不成熟的思路：

1. 比特币的SPV（Simplified payment verification）技术使得用户在不需要下载全链数据的情况下可以对某笔交易进行验证，可以视为全链的一个精简，也可以视为一个实时同步的支链
   1. 那么，不需要下载全链的情况下进行查询？或者设计一种用于查询的支链？
2. 同时，以太坊也有一个类似的操作，即state-tree pruning，是将以太坊全数据的中的历史程序运行状态数据删除。这样的话，相当于每个人都存有一个自己的支链，同时通过主链完成共识
   1. 是否可以模仿这种不对称的主链-支链结构？
3. Cosmos Network是一个“区块链网络”，可以在运行同一的拜占庭容错协议（例如现在使用的是Tendermint）的基础上，实现链间的交互和交易
   1. 能不能在运行不同容错协议的平台上，利用智能合约等手段，实现交互（不一定是交易，也可能作为认证等功能的载体）
   2. 既然能区块链间网络，那理论上也可以在区块链和DAG（有向无环图，例如IOTA等加密货币正在使用）之间进行交互，或是区块链和传统数据库进行交互
4. 如果将实现了智能合约的区块链称作“虚拟机”（事实上，以太坊就实现了“以太坊虚拟机”），那么，现在的区块链就是高价的“内存”，而链外的交易（如闪电网络等）就是低价的“硬盘”。如果从这个角度做文章
   1. 这部分不了解，考虑参考一下体系结构内二级存储方面的文章
   2. 软件结构方向有几篇区块链相关的论文（不过基本没做出什么东西）可以参考一下。

偏可行的思路：

1. IPFS（InterPlanetary File System）和分布式存储的SiaCoin等应用使得区块链的一些节点有了距离，时间等概念，可以试着设计一种新的区块链结构，以优化链上的查询需求。
   1. 进度：做IPFS和SiaCoin的调研中，对“需求”增加了解
   2. 其它：本思路未必能有结果，主要还是看灵感
2. 通过将数据库日志存储在链上，实现数据的溯源
   1. 应该可以通过Hyperledger Fabric实现，整体来说是实现一个接口，将Oracle等数据库的日志写到链上，以实现多个（不同）数据库之间数据溯源，数据认证。
   2. 进度：正在配置HyperFabric
   3. 其它：主要的难度在于链的出块速度可能跟不上日志产生速度。
   4. 其它2：比较工程，方便上手，所以先以这个为例进行实现。

可以参考的项目/文章：（未整理）

Dinh, Tien Tuan Anh, et al. "Blockbench: A framework for analyzing private blockchains." Proceedings of the 2017 ACM International Conference on Management of Data. ACM, 2017.

K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels,

A. Kosba, A. Miller, P. Saxena, E. Shi, and E. G¨un.

On scaling decentralized blockchains. In Proc. 3rd

Workshop on Bitcoin and Blockchain Research, 2016.

ipfs ipdb

D. Ongaro and J. Ousterhout. In search of an

understandable consensus algorithm. In USENIX

ATC, 2014.

CUB, a Consensus Unit-based Storage Scheme for Blockchain System（ICDE2018，没有原文）

Zihuan XU (Hong Kong University of Science and Technology)

Siyuan HAN (Hong Kong University of Science and Technology)

Lei Chen (Hong Kong University of Science and Technology)

Tutorial: Blockchains and Databases(VLDB2017), By C.Mohan from IBM

https://www.facebook.com/notes/mohan-c-mohan/permissioned-blockchains-and-databases/10155027556287295

McConaghy, Trent, et al. "BigchainDB: a scalable blockchain database." white paper, BigChainDB (2016).

Gaetani, Edoardo, et al. "Blockchain-based database to ensure data integrity in cloud computing environments." (2017).

Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." Open and Big Data (OBD), International Conference on. IEEE, 2016.

Zikratov, I.A., Kuzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L. (2017). Ensuring data integrity using blockchain technology. 2017 20th Conference of Open Innovations Association (FRUCT), 534-539.

S. Wang, T. T. A . Dinh, Q. Lin, Z. Xie, M. Zhang, Q. Cai, G. Chen, W. Fu, B.C. Ooi, P. Ruan: ForkBase: An Efficient Storage Engine for Blockchain and Forkable Applications. February 2018

When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies

A. Miller, M. M?ser, K. Lee, and A. Narayanan, “An empirical analysis of linkability

in the Monero blockchain,” arXiv preprint arXiv:1704.04299, 2017.

M. M?ser and R. B?hme, “The price of anonymity: empirical evidence from a

market for Bitcoin anonymization,” Journal of Cybersecurity, 2017.

A fistful of Bitcoins: characterizing payments among men with no names in International Conference

on Applied Cryptography and Network Security. Springer, 2016,

Corda

Toward Open Data Blockchain Analytics: A Bitcoin Perspective

D. McGinn, D McIlwraith, Y.Guo

Database Perspectives on Blockchains

Sara Cohen, Aviv Zohar

(Submitted on 15 Mar 2018)

Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]// Conference on Internet Measurement Conference. ACM, 2013:127-140.

Bitcoin's Security Model Revisited

Yonatan Sompolinsky, Aviv Zohar

Yasin, Affan, and Lin Liu. "An online identity and smart contract management system." Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual. Vol. 2. IEEE, 2016.

The challenge of decentralized marketplaces arxiv

Dynamic Distributed Storage for Scaling Blockchains arxiv

New kids on the block: an analysis of modern blockchains

Bitcoin API：This is a C++ wrapper library for JSON-RPC communication with the Bitcoin daemon. It allows developers to communicate with the Bitcoin daemon without the need to pack and unpack JSON-RPC messages and thus simplifies the interaction with it.

https://github.com/hkalodner/bitcoin-api-cpp/tree/995357f62aa09d8abacf2bee6941b2a024272a34

J. Rubin, “Bitcoin spark framework (btcspark),” https://github.com/JeremyRubin/

BTCSpark.

“Private blockchain” is just a confusing name for a shared database， Arvind Narayanan， AP of Princeton， writer of "BlockSci"

https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/

"The use of these crypto techniques for building a tamper-resistant database has been known for 25 years. At first there wasn’t much impetus for Wall Street to pay attention, but gradually there has arisen a great opportunity in moving some types of financial infrastructure to an automated, cryptographically secured model."

Blockchain vs. Centralized Database https://www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/

How to TIme-Stamp a Digital Document， Stuart Haber(\*a database that is hard to tamper and easier to audit\*)

Taylor, M.B. (2013). Bitcoin and the age of Bespoke Silicon. 2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), 1-10.

Liang, X., Shetty, S., Tosh, D.K., Kamhoua, C.A., Kwiat, K.A., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 468-477.

Dorri, A., Kanhere, S.S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 618-623.

Weaver: A High-Performance, Transactional Graph Database Based on Refinable Timestamps

piChain: When a Blockchain meets Paxos.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A.B., & Chen, S. (2016). The Blockchain as a Software Connector. 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), 182-191.

https://www.factom.com/products/harmony

Harmony is a new blockchain base document technology that works with your existing imaging or document management solution to create a secure, transparent, unalterable record for the final loan documents.

https://www.rsk.co/

RSK is the first open-source smart contract platform with a 2-way peg to Bitcoin that also rewards the Bitcoin miners via merge-mining, allowing them to actively participate in the Smart Contract revolution. RSK goal is to add value and functionality to the Bitcoin ecosystem by enabling smart-contracts, near instant payments and higher-scalability.

IoTex

use sidechains(they called it blockchain-in-blockchain) to provide service for IoT