区块链扩容的难点和误区

任之勘
VeChain

About me

- 唯链高级研究员
- 荷兰代尔夫特理工大学博士，博士后，主要研究方向区块链共识算法，区块链应用，网络信息论
- 在国际学术会议上发表多篇区块链论文，包括
  - FC2019 – 区块链领域实质上的旗舰会议
  - CVCBT2018 – IEEE旗下第一个区块链会议
  - DISC2018，INFOCOM2019等
- 在知乎上著有专栏区块链演义
- 开设国内第一个共识算法课程

比特币扩容

“为什么比特币不可扩展”

- 输出只有7TPS，而主流支付系统至少1,000-10,000 TPS，双十一支付宝峰值可达到十万TPS。
  - *问题1：比特币的7TPS是怎么算出来的*
- 比特币扩容
  - 增大区块
  - 缩小区块间隔
- *问题2：这么做会有什么问题?*

比特币扩容

- POW的意义是什么？
  - 一个每隔一段时间，无偏向地随机选取一个节点出块的机制。并且保证被选中概率正比于某种可以验证的资源。

- POW采用的方式：算力竞赛
  - 然而，我们其实并不是在比算力，而是累积算力
    - 即：算力*有效挖矿时间
  - 而不同节点的有效挖矿时间并不相同

有效挖矿

- 什么是有效挖矿?
  - 当你挖的区块有可能最终成为最长链的一部分的时候
  - ≈ 当你在目前的最长链上挖矿的时候
- 什么时候矿工在无效挖矿?
  - 当没有在目前的最长链上挖矿的时候。
    - 出了新的合法区块但是矿工还在旧区块上挖矿的时候
    - 在某个不会成为主链的分叉上挖矿的时候
    - 在非法区块上挖矿的时候
- 矿工并不总是在有效挖矿
  - 因为他们需要时间来同步和验证最新的区块

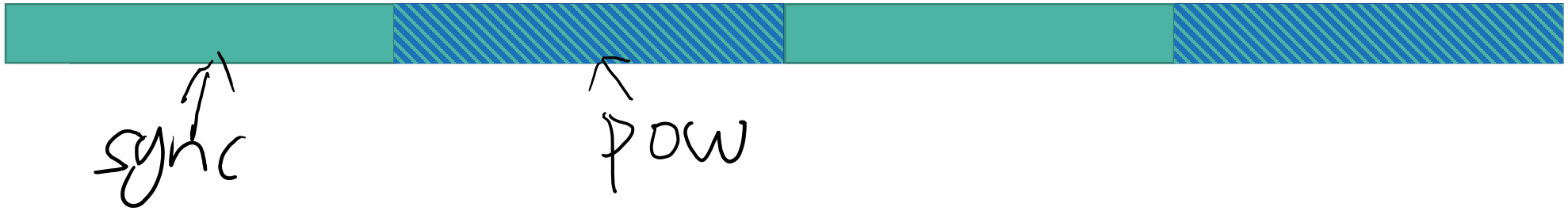
比特币POW的结构

- 比特币POW的结构是串行的。
  - 理想状态下，比特币要求所有节点同步最新区块后，再开始算力竞赛

- 异步系统不支持这种串行结构
  - 所以，我们要求同步时间远小于区块间隔
  - 然而，（同步时间/区块间隔）与输出成正比

比特币POW的结构

- 如果（同步时间/区块间隔）增大会发生什么?



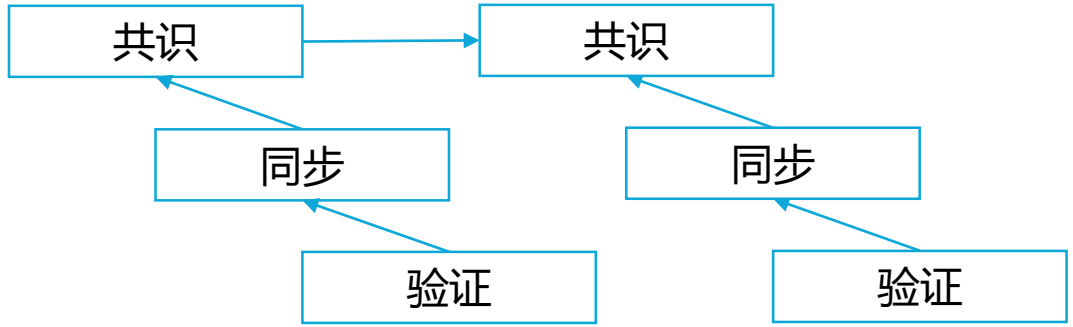
- 同步过程中无效挖矿增加
- 分叉几率增加导致POW过程中算力被浪费。

POW的安全性

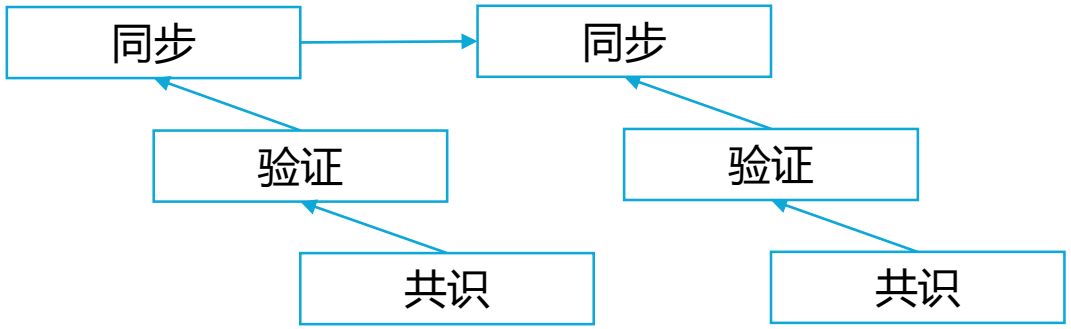
- 比特币只认最长链，即：只有有效挖矿才对安全性有贡献
  - 比特币的安全性：恶意节点的累积算力>D
  - D = 诚实节点的累积的有效算力
    - 换言之，如果节点都在无效挖矿，系统的安全性会下降。
  - *问题3：为什么？*
    - *如何在比特币中进行双重支付攻击?*
- （同步时间/区块间隔）增大 → 安全性下降
  - 提高输出 →（同步时间/区块间隔）增大
  - 结论：提高输出 → 安全性下降，同步时间/区块间隔 = I 时，安全性=0

可扩展POW

- 想要扩展比特币POW，需要并行同步和POW
- 领袖选择:

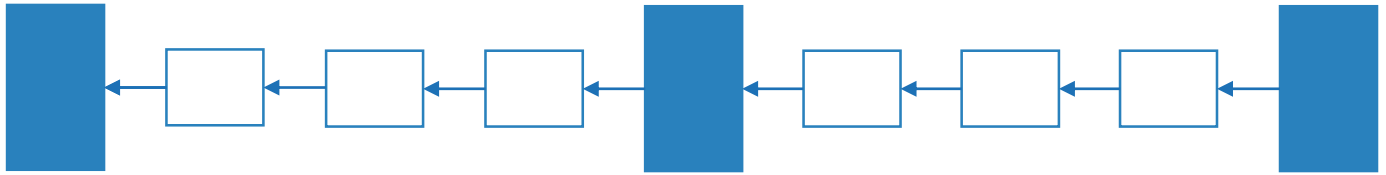


- DAG（有向无环图）+POW:



领袖选择

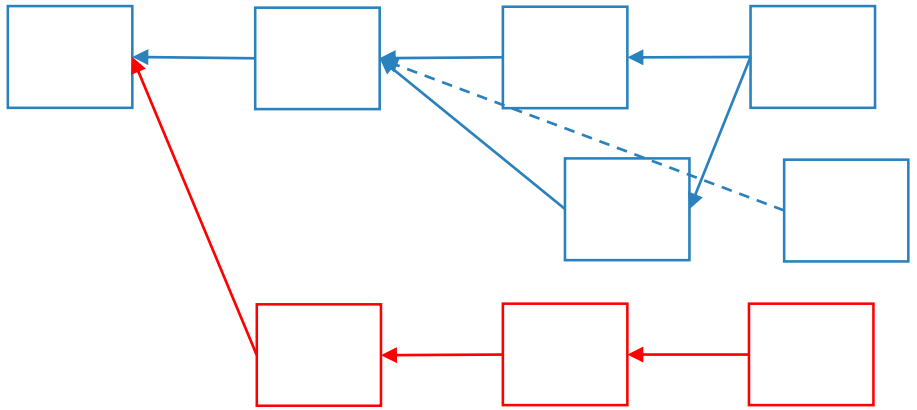
- 与其对于区块达成共识，我们可以只采用POW对出块者达成共识
  - *问题4：这里有什么问题?*
  - Bitcoin-NG: 一个领袖，采用有毒交易惩罚恶意领袖



    - *问题5：为什么不分叉?*
  - Byzcoin, Hybrid consensus: 多个领袖（委员会），用大数定理保证领袖大概率诚实
  - 两者在输出上的优劣
    - 单个领袖：恶意领袖会造成输出下降
    - 多个领袖：领袖之间的通信复杂度

POW+DAG

- 从矿工的看比特币POW的问题：为什么需要同步？
  - 如果没有同步，那么你的算力并没有贡献给系统的安全性
    - 那么，如果我们对此加以改进呢，使得即便没有及时同步，你的算力仍旧会贡献给安全性呢？
    - GHOST：采用DAG结构，并且用“最重子树”规则代替“最长链”规则
  - 同步时间延长。
    - *问题6：同步时间增加了多少？*



POS和POW-DAG

- POS和POW-DAG是以上思路的继承者：
- 基于随机数发生器的POS
  - Bitcoin-NG：Snow White，Ouroboros
  - Byzcoin，Hybrid Consensus：ALGORAND，Dfinity
- POW-DAG
  - GHOST：Spectre，Phantom，the tangle，Conflux，Prism
- 第四课

区块链可扩展性问题

- 现在，我们理解了比特币扩容的问题
  - 然而，比特币扩容 ≠ 区块链可扩展性
- 一个“可扩展的区块链” 可能是:
  - Bitcoin Cash（SV），Segwit
  - 可扩展POW
  - 采用了可扩展BFT的联盟链（第二课）
  - 采用了分片或者链下技术达到无限扩展的区块链算法（第五课）

课后讨论

- 这节课我们学习了比特币扩容问题和一些基本解决方法。
  - 核心：POW与消息同步的并行
- 同时，我们也知道了区块链扩容 ≠ 比特币扩容
  - 在今后看到“可扩展区块链”的时候需要留心
- 课后讨论题：
  1. *比特币POW的串行结构是不是中本聪的设计失误?*
  2. *Bitcoin Cash为什么可以将区块大小提升到8M?*
  3. *Bitcoin-NG是不是可以让领袖上传任意大小和数量的微区块，从而任意提高输出?*

References

- Narayanan, Arvind, et al. *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press, 2016.
- Croman, K., et al. “On scaling decentralized blockchains.” *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2016.
- Eyal, Ittay, et al. “Bitcoin-ng: A scalable blockchain protocol.” *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*. 2016.
- Pass, Rafael, and Elaine Shi. “Hybrid consensus: Efficient consensus in the permissionless model.” *31st International Symposium on Distributed Computing (DISC 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.
- Kogias, Eleftherios Kokoris, et al. “Enhancing bitcoin security and performance with strong consistency via collective signing.” *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 2016.
- Sompolinsky, Yonatan, and Aviv Zohar. “Secure high-rate transaction processing in bitcoin.” *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2015.
- Bagaria, Vivek, et al. "Deconstructing the blockchain to approach physical limits." *arXiv preprint arXiv:1810.08092* (2018).

References

- Kiayias, Aggelos, et al. “Ouroboros: A provably secure proof-of-stake blockchain protocol.” *Annual International Cryptology Conference*. Springer, Cham, 2017.
- Daian, Phil, Rafael Pass, and Elaine Shi. “Snow white: Robustly reconfigurable consensus and applications to provably secure proofs of stake.” *International Conference on Financial Cryptography and Data Security*. Springer, St. Kitts, 2019.
- Gilad, Yossi, et al. “Algorand: Scaling byzantine agreements for cryptocurrencies.” *Proceedings of the 26th Symposium on Operating Systems Principles*. ACM, 2017.
- Sompolinsky, Yonatan, and Aviv Zohar. “PHANTOM: A Scalable BlockDAG Protocol.” *IACR Cryptology ePrint Archive*2018 (2018): 104.
- Li, Chenxing, et al. “Scaling nakamoto consensus to thousands of transactions per second.” *arXiv preprint arXiv:1805.03870* (2018).
- https://dfinity.org/
- https://www.iota.org/

谢谢!