区块链的五张面孔

可信数据库的观点

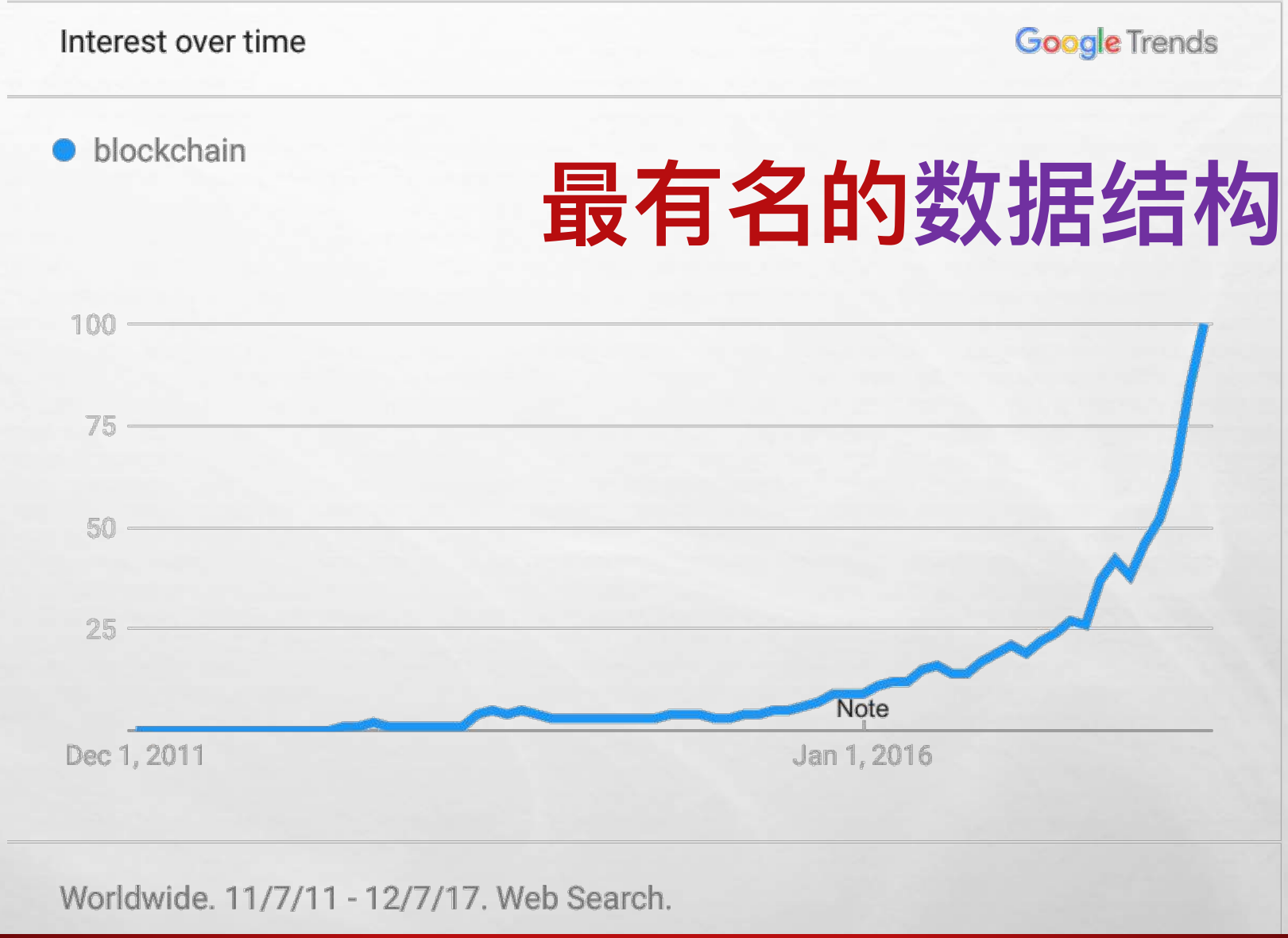
MULTI-FACES OF BLOCKCHAINS

钱卫宁
华东师范大学
数据科学与工程学院

五张面孔

数据结构

$$\mathrm{Hash}\left([tx_1, tx_2, \ldots] \,||\, h_{t-1} \,||\, t \right) \rightarrow h_t$$

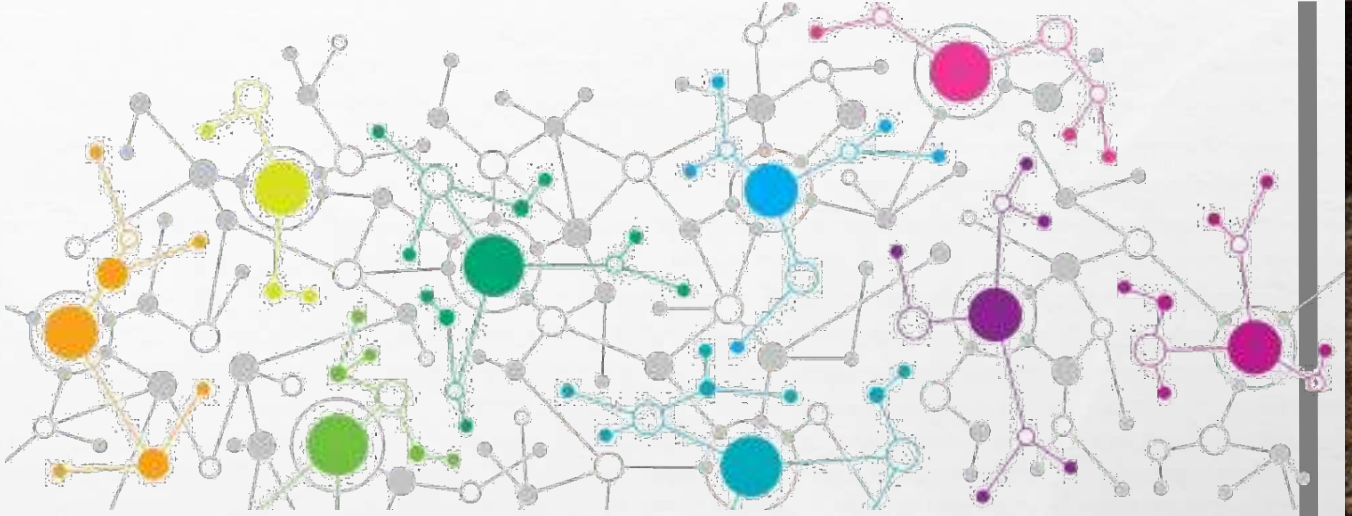

Interest over time
Google Trends
blockchain
100
75
50
25
Note
Dec 1, 2011
Jan 1, 2016
Worldwide. 11/7/11 - 12/7/17. Web Search.

最有名的数据结构

防篡改

- 票根与区块构成钩稽关系
  - 根据密码学原理，由前驱区块确定票根的计算过程，是算力的刚性开销。
  - 如果在任一区块篡改数据，必须花等量算力重新计算后继票根，否则将破坏钩稽关系。
  - 由于票根的本质是哈希链，篡改历史数据会导致重复计算所有后续票根，密码学原理保证这将得不偿失。

去中心



- 节点对等 PEER-TO-PEER
- 全副本存储 FULL REPLICATION
- 强一致 STRONG CONSISTENCY
- 分布式共识 CONSENSUS

完整性（Integrity）

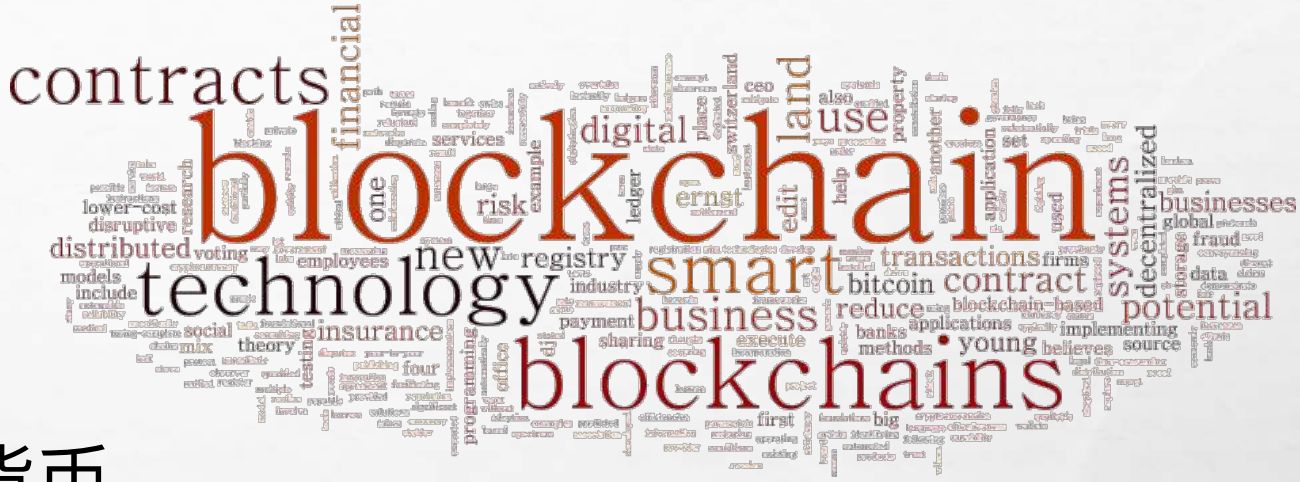
- 智能合约：

以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议。

A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.

Nick Szabo: Smart Contracts: Building Blocks for Digital Markets. 1996
http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

FINTECH



- 电子加密货币
  - 比特币
  - 国家货币
  - 社区货币
- ICO代币
- 非赢利组织/慈善
- 社交网络
- …

区块链 vs 数据库

方面	区块链	数据库系统
结构	链式结构	日志
	–	数据库状态 (snapshot)
可信	防篡改	–
架构	去中心	强中心
数据访问与处理	K–V	模式管理
	API	SQL
	智能合约	触发器，存储过程
应用	FinTech +++	通用

两个应用

上海钢贸诈骗案的风险警示与对策

文 / 本刊记者 李静宇

10 年前，只有少数几家商业银行探索仓单质押这项业务，现在，几乎所有的银行都在开展此项业务。以中储为例，与中储合作的银行已有 20 多家总行，2 百多家分支行。

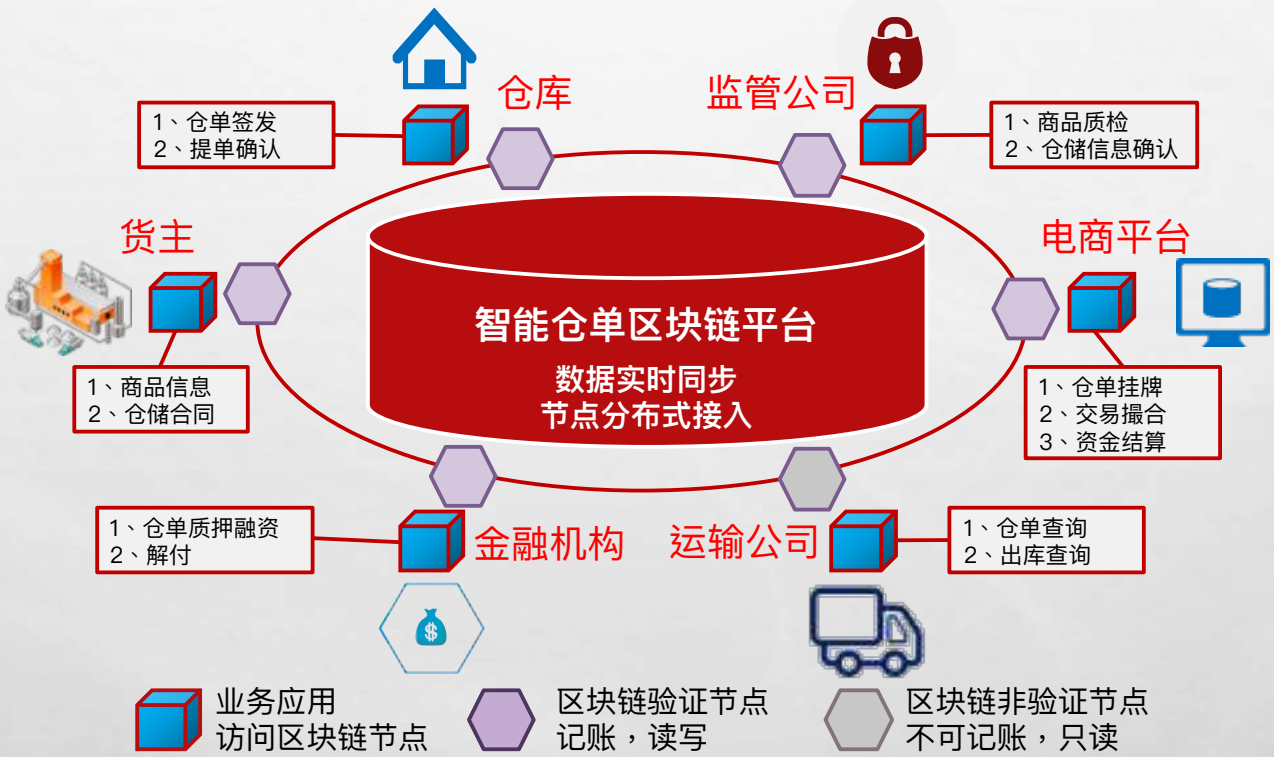
从物流企业看，除中储、中远、中外运等开展此项业务较早的企业之外，铁路、港口码头、资产管理公司、担保公司也纷纷加入，有的银行还专门成立了自己的监管公司。

然而在历经多年度高速度发展之后，质押监督积累多年的问题也逐渐暴露出来，尤其因质押监管不利或是不当所引发的问题在 2012 年集中而且大面积爆发，正如中国物资储运协会会长姜超峰所说，“无论是发案次数、涉案金额、涉案企业，还是案件的复杂程度，都是前所未有的。”

应用场景A－仓单管理

应用场景A–仓单管理

华师大 — 欧冶
产业互联网大数据与区块链实验室
ECNU-Ouyeel Joint Lab on Big Data and Blockchain for Industrial Internet



欧冶物流电子仓单 凭单提货 L-OYCD17010400014

存货人：河南钢铁加工有限公司
持有人：河南钢铁加工有限公司
有效期：2017-01-11~2017-01-27
仓库地址：上海市广灵四路开隆大厦甲24号
生成日期：2017-01-04

品种	规格	单位	数量	包装	仓储费率	重量
冷轧卷	0.5*1500*32		1	xxxxx	*元/吨	10吨
备注：||						
冷轧	0.7*1387*C		1	xxxxx	*元/吨	65吨
备注：||						
冷轧	8*1600*6000*切边*Q/BQB 310 QStE380TM* *IB 1		1	xxxxx	*元/吨	123吨
备注：||						

捆包清单 重量合计：208吨

监管人：欧冶物流
复核人： 复核日期：

应用场景B–“安全屋”

UCLOUD

交易场地

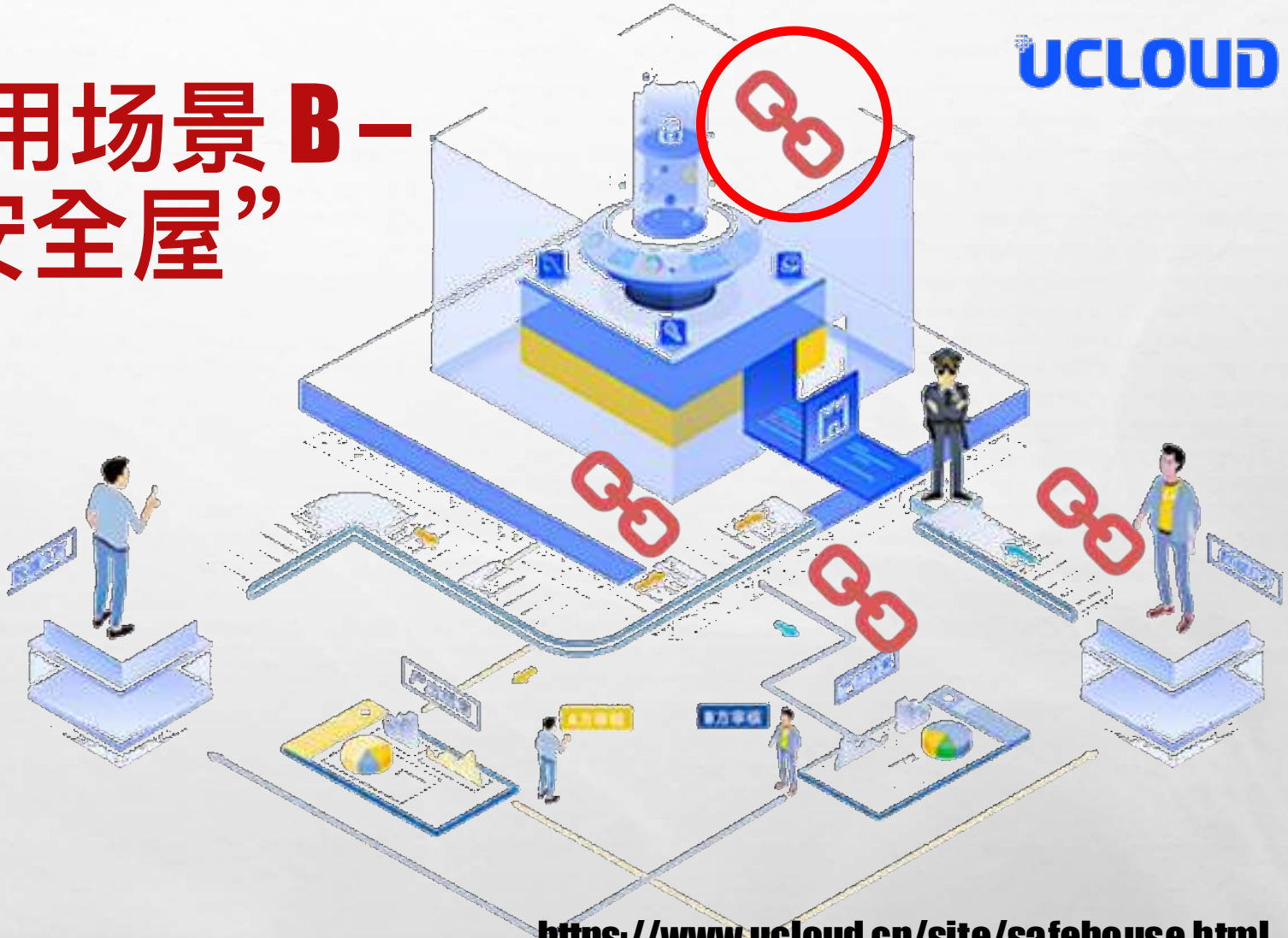
+

保安

+

监控摄像头

应用场景 B – “安全屋”



https://www.ucloud.cn/site/safehouse.html

应用需求

更高

事务

回溯

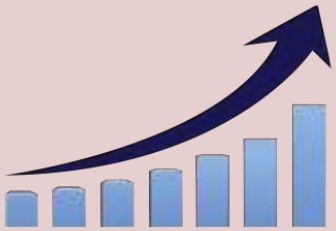
SQL

多库

模式

API

更快



Scalability

Throughput: 1,000→100,000

Latacy: s → ms

更强

机器学习算法

智能合约

A → B

A → B

可审计

可校验

更高？
API => SQL

- 众享比特 **ChainSQL** 2017年1月
- 德国 **BigchainDB** 2016年2月
- 腾讯 **Trust SQL** 2017年4月

更高？
联动＝链上＋链下

物流企业

- (本地)运输/仓单信息 ＋ (链上)货物信息

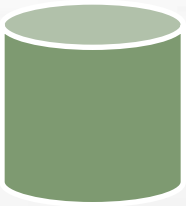
银行

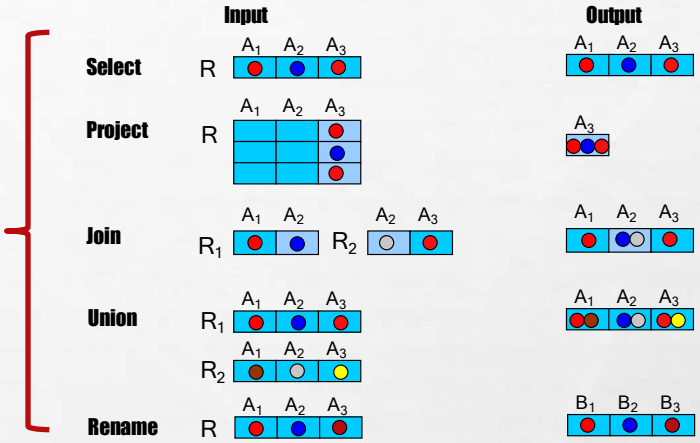
- (本地)企业信息 ＋ (链上)货物信息

监管

- (本地)本地数据库 ＋ (链上)货物流转信息

更高？
溯源查询



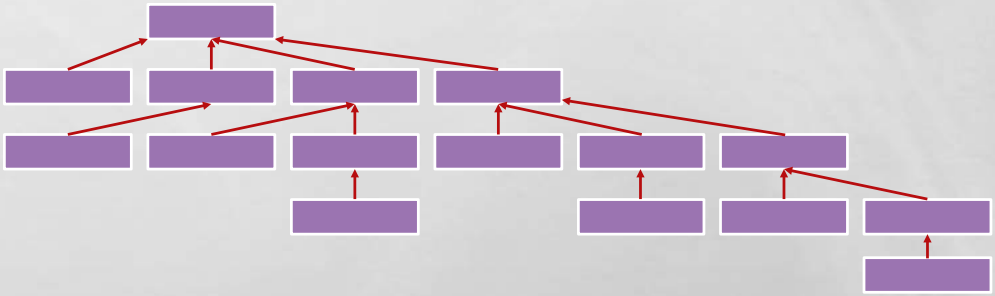


在传统关系数据库系统中可以通过标记传播的方式记录数据的世系（lineage，provenance）

Peter Buneman, Wang Chiew Tan:Provenance in databases. SIGMOD Conference 2007: 1171-1173

在区块链上，由于没有数据库的“当前状态”，需要构建索引，避免扫描整链。

- 随之带来链和索引间的同步问题
- 索引的可信性需要保障



更快？
吞吐率

System	Consensus Protocol	Throughput	Environment Setting
Kadena/Juno	ScalableBFT	7,000 tps	256 node cluster
Symbiont	BFT-SMaRt	80,000 tps	4 node cluster in LAN
Ripple	RPCA	1,000 tps	-
Sawtooth Lake	Proof of Elapsed Time	70,000 tps	LAN

Christian Cachin, Marko Vukolic:
Blockchain Consensus Protocols in the Wild (Keynote Talk).
DISC 2017: 1:1-1:16

更快？
吞吐率

- 事务处理性能与事务复杂性紧密相关
- TPC–C 事务高度复杂
- 分布式事务处理的可扩展性是难题

TPC

http://www.tpc.org/tpcc/results/tpcc_advanced_sort.asp

~50,000 tps for TPC-C workload

TPC-C - All Results - Sorted by Performance
Version 5 Results As of 2-Dec-2017 at 8:06 AM [GMT]

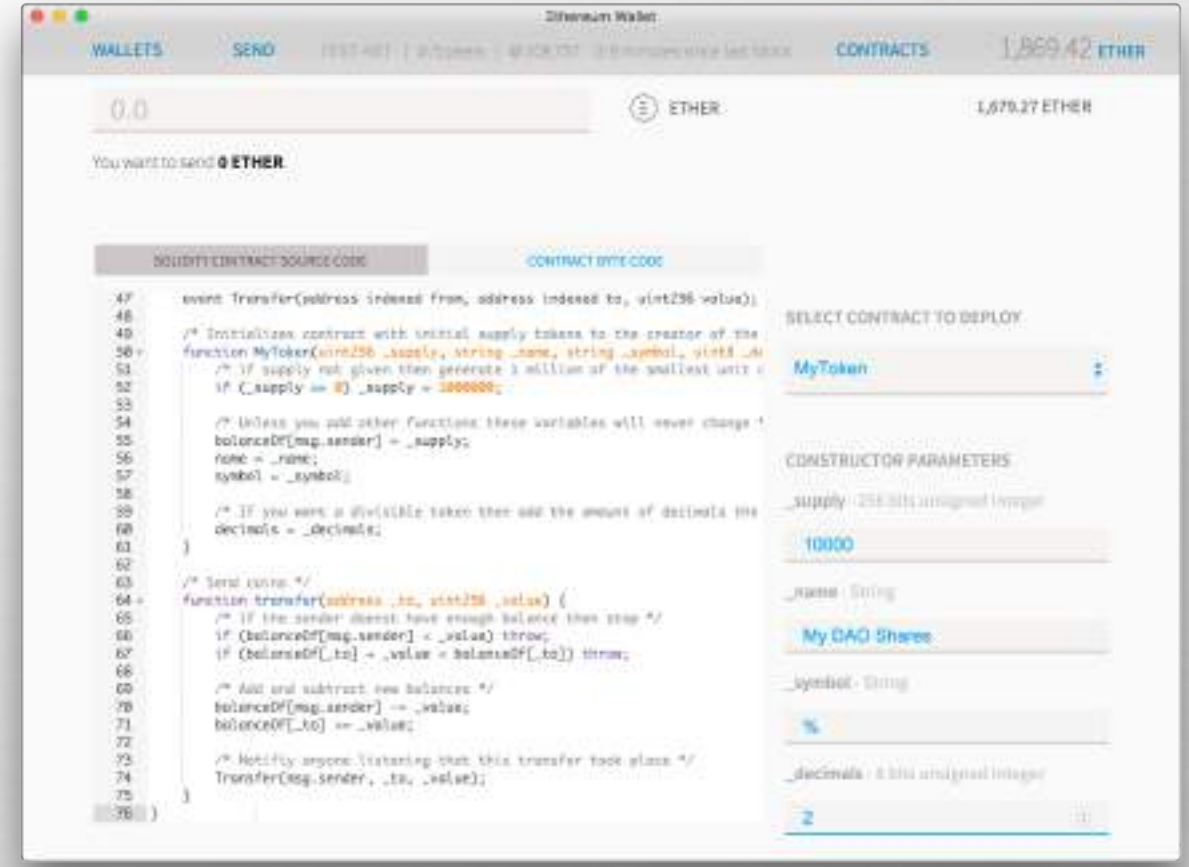
Results displayed with a grey background are ***Historical Results***, which might not be up to date with regards to pricing and/or availability of HW or SW.

Click on the column header to sort on that column; click again to reverse the sort order.

Hardware Vendor	System	tpmC	Price/tpmC	Watts/KtpmC	System Availability	Database	Operating System	TP Monitor	Date Submitted
ORACLE	SPARC SuperCluster with T3-4 Servers	30,249,688	1.01 USD	NR	06/01/11	Oracle Database 11g R2 Enterprise Edition w/RAC w/Partitioning	Oracle Solaris 10 09/10	Oracle Tuxedo CFSR	12/02/10
IBM	IBM Power 780 Server Model 9179-MHB	10,366,254	1.38 USD	NR	10/13/10	IBM DB2 9.7	AIX Version 6.1	Microsoft COM+	08/17/10
ORACLE	SPARC T5-8 Server	8,552,523	.55 USD	NR	09/25/13	Oracle 11g Release 2 Enterprise Edition with Oracle Partitioning	Oracle Solaris 11.1	Oracle Tuxedo CFSR	03/26/13
ORACLE	Sun SPARC Enterprise T5440 Server Cluster	7,646,486	2.36 USD	NR	03/19/10	Oracle Database 11g Enterprise Edition w/RAC w/Partitioning	Sun Solaris 10 10/09	Oracle Tuxedo CFSR	11/03/09
IBM	IBM Power 595 Server Model 9119-FHA	6,085,166	2.81 USD	NR	12/10/08	IBM DB2 9.5	IBM AIX 5L V5.3	Microsoft COM+	06/10/08

更强？
智能合约

- 正确性验证
- 事前、
  事中、
  事后审计



更强？
机器学习算法

- 正确性验证
- 算法理解
  - 是否泄漏隐私？
- 事后审计

```scala
package org.apache.spark.examples

import org.apache.spark.SparkContext._
import org.apache.spark.{SparkConf, SparkContext}

object SparkPageRank {

  def showWarning() {
    System.err.println(
      """WARN: This is a naive implementation of PageRank and is given as an example!
        |Please use the PageRank implementation found in org.apache.spark.graphx.lib.PageRank
        |for more conventional use.
      """.stripMargin)
  }

  def main(args: Array[String]) {
    if (args.length < 1) {
      System.err.println("Usage: SparkPageRank <file> <iter>")
      System.exit(1)
    }

    showWarning()

    val sparkConf = new SparkConf().setAppName("PageRank")
    val iters = if (args.length > 1) args(1).toInt else 10
    val ctx = new SparkContext(sparkConf)
    val lines = ctx.textFile(args(0), 1)
    val links = lines.map{ s =>
      val parts = s.split("\\s+")
      (parts(0), parts(1))
    }.distinct().groupByKey().cache()
    var ranks = links.mapValues(v => 1.0)

    for (i <- 1 to iters) {
      val contribs = links.join(ranks).values.flatMap{ case (urls, rank) =>
        val size = urls.size
        urls.map(url => (url, rank / size))
      }
      ranks = contribs.reduceByKey(_ + _).mapValues(0.15 + 0.85 * _)
    }

    val output = ranks.collect()
    output.foreach(tup => println(tup._1 + " has rank: " + tup._2 + "."))

    ctx.stop()
  }
}
```

讨论与思考

去中心 vs 弱中心 vs 多中心

多个可信中心的场景更常见

- 政府部门
- “联盟”盟主、副盟主
- 常务理事单位
- ……

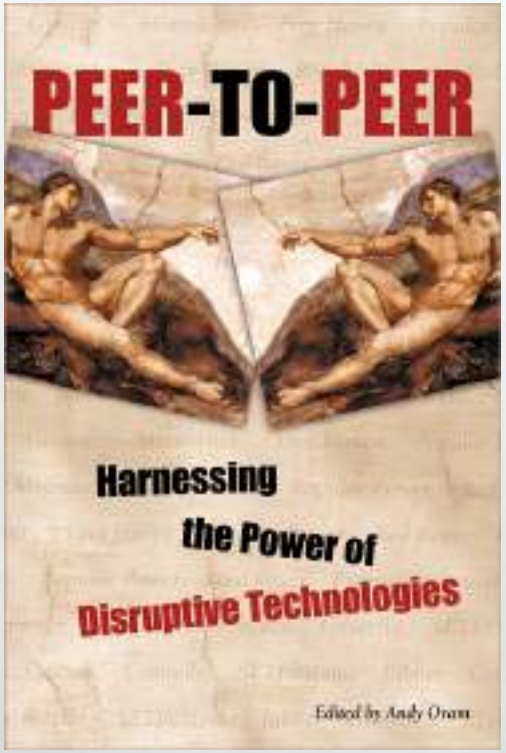
数据全副本操作性低

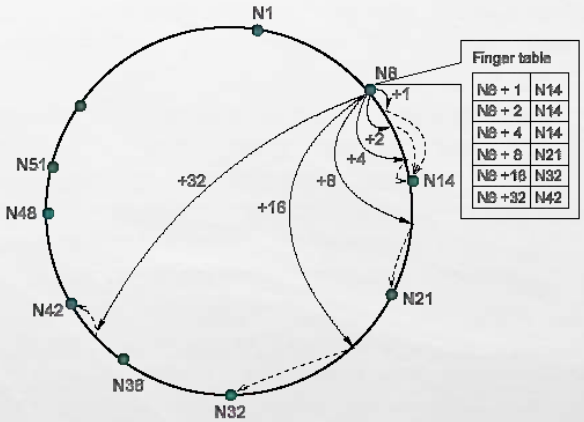
- 每个中心只负责管理自己的那部分数据

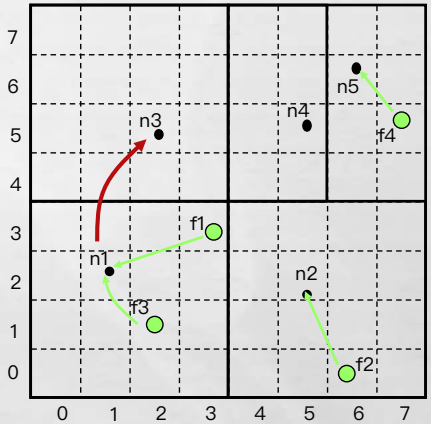
部分数据间存在关联

- 可以进行相互验证

10+年以前：P2P Computing



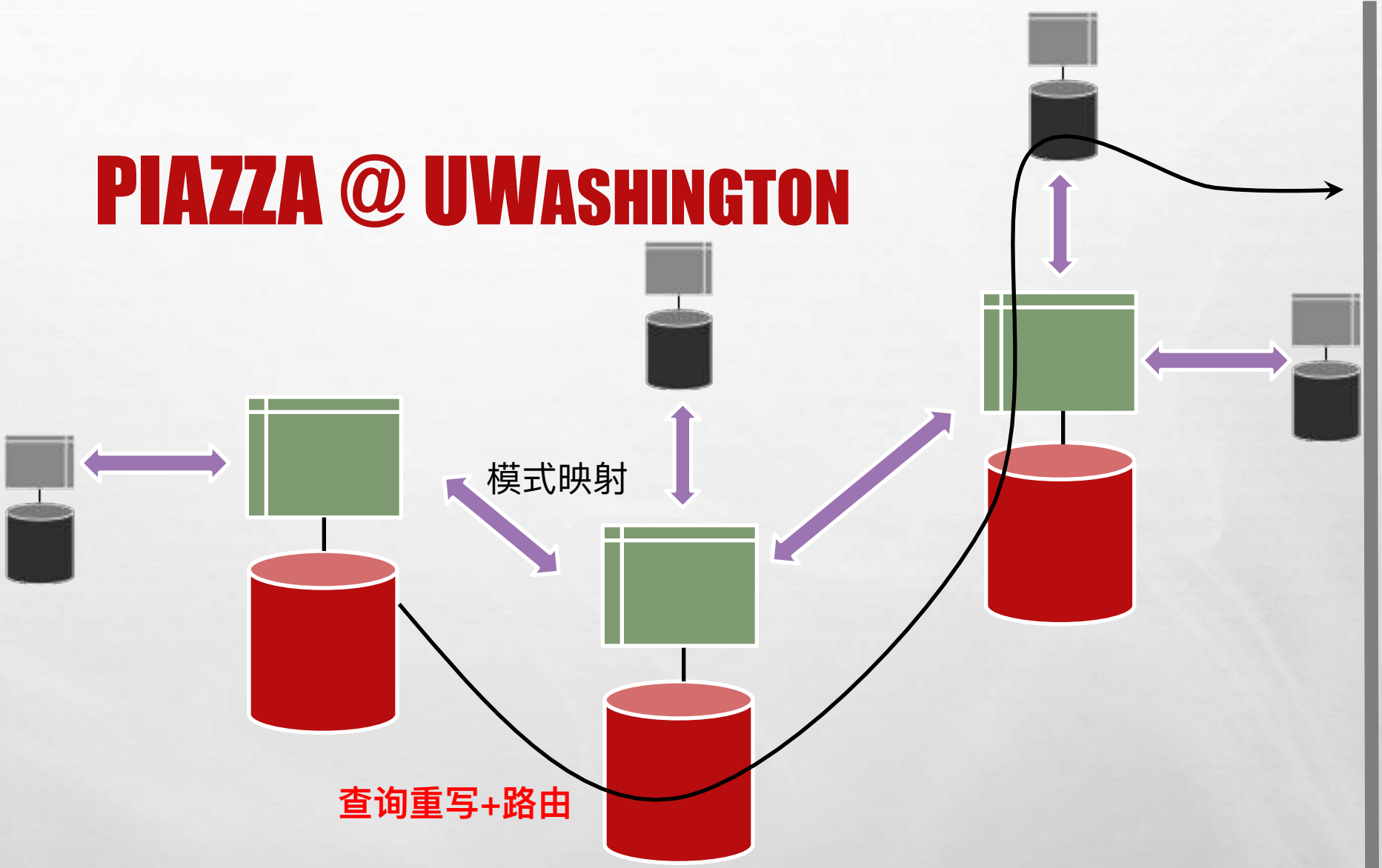




Ion Stoica, Robert Tappan Morris, David R. Karger, M. Frans Kaashoek, Hari Balakrishnan: Chord: A scalable peer-to-peer lookup service for internet applications. SIGCOMM 2001: 149-160

Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard M. Karp, Scott Shenker: A scalable content-addressable network. SIGCOMM 2001: 161-172

PIAZZA @ UWASHINGTON



技术创新需求

- **结构化数据**（可信）管理
- 多级数据管理：主链-支链-链下**联动**
- **高性能**分布式共识
- **丰富**的数据访问、管理、处理**功能**
- 基于区块链的数据**分析处理**

应用模式创新

- 数据共享和交易机制，隐私保护
- 数据表示与语义映射规范
- 跨领域、跨行业、跨机构合作
- 社会与法律对于智能合约的认可
- …

小结

分享型数据库

- 支持核心业务（mission critical）
- 支持分享经济业务模式
- 甚至本身也是以分享经济的方式实现
- **分享经济时代的数据库**

本质问题

- 在不依赖于信用的前提下建立信任

THANKS!

WNQIAN@DASE.ECNU.EDU.CN

HTTP://DASE.ECNU.EDU.CN

BDTC 2017, BEIJING ★ 2017/12/09