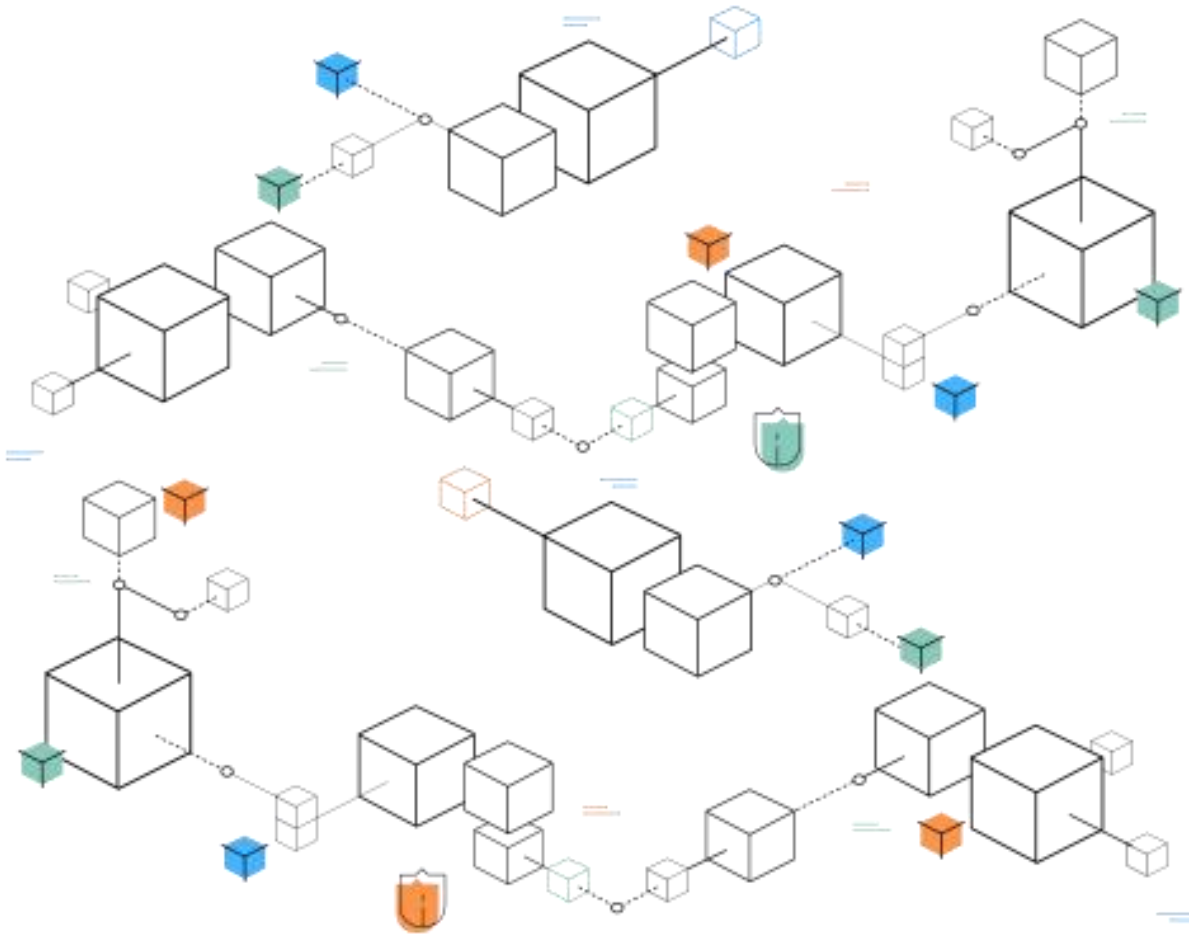
基于密接技术的区块链开发

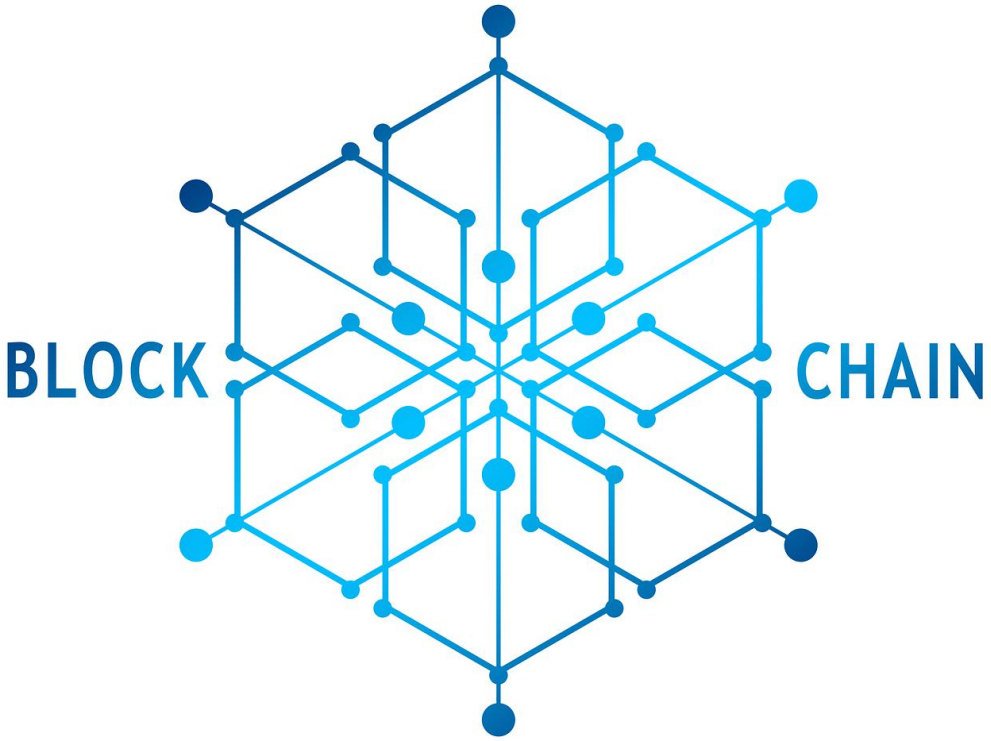
创新实验　第一次项目展示

小组成员：庄湛　潘泰仰　邹若彤

指导老师：宋轩老师　张浩然老师(东京大学)
云沐晟学长(RA)　林贵旭学长(RA)

2020/10/29　创园10栋504





Contents

研究背景和文献回顾

- 什么是区块链?
- 为什么要用区块链?
- 现有的区块链有什么问题?

研究背景和文献回顾

区块链实际上是一种**分布式账本**的技术，即一个由许多网络节点共同参与和维护的数据库，主要是基于P2P网络的技术。

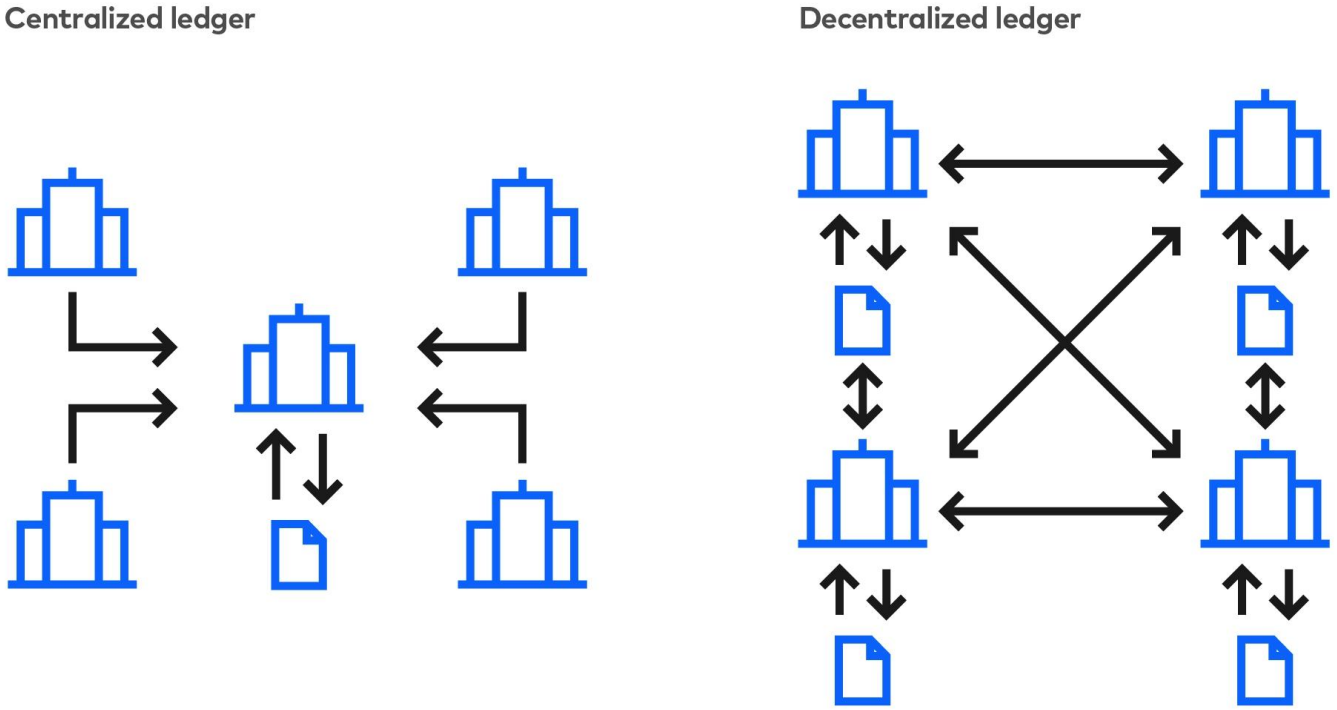


图 1 中心化账本和去中心化账本对比[2]

安全性

公证人，律师，银行，监管合规官，政府

稳定性

信用

所有诚实的记账人

[2] “How blockchain will disrupt your industry”, https://www.slalom.com/insights/how-blockchain-will-disrupt-your-industry[Online]

研究背景和文献回顾

区块链的流程和特性

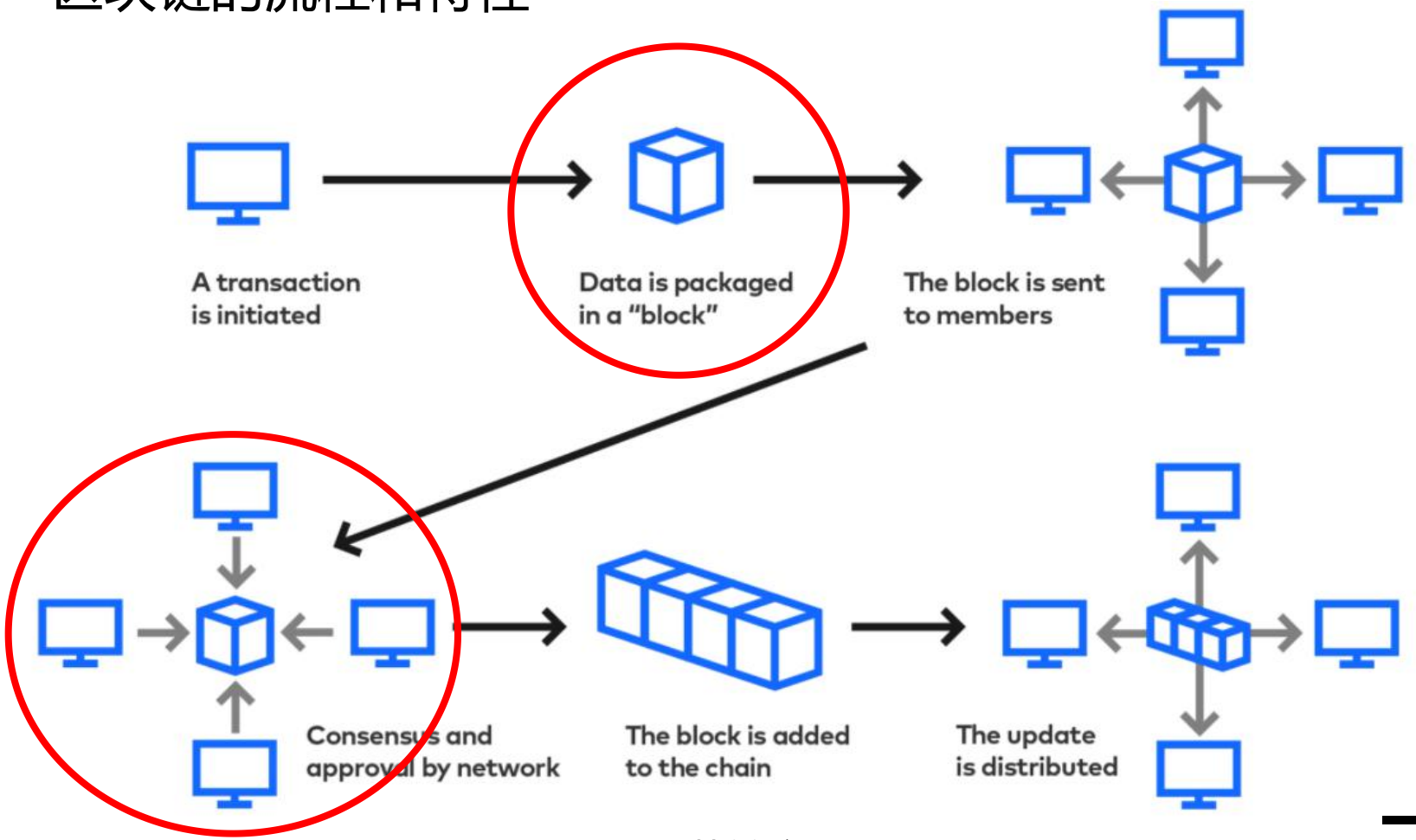


图 2 区块链流程[2]

- ✓ 去中心化
- ✓ 开放性
- ✓ 不可篡改
- ✓ 可追溯性
- ✓ 匿名性
- ✓ 民主性

一人一票 ➡ **共识机制**

[2] “How blockchain will disrupt your industry”, https://www.slalom.com/insights/how-blockchain-will-disrupt-your-industry[Online]

研究背景和文献回顾

工作量证明机制(POW)	股权证明机制(POS)	委任权益证明(DPOS)
BTC, ETH, LTC	**Peercoin, Algorand**	**Bitshare**
按劳分配	股权分配	民主投票
计算资源: 算力x时长	币龄: 数量x时间	生成候选代表名单
内存困难/计算困难	调整困难/加密随机	限时出块
挖矿难度自动调整	持币有利息	维护周期更新
区块奖励逐步减半	币龄清空	“代表竞选”

约束： 资产抵押，控制哈希运算难度，控制出块奖励，限制时间和频率

现阶段区块链挖矿共识机制缺点

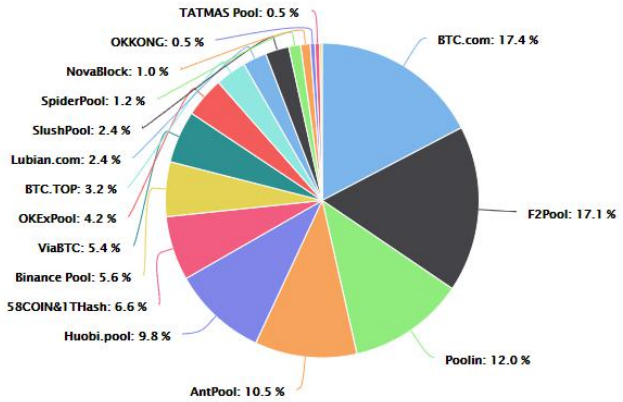


图 3 矿池分布比例[4]

- 矿机与GPU大量参与挖矿，造成**计算资源浪费**
- 部分共识机制所需计算难度大，**结算周期长**
- 算力资源集中，有**中心化趋势**，易产生分叉攻击等恶意行为
- 因计算资源、持币数量等因素导致不公平性，参与挖矿的群体较总人口较少，**缺少普及度**
- 挖矿方式与日常生活脱节，挖矿过程较为枯燥，**趣味性低**

[4] “Pool Distribution”，https://btc.com/stats/pool[Online]

系统设计

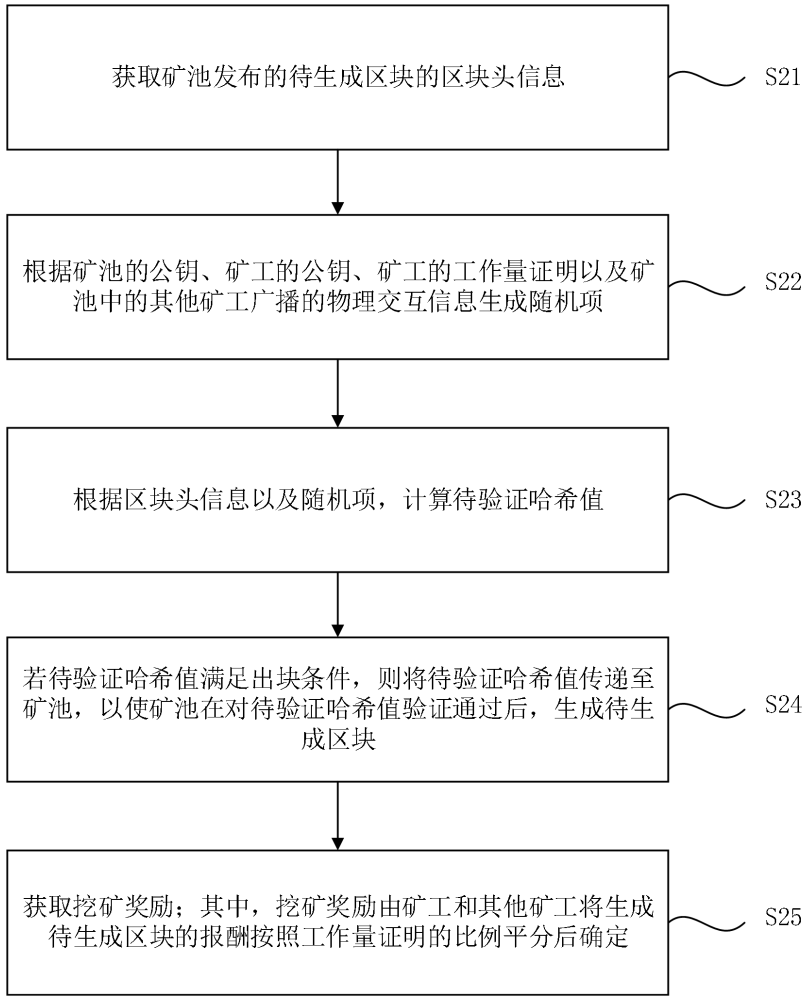


图 4 专利方案实现流程[1]

参考和改进《基于区块链的挖矿方法》专利来学习并开发

一款用于**移动设备**端，基于**物理密接交互**的新型**区块链**系统。

[1] 宋轩,张浩然. 基于区块链的挖矿方法、装置、计算机设备及 存储介质[P]. 广东省：CN111682946A, 2020-09-18.

系统设计：共识算法

POW的改进：通过**密接交互信息**产生的随机项代替计算资源高速生成的随机项进行区块链挖矿

利用密接交互信息具有**有限性**和**多重置信性**

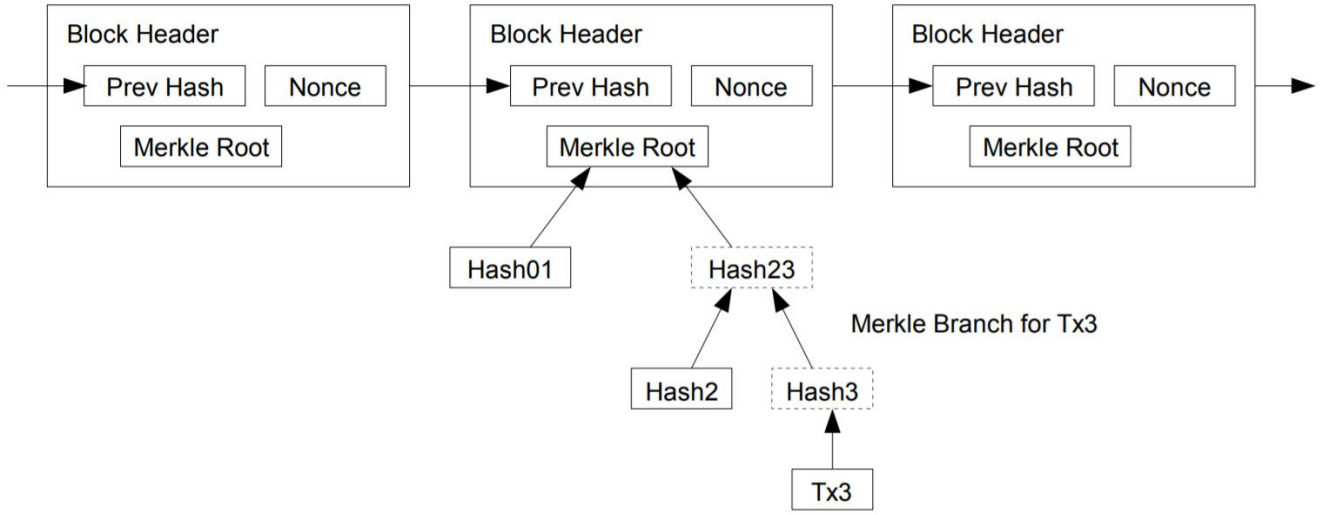


图 5 区块链结构[3]

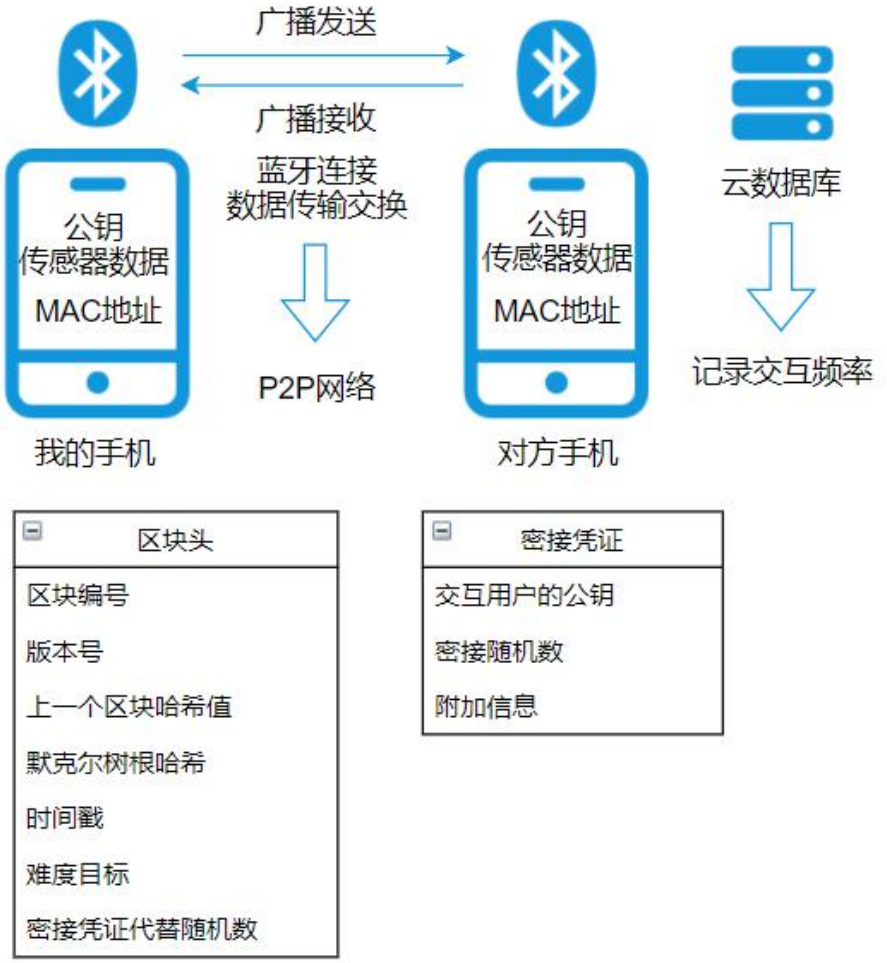


图 6 密接凭证代替方案

[3] Nakamoto S, "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf[Online], 2008

系统设计：共识算法和奖励机制

POS的改进：通过密接发生量代替货币持有量，且密接次数在中等偏上区间拥有更高几率出块(调整奖励和难度)

假设正常人密接次数呈正态分布*，利用中位数作为评价基准，利用3σ原则判别异常数据

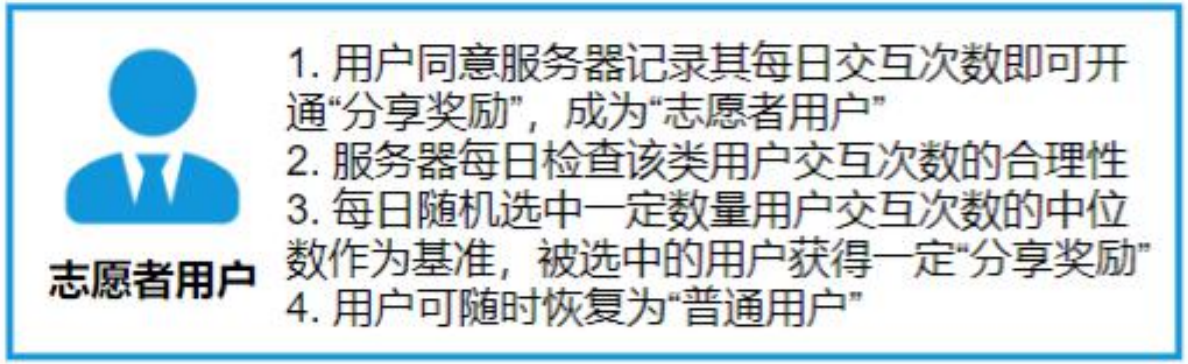


图 7 志愿者用户

出块奖励

出块奖励是用户与其他用户进行密接交互并成功解决区块链哈希难点时所获得的奖励。

打包奖励

用户在成功获得出块奖励的同时获得该奖励。根据打包的交易量可以获得一定的Mcoin奖励

分享奖励

选择一组志愿者用户作为“基准”时，当成功出块时，这组志愿者用户可以获得一定的Mcoin奖励。

* 还没有得到确切的理论根据

系统设计：安卓开发

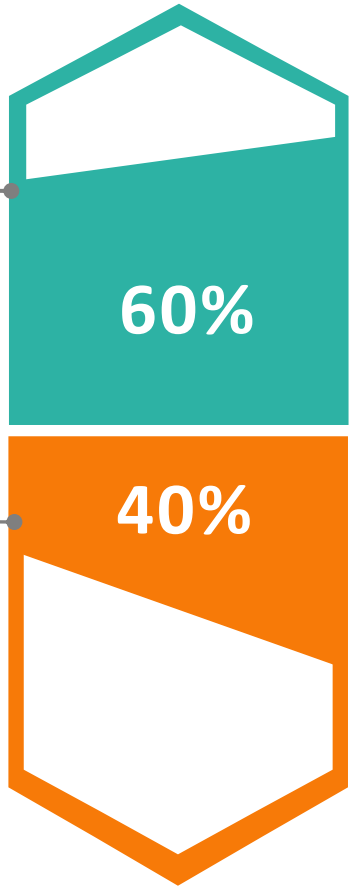
- 创建用户(公私钥对)
- 查看区块链信息
- 检测异常区块(Mcoin来源)
- 交易和查看余额
- 通过密接交互进行挖矿

客观性

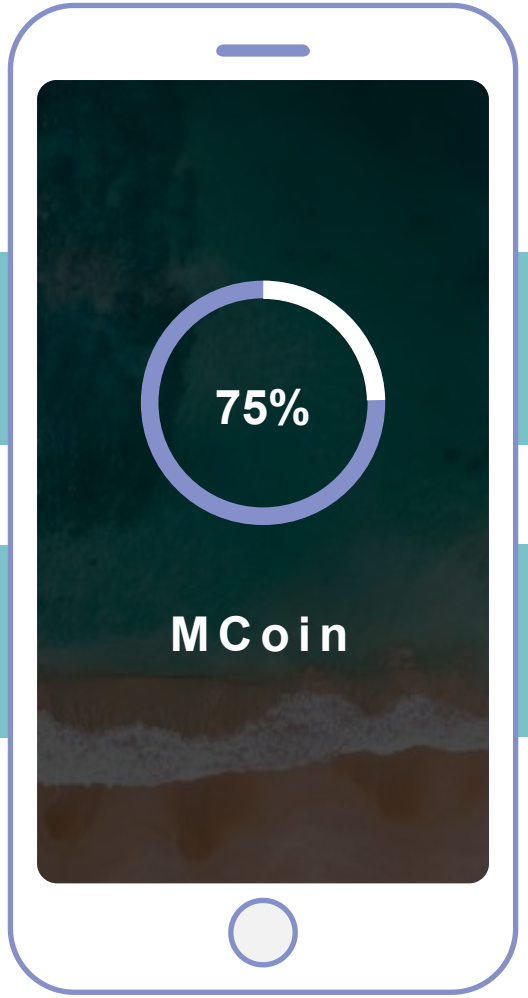
依靠软件，加密，算法等约束形成共识，通过多种奖励方式鼓励参与网络。

主观性

通过发掘社会信息，发掘主观性带来性能价值。（在这一方面可以增添民主投票）



预期产出



1. 三篇相关专利
2. 校园内小规模应用测试
3. 一款新型区块链安卓应用
4. 基于实际志愿者的测试报告

评价方法

检测可行性测试

最终应用能够自动检测出区块链上的非法交易

我们将设计十组不同的测试数据，如果该应用应准确检测出所有异常值，否则项目失败

交易可行性测试

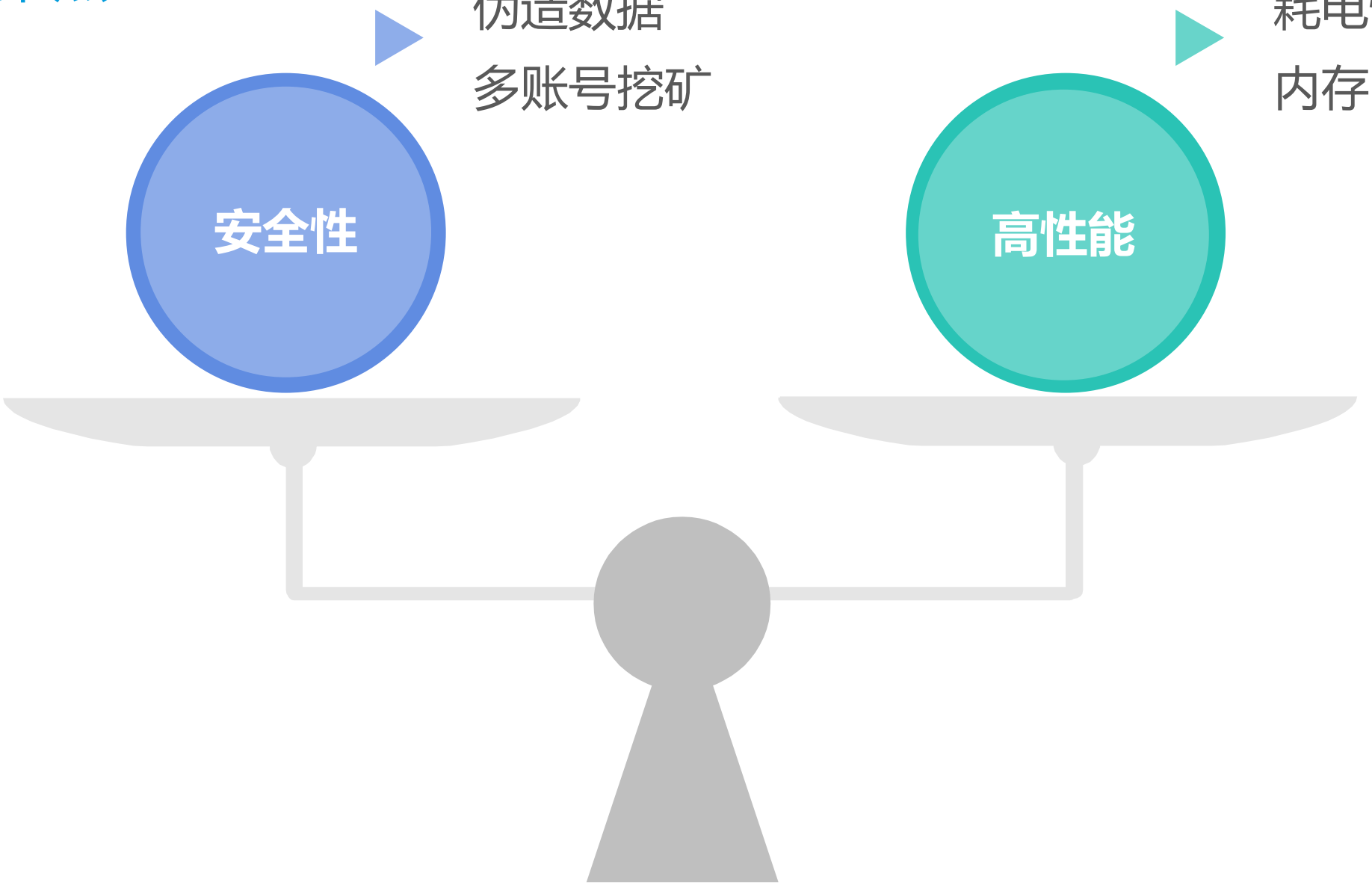
最终应用能够良好地完成转账操作并避免出现双花问题

我们将设计十组不同的测试数据，如果该应用没有实现所有交易的正常进行，则项目失败

挖矿可行性测试

最终应用使用的区块链应保持一个较为平稳的出块时间，并且出块奖励分配合理。如果在实际测试中，平均出块时间M‘，超过预期时间M的三倍或低于其三分之一，则项目失败

项目难点



项目进度

申请专利

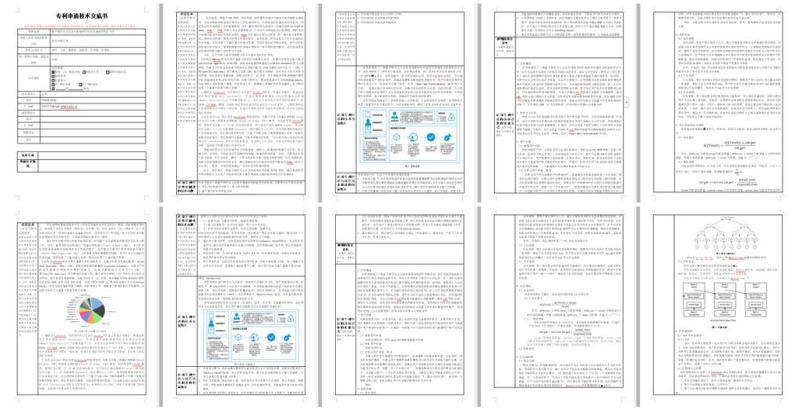


图 8 专利申请

区块生成

```
public class Block {
    private int index;
    private String timestamp;
    private int vac;
    private String hash;
    private String prevHash;
    private int difficulty;
    private String nonce;

    /** getters and setters**/
    public int getIndex() { return index; }
    public void setIndex(int index) { this.index = index; }
    public String getTimestamp() { return timestamp; }
    public void setTimestamp(String timestamp) { this.timestamp = timestamp; }
    public int getVac() { return vac; }
    public void setVac(int vac) { this.vac = vac; }
    public String getHash() { return hash; }
    public void setHash(String hash) { this.hash = hash; }
    public String getPrevHash() { return prevHash; }
    public void setPrevHash(String prevHash) { this.prevHash = prevHash; }
    public int getDifficulty() { return difficulty; }
    public void setDifficulty(int difficulty) { this.difficulty = difficulty; }
    public String getNonce() { return nonce; }
    public void setNonce(String nonce) { this.nonce = nonce; }

}
```

区块定义

```
private String calculateBlockHash() {
    String dataToHash = previousHash + timeStamp + nonce + data;
    MessageDigest digest;
    byte[] bytes = null;
    try {
        digest = MessageDigest.getInstance("SHA-256");
        bytes = digest.digest(dataToHash.getBytes(UTF_8));
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    }
    StringBuilder buffer = new StringBuilder();
    assert bytes != null;
    for (byte b : bytes) {
        buffer.append(String.format("%02x", b));
    }
    return buffer.toString();
}
```

区块哈希计算

```
void mineBlock(int prefix) {
    String prefixString = new String(new char[prefix]).replace( oldChar: '\0',  newChar: '0');
    while (!hash.substring(0, prefix).equals(prefixString)) {
        this.nonce++;
        this.hash = calculateBlockHash();
    }
}
```

挖矿算法

图 9 区块生成算法

P2P网络

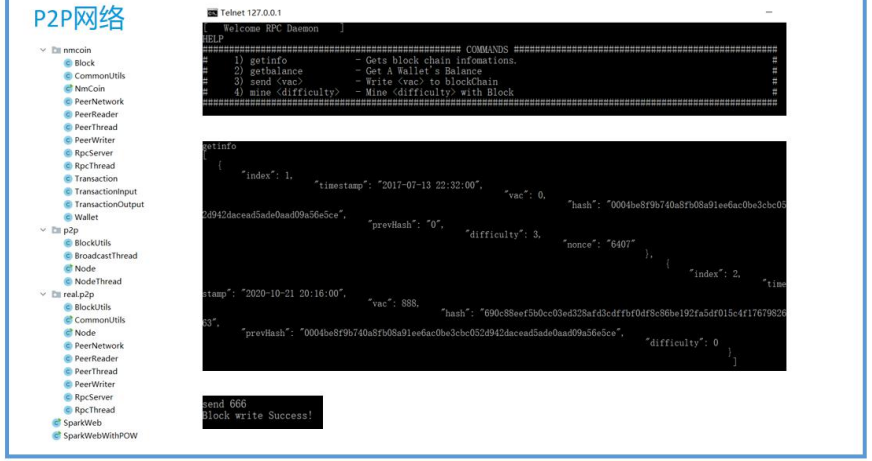


图 10 P2P网络代码

默克尔树

```
public class MerkleTree
{
    // Child trees
    private MerkleTree leftTree = null;
    private MerkleTree rightTree = null;

    // Child leaves
    private Leaf leftLeaf = null;
    private Leaf rightLeaf = null;

    // The hash value of this node
    private byte[] digest;

    // The digest algorithm
    private final MessageDigest md;
```

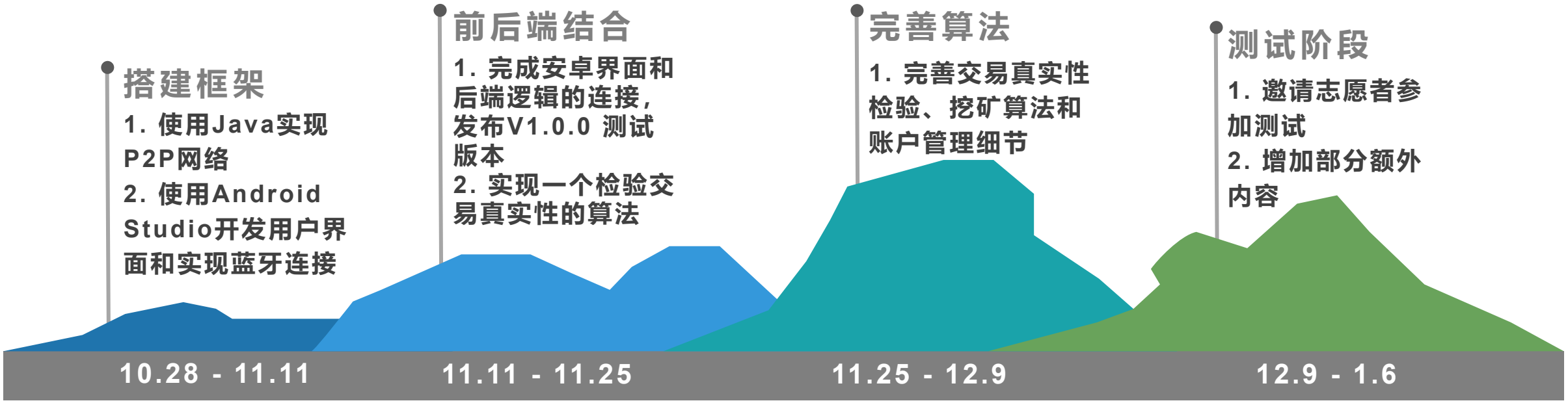
默克尔树结构

```
private byte[] digest(Leaf leaf)
{
    final List<byte[]> dataBlock = leaf.getDataBlock();

    // Create a hash of this data block using the
    // specified algorithm
    final int numBlocks = dataBlock.size();
    for (int index=0; index<numBlocks-1; index++)
    {
        md.update(dataBlock.get(index));
    }
    // Complete the digest with the final block
    digest = md.digest(dataBlock.get(numBlocks-1));

    return (digest);
}
```

加密摘要

图 11 默克尔树

下一步计划


搭建框架
1. 使用Java实现P2P网络
2. 使用Android Studio开发用户界面和实现蓝牙连接
前后端结合
1. 完成安卓界面和后端逻辑的连接，发布V1.0.0 测试版本
2. 实现一个检验交易真实性的算法
完善算法
1. 完善交易真实性检验、挖矿算法和账户管理细节
测试阶段
1. 邀请志愿者参加测试
2. 增加部分额外内容
10.28 - 11.11
11.11 - 11.25
11.25 - 12.9
12.9 - 1.6

参考文献

[1] 宋轩, 张浩然. 基于区块链的挖矿方法、装置、计算机设备及 存储介质[P]. 广东省：CN111682946A, 2020-09-18.

[2] “How blockchain will disrupt your industry”, https://www.slalom.com/insights/how-blockchain-will-disrupt-your-industry[Online]

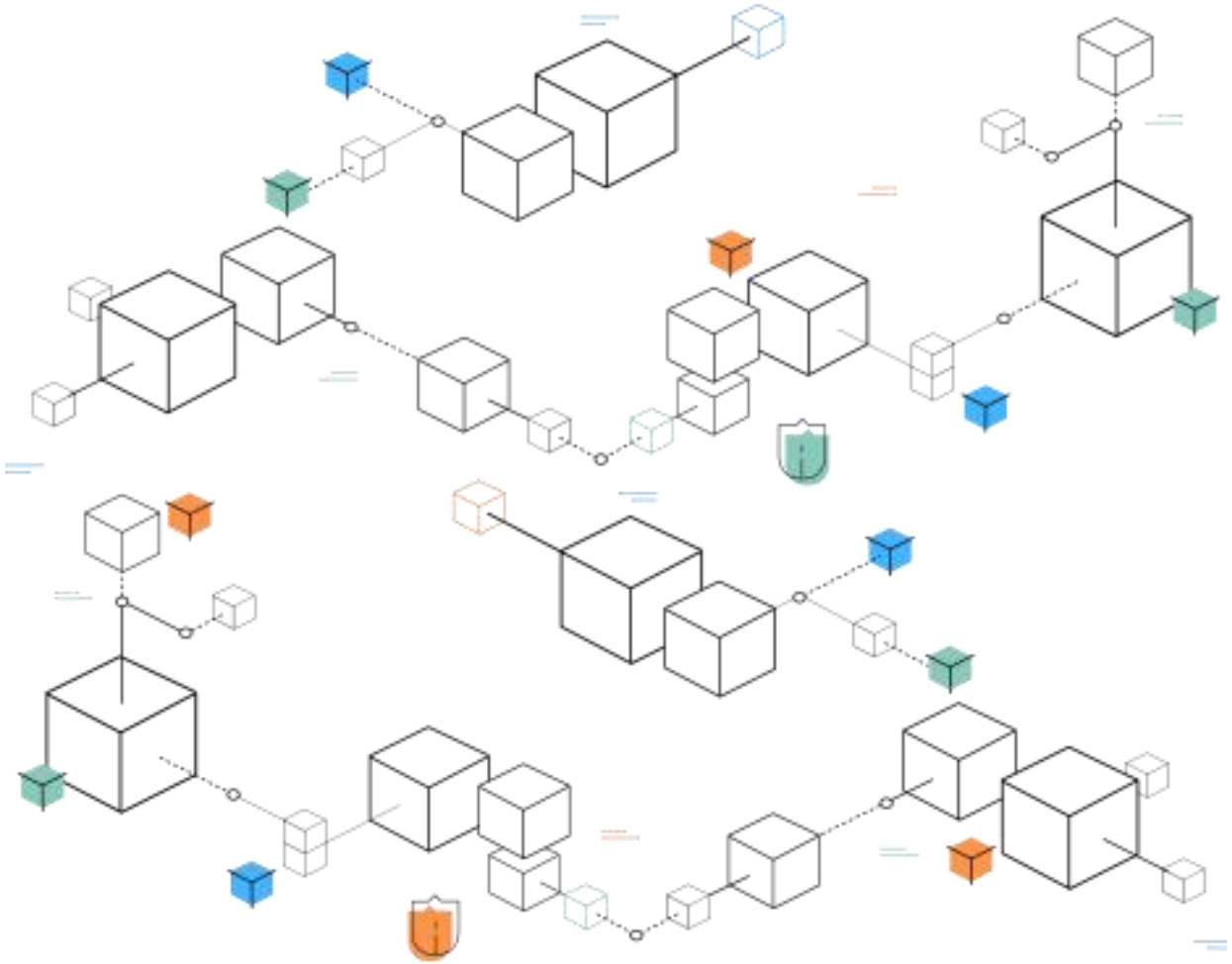
[3] Nakamoto S, "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf[Online], 2008

[4] “Pool Distribution”， https://btc.com/stats/pool[Online]

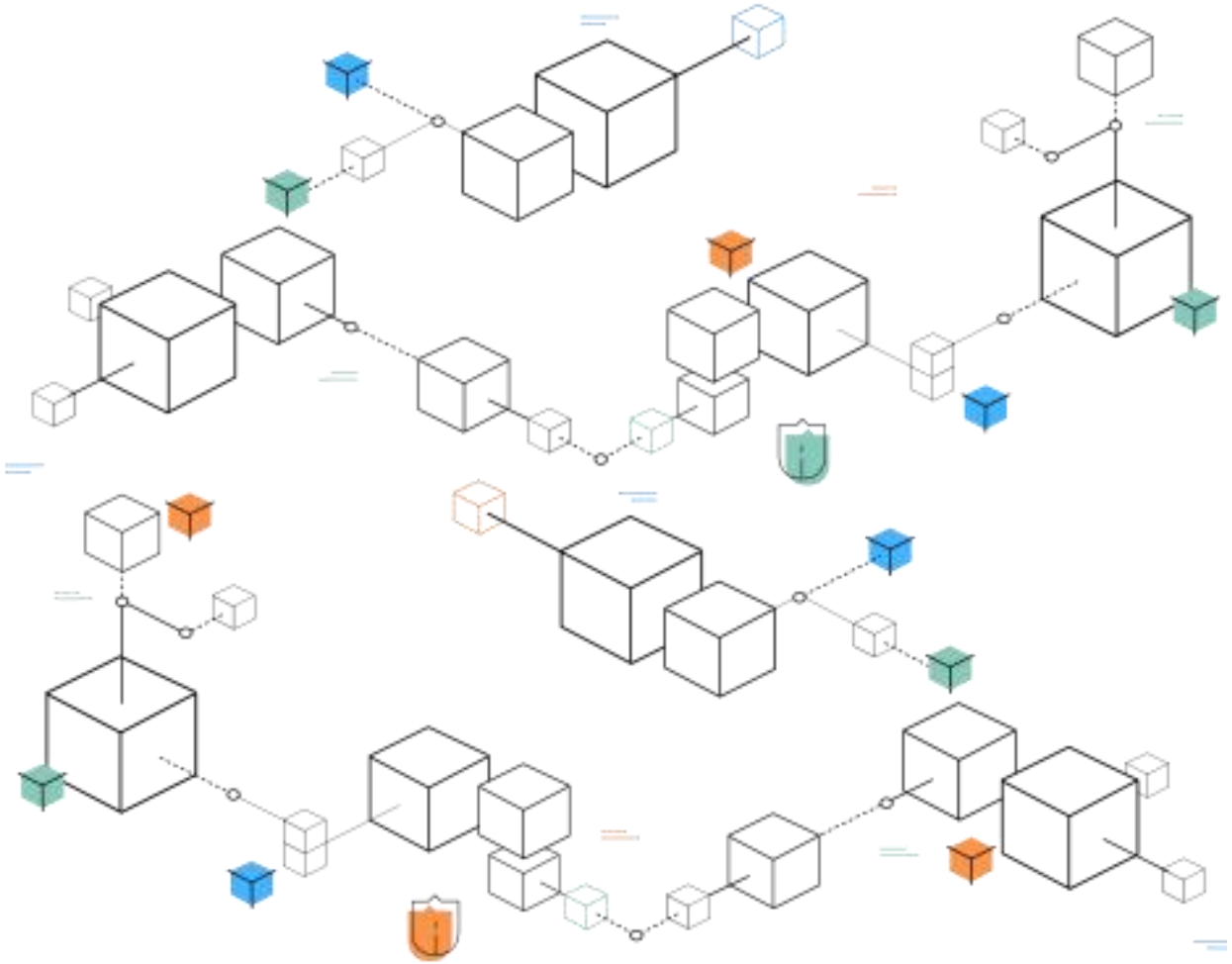
Q & A

要推动**区块链底层技术服务**和**新型智慧城市建设**相结合，探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平。

——习近平总书记 2019.10.24



THANK YOU



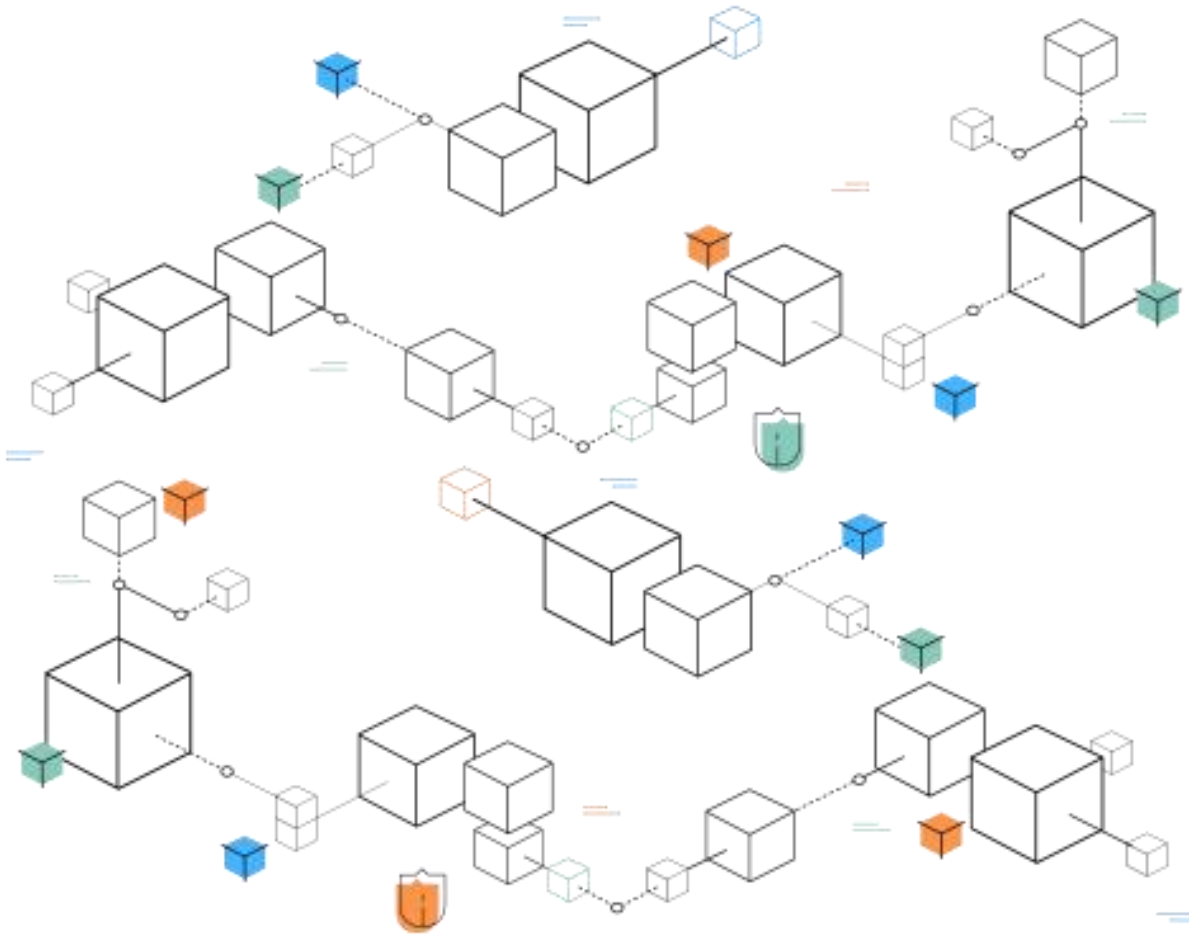
基于密接技术的区块链开发

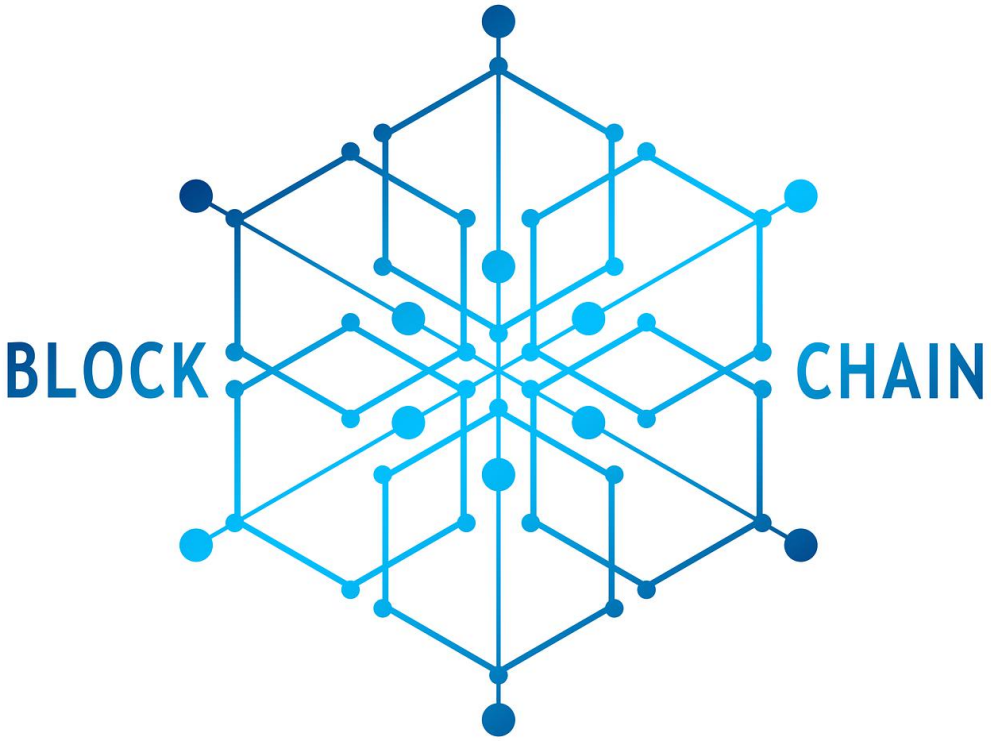
创新实验　第二次项目展示

小组成员：庄湛　邹若彤　潘泰仰

指导老师：宋轩老师　张浩然老师(东京大学)
云沐晟学长(RA)　林贵旭学长(RA)

2020/12/3　创园10栋504





Contents

系统设计：共识算法

POW的改进：通过**密接交互信息**产生的随机项代替计算资源高速生成的随机项进行区块链挖矿

利用密接交互信息具有**有限性**和**多重置信性**

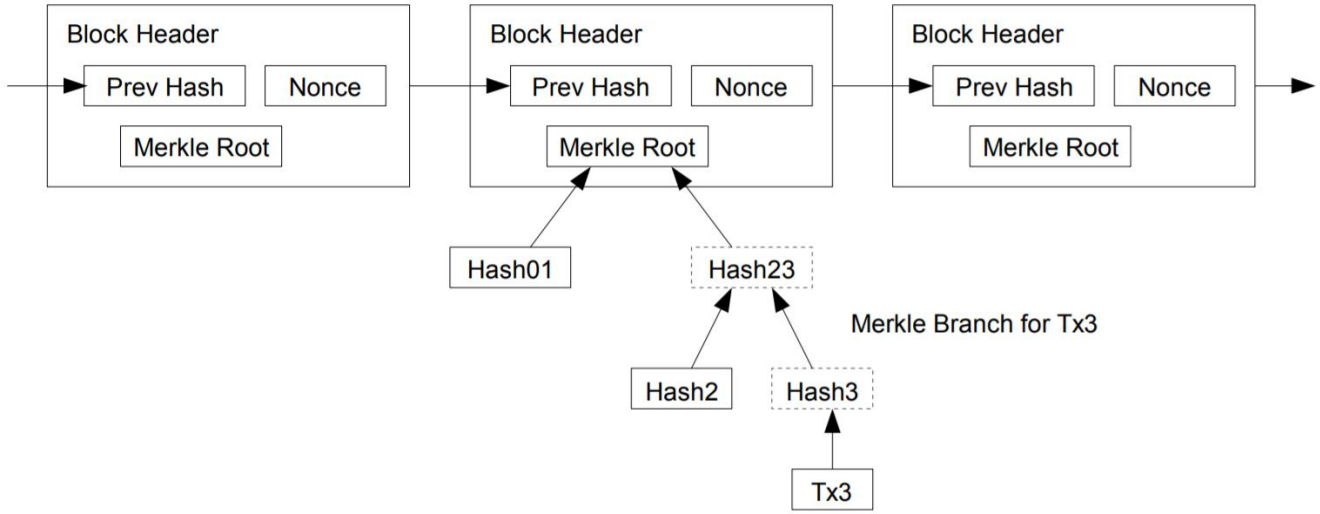


图 1 区块链结构[1]

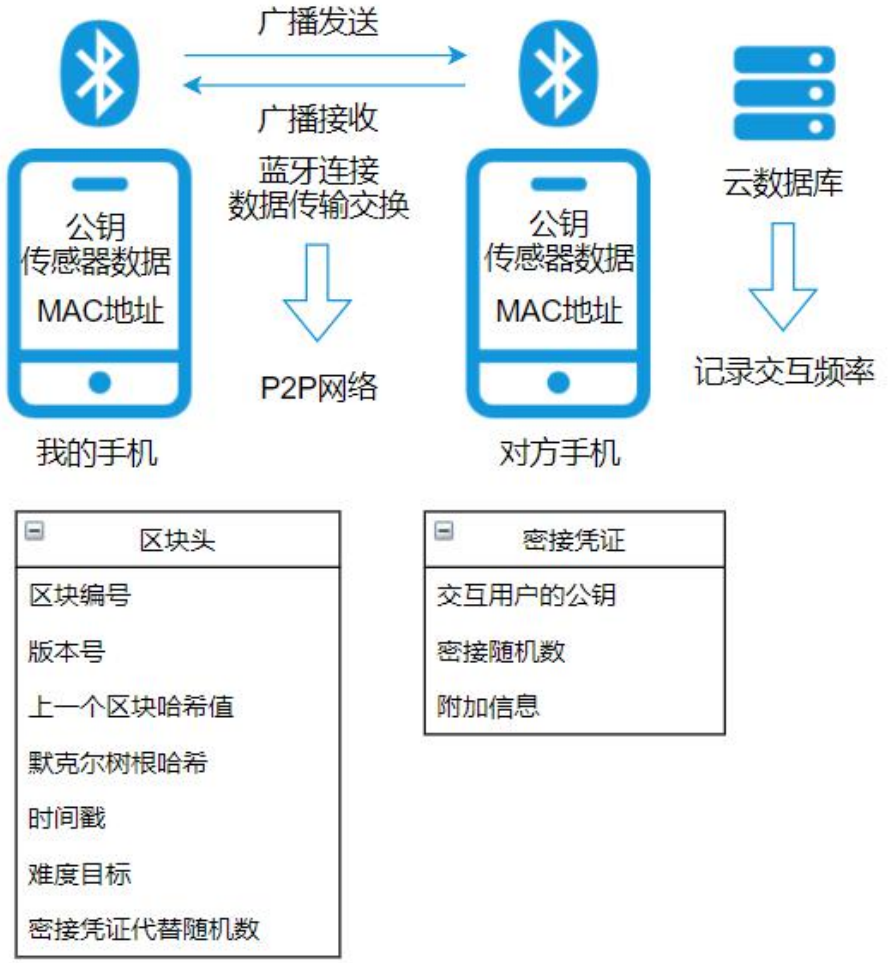


图 2 密接凭证代替方案

[1] Nakamoto S, "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf[Online], 2008

系统设计：共识算法和奖励机制

POS的改进：通过密接发生量代替货币持有量，且密接次数在中等偏上区间拥有更高几率出块(调整奖励和难度)

假设正常人密接次数呈**幂律分布**，利用中位数作为评价基准。

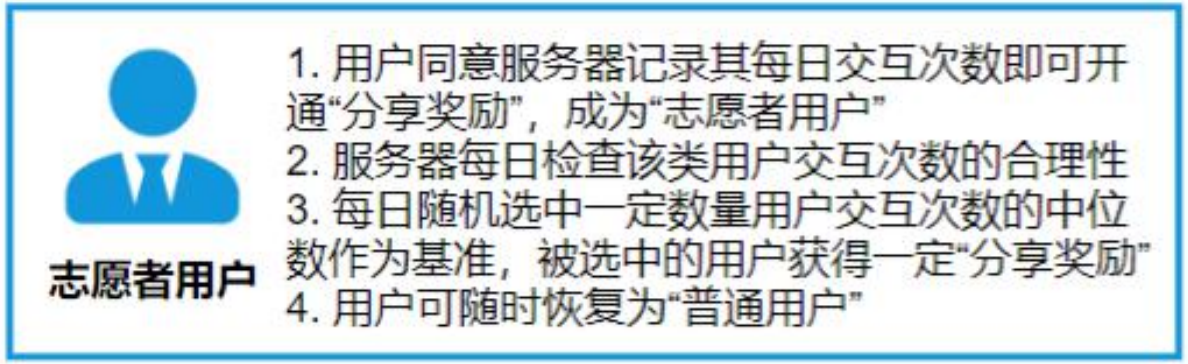


图 3 志愿者用户

出块奖励

出块奖励是用户与其他用户进行密接交互并成功解决区块链哈希难点时所获得的奖励。

打包奖励

用户在成功获得出块奖励的同时获得该奖励。根据打包的交易量可以获得一定的Mcoin奖励

分享奖励

选择一组志愿者用户作为“基准”时，当成功出块时，这组志愿者用户可以获得一定的Mcoin奖励。

系统设计

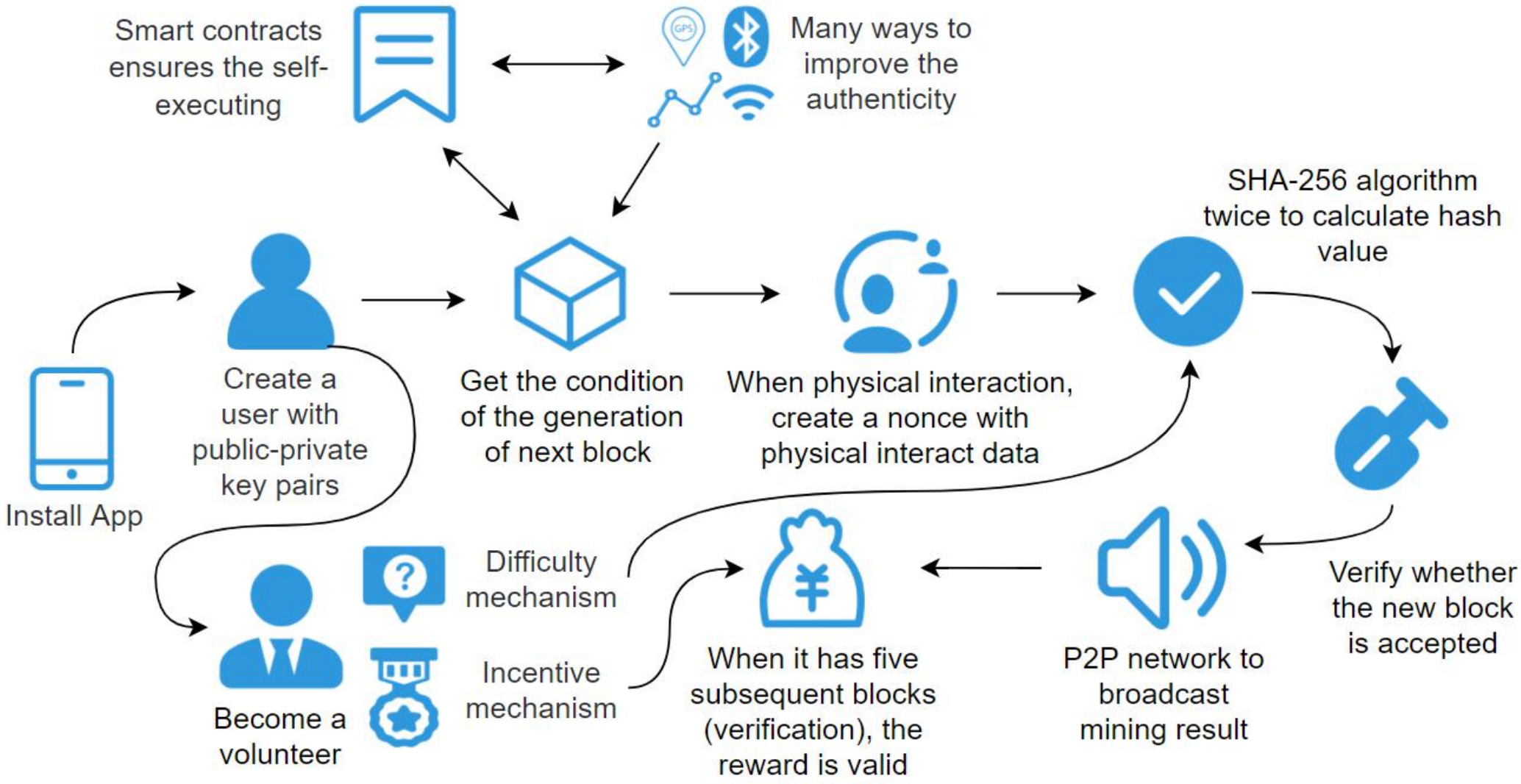

Smart contracts ensures the self-executing
Many ways to improve the authenticity
SHA-256 algorithm twice to calculate hash value
Create a user with public-private key pairs
Get the condition of the generation of next block
When physical interaction, create a nonce with physical interact data
Install App
Verify whether the new block is accepted
Difficulty mechanism
Incentive mechanism
When it has five subsequent blocks (verification), the reward is valid
P2P network to broadcast mining result
Become a volunteer

图 4 系统设计

物联网区块链技术

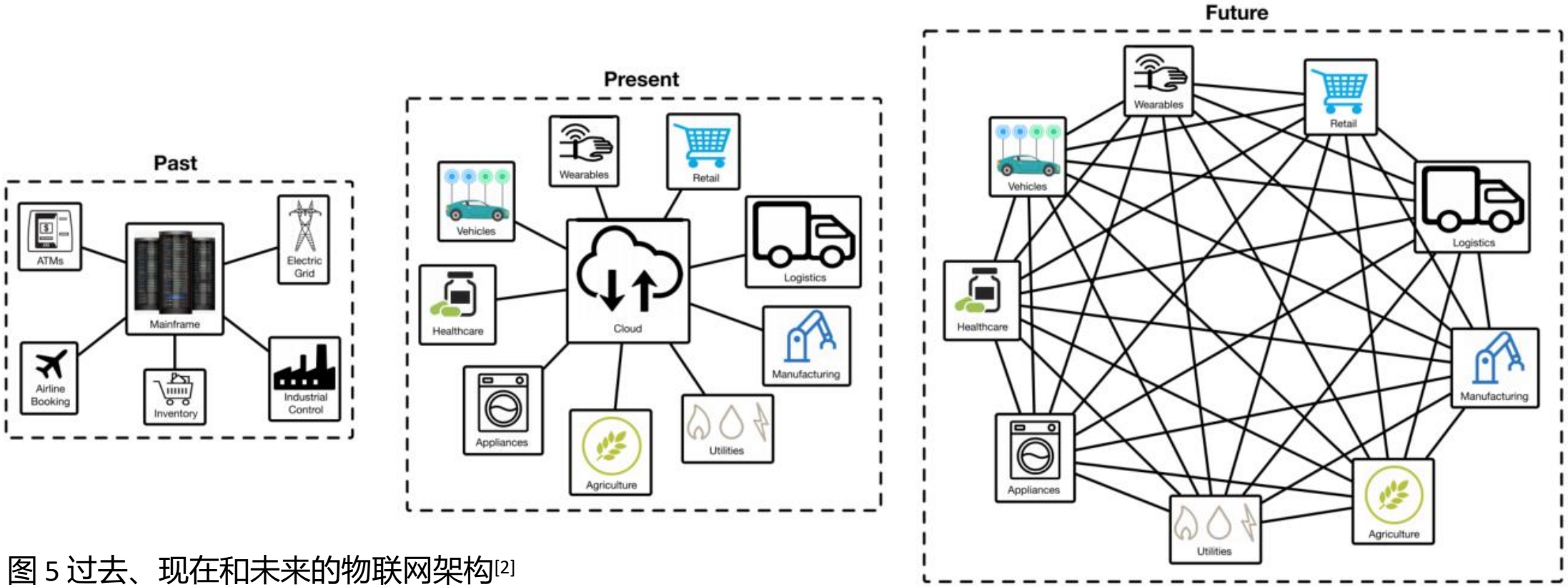


图 5 过去、现在和未来的物联网架构[2]

目前物联网技术难点：

- 设备访问和控制权的中心化导致的隐私安全问题是未来物联网解决方案的核心。
- 设备数量的指数级增长导致的数据记录和存储困难以及数据管理自动化困难。

[2] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. Ieee Access , 6 , 32979-33001.

物联网区块链技术

物联网区块链的趋势[3]：

- 受欢迎程度
- 应用范围
- 底层技术的发展
- 商业模式

物联网区块链的难点[3]：

- 资源限制
- 设备支持
- 规模
- 通信性能

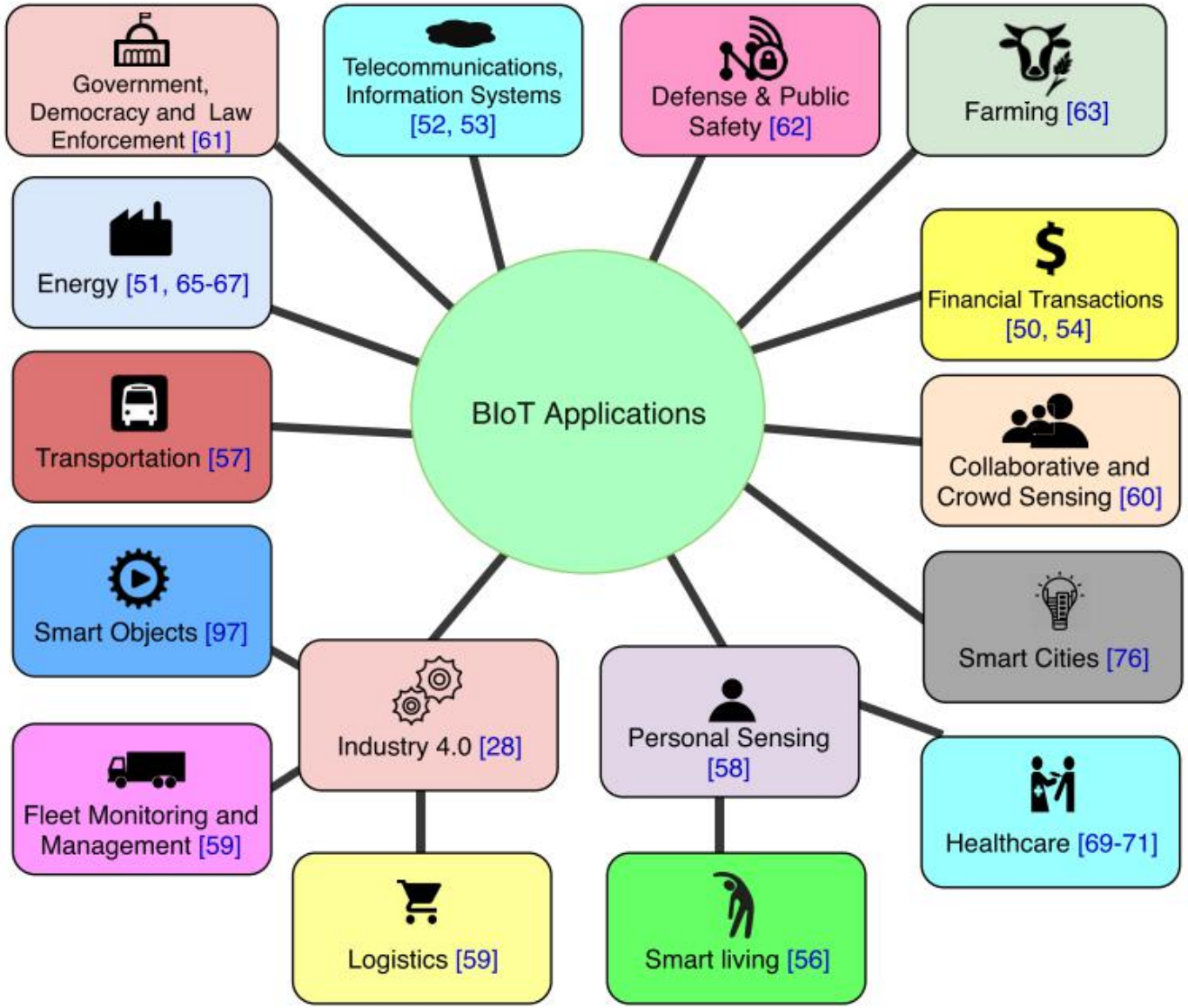


图 6 物联网区块链的应用[2]

[2] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. Ieee Access , 6 , 32979-33001.
[3] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR) , 53 (1), 1-32.

物联网区块链技术

时间	技术	细节
2019.01	Algorand	一个安全和有效的分布式账本，解决了伪三角（去中心化、可扩展性、安全性）
2019.06	PoET	一种基于彩票式共识的**轻量级**共识机制
2019.08	PoRX	一种基于声誉证明的**物联网区块链**的共识机制
2020.03	PoBT	可扩展的基于物联网区块链的**轻量级**共识机制
2020.06	PoWP	一种基于**物理世界**证人在场的增强民主的区块链共识
2020.08	SURFACE	一个用于**现实网络**的实用区块链共识算法
2020.09	PoQF	一种基于**车载自组织网络**和边缘计算的区块链共识机制
2020.11	PoEWAL	一种物联网中区块链的**轻量级共识机制**，基于限时工作和幸运值
2020.11	Blockene	**首个**在**移动手机**上提出的区块链架构

物联网区块链技术

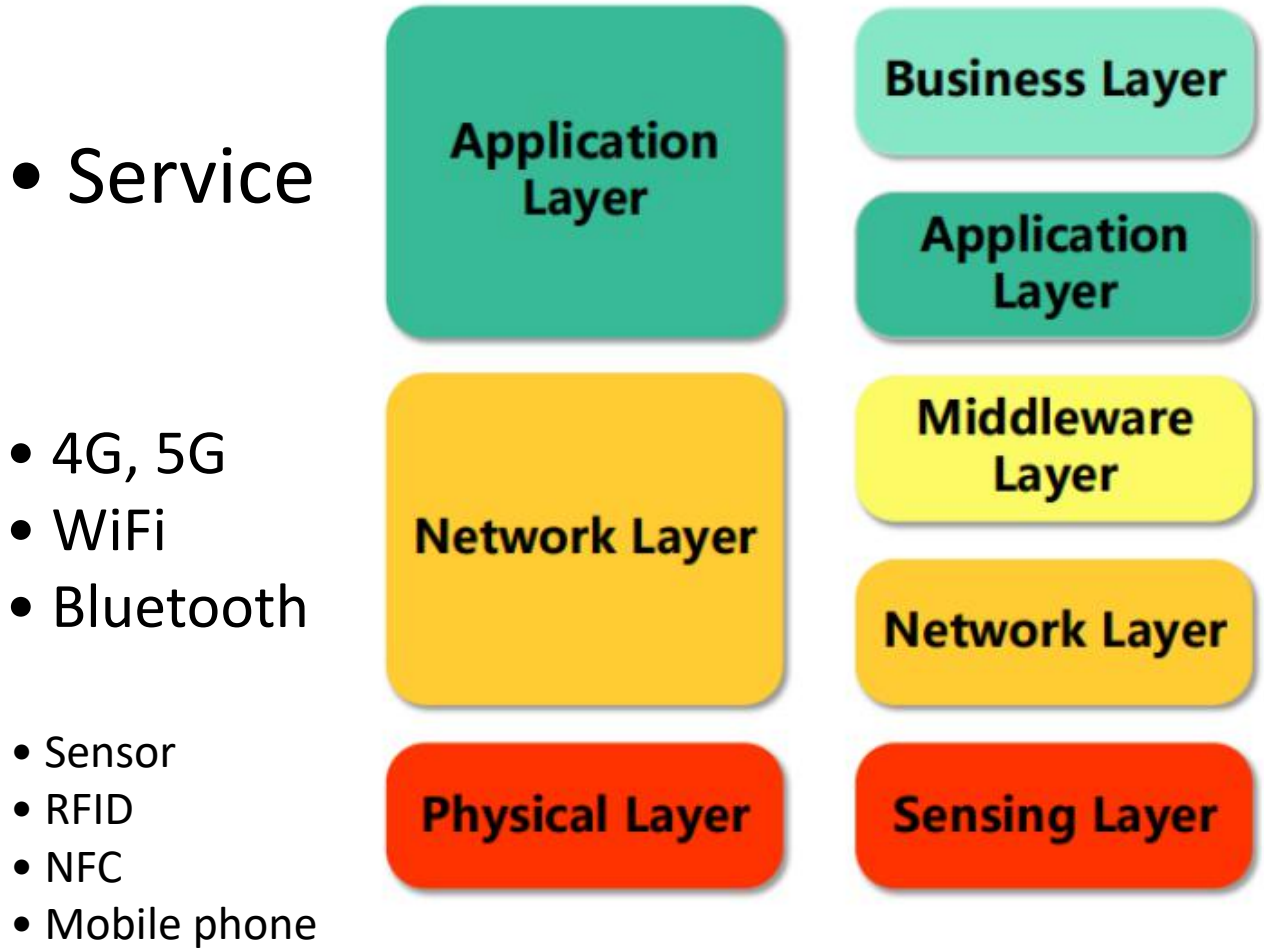


图 7 物联网架构层[3]

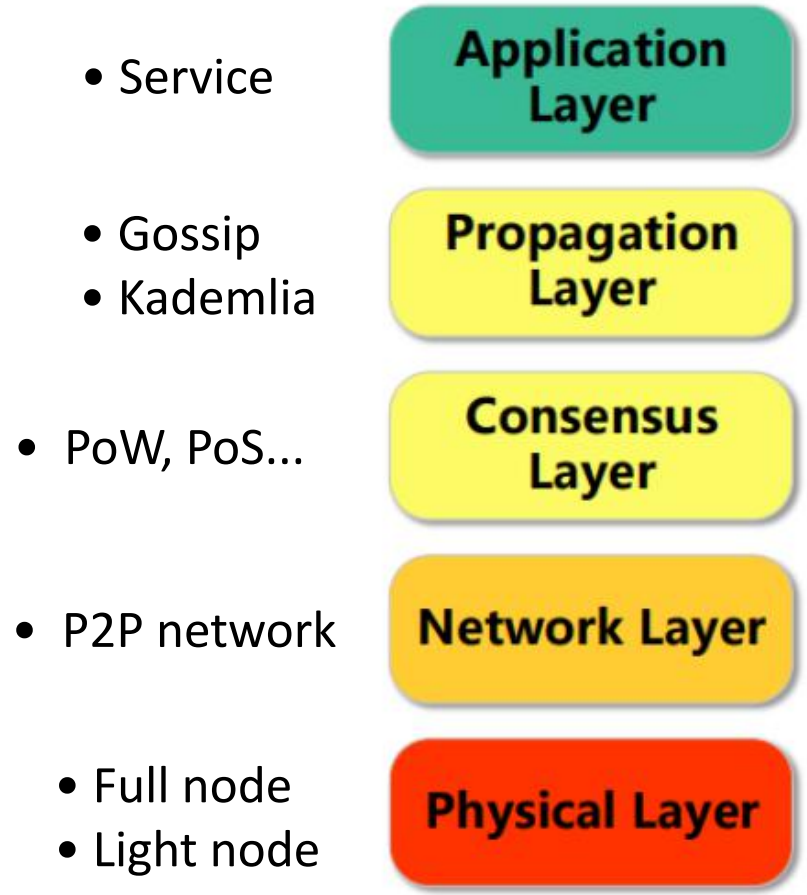


图8 区块链架构层[3]

[3] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR) , 53 (1), 1-32.

物联网区块链架构

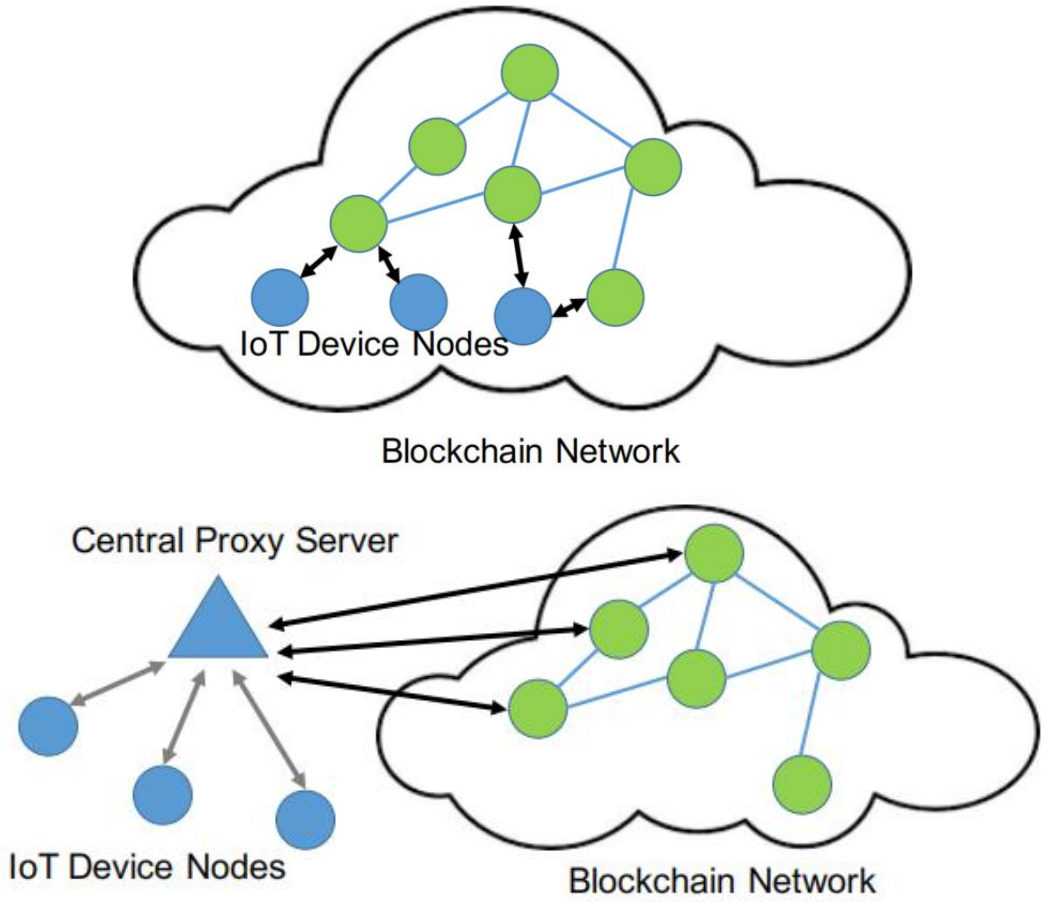


图 9 两种物联网区块链模型[3]

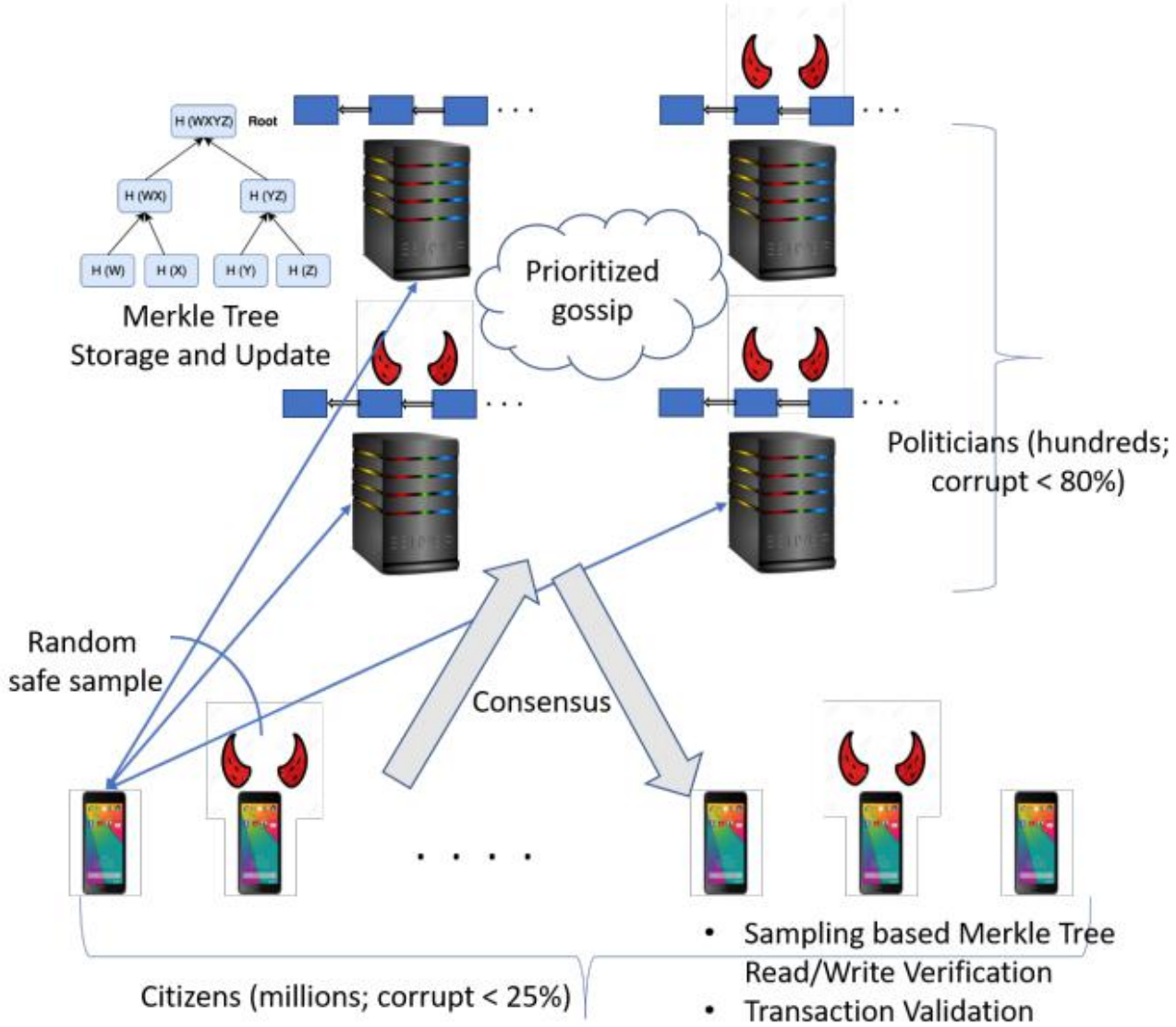


图 10 Blockene的架构[4]

[3] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR) , 53 (1), 1-32.
[4] Satija, S., Mehra, A., Singanamalla, S., Grover, K., Sivathanu, M., Chandran, N., ... & Lokam, S. (2020). Blockene: A High-throughput Blockchain Over Mobile Devices. In 14th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 20) (pp. 567-582).

物联网区块链架构

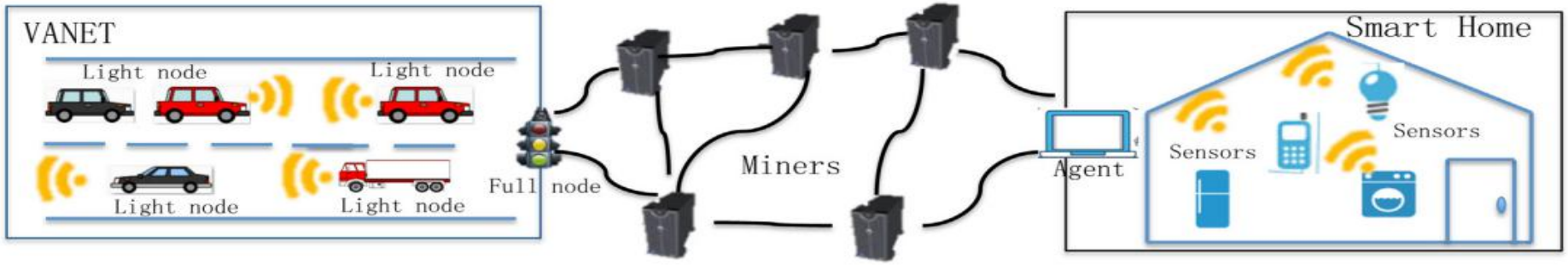


图 11 VANET区块链的架构[5]

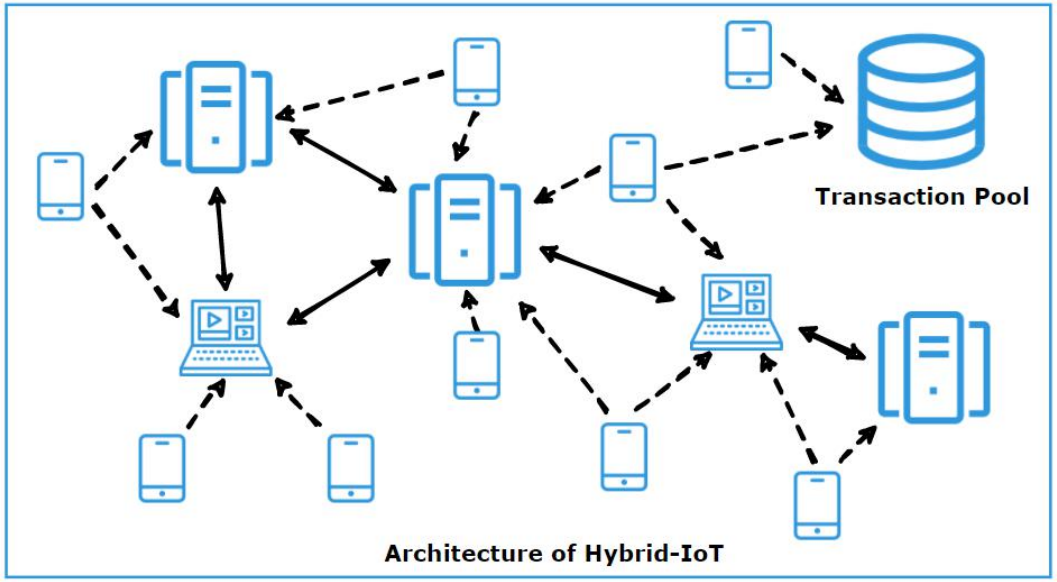


图 12 混合物联网区块链架构[7]

[5] Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. Computer Communications , 136 , 10-29.

[7] Ometov, A., Bardinova, Y., Afanasyeva, A., Masek, P., Zhidanov, K., Vanurin, S., ... & Bezzateev, S. (2020). An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access , 8 , 103994-104015.

物联网区块链技术

Table 1
Comparison between existing consensus method with PoEWAL.

Consensus method	Type	Energy consumption	Latency	Throughput	IoT suitable
PoW	Probabilistic	High	High	Low	No
PoS	Probabilistic	Low	Medium	Low	maybe
DPoS	Probabilistic	Medium	Medium	High	No
PoB	Probabilistic	medium	High	Low	No
PoET	Absolute	Low	Low	High	maybe
PoA	Probabilistic	High	Medium	Low	No
Pbft	Absolute	Low	Low	High	maybe
PoAu	Probabilistic	medium	Medium	Low	No
dPbft	Absolute	Low	Medium	High	maybe
PoBT	Absolute	Low	High	Medium	maybe
Tangle	Absolute	Low	Low	High	maybe
Raft	Absolute	Low	Low	High	maybe
Algorand	Probabilistic	Medium	High	Medium	No
PoEWAL	Probabilistic	Low	Low	Medium	yes

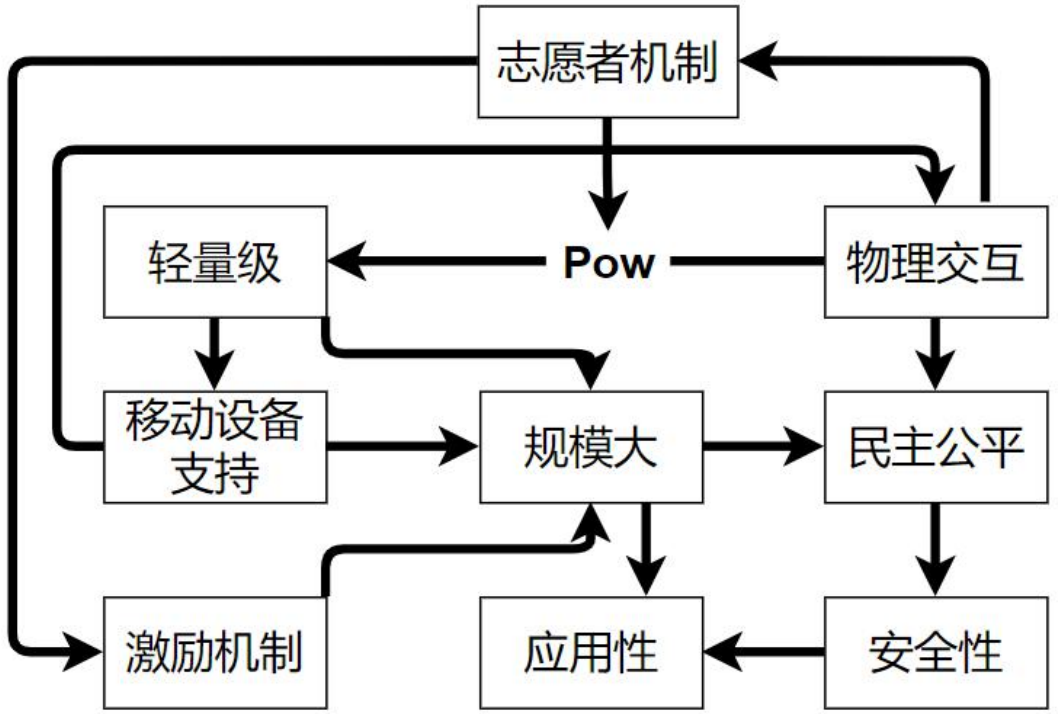
图 13 物联网区块链共识机制的对比[6]

- 我们的共识机制的贡献是什么？
- 为什么采用移动设备？

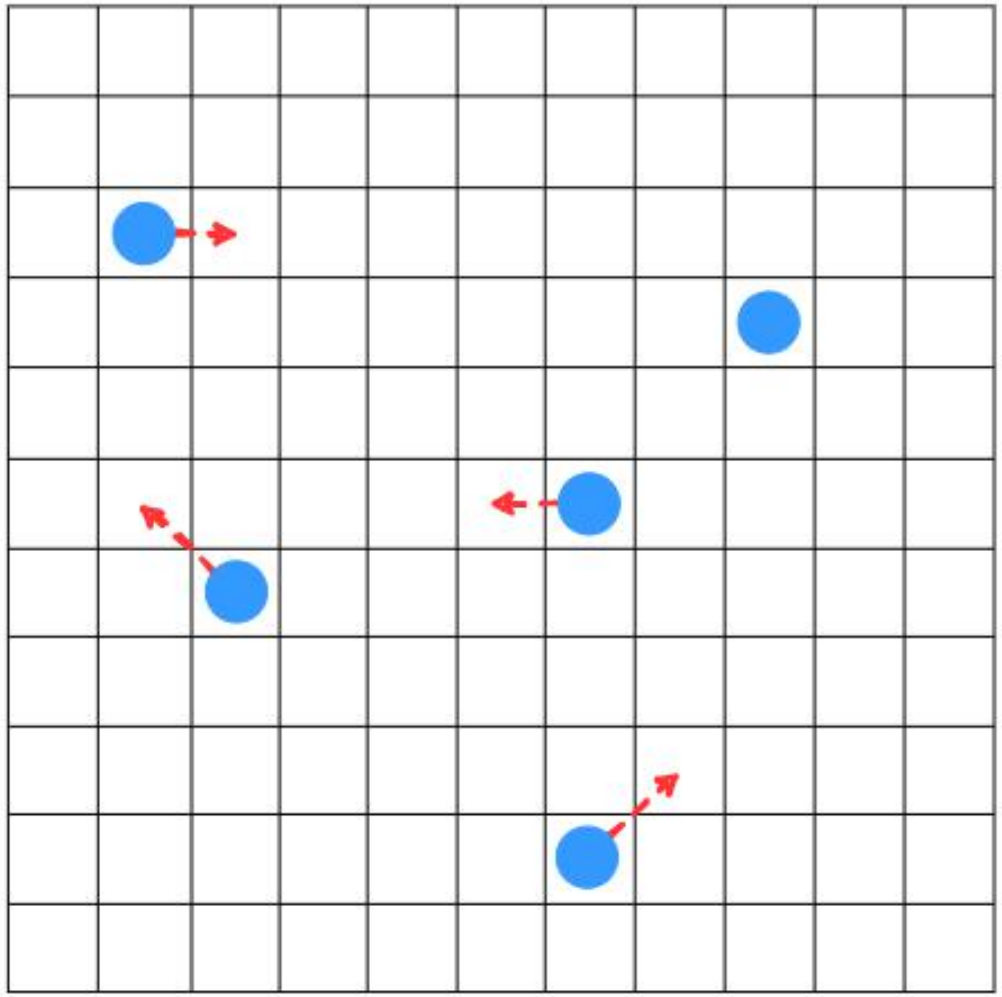
[6] Wang, E. K., Liang, Z., Chen, C. M., Kumari, S., & Khan, M. K. (2020). PoRX: A reputation incentive scheme for blockchain consensus of IIoT. Future Generation Computer Systems , 102 , 140-151.

PoPI 共识机制的贡献

- 基于移动设备的区块链共识机制，规模大
- 基于物理交互的区块链共识机制，动态证人在场证明，民主公平
- 基于志愿者机制的难度调整机制和奖励机制



实验和项目进度



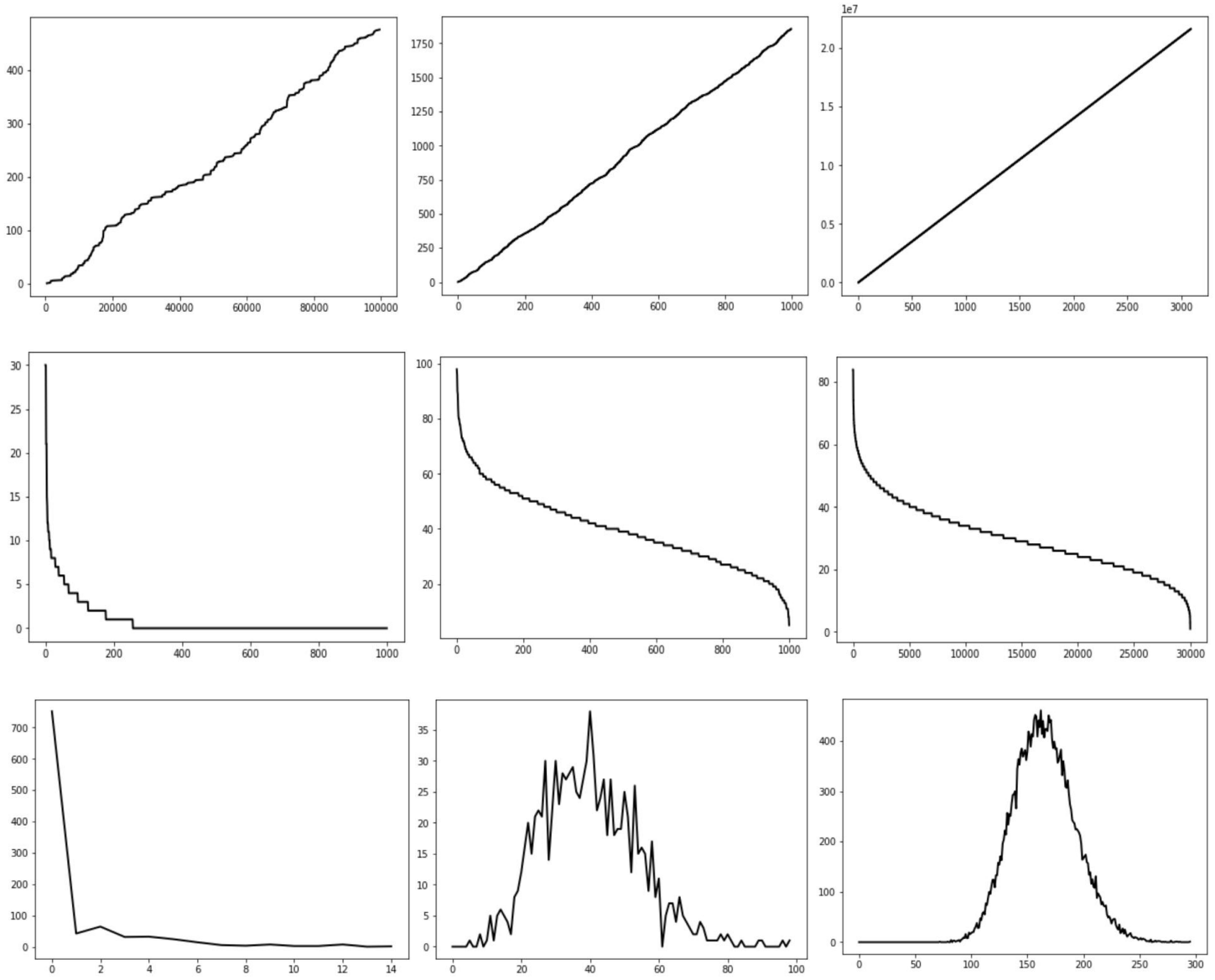
- 模拟环境
  - 棋盘式
  - 障碍
- 模拟人群
  - 不同模式
    - 走走停停型
    - 趋向人群型
    - 来回往复型
  - 人群密度

实验和项目进度

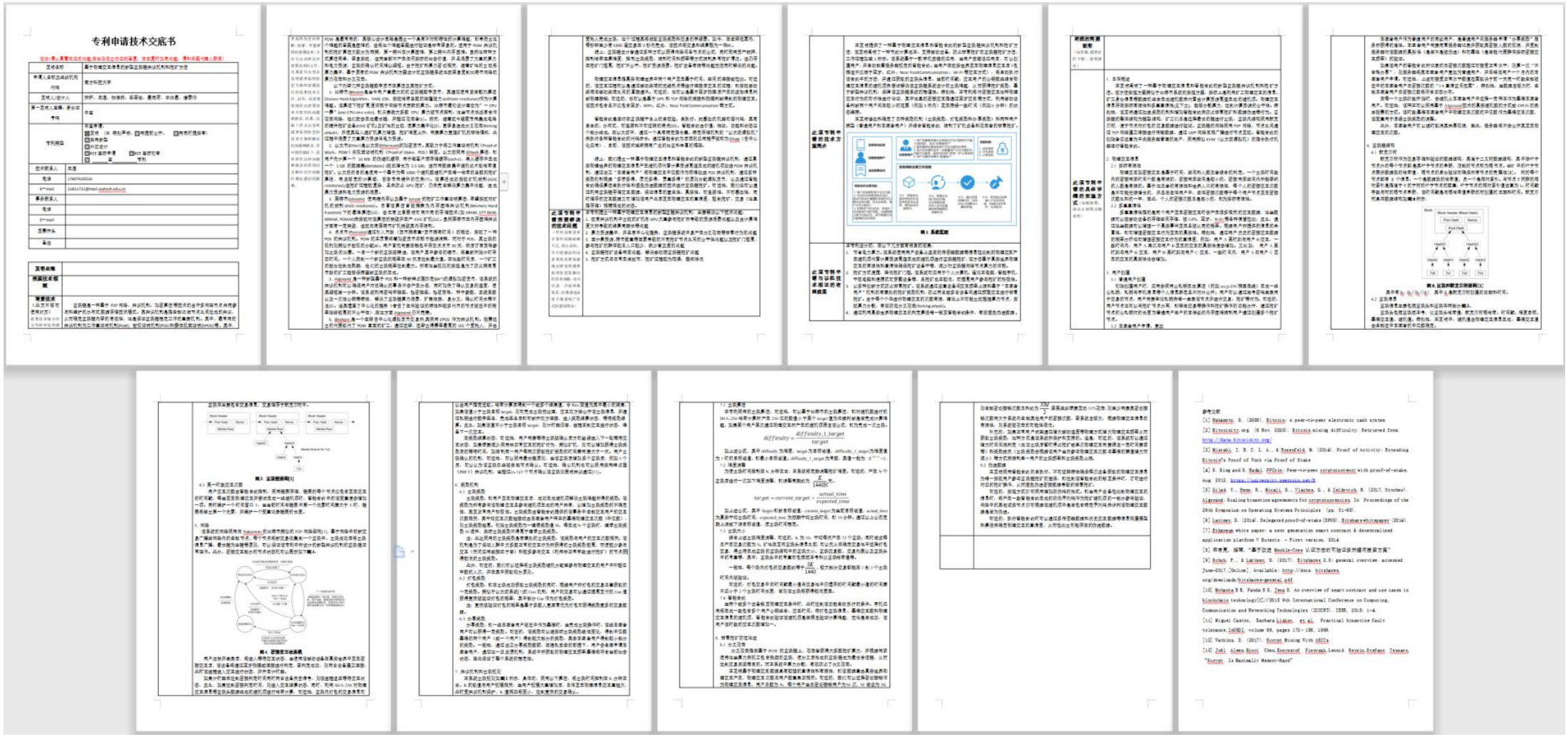
```
445,819,376
279,983,1443
279,983,1445
197,660,1493
175,434,1533
175,434,2210
347,938,4924
347,938,4929
347,938,4932
347,938,4933
194,634,5373
670,769,5580
670,769,5581
936,948,5796
881,951,7489
```

探究时间和总密接次数的关系

探究个体密接次数的分布



专利完成： 基于物理交互信息的新型区块链共识机制和挖矿方法



论文进度：摘要

PoPI: A Lightweight Blockchain Consensus Over Mobile Devices

Abstract—Nowadays, the Internet of Things (IoT) with Cloud App distributed among multiple peers have the trend of becoming the next generation network architecture, and even have the prospect of changing the way of social operation. Blockchain which implements a distributed, traceable and tamper-resistant ledger can not only address the privacy and security concerns in IoT but also combine the smart contract and cryptography technology to develop Blockchain-based IoT ecosystem, which have played an important role in energy, health, supply chain, smart city and other fields. However, for the blockchain based on the existing consensus mechanism, there are disadvantages such as small scale, waste of resources and the inequity caused by centralization trend. In this article, we propose a universal and lightweight proof of physics interaction (PoPI) consensus mechanism and its integration framework based on a mobile device app. Also, we propose the incentive mechanism and difficulty mechanism based on a volunteer mechanism to guaranteed the robustness. Through theoretical derivation and experimental results of a certain scale of volunteers in SUSTech, we demonstrate the scalability of this solution. Furthermore, PoPI is compared with some existing consensus mechanisms in terms of energy, consensus time, and network latency.

Index Terms—Internet of Things (IoT), blockchain, consensus mechanism, physical interaction, mobile device, scalability

摘要

区块链是一种分布式、可跟踪、抗篡改的账本，其实现了安全的加密货币交易。如今，将云功能分布在多个对等节点的物联网有成为下一代网络架构的趋势，甚至有改变社会运作方式的前景。利用区块链技术，不仅可以解决物联网中的隐私和安全问题，还可以结合智能合约和加密技术，构建基于区块链的物联网生态系统，在能源、健康、供应链、智慧城市等领域已经发挥了重要作用。然而，基于现有的共识机制，区块链存在规模小、资源浪费、集中化趋势带来的不公平等弊端。本文提出了一种通用的、轻量级的基于移动设备应用的物理交互证明(PoPI)共识机制及其集成框架，并提出了基于志愿者机制的激励机制和难度调整机制以保证系统的鲁棒性。本文通过理论推导和一定规模志愿者的实验结果，证明了该解决方案的可扩展性，并将 PoPI 与现有的共识机制在能耗、共识时间和网络延迟等方面进行了比较。

论文进度：介绍

PoPI: A Lightweight Blockchain Consensus Over Mobile Devices

Zhan Zhuang, Ruotong Zou, Taiyang Pan

***Abstract*—Nowadays, the Internet of Things (IoT) with Cloud App distributed among multiple peers have the trend of becoming the next generation network architecture, and even have the prospect of changing the way of social operation. Blockchain which implements a distributed, traceable and tamper-resistant ledger can not only address the privacy and security concerns in IoT but also combine the smart contract and cryptography technology to develop Blockchain-based IoT ecosystem, which have played an important role in energy, health, supply chain, smart city and other fields. However, for the blockchain based on the existing consensus mechanism, there are disadvantages such as small scale, waste of resources and the inequity caused by centralization trend. In this article, we propose a universal and lightweight proof of physics interaction (PoPI) consensus mechanism and its integration framework based on a mobile device app. Also, we propose the incentive mechanism and difficulty mechanism based on a volunteer mechanism to guaranteed the robustness. Through theoretical derivation and experimental results of a certain scale of volunteers in SUSTech, we demonstrate the scalability of this solution. Furthermore, PoPI is compared with some existing consensus mechanisms in terms of energy, consensus time, and network latency.**

***Index Terms*—Internet of Things (IoT), blockchain, consensus mechanism, physical interaction, mobile device, scalability**

I. Introduction

A. Background

Blockchain implements a distributed,traceable and tamper-resistant ledger. Most blockchains existing today needs their users to run a powerful server or needs significant compute resources because they are basing on PoW(proof-of work) or other similar consensus mechanism.

One the one hand, these compute-intensive blockchains maks a large resource consumption, which causes they are mostly using in cryptocurrencies or other high earning applications. The high threshold of those blockchain applications is also preventing those who do not have a powerful client to be their member.

On the other hand, the difficulty in computing of those blockchains also lead to another problem that the reliability of them can be reduced. One of the widely known example is the 51-percent-attack. Blockchains usually require majority of members to be honest. This can works easily when the member amount is huge. But obviously, the high threshold blockchains cannot be adopted widely and only a small number of members can participate, especially in those don't have a high earning applications to attract new members.

In this paper, we offered a light-weight blockchain consensus, which provide a possibility to being high-throughput. The most difference is that it can run on the IoT devices instead of requiring a huge mount of computing-unit, which makes the spreading possible. One of the most common application is running on the smart phone. It makes the cost of participation lower than ever before. And the explosive increase of the members can significantly increase the reliability of the system.

B. Literature review

To ensure that the ledger recorded by the nodes in the system are whole, timely, and creditable, blockchain systems typically use a consensus mechanism to dictate which bookkeepers can record the data on the blockchain.

The most idealistic consensus mechanism is like democratic voting, which means everyone can vote, and everyone has the same voting weight. This scheme may be possible to implement in a real world, but, in a public blockchain, it is hard to find a strategy that can not only attract and motivate users to participate in the maintenance of the blockchain system but also ensure a relatively level playing field for each user.

For the blockchain based on mobile devices, we also need to consider its battery consumption, throughput, latency and scalability. In recent years, many new consensus mechanisms based on the IoT have been proposed. Meanwhile, some blockchain systems based on mobile devices were proposed by Sambhav Satija et al. Below, we will analyze several existing consensus mechanisms and blockchain systems.

1) Proof of Work (PoW): PoW is applied in Bitcoin successfully. Its core idea is to distribute the block accounting rights through the competition of computing power among nodes. After a block is generated, the message would be broadcasted to the entire network for verification by other nodes. However, the generation of blocks requires a lot of computational power, and the block confirmation time delay is too much, resulting in low efficiency, low transaction throughput, thus it cannot adapt to many real scenarios.

2) Proof of Stake (PoS): PoS is an alternative protocol for PoW, without the problem of too much computation cost and consensus time delay. The main idea of PoS is that the proportion of users' stake in the system is inversely proportional to the difficulty of block generation. The larger the stake held by nodes in the system, the easier he wins.

3) Proof of Activity (PoA): PoA is a protocol that combines PoW and PoS. It is base on a hypothesis of economic phenomenon known as the "tragedy of the commons". The proposed PoA protocol aims to increase attack costs of malicious miners by forcing them to achieve eight times hash rate than the honest miners in the network. In addition, it reduces computational complexity to 1/10 of Bitcoin PoW, minimizing energy consumption. However, the proof of activity is also intended to protect only cryptocurrency applications.

4) Proof of Authority (PoAu): In PoAu blockchain, which be viewed as protected by trusted validation nodes, miners were chosen as the verifiers of the block on the basis of personal credibility. Compared with PoW and PoS, the PoAu is more energy friendly, but it still has large delays and energy costs. Because a node with a high authority is not necessarily evil and becoming a verifier requires a lot of conditions which reveals the real identity, the consensus mechanism is controversial in terms of security and privacy, and is not suitable for large-scale blockchain.

5) Proof of Block and Trade (PoBT): PoBT is a lightweight consensus algorithm for scalable IoT blockchain which allows validation of transactions and blocks and incorporates peers based on the number of nodes participating in a session to reduce the computing time. it is considered a absolute consensus and suitable for the blockchain systems on the IoT.

6) Proof of Elapsed Time (PoET): In PoET, every node in the network generates random time. After this, everyone goes to sleep for that random time. Whoever wakes up first, can mine the block. It is used in a cooperative environment or requires a trusted setup for removing malicious attacks. However, it is an absolute consensus method that can only be used in a cooperative environment.

7) Proof of Reputation-X (PoRX): PoRX is a blockchain consensus mechanism on the IoT based on a proof of reputation. It uses some rules to control the reputation, such as adjusting the reputation based on the number of self-generated blocks and malicious behaviors of a user. Experimental results show that the scheme can effectively stimulate the cooperative behavior of nodes in the network and avoid the Matthew effect usually in the PoS consensus mechanism. However, this consensus mechanism has a high latency due to the need to check and modify reputation values multiple times.

8) Proof of Witness Presence (PoWP): PoWP proposed the presence of a witness based on the scanning of the code as the basis for democratic voting. This dynamic solution enhances democracy and fairness by verifying the physical existence of location. Theoretically, it is an advanced consensus mechanism. However, the scanning method according to the scenic spot has limitations, and it is easy to generate data forgery and other attacks.

9) Proof of Elapsed Work and Luck (PoEWAL): PoEWAL is a lightweight probabilistic consensus algorithm for non-cooperative cases based on proof of elapsed work and proof of luck mechanisms. Moreover, it has little energy consumption, latency and consensus time for mining and sending transactions to other nodes. However, its incentive mechanism is mainly two kinds of energy-saving incentives, which cannot be applied to mobile devices.

10) Algorand: Algorand uses verifiable random function (VRF) by randomly selecting a group of users in a decentralized way. VRF selects users based on the amount of money stored in their wallet. These users mine the new block using the byzantine agreement. It does not require high computational power, but needs a monetary system and has a large latency delay.

11) Byzantine Fault Tolerance(BFT): BFT needs all the nodes of the network have to take part in the voting to mine the new block, but the consensus is reached only when less than one-third nodes behave maliciously. It is not suitable for the Non-cooperative IoT blockchain network.

C. Key techniques in PoPI

In PoPI consensus, a nonce is created when physical interaction (detected by bluetooth technology) occurs. If the hash value of block header is no more than the current mining difficulty, a new block is created. The new block requires double verification. The system adopts communication technologies (such as Bluetooth, WIFI and GPS) together with time stamp to verify if the nonce is authentically created according to physical interactions. In addition, P2P network broadcasts the block information to nodes, and they will perform transaction validation.

When five subsequence blocks are verified, the block reward is valid. To avoid malicious physical interaction, we stipulate that the user gets higher block reward if the number of his physical interaction is slightly above the median. Additionally, users who volunteer to provide their number of physical interaction can get extra reward. The reward will be discussed in . . . (e.g. § 4.2) in detail.

D. Contribution

Compared to a traditional financial transaction model, our decentralized system does not have to rely on a trustworthy third party and the transaction information is impossible to be modified. Compared to PoW, our consensus produces nonce according to physical interaction, which is less energy consuming. Compared to PoWP (Proof of Witness Presence), our consensus is more scalable and easier for miners to get involved. In summary, the contributions of this paper are outlined as follow:

- We provide a new blockchain system consensus "Proof of Physics Interaction" based on PoW, and theoretically proof how it realizes.
- We provide a new blockchain integration framework with the characteristics of fairness and safety.
- We provide a new communication network with low energy consumption and short latency.
- A thorough empirical experiment is performed to demonstrate the scalability and high performance of the system.
- A lightweight blockchain architecture that leads to scale and security.

下一步任务

- 完成论文：方法论
- 完成论文：模拟实验，真人实验
- 完成论文：对比结果（耗电，吞吐量，延迟）
- 开发应用：基于P2P网络的Mcoin应用

参考文献

[1] Nakamoto S, "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf[Online], 2008

[2] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. Ieee Access , 6 , 32979-33001.

[3] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR) , 53 (1), 1-32.

[4] Satija, S., Mehra, A., Singanamalla, S., Grover, K., Sivathanu, M., Chandran, N., ... & Lokam, S. (2020). Blockene: A High-throughput Blockchain Over Mobile Devices. In 14th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 20) (pp. 567-582).

参考文献

[5] Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. Computer Communications , 136 , 10-29.

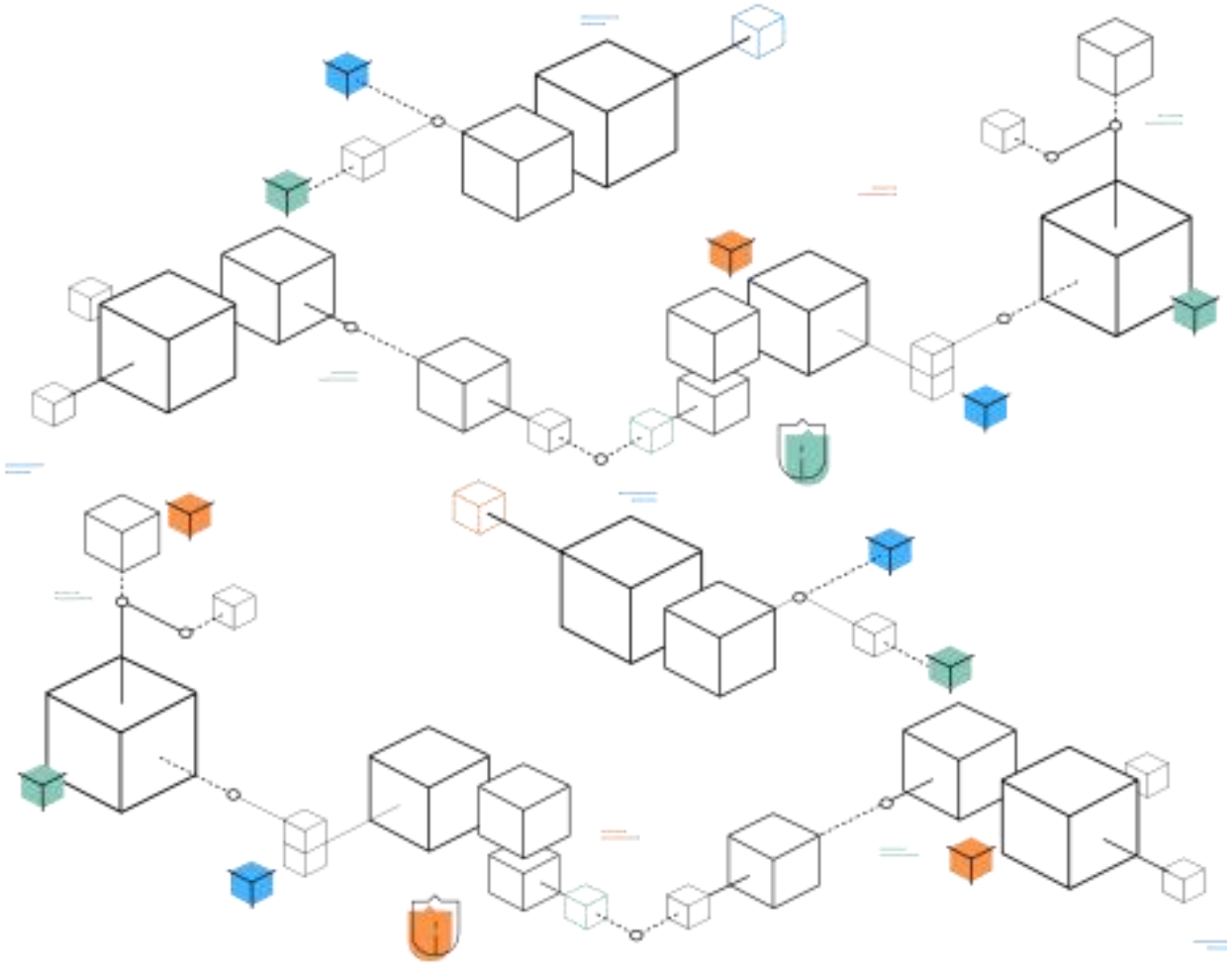
[6] Wang, E. K., Liang, Z., Chen, C. M., Kumari, S., & Khan, M. K. (2020). PoRX: A reputation incentive scheme for blockchain consensus of IIoT. Future Generation Computer Systems , 102 , 140-151.

[7] Ometov, A., Bardinova, Y., Afanasyeva, A., Masek, P., Zhidanov, K., Vanurin, S., ... & Bezzateev, S. (2020). An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access , 8 , 103994-104015.

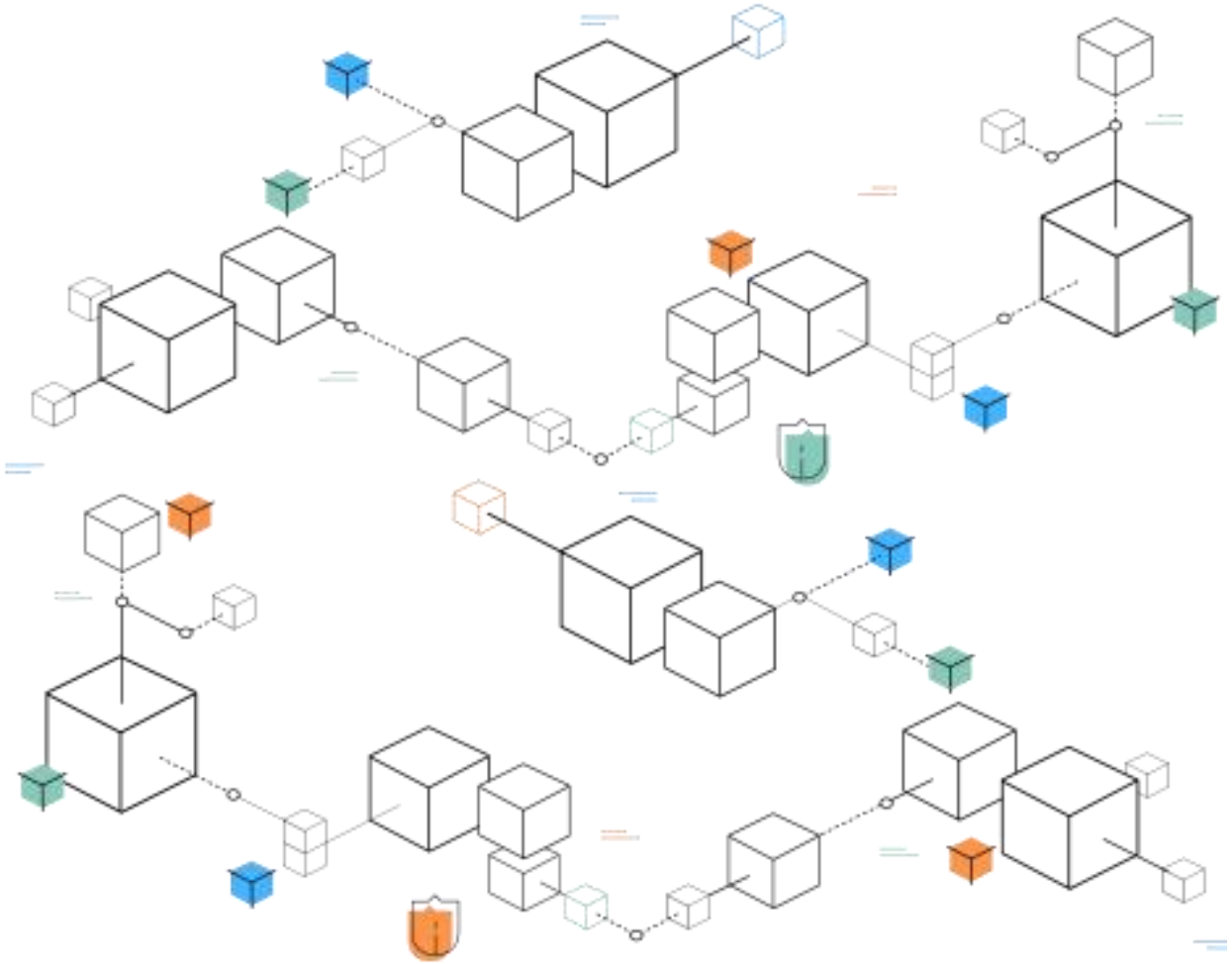
Q & A

要推动**区块链底层技术服务**和**新型智慧城市建设**相结合，探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平。

——习近平总书记 2019.10.24



THANK YOU



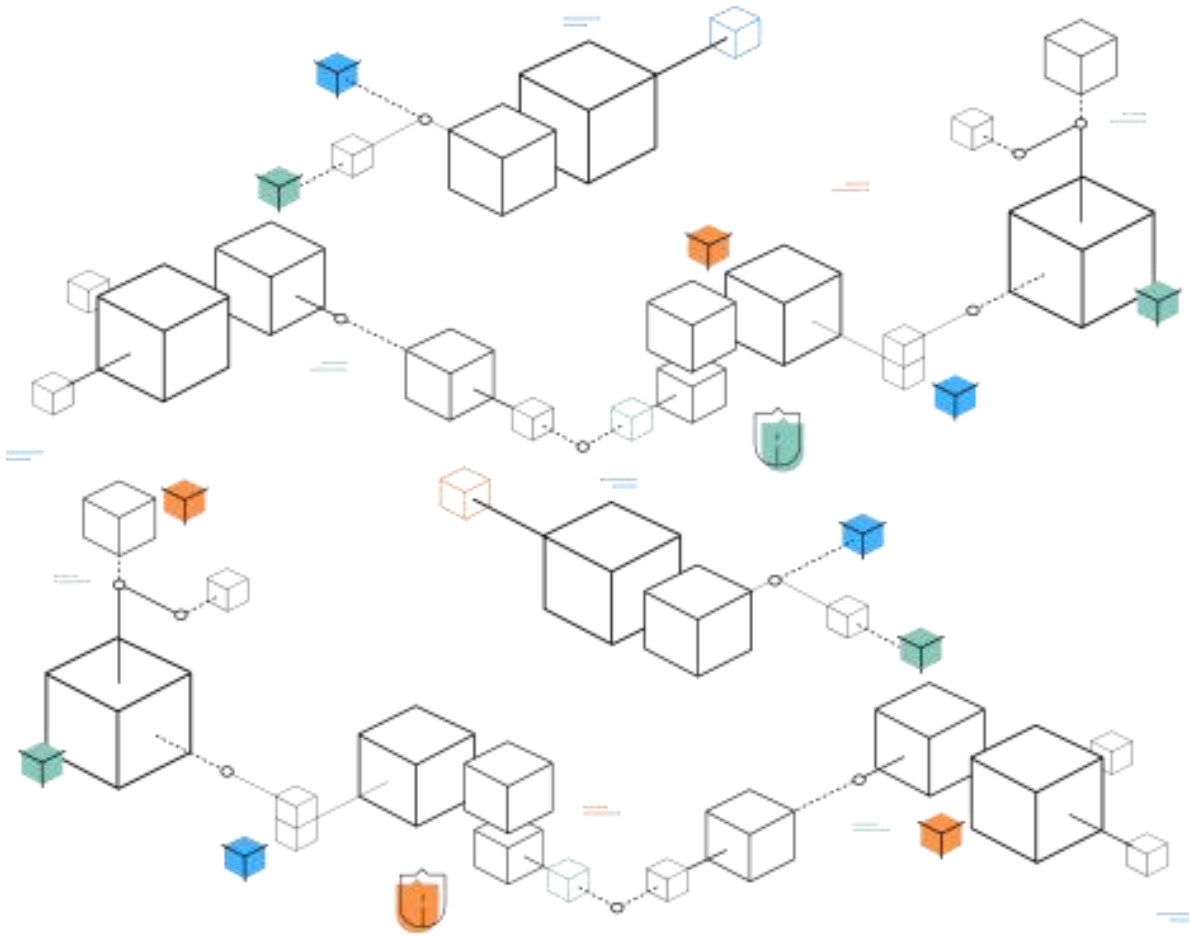
基于密接技术的区块链开发

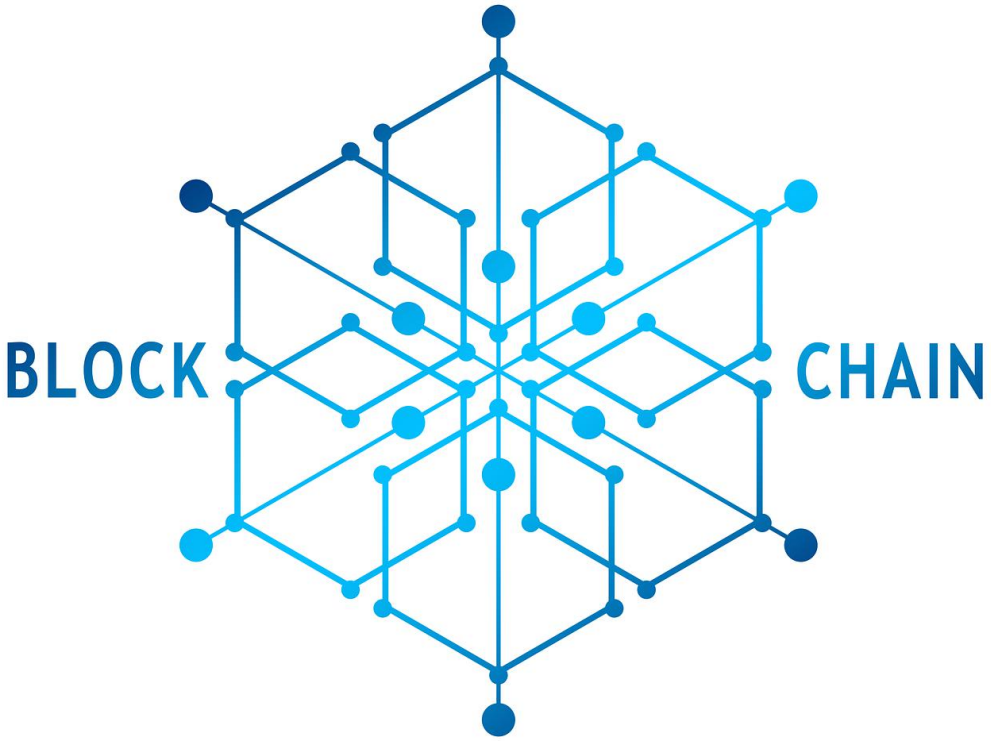
创新实验　第三次项目展示

小组成员：庄湛　邹若彤　潘泰仰

指导老师：宋轩老师　张浩然老师(东京大学)
云沐晟学长(RA)　林贵旭学长(RA)

2020/1/7　创园10栋504





Contents

系统设计：共识算法

POW的改进：通过**密接交互信息**产生的随机项代替计算资源高速生成的随机项进行区块链挖矿

利用密接交互信息具有**有限性**和**多重置信性**

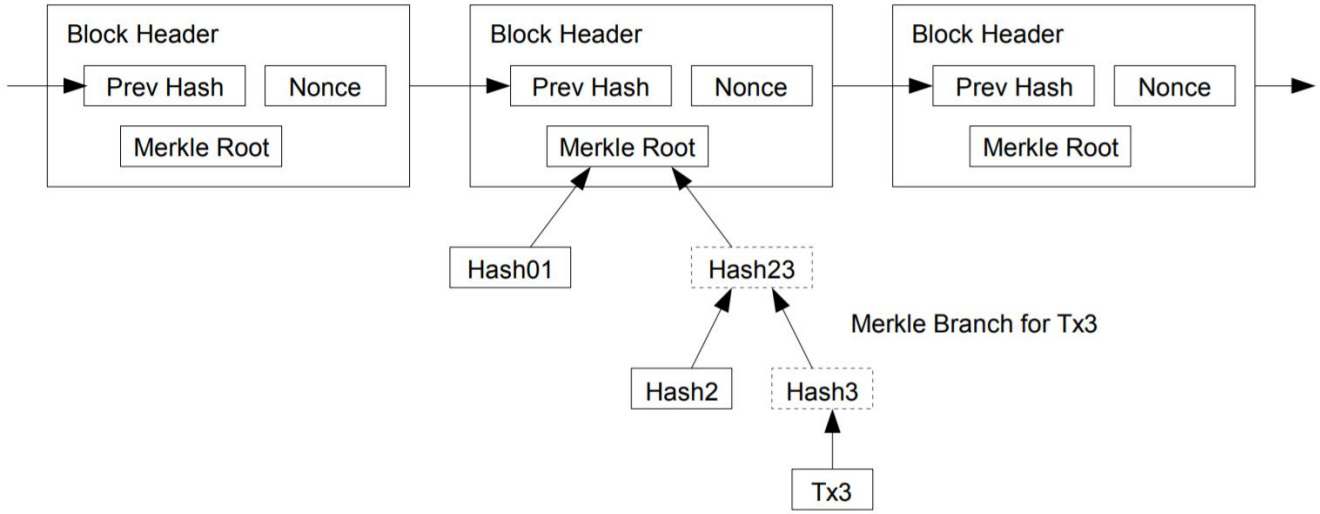


图 1 区块链结构[1]

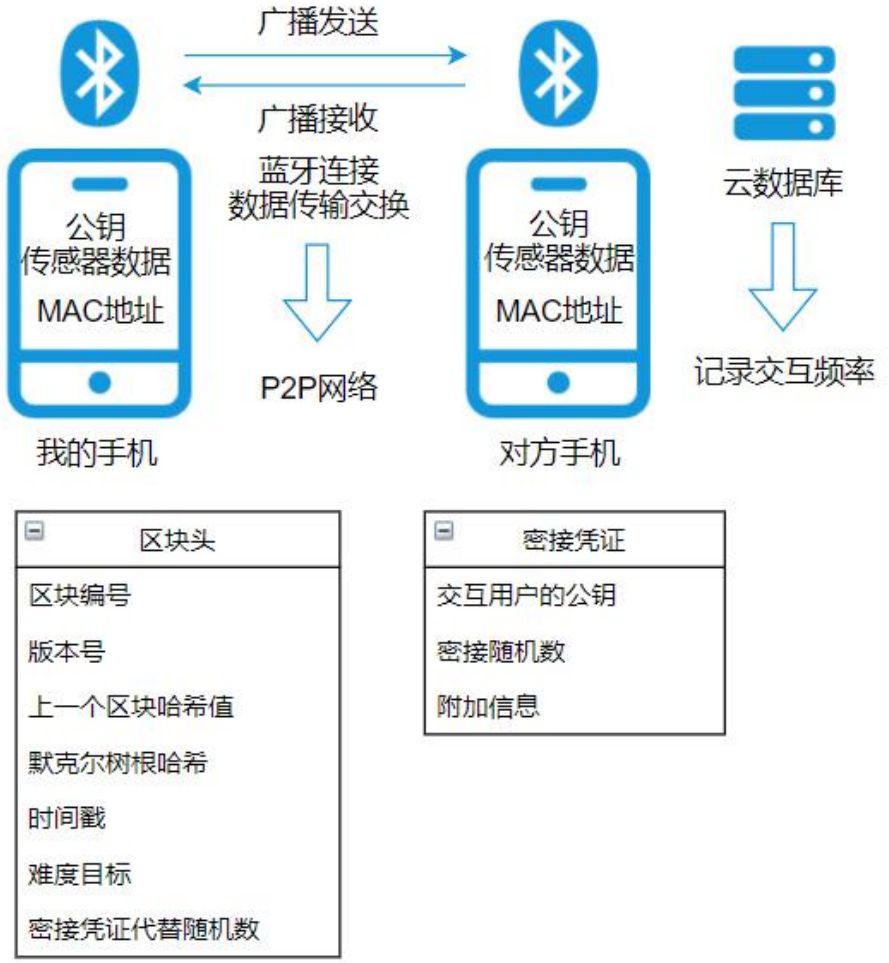


图 2 密接凭证代替方案

[1] Nakamoto S, "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf[Online], 2008

系统设计：共识算法和奖励机制

POS的改进：通过密接发生量代替货币持有量，且密接次数在中等偏上区间拥有更高几率出块(调整奖励和难度)

假设正常人密接次数呈**幂律分布**，利用中位数作为评价基准。

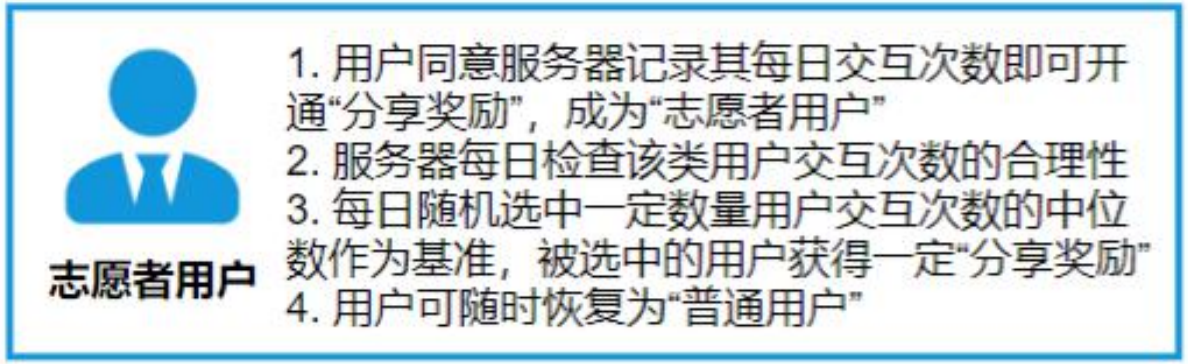


图 3 志愿者用户

出块奖励

出块奖励是用户与其他用户进行密接交互并成功解决区块链哈希难点时所获得的奖励。

打包奖励

用户在成功获得出块奖励的同时获得该奖励。根据打包的交易量可以获得一定的Mcoin奖励

分享奖励

选择一组志愿者用户作为“基准”时，当成功出块时，这组志愿者用户可以获得一定的Mcoin奖励。

系统设计

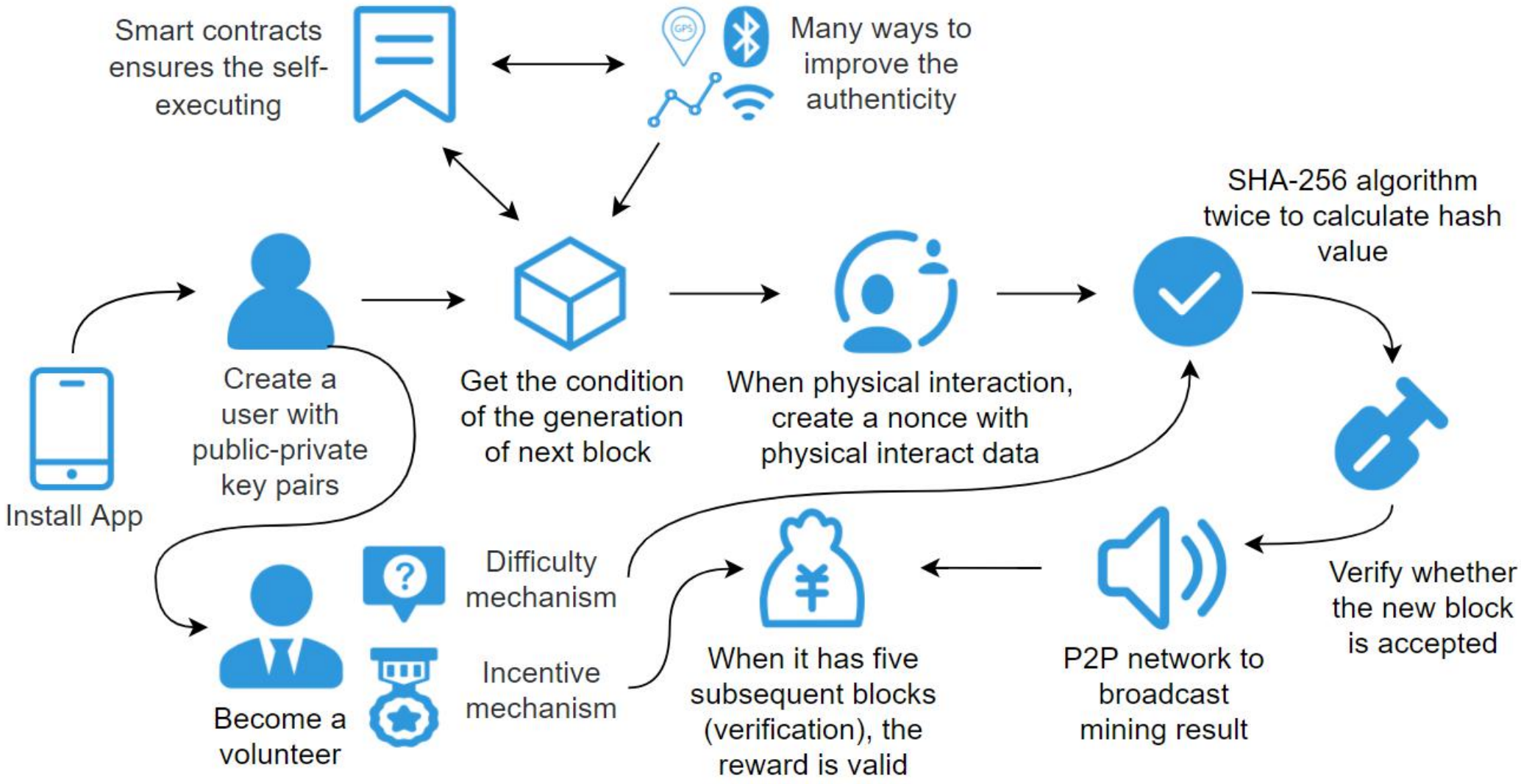
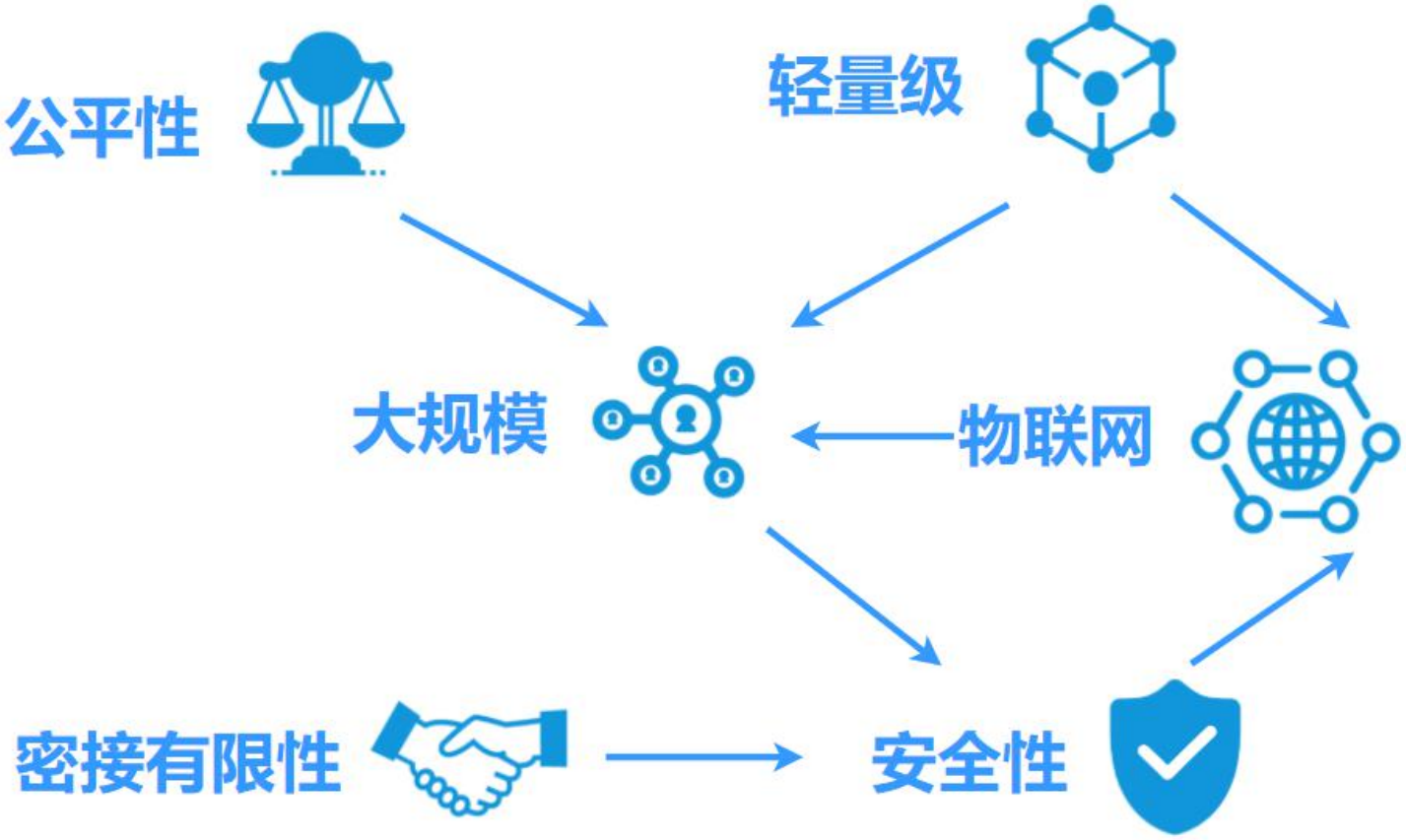

Smart contracts ensures the self-executing
Many ways to improve the authenticity
SHA-256 algorithm twice to calculate hash value
Install App
Create a user with public-private key pairs
Get the condition of the generation of next block
When physical interaction, create a nonce with physical interact data
Verify whether the new block is accepted
P2P network to broadcast mining result
When it has five subsequent blocks (verification), the reward is valid
Difficulty mechanism
Incentive mechanism
Become a volunteer

图 4 系统设计

POPI整体优势

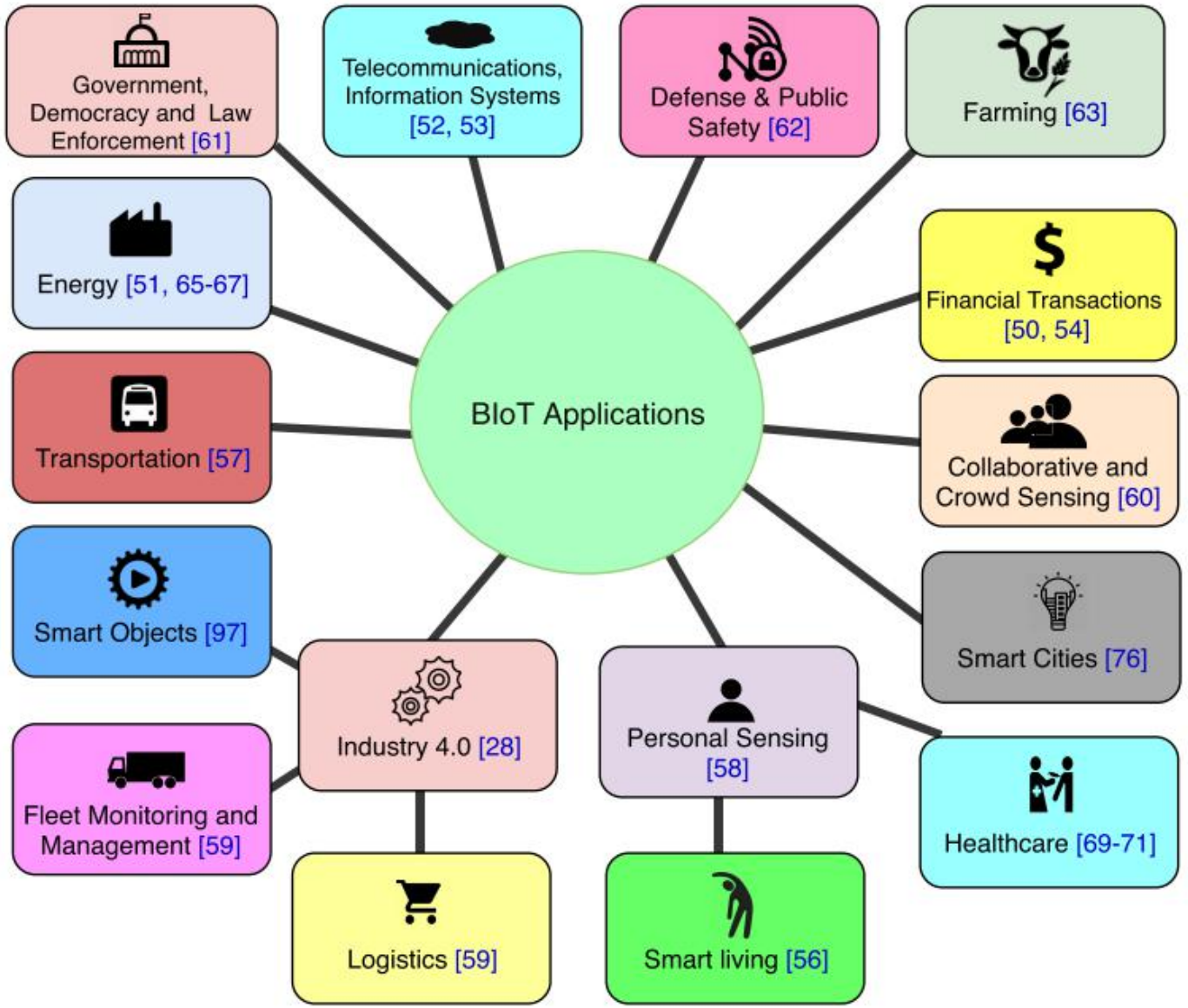
- **轻量级：**带来用户规模
- **安全性：**物理交互有限性
- **公平性：**保证挖矿设备平等
- **低能耗、低时延：**实验证明
- **应用前景：**物联网



POPI整体优势

应用于物联网

- 带来更大用户规模
  安全性更高
- 政府支持
- 资本流入



项目成果

9.1 ~ 9.10

1.初步确定项目方向
2.完成区块链基础知识学习

9.10 ~10.29

1.进一步优化项目思路、确定项目目标
2.写出两篇专利
3.初步写出区块算法、默克尔树等区块链基础代码

10.29 ~ 11.18

1.大量阅读文献，提出基于物理交互信息的新共识机制（POPI）的想法
2.提出新共识机制在物联网上的应用

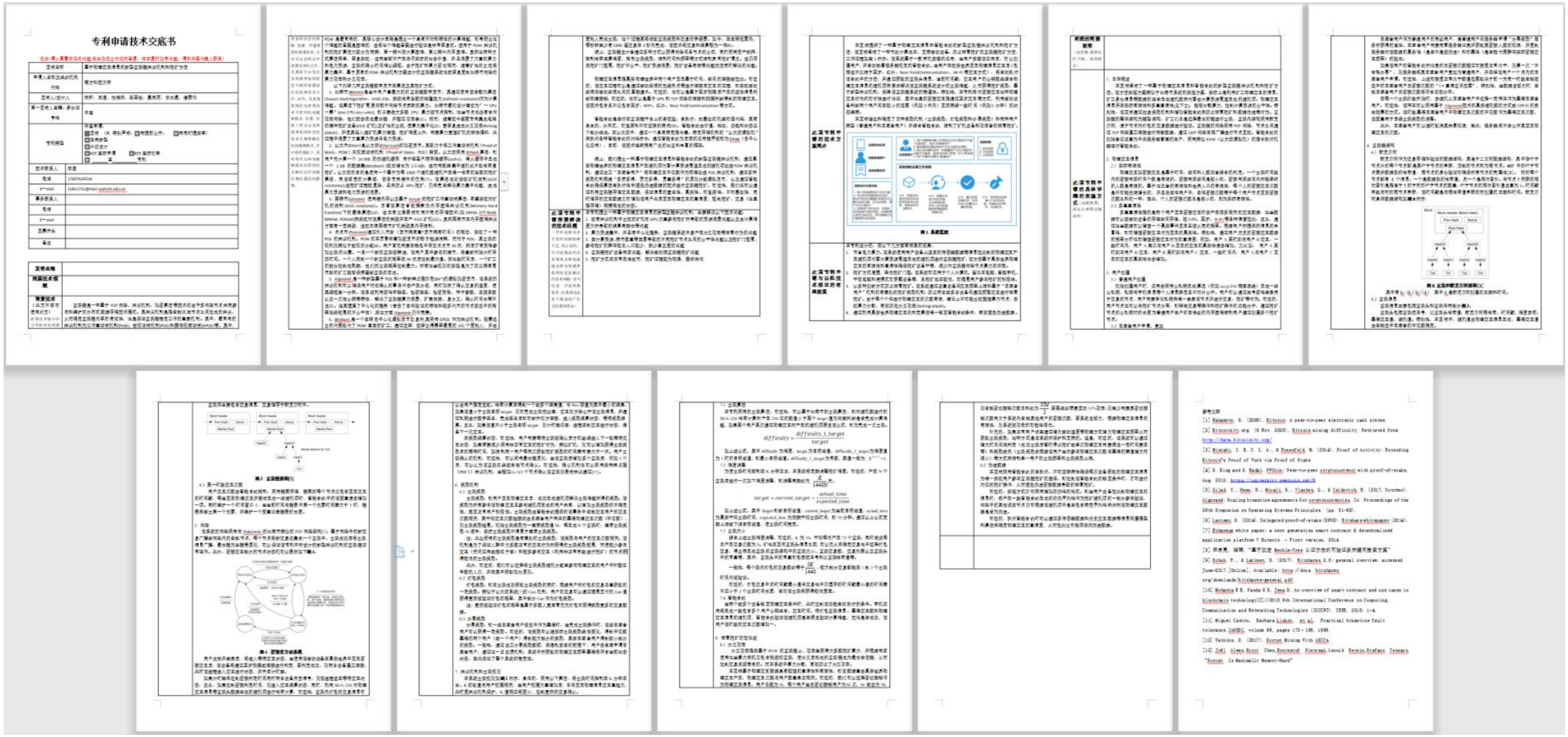
11.18 ~ 12.3

1.完成论文摘要及引言部分
2.进行简单模拟实验判断不同走路方式（走走停停、来回往复、趋向密集）人群密接次数与人数关系

12.3 ~ 1.6

1.完成POW、POS共识机制代码复现
2.完成POPI代码初步实现
3.开发安卓挖矿APP实现移动设备挖矿

专利完成： 基于物理交互信息的新型区块链共识机制和挖矿方法



文献阅读：前沿物联网区块链技术的文献综述

时间	技术	细节
2019.01	Algorand	一个安全和有效的分布式账本，解决了伪三角（去中心化、可扩展性、安全性）
2019.06	PoET	一种基于彩票式共识的**轻量级**共识机制
2019.08	PoRX	一种基于声誉证明的**物联网区块链**的共识机制
2020.03	PoBT	可扩展的基于物联网区块链的**轻量级**共识机制
2020.06	PoWP	一种基于**物理世界**证人在场的增强民主的区块链共识
2020.08	SURFACE	一个用于**现实网络**的实用区块链共识算法
2020.09	PoQF	一种基于**车载自组织网络**和边缘计算的区块链共识机制
2020.11	PoEWAL	一种物联网中区块链的**轻量级共识机制**，基于限时工作和幸运值
2020.11	Blockene	**首个**在**移动手机**上提出的区块链架构

文献阅读: blockene

论文内容：提出了一种低能耗、轻量级移动端设备的区块链移动端模型

受到启发：

1.解决了移动端P2P网络是否成熟的疑问

2.确认POPI主要优势为轻量级与安全性

3.大致确认实验思路和需测试数据

Blockchain	*Scale of members*	*Trans.* rate	*Cost*	*Incentive needed?*
Public (*e.g.*, Bitcoin)	**Millions**	4-10 /sec.	Huge (PoW)	Yes
Consortium (*e.g.*, [13])	Tens	**1000s /sec.**	High	Yes
Algorand [21]	**Millions**	**1000-2000/sec.**	High	Yes
Blockene	**Millions**	**1045 /sec.**	**Tiny**	**No**

Blockene: A High-throughput Blockchain Over Mobile Devices

Sambhav Satija*, Apurv Mehra*, Sudheesh Singanamalla†*, Karan Grover*, Muthian Sivathanu*, Nishanth Chandran*, Divya Gupta*, Satya Lokam*

*Microsoft Research India †University of Washington

Abstract

We introduce Blockene, a blockchain that reduces resource usage at member nodes by orders of magnitude, requiring only a smartphone to participate in block validation and consensus. Despite being lightweight, Blockene provides a high throughput of transactions and scales to a large number of participants. Blockene consumes negligible battery and data in smartphones, enabling millions of users to participate in the blockchain without incentives, to secure transactions with their collective honesty. Blockene achieves these properties with a novel split-trust design based on delegating storage and gossip to untrusted nodes.

We show, with a prototype implementation, that Blockene provides throughput of 1045 transactions/sec, and runs with very low resource usage on smartphones, pointing to a new paradigm for building secure, decentralized applications.

1 Introduction

Blockchains provide a powerful systems abstraction: they allow mutually untrusted entities (*members*) to collectively manage a *ledger* of transactions in a decentralized manner.

All blockchains today require member nodes to run powerful servers with significant network, storage, and compute resources. Blockchains based on *proof-of-work* [5, 30] push resource usage to an extreme, requiring significant compute for puzzle-solving, but even consortium blockchains [13] and blockchains based on *proof-of-stake* [21] incur significant network and storage costs to keep the blockchain up to date at a high transaction throughput. Blockchains today are therefore limited to use-cases where members have a strong incentive to participate, and can hence afford the high resource cost. For example, in consortium blockchains [13], business efficiency improves, while in cryptocurrencies [21, 30], members earn currency.

Interestingly, the high resource requirement of blockchains also weakens *reliability* for several real-world applications. Blockchains require that majority (typically two-thirds) of members are honest, a property that is easier to guarantee when a large number of members participate. However, wide-scale adoption of a blockchain is hard given the high resource requirement, especially in scenarios where members do not have a direct incentive to participate. Not surprisingly, public blockchains with high membership today target cryptocurrencies [5, 30].

In this paper, we present *Blockene*[1], an ultra-lightweight, large scale blockchain that provides high throughput for real-world transactions. By being lightweight and scalable, it enables wide-scale adoption by millions of users. By enabling large scale of participation, *Blockene* makes it plausible to assume honest-majority. By being high-throughput, *Blockene* supports real-world transaction rates.

The key breakthrough in *Blockene* is that instead of requiring members to run powerful servers, *Blockene* is the first blockchain that enables members to participate as first-class citizens in consensus even while running on devices as lightweight as smartphones, lowering cost by orders of magnitude.

Network: Blockchains rely on peer-to-peer gossip between members; at a high transaction rate, gossip would require tens of GBs of data transfer per day; *Blockene* requires only about 60MB of data transfer per day on a smartphone.

Storage: Member nodes in blockchains keep a copy of the entire blockchain (terabytes at high-throughput); in *Blockene*, members incur only a few hundred MBs of storage.

Compute: Even the gossip cost of typical blockchains would drain battery on mobile nodes; *Blockene* ensures that battery drain is less than 3% per day.

Thus, a user incurs no perceptible cost while running *Blockene*. As the low resource usage in *Blockene* makes it feasible even in a smartphone, *Blockene* can also run on desktops, with much lighter resource usage than state-of-the-art.

Blockene achieves three conflicting properties: large scale of participation, high throughput, and lightweight resource usage, catering to even scenarios where there is no direct incentive (*e.g.*, altruistic participation), and handling transactions across variety of use-cases including those on public funds. A comparison of *Blockene* with other blockchain architectures is depicted in Table 1.

Example application: Audited Philanthropy. Charitable donations to non-profits are in excess of USD 500 billion *annually* worldwide [7, 8, 10]. However, from a donor's perspective, the lack of transparency on the end-use of funds makes donations vulnerable to sub-optimal use or mismanagement by non-profits, especially in regions where regulatory enforcement is ineffective or crippled by corruption. A sys-

*Sudheesh was with Microsoft Research India while doing this work.

[1]Named after *Graphene*, one of the lightest and strongest materials.

论文成果：摘要

PoPI: A Lightweight Blockchain Consensus Over Mobile Devices

Abstract—Nowadays, the Internet of Things (IoT) with Cloud App distributed among multiple peers have the trend of becoming the next generation network architecture, and even have the prospect of changing the way of social operation. Blockchain which implements a distributed, traceable and tamper-resistant ledger can not only address the privacy and security concerns in IoT but also combine the smart contract and cryptography technology to develop Blockchain-based IoT ecosystem, which have played an important role in energy, health, supply chain, smart city and other fields. However, for the blockchain based on the existing consensus mechanism, there are disadvantages such as small scale, waste of resources and the inequity caused by centralization trend. In this article, we propose a universal and lightweight proof of physics interaction (PoPI) consensus mechanism and its integration framework based on a mobile device app. Also, we propose the incentive mechanism and difficulty mechanism based on a volunteer mechanism to guaranteed the robustness. Through theoretical derivation and experimental results of a certain scale of volunteers in SUSTech, we demonstrate the scalability of this solution. Furthermore, PoPI is compared with some existing consensus mechanisms in terms of energy, consensus time, and network latency.

Index Terms—Internet of Things (IoT), blockchain, consensus mechanism, physical interaction, mobile device, scalability

摘要

区块链是一种分布式、可跟踪、抗篡改的账本，其实现了安全的加密货币交易。如今，将云功能分布在多个对等节点的物联网有成为下一代网络架构的趋势，甚至有改变社会运作方式的前景。利用区块链技术，不仅可以解决物联网中的隐私和安全问题，还可以结合智能合约和加密技术，构建基于区块链的物联网生态系统，在能源、健康、供应链、智慧城市等领域已经发挥了重要作用。然而，基于现有的共识机制，区块链存在规模小、资源浪费、集中化趋势带来的不公平等弊端。本文提出了一种通用的、轻量级的基于移动设备应用的物理交互证明(PoPI)共识机制及其集成框架，并提出了基于志愿者机制的激励机制和难度调整机制以保证系统的鲁棒性。本文通过理论推导和一定规模志愿者的实验结果，证明了该解决方案的可扩展性，并将 PoPI 与现有的共识机制在能耗、共识时间和网络延迟等方面进行了比较。

论文成果：介绍

PoPI: A Lightweight Blockchain Consensus Over Mobile Devices

Zhan Zhuang, Ruotong Zou, Taiyang Pan

***Abstract*—Nowadays, the Internet of Things (IoT) with Cloud App distributed among multiple peers have the trend of becoming the next generation network architecture, and even have the prospect of changing the way of social operation. Blockchain which implements a distributed, traceable and tamper-resistant ledger can not only address the privacy and security concerns in IoT but also combine the smart contract and cryptography technology to develop Blockchain-based IoT ecosystem, which have played an important role in energy, health, supply chain, smart city and other fields. However, for the blockchain based on the existing consensus mechanism, there are disadvantages such as small scale, waste of resources and the inequity caused by centralization trend. In this article, we propose a universal and lightweight proof of physics interaction (PoPI) consensus mechanism and its integration framework based on a mobile device app. Also, we propose the incentive mechanism and difficulty mechanism based on a volunteer mechanism to guaranteed the robustness. Through theoretical derivation and experimental results of a certain scale of volunteers in SUSTech, we demonstrate the scalability of this solution. Furthermore, PoPI is compared with some existing consensus mechanisms in terms of energy, consensus time, and network latency.**

***Index Terms*—Internet of Things (IoT), blockchain, consensus mechanism, physical interaction, mobile device, scalability**

I. Introduction

A. Background

Blockchain implements a distributed,traceable and tamper-resistant ledger. Most blockchains existing today needs their users to run a powerful server or needs significant compute resources because they are basing on PoW(proof-of work) or other similar consensus mechanism.

One the one hand, these compute-intensive blockchains maks a large resource consumption, which causes they are mostly using in cryptocurrencies or other high earning applications. The high threshold of those blockchain applications is also preventing those who do not have a powerful client to be their member.

On the other hand, the difficulty in computing of those blockchains also lead to another problem that the reliability of them can be reduced. One of the widely known example is the 51-percent-attack. Blockchains usually require majority of members to be honest. This can works easily when the member amount is huge. But obviously, the high threshold blockchains cannot be adopted widely and only a small number of members can participate, especially in those don't have a high earning applications to attract new members.

In this paper, we offered a light-weight blockchain consensus, which provide a possibility to being high-throughput. The most difference is that it can run on the IoT devices instead of requiring a huge mount of computing-unit, which makes the spreading possible. One of the most common application is running on the smart phone. It makes the cost of participation lower than ever before. And the explosive increase of the members can significantly increase the reliability of the system.

B. Literature review

To ensure that the ledger recorded by the nodes in the system are whole, timely, and creditable, blockchain systems typically use a consensus mechanism to dictate which bookkeepers can record the data on the blockchain.

The most idealistic consensus mechanism is like democratic voting, which means everyone can vote, and everyone has the same voting weight. This scheme may be possible to implement in a real world, but, in a public blockchain, it is hard to find a strategy that can not only attract and motivate users to participate in the maintenance of the blockchain system but also ensure a relatively level playing field for each user.

For the blockchain based on mobile devices, we also need to consider its battery consumption, throughput, latency and scalability. In recent years, many new consensus mechanisms based on the IoT have been proposed. Meanwhile, some blockchain systems based on mobile devices were proposed by Sambhav Satija et al. Below, we will analyze several existing consensus mechanisms and blockchain systems.

1) Proof of Work (PoW): PoW is applied in Bitcoin successfully. Its core idea is to distribute the block accounting rights through the competition of computing power among nodes. After a block is generated, the message would be broadcasted to the entire network for verification by other nodes. However, the generation of blocks requires a lot of computational power, and the block confirmation time delay is too much, resulting in low efficiency, low transaction throughput, thus it cannot adapt to many real scenarios.

2) Proof of Stake (PoS): PoS is an alternative protocol for PoW, without the problem of too much computation cost and consensus time delay. The main idea of PoS is that the proportion of users' stake in the system is inversely proportional to the difficulty of block generation. The larger the stake held by nodes in the system, the easier he wins.

3) Proof of Activity (PoA): PoA is a protocol that combines PoW and PoS. It is base on a hypothesis of economic phenomenon known as the "tragedy of the commons". The proposed PoA protocol aims to increase attack costs of malicious miners by forcing them to achieve eight times hash rate than the honest miners in the network. In addition, it reduces computational complexity to 1/10 of Bitcoin PoW, minimizing energy consumption. However, the proof of activity is also intended to protect only cryptocurrency applications.

4) Proof of Authority (PoAu): In PoAu blockchain, which be viewed as protected by trusted validation nodes, miners were chosen as the verifiers of the block on the basis of personal credibility. Compared with PoW and PoS, the PoAu is more energy friendly, but it still has large delays and energy costs. Because a node with a high authority is not necessarily evil and becoming a verifier requires a lot of conditions which reveals the real identity, the consensus mechanism is controversial in terms of security and privacy, and is not suitable for large-scale blockchain.

5) Proof of Block and Trade (PoBT): PoBT is a lightweight consensus algorithm for scalable IoT blockchain which allows validation of transactions and blocks and incorporates peers based on the number of nodes participating in a session to reduce the computing time. it is considered a absolute consensus and suitable for the blockchain systems on the IoT.

6) Proof of Elapsed Time (PoET): In PoET, every node in the network generates random time. After this, everyone goes to sleep for that random time. Whoever wakes up first, can mine the block. It is used in a cooperative environment or requires a trusted setup for removing malicious attacks. However, it is an absolute consensus method that can only be used in a cooperative environment.

7) Proof of Reputation-X (PoRX): PoRX is a blockchain consensus mechanism on the IoT based on a proof of reputation. It uses some rules to control the reputation, such as adjusting the reputation based on the number of self-generated blocks and malicious behaviors of a user. Experimental results show that the scheme can effectively stimulate the cooperative behavior of nodes in the network and avoid the Matthew effect usually in the PoS consensus mechanism. However, this consensus mechanism has a high latency due to the need to check and modify reputation values multiple times.

8) Proof of Witness Presence (PoWP): PoWP proposed the presence of a witness based on the scanning of the code as the basis for democratic voting. This dynamic solution enhances democracy and fairness by verifying the physical existence of location. Theoretically, it is an advanced consensus mechanism. However, the scanning method according to the scenic spot has limitations, and it is easy to generate data forgery and other attacks.

9) Proof of Elapsed Work and Luck (PoEWAL): PoEWAL is a lightweight probabilistic consensus algorithm for non-cooperative cases based on proof of elapsed work and proof of luck mechanisms. Moreover, it has little energy consumption, latency and consensus time for mining and sending transactions to other nodes. However, its incentive mechanism is mainly two kinds of energy-saving incentives, which cannot be applied to mobile devices.

10) Algorand: Algorand uses verifiable random function (VRF) by randomly selecting a group of users in a decentralized way. VRF selects users based on the amount of money stored in their wallet. These users mine the new block using the byzantine agreement. It does not require high computational power, but needs a monetary system and has a large latency delay.

11) Byzantine Fault Tolerance(BFT): BFT needs all the nodes of the network have to take part in the voting to mine the new block, but the consensus is reached only when less than one-third nodes behave maliciously. It is not suitable for the Non-cooperative IoT blockchain network.

C. Key techniques in PoPI

In PoPI consensus, a nonce is created when physical interaction (detected by bluetooth technology) occurs. If the hash value of block header is no more than the current mining difficulty, a new block is created. The new block requires double verification. The system adopts communication technologies (such as Bluetooth, WIFI and GPS) together with time stamp to verify if the nonce is authentically created according to physical interactions. In addition, P2P network broadcasts the block information to nodes, and they will perform transaction validation.

When five subsequence blocks are verified, the block reward is valid. To avoid malicious physical interaction, we stipulate that the user gets higher block reward if the number of his physical interaction is slightly above the median. Additionally, users who volunteer to provide their number of physical interaction can get extra reward. The reward will be discussed in . . . (e.g. § 4.2) in detail.

D. Contribution

Compared to a traditional financial transaction model, our decentralized system does not have to rely on a trustworthy third party and the transaction information is impossible to be modified. Compared to PoW, our consensus produces nonce according to physical interaction, which is less energy consuming. Compared to PoWP (Proof of Witness Presence), our consensus is more scalable and easier for miners to get involved. In summary, the contributions of this paper are outlined as follow:

- We provide a new blockchain system consensus "Proof of Physics Interaction" based on PoW, and theoretically proof how it realizes.
- We provide a new blockchain integration framework with the characteristics of fairness and safety.
- We provide a new communication network with low energy consumption and short latency.
- A thorough empirical experiment is performed to demonstrate the scalability and high performance of the system.
- A lightweight blockchain architecture that leads to scale and security.

代码展示：POW复现

```python
from hashlib import sha256
import time

class BlockforPOW:
    #初始化函数用来定义一个区块需要哪些信息（这个你们可以自定义）
    def __init__(self,index, timestamp, data, previousHash="" ):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previousHash = previousHash
        self.nonce = 0
        self.hash = self.calculateHash()
    #这里是POW的核心，也就是使用一种多劳多得的，不可取巧的计算算法（BTC定义的是SHA256）
    def calculateHash(self):
        #这里不够严谨，最严谨的方式是加上prehash来一起计算hash值！！！！！！！！！！！！
        plainData = str(self.index) + str(self.timestamp) + str(self.data) + str(self.nonce)
        #print("此时的区块头为："+plainData)
        return sha256(plainData.encode('utf-8')).hexdigest()
    #这里我是参考了网上的代码用到了固定难度以控制变量，但是这个变量后期是可以改变的
    #具体方法为：目前difficulty是一个数字，它代表需要多少位前置0来满足难度，并且因为是单人模式，所以这边的挖矿策略是+1的方法，实际上挖矿的策略是自带no
    def minerBlock(self, difficulty):
        while (self.hash[0:difficulty] != str(0).zfill(difficulty)):
            self.nonce += 1
            self.hash = self.calculateHash()
    #此处是用来设计输出的str
    def __str__(self):
        return str(self.__dict__)
```

```python
class BlockChain:
    #目前先设置固定难度5
    def __init__(self):
        self.chain = [self.createGenesisBlock()]
        self.difficulty =5
    #生成初始块
    def createGenesisBlock(self):
        print("开始生成创世区块")
        return BlockforPOW(0, str(time.time()), "genesis block")
    #获得链内最后一块
    def getLatestBlock(self):
        return self.chain[len(self.chain) - 1]

    #这里是区块链的核心，目前没有多用户，所以写的是单人模式！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！！
    def addBlock(self, newBlock):
        newBlock.previousHash = self.getLatestBlock().hash
        newBlock.minerBlock(self.difficulty)
        self.chain.append(newBlock)

    def __str__(self):
        return str(self.__dict__)

    #验证区块是否被恶意篡改，这里不够严谨，不光是计算前后的hash值是否变动，应该测试用前面的hash是否能算出现在的hash的值！！！！！！！！！！！！！！！！！！
    #此外这里还需要验证前后index，一共三步来验证是否判断准确。
    def chainIsValid(self):
        for index in range(1, len(self.chain)):
            currentBlock = self.chain[index]
            previousBlock = self.chain[index - 1]
            if (currentBlock.hash != currentBlock.calculateHash()):
                return False
```

代码展示：POW结果

```
开始生成创世区块
start to miner first block time :1609992314.9441216
miner first block time completed,used 4.29850435256958s
start to miner second block time :1609992319.242626
miner second block time completed,used 0.8088381290435791s

print block info ####:



{'index': 0, 'timestamp': '1609992314.9431248', 'data': 'genesis block', 'previousHash': '', 'nonce': 0, 'hash': '70800c1439b7b4b7f43e5e7cd2ca7e500f44a5260268d7e70602a8ba75e74b5d'}


{'index': 1, 'timestamp': '1609992314.9441216', 'data': '{amount:4}', 'previousHash': '70800c1439b7b4b7f43e5e7cd2ca7e500f44a5260268d7e70602a8ba75e74b5d', 'nonce': 1714195, 'hash': '


{'index': 2, 'timestamp': '1609992319.242626', 'data': '{amount:5}', 'previousHash': '000004146e1f20fa2e4bf11e28c509f542dfd4502da153a83b435ae8b1954206', 'nonce': 325806, 'hash': '00
before tamper block,blockchain is valid ###
True
after tamper block,blockchain is valid ###
False

Process finished with exit code 0
```

代码展示：POS复现

```
def __init__(self):
    self.chain = [self.createGenesisBlock()]


def createGenesisBlock(self):
    print("开始生成创世区块")
    return BlockforPOS(0, str(time.time()), "genesis block","0000",15)

def getLatestBlock(self):
    return self.chain[len(self.chain) - 1]
# 这里是POS的核心，这里要挑选出哪个结点拥有记账权
def choosecandidate(self, validator=[BlockforPOS]):
    count = 0
    stakerecord = []
    while (count < len(validator)):
            coinnum=validator[count].getbalance()
            print("第"+str(count)+"个候选区块的代币数是："+str(coinnum))
            for i in range(coinnum):
                stakerecord.append(validator[count])
            count+=1
            print("此时count为："+str(count))
    index=random.randint(0,len(stakerecord))
    winner=stakerecord[index]
    print("胜出者的地址是" + winner.getaddress())
    return winner


def addBlock(self, candicates=[BlockforPOS]):
    newBlock=self.choosecandidate(candicates)
    newBlock.previousHash = self.getLatestBlock().hash
    self.chain.append(newBlock)
```

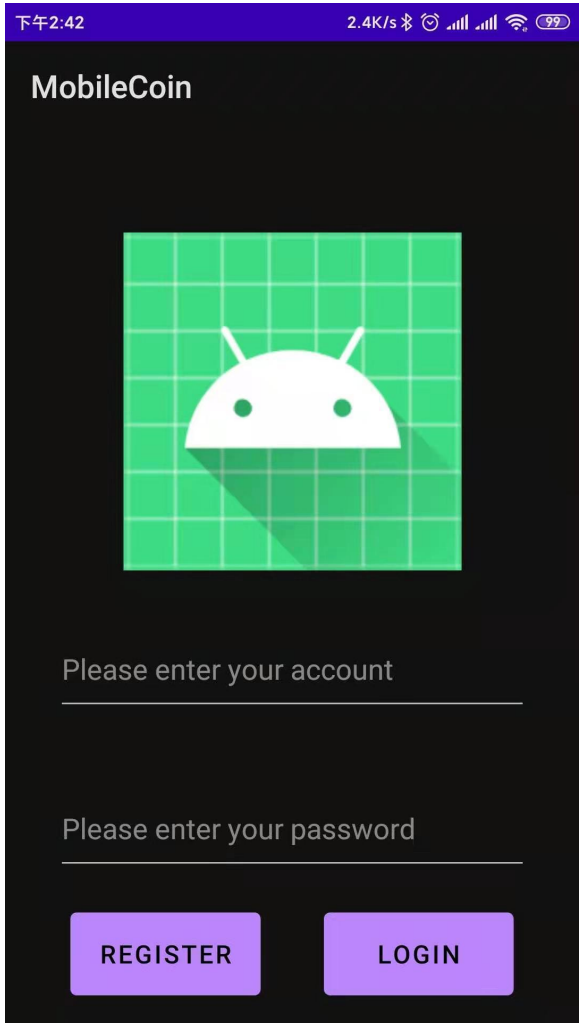
```
class BlockforPOS:
    #初始化函数用来定义一个区块需要哪些信息（这个你们可以自定义）
    def __init__(self,index, timestamp,data, address="", balance=int,previousHash=""):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previousHash = previousHash
        self.address = address
        self.balance =balance
        self.hash = self.calculateHash()



    #这里是把nonce换成了address来求该区块的hash值，每个区块还是要有自己的hash值的
    def calculateHash(self):
        #这里不够严谨，应该加入prehash来计算！！！！！！！！！！！！！！！！！！
        plainData = str(self.index) + str(self.timestamp) + str(self.data) + str(self.address)
        return sha256(plainData.encode('utf-8')).hexdigest()

    #这里是
    def getbalance(self):
        return self.balance

    def getaddress(self):
        return self.address

    #此处是用来设计输出的str
    def __str__(self):
        return str(self.__dict__)
```

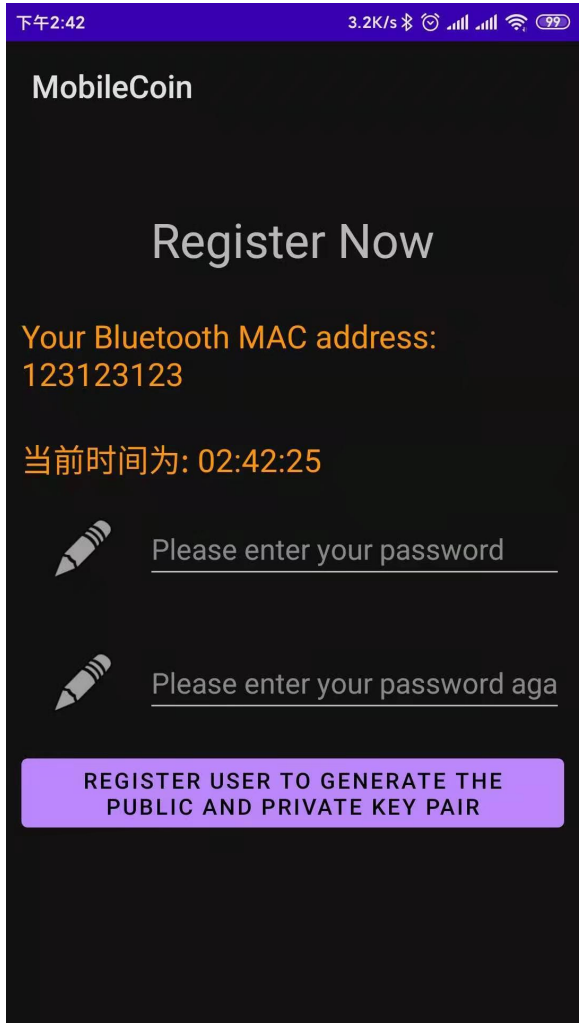
代码展示：POS结果

```
D:\programe\py_project\pythonProject\Scripts\python.exe D:/programe/pythonProject/POS/test.py
开始生成创世区块
start to miner first block time :1609992580.3130965
第0个候选区块的代币数是：2
此时count为：1
第1个候选区块的代币数是：1
此时count为：2
第2个候选区块的代币数是：3
此时count为：3
第3个候选区块的代币数是：10
此时count为：4
胜出者的地址是0004
miner first block time completed,used 0.0s
start to miner second block time :1609992580.3130965
生成候选区块0
生成候选区块1
生成候选区块2
生成候选区块3
第0个候选区块的代币数是：200000
此时count为：1
第1个候选区块的代币数是：100000
此时count为：2
第2个候选区块的代币数是：300000
此时count为：3
第3个候选区块的代币数是：10000
此时count为：4
胜出者的地址是0001
miner second block time completed,used 0.05684781074523926s

print block info ####:
```

代码展示：安卓app - 登录界面

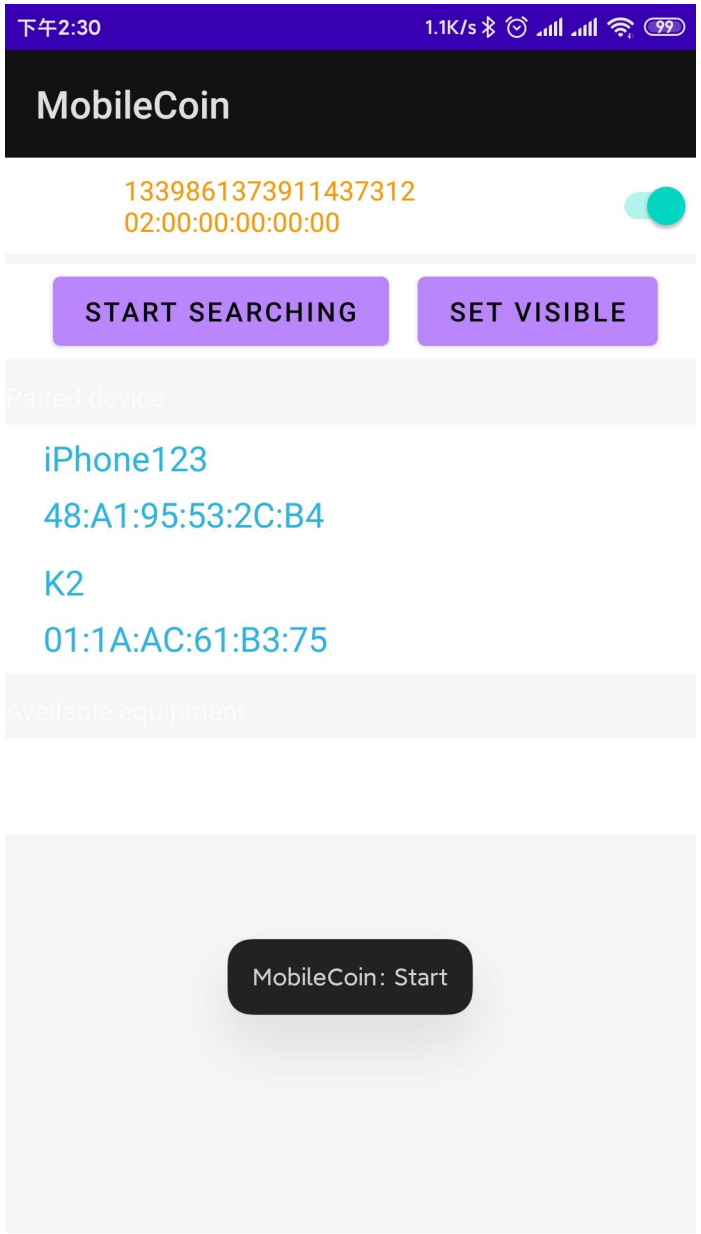
```
23  public class Login extends AppCompatActivity {
24      private EditText account; //账号输入框
25      private EditText password;//密码输入框
26      private Connection conn;
27      private String passwordNumber;
28      private String accountNumber;
29      @Override
30      protected void onCreate(Bundle savedInstanceState) {...}
40
41      @Override
42      protected void onDestroy() {...}
54
55      public void click(View view) {...}
80
81      public void register_click(View view) {...}
85
86      public static String[] checkPassword(Connection conn, String nam
109
110     class Task extends AsyncTask<Void, Void, Void> {...}
145 }
```





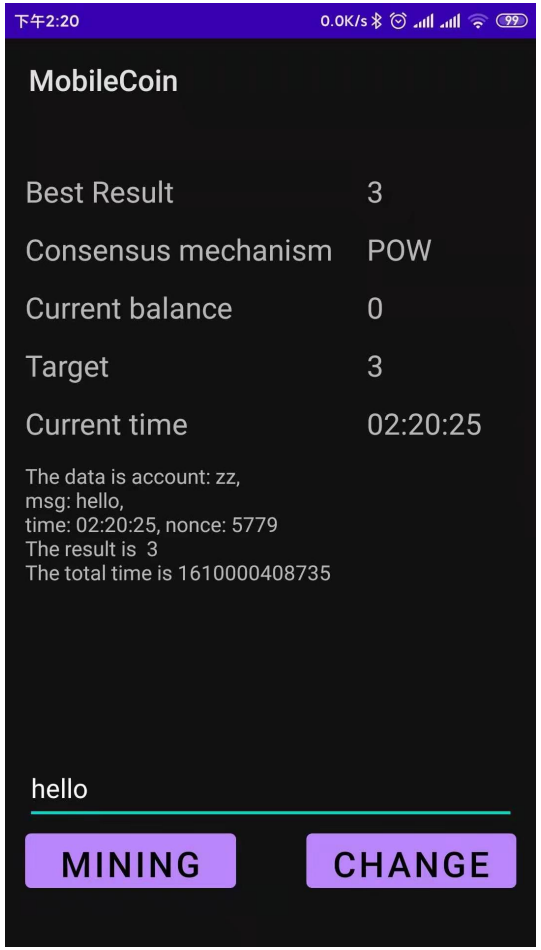
代码展示：安卓app - 基于蓝牙密接判定

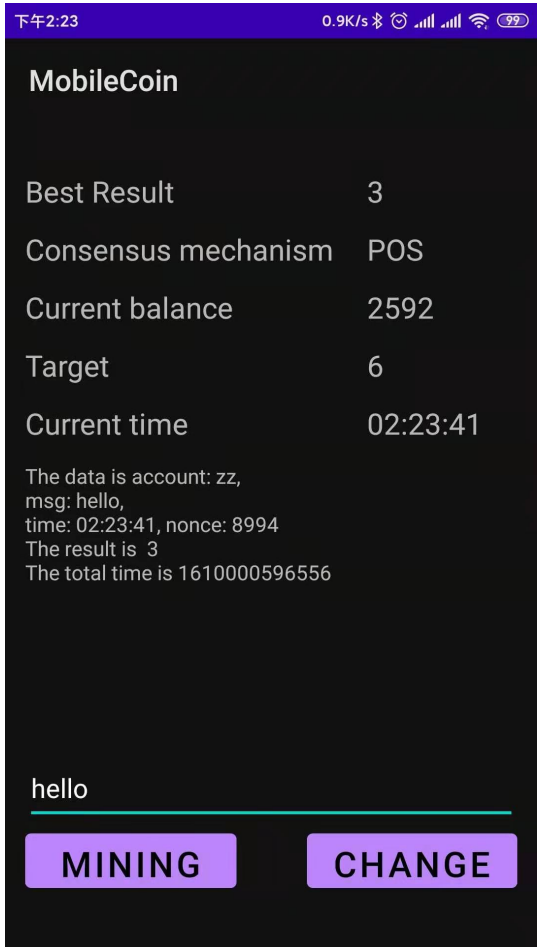
```
52      @Override
53      protected void onCreate(Bundle savedInstanceState) {...}
59
60      private void initView() {...}
70
71  @   private final BroadcastReceiver mReceiver = (context, intent) → {
74              String action = intent.getAction();
75              boolean judge = BluetoothDevice.ACTION_FOUND.equals(action);
76              if (judge) {...}
93      };
95
96      private void initEvent() {...}
162
163     @Override
164     protected void onResume() {...}
171
172     private void ensureDiscoverable() {...}
180
181     @Override
182     protected void onDestroy() {...}
189
190     class MyAdapter extends RecyclerView.Adapter<MyAdapter.ViewHolder> {...}
239 }
```



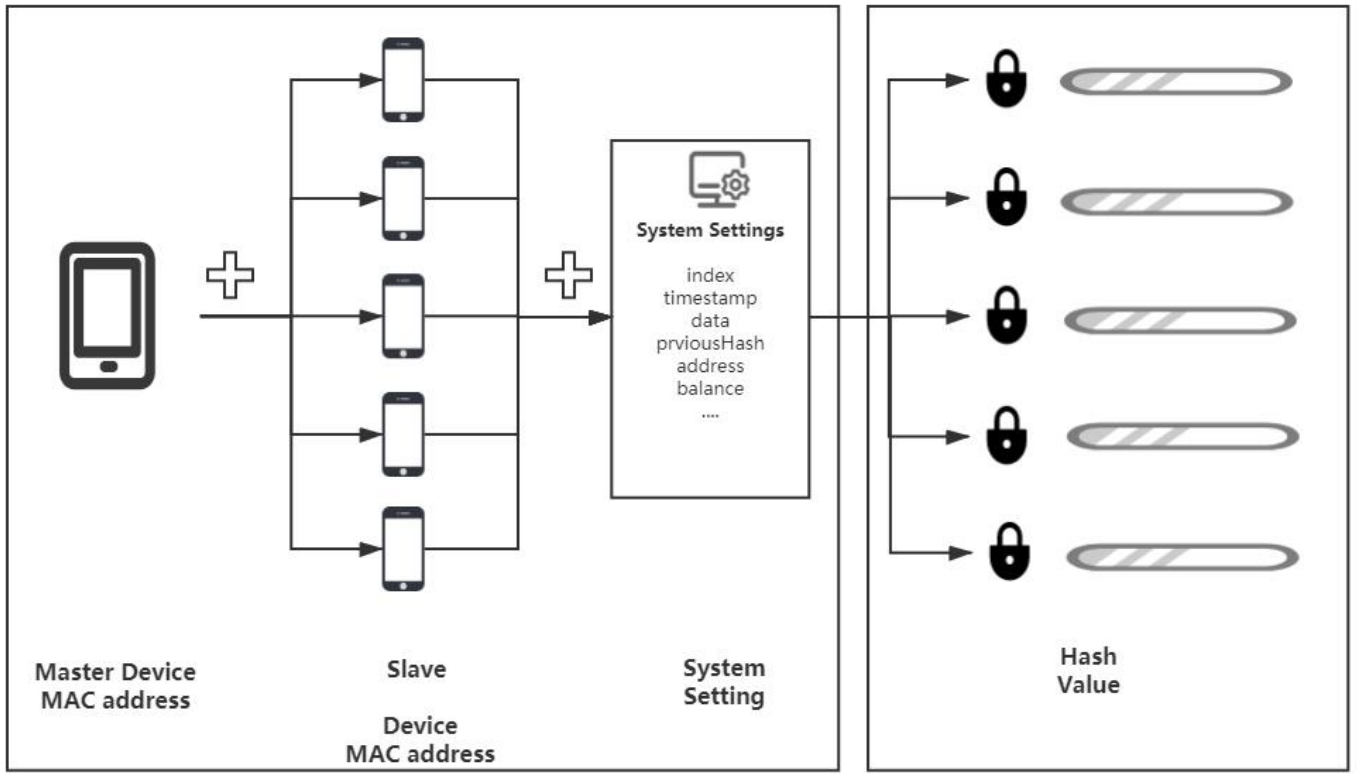
代码展示：安卓app - 共识机制（多机测试未完成）

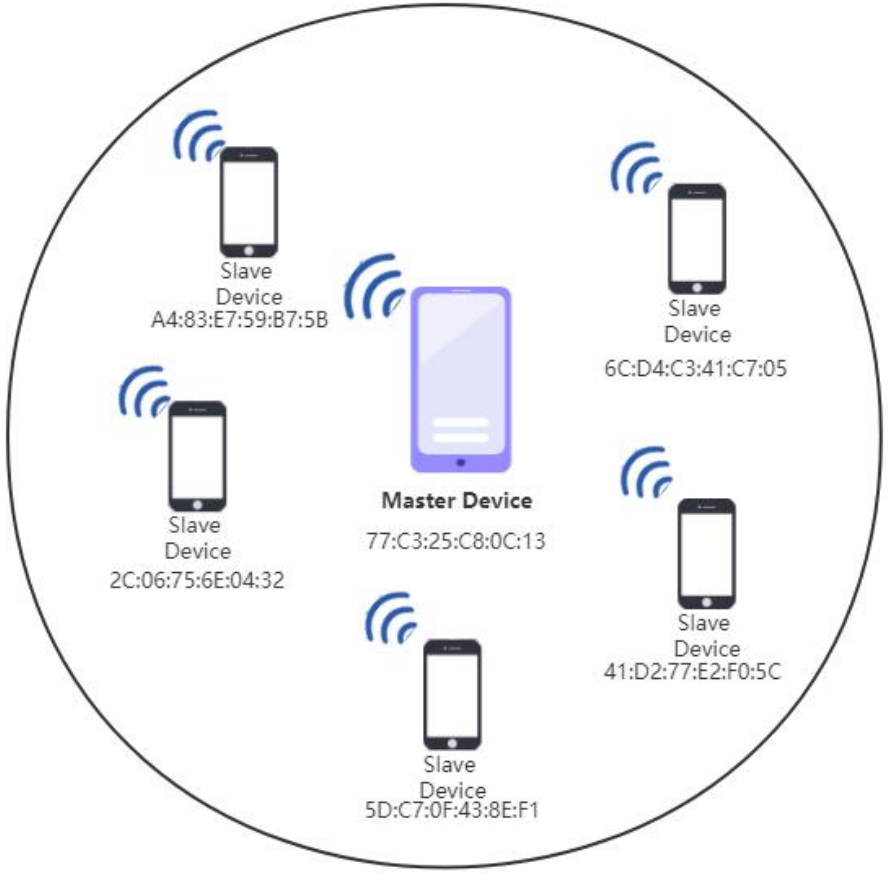
```
38      @Override
39      protected void onCreate(Bundle savedInstanceState) {...}
51      private void Init_view() {...}
60      public void mining(View view) {...}
92      public void change(View view) {...}
119
120     //
121     class Thread_POS extends Thread{...}
164     class Thread_POW extends Thread{...}
210     class Thread_POEWAL extends Thread{...}
256     public void Thread_POPI(){...}
278 @   private static String getDatagram(String account, String m
281 @   private static String getMAC(){...}
293 @   private static String getResult(String datagram, int res,
298     static class Encrypt {...}
338 }
```





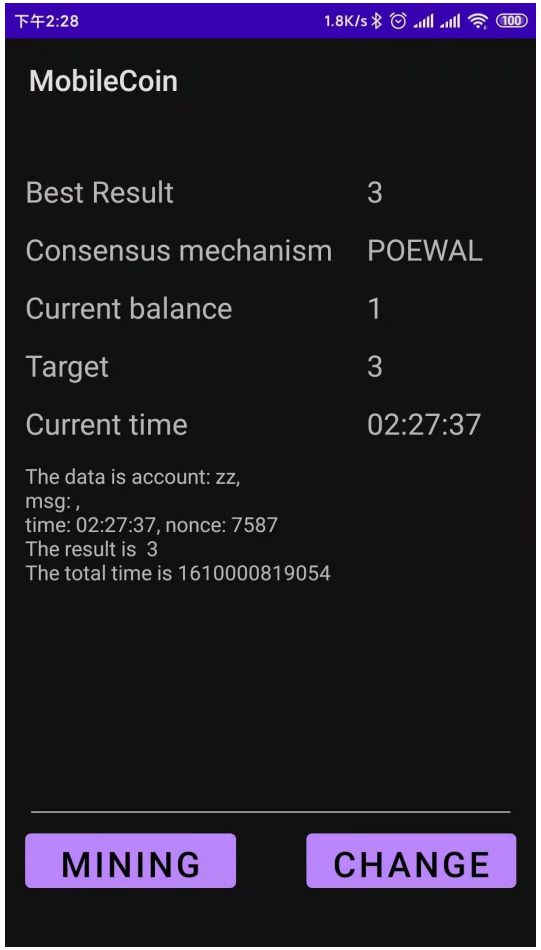
代码展示：安卓app - 共识机制（多机测试未完成）

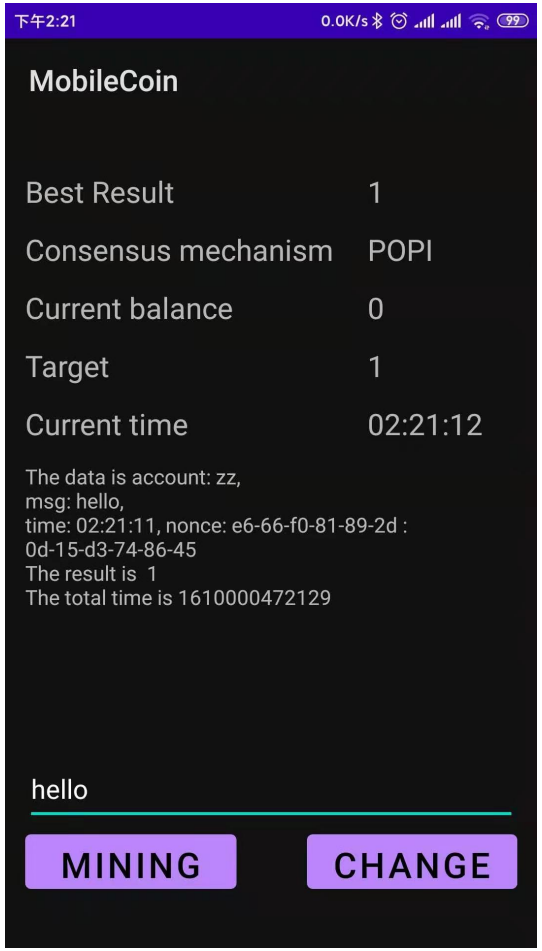




代码展示：安卓app - 共识机制（多机测试未完成）

```
38      @Override
39      protected void onCreate(Bundle savedInstanceState) {...}
51      private void Init_view() {...}
60      public void mining(View view) {...}
92      public void change(View view) {...}
119
120     //
121     class Thread_POS extends Thread{...}
164     class Thread_POW extends Thread{...}
210     class Thread_POEWAL extends Thread{...}
256     public void Thread_POPI(){...}
278 @   private static String getDatagram(String account, String m
281 @   private static String getMAC(){...}
293 @   private static String getResult(String datagram, int res,
298     static class Encrypt {...}
338 }
```





总结与展望

- 学期初所定目标基本完成
- 中期项目进度略微拖沓，熬夜赶ddl的次数较多
- 寒假将继续完成论文写作（等待真人密接实验结果）
- 寒假将继续完成基于拜占庭的Mcoin手机App

参考文献

[1] Nakamoto S, "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf[Online], 2008

[2] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. Ieee Access , 6 , 32979-33001.

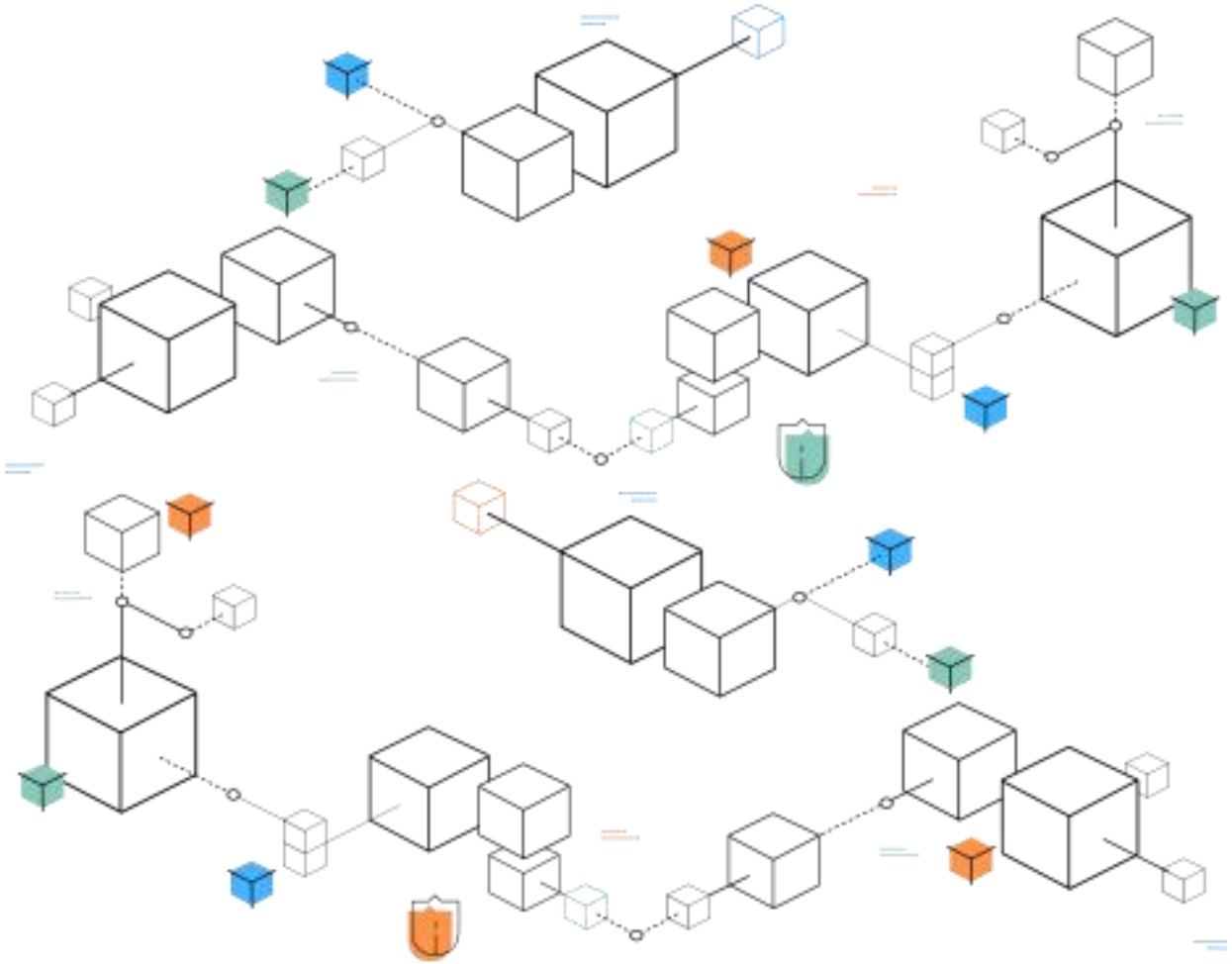
[3] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Computing Surveys (CSUR) , 53 (1), 1-32.

[4] Satija, S., Mehra, A., Singanamalla, S., Grover, K., Sivathanu, M., Chandran, N., ... & Lokam, S. (2020). Blockene: A High-throughput Blockchain Over Mobile Devices. In 14th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 20) (pp. 567-582).

Q & A

要推动**区块链底层技术服务**和**新型智慧城市建设**相结合，探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平。

——习近平总书记 2019.10.24



THANK YOU