数领先机 智赢未来

DTCC 第九届中国数据库技术大会

DATABASE TECHNOLOGY CONFERENCE CHINA 2018

2018.05.10 – 12 北京国际会议中心

IT168.com ChinaUnix ITPUB

HPB: 如何解决区块链性能瓶颈问题？

李琼

2018/5

内容概述

市场分析

性能分析

解决方案

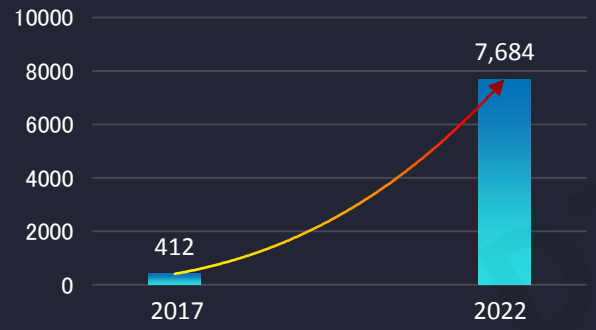
HPB芯链

PART1

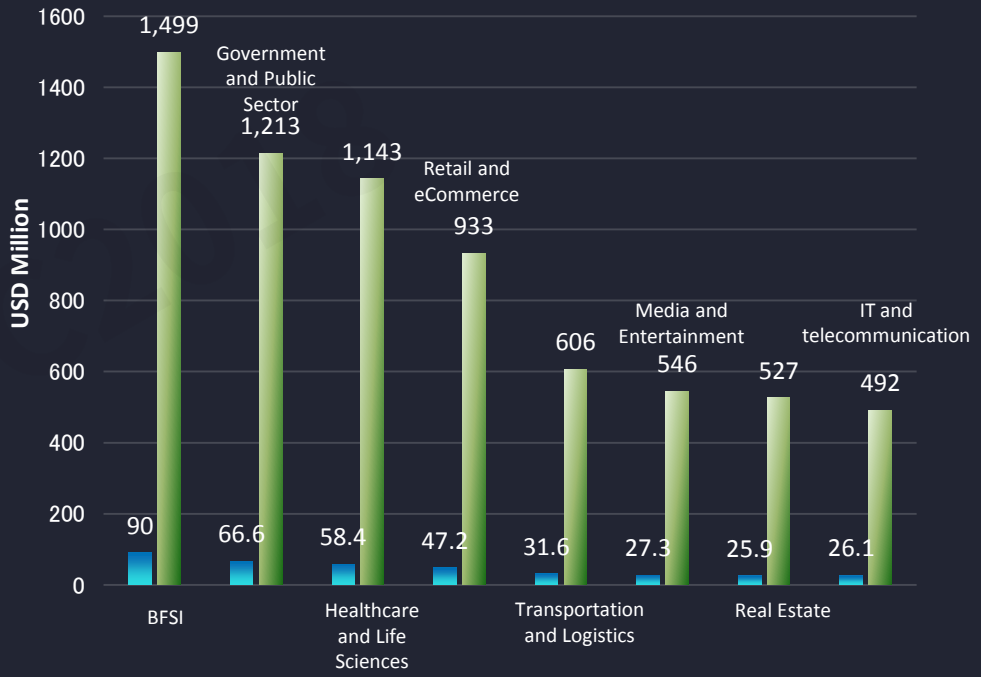
市场分析

PART1 区块链市场需求

MARKETSANDMARKETS



全球区块链市场
CAGR 79.6%



区块链垂直市场

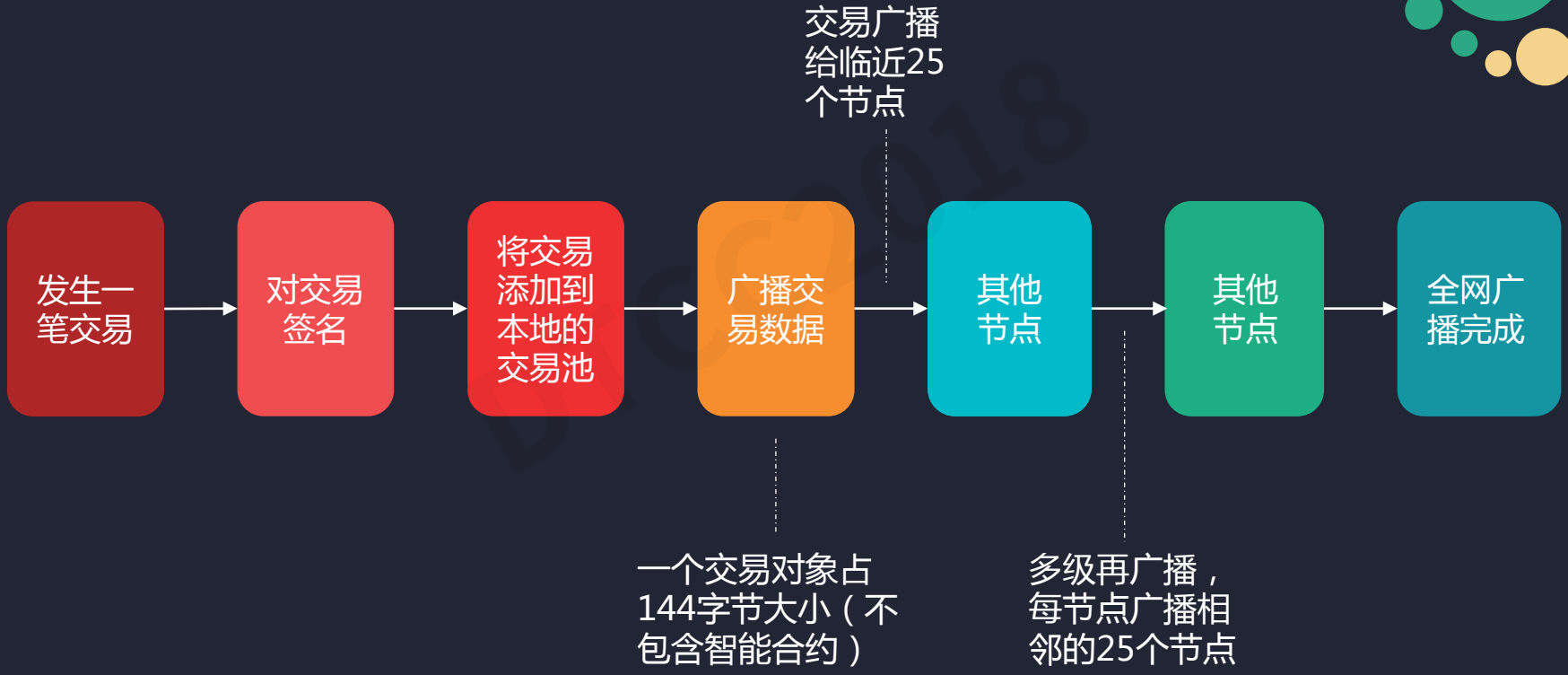
www.gxn.io

PART1 区块链性能与商用系统的差距

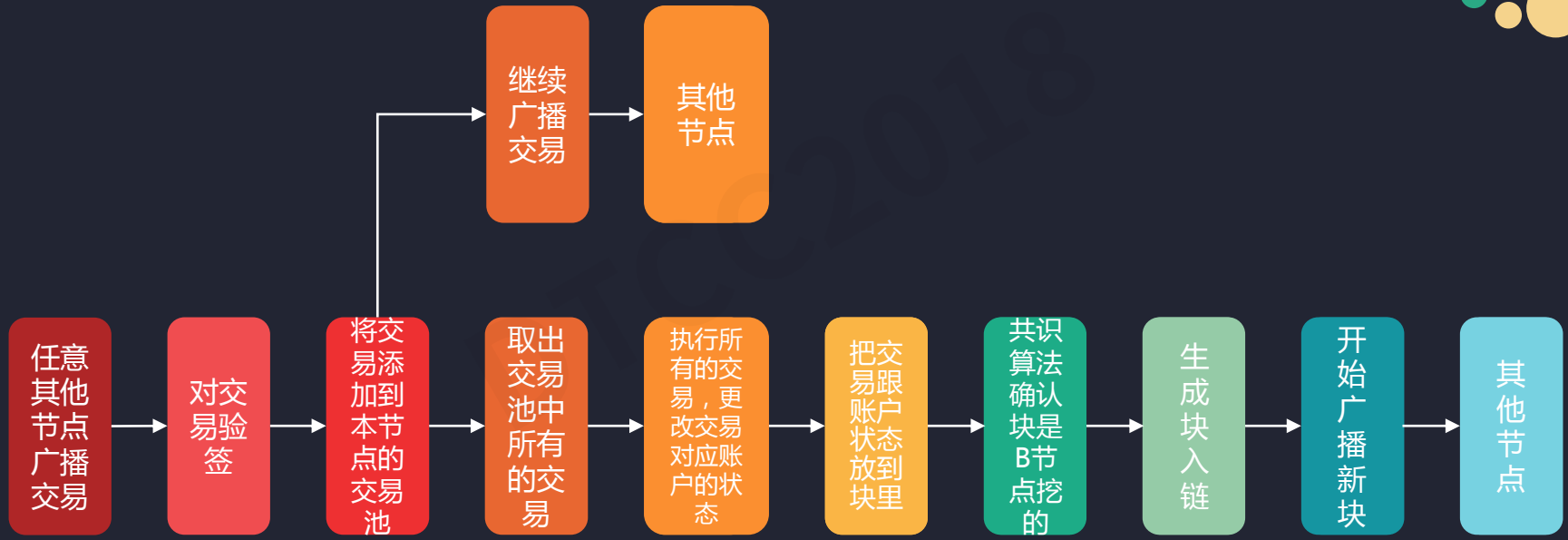
PART2

性能分析

PART2 区块链性能瓶颈分析——交易发生



PART2 区块链性能瓶颈分析——交易确认与出块



PART2 区块链性能瓶颈分析——交易广播带宽

- 以太坊中任意一个节点
- 任意一笔交易
- 需广播给临近的25个节点
- 以TPS 10万次计算

则任意一个节点需要广播的数据量为：

以上行速率4Mbps计算，10万次突发交易数据，需要12分钟才能全部广播完成

PART2 区块链性能瓶颈分析——区块同步广播带宽

- 以TPS 10万次/秒计算（峰值）
- 每笔交易入块数据144Byte

则每秒同步区块数据量约为：

要求每个节点理论上行带宽必须达到2.88Gbps,才能完成全部区块广播

PART2 区块链性能瓶颈分析——区块同步广播带宽分析

举例

- 以某叫车平台平均交易次数115笔/秒计算（均值）
- 每笔交易入块数据144Byte
- 以10分钟一个区块计算

则每个区块数据量约为：

每秒交易**115**笔 × 每笔交易入块数据**144**Byte × 10分钟**(600秒)**一个区块 = 9,936,000Byte

则任意一个节点，需要广播的数据量约为：

$$9{,}936{,}000 \times 25 \times 8 \times 2 = 3{,}974{,}400{,}000 \text{ bits} = 3.9744\text{G bits}$$

要求每个节点理论上行带宽必须达到6.624Mbps,才能完成全部区块广播

PART2 区块链性能瓶颈分析——存储容量分析

- 以太坊中任意一个节点
- 任意一笔交易
- 以TPS 10万次计算

每秒账本新增数据量：

每个交易数据量为144Byte × 以TPS 10万次计算 ＝14,400,000 Byte(14.4MBps)

每天新增账本： 14.4MB × 3600 × 24 = 1,244,160MB = 1.2TB

PART2 区块链性能瓶颈分析——存储容量分析

- 以太坊中任意一个节点
- 任意一笔交易
- 以某叫车平均每秒交易量115笔计算

举例

每秒账本新增数据量：

每秒交易**115**笔 × 每笔交易入块数据**144**Byte × 1天 86400 = 1,430,784,000 Byte

年新增账本：1.44GB × 365 = 525.6GB

PART2 区块链性能瓶颈分析——计算能力分析

CPU测试ECC处理性能如下：

- x86测试，i5双核2.0G处理器，一次验签耗费时间>20ms
- 意味着双核全部做ECC验签，每秒钟处理50次（理论性能，CPU不处理其他任何运算）
- 如果遇到突发上万TPS时，就会出现交易溢出，系统内存耗尽，崩溃宕机现象

- 任意节点，收到一笔新的交易，都需要做交易验证
- ETH采用的算法为ECC
- ECC是一个较为复杂的数字加密算法

PART2 区块链性能瓶颈分析——计算能力分析

- ETH的处理方法是每发一笔交易，在广播交易事件时，都会导致开启一个线程
- 当交易量上升时，线程会逐渐累积，累积过大，可能导致golang虚拟机宕机。
- 当交易量较大时，因事件机制不完善，导致交易广播线程不能顺序处理，使得某个账户发送的交易不能按照nonce的顺序广播，其他节点会抛弃相应交易。
- 交易量过大时，导致内存占用较多，并且碎片化严重，可能导致内存耗尽，系统崩溃。

任意一笔新的交易，都由CPU来进行转发

PART3

解决方案

PART3 区块链性能解决方案

1、减少需求：减少计算、网络、存储数据需求

2、加快速度：单节点Performance

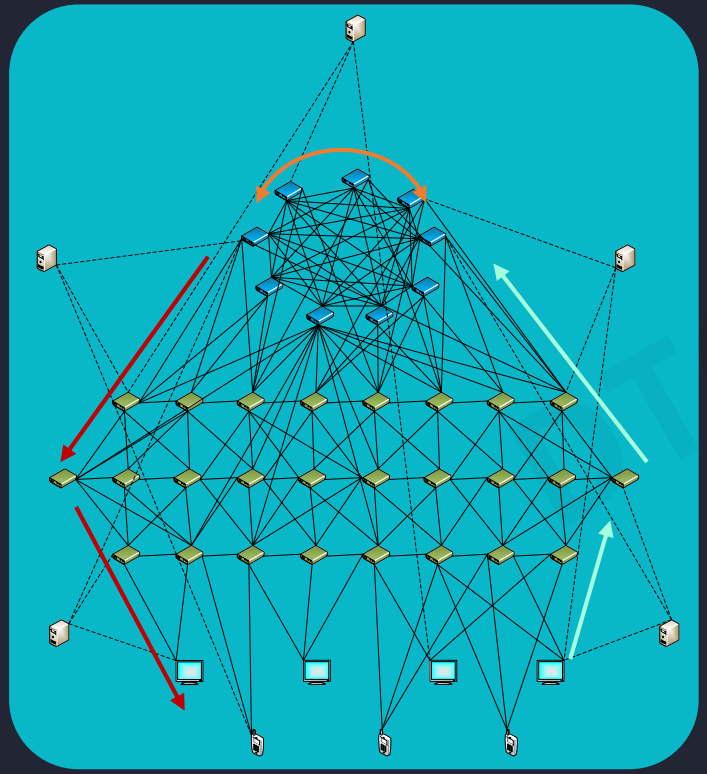
PART3.1 区块链性能解决方案——减少需求

HPB以优化减少广播数据量的方式来减少区块链对于网络和存储的数据量，达到性能提升的目的。HPB通过以下方式减少广播数据量：

1、分层网络架构

2、区块分片发送

PART3.1 区块链性能解决方案——减少数据量



1、分层网络架构

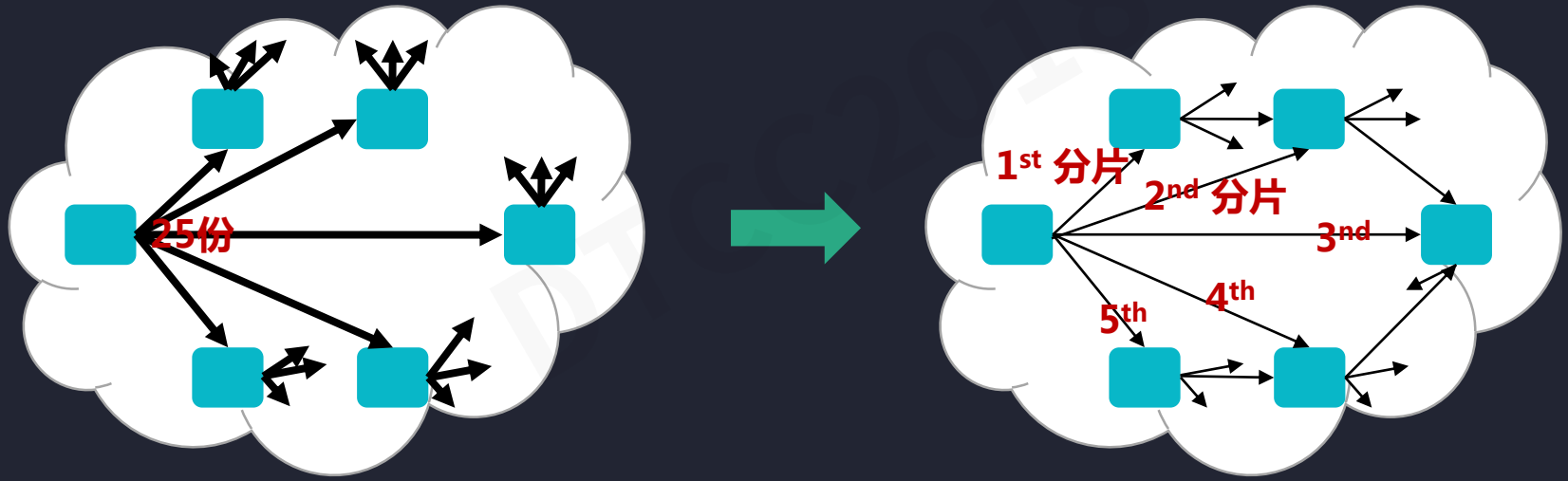
- 高性能节点间全连接，高性能节点只从候选节点接收交易，互相之间不转发交易只转发区块数据。
- 每个高性能节点与部分候选节点动态连接，每个高性能节点连接的候选节点数量越多，交易入块的平均时间越短。
- 候选节点与候选节点之间部分动态连接，候选节点只有在跟所有高性能节点连接都断开时，才会向其它候选节点转发交易。
- 每个轻节点与2-3个候选节点动态连接

带宽/存储需求：

高性能节点有效收发带宽约60Mbps。 考虑到冗余情况，建议带宽80～100Mbps；
只有高性能节点存储整网交易，降低了存储资源。

PART3.1 区块链性能解决方案——减少数据量

2、区块数据分片发送同步



PART3.1 区块链性能解决方案——减少需求

3、其他方案

一个是建立分层结构（Layer2），把不必要的交易从最底层的主链分离到附属结构上，例如比特币的闪电网。

另一个方向叫分片技术（Sharding），这项技术着眼于改进主链本身的协议来提高它的性能

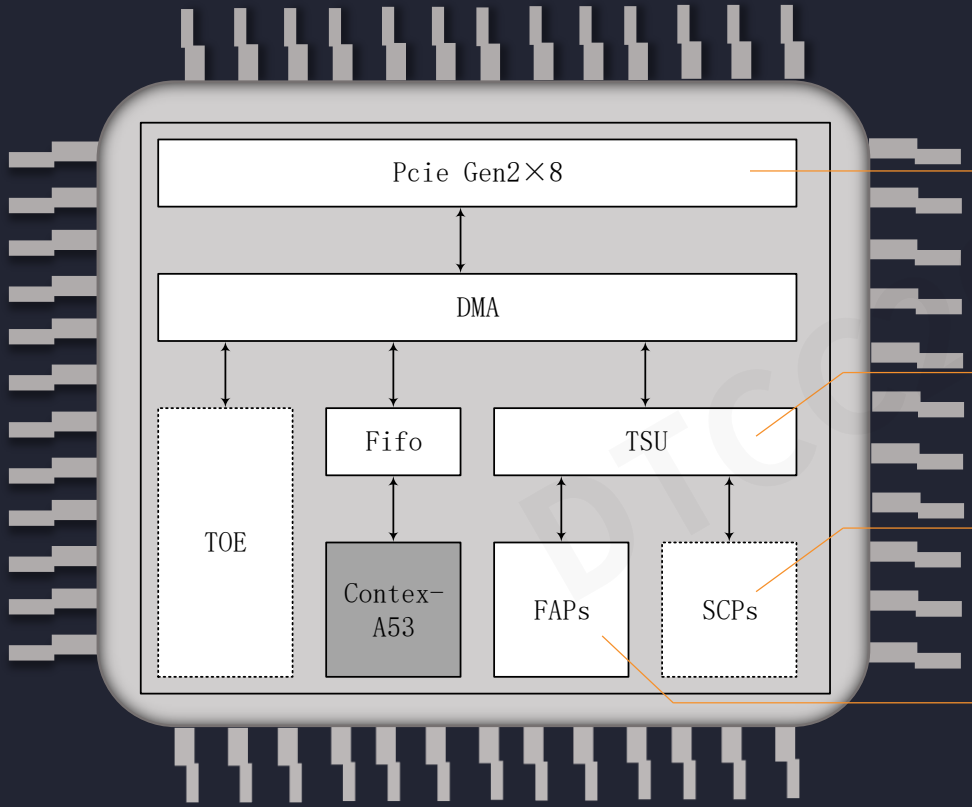
PART3.2 区块链性能解决方案——加快速度（ HPB BOE ）

1、BOE（Blockchain Offload Engine）系统是区块链卸载引擎的缩写，利用硬件并发处理能力对区块链节点上的交易、区块、账户等处理过程进行加速。

2、系统特性：

PCIE Gen2×8接口	系统升级功能	函数加速处理器	智能合约处理器
◆ 40Gbps传输带宽，32Gbps净荷速率 ◆ 支持SG-DMA，效率可达88%	◆ 可通过miniSD卡升级 ◆ 可通过网络远程升级 ◆ 升级与加载可独立控制 ◆ 双系统备份	◆ 支持多种函数加速运算 ● ECC验签 ● Hash运算 ● AES加密 ● AES解密 ● RLP编码 ● RLP解码 ◆ 支持每个函数多核调度	◆ 独立复位 ◆ 兼容以太坊虚拟机EVM

PART3.2 区块链性能解决方案——HPB BOE芯片架构



用户接口，40Gbps带宽；内置DMA控制器提供AXI4接口和AXI-lite接口，分别用作收发报文数据传输和用户控制接口。

Task Schedule Unit，任务调度单元

Smart Contract Processor，为智能合约处理器

Function Accelerate Processor，为函数加速处理器

PART4

HPB芯链

PART4 HPB目标

HPB(High-performance Blockchain)是一种全新的区块链软硬件体系架构，其中包含芯片加速引擎和区块链底层平台，旨在实现分布式应用的性能扩展。定位为易用的高性能区块链平台，跟产业深度结合，满足现实世界的真实商业需求。

打造基于硬件加速芯片驱动的高性能公链

打造芯链高速区块链上的DAPP应用生态圈

为其他区块链提供定制化硬件加速芯片解决方案与技术支持

PART4 HPB HIGHLIGHTS

芯片级加速引擎

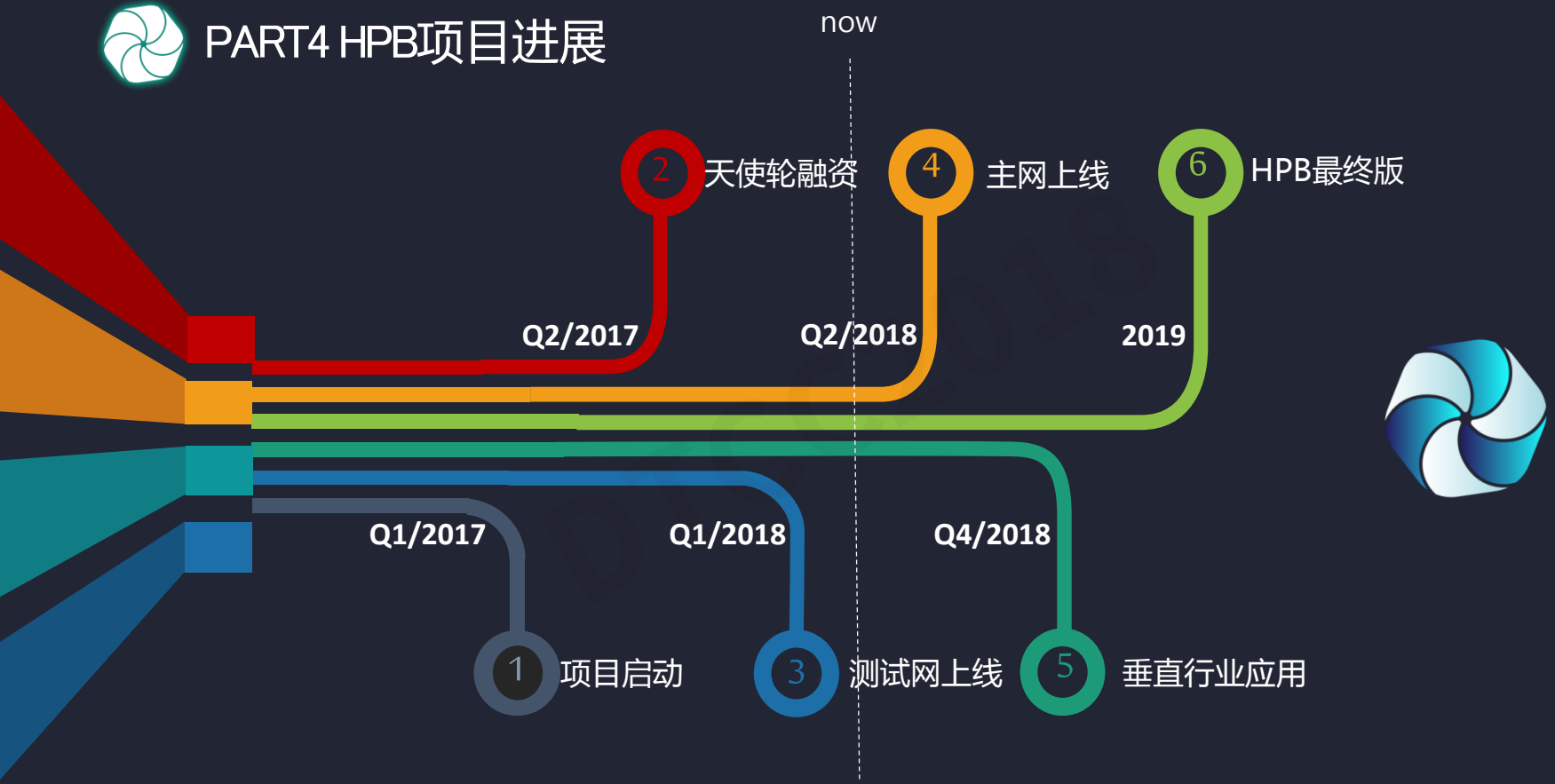
软件架构和算法深度优化

软硬件开源

PART4 软硬件区块链对比

	SOFTWARE-CHAIN	
架构	软件	硬件加速+软件优化
DAPPs	支持	支持
TPS	7, 25, 1k TPS	目前: 10k TPS 目标: 1 million TPS
共识算法	PoW PoS	更有效更公平
共识节点	部分链支持有限数目	不限
开源	软件	软件+硬件 Github：https://github.com/HPBProject/TOE
是否对其他链提供支持	有些链不行	Yes

PART4 HPB项目进展



UNLIMITED SPEED EVOLUTION

THANKS

MERCI

讲师申请
联系电话（微信号）：18612470168

关注“ITPUB”更多
技术干货等你来拿~

与百度外卖、京东、魅族等先后合作系列分享活动

微学堂

让学习更简单

微学堂是以ChinaUnix、ITPUB所组建的微信群为载体，定期邀请嘉宾对热点话题、技术难题、新产品发布等进行移动端的在线直播活动。

截至目前，累计举办活动期数60+，参与人次40000+。

ITPUB学院

ITPUB学院是盛拓传媒IT168企业事业部（ITPUB）旗下
企业级在线学习咨询平台
历经18年技术社区平台发展
汇聚5000万技术用户
紧随企业一线IT技术需求
打造全方式技术培训与技术咨询服务
提供包括企业应用方案培训咨询（包括企业内训）
个人实战技能培训（包括认证培训）
在内的全方位IT技术培训咨询服务

ITPUB学院讲师均来自于企业
一些工程师、架构师、技术经理和CTO
大会演讲专家1800+
社区版主和博客专家500+

培训特色

无限次免费播放
随时随地在线观看
碎片化时间集中学习
聚焦知识点详细解读
讲师在线答疑
强大的技术人脉圈

八大课程体系

基础架构设计与建设
大数据平台
应用架构设计与开发
系统运维与数据库
传统企业数字化转型
人工智能
区块链
移动开发与SEO

联系我们

联系人：黄老师
电　话：010-59127187
邮　箱：edu@itpub.net
网　址：edu.itpub.net
培训微信号：18500940168