QCon 全球软件开发大会
INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

BEIJING 2017

彪悍的区块链来了！

SPEAKER / 張韡武

主办方 Geekbang 极客邦科技 InfoQ

中本聪的区块链里有什么？

去中心化

转账无需金融机构
发行货币无需央行

智能合约

有重要限制
人们常说的“没有循环”其实不重要

票款对付

一手交钱一手交货
（虽然，没有定义证券）

有点隐私

隐私不是重点
有需求但是囿于技术条件
只做出来匿名（不等于隐私）

人们想用区块链做什么？（中国版）

加强中心

央行货币政策
减少对金融机构
执行力的依赖

智能合约

设计新资产类型
因特网金融
及银行发债特权

票款对付

一手交钱一手交货
央行有兴趣
设计依赖数字货币

监管透明

隐私仍然不是重点
对于数字货币，
实名化，反洗钱是重点

人们想用区块链做什么？（澳洲版）

（澳洲版很接近欧美版本）

集成总线

信任关系由
信任系统改为
信任数据
跨机构集成工作流

智能合约

主要用于现有业务
银行业及供应链

票款对付

一手交钱一手交货
减少中间人
大银行有兴趣央行观望

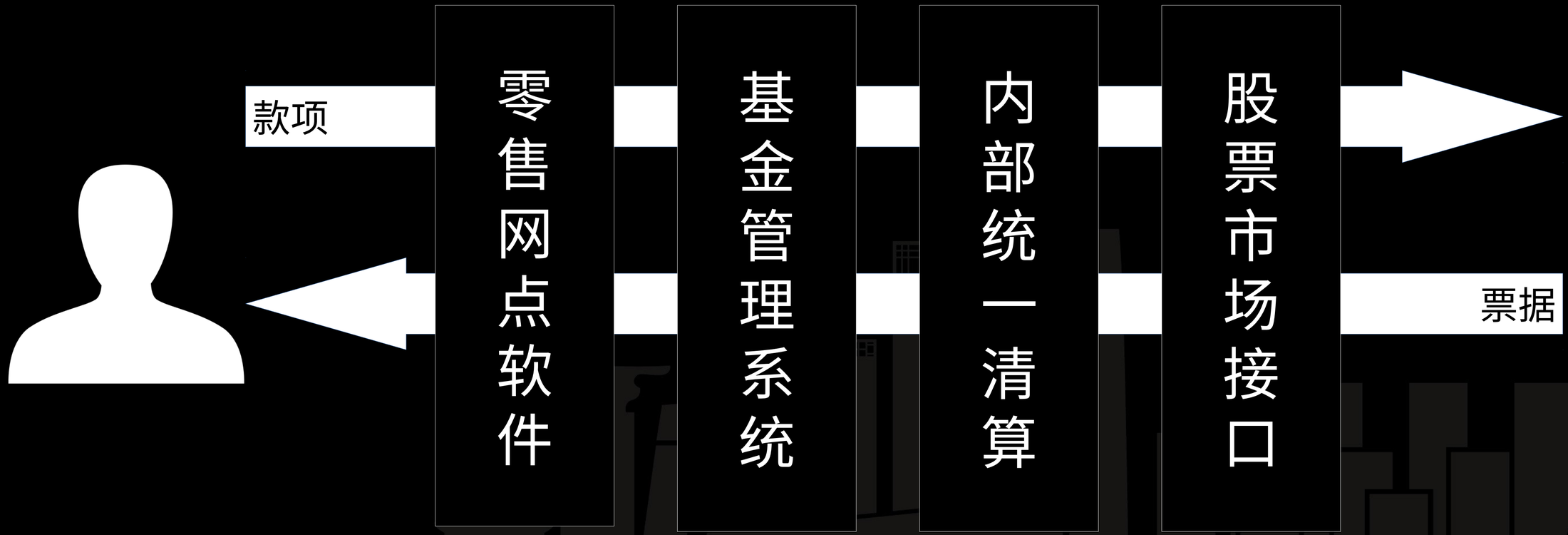
身份验证

在隐私和监管之间
找平衡点
提高效率（重用身份证明）

票款对付

当前状况

例：用户从一个金融机构购买一个理财产品



票款对付

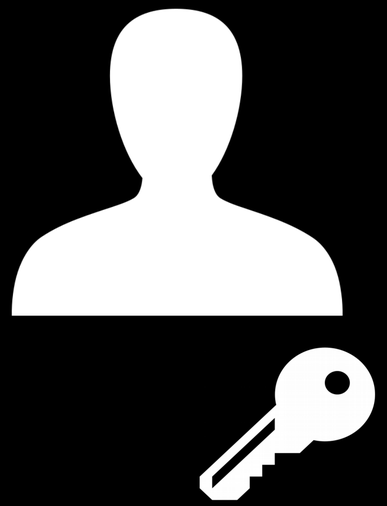
完全使用区块链的极端情况

零售网点软件

基金管理系统

内部统一清算

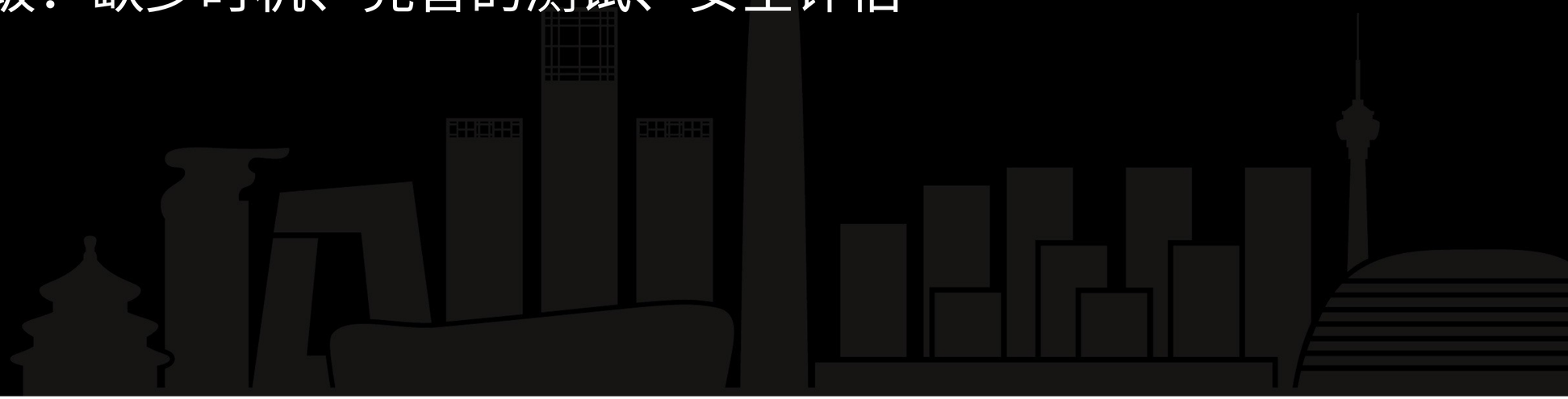
股票市场接口



票款对付

实际使用的条件

- 无法“插入”部署，一动至少两个系统
- 仅在单一金融机构内部署没有太大意义
- 缺少数字货币 Cryptocurrency
- 核心系统的升级：缺少时机、完善的测试、安全评估



票款对付

取代游戏：大家都觉得别人是中间人

谁是中间人？从后端往前算：

- 金融市场工具（如 CLS ）
- 基金管理
- 银行的零售业务

取代他们意味着什么？

身份验证

区块链的优点

隐私 哈希树提供的有限事实证明
零知识证明提供有时限的证明

效率 一次验明证身，多次远程证明
（直到用户丢失私钥）

抗伪 防止证书发行单位做伪证 †
不依赖对身份验证软件的信任

分布 没有一个“全知识点”
防攻击、防贿赂、合规

† 中国互联网络信息中心 2015 年发行过假证书

身份验证

区块链应用的情景

身份确立

身份确认

身份验证

实际应用的困难

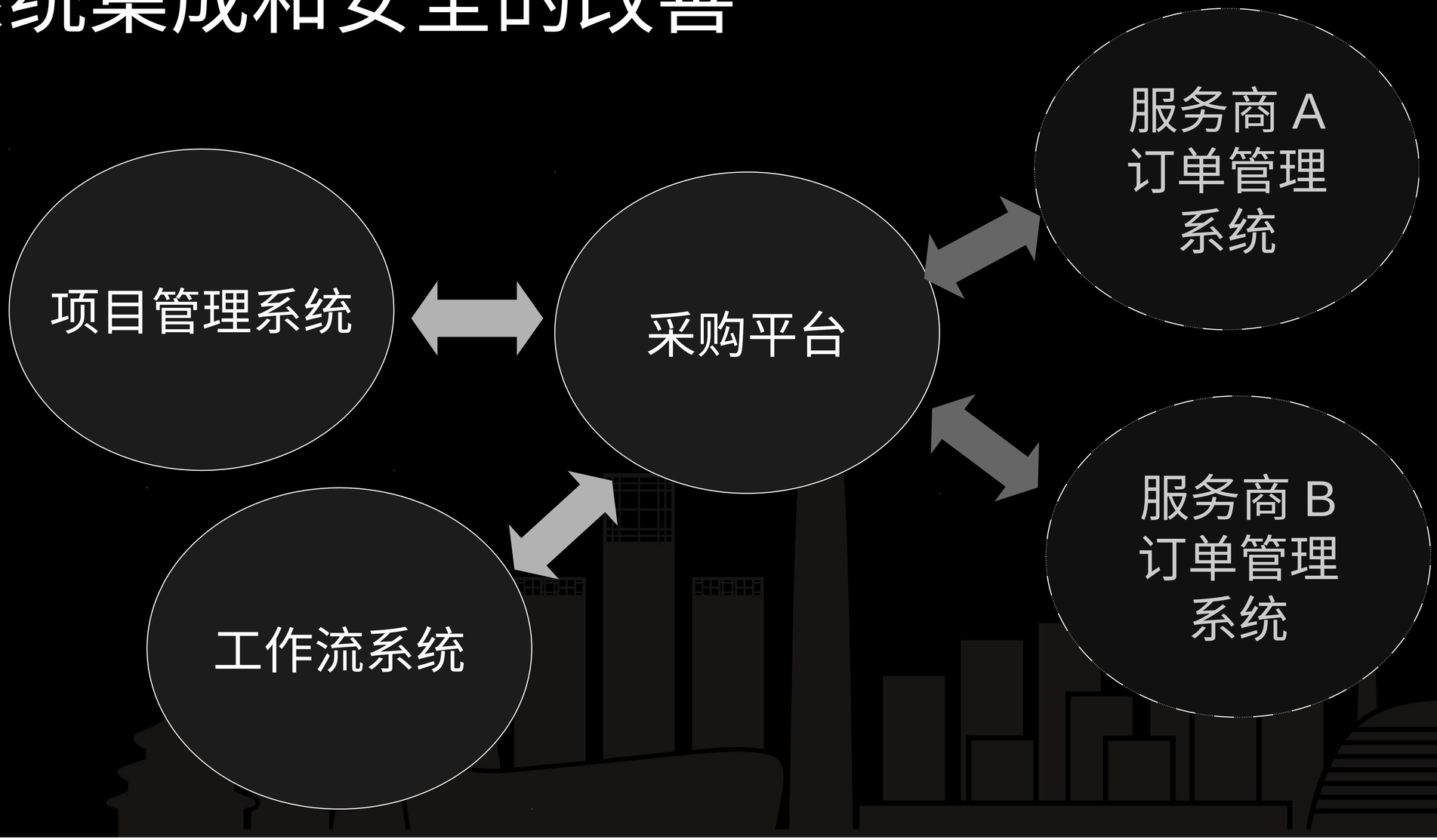
- 银行业认为掌握用户的数据是一项业务
- 监管机构没有执行力，只有罚款力
- 民间没有形成意见，因此无法立法支持

因此，考虑旁门左道。

集成总线

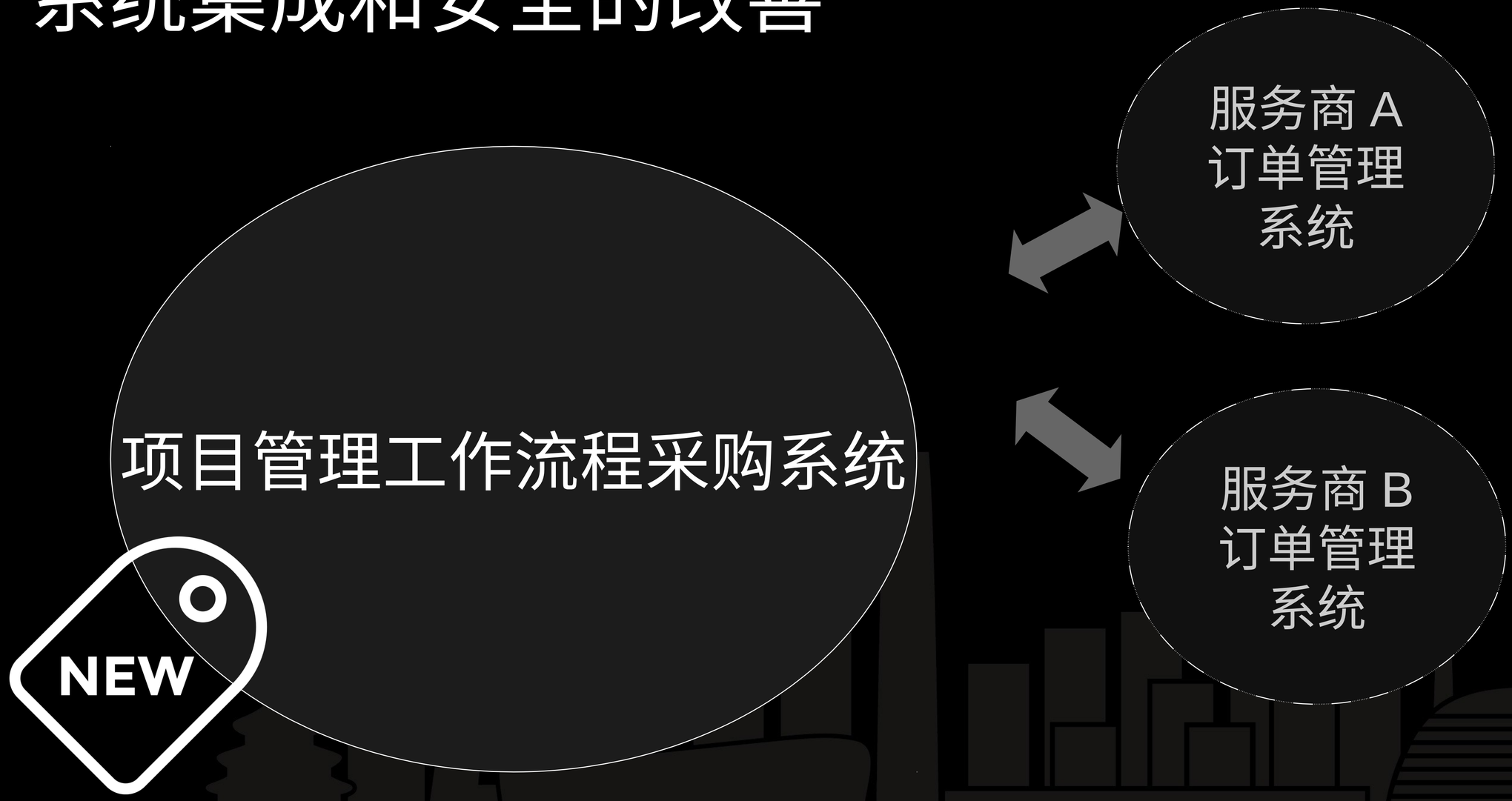
系统集成和安全的改善

一个例子：



集成总线

系统集成和安全的改善



集成总线

系统集成的视界

集成总线

你会用什么角度射?

智能合约

开放游戏

智能合约

秘密游戏

智能合约

智能合约和隐私协议

开放游戏

货币发行
股票市场

区块链技术：
- Bitcoin
- Ethereum
- Factom

秘密游戏

Commodity Market
Trade Finance
IMT

区块链技术：
- Corda
- Hyperledger （自从 v1.0）
- Zcash （但是没有智能合约）

智能合约

智能合约的海外应用困难

市场不在海外。

- 最先开始的应用可能是供应链管理
- 最需要它的是中国

技术限制。

- 开放的智能合约仍然会死机
- 秘密智能合约见证太少
- 平台今年才出来还不成熟（不过可以动手了！！）

关注QCon微信公众号，
获得更多干货！

Thanks!

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

主办方 Geekbang. 极客邦科技 InfoQ