区块链研究现状概览

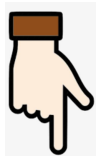
——理论、模型 与 工具

吴嘉婧

副教授

中山大学 计算机学院

提纲



近况概览

提升区块链性能的方案

加深理解区块链

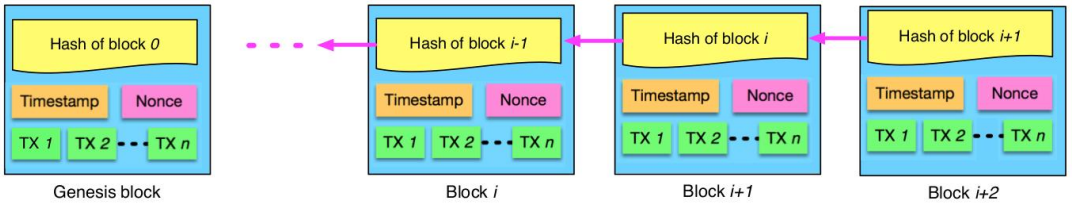
区块链实验工具与数据集

开放问题

区块链背景与现状

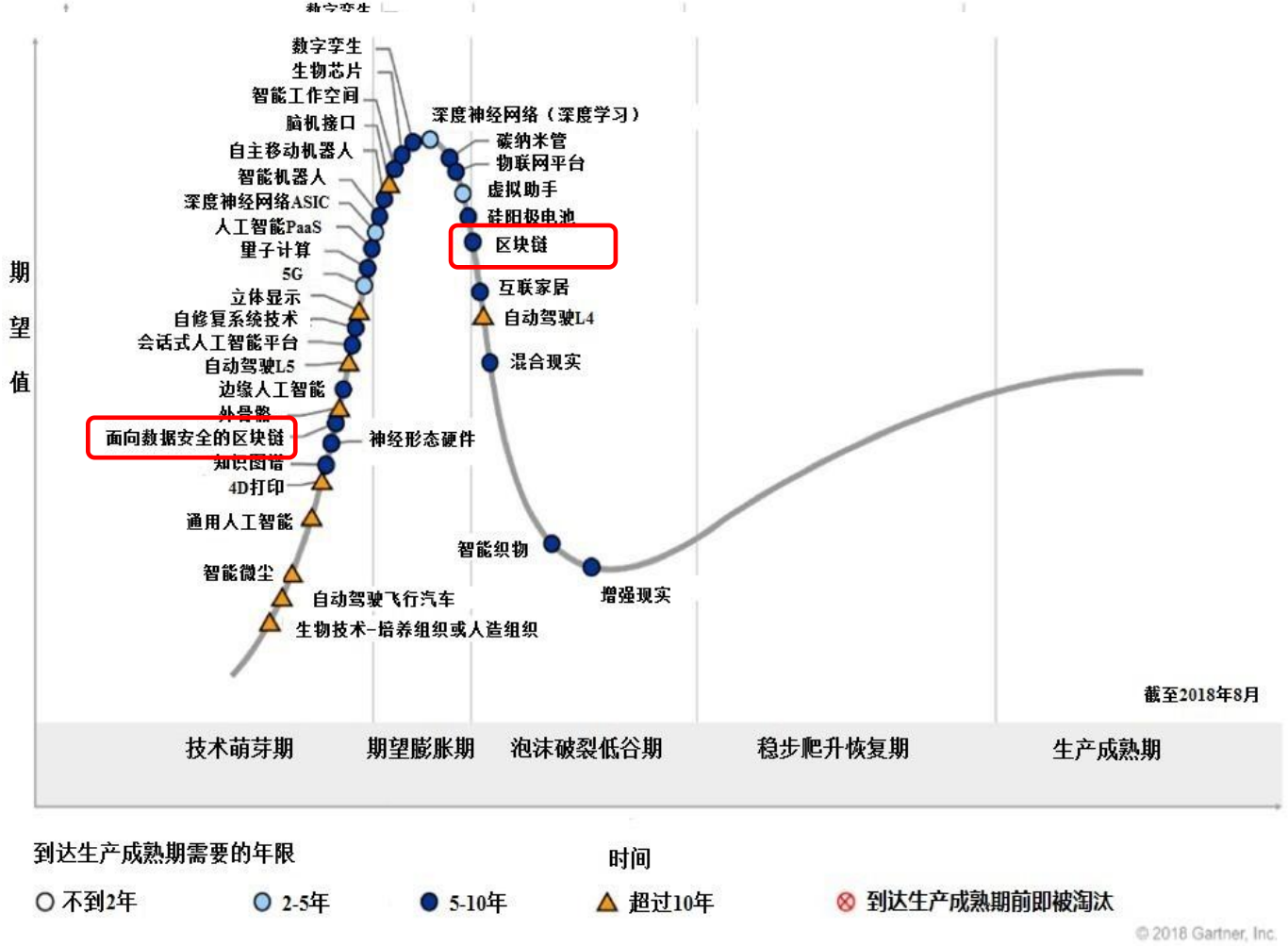
区块链 (Blockchain) ——简单背景

- 区块链定义
  - 按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构

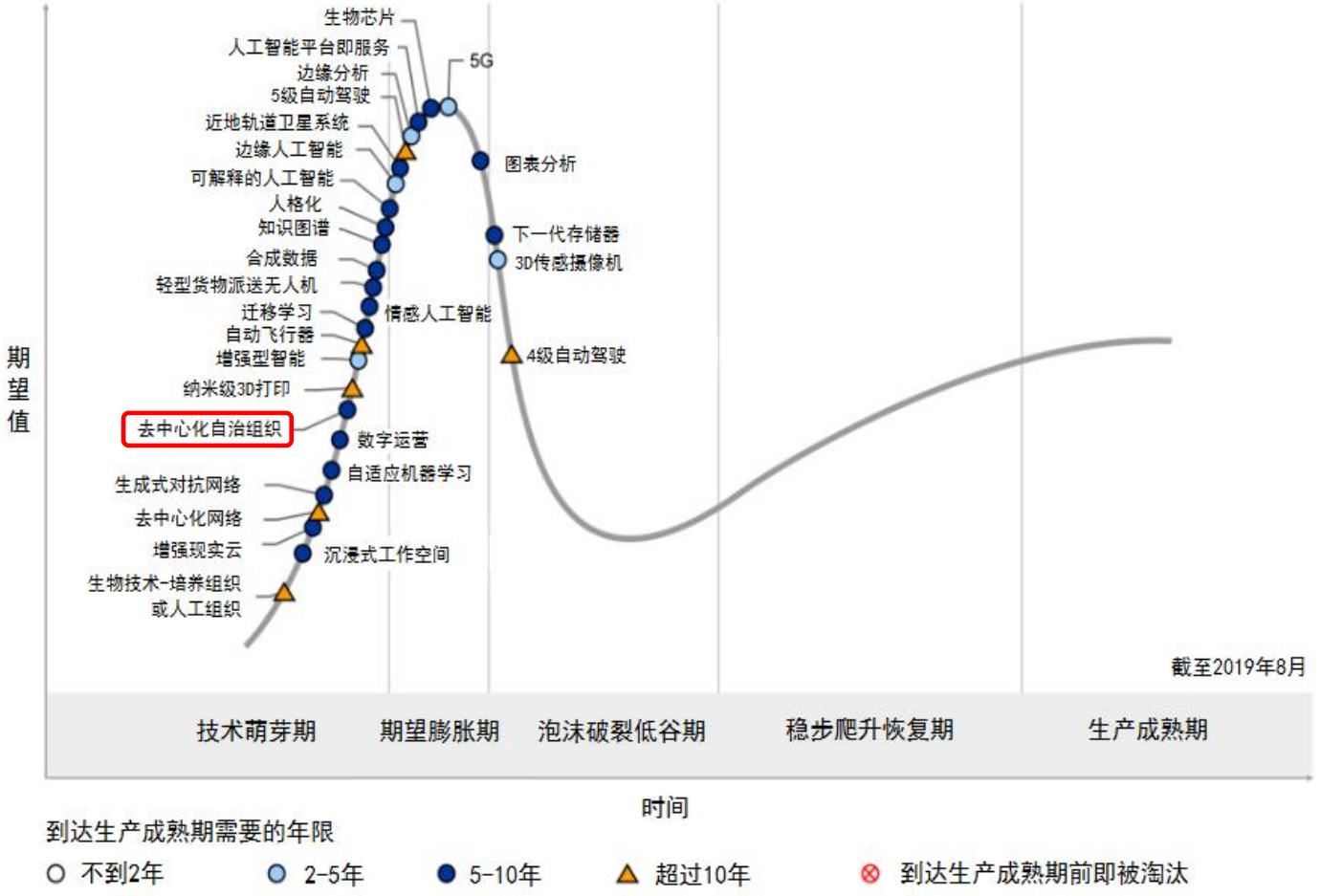


  - 区块链是一个**分布式的账本数据库**
  - 网络中的每个节点都有一本完整的账本
  - 无法篡改
  - 去中心化，降低成本，提高效率

Gartner新兴技术成熟度曲线-2018

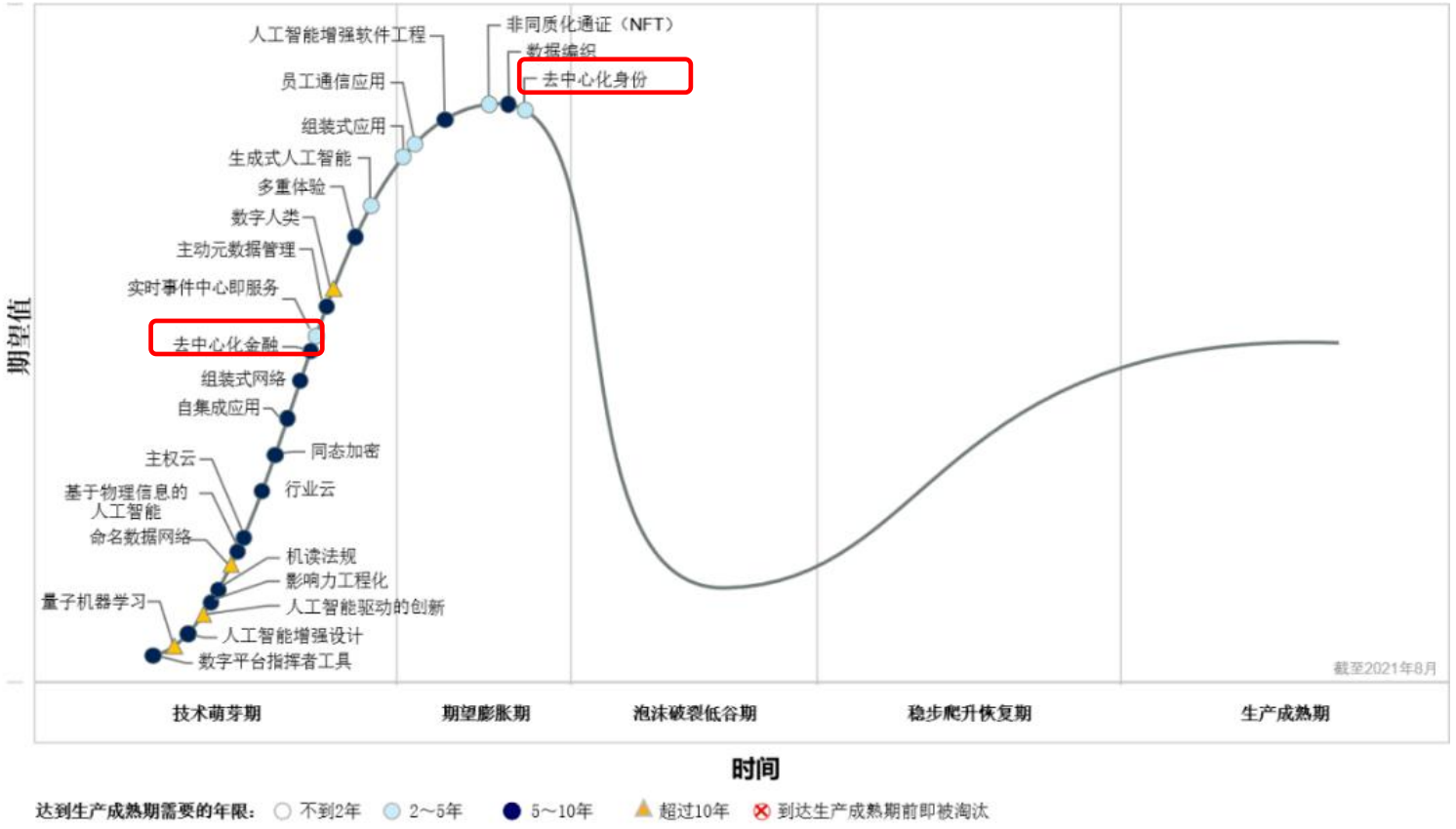


Gartner新兴技术成熟度曲线-2019



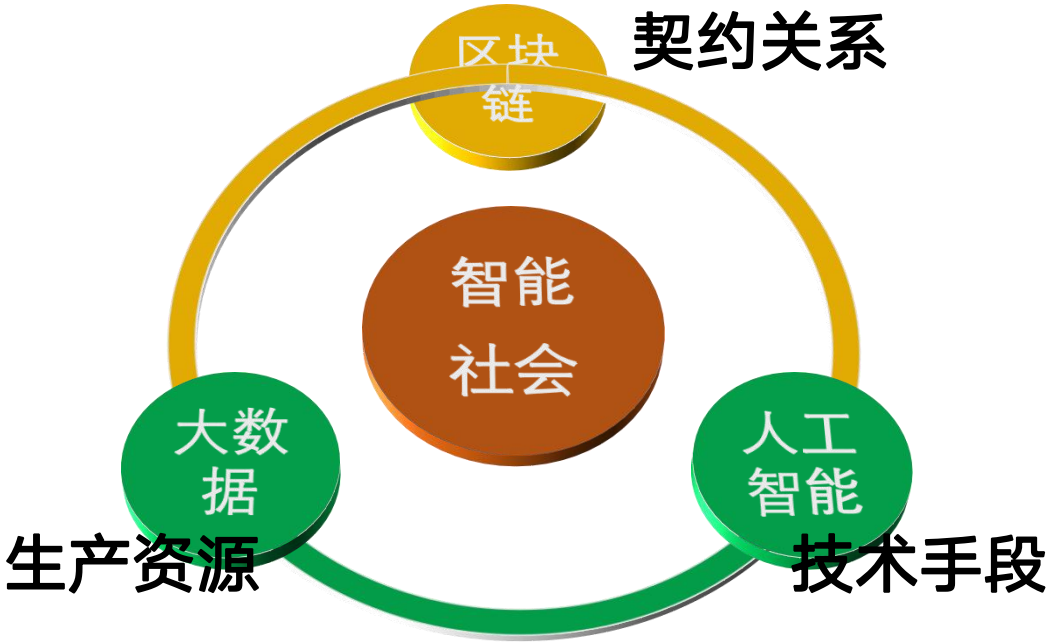
Gartner新兴技术成熟度曲线-2020

Gartner新兴技术成熟度曲线-2021



导言：大数据，人工智能 与 区块链

- **契约**：对生产资料、技术手段的分配

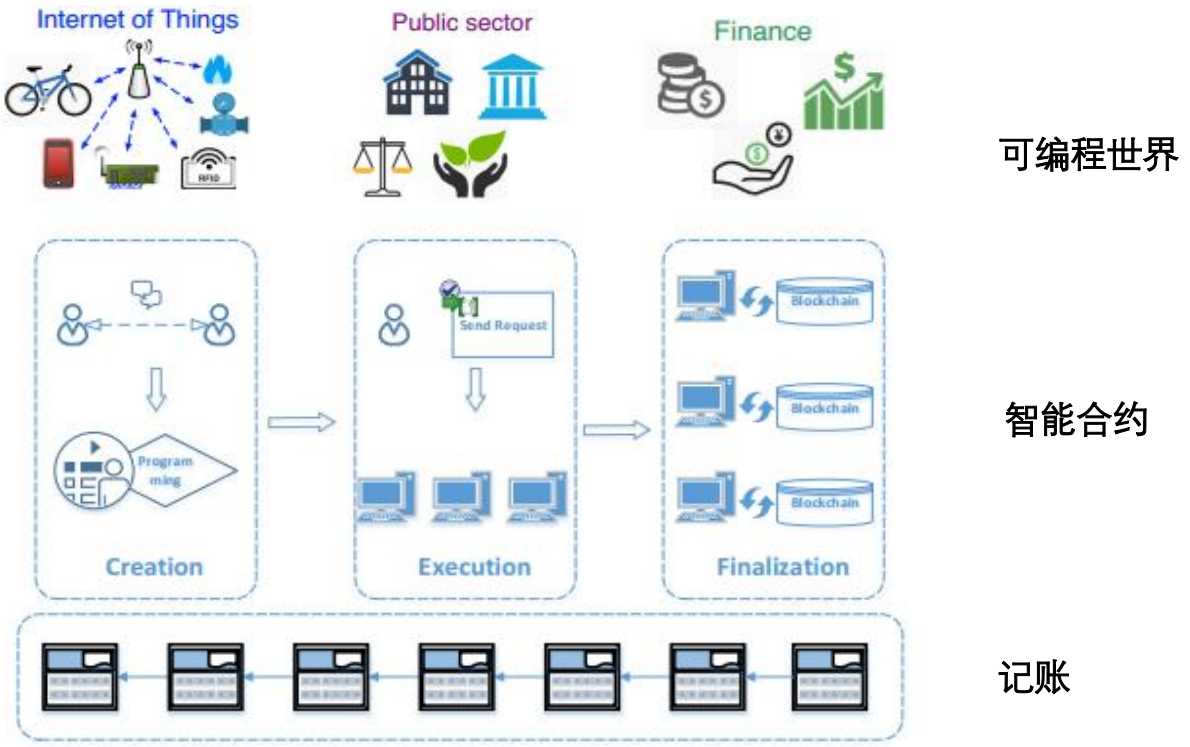


导言：生产力 vs 生产关系

- 人工智能：解放生产力
  - 虽然 剧烈地改变了人类的生活
  - 但是 没有改变 组织模式（银行柜台，移动支付 依然存在）
  - 而且 以人为中心来执行判断，做决策

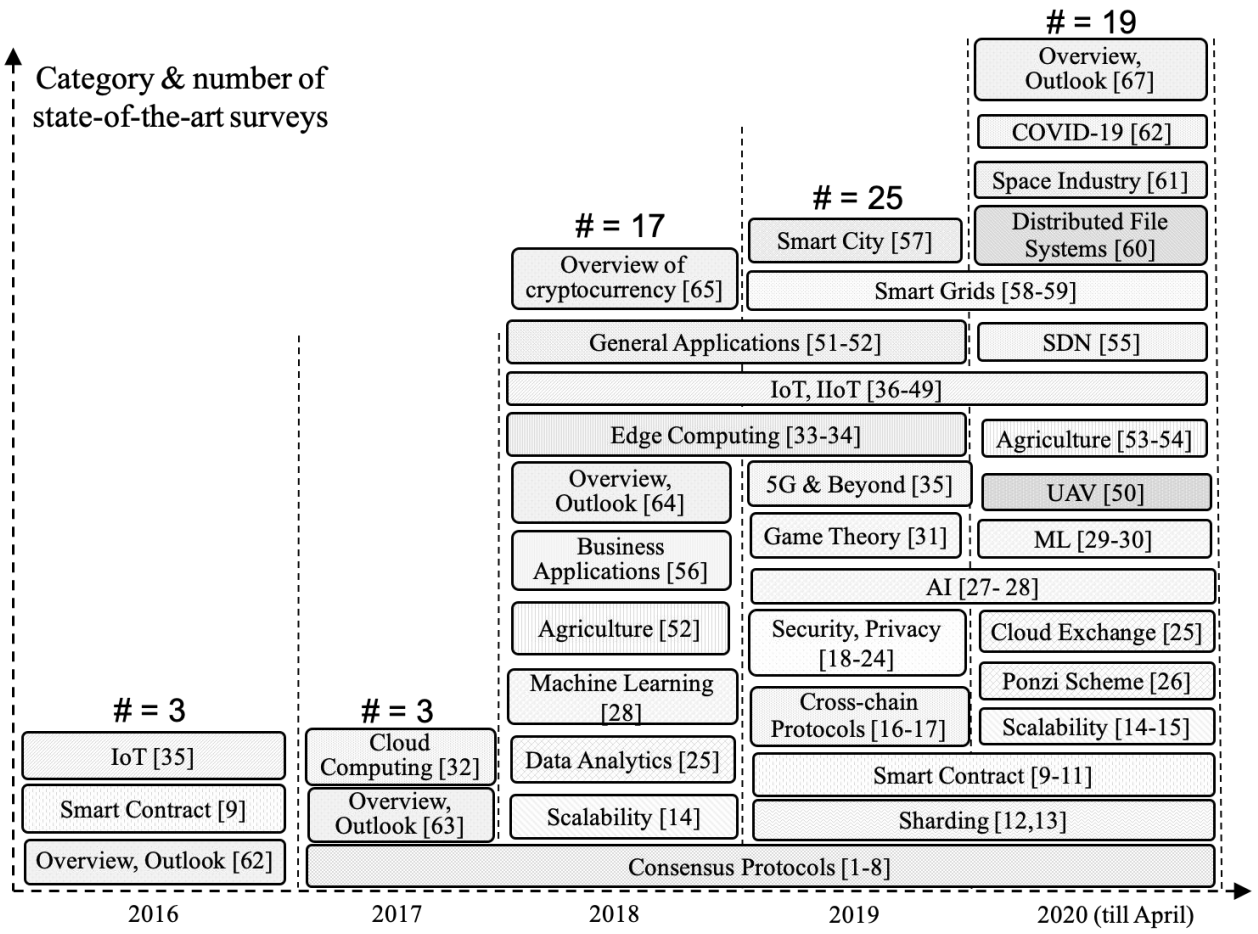
- 区块链：改变生产关系
  - 它挑战和改变了人类的组织模式
  - 几十年后回头看可能发现很多机构都消失不见

导言：区块链的发展路径

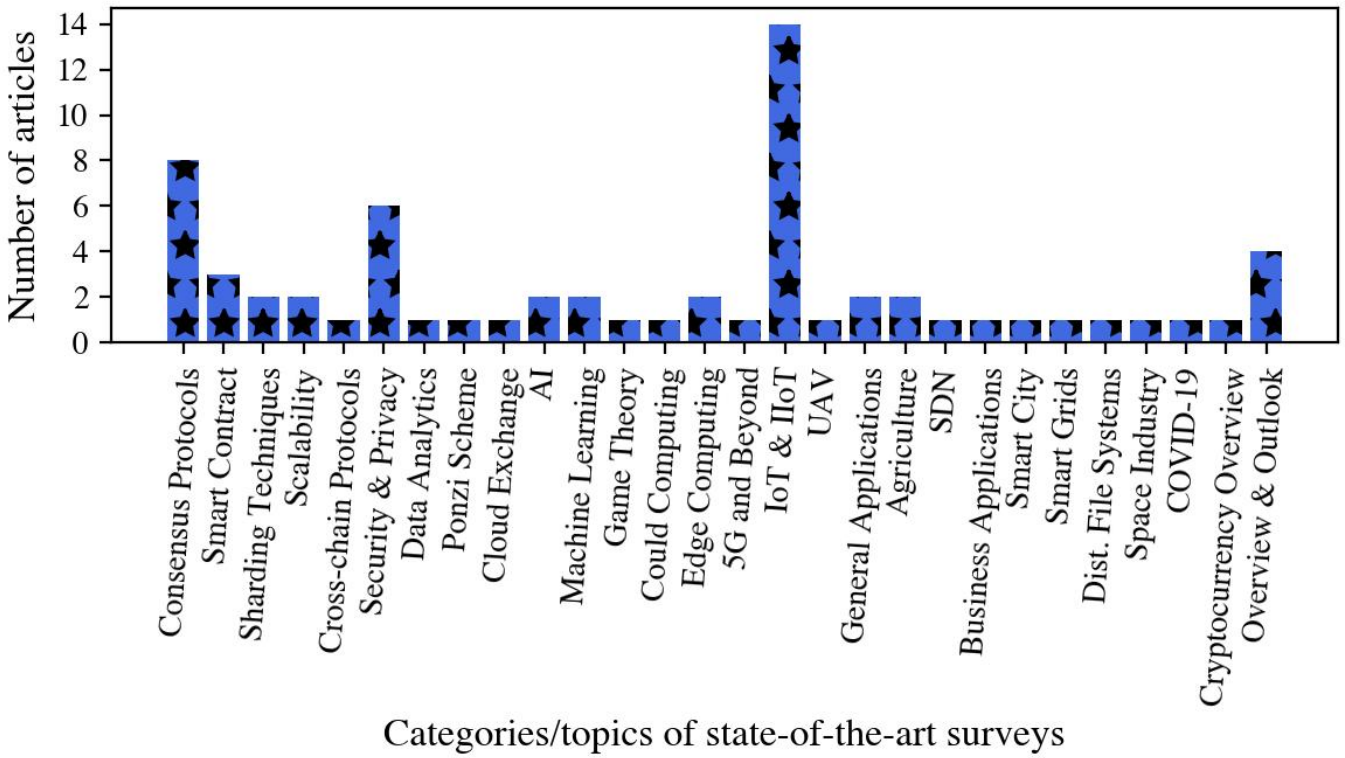

Blockchain3.0
Internet of Things
Public sector
Finance
可编程世界
Blockchain2.0
Program ming
Creation
Send Request
Execution
Blockchain
Blockchain
Blockchain
Finalization
智能合约
Blockchain1.0
记账

区块链的研究现状概览
Overview of State-of-the-art studies

概览发现——67篇代表性Survey



概览发现——28个代表性方向



概览发现——7个典型的分组

- Group 1: 关于区块链本身的 (Blockchain Essentials)
  - 共识协议 (Consensus Protocols) [1]
  - 智能合约 (Smart Contract) [2]
  - 分片机制 (Sharding) [3]
  - 可扩展性 (Scalability) [4]
  - 跨链方案 (Cross-chain) [5]
  - 安全、隐私与可靠性 (Security & Privacy, Reliability) [6]

[1] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2017, pp. 1–5.

[2] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on ethereum smart contracts,” IACR Cryptology ePrint archive, vol. 2016, pp. 1007–1030, 2016.

[3] G. Wang, Z. J. Shi, M. Nixon, and S. Han, “Sok: Sharding on blockchain,” in Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT’19), 2019, pp. 41–61.

[4] C. Pan, Z. Liu, Z. Liu, and Y. Long, “Research on scalability of blockchain technology: Problems and methods,” Journal of Computer Research and Development, vol. 55, no. 10, pp. 2099–2110, 2018.

[5] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, “Sok: Communication across distributed ledgers,” IACR Cryptology ePrint Archive, 2019: 1128, Tech. Rep., 2019.

[6] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,” Digital Communications and Networks, 2019.

概览发现——7个典型的分组

- Group 2: 针对区块链的数据挖掘 (Data Mining)
  - 数据解析 (Data Analytics) [1][2]
  - 智能合约欺诈行为的识别 (如庞氏骗局，Ponzi Scheme, 钓鱼诈骗 Phishing) [3][4]

[1] W. Chen and Z. Zheng, “Blockchain data analysis: A review of status, trends and challenges,” Journal of Computer Research and Development, vol. 55, no. 9, pp. 1853–1870, 2018.

[2] J. Wu, J. Liu, Y. Zhao, Z. Zheng, ”Analysis of cryptocurrency transactions from a network perspective: An overview”, Journal of Network and Computer Applications, vol. 190, p.103139.

[3] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, “Dissecting ponzi schemes on ethereum: identification, analysis, and impact,” Future Generation Computer Systems, vol. 102, pp. 259–277, 2020.

[4] J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, Z. Zheng, ” Who are the phishers? phishing scam detection on ethereum via network embedding”, IEEE Transactions on Systems, Man, and Cybernetics: Systems

概览发现——7个典型的分组

- Group 3: 区块链相关的智能决策 (Decision-Making Techniques)
  - 人工智能 (AI) [1]
  - 机器学习 (ML) [2]
  - 博弈论 (Game Theory) [3]

[1] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for ai: review and open research challenges,” IEEE Access, vol. 7, pp. 10 127–10 149, 2019.

[2] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, “Blockchain and machine learning for communications and networking systems,” **IEEE Communications Surveys & Tutorials**, 2020.

[3] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, “A survey on blockchain: A game theoretical perspective,” IEEE Access, vol. 7, pp. 47 615–47 643, 2019.

概览发现——7个典型的分组

- Group 4:与计算/通信网络的融合 (Communication Networking)
  - 云计算 (Cloud Computing) [1]
  - 边缘计算 (Edge Computing) [2]
  - 5G 和 Beyond 5G (5G and beyond) [3]

[1] J. H. Park and J. H. Park, “Blockchain security in cloud computing: Use cases, challenges, and solutions,” Symmetry, vol. 9, no. 8, p. 164, 2017.

[2] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” **IEEE Communications Magazine**, vol. 56, no. 8, pp. 33–39, 2018.

[3] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for 5g and beyond networks: A state of the art survey,” arXiv preprint arXiv:1912.05062, 2019.

概览发现——7个典型的分组

- Group 5: 物联网与工业物联网 (IoT & IIoT)
  - 物联网 (IoT/IIoT) [1][2][3]
  - 无人机 (UAV) [4]

[1] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[2] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of blockchains in the internet of things: A comprehensive survey,”, **IEEE Communications Surveys & Tutorials**, vol. 21, no. 2, pp. 1676–1717, 2018.

[3] T. M. Fernández-Caramés and P. Fraga-Lamas “A review on the use of blockchain for the internet of things,” IEEE Access, vol. 6, pp. 32 979–33 001, 2018.

[4] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, “Applications of blockchain in unmanned aerial vehicles: A review,” Vehicular Communications, February 2020.

概览发现——7个典型的分组

- Group 6: 区块链应用 (Blockchain Applications)
  - 总览 (General Applications) [1]
  - 农业 (Agriculture) [2]
  - 软件定义网络 (Game Theory) [3]
  - 商业应用 (Business Apps) [4]
  - 智慧城市 (Smart City) [5]
  - 智能电网 (Smart Grid) [6]
  - 文件系统 (File Systems) [7]
  - 航天工业 (Space Industry) [8]
  - COVID-19 [9]

[1] Y. Lu, “Blockchain: A survey on functions, applications and open issues,” **Journal of Industrial Integration and Management,** vol. 3, no. 04, p. 1850015, 2018

[2] O. Bermeo-Almeida, M. Cardenas-Rodriguez, T. Samaniego-Cobo, E. Ferruzola-Gómez, R. Cabezas-Cabezas, and W. Bazán-Vera, “Blockchain in agriculture: A systematic literature review,” in International Conference on Technologies and Innovation. Springer, 2018, pp. 44–56.

[3] T. Alharbi, “Deployment of blockchain technology in software defined networks: A survey,” IEEE Access, vol. 8, no. 1, pp. 9146–9156, 2020.

[4] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, “Blockchain for business applications: A systematic literature review,” in International Conference on Business Information Systems. Springer, 2018, pp. 384–399.

[5] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” **IEEE Communications Surveys & Tutorials**, vol. 21, no. 3, pp. 2794–2830, 2019.

[6] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, “Blockchain in smart grids: A review on different use cases,” Sensors, vol. 19, no. 22, pp. 4862–4886, 2019.

[7] H. Huang, J. Lin, B. Zheng, Z. Zheng, and J. Bian, “When blockchain meets distributed file systems: An overview, challenges, and open issues,” IEEE ACCESS, vol. 8, pp. 50 574–50 586, March 2020.

[8] M. Torky, T. Gaber, and A. E. Hassanien, “Blockchain in Space Industry: Challenges and Solutions,” arXiv preprint arXiv:2002.12878, 2020.

[9] D. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, “Blockchain and AI-based Solutions to Combat Coronavirus (COVID-

概览发现——7个典型的分组

- Group 7: 区块链的总览 (General Overview)
  - Yuan et al. ’16
  - Zheng et al. ’17
  - Zheng et al. ’18
  - Yuan et al. ’18
  - Kolb et al. ’20

[Yuan et al. ’16] Y. Yuan and F.-Y. Wang, “Blockchain: the state of the art and future trends,” Acta Automatica Sinica, vol. 42, no. 4, pp. 481–494, 2016

[Zheng et al. ’17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in Proc. of IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557–564.

[Zheng et al. ’18] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[Yuan et al. ’18] Y. Yuan and F.-Y. Wang, “Blockchain and cryptocurrencies: Model, techniques, and applications,” **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, vol. 48, no. 9, pp. 1421–1428, 2018.

[Kolb et al. ’20] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, “Core Concepts, Challenges, and Future Directions in Blockchain: A Centralized Tutorial,” **ACM Computing Surveys (CSUR)**, vol. 53, no. 1, pp.

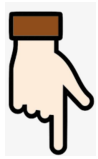
我们发现: 以下方面尚且缺乏概览

- 提高区块链性能的方案
  - 可扩展性 (Scalability)
  - 新框架、新模型

- 加深区块链理解的模型与技术
  - 基于图的理论 (graph-based theories)
  - 基于概率/随机理论 (stochastic/probabilistic models)
  - 基于排队理论 (queueing model-based)

- 区块链研究的工具
  - 实用度量 (Useful measurement)
  - 数据集与实验工具

提纲



近况概览

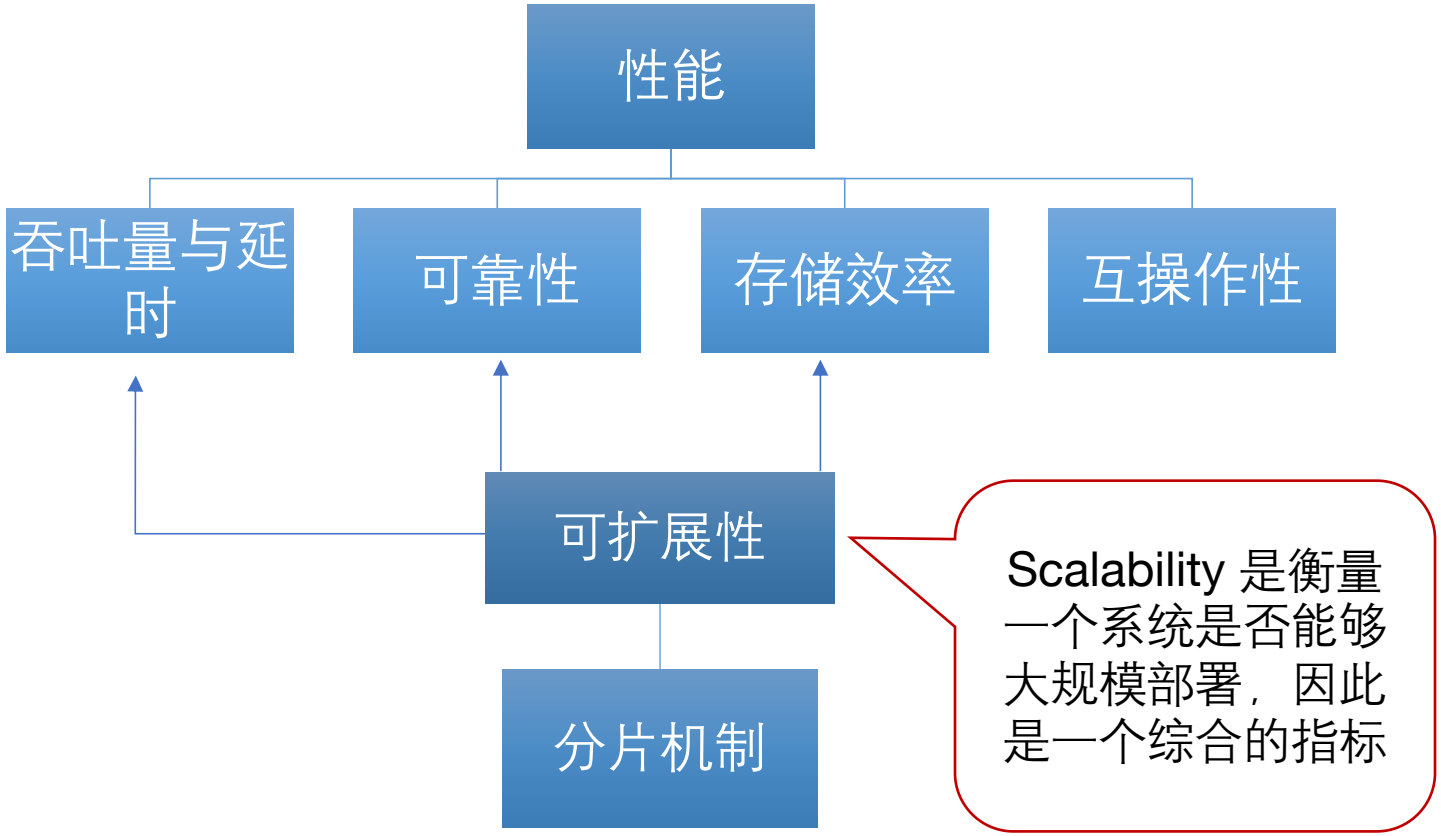
提升区块链性能的方案

加深理解区块链

区块链实验工具与数据集

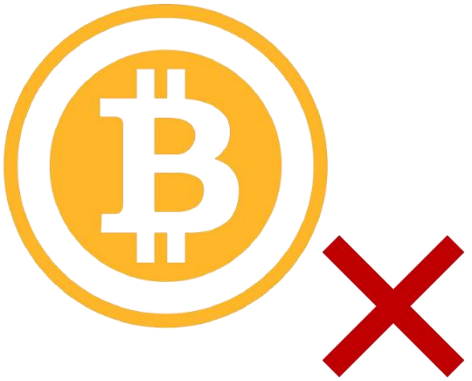
开放问题

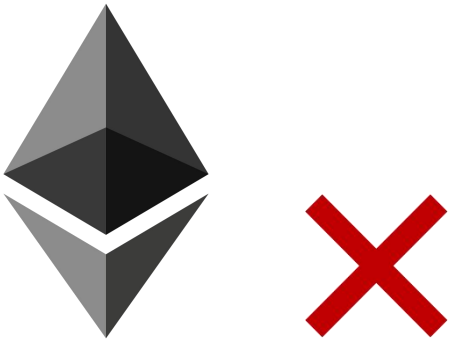
区块链的性能表现
Performance


性能
吞吐量与延时
可靠性
存储效率
互操作性
可扩展性
分片机制
Scalability 是衡量一个系统是否能够大规模部署，因此是一个综合的指标

吞吐量与延时

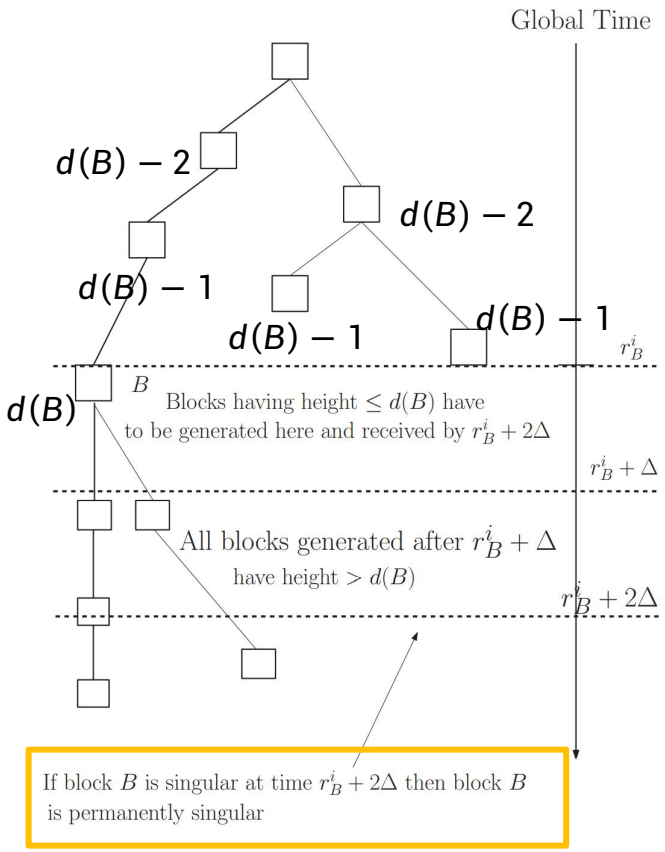
- 关于吞吐量的现状
  - Bitcoin: 3~7 TPS
  - Ethereum1.0: 7~15 TPS
  - Visa: > 1700 TPS
- 关于确认延时 (confirmation latency) 的现状
  - Bitcoin: 60 min in average
  - Ethereum1.0: 6 min in average
- 一个影响区块链落地的重要因素





吞吐量与延时

- 减少确认所需的时间 (confirmation time)
  - 现存问题: 类 Bitcoin 区块链的分叉问题
    - 矿工不能马上决定跟在哪一个块后面进行挖矿
    - 需要等待 6 个块来确认
  - 一个事实: End-to-end latency << inter-block spacing
  - 加速方法：检测出某个高度的 *永久奇异块*

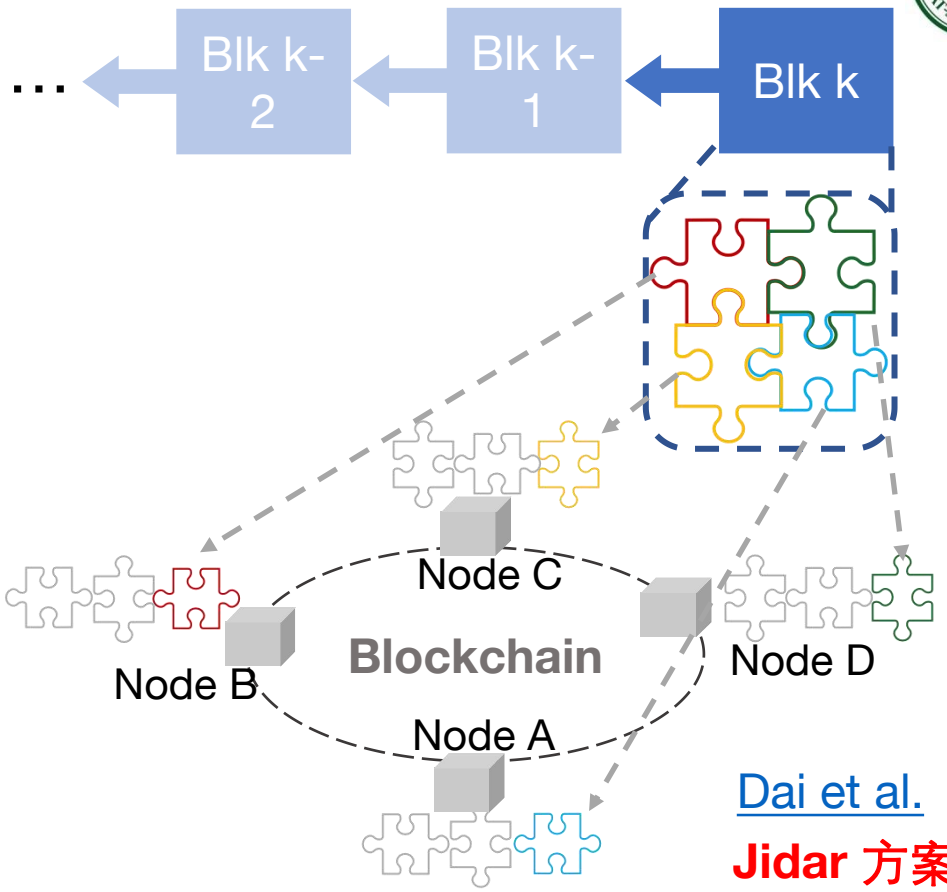


ACCEL

A. Hari, M. Kodialam, and T. Lakshman, “Accel: Accelerating the bitcoin blockchain for high-throughput, low-latency applications,” in IEEE Conference on Computer Communications (**INFOCOM’19**). IEEE, 2019, pp. 2368–2376.

存储效率

- 全节点通常需要存储区块链的整个历史交易！
- 新方案：
  - 基于编码的方案：e.g., 纠删码 Perard et al.
  - 节点只存储一部分历史交易 Dai et al., Xu et al.



[Dai et al.] X. Dai, J. Xiao, W. Yang, C. Wang, and H. Jin, “Jidar: A jigsaw-like data reduction approach without trust assumptions for bitcoin system,” in IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2019, pp. 1317–1326.
[Perard et al.] D. Perard, J. Lacan, Y. Bachy, and J. Detchart, “Erasure code-based low storage blockchain node,” in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018, pp. 1622–1627.
[Xu et al.] Y. Xu and Y. Huang, “Segment blockchain: A size reduced storage mechanism for blockchain,” Preprint, 2020.

可靠性

- 挖矿节点选择 可靠的邻居节点
  - 挖矿的收益 是和 peer 的可靠性 成正比的
  - Peer 的可靠性会影响 TX 的正确性和确认延时

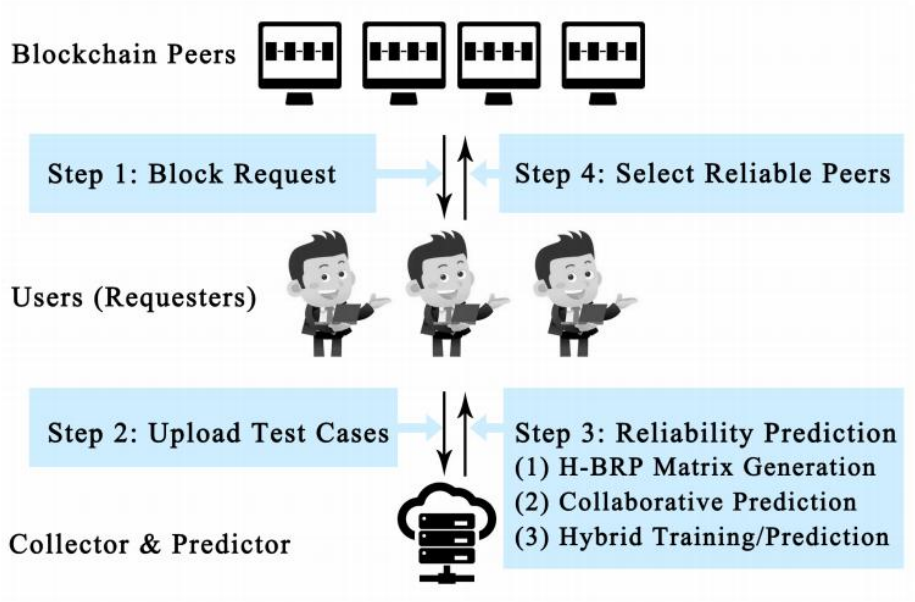


Figure 5: Architecture of the Blockchain Reliability Prediction

Zheng et al. 2019

[Zheng et al.] P. Zheng, Z. Zheng, and L. Chen, “Selecting reliable blockchain peers via hybrid blockchain reliability prediction,” arXiv preprint arXiv:1910.14614, 2019.

互操作性

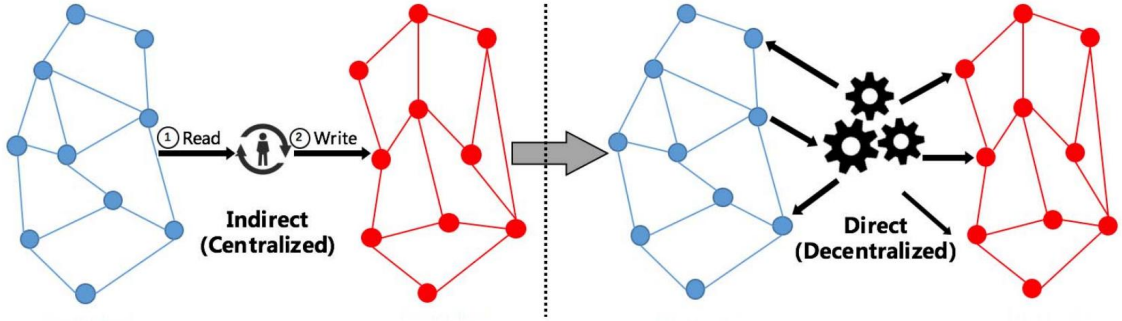
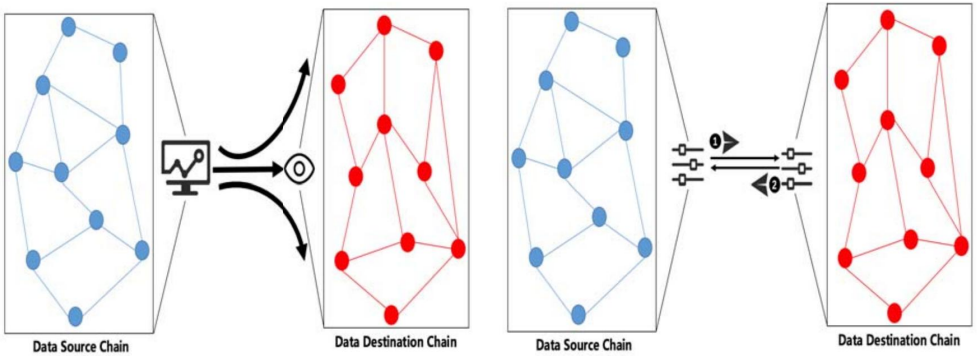


Figure 1: A sketch map of interoperability



(a) Passive mode (b) Active mode

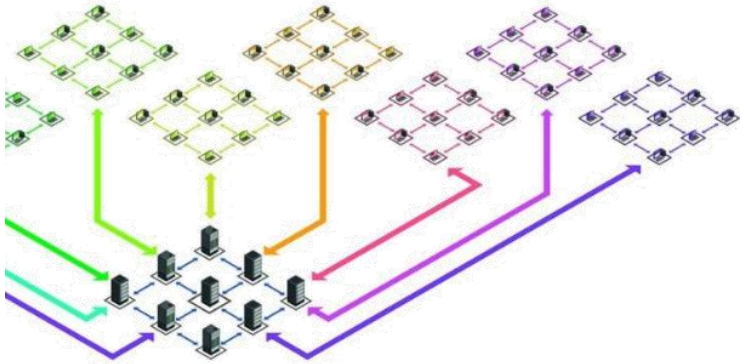
Figure 2: A comparison of two modes of interoperability

- 被动模式
  - 目标链 监听源链
  - 存在问题：沟通开销
  - 解决方法：I/O multiplexing (I/O 多路复用)
- 主动模式
  - 源链 (source chain) 主动向 目标链 (target chain) 发送消息

H. Jin, X. Dai, and J. Xiao, “Towards a Novel Architecture for Enabling Interoperability amongst Multiple Blockchains,” in 2018 IEEE 38th International Conference on Distributed Computing Systems (**ICDCS**). IEEE, 2018, pp. 1203–1211.

提升“可扩展性”—— 分片(Sharding) 方案

- 节点分配方案
  - 随机把节点分配到更小的委员会中，并行地处理交易，每轮重新分配节点 Luu et al.
- 跨片交易效率
  - 减少跨片交易 Nguyen et al.
  - 路由委员会 Zamani et al.
- “委员会”成员分配方案
  - 按节点能力分配 -> 委员会验证能力更均衡 Wang et al.
- 区块的全局排序
  - 区块的逻辑顺序是至关紧要的 Niu et al.



[Luu et al.] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in Proc. of the 2016 ACM SIGSAC **Conference on Computer and Communications Security**, 2016, pp. 17–30.

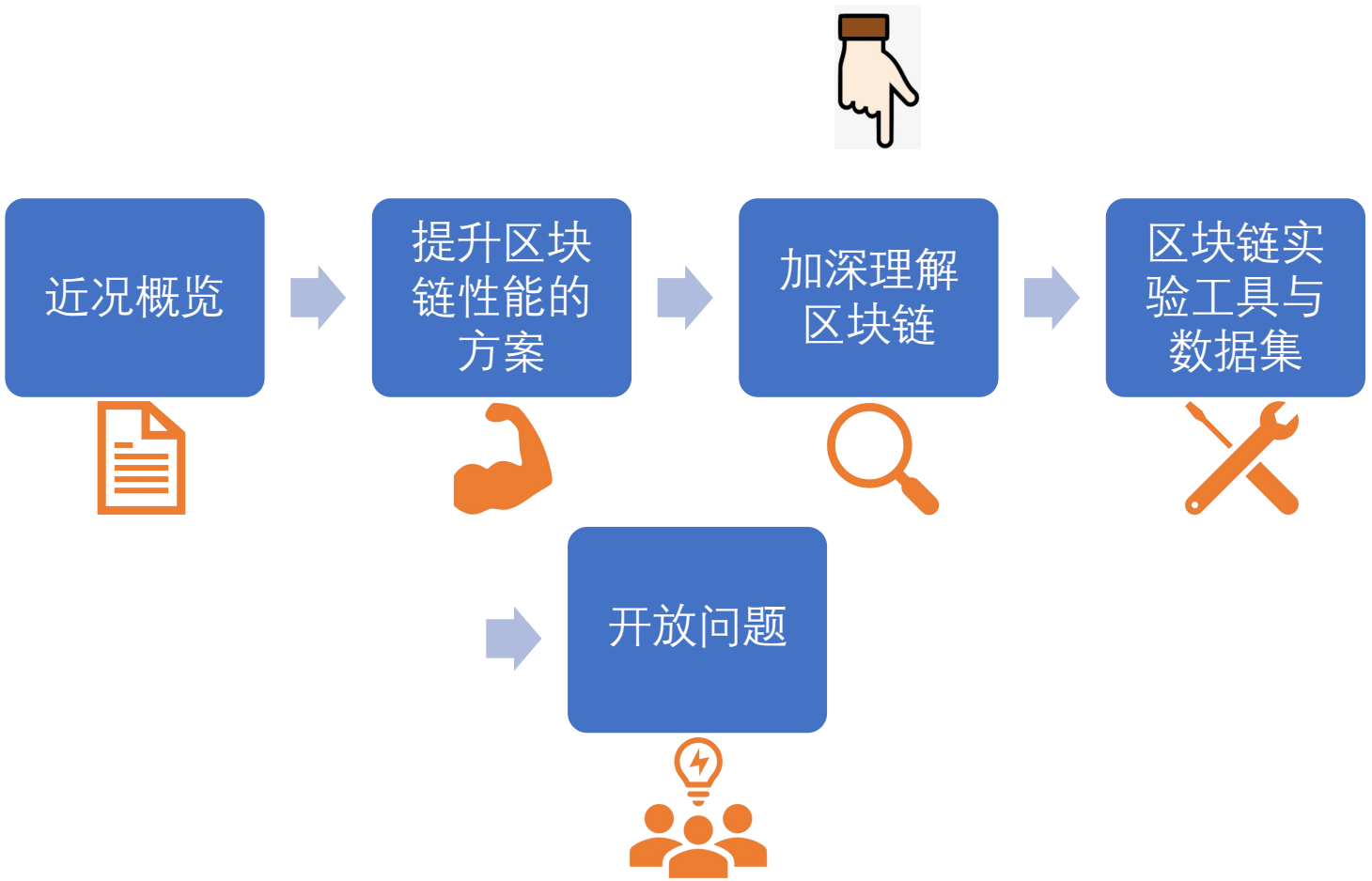
[Nguyen et al.] L. N. Nguyen, T. D. Nguyen, T. N. Dinh, and M. T. Thai, “Optchain: optimal transactions placement for scalable blockchain sharding,” in Proc. of IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019, pp. 525–535.

[Zamani et al.] M. Zamani, M. Movahedi, and M. Raykova, “Rapidchain: Scaling blockchain via full sharding,” in Proceedings of the 2018 ACM SIGSAC **Conference on Computer and Communications Security**, 2018, pp. 931–948.

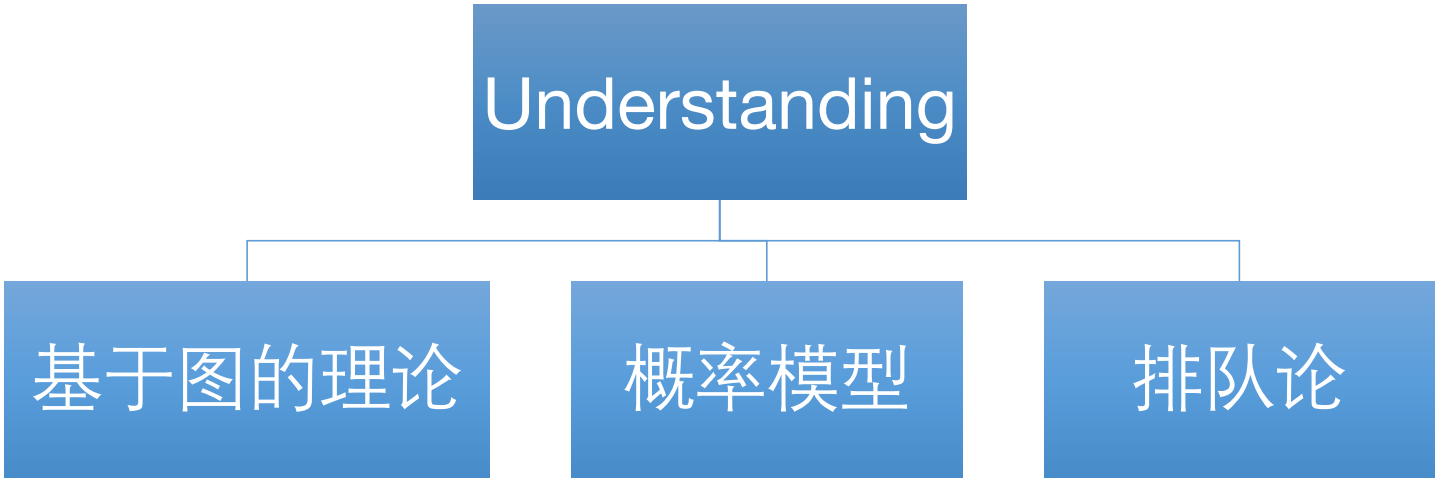
[Wang et al.] J. Wang, Y. Zhou, X. Li, T. Xu, and T. Qiu, “A Node Rating Based Sharding Scheme for Blockchain,” in Proc. of IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2019, pp. 302–309.

[Niu et al.] J. Niu, “Eunomia: A Permissionless Parallel Chain Protocol Based on Logical Clock,” arXiv preprint arXiv:1908.07567, 2019.

提纲

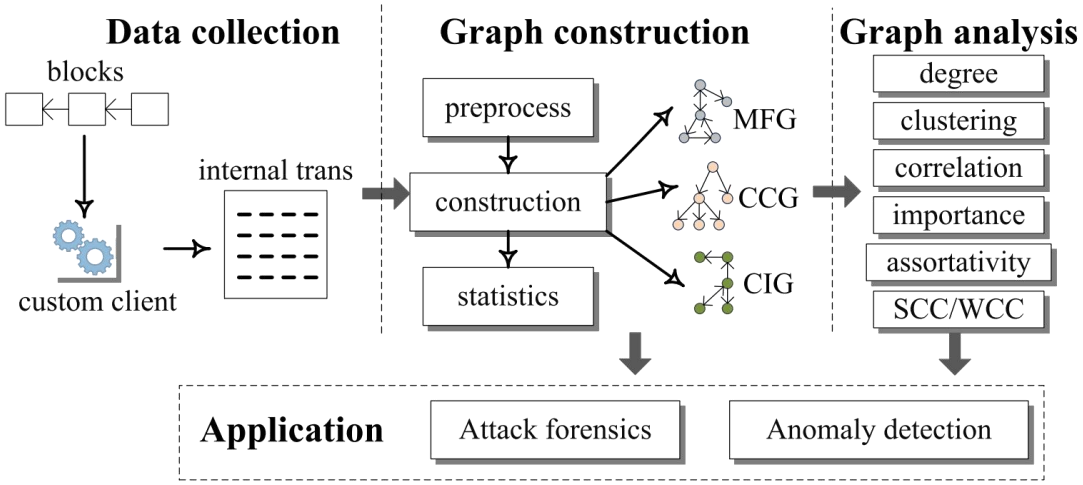


更好地理解区块链
Understanding


Understanding
基于图的理论
概率模型
排队论

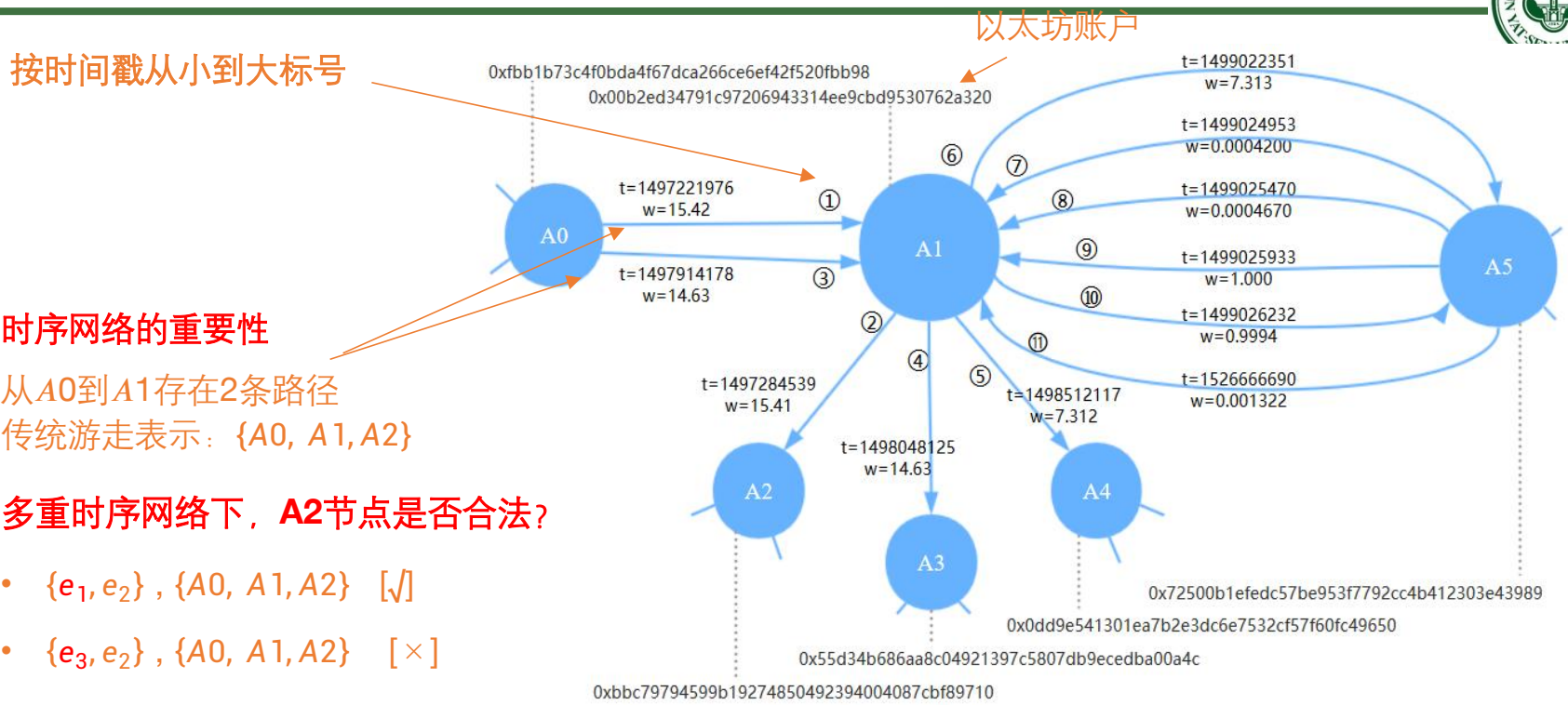
基于图的理论（1/2）

- 基于图的分析方法
- 问题: 分析区块链网络特征
  - 以太坊用户
  - 智能合约
  - 两者间的关系
- 表示形式
  - Money flow graph (MFG)
  - Smart contract creation graph (CCG)
  - Contract invocation graph (CIG)



T. Chen, Y. Zhu, Z. Li, J. Chen, X. Li, X. Luo, X. Lin, and X. Zhange, “Understanding ethereum via graph analysis,” in Proc. of IEEE Conference on Computer Communications (**INFOCOM**). IEEE, 2018, pp. 1484–1492.

基于图的理论（2/2）



时序网络的重要性

从$A0$到$A1$存在2条路径

传统游走表示：$\{A0, A1, A2\}$

多重时序网络下，A2节点是否合法？

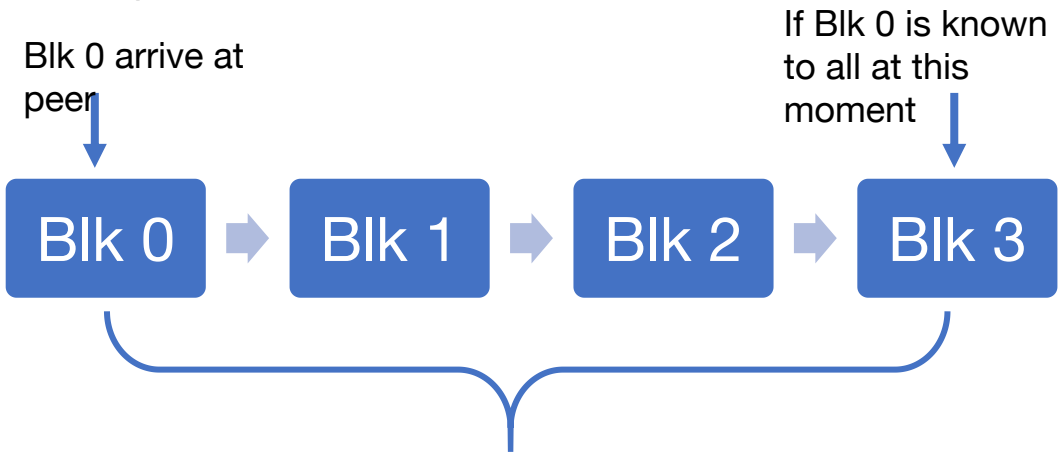
- $\{e_1, e_2\}$, $\{A0, A1, A2\}$ [√]
- $\{e_3, e_2\}$, $\{A0, A1, A2\}$ [×]

- 数学定义：网络$G=(V,E)$, 边$e=(u,v,w,t)$
- 主要特点：允许存在平行边，每个节点表示一个以太坊账户，每条边表示一次交易，包含交易时间t和交易金额w，并按照t从小到大对边进行标号

D. Lin, J. Wu, Q. Yuan, Z. Zheng, “Modeling and Understanding Ethereum Transaction Records via A Complex Network Approach.” in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 11, pp. 2737-2741, Nov. 2020

基于概率的分析模型 (1/2)

- 常用于区块链的性能分析，研究各指标间的 tradeoff
- 常见的性能指标
  - 区块产生速率 [1]
  - 区块的全局确认时间 [2]
  - 区块上链的周期长度 [2]
  - 攻击的成功概率
  - …
- 分片技术的指标:
  - 随机事件使委员会失效的概率边界 [3]
  - …



Papadis et al., Gopalan et al., Hafid et al.

[1] N. Papadis, S. Borst, A. Walid, M. Grissa, and L. Tassiulas, “Stochastic models and wide-area network measurements for blockchain design and analysis,” in Proc. of IEEE Conference on Computer Communications (**INFOCOM**). IEEE, 2018, pp. 2546–2554.

[2] A. Gopalan, A. Sankararaman, A. Walid, and S. Vishwanath, “Stability and Scalability of Blockchain Systems,” arXiv preprint arXiv:2002.02567, 2020.

[3] A. Hafid, A. S. Hafid, and M. Samih, “A probabilistic security analysis of sharding-based blockchain protocols,” in Proc. of International Congress on Blockchain and Applications (Blockchain), March 2019, pp. 55–60.

基于概率的分析模型 (2/2)

- 其他一些有趣的探索 Papadis et al., Gopalan et al., Hafid et al.
  - 如何改变挖矿难度而不牺牲安全水平 (How to change difficulty mining without sacrificing safety level) [1]
  - 区块链稳定性受底层 P2P 网络的连通性的影响 (Bounds on blockchain stability depend on the connectivity of the P2P network) [2]
  - 使用委员会失效的 概率边界 用于分析整个分片区块链系统 (Using the bound of committee failure we can analyze the whole sharding blockchain system) [3]

[1] N. Papadis, S. Borst, A. Walid, M. Grissa, and L. Tassiulas, “Stochastic models and wide-area network measurements for blockchain design and analysis,” in Proc. of IEEE Conference on Computer Communications (**INFOCOM**). IEEE, 2018, pp. 2546–2554.

[2] A. Gopalan, A. Sankararaman, A. Walid, and S. Vishwanath, “Stability and Scalability of Blockchain Systems,” arXiv preprint arXiv:2002.02567, 2020.

[3] A. Hafid, A. S. Hafid, and M. Samih, “A probabilistic security analysis of sharding-based blockchain protocols,” in Proc. of International Congress on Blockchain and Applications (Blockchain), March 2019, pp. 55–60.

基于排队论的分析模型

- 研究/解决的问题
  - 对挖矿过程、块生成过程进行建模 [1][2]
    - **Markovian** batch-service queueing system
  - 减少块确认时间 [3]
    - Queueing model to characterize confirmation time
    - Early distinguish using the characteristics and ML method
  - 挖矿资源分配 [4] — Prof. LIU Jia, Iowa State University
    - **Lyapunov optimization**-based queueing analytical model

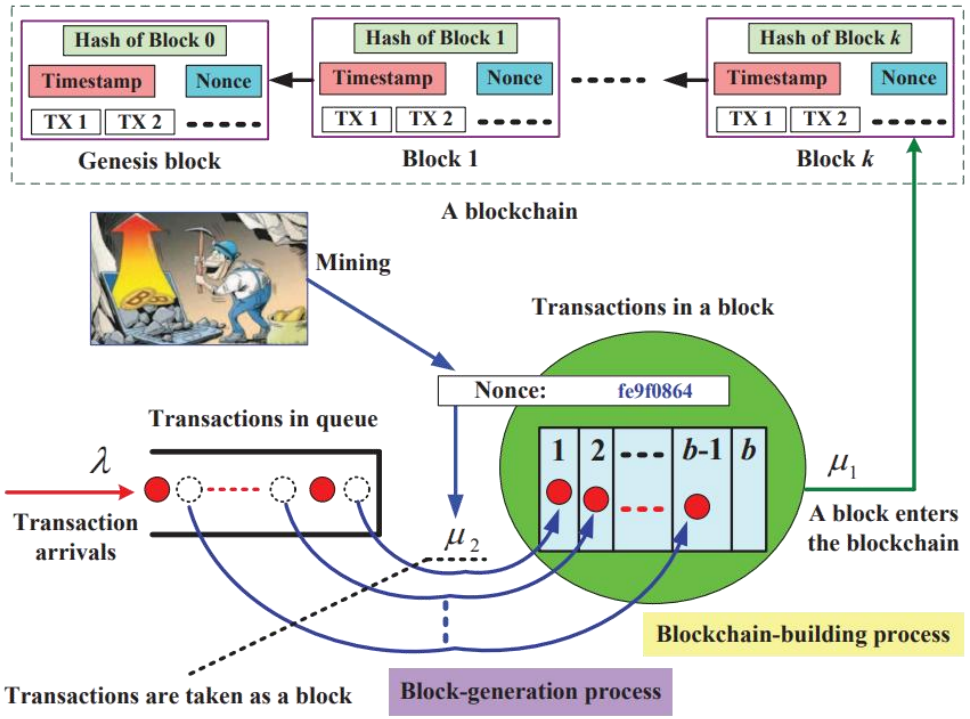


Fig. 1. A blockchain queueing system [1]

[1] Q.-L. Li, J.-Y. Ma, and Y.-X. Chang, "Blockchain queue theory," in International Conference on Computational Social Networks. Springer, 2018, pp. 25–40.

[2] Q.-L. Li, J.-Y. Ma, Y.-X. Chang, F.-Q. Ma, and H.-B. Yu, "Markov processes in blockchain systems," Computational Social Networks, vol. 6, no. 1, pp. 1–28, 2019.

[3] S. Ricci, E. Ferreira, D. S. Menasche, A. Ziviani, J. E. Souza, and A. B. Vieira, "Learning blockchain delays: a queueing theory approach," ACM SIGMETRICS Performance Evaluation Review, vol. 46, no. 3, pp. 122–125, 2019.

[4] M. Fang and J. Liu, "Toward low-cost and stable blockchain networks," arXiv preprint arXiv:2002.08027, 2020.

针对数字货币用户行为/智能合约的数据挖掘

- 欺诈行为的检测
  - 智能合约中有潜在的诈骗风险，如庞氏骗局
  - 特征提取
    - 用户
    - 合约代码
  - 常用方法：回归树分类器

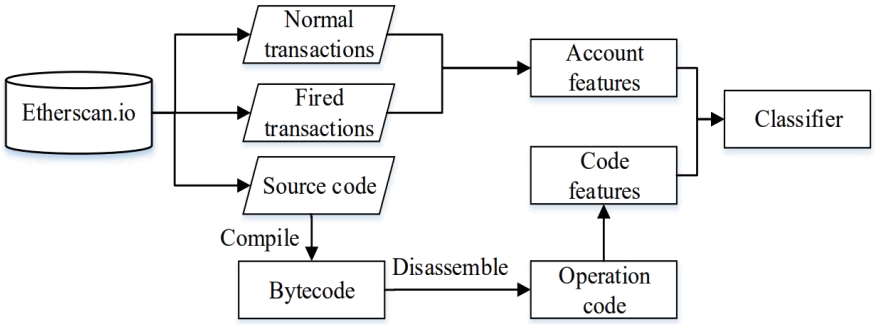
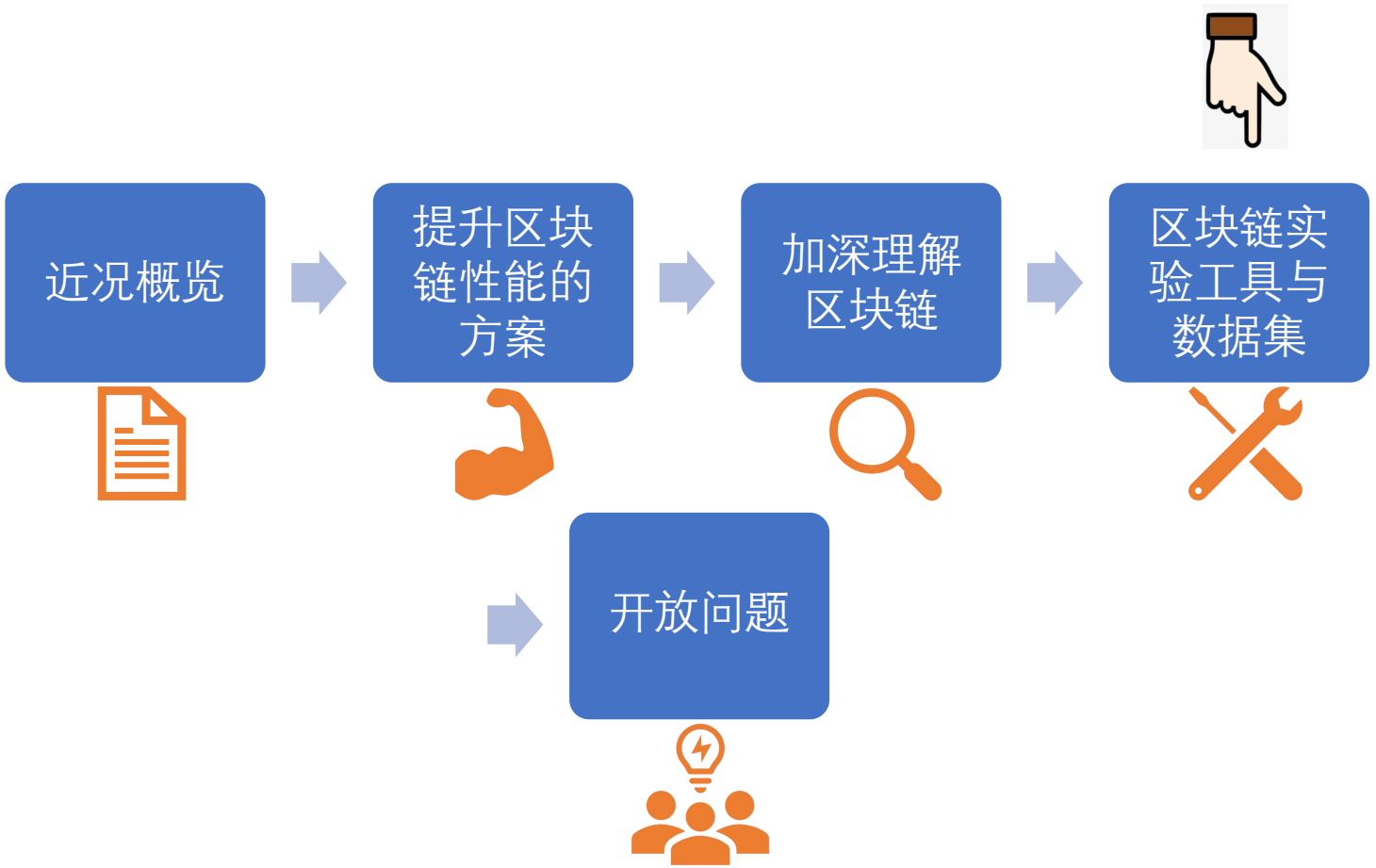


Figure 2: The Framework of Smart Ponzi Schemes Detection

W. Chen, **Z. Zheng**, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in Proceedings of the 2018 World Wide Web Conference (WWW), 2018, pp. 1409–1418.

提纲



实验数据与工具
Tools

针对三种区块链的性能测量

- 公链，联盟链，私有链

Tools	Metrics	Target Blockchain
Gervais et al. [1]	Block interval, block size, and throughput	Public Chain: Bitcoin, Litecoin, Dogecoin, Ethereum
Blockbench [2]	Throughput and latency, Scalability, Fault tolerance and security, CPU utilization, Network utilization, etc.	Private blockchains
Nasir et al. [3]	Execution time, latency, throughput, scalability vs the number of blockchain nodes	Consortium blockchains: Hyperledger Fabrics

[1] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in Proceedings of the 2016 ACM SIGSAC **conference on computer and communications security**, 2016, pp. 3–16.
[2] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, “Blockbench: A framework for analyzing private blockchains,” in Proc. of the 2017 ACM International Conference on Management of Data, 2017, pp. 1085–1100.
[3] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, “Performance analysis of hyperledger fabric platforms,” Security and Communication Networks, vol. 2018, 2018.

常见的数据集与性能测量工具

Tools	Utilization	Target Blockchain
Xblock [1] [2] [3]	**Dataset:** TPS, Average response delay, Transactions per CPU, TX per memory second, TX per disk I/O and TX per network data	Ethereum, Parity, CITA, Hyperledger Fabric , EOS
Blockbench [4]	**Measuring tool:** Authors proposed a benchmarking framework for measuring the **data processing capability** and **performance** of different layers of a blockchain system.	Private blockchains
Nodefinder [5]	**Measuring tool:** Network size and geographic distribution of Ethereum network nodes	Ethereum
Alsahan et al. [6]	**Network simulator:** for the performance measurements of Bitcoin using lightweight virtualization technologies.	Bitcoin network

[1] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," in Proc. of IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP), 2018, pp. 134–143.

[2] P. Zheng, Z. Zheng, and H.-n. Dai, "Xblock-eth: Extracting and exploring blockchain data from etherem," arXiv preprint arXiv:1911.00169, 2019.

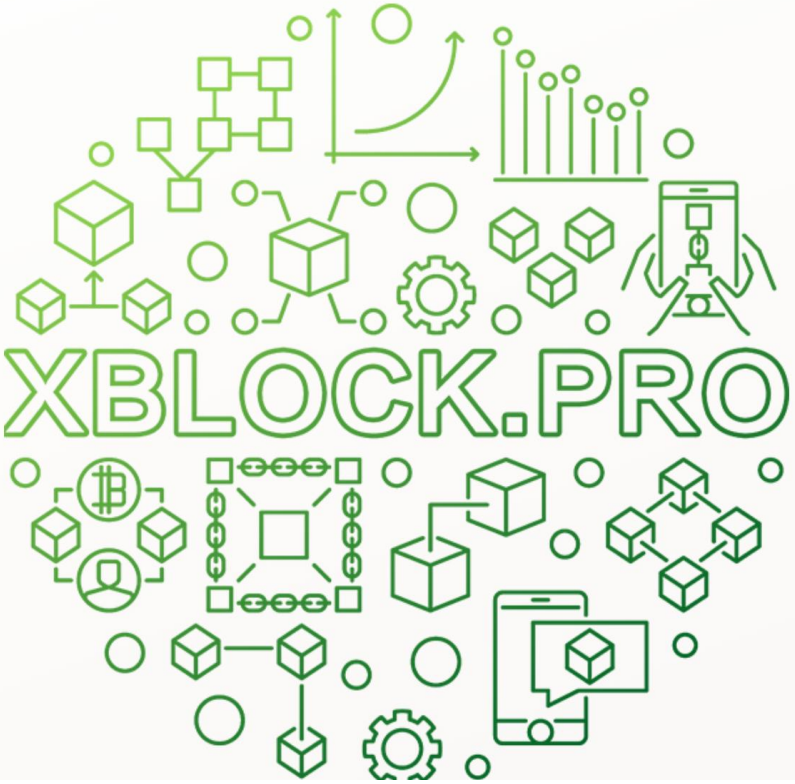
[3] W. Zheng, Z. Zheng, H.-N. Dai, X. Chen, and P. Zheng, "Xblock-eos: Extracting and exploring blockchain data from eosio," arXiv preprint arXiv:2003.11967, 2020.

[4] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in Proc. of the 2017 ACM International Conference on Management of Data, 2017, pp. 1085–1100.

[5] S. K. Kim, Z. Ma, S. Murali, J. Mason, A. Miller, and M. Bailey, "Measuring Ethereum Network Peers," in Proc. of the Internet Measurement Conference (IMC'18), 2018, pp. 91–104.

[6] L. Alsahan, N. Lasla, and M. M. Abdallah, "Local bitcoin network simulator for performance evaluation using lightweight virtualization,"

xblock.pro



eXplore Blockchain Reliability

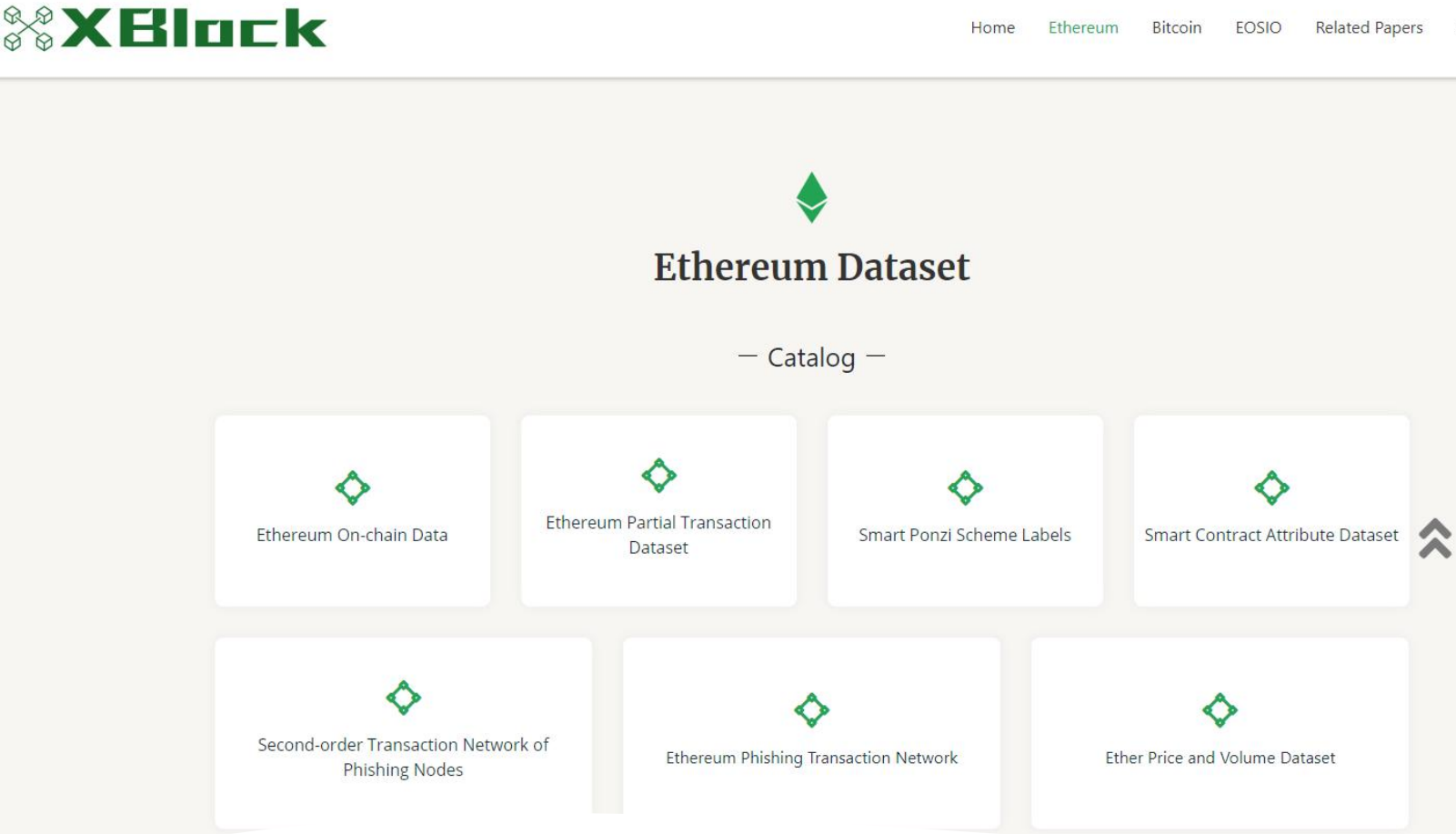
XBLOCK.PRO

XBlock collects the current mainstream blockchain data and is one of the blockchain data platforms with the largest amount of data and the widest coverage in the academic community.

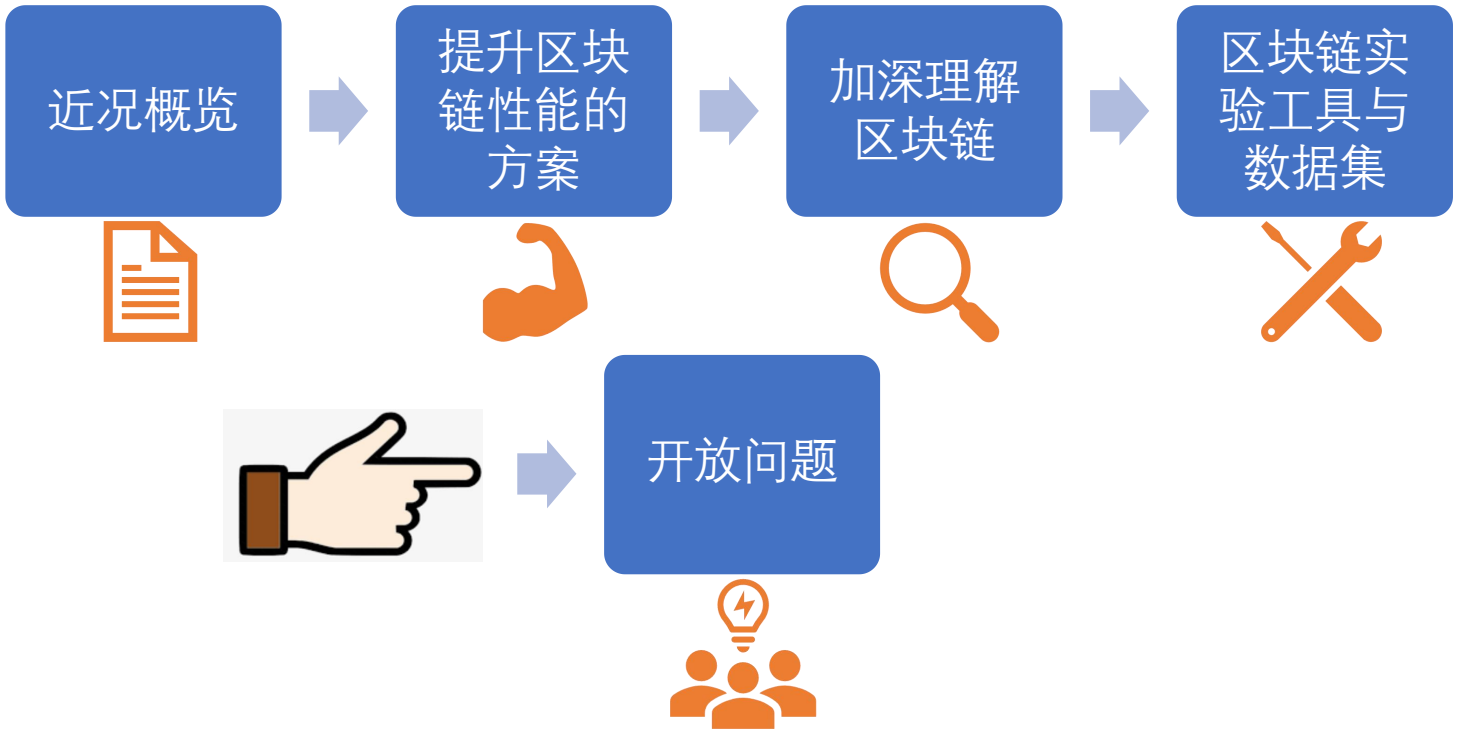
All blockchain datasets have been cleaned and classified in a standardized way, which can be easily downloaded into a standard and consistent format.

Xblock

Dataset for Various Blockchains



提纲



开放问题
Open Issues

开放问题

- 区块链性能提升
  - 可扩展性：分片、侧链、链下扩容、DAG …
  - 跨片性能
    - 只能容忍至多 1/3 的恶意节点
    - 额外的跨片开销、延时
  - 硬件支持/网络层技术加速区块链: RDMA, SGX
- 大数据与区块链的融合
  - 中心化与去中心化
  - 用户数据的隐私保护问题
  - 打破数据孤岛

开放问题

- 开发更加健全的理论模型来加深对区块链的理解
  - 使用更一般化的排队论模型来描述现实系统中交易到达，挖矿等与排队相关的阶段
  - 使用基于优先级的交易处理、块处理策略，以达到某个预定义的安全等级
- 安全问题
  - 用户上链数据的隐私保护
  - 各种攻击的应对机制，如“挖矿劫持(Cryptojacking)”
- 实验工具
  - 更强大、标准的 实验平台/模拟工具