BDTC 2017 中国大数据技术大会
Big Data Technology Conference 2017

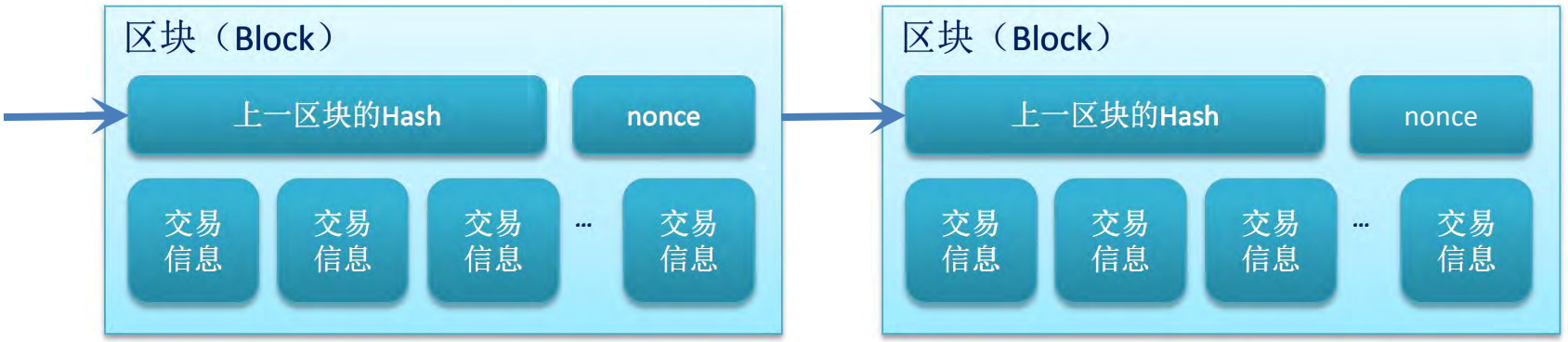
自主可控联盟区块链
——技术、系统及应用

杭州趣链科技有限公司
邱炜伟

目 录

区块链的三点技术特征

- 区块链（Block Chain）源自比特币（Bitcoin），技术的本质是一种分布式账簿数据库
  - 1. 利用块链式数据结构来验证与存储数据

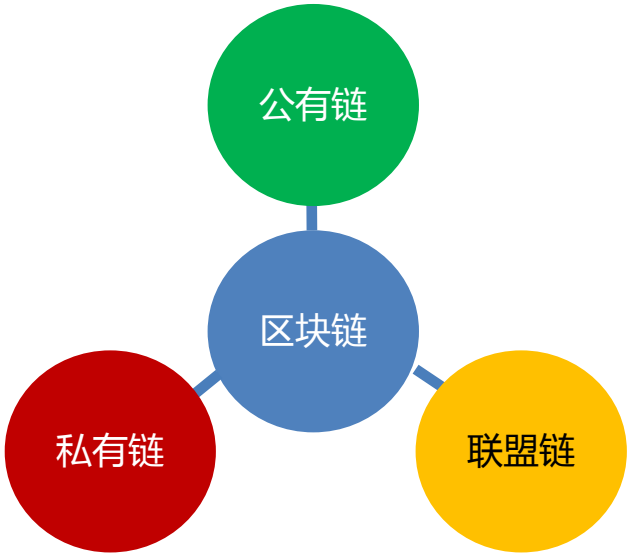


  - 2. 利用分布式共识算法来生成和更新数据
  - 3. 利用密码学的方式保证数据传输和访问的安全

区块链的三点功能特征

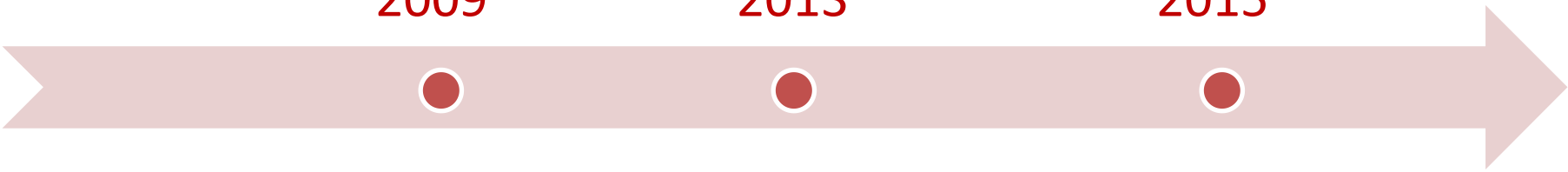
1.多中心	多个机构在区块链网络中相互监督并实时对账
2.自动化	智能合约大大提高了经济活动与契约的自动化程度
3.可信任	记录不可篡改，无需第三方可信中介

区块链的三种组织形态



	公有链	联盟链	私有链
中心化程度	分布式去中心化	多中心式	单中心式
参与主体控制	任何节点可接入	预先设定具有特定特征的参与主体	由中心控制者制定参与成员
信息公开程度	账本完全公开（可匿名）	联盟内部公开（可匿名）	公司内部公开（可匿名）

区块链的三次演进



	2009	2013	2015
代表产品：	比特币	以太坊	Fabric/趣链（Hyperchain）
功能：	数字货币	可编程	权限控制、隐私保护、复杂合约
核心技术：	基于POW的共识算法	智能合约	高效共识
性能指标：	每秒几笔交易	每秒几百笔交易	每秒几千到万笔交易
组织形态：	公有链	公有链	联盟链

联盟区块链的三点核心优势

从监管角度看，联盟区块链可以通过CA认证准入、制定监管规则合约等方式为监管提供便利

商业机构及用户对帐户和部分交易信息有隐私保护的需求，联盟区块链可以通过加密、分区等方式实现隐私保护。

从商业应用角度来看，交易吞吐量和时延是企业最关心的交易性能指标，联盟区块链通过通过共识算法的创新使交易效率得到很大提升。

目 录

联盟区块链技术难点

1.高性能

- 高性能共识算法设计（多节点之间）
- 智能合约执行引擎的效率优化（节点）

2.高可用

- 动态成员准入
- 节点快速恢复技术

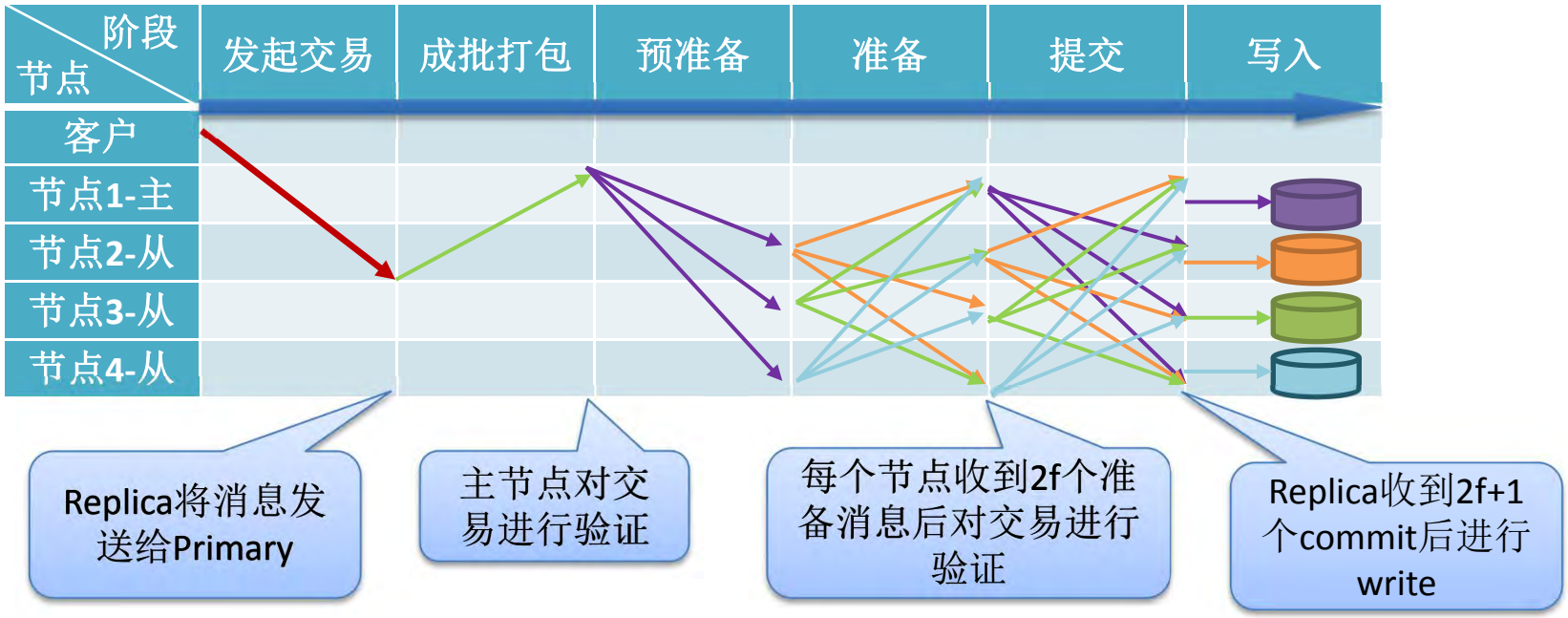
3.安全隐私

- 节点准入控制与国家安全标准支持
- 业务数据的隐私保护

4.可编程

- 图灵完备且安全的智能合约引擎
- 复杂智能合约支持

– 鲁棒拜占庭容错算法（Robust Byzantine Fault Tolerance ）



形成产品的性能指标

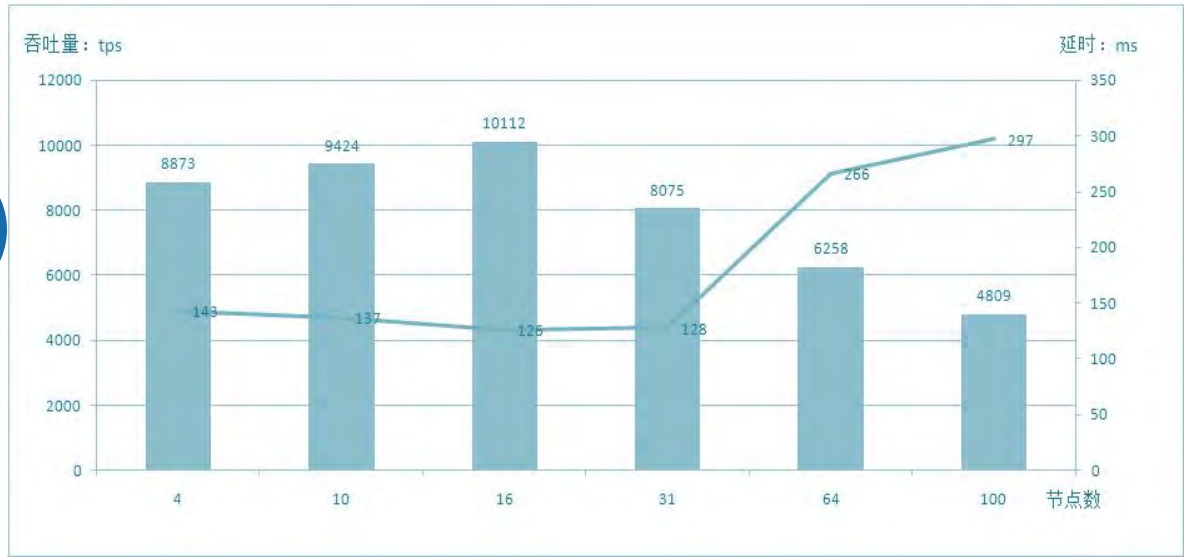
- 平台具有高吞吐量和低系统延迟
- 交易吞吐量大于10000笔/秒
- 系统延迟小于300毫秒

Throughput

>10000TPS

Latency

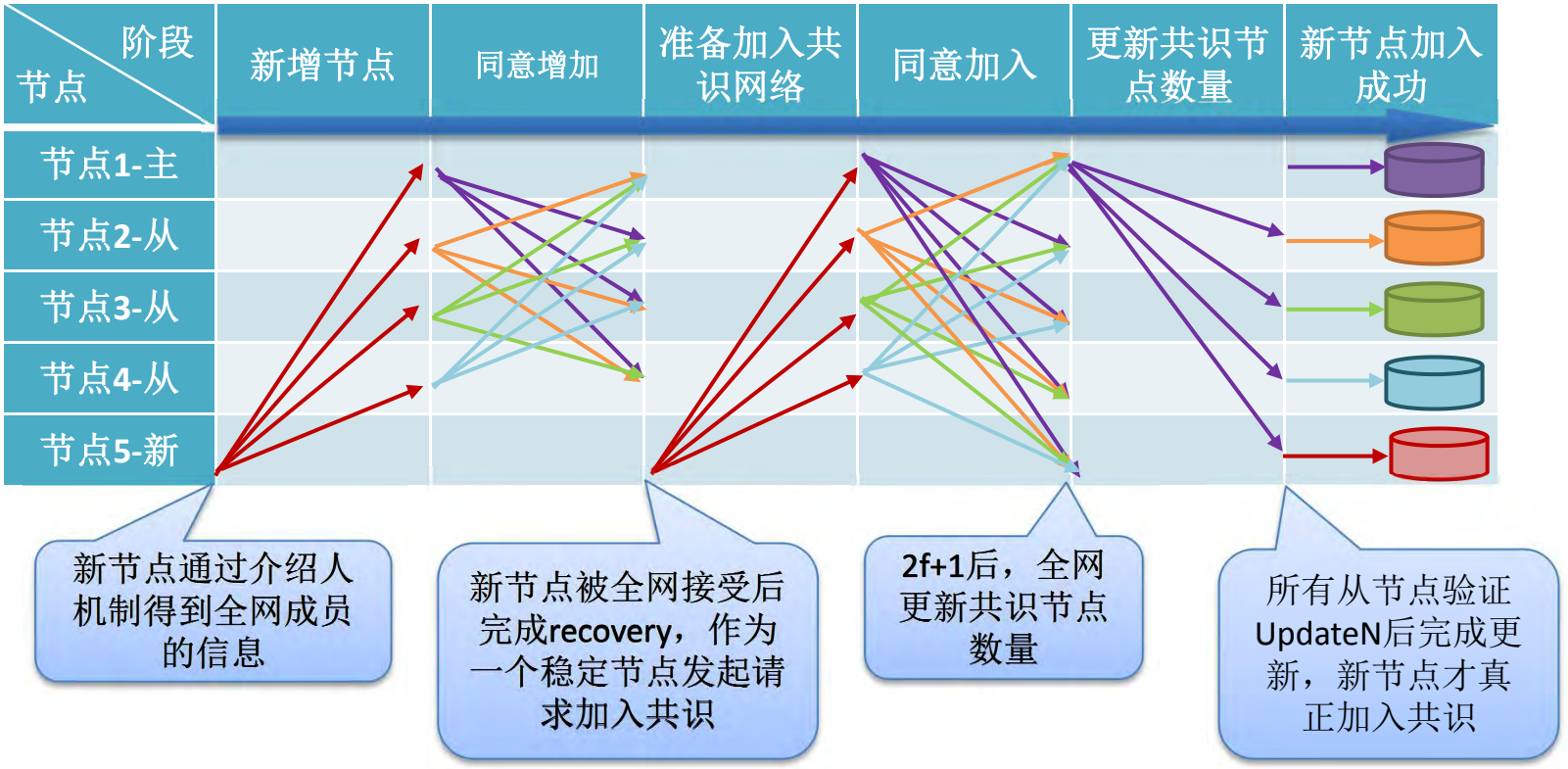
<300ms



节点机器配置：16核32G内存云 服务器，主频3.2GHz，SSD存储

联盟区块链关键技术突破二：高可用

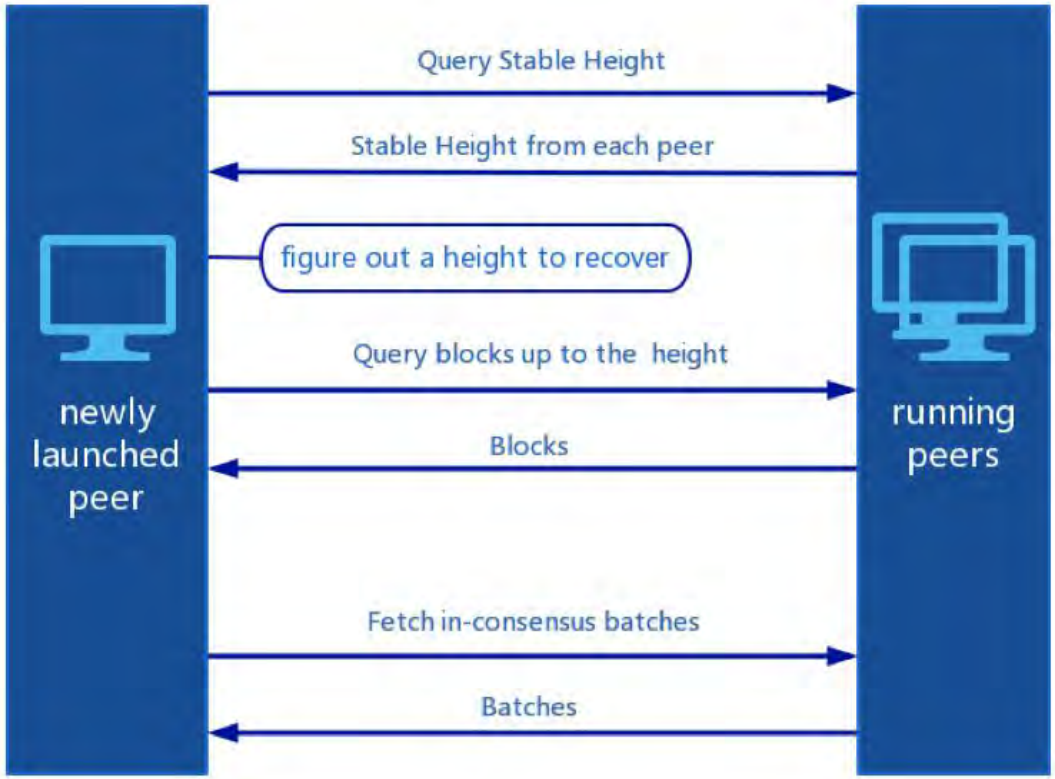
- 动态节点（成员）准入（Dynamic Membership Management）



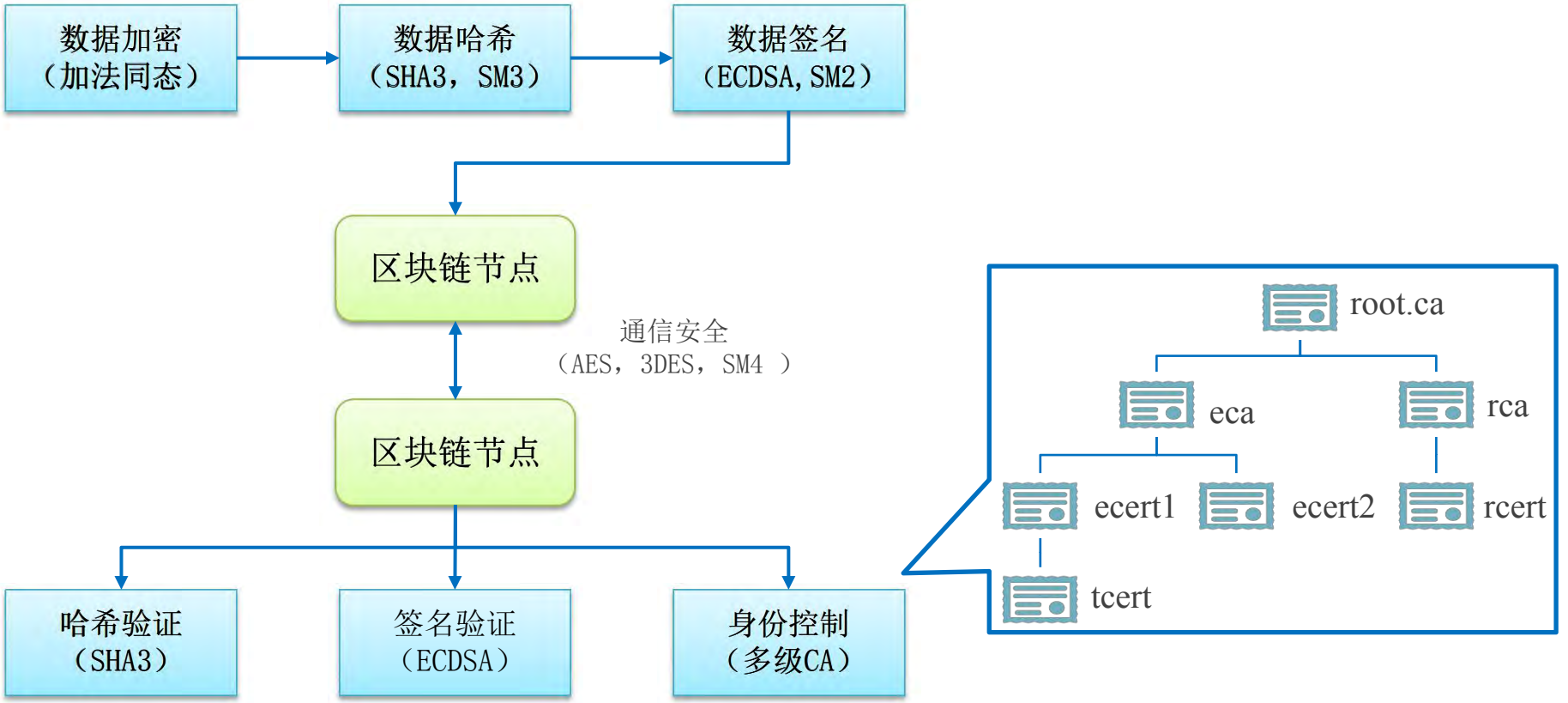
联盟区块链关键技术突破二：高可用

- 快速恢复技术（Active Recovery Technology）

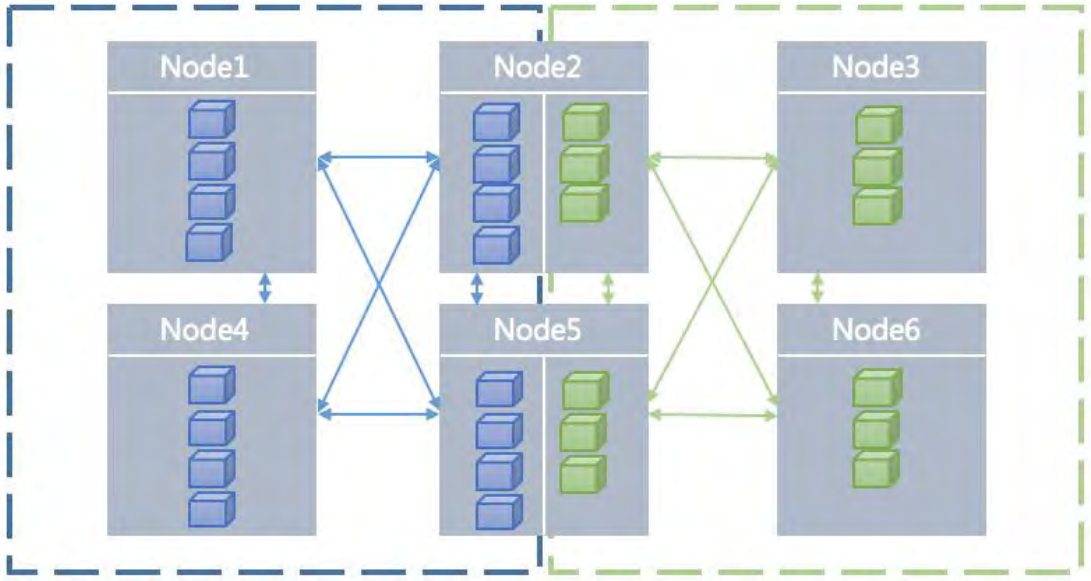
除了传统PBFT中提及的Checkpoint机制、StateUpdate机制和ViewChange机制，为了适应生产环境的需求，我们还加入了Recovery机制。



◆基于密码学的多级加密机制



联盟区块链关键技术突破三：数据隔离



分区共识

- 交易按名字空间独立共识
- 验证节点仅共识其参与的名字空间交易
- 验证节点支持多个名字空间的交易共识

数据隔离

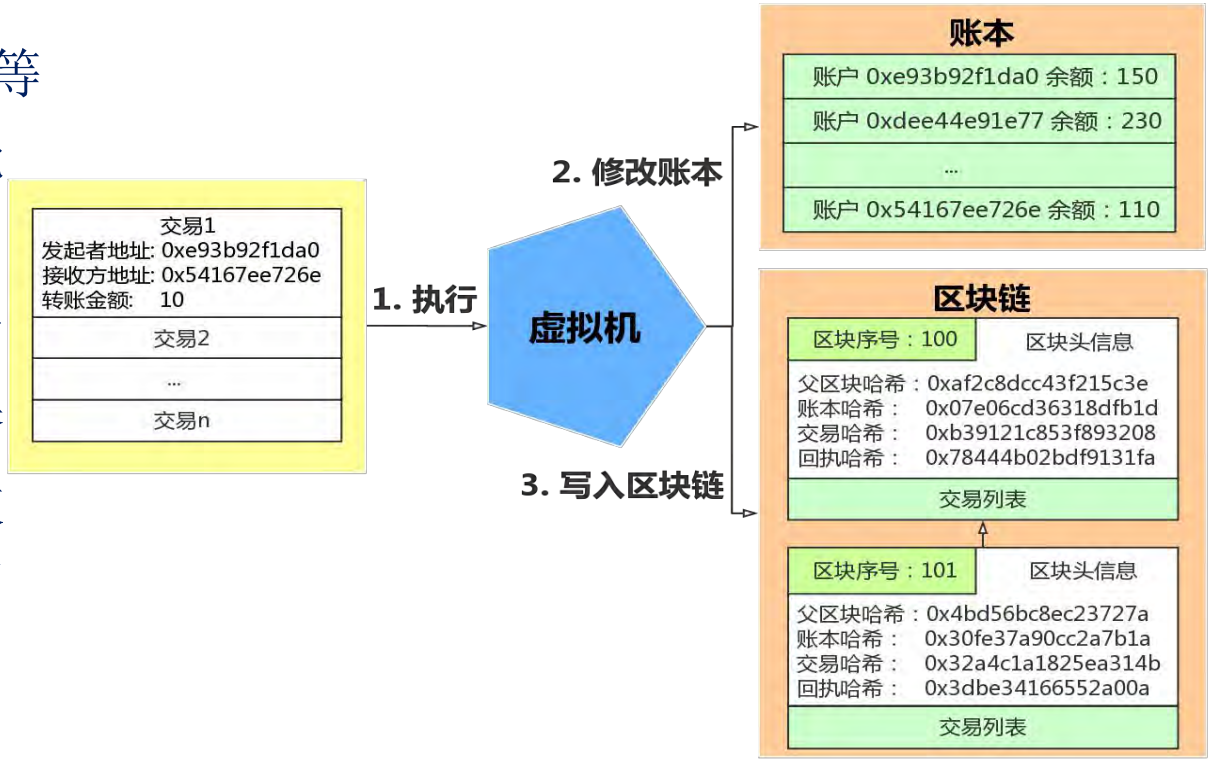
- 数据的传输和存储按照名字空间划分
- 节点内不同名字空间中的账本实现物理隔离
- 节点仅存储其参与的名字空间的账本数据

并行执行

- 不同名字空间内部交易并行执行
- 名字空间之间的交易结果互不干扰

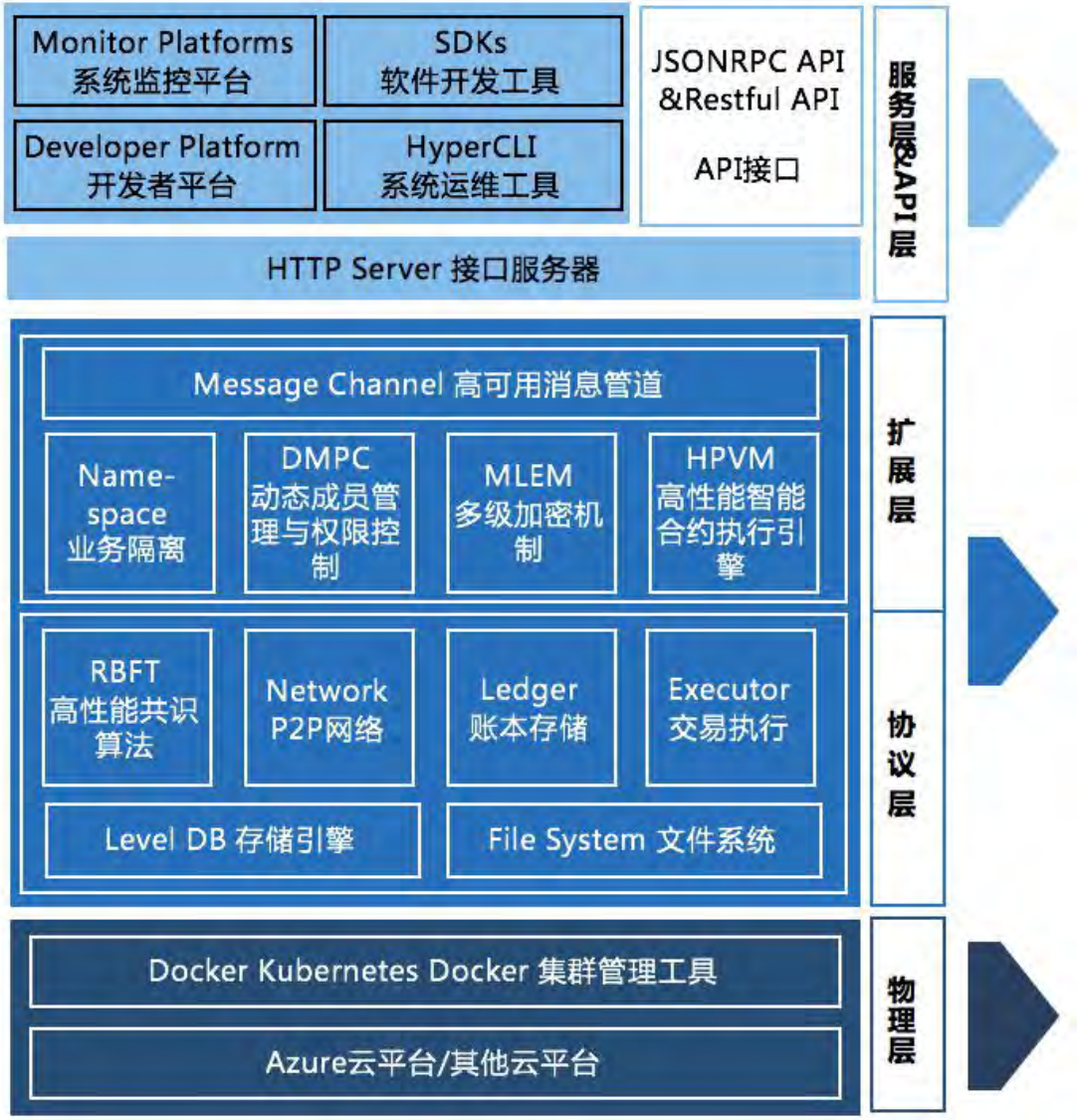
联盟区块链关键技术突破四：多语言可编程

- 支持包括Solidity、Java等多种语言可编程的智能合约引擎
- 智能合约是经过共识的执行逻辑，区块链各参与方通过调用合约修改账本状态，执行结果同步到各记账节点

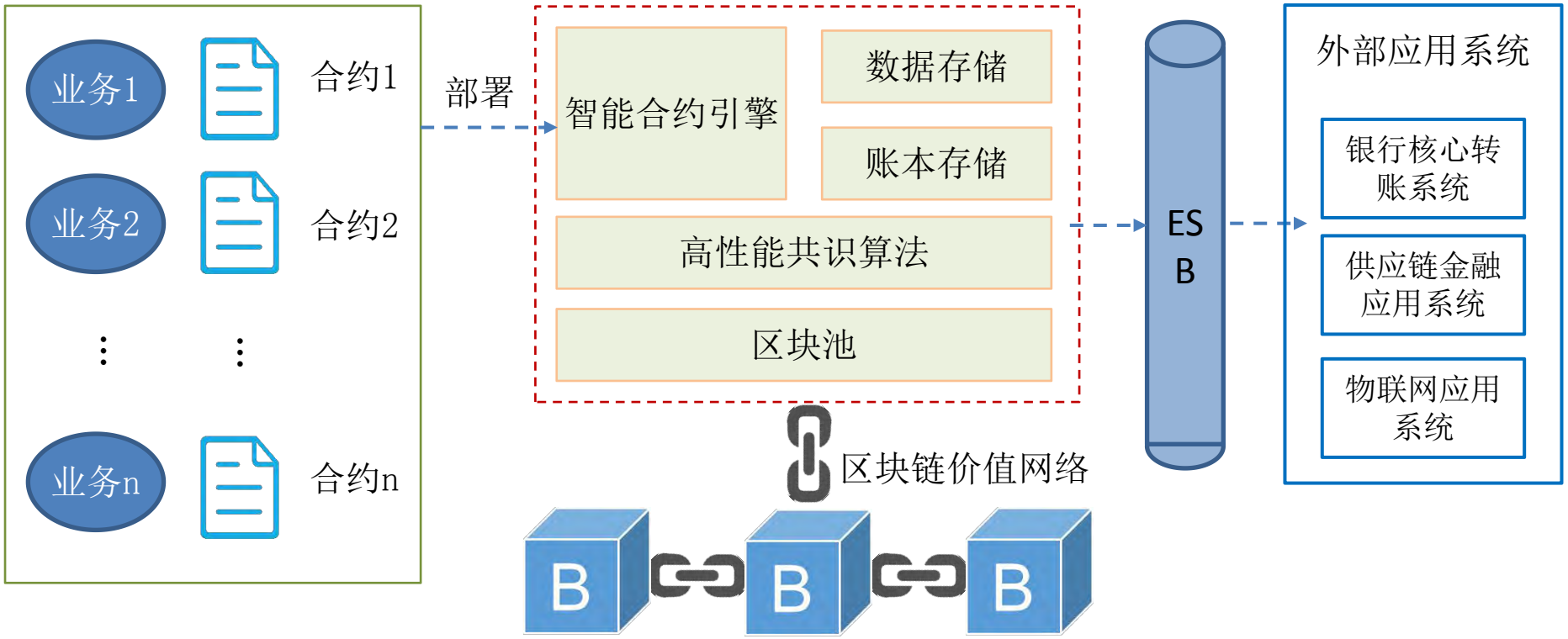


目 录

趣链（Hyperchain）联盟区块链系统



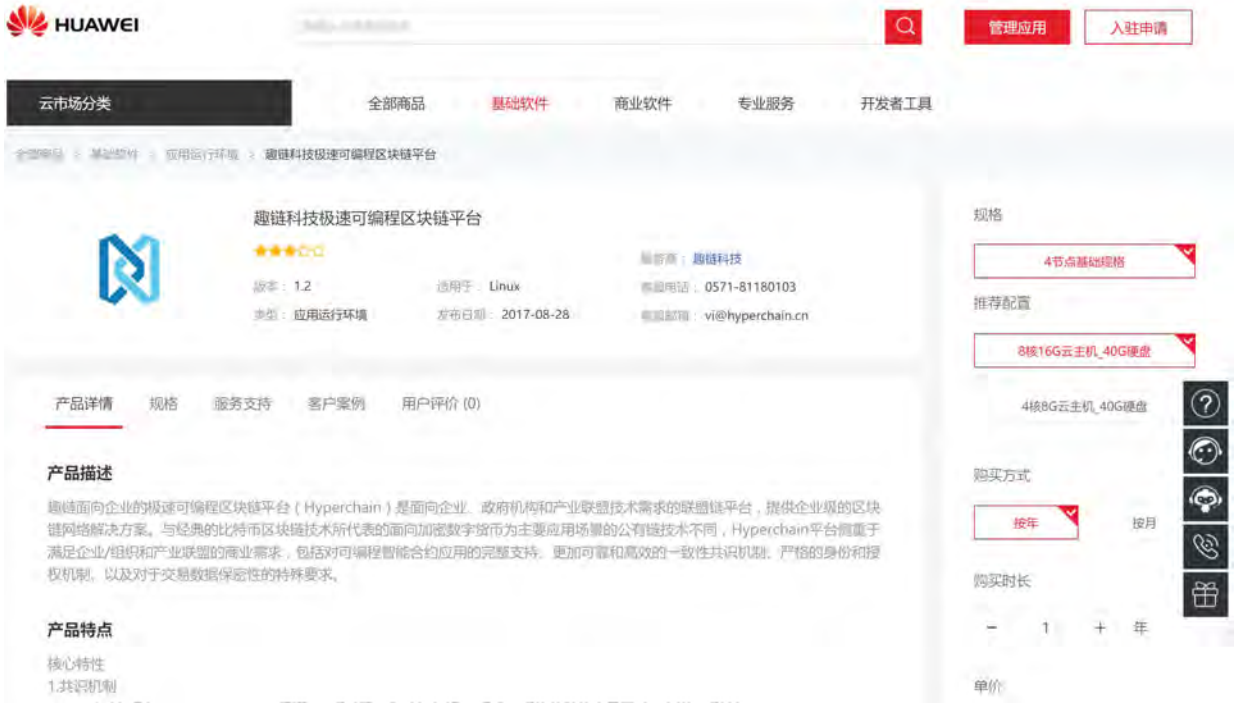
趣链联盟区块链应用部署架构



技术指标横向对比

产品名	共识	种类	语言	合约引擎	智能合约语言	权限	隐私保护	TPS	Latency	归档支持	可视化支持
Hyperchain	**RBFT**	**联盟链**	**GO**	**HyperVM**	**Java/Solidity**	**共识审批**	**同态加密/命名空间**	**>10000**	**<300ms**	**账本数据归档**	**企业级区块链监控**
Fabric	PBFT	联盟链	Go	Docker	Go	CA	N/A	~3000	未公布	v1.0支持	blockchain-explorer（不成熟）
Bletchley(EEA)	Cryptlets	联盟链	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Azure集成	Azure集成
Corda 1.0	N/A	联盟链	Kotlin	JVM	Kotlin/JAVA	N/A	N/A	N/A	N/A	N/A	N/A
Chain 1.2	FC	联盟链	Go	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
云象	PBFT	联盟链	GO	Docker	Go	CA	N/A	~3000	未公布	N/A	N/A
PDX	PBFT	联盟链	GO	Docker	Go	CA	N/A	~3000	未公布	N/A	N/A
Bitcoin	POW	公链	C++	N/A	N/A	N/A	N/A	7	10min	N/A	N/A
Ethereum	PoW+PoS	公链	GO	EVM	Solidity	N/A	N/A	~100	14s	N/A	eth-stats (星火计划)
小蚁	dBFT	公链	C#	AVM	C#	N/A	N/A	N/A	15s	N/A	官网公示
布比	未公布	公链	GO	EVM	Solidity	N/A	N/A	3000	>3s	N/A	官网公示
QTUM	Pos	公链	C	N/A	N/A	N/A	N/A	1000	N/A	N/A	N/A

上线华为云平台



基于“可信、开放、全球服务”的华为云，并联合趣链科技Hyperchain区块链平台，双方共同打造端到端的一体化区块链服务，未来将基于此平台共同为客户提供数字票据，供应链金融，数字存证等行业解决方案，为更多企业客户提供创新的服务支持

趣链科技极速可编程区块链平台

https://app.hwclouds.com/product/00301-46041-0--0

开发者平台

9月13日上线

基于联盟链的“趣链科技开发者平台”

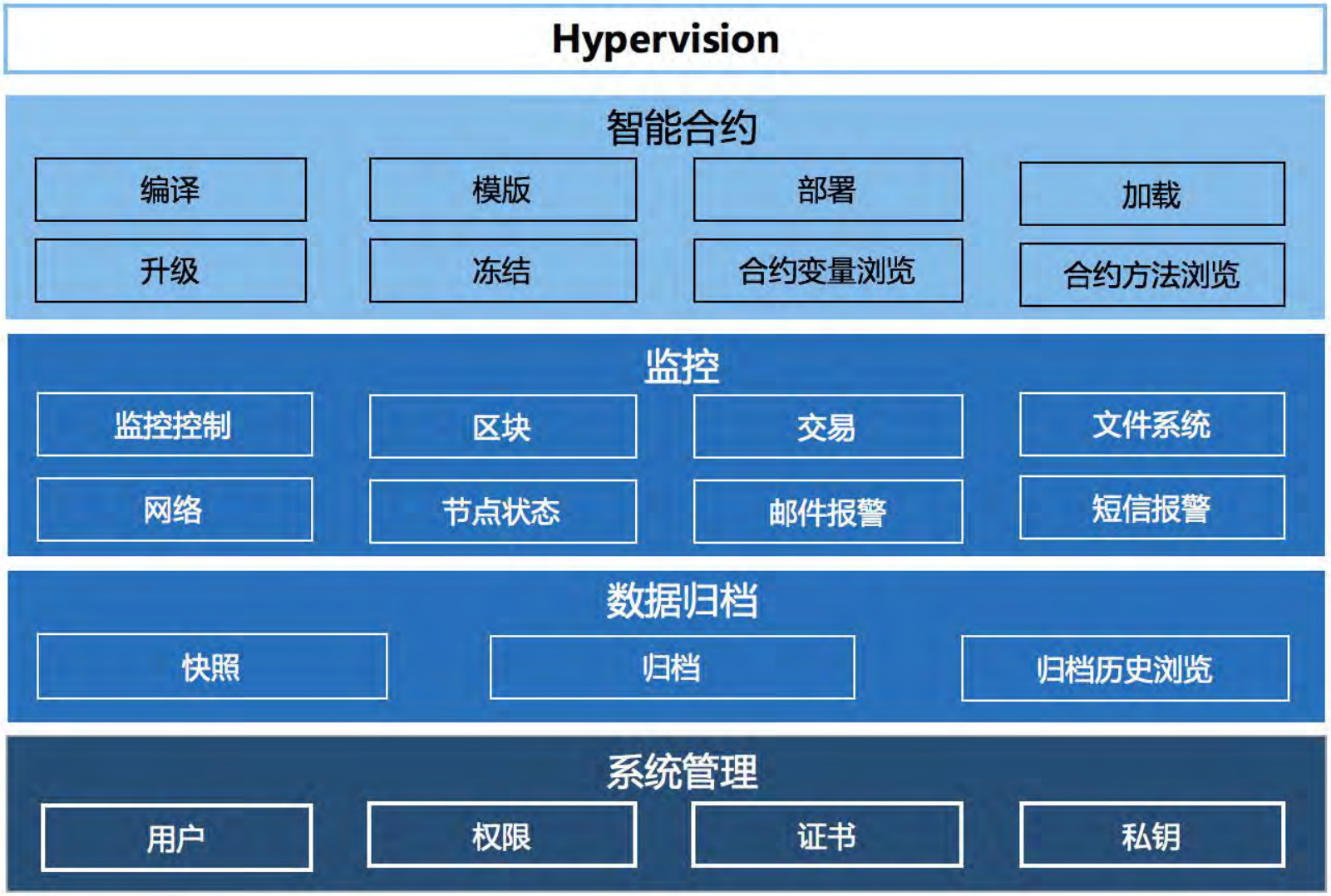
用户可以创建、发布和使用多中心化的应用程序

- 强大、易用、免费的智能合约在线编辑器：提供了针对Solidity语言（未来将支持JAVA语言）的智能合约代码编辑器
- 智能合约场景案例：附智能合约源码，方便部署体验和修改定制使用
- 区块链浏览器：展示区块信息、交易信息，区块链节点状态、节点维护方信息等

开发者平台地址：https://dev.hyperchain.cn

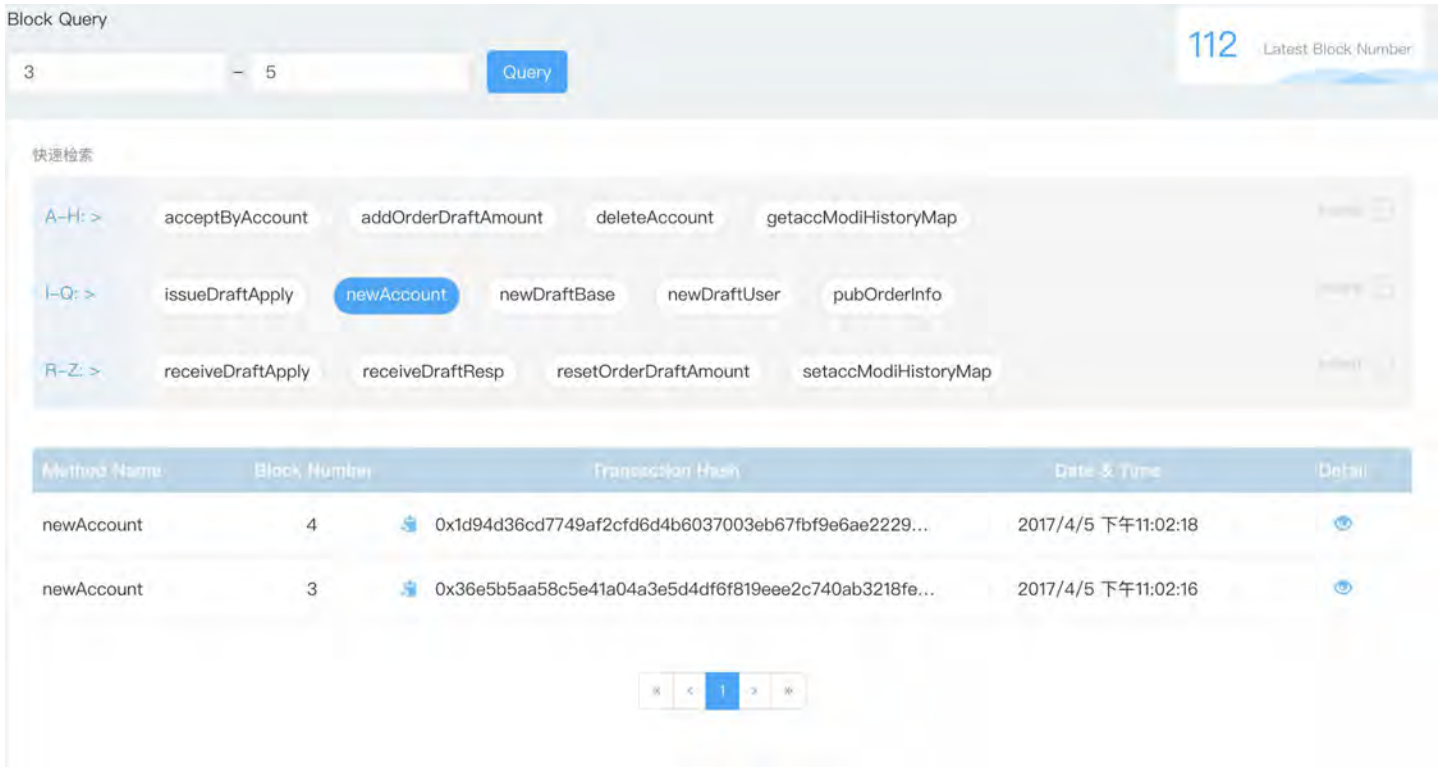
智能合约在线编辑器: https://editor.hyperchain.cn

监控运维-Hypervision



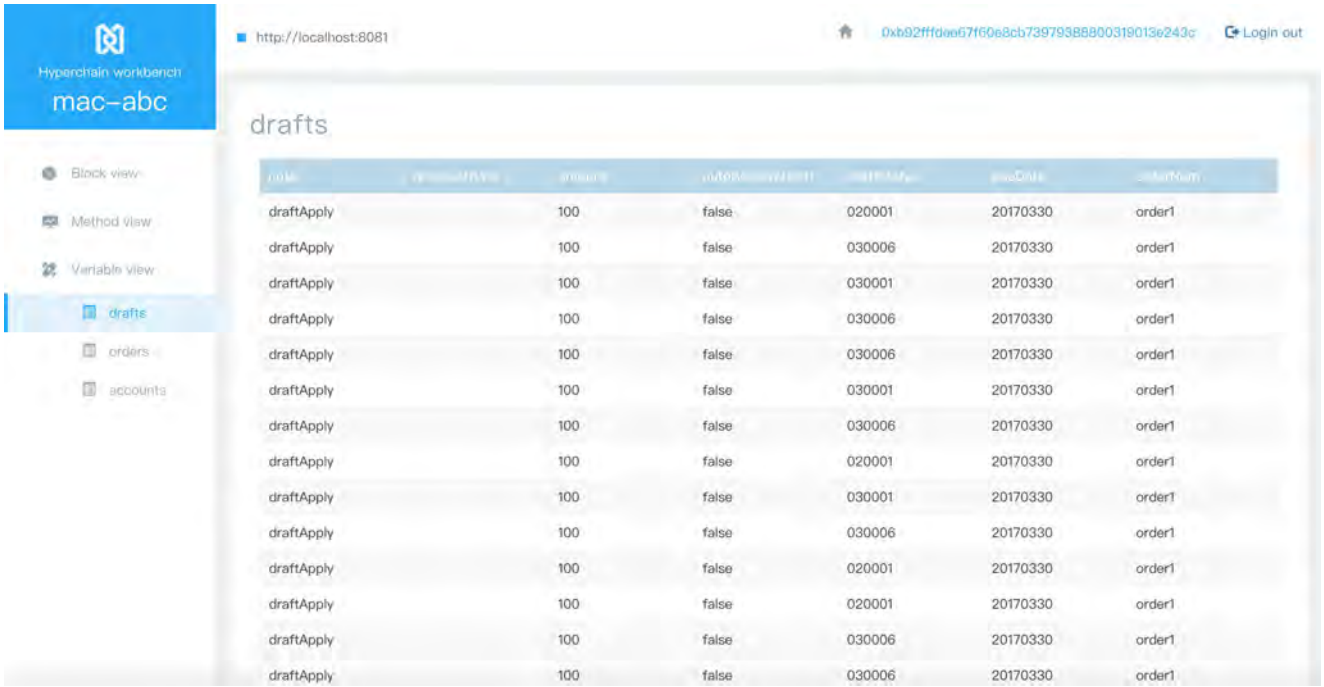
监控运维-智能合约

智能合约方法浏览



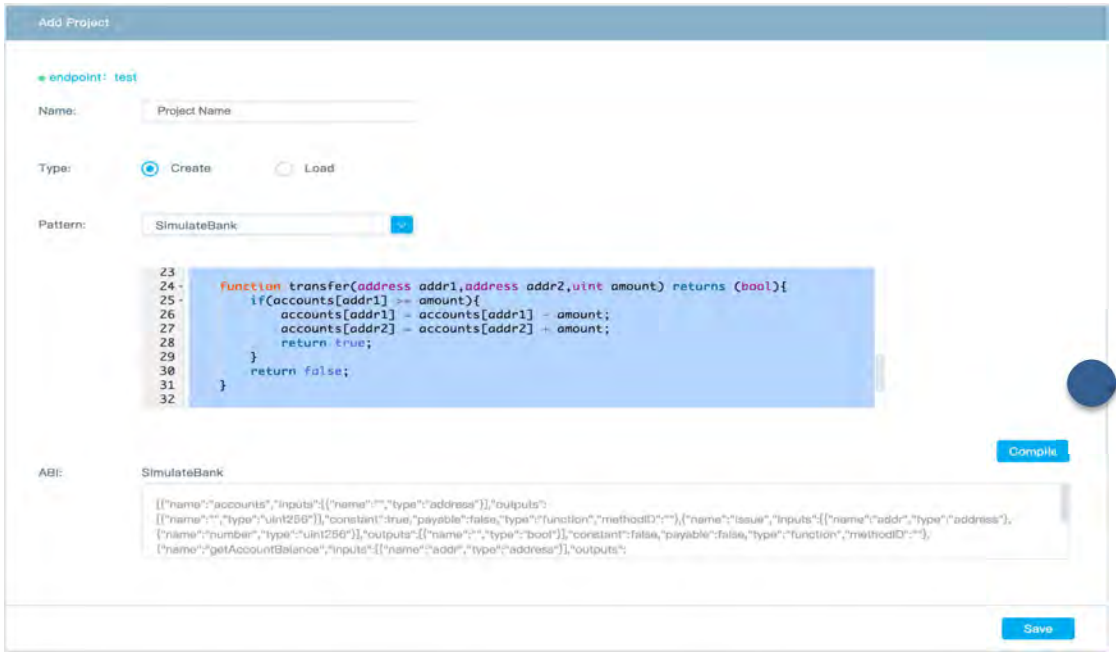
方法浏览通过解析区块链底层交易信息，使得不通过调用智能合约函数便能得知指定的智能合约方法在指定区块范围内的调用历史

智能合约变量浏览



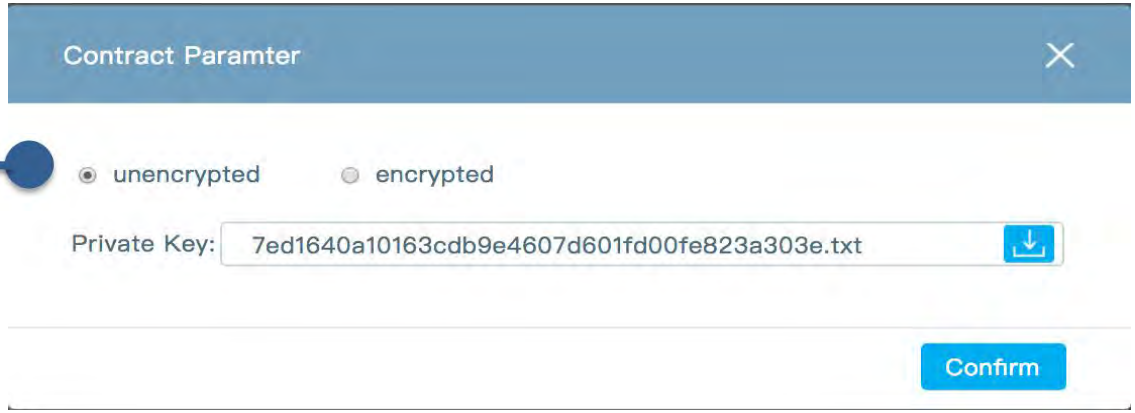
无需调用具体合约方法，通过解析区块链底层交易信息来得到智能合约中定义的变量的值

监控运维-智能合约

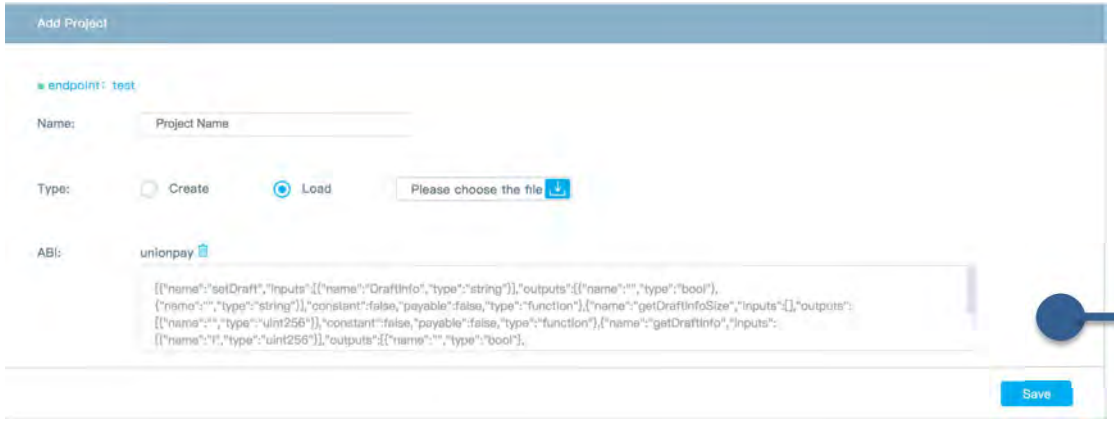


创建或升级合约

合约部署

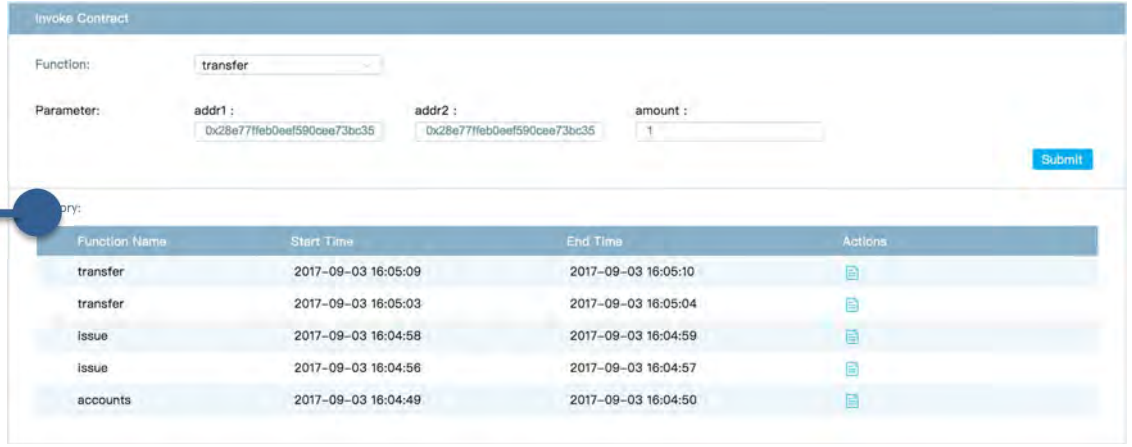


监控运维-智能合约



加载已部署合约

合约调用



监控运维- 监控

监控板面
- 区块信息
- 交易信息

区块链监控
- 监控控制
- 报警控制

监控运维- 监控

Host name	Rpc Address	Create Time	Block Height	Status	Disk Rate	File Count
peer4	172.16.2.4:8281	2017-09-02 22:55:01	13770	Live	28.89%	9
peer3	172.16.2.3:8281	2017-09-02 22:54:56	13770	Live	32.90%	9
peer2	172.16.2.2:8281	2017-09-02 22:54:52	13770	Live	30.20%	9
peer1	172.16.2.1:8281	2017-09-02 22:54:43	13770	Live	29.70%	9

节点状态
- 磁盘占用
- 区块高度

报警配置
- 监测范围
- 检测间隔

Chain Paramter

Chainlist Name : test

Total Volumn

Interval(Minute) : 1440 Upper Limit : 60000

Change Rate

Interval(Second) : 120 Upper Limit(%) : 1000

Throughput

Interval(Second) : 120 Upper Limit : 200

Success Rate

Interval(Second) : 120 Lower Limit(%) : 80

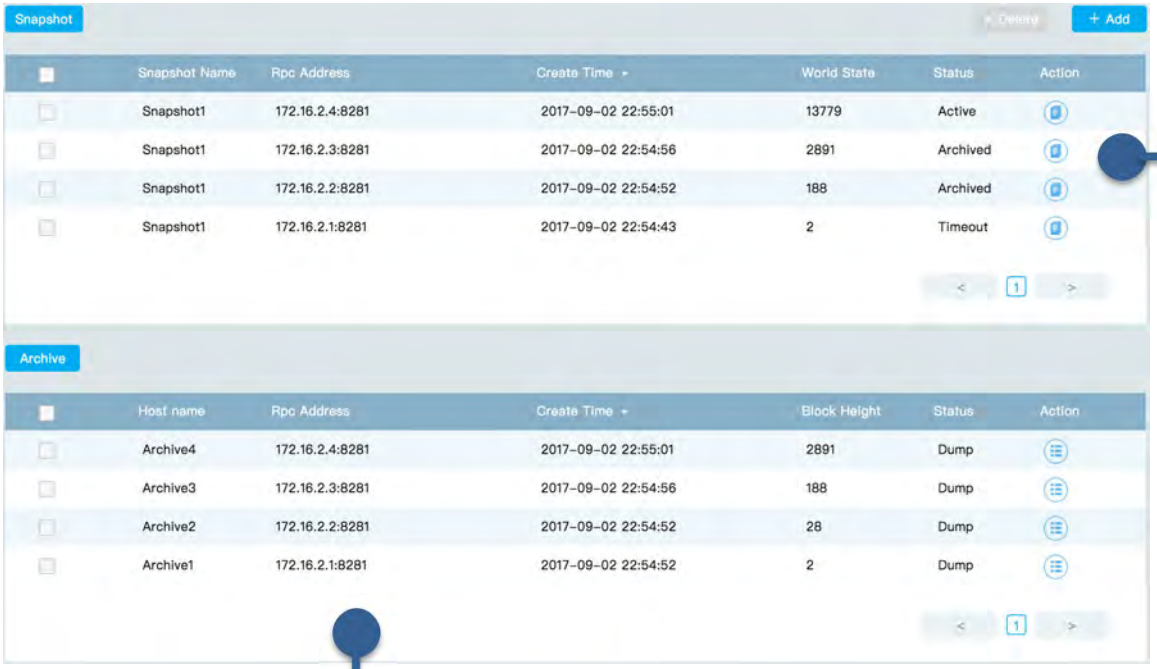
Average Response Time

Interval(Second) : 120 Upper Limit(ms) : 5000

Fail Number

Add

监控运维- 数据归档



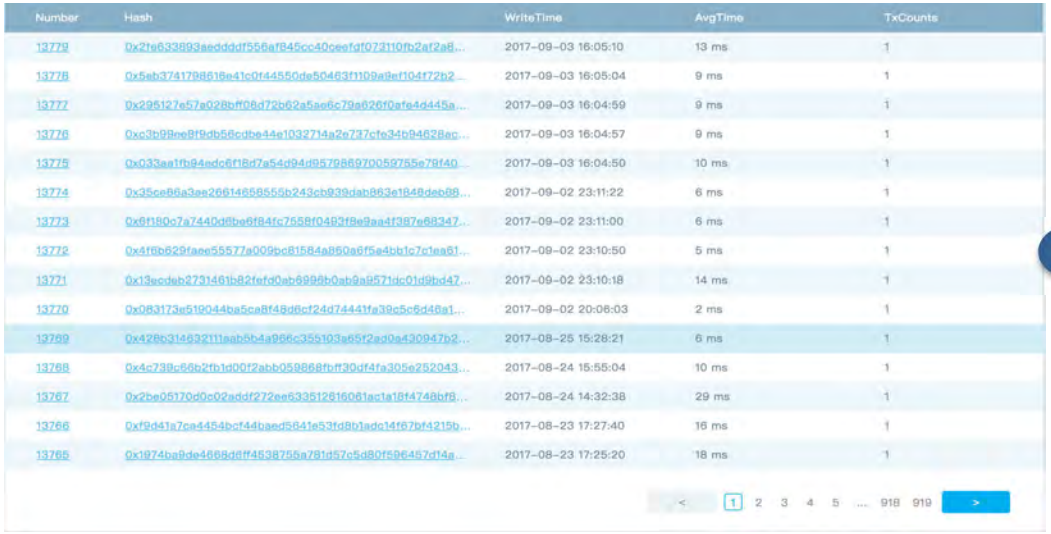
快照管理

快照是对某一个区块链世界状态的描述，包括该状态下的创世区块状态以及至该状态为止所产生的区块和交易记录等

归档管理

区块和交易记录可以通过归档管理模块进行归档转储，归档操作是基于快照进行的，实际上是按照快照所描述的世界状态信息进行归档操作，并更新新的世界状态

监控运维- 数据归档

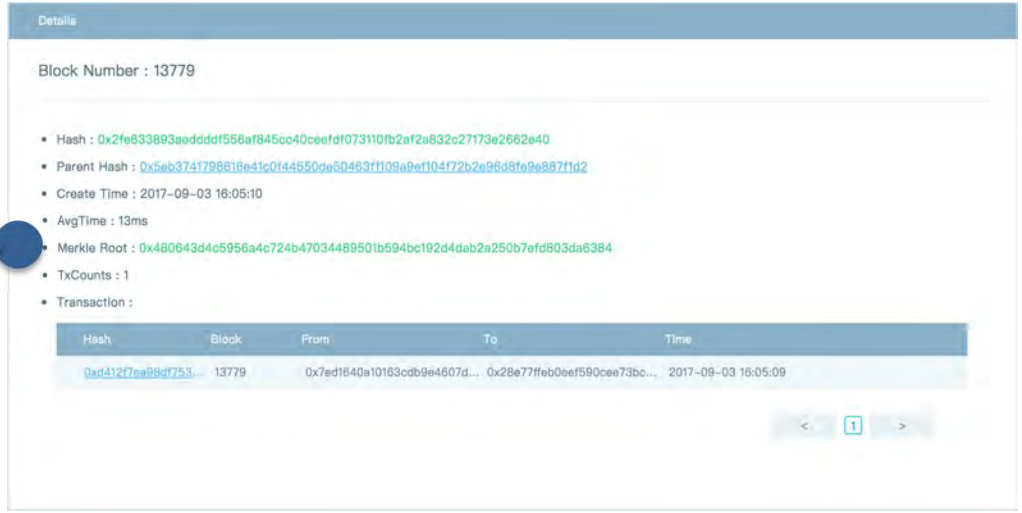


Number	Hash	WriteTime	AvgTime	TxCounts
13779	0x2fe633893aedddf556af845cc40ceefdf073110fb2af2a8...	2017-09-03 16:05:10	13 ms	1
13778	0x5eb3741798616e41c0f44550de50463f1109a9ef104f72b2...	2017-09-03 16:05:04	9 ms	1
13777	0x295127e57a028bff08d72b62a5ae6c79a626f0afe4d445a...	2017-09-03 16:04:59	9 ms	1
13776	0xc3b99ee8f9db56cdbe44e1032714a2e737cfe34b94628ac...	2017-09-03 16:04:57	9 ms	1
13775	0x033aa1fb94edc6f18d7a54d94d957986970059755e78f40...	2017-09-03 16:04:50	10 ms	1
13774	0x35ce86a3ae26614656555b243cb939dab863e1848deb88...	2017-09-02 23:11:22	6 ms	1
13773	0x6f180c7a7440d6be6f84fc7558f04f3f8e9aa4f387e68347...	2017-09-02 23:11:00	6 ms	1
13772	0x4f6b629faee55577a009bc81584a860a6f5e4bb1c7c1ea61...	2017-09-02 23:10:50	5 ms	1
13771	0x13ecdeb2731461b82fefd0ab6996b0ab9a9571dc01d9bd47...	2017-09-02 23:10:18	14 ms	1
13770	0x083173e519044ba5ca8f48d6cf24d74441fa39c5c6d46a1...	2017-09-02 20:06:03	2 ms	1
13769	0x426b3146321111aab5b4a966c355103a65f2ed0a430947b2...	2017-08-25 15:28:21	6 ms	1
13768	0x4c739c66b2fb1d00f2abb059868fbff30df4fa305e252043...	2017-08-24 15:55:04	10 ms	1
13767	0x2be05170d0c02addf272ee63351261606 1ac1a18f4748bf8...	2017-08-24 14:32:38	29 ms	1
13766	0xf9d41a7ca4454bcf44baed5641e53fd8b1adc14f67bf4215b...	2017-08-23 17:27:40	16 ms	1
13765	0x1974ba9de4668d8ff4538755a781d57c5d80f596457d14a...	2017-08-23 17:25:20	18 ms	1

< 1 2 3 4 5 ... 918 919 >

归档数据浏览

归档数据详情



Details

Block Number : 13779

- Hash : 0x2fe633893aedddf556af845cc40ceefdf073110fb2af2a832c27173e2662e40
- Parent Hash : 0x5eb3741798616e41c0f44550de50463ff109a9ef104f72b2e96d8fe9e887f1d2
- Create Time : 2017-09-03 16:05:10
- AvgTime : 13ms
- Merkle Root : 0x480643d4c5956a4c724b47034489501b594bc192d4dab2a250b7efd803da6384
- TxCounts : 1
- Transaction :

Hash	Block	From	To	Time
0xd412f7ea98df753...	13779	0x7ed1640a10183cdb9e4607d...	0x28e77ffeb0eef590cee73bc...	2017-09-03 16:05:09

< 1 >

目 录

应用案例

类别	应用	合作单位	状态
数字资产类	移动汇票	浙商银行	已上线
	应收账款	浙商银行	已上线
	数字票据	中国农业银行	已上线
	商业保函	兴业银行	准备上线
	供应链	浙江国金数据科技有限公司	准备上线
	跨境汇款	银联国际	开发中
	权益系统	权益系统	开发中
	数据交易	上海数据交易中心	开发中
	企业债券	中国银行间市场交易商协会	开发中
	证券交易	上海证券交易所	开发中
	场外交易	招商证券	开发中
	信贷管理	国家开发银行	开发中
	…	…	…
数字存证类	电子签购单	银联+光大	已上线
	存证溯源	甲骨文超级码	已上线
	股票审查	道富银行	开发中
	…	…	…

Q&A
Thanks

BDTC 2017 中国大数据技术大会
Big Data Technology Conference 2017