Welcome to

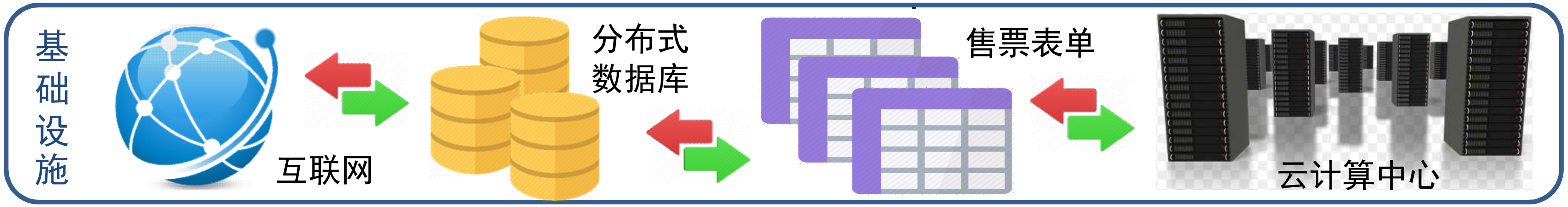
Networking Technologies for Cloud Computing

USTC-CYSC6402P
Instructor: Chi Zhang
Fall 2020

信息系统：以12306铁路购票系统为例

用户1
用户2
用户3
欢迎使用自动售取票机
自助售票机
网络终端
移动终端

12306技术部显示大屏

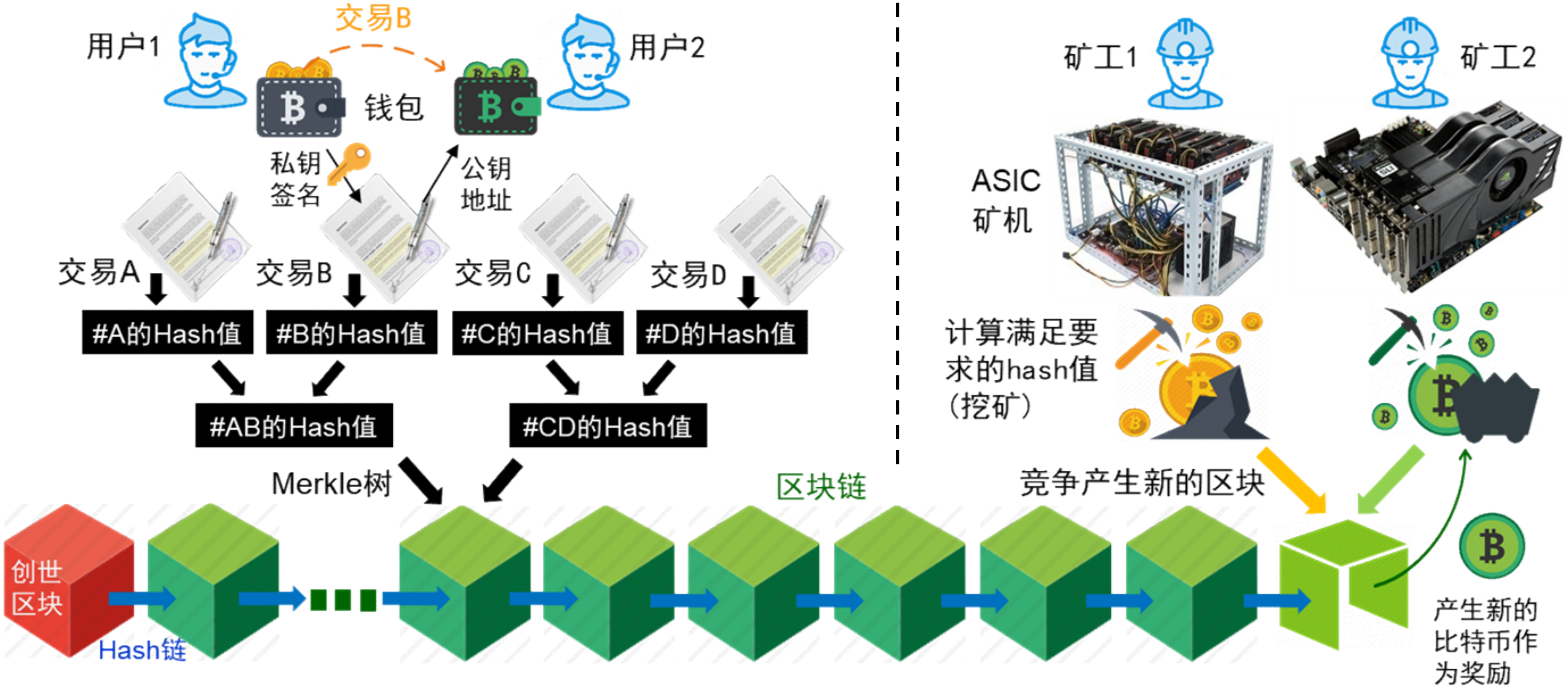


- ☐ 用户：购票、查询售票信息
- ☐ 系统维护者：维护购票系统

} 用户与系统维护者的分化

- ☐ 购票系统是半开放式的：对用户没有任何的限制
  对系统维护者有严格限制

区块链：以比特币为例



- □ 用户：产生交易、查询区块链
- □ 矿工：产生与维护区块链

} 用户与矿工的分化已不可避免

- □ 比特币区块链是完全开放式的：对用户和矿工没有任何的限制

区块链的分类-1

- BitFury Group 对区块链的分类方法（2015）

依照对矿工操作的限制程度分类

依照对用户操作的限制程度分类

	基于许可的	无需许可的
开放式	某些彩色币的区块链	现有的比特币区块链
封闭式	政府、公司用区块链	无实例

- 无需许可(permissionless) vs. 基于许可(permissioned)的区块链
  - 对于区块的产生与处理（矿工操作）是否有限制
- 开放式(public) vs. 封闭式(private)的区块链
  - 对于交易和区块数据的读取（用户操作）是否有限制
  - 更多的中文文献翻译成 公有链 vs. 私有链

区块链的分类-2

- BitFury Group 对区块链的分类方法（2015）

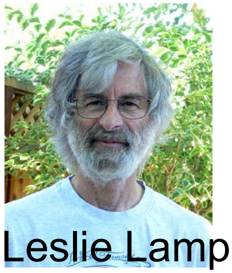
		依照对矿工操作的限制程度分类	
		基于许可的	无需许可的
依照对用户操作的限制程度分类	开放式	某些彩色币的区块链	现有的比特币区块链
	封闭式	政府、公司用区块链	无实例

- 这两种区块链有本质的差别
  - 其安全性所基于的原理完全不同
  - 应用场景和能够解决的问题也不同
- 学术界对于“基于许可的封闭式区块链”有很大争议
  - 一种观点认为：这只是分布式的数据库，不是区块链
  - 但不可否认它有应用价值，我们仅从应用角度来看问题

比特币对分布式系统安全的理论贡献

- 比特币是一个伟大创举，因为它颠覆了传统的安全理论
  - □ 传统理论认为：一个开放式系统不可能是安全的
  - □ 一个安全的系统中，“好人”要比“坏人”多，甚至要是“坏人”的两倍以上，系统才能按照“好人”的期望运行
  - □ 开放式系统无法控制“坏人”的数量

Byzantine Generals Problem: In a system with n nodes and f Byzantine nodes, there is NO algorithm that solves the consensus problem if n≤3f.

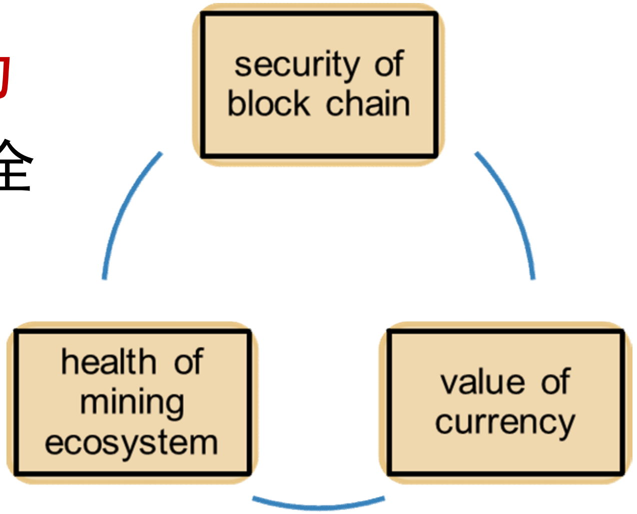


Leslie Lamport

- 比特币认为，传统理论的假设是错误的
  - □ 没有“好人”与“坏人”，只有“理性的人”
  - □ 如果维护系统比攻击系统所能获得的收益要大，“理性的人”为什么要去做攻击系统的“坏人”呢？
  - □ 加密货币的发行机制确保了维护系统的收益更高

比特币为什么是安全的？

- 数字签名解决了数字货币的绝大多数安全问题，只剩下
  - 数字货币转移的“双花问题”（数字复制零成本）
  - 数字货币发行的“去中心化问题”（通货膨胀的根源）
- 区块链同时解决了这两个问题
  - 区块链的一致性确保只有一次“数字货币使用记录”上链
  - 而数字货币的程序化发行确保了区块链的安全
- 区块链安全：维护者算力>攻击者算力
  - 算力的积累确保了比特币区块链的安全
  - 数字货币的发行为吸引算力提供激励
  - 两者互相激荡，形成了正反馈



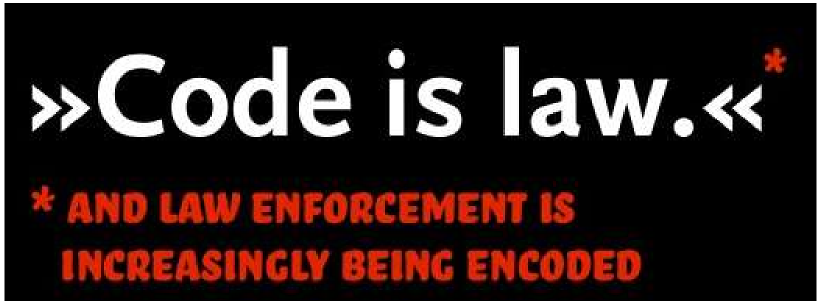
对比特币区块链的扩展充满陷阱

- 基于应用类型的区块链分类
  - □ 面向货币化应用(如数字货币 Cryptocurrency)的区块链
  - □ 面向非货币化应用(Non-currency App)的区块链
- 在比特币的区块链中
  - □ 数字货币和区块链安全是相互支撑，缺一不可
  - □ 数字货币提供激励：确保区块链维护者算力>攻击者算力
  - □ 区块链提供全局一致性账本：确保只有一次“数字货币使用记录”上链（被认可）
- 扩展到其它应用中，还需要“区块链”的数据结构吗？
  - □ 是基于“数字货币”的激励确保算力安全吗？
  - □ 上链数据需要一致性验证（不矛盾验证）吗？

智能合约为什么是安全的？

- 智能合约：并不智能，也不是合约
  - 代码预先写死（上链之后不可变动）
  - 没有法律保护和救济机制（不要法官）

- 智能合约的安全取决于
  - 所有维护者执行智能合约代码，并对代码执行的中间状态和最终结果达成一致

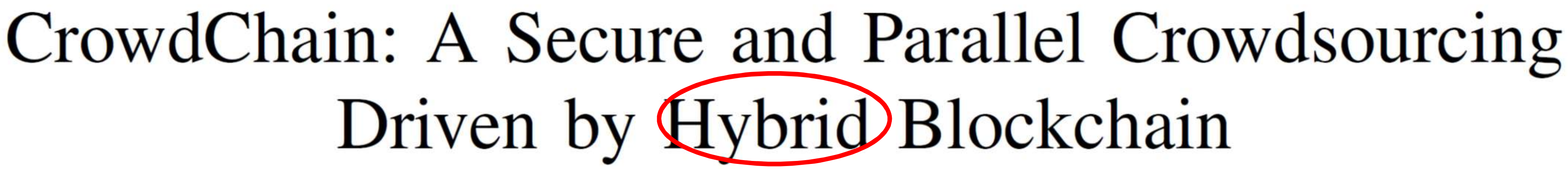


»Code is law.«*

* AND LAW ENFORCEMENT IS INCREASINGLY BEING ENCODED

- 智能合约的局限性
  - 单线程虚拟机抽象：虽然图灵完备但执行效率很低，和法院执法流程费时费力一样
  - 无法保存秘密：无法在智能合约中执行加密、解密、签名操作
  - 不支持随机数：一致性验证要求确定性代码

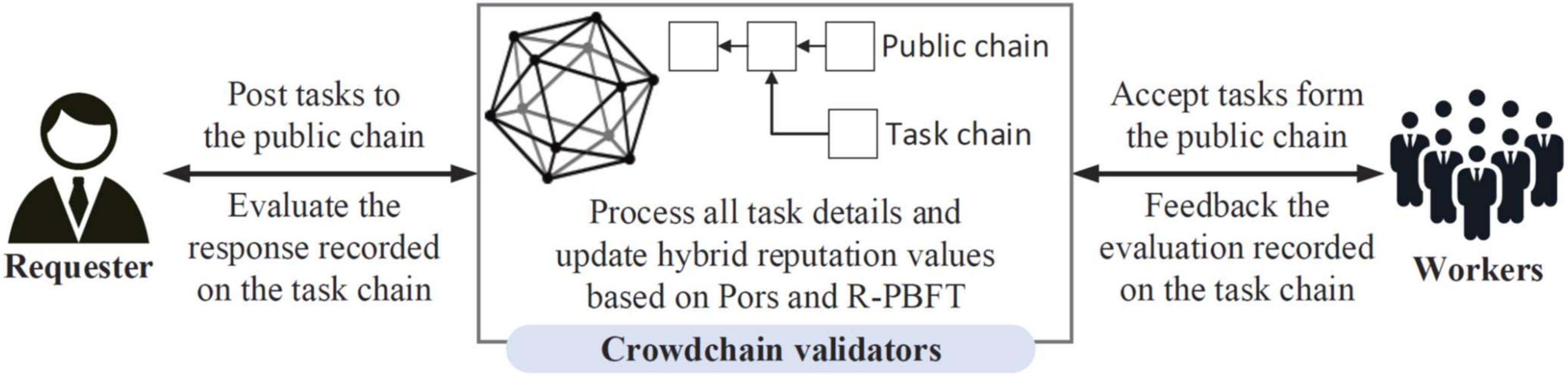
论文分析



CrowdChain: A Secure and Parallel Crowdsourcing Driven by Hybrid Blockchain

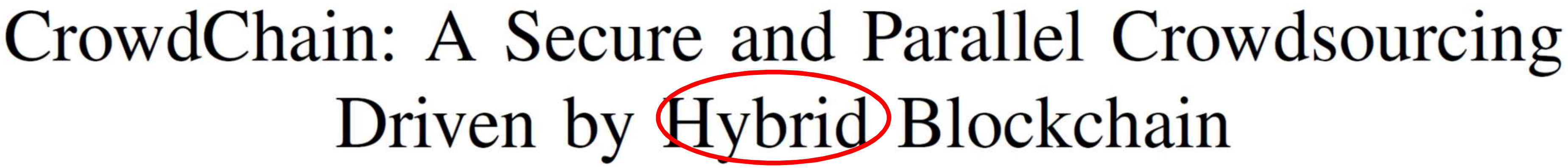
- The authors identify three main limitations of current blockchain-based solution for crowdsourcing
  - □ task privacy protection
  - □ limited transaction throughput
  - □ low fault-tolerance ability

论文要解决的问题



- The authors identify three main limitations of current blockchain-based solution for crowdsourcing
  - □ task privacy protection
  - □ limited transaction throughput
  - □ low fault-tolerance ability

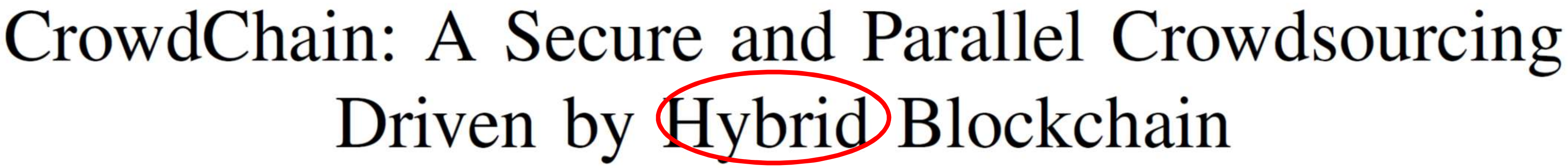
论文的基本工作1



CrowdChain: A Secure and Parallel Crowdsourcing Driven by Hybrid Blockchain

- task privacy protection
  - □ propose a “hybrid” blockchain system as the underlying data storage architecture for crowdsourcing platform,
  - □ in which the private information of each task is stored in corresponding private chain and other public information of tasks is stored in a public chain. 有可能，但不够

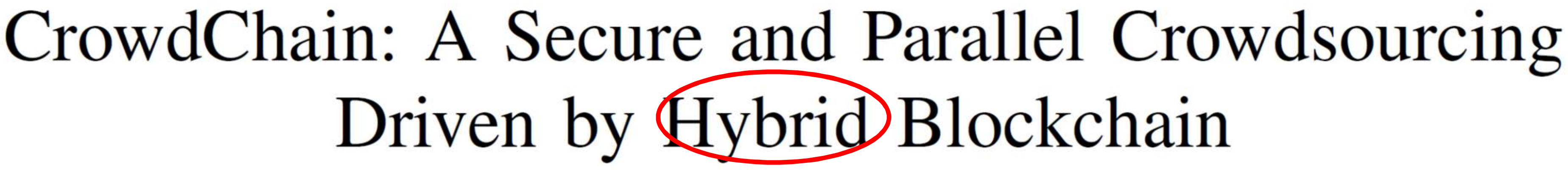
论文的基本工作2



CrowdChain: A Secure and Parallel Crowdsourcing Driven by Hybrid Blockchain

- limited transaction throughput
  - □ limited transaction throughput caused by serial transaction processing
  - □ design a smart contract called Pors to process transactions of each task independently on its own task chain. 反常，SC不可能解决效率问题

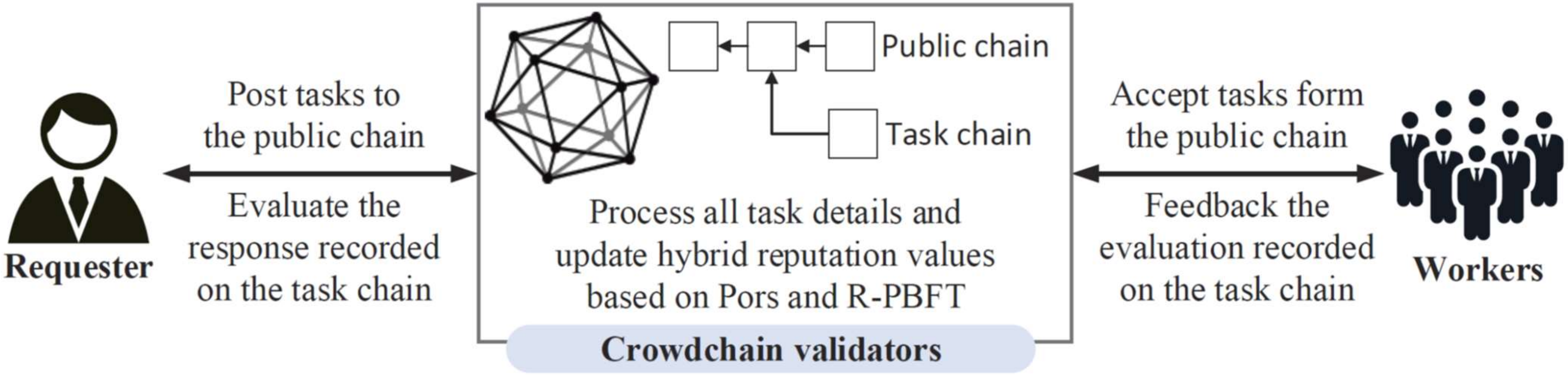
论文的基本工作3



CrowdChain: A Secure and Parallel Crowdsourcing Driven by Hybrid Blockchain

- low fault-tolerance ability
  - Low fault-tolerance ability of their practical byzantine-fault-tolerance (PBFT) consensus protocols.
  - the authors first propose a new hybrid reputation evaluation model to calculate the hybrid reputation values of platform users.
  - They then select users with reputation values above a threshold as the participants of consensus protocol (R-PBFT) Reputation本身如何安全维护？

论文总结

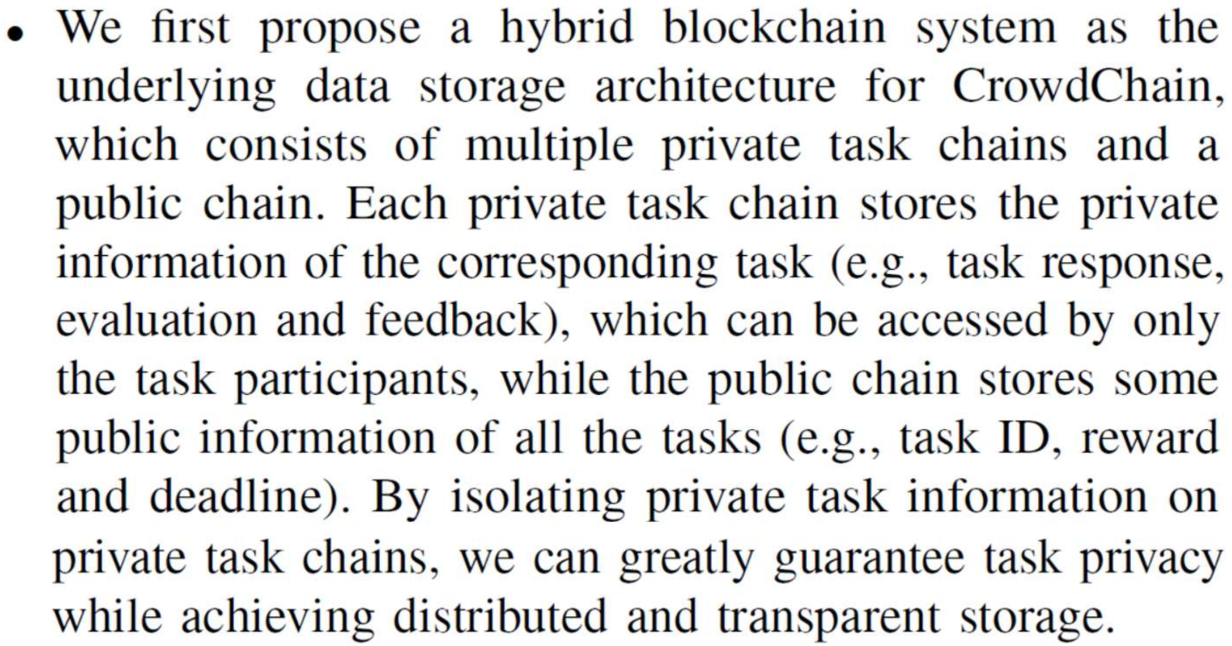

Public chain
Task chain
Post tasks to the public chain
Evaluate the response recorded on the task chain
Requester
Process all task details and update hybrid reputation values based on Pors and R-PBFT
Crowdchain validators
Accept tasks form the public chain
Feedback the evaluation recorded on the task chain
Workers

- three main limitations & their solutions
  - □ task privacy protection -> hybrid blockchain
  - □ limited transaction throughput -> SC: Pors
  - □ low fault-tolerance ability -> R-PBFT

论文的研究内容1：Hybrid Blockchain

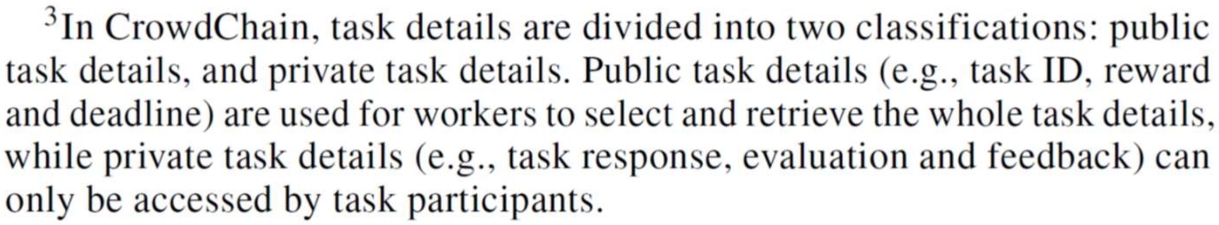
- 如何保护task privacy？

P1：
右下



- We first propose a hybrid blockchain system as the underlying data storage architecture for CrowdChain, which consists of multiple private task chains and a public chain. Each private task chain stores the private information of the corresponding task (e.g., task response, evaluation and feedback), which can be accessed by only the task participants, while the public chain stores some public information of all the tasks (e.g., task ID, reward and deadline). By isolating private task information on private task chains, we can greatly guarantee task privacy while achieving distributed and transparent storage.

P3：
左下



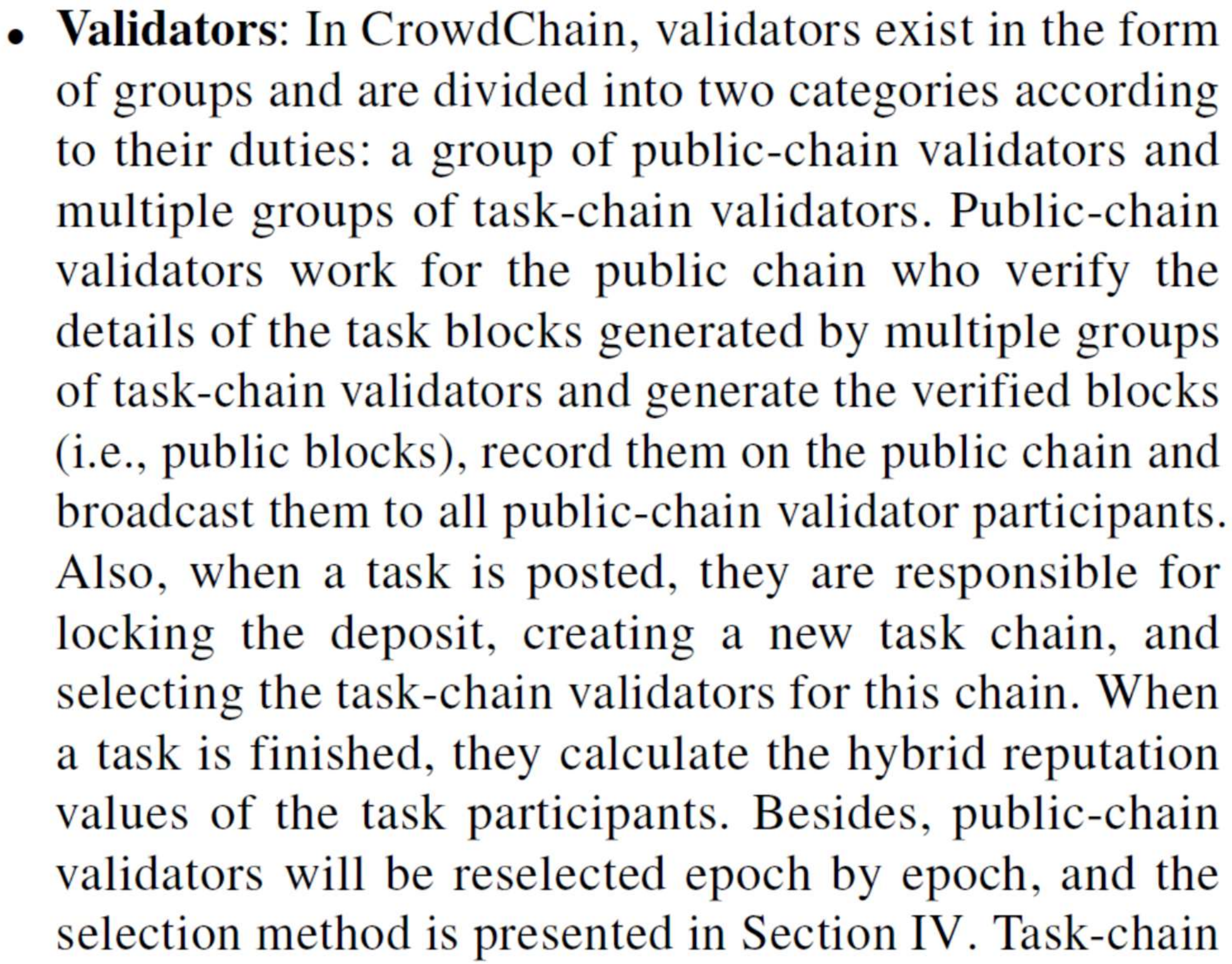
[3] In CrowdChain, task details are divided into two classifications: public task details, and private task details. Public task details (e.g., task ID, reward and deadline) are used for workers to select and retrieve the whole task details, while private task details (e.g., task response, evaluation and feedback) can only be accessed by task participants.

作者对public chain和private chain的理解有误

论文的研究内容1：Hybrid Blockchain

- Hybrid blockchain如何体现？

P3：
左中

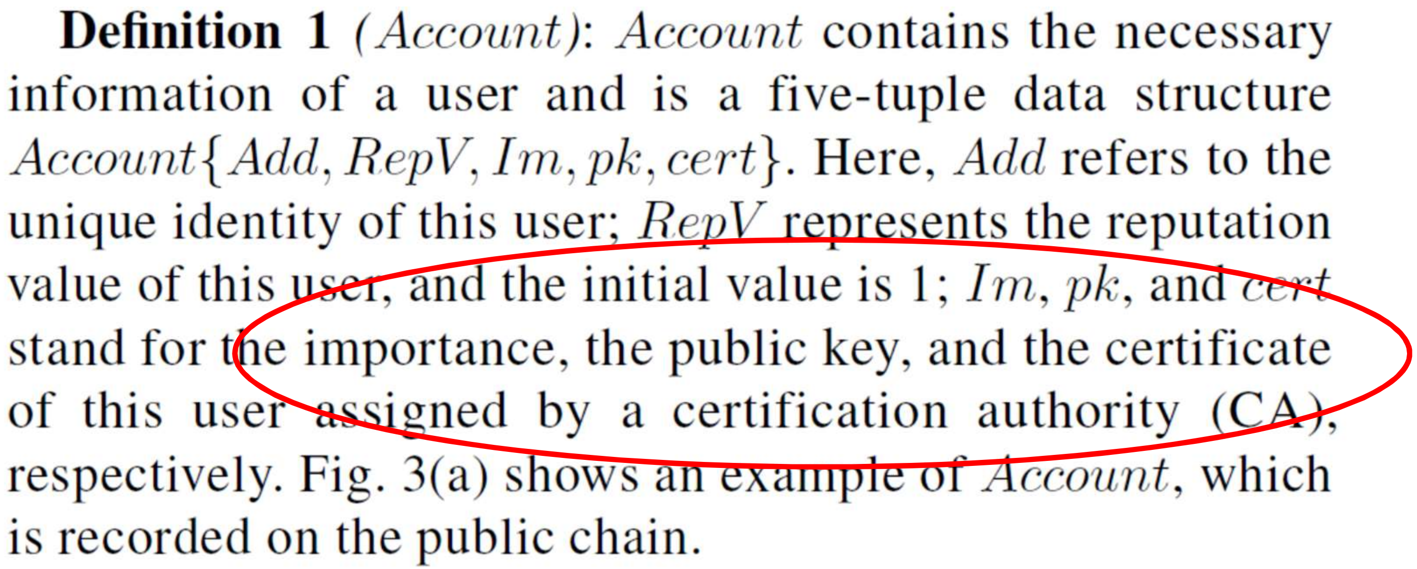


- **Validators**: In CrowdChain, validators exist in the form of groups and are divided into two categories according to their duties: a group of public-chain validators and multiple groups of task-chain validators. Public-chain validators work for the public chain who verify the details of the task blocks generated by multiple groups of task-chain validators and generate the verified blocks (i.e., public blocks), record them on the public chain and broadcast them to all public-chain validator participants. Also, when a task is posted, they are responsible for locking the deposit, creating a new task chain, and selecting the task-chain validators for this chain. When a task is finished, they calculate the hybrid reputation values of the task participants. Besides, public-chain validators will be reselected epoch by epoch, and the selection method is presented in Section IV. Task-chain

论文的研究内容1：Hybrid Blockchain

- Public blockchain 在哪里？

P3：
右中

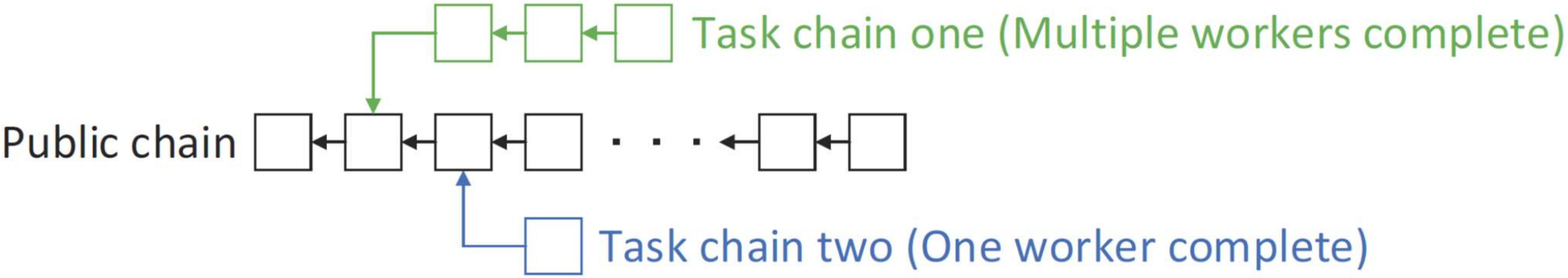


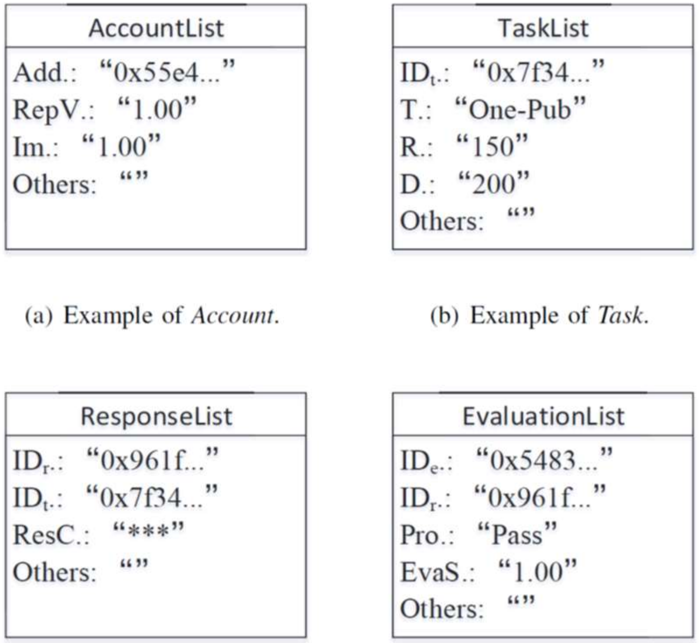
Definition 1 *(Account)*: *Account* contains the necessary information of a user and is a five-tuple data structure $Account\{Add, RepV, Im, pk, cert\}$. Here, Add refers to the unique identity of this user; $RepV$ represents the reputation value of this user, and the initial value is 1; Im, pk, and $cert$ stand for the importance, the public key, and the certificate of this user assigned by a certification authority (CA), respectively. Fig. 3(a) shows an example of *Account*, which is recorded on the public chain.

本文没有public chain
主链和辅链都是private chain

论文的研究内容1：Hybrid Blockchain

- 主链和辅链上都是什么内容？


Task chain one (Multiple workers complete)
Public chain
. . .
Task chain two (One worker complete)



AccountList

Add.: “0x55e4...”
RepV.: “1.00”
Im.: “1.00”
Others: “”

(a) Example of *Account*.

TaskList

ID$_t$.: “0x7f34...”
T.: “One-Pub”
R.: “150”
D.: “200”
Others: “”

(b) Example of *Task*.

ResponseList

ID$_r$.: “0x961f...”
ID$_t$.: “0x7f34...”
ResC.: “***”
Others: “”

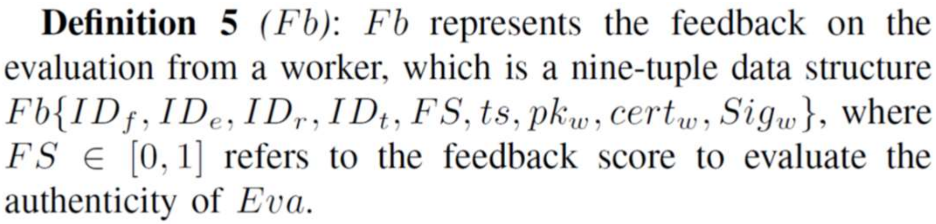
(c) Example of *Res*.

EvaluationList

ID$_e$.: “0x5483...”
ID$_r$.: “0x961f...”
Pro.: “Pass”
EvaS.: “1.00”
Others: “”

(d) Example of *Eva*.

- □ 需要区块链的数据结构吗？
- □ serial transaction processing？



Definition 5 (Fb): Fb represents the feedback on the evaluation from a worker, which is a nine-tuple data structure $Fb\{ID_f, ID_e, ID_r, ID_t, FS, ts, pk_w, cert_w, Sig_w\}$, where $FS \in [0,1]$ refers to the feedback score to evaluate the authenticity of Eva.

论文的研究内容1：Hybrid Blockchain

- 研究内容一小结
- 如何保护task privacy？
  - □ 没有安全目标、安全假设、安全机制设计、安全证明
  - □ 作者对public chain和private chain的理解有误
- Hybrid blockchain如何体现？
  - □ 本文没有public chain
  - □ 主链和辅链都是private chain
- 主链和辅链上都是什么内容？
  - □ 这些内容（TX）需要上链的serial transaction processing？

论文的研究内容2：Pros

- 智能合约Pros做了什么？

P4：
左下

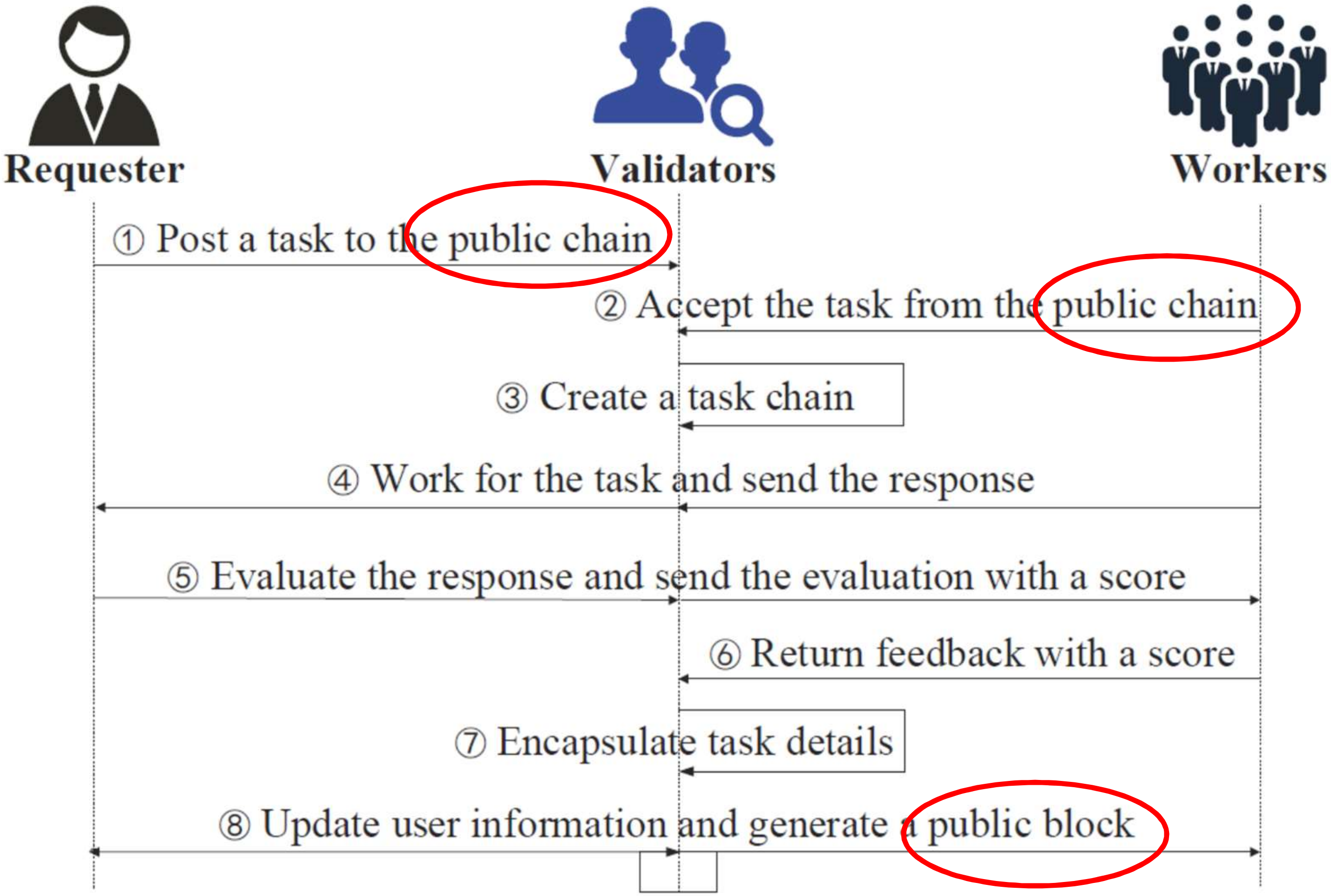
C. Pors Component

Step 1. Post a task
Step 2. Accept the task
Step 3. Create a task chain
Step 4. Work for the task and send the response
Step 5. Evaluate and send the evaluation
Step 6. Return feedback
Step 7. Encapsulate task details
Step 8. Generate the public block

论文的研究内容2：Pros

- 智能合约Pros做了什么？

P4：
右上



① Post a task to the public chain

② Accept the task from the public chain

③ Create a task chain

④ Work for the task and send the response

⑤ Evaluate the response and send the evaluation with a score

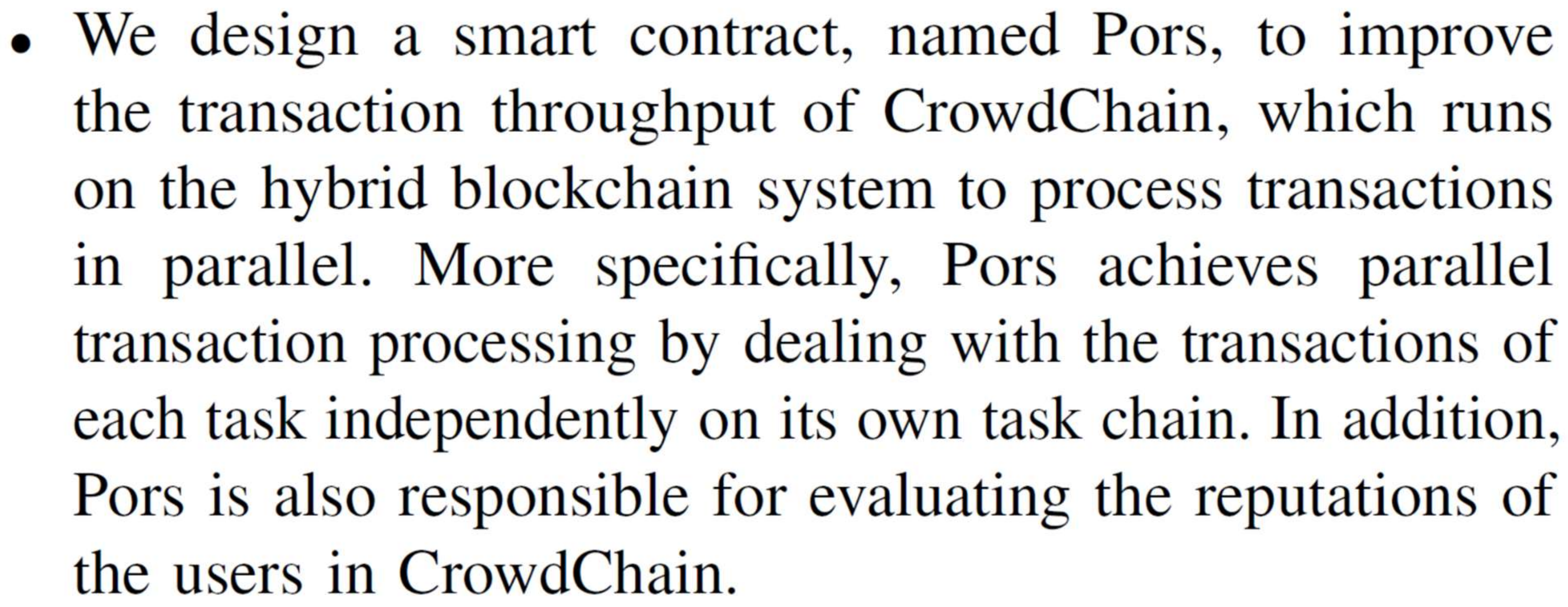
⑥ Return feedback with a score

⑦ Encapsulate task details

⑧ Update user information and generate a public block

论文的研究内容2：Pros

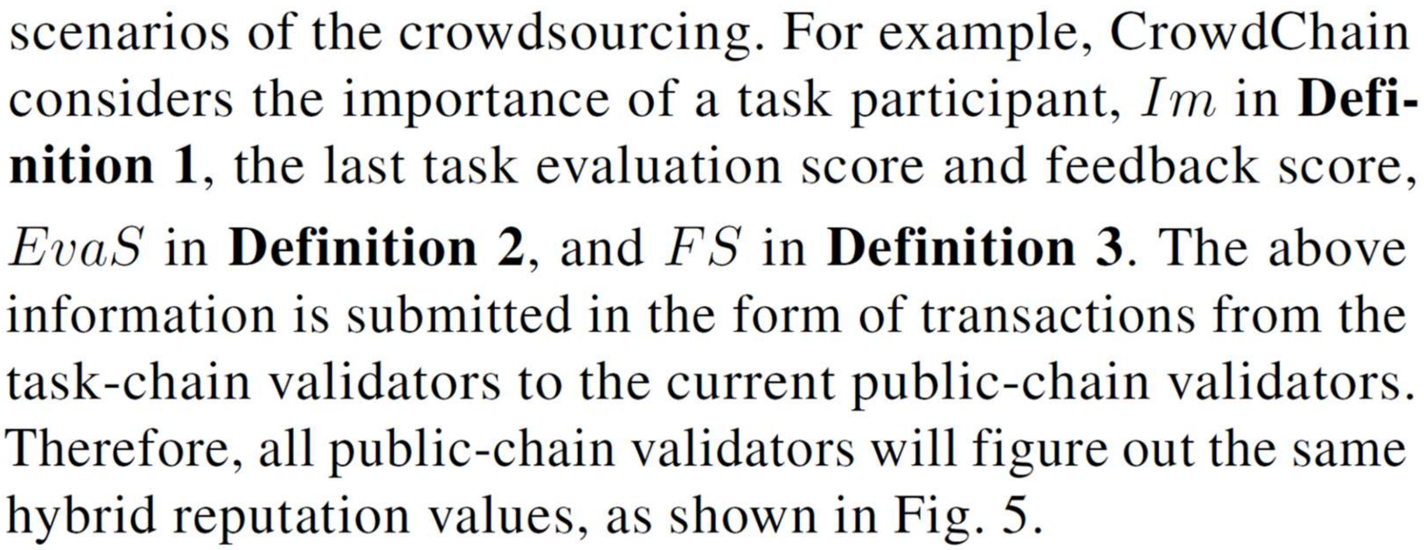
- 研究内容二小结
- 智能合约Pros做了什么？
  - 所有操作都在上面做
  - 如何支持不同task chain上的并行？没有解释



- We design a smart contract, named Pors, to improve the transaction throughput of CrowdChain, which runs on the hybrid blockchain system to process transactions in parallel. More specifically, Pors achieves parallel transaction processing by dealing with the transactions of each task independently on its own task chain. In addition, Pors is also responsible for evaluating the reputations of the users in CrowdChain.

论文的研究内容3：R-PBFT

- 基于R-PBFT的工作流程
  - □ Step 1. Calculate hybrid reputation values of platform users



scenarios of the crowdsourcing. For example, CrowdChain considers the importance of a task participant, Im in **Definition 1**, the last task evaluation score and feedback score, $EvaS$ in **Definition 2**, and FS in **Definition 3**. The above information is submitted in the form of transactions from the task-chain validators to the current public-chain validators. Therefore, all public-chain validators will figure out the same hybrid reputation values, as shown in Fig. 5.

上述操作上链，只能确保验证者得到一致的信誉分数，无法确保分数本身是安全的

论文的研究内容3：R-PBFT

基于R-PBFT的工作流程

- □ Step 1. Calculate hybrid reputation values of platform users
- □ Step 2. Select PBFT participants from platform users
- □ Step 3. Reach consensus among the PBFT participants

（1）信誉的语义不符问题：
就算是第一步中获得的信誉分数是安全的，第一步中的信誉分数是用户参与众包的信誉，而不是作为验证者的信誉。一个人是好爸爸，不等于就是一个好老师。
（2）其它对信誉的攻击：
洗白（与ID关联才可防止）；无法观察的行为（隐私泄露）；积攒信誉后的恶意攻击