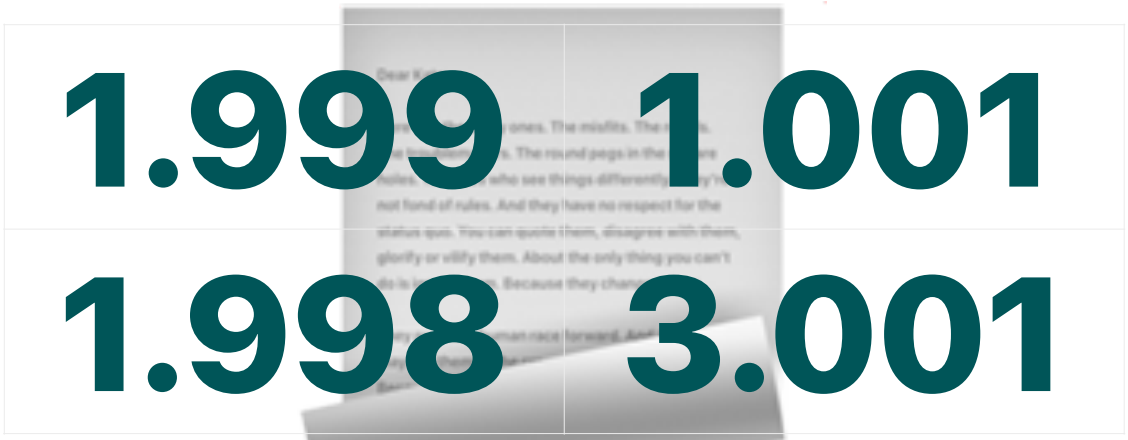


Evolutionary: Crossover

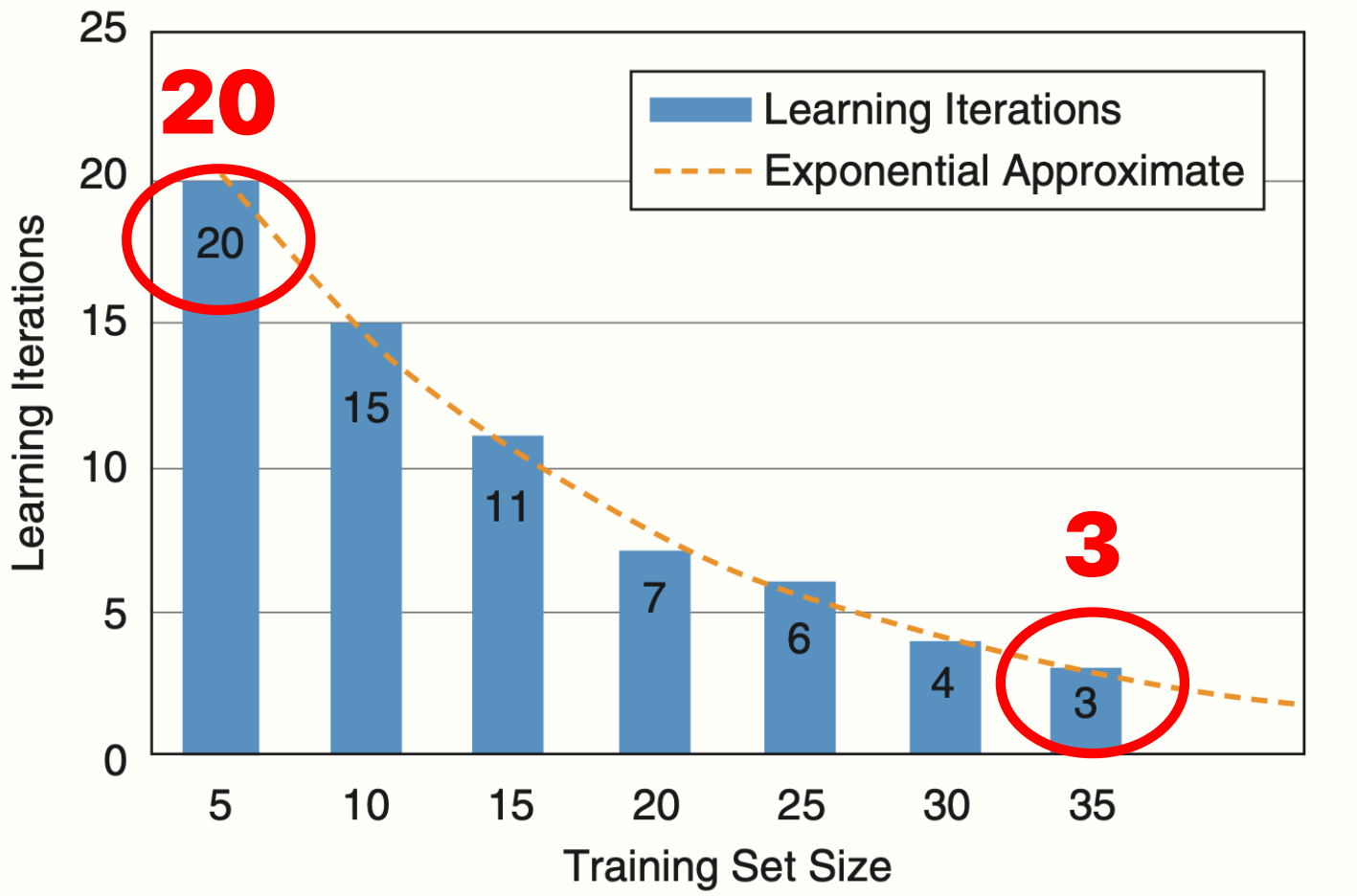
Evolutionary: Crossover



Evolutionary: Mutation



Evolutionary: Result



A Self-Healing Mechanism for Internet of Things

物联网设备自愈机制

谢谢！

Blockchain Access Privacy: Challenges and Directions

报告人：刘鑫

2020年11月18日

密码学的拯救？

- 区块链的核心是大规模分布和可公开访问的数据库，应用广泛，但容易泄露隐私
- 研究者们提出改进，但都依赖外部匿名网络，如Tor网络
- 本文主要关注
  - 匿名发布交易
  - 私下获取交易

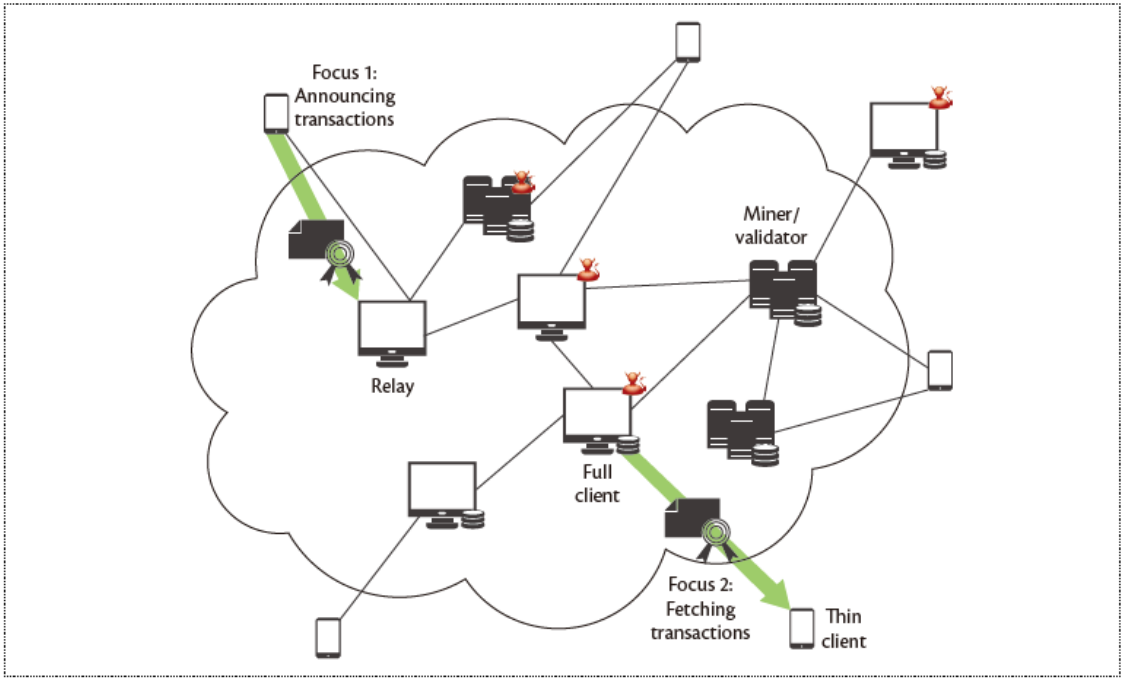


Figure 1. Topology of a typical blockchain system. The two bold arrows (highlighted in green) illustrate sensitive information flows that must be protected to prevent attackers from leveraging network-level information to compromise the privacy of blockchain users.

匿名发布交易

- 利用现有的覆盖网络结构实现，将用户网络级信息与其交易分离，而不是依赖Tor之类的外部服务

- 共识机制
  - 无许可
    - 比特币和以太坊底层
  - 有许可
    - Hyperledger底层

私下发布交易

- 使用加密技术避免集中化和可信赖的中间人，并确保抵制历史数据“篡改”
- 简化付款验证SPV
- 瘦客户端查询缺乏隐私性、匿名性
- 私有信息检索PIR

Thanks

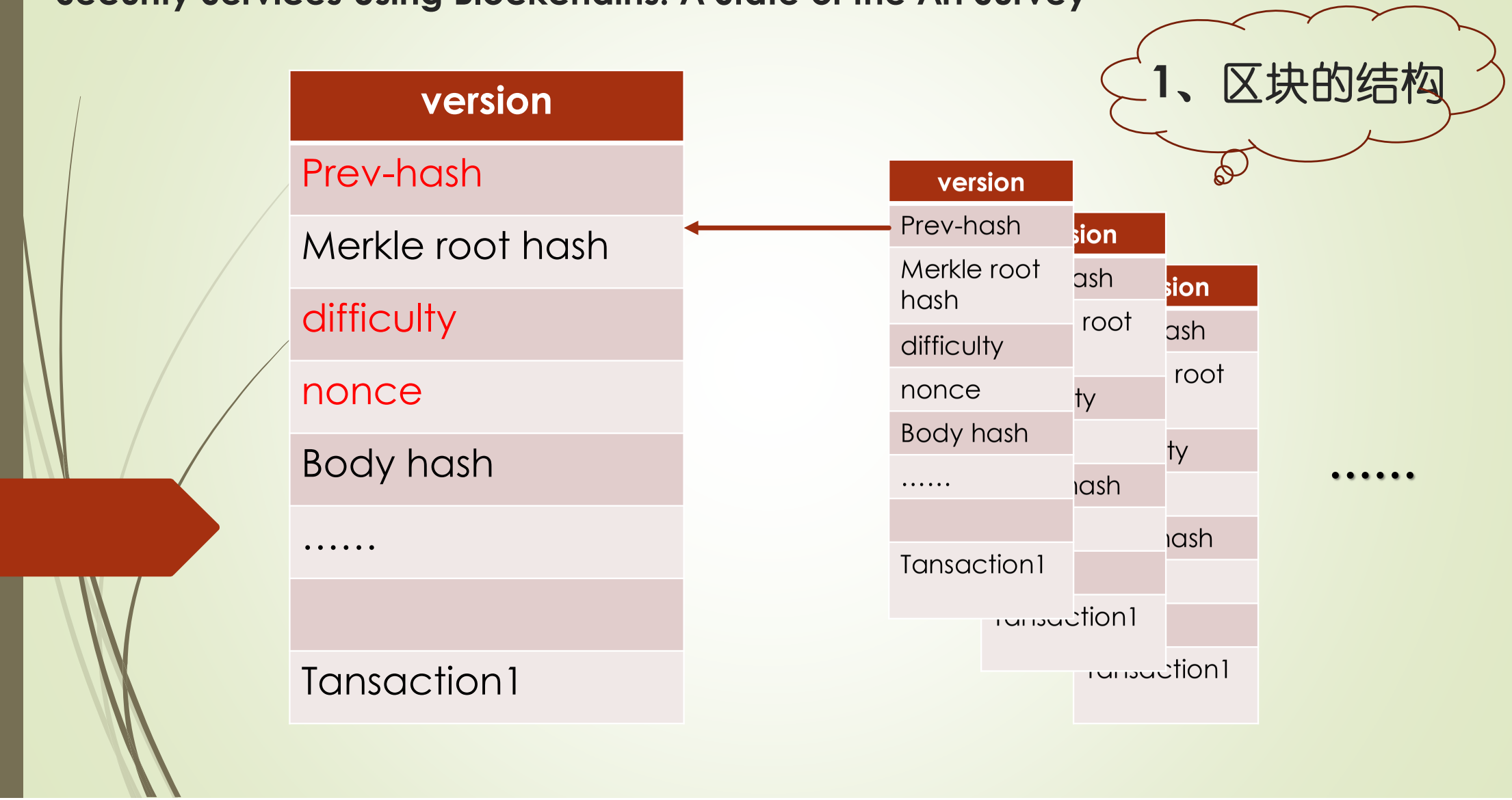
Security Services Using Blockchains: A State of the Art Survey

1、区块结构

2、共识算法

3、主要应用

报告人：谭诗意
时间：2020年11月18号


1、区块的结构
version
Prev-hash
Merkle root hash
difficulty
nonce
Body hash
……
Tansaction1
version
Prev-hash
Merkle root hash
difficulty
nonce
Body hash
……
Tansaction1
……

2、典型共识算法

共识算法	概述
pow	解数学题，难于求解，易于验证；浪费算力
pos	按钱分配，有钱者更有钱，可能导致集中化
PoSpace	类似POW，不过依靠的存储能力
POI	依据节点的交易金额和余额来计算重要性
最小块哈希	选择网络中生成哈希值更小的区块，完全随机
PBFT	选举leader，leader来验证打包，新区块需要2/3以上通过

3、加密认证服务

核心：非对称加密

栗子：公钥管理基础设施（PKI）——如何管理密钥？

CA集中管理

- 可信度
- 单点故障
- 成本

WOT分散管理

- 事先建立信任
- 门槛增大

区块链管理

- 分布式
- 无需信任

Security Services Using Blockchains: A State of the Art Survey

谢谢大家！

报告人：谭诗意
时间：2020年11月18号

A First Look at Identity Management Schemes on the Blockchain

姓名：王云璇

学号：2001210674

背景

身份管理系统的发展

- 公钥密码技术
- 层级证书认证
- 一次性身份验证
- 将DLT应用于IdM
  - 优势：分布式、防篡改、包容性、用户控制

区块链上的身份管理系统

自我主权身份

(Self-sovereign identity)

e.g. Sovrin, uPort, OneName …

分散信任身份

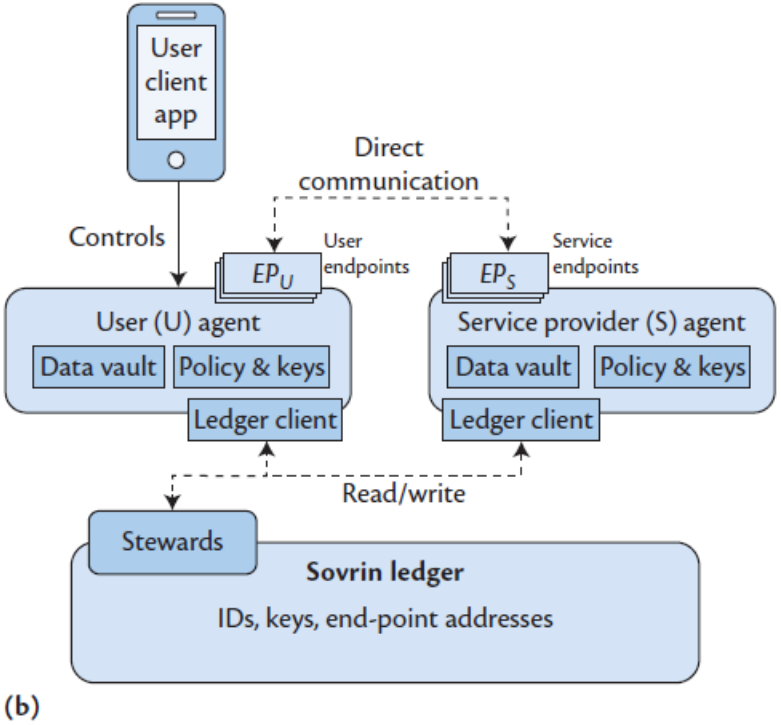
(Decentralized trusted identity)

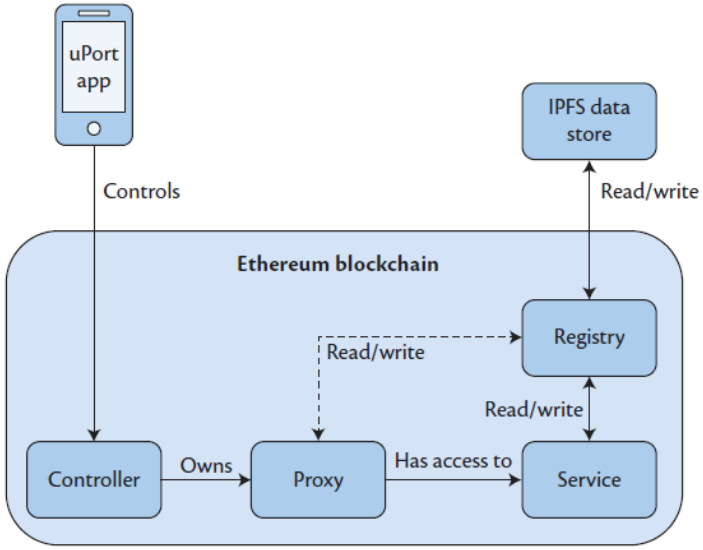
e.g. ShoCard, BitID, ID.me, IDchainZ …

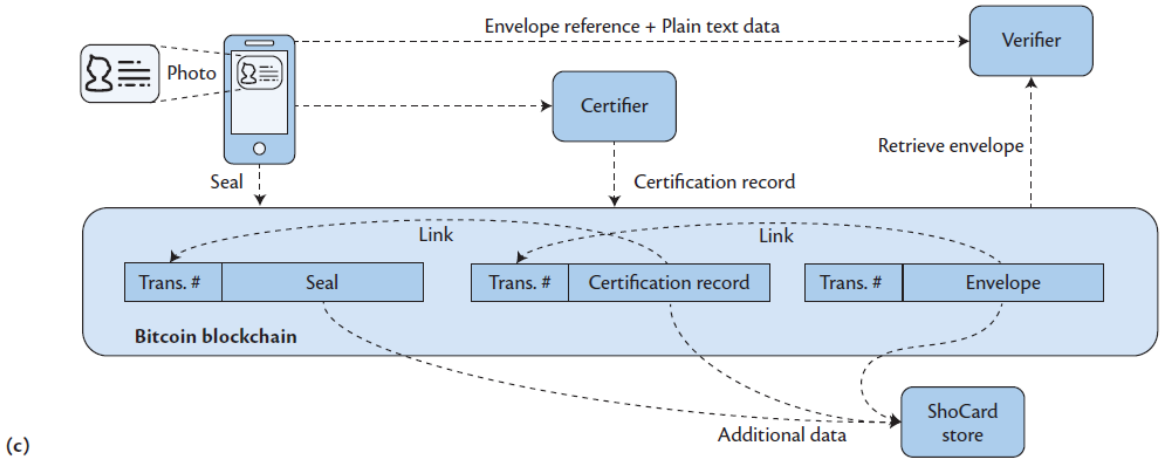
身份法则评估框架

1. 用户控制和同意(User control and consent)
2. 限制使用的最少披露(Minimal disclosure for a constrained use)
3. 有正当理由的各方(Justifiable parties)
4. 定向身份(Directed identity)
5. 为运营商和技术的多元化而设计(Design for a pluralism of operators and technology)
6. 人工集成(Human integration)
7. 跨上下文的一致体验(Consistent experience across contexts)

设计思路


User client app
Controls
Direct communication
User endpoints
Service endpoints
EP_U
EP_S
User (U) agent
Data vault
Policy & keys
Ledger client
Service provider (S) agent
Data vault
Policy & keys
Ledger client
Read/write
Stewards
Sovrin ledger
IDs, keys, end-point addresses
(b)


uPort app
Controls
IPFS data store
Read/write
Ethereum blockchain
Registry
Read/write
Read/write
Controller
Owns
Proxy
Has access to
Service
(a)


Envelope reference + Plain text data
Verifier
Photo
Certifier
Retrieve envelope
Seal
Certification record
Link
Link
Trans. #
Seal
Trans. #
Certification record
Trans. #
Envelope
Bitcoin blockchain
ShoCard store
Additional data
(c)

设计方案评估比较

规则	uPort	ShoCard	Sorvin	Facebook Connect
规则一 用户控制和同意	No	Yes	Yes	Yes
规则二 限制使用的最少披露	Yes	No	Yes	Yes
规则三 有正当理由的各方	No	No	Yes	No
规则四 定向身份	Yes	Yes	Yes	Yes
规则五 设计的多元化	Yes	No	Yes	No
规则六 人工集成	No	No	No	No
规则七 跨上下文的一致体验	Yes	Yes	No	Yes

总结

- 分布式分类帐技术并不是身份管理的灵丹妙药。这个新兴研究领域的未来工作面临两个特别的障碍。
- 首先，可用性是一个尤为紧迫的未知因素，因为似乎有一个广泛的假设，即用户有能力进行有效的密码密钥管理，并且会直观地理解在DLT中引用身份属性的含义。
- 其次，用于存储和处理个人数据的法规环境越来越严格。这给设计以身份为中心的不可变分类帐带来了挑战，该分类帐参考个人数据并为其存储的数据提供固有的透明性。

Thanks