FAB
Fast Access Blockchain

系统白皮书
2017. 10. 10

敏捷公共区块链

面向实际应用的高可扩展公用区块链网络

敏捷区块链基金会 / 共识联盟组织
Fast Access Blockchain Foundation

68 West Bay Road, Cayman Islands
1-800-734-9388 info@fa.biz fabcoin.co

技术合作伙伴: FA Enterprise System Inc.
665 Hood Road, Markham ON L3R4E1 Canada

目录

1. 概述

区块链技术是下一代互联网 – 价值互联网的基础，比特币及以太坊等区块链平台的成功运行，为区块链应用展示了良好的前景。

然而，由于受通讯、节点性能及共识机制等因素的制约，目前的公有区块链系统都面临交易处理能力严重不足的瓶颈问题，如比特币及以太坊每秒钟处理交易量都不超过7笔。

这是区块链迈向实用面临的巨大障碍，现实经济活动中，许多应用场景下的交易量都超过这一规模，如交易所、物联网平台、电商平台、供应链、医疗等，单个平台的实际交易量往往每秒钟几十笔、几百笔，甚至数千笔，而公共区块链是同时面向众多应用场景的，实际要求的处理能力要高得多。

解决这一问题迫在眉睫。

加拿大发企业系统公司区块链研发团队，历时三年深入探索研究，提出多项突破性创新技术，推出了具有良好扩展性能的全新区块链系统架构完善设计方案 – 快捷公用区块链(发链)系统(Fast Access Blockchain network – FAB)，致力于有效突破区块链技术障碍，为构造满足实际商业应用需求的区块链系统铺平了道路。

快捷公用区块链系统(Fast Access Blockchain Network)，也称发链(FAB)，是由经过一体化设计的三大组成部份 – 基础区块链、辅助区块链及开放存储架构组成，三位一体，相互配合，构建了具有统一协议基础、功能相互协调、具有全程合法性及有效性验证、真正去中心化的、安全可靠的高性能区块链完整架构。

1. 1 系统设计原则与哲学

发链严密的设计逻辑是建立在严格的设计原则与哲学基础上的，区块链系统的鲜明特性与应用需求相冲突，技术方法与现实条件相矛盾，难以调和，系统设计需要遵循完整的因果循环原则，这是建立在一套哲学思想基础上的。

1. 1. 1 系统设计原则

构造信任 – 这是区块链的核心使命，系统设计的目的就是为应用构建一个可信任的系统。

去中心化 – 是区块链的核心特征，是构造信任的根本手段。

开放架构 – 开放是去中心化的必要条件，开放意味人人平等、代码开源、设施平民化。

面向应用 – 开放架构导致平等参与、平等使用，互不信任的参与者需要信任机制保证。

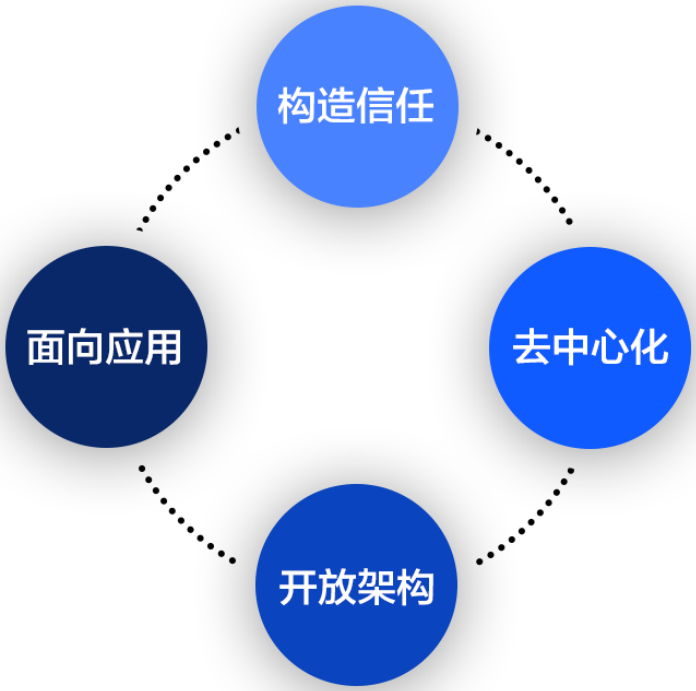

图1. 系统设计原则关系图

1．1．2 哲学思想

根据上述设计原则构建系统，面临一个无法调和的矛盾：去中心化、可扩展性、可靠性三者不可兼得，去中心化而又可扩展，则系统不可靠；可扩展而又可靠则无法去中心化；去中心化而又可靠则不可扩展。

要解决这一矛盾，需要一套可行的哲学理论，我们归纳出四项哲学原则：

信任源于非信任 – 区块链系统值得信任，但参与节点互不信任；

可扩展的不可扩展性 – 可信任的去中心化系统不可扩展，但局部节点可扩展；

无裁决权的中心化非中心化 – 扩展局部节点形成中心化，若将裁决权上交变成去中心化；

可靠的不可靠性 – 非中心化的局部中心节点不可靠，但去中心化的裁决机制是可靠的。

1．2 技术要点

按照系统设计原则，专注公共区块链核心特性的同时面向实际商业应用，必须解决哲学上的矛盾，这不仅需要理论方案，还需要可行的技术方法。

1．2．1 解除理论矛盾的措施

要解除这些客观存在的矛盾，需要创新思维，我们提出了一个全新的解决方法：构造制约错位结构。

系统每一个环节制约与载体有机相连，但将系统各环节的制约与载体错位置放，就可以有效解决这一难题。

为此，确立如下设计思想：

建立一条开放的公共区块链 – 基础区块链，它高度去中心化但难以扩展，必须以最小数据量、最小计算量、最小网络带宽为目标，以实现最大的开放度、最高程度的去中心化、最强的可靠性，这样的系统不可扩展，但应用要求系统必须扩展。

建立辅助链，从局部实现扩展 – 实际应用要求系统有强大处理能力，因而，必须使系统具有可扩展性，将扩展性错位投放到局部节点，成为可行之路，但这样的系统呈现中心化，变得不可信任。

建立开放存储系统使数据及裁决去中心化，局部节点的离链及中心化特征使其不可信任，必需解除其中心化机制，因而设立去中心化的开放存储架构，但存储架构无法构成完整的去中心化机制，因此设计SCAR机制与去中心化的基础区块链关联。

1．2．2 实现的技术措施

要实现错位机制的完整性，仅有基础链、辅助链及存储机制不够，还需要其它技术手段。

为此，我们提出了三项关键技术应用方案：KanBan、SCAR、Sharding分别与基础链、辅助链、存储系统相配合的技术方案。

其中Sharding系引用现有大数据中的技术，这里用作快速数据查询及共识决策；

KanBan及SCAR是我们在本区块链系统中提出的创新设计；

基础区块链 + KanBan – 辅助链 + SCAR – 开放存储架构 + MapReduce技术支撑的矛盾错位架构，形成了完整的解决方案。

技术措施的组成及相互关系如下图：

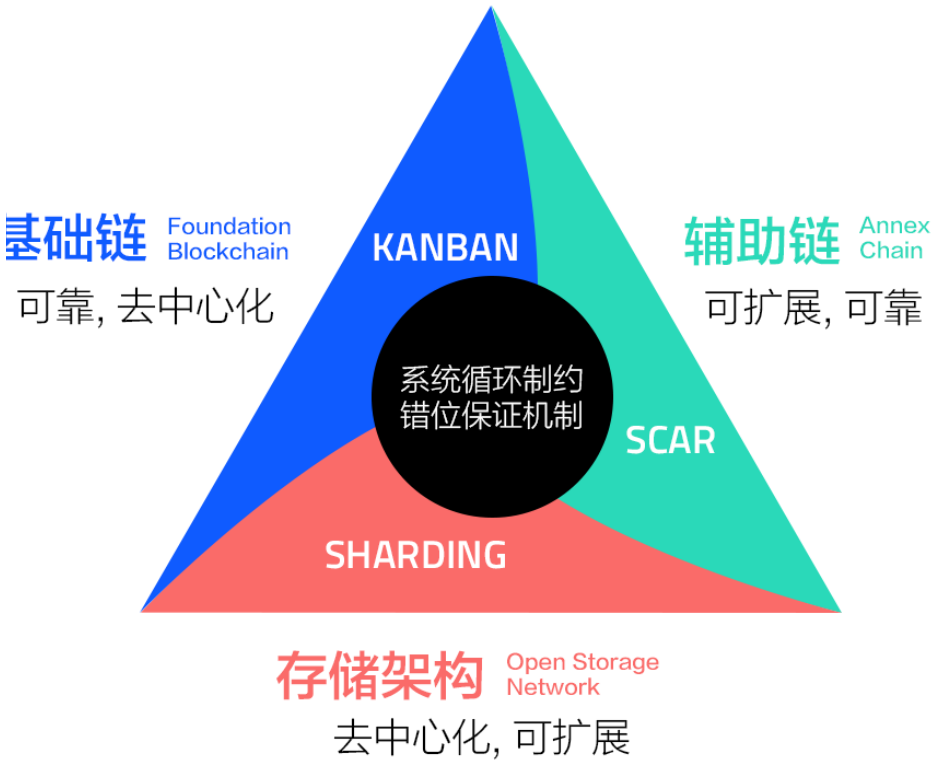

图2. 系统循环制约错位保证机制

为了使方案流线作业，易于实施，同时也为了使系统具有更广泛适应的标准性，我们提出了三项创新技术协议：

跨链统一地址协议(CCUA – Cross Chain Unified Address);

交易互换协议(TEP – Transaction Exchange Protocol);

开放验证规则协议(OVP – Open Verification Protocol);

至此，系统在理论上和技术上具备了完整的解决方案，也广泛兼容准备了条件。

这些措施为使整个系统在去中心化、可信任性及可扩充性方面提供了充分的理论及技术保证，并在诸如防范

辅助链双花攻击、解除交易账户关联、简化交易验证程序等环节提出许多技术细节，为系统成功突破区块链技术瓶颈提供了切实有效的手段，圆满解决了区块链开发中普遍面临的去中心化、安全性及可扩展性不可兼得的难题，也为系统的广泛兼容及流线化作业提供了技术保证。

本系统是第一个真正满足实际商业应用需要的公共区块链系统。

2. 技术方案

由于面临的通讯条件和节点处理能力千差万别及共识机制的制约，公有链底层无法单独处理大量交易已经成为公认的事实，因此，要突破这一障碍，必须在整体架构上创新。

2. 1 系统整体架构

快捷区块链系统旨在利用利益激励机制构建满足大规模日常商业需求的快速、低费用、高效而又安全、可靠的去中心化公共区块链经济生态体系。

系统由三部份构成：基础区块链(Foundation blockchain)、辅助链(Annex chain)及开放存储架构(Open Storage Architecture)，是根据矛盾错位机制建立在统一底层协议与共识机制核心规则基础上的开放经济生态的组成部份，分别执行不同的功能，整体上相互协作、相互验证，构成完整的信任保证及价值维护机制，解决了去中心化、可扩展性、安全性三者不可兼得的难题。

系统的总体逻辑架构如下图所示：

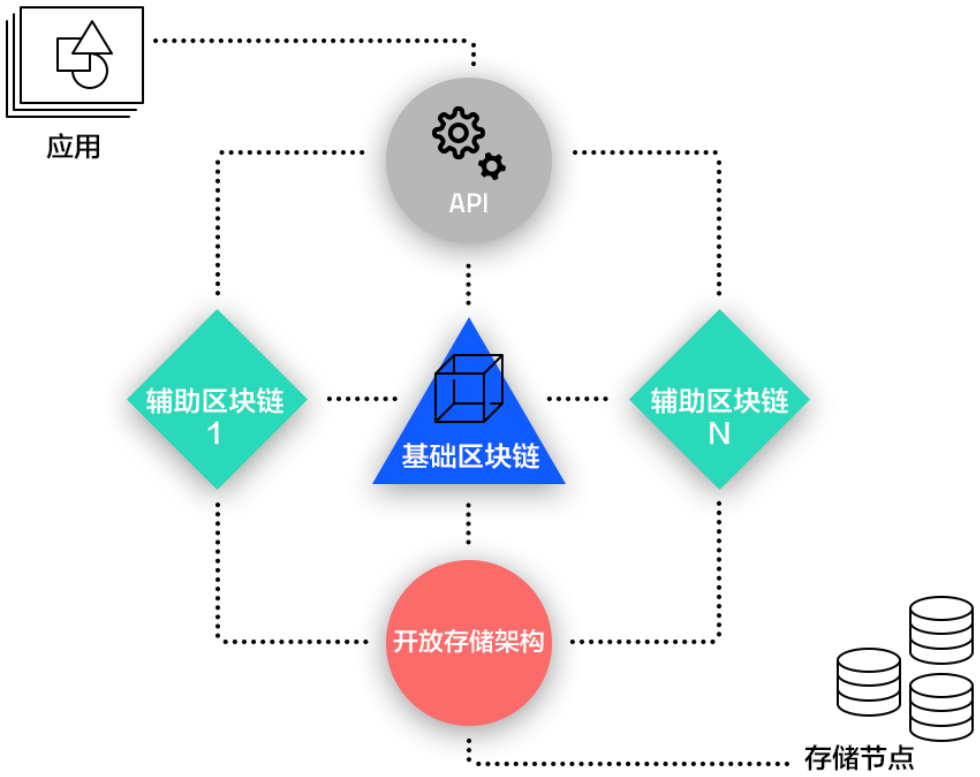

图3. 系统总体逻辑架构

与现有的比特币主链/侧链机制不同，本系统的基础链-辅助链-存储架构机制是经过底层协议统一设计的完整架构，数据加密及验证机制相互兼容、互相配合，是交易高效协同认证核准与安全保证机制兼备的一体化设计，即避免了中心化问题又能大幅提高效率，并保证了安全性，且易于灵活配置，使用户可以自由方便地加入网络节点，第一次真正实现了能够满足海量业务需求的、去中心化的、具有可靠性及安全性的公共区块链完整设计。

系统的设计思想是：基础区块链以最小数据量、最小计算量及最小网络带宽需求为目标，提供底层协议、智能合约、终极账本、终极裁决权；辅助链或区域性节点执行大规模本地离链交易；开放存储架构确保本地数据的去中心化存储。

系统开创性地提出KanBan、SCAR及CCUA三项技术，使本地离链交易状态可以在整个区块链范围以去中心化方式实时更新及核查，防止双花，从而使系统可以满足包括交易所、物联网、电子商务、供应链、医疗等大交易量场景下去中心化大规模实时交易的要求；为了强化本地交易的去中心化功能，系统设计了开放存储架构，以经济激励机制及强制性规则，通过协议及共识机制强制辅助链或本地化节点支持本地交易的去中心化开放存储。

基础区块链的激励机制是挖矿收益，辅助链的激励机制是业务收入及挖矿收益，存储节点的激励机制是数据、费用及挖矿收益。

2．2 基础区块链（又称主链）

基础区块链是系统的核心，设计以最小数据量、最小计算量及最小网络带宽需求为目标，主要提供基础协议、账本、智能合约、价值体系，拥有最高裁决权，基础区块链的信任合法性来源于全部参与节点。

基础区块链设计采用与生产结合的Proof-of-Production (PoP)共识机制，一种权益证明与生产力证明混合机制，但在具备足够生产力之前，仍采用与比特币类似的PoW共识机制。

2．2．1 基础区块链全节点功能构成

基础区块链全节点除具有通常的区块链、钱包、矿工、路由、虚拟机等功能模块外，特别引入KanBan功能。KanBan是中文“看板”的意思，源于现代供应链/制造链系统，在流水线上工人们从事着固定流程工作，但KanBan向大家提供即时信息，以提示注意事项或特别变更。

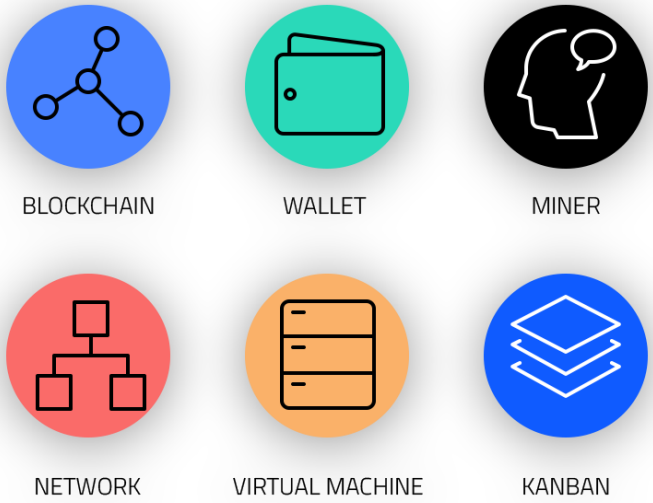

图4. 基础区块链全节点功能构成

2．2．2 KanBan

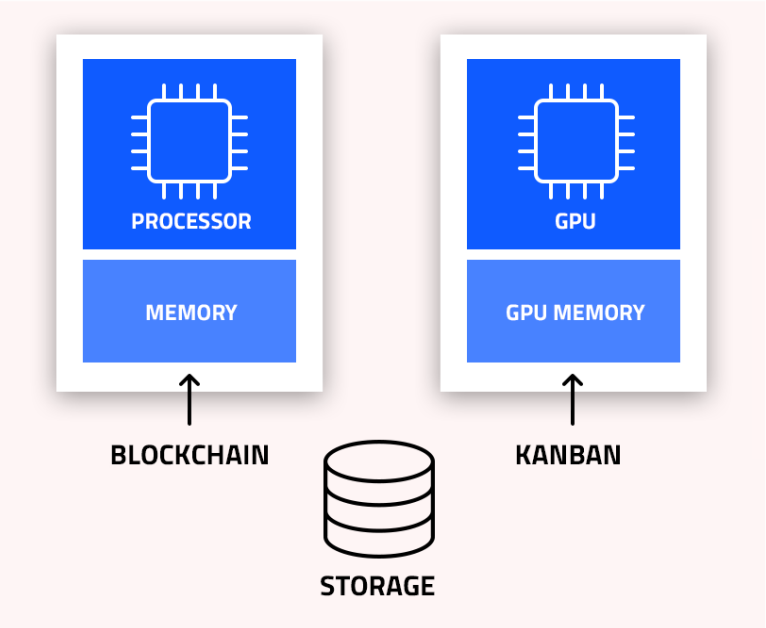

图5. 基础区块链节点KanBan示意图

KanBan的设计目的是，在不显著增加主区块链负担的情况下，在全局范围提供对辅助链交易状态的实时更新及查询能力，是专为有效防止辅链双花攻击的特殊模块。

本系统中，KanBan以内存数据管理程序或内存数据库的形式，运行于基础区块链的节点计算机或与基础区块链相配合的独立计算机的GPU中，以全局呈现辅助链交易状态，本系统将KanBan设计为GPU内存数据库，一方面基本不占用节点普通资源，保证其基础区块链作业效率，另一方面，GPU内存数据库数据处理能力远超计算机主处理器，可以大幅度提高KanBan运行效率，使小批量状态更新及查询操作可以在毫秒级时间内完成。

由于KanBan功能，辅助链的交易均以去中心化方式实时全局呈现，可以有效实现防止双花的目的。但由于KanBan运行于计算机的GPU中并占用GPU内存，因此，对于运行基于GPU的矿工软件的节点，矿工软件

须与KanBan分别运行于不同的计算机中。

KanBan状态的维持与更新是由智能合约控制的，并且KanBan与主、辅链节点及存贮节点之间存在严格的有效性验证确认关系，以确保KanBan数据的准确、合法。

KanBan的处理流程是：收到来自辅助链的包 → 验证包的合法性 → 验证交易合法性 → 更新KanBan状态 → 向辅助链提交收据。

这样KanBan中终始保存着在辅助链交易的地址或账户的准确状态，如果需要，还可进一步向存储节点核实辅助链上的详细交易记录。

2．2．3 KanBan中的数据

辅助链表：

编号	公钥	末块Hash	未锁块交易Merkle Root	公钥	公钥
1	4ds5kgce3...vd3	309ew98gweio	hgurs2ua6serhufdsfe423	40000	20160223T021405
2	ly8r5gdt4s...gte	9rc6ghd8fjcndu	goir7q3c9sk4ge8rd3afrb	1200000	20160508T223611
...	...	...			...
n					

图6. KanBan中的辅助链表

地址(账户)状态表：

地址	余额	可疑	时间
0m5frtfgdesr.....	200000	F	20160312T100325
0msetvuehfe.....	16000000	T	20160520T081220
...	...		...

图7. KanBan中的地址状态表

未锁块交易表：

交易号	出地址	入地址	数量	时间
1	4ds5kgce3...vd3	309ew98gweio	40000	20160223T021405
2	ly8r5gdt4s...gte	9rc6ghd8fjcndu	1200000	20160508T223611
...	...	...		...
n				

图8. KanBan中的未锁块交易表

KanBan在收到辅助链数据包后，验证包及其中交易的合法性，经验证合格后更新相关地址状态，并向辅助链返回收据并通知存储节点，包括节点余额、合约签名，如不合格则拒收并通知辅助链。

KanBan可以实时的方式提供每个地址的当前状态，以防止双花。KanBan还提供每个辅助链的当前块的签名存根，以证实辅助链中块的有效性。

2．2．4 验证交易有效性

对辅助链上的新交易，系统通过KanBan状态及基础区块链交易状态验证交易的有效性。

对于同一账户或地址有冲突的，时间优先，时间相同的，hash值优先。

如果交易发生冲突，对产生冲突的地址或账户设置可疑标识。

对于KanBan中设置可疑标记的地址，在新交易发生时，要通过开放存储架构节点清查详细交易记录。

技术上为了强化KanBan处理性能，开发专用GPU数据处理模块，使KanBan运行于节点计算机GPU中，不占用节点普通资源，以使其有效处理基础区块链交易。

KanBan除了用于快速处理辅助链交易、维护辅助链地址状态外，同时还执行辅助链挖矿任务。

KanBan还可周期性地向硬盘镜像数据，以备掉电后快速恢复。

2．2．5 基础区块链网络中KanBan构成

KanBan可以运行于基础区块链节点主算机中，也可以运行于与基础区块链节点相联的独立主算机，甚至可以运行于存储节点主算机中。技术上，一个节点也可以没有主链节点、辅链节点或存储节点，而仅仅是一个独立的KanBan节点。

由于KanBan程序设计为GPU数据库程序，运行于计算机GPU中并占用GPU内存，因此，未配有适当图形加速卡的设备无法运行KanBan。

设计方案上，系统并不要求基础区块链上所有全节点都带有KanBan功能，但带有KanBan功能的节点均拥有KanBan标识。

不带KanBan功能的节点不参与KanBan服务，也不参与辅链共识机制；提供KanBan功能的节点则可以赚取辅助链采矿收益，此收益来自辅助链的交易费用。

事实上，对于基础条件比较好的节点，可以提供包括基础区块链、KanBan、辅链及开放存储节点在内的全部系统功能。

基础区块链网络及KanBan分布示意图如下：

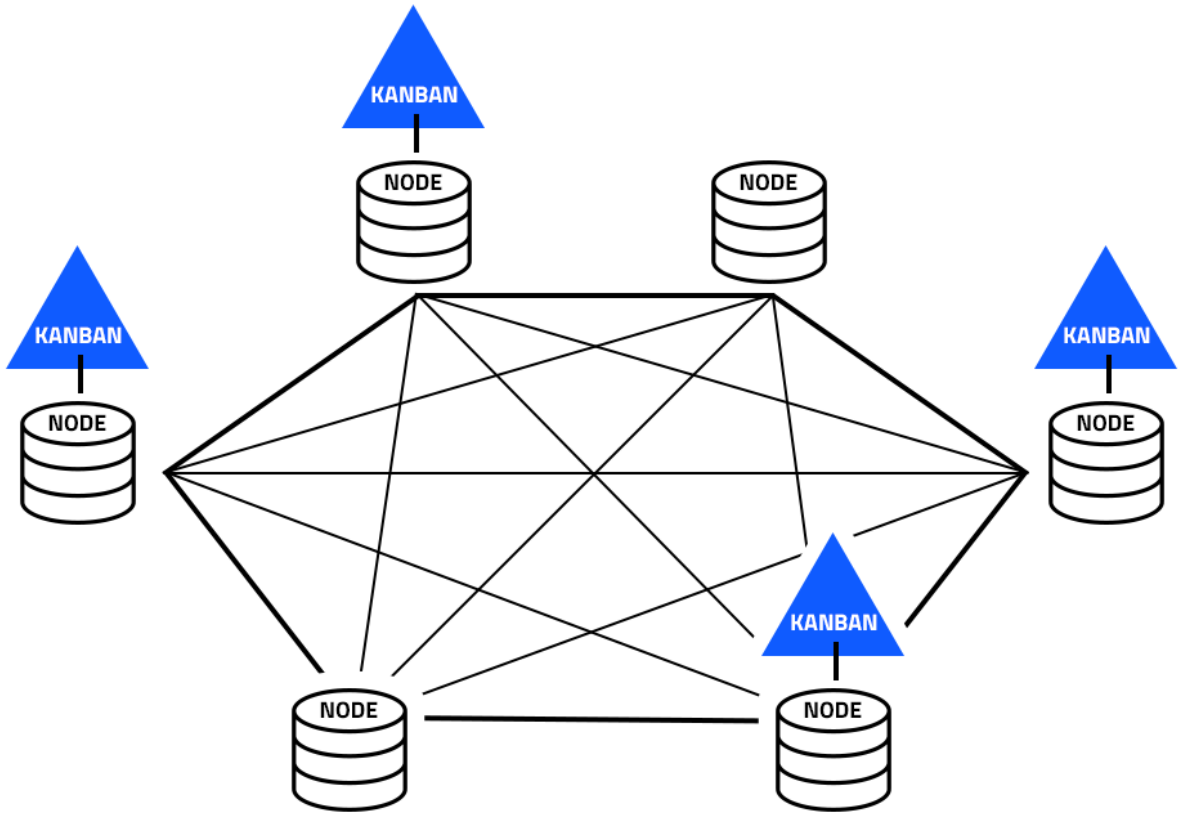

图9. 主区块链网络图(并非所有节点均为KanBan节点)

2．2．6 KanBan的配置要求

节点计算机若要运行KanBan，须配有运行适当算法的图形加速卡，初始KanBan节点的硬件要求是安装16GB以上内存的图形加速卡，但随着数据量的增加，要求会提高。

提高GPU硬件要求不影响共识机制，但可能影响运作效应。因为系统中KanBan节点是根据性能分类的，并分别作也标识，如16GB为KB1, 32GB为KB2。

假设保留2GB GPU内存作为节点其它用途，2GB用作辅助链相关数据，其余用作最重要的离链账户地址状态表。

一条账户状态记录数据不超过64字节，则12GB可以提供大约2亿个活动账户状态记录；如果安装32GB图形加速卡则可以提供约5亿个活动账户状态信息。

系统设计方案上，支持KanBan分组功能，一组KanBan服务于某一或某些辅助链。

2．2．7 基础区块链实施方案

基础区块链在比特币系统上改进实施，其核心是增加对KanBan、SCAR及CCUA的支持，增加辅助链验证及根合约状态设置机制，增加智能合约机制，减少交易及块的数据量。

核心架构如下图所示：

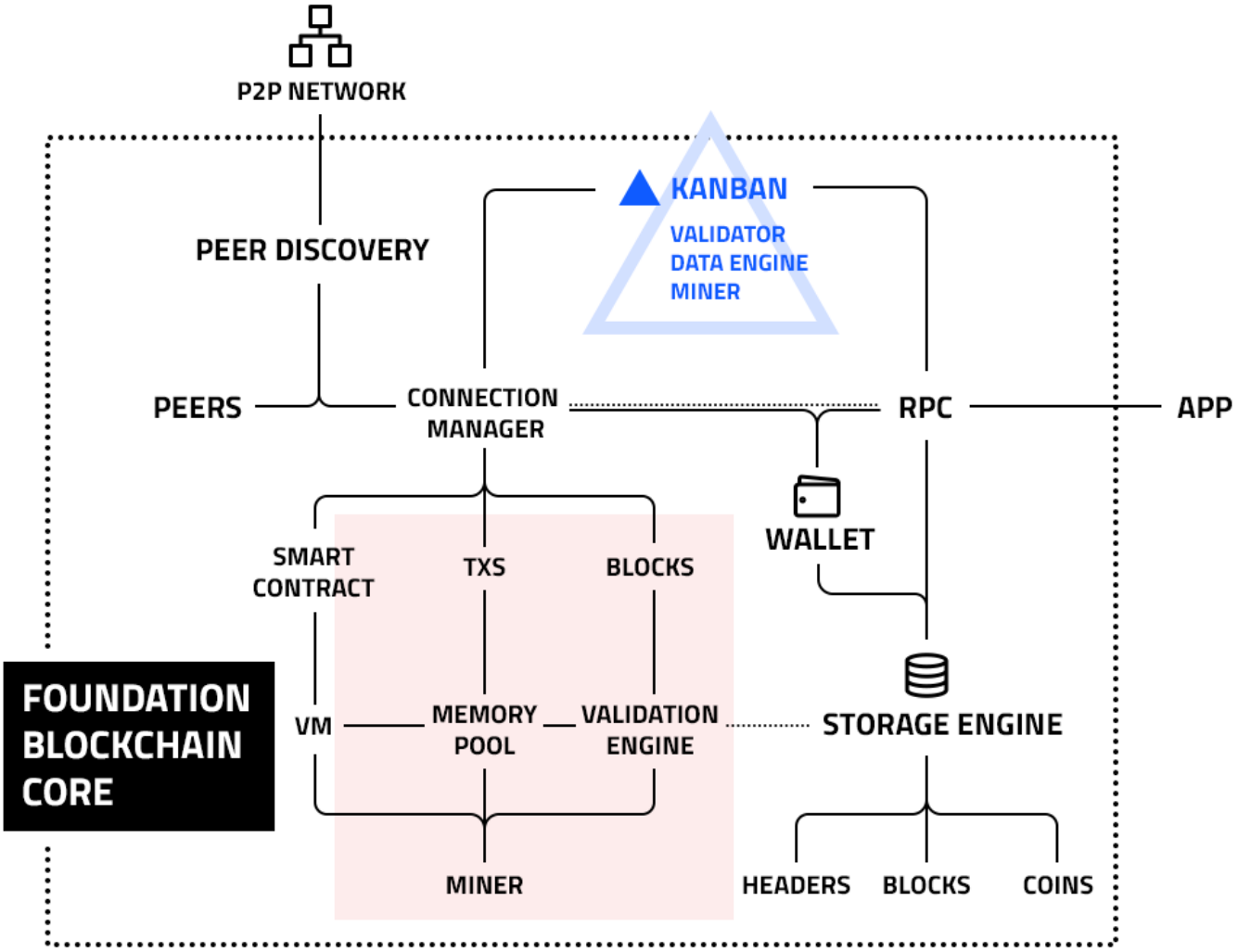

图10. 基础区块链内核架构

系统开发采用流线型独立模块结构，易于配置、管理及维护。基础区块链内核中的许多模块也将应用于辅助链及开放存贮架构模块中。

2. 3 辅助链

辅助链是系统的重要组成部份，通常辅助链节点承载大量具体业务，如汇兑交易、电子商务、供应链、物联网平台或医疗平台等。

辅助链节点业务呈现中心化特征，但根据本系统设计，价值确认及交易最终裁决权是由基础链以去中心化方式执行的，配合开放存储架构的去中心化数据存储，从根本上保证了辅助链具有中心化特征的本地交易实现完全去中心化，而且安全、可靠。

根据系统设计，即便一个辅助链专为欺诈目的而设，也无法给离链客户造成任何损失。

2．3．1 辅助链技术方案

辅助链起源于基础区块链授权，由基础链提供原始证据及身份，并通过基础链签发的智能合约确定本辅助链的属性及参数，交易过程中由主链、KanBan及存储架构参与验证。

设计思想上，主要的网络传输及数据处理尽量在辅助链节点执行，而仅将必要的证据及数据提交到KanBan及开放存储系统。

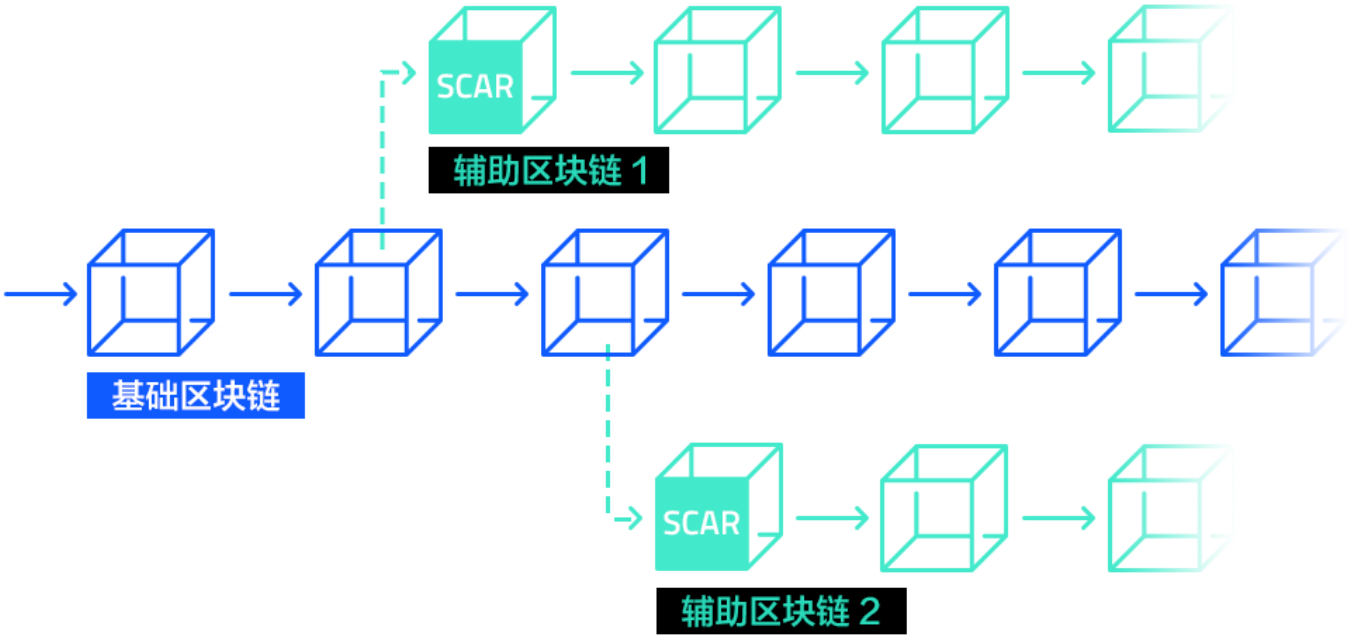

图11. 辅助链构造示意图

注意，图示的辅链并非从主链分叉形成，虚线仅表示依赖关系。

辅助链包含如下关键要素：初始块、智能合约地址路由(SCAR)、跨链统一地址(CCUA)协议及KanBan证明，它们保证了辅链交易的可靠性、安全性和有效性。

每条辅助链的起始块是由基础区块链签署的特别块，并为辅助链定义一个特别账号，称为智能合约代理路由(Smart Contract Agent Route，简称SCAR)，以代理辅助链与外部的一切交易。

在系统总体设计方案上，辅助链可以为从同一个根上生成的两条独立区块链，分别为价值链和事务链，用于服务于辅助链的价值维护与事务管理。如下图所示:

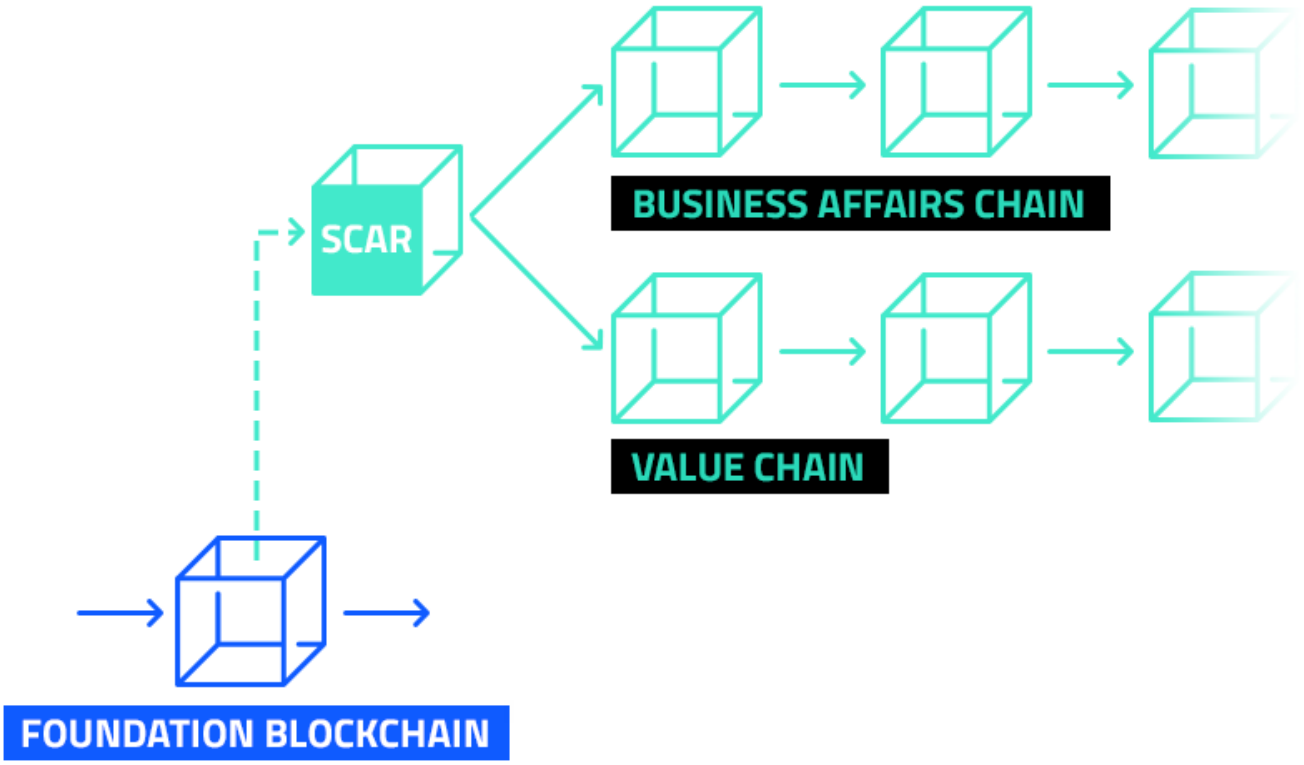

图12. 完整的辅助链双链结构

价值链记录价值交易，事务链记录业务逻辑和业务数据。这种双链机制使本系统可以在底层区块链与上层业务逻辑之间，构建通用的功能层，全方位支持各类具体商业应用需求。

本方案仅限于介绍价值链部分，事务链将及通用功能层另设方案处理。

原则上，辅助链采用基础区块链价值体系，即在辅助链上直接交易基础链货币。但为了使系统具有更广泛的灵活性以适应各种应用场景，本系统设计方案支持定制辅助链协议和共识机制，允许用户发行自己的独立货币。

2．3．2 辅助链的价值及信任机制维护

辅助链的信任机制源于基础区块链、过程中受基础区块链及其制订的规则制约、结果及最终裁决权归于基础区块链。

通俗地说，辅助链的身份及属性由主链确定，交易的有效性需经主链认可，数据存储按主链要求，最后结算由主链裁决。系统的设计原则是在满足此条件前提下运算尽量由辅链节点承担。

关于辅助区块链内的价值维护，要根据情况区别对待：

对于采用基础区块链价值体系的辅助链，其价值机制同样源于基础区块链、按照基础区块链协议、规范及共识机制运行、受基础区块链签署合约的约束、受基础区块链监督并最终接受基础区块链的裁决。

对于采用独立价值体系的辅助链，其价值非源于基础区块链，与辅助链外的交易也受到限制，仅能通过本地兑换方式进行，基础区块链不核查其共识机制，但基础区块链仍拥有监督权及最终裁决权，交易的验证规则仍由基础区块链通过合约制订。

2．3．3 辅助链的起始块

辅助链初始化时，向主链申请认证，生成该辅助链的ID、私/公钥对及属性合约，这些数据均存储在起始块中，系统以可选的方式支持KYC功能，可以确认辅助链拥有者身份(非必须)。

需要注意的是，辅助链ID与节点ID不同，一个节点可以运行多个辅助链，每个辅助链有自己独立的ID及钥匙对，而同一辅助链也可以运行于多个节点。

每条辅助链在初始化时，同时生成一个主链认证的唯一账户，作为主链与辅助链之间交易的代理，称为智能合约代理路由(Smart Contract Agent Route，简称SCAR)，SCAR为特殊账户，由主链智能合约控制，具有特殊性，任何人无法人为操作该账户，包括辅助链及节点的拥有者也无操纵权。该账户仅能由基础区块链执行其与辅助链之间对等账户的交易或依逻辑执行辅助链内部账户之间的交易。

同时，辅助链ID、公钥及属性参数存贮在KanBan辅助链列表中。

辅助链的起始块为基础链签发的授权块，包含辅助链的可验证ID，在基础链及KanBan中留有存根。

2．3．4 辅助链内核结构

辅助链的内核结构及大部份功能与基础区块链相同，许多模块甚至可以通用。

但共识机制及矿工软件不同，辅助链比基础区块链内核模块具有更多的选择性。

由于辅助链可以定制自己的货币体系，并且有交易包处理和发送开放存储架构数据功能，辅助链内核还有包处理模块、KanBan通讯及数据交换模块、数据外部存储管理模块等。

辅助链核心功能中一个非常重要的特殊模块为SCAR处理模块，以将所有的交易转换为与SCAR之间的交

易，并维护关联交易状态。

另外辅助存储模块需扩充开放存储架构(OSN)支持功能。

辅助链中，KanBan功能是可选的，仅当有下级子链时才需要。

具体结构如图所示：

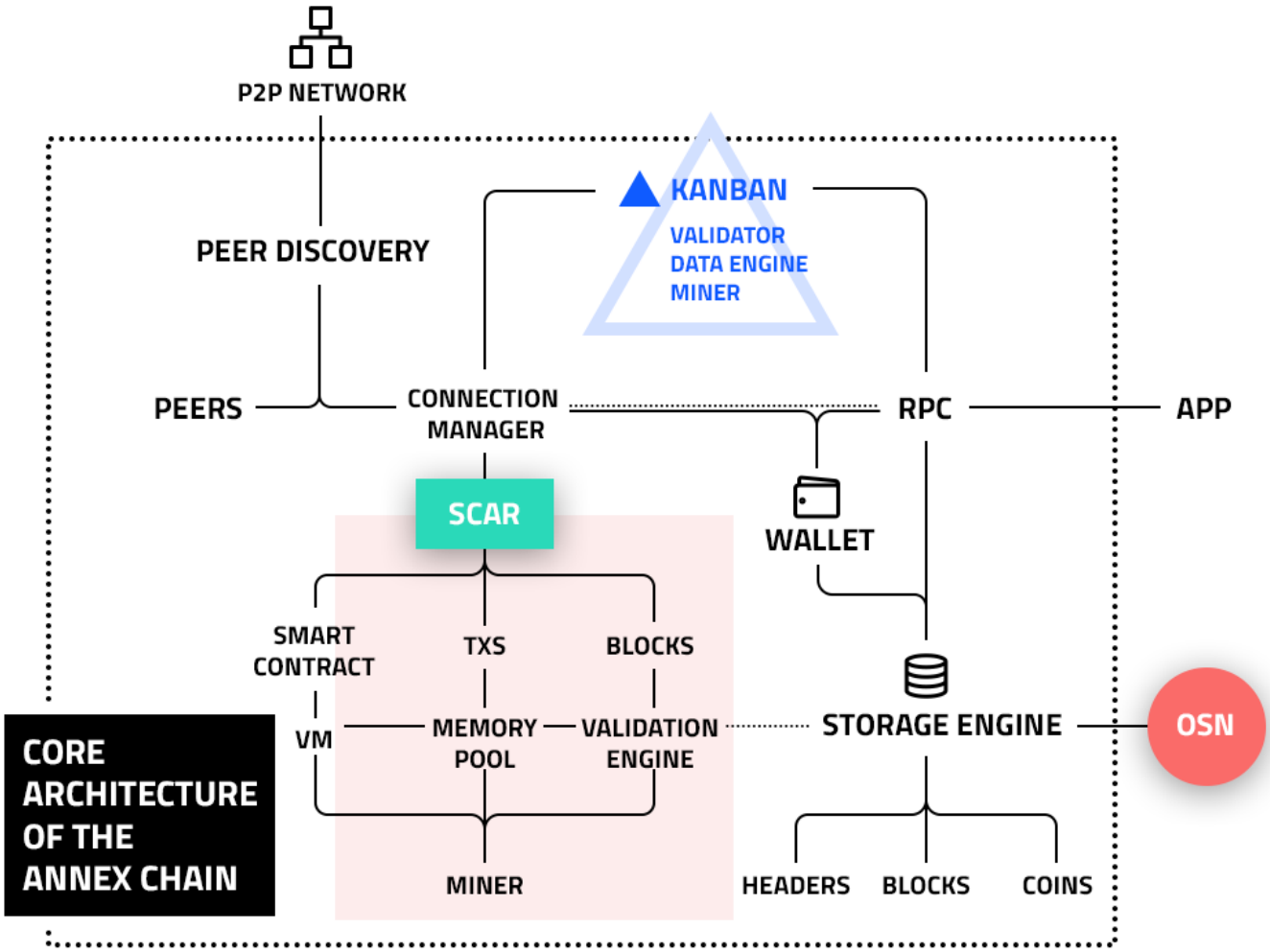

图13. 辅链内核架构

上图仅显示与价值相关的辅链架构，系统设计上，由于辅助链还支持事务链，实际还有更多模块，这里已经省略。

2．3．5 地址格式

本系统为地址设计制订一了套专门规则 – 跨链统一地址协议(Cross Chain Unified Address, 简称CCUA)，即地址专属规则，地址码段相同的地址属于同一拥有人，具体规则如下：

一个地址由四个码段组成，即： 地址类型码 – 链码 – 地址码 – 校验码

地址类型码为2个字节，目前0m为基础链PKH地址，1a为辅助链PKH地址；

链码为4字节，代表所在链的编号，基础链编号为0000;

目前仅假定地址码为PKH值，辅助链与基础区块链采用相同私钥及公钥，因而，对应地址相同；

校验码是对组合地址串二次Hash后取前4个字节。

任何两个地址码段相同的账户均属于同一拥有人，无论在哪个链上，如：

0m 0000 aaabbbccc123 y4sg

1a 0a4u aaabbbccc123 g8rj

这两个账户，一个位于基础区块链，一个位于链码为0a4u的辅助链，由于地址码段相同，这两个地址属于同一个拥有者。

辅助链与基础链之间仅限同一拥有者在相同地址码的地址间交易。

当一个辅助链用户向基础区块链提交清算时，必须转到相对应的地址。

一个地址在辅助链上为交易状态型地址，即每次交易不会改变地址，而只是更新余额。

跨链统一地址协议CCUA为实施交易验证及简化辅链交易的管理提供了方便的手段，事实上，跨链统一地址协议不限于本系统，完全可以作为唯一跨链统一地址协议，适应于所有的区块链，可以为实施通用去中心化的交易管理，提供非常方便的手段。

2．3．6 SCAR账户及交易方式

每个辅助链均有一个特殊账户，称为智能合约代理路由账户Smart Contract Agent Route，简称SCAR，该账户的支配权仅限于基础区块链授权的智能合约，用于执行基础链与辅助链对应账户之间的交易，该路由

中的智能合约亦由主链确立及控制。

SCAR是辅助链交易枢纽，辅助链上账户间的一切交易均转化为辅助链账户与SCAR之间的交易，所有辅助链与主链及其它辅助链之间的交易也均通过SCAR账户执行，这样，就使辅助链上的所有交易流线化，目的是当用户向基础区块链申请清算时，减少基础链交易数据，且无需交易对方同意即可执行，而SCAR也为基础链防范辅助链欺诈提供了可能措施。

这种方式看似中心化，但交易是由去中心化的KanBan验证且数据由去中心化的开放存储节点保存的，辅助链本身不具有裁决权，也不存在数据的独占权，所以也完全是去中心化的。

辅助链的SCAR账户私钥由主链智能合约控制。

辅助链上的任何交易均由智能合约及SCAR进行合法性检查。

辅助链上任何两账户间的交易均被流线化为用户与SCAR之间的交易。

辅助链上账户A与账户B之间交易：A → B 转换为 A → SCAR 和 SCAR → B

辅助链账户A与主链账户X音交易：A → X 转换为 A → X1, X1 → SCAR 和 SCAR → X

主链账户X与辅助链账户A间交易：X → A 转换为 X → SCAR， SCAR → X1 和 X1 → A

不同辅助链用户AB间交易：A → B 转换为A → SCAR1， SCAR1 → SCAR2 和 SCAR2 → B

KanBan始终保持每个辅助链SCAR的总状态，并可通过对辅助链UTXO集合清查核算。

2．3．7 辅助链交易状态

系统为辅助链有效交易制定4种状态，即：已执行、已见证、已确认、已完成，分别代表四种不种的交易过程。

辅助链收到交易后，立即本地执行，生成交易，为交易已执行状态，通常在以毫秒为单位的时间内完成，这只是辅助链内部的交易，如果辅助链为单个全节点链，则等同于目前的中心化交易，此状态下交易的可信任性等同于辅链的可信任性；

辅助链将交易打包提交到KanBan, 并收到KanBan确认，为已见证状态，通常在数秒至数分钟内完成。提交到KanBan，则交易状态由KanBan维护，可信任性大幅提升。但由于提交到KanBan是辅助链单向自主提交

的，并非由主链P2P网络传播，因而，KanBan确认为数值型参数，代表确认KanBan数量，数字越高，越可靠；

辅助链生成块，并经KanBan签证且传送到开放存储节点保存，称为已确认，通常在数分钟内完成，提交到开放存储架构表示数据存储去中心化完成，交易已经非常可信任，与KanBan类似，所提交的开放存储架构(OSN)节点数越多，可信任性越高；

当用户向基础区块链提交清算，并完成，为已完成状态，取决于用户何时提交。这种情况下，与账户相关的交易已经提交到主区块链。具有最高信任等级。

通常已见证状态的交易基本为无风险交易，一般的小额交易均可视为可靠；而已确认状态的交易则具有足够的安全保证，较大额度的交易也可放心。

由于已见证状态的可信用性由KanBan数量决定，已确认状态的可信任性由提交到的存储节点数量决定，系统提供专门接口，通过智能合约，为客户端提供简易的判定手段。

2．3．8 辅助链交易处理流程

辅助链价值交易处理流程是：

图14.
辅助链价值交易处理流程

辅助的交易需要经KanBan核实的，这是防止双花攻击的必要条件，只有通过KanBan验证并收到KanBan签收存根的交易才有效。

主链收到辅链提交的数据包后，对包进行验证，首先验明正身，然后验证数据包的有效性，最后核实数据包中记录有效性，如有问题拒收并通知辅链，如通过验证，则更改KanBan相关记录状态，并将交易放入未清算交易表，并签收，将收据发给辅助链；

当从主链KanBan收到否决后，辅助链应将可疑交易剔除，重新打包提交。

辅助链及KanBan包数据及交易记录的保存应具有完全相同的顺序和时间记录，每次发送包里，均包含上一数据包的Hash值。这样可以使数据传输最少化，所有节点通过PoS生成块时，仅需知会各方最后一个包的Hash值即可。

一般情况下，基础链KanBan收到辅助链的数据包，包含一条或以上交易；

辅助链在收到KanBan节点验证后该交易全局有效，一个辅助链交易收到的KanBan节点确认越多，可信性越高。

辅助链中的交易是由辅助链打包后自主向KanBan节点发送的，KanBan节点间不再自动进行P2P节点间传播。

2．3．9 辅助链的块处理流程

辅助链中，块采用由辅助链节点、KanBan、开放存储节点参与的POS共识机制产生的，并可通过KanBan或存储框架进行验证。

客户端确认块有效的条件是：块通过有效性验证、该块或其下游块经KanBan签收、块数据在开放存储节点保存。

辅助链中的交易是由辅助链打包向KanBan节点发送的，KanBan节点间不再自动广播。

当一个辅助链的块根据其共识机制产生后，将被在辅助链p2p网络的节点之间传播，传输的数据包括nonce，最后一个数据包id和新块中的merkle root，p2p网络涉及的节点包括该辅助链的所有全 节点、参与KanBan及参与OSN节点。

辅助链中块锁定后，向开放存储节点广播块数据。

2．3．10 辅助链双花攻击防范

本系统设计方案可以有效杜绝辅助链双花攻击。

首先，在辅助链诚实的情况下，链内攻击无法实施，同一辅助链上每个账户的状态均可以从本地实时获取，不存在链内攻击漏洞；

如果辅助链专为欺诈而设，客户端通过向KanBan及开放存储节点验证交易有效性。KanBan及开放存储架构的验证机制可以判定是客户端欺诈还是辅助链欺诈，若为客户端欺诈，交易无效，若为辅助链欺诈，向基础区块链申请执行禁止智能合约，冻结该辅助链特殊账户SCAR交易，并启动清查程序，查验该辅助链所有未清算交易详情；

对于辅助链与基础链间的双花攻击，由于系统限定了在基础链与辅助间只能进行同属账户间交易，因而只要杜绝辅助链上的双花攻击，就无法实施辅助链与基础链间的双花攻击。

跨辅助链双花攻击，是指在两个或多个不同辅助链之间实施的双花攻击，有几种情况需要考虑：

a)　所有涉及的辅助链均诚实，仅账户节点实施的攻击:

这种情况下，交易无法通过KanBan及存储系统验证，辅助链全节点及客户端均可及时获取交易状态，交易失败；

b)　部份参与交易的辅助链不诚实的双花攻击:

客户端可以通过KanBan及存储系统验证交易的有效性，而不能仅通过辅助链节点验证。如认为欺诈，客户端也可向基础链通报，由基础链执行验证和禁止；

c)　参与交易的两条辅助链均不诚实的双花攻击:

客户端可通过KanBan及开放存储架构进行验证。事实上，由于SCAR及SCAR通道的设立，交易跨越的辅助链越多，漏洞越多，欺诈越难实施。

由此可以看出，KanBan及开放存储架构在防止双花攻击中起至关重要的作用。

另外KanBan中的辅助链列表，记录辅助链的起始时间及交易总量，可以作为辅助链的信用参数供客户端参考。

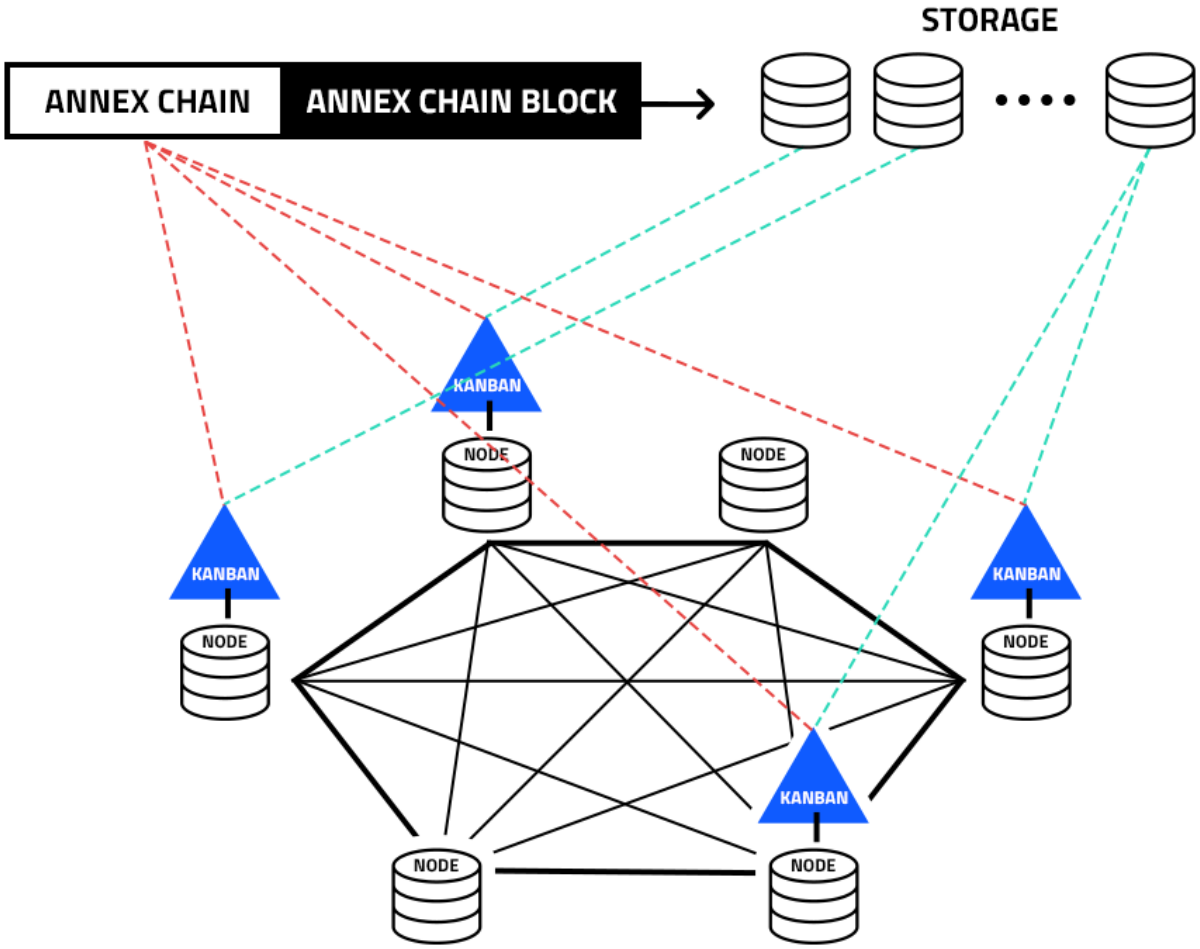

图15. 整个系统的验证关系图

2．3．11 辅助链账户清算

辅助链的价值交易具有全局有效性，这是通过KanBan功能及去中心化的存储架构实施的，即辅助链的账户状态始终与KanBan同步，而包含交易记录的块被提交到KanBan指定的存储节点存储。

当辅助链客户向基础区块链提交账户清算时，即使所在的辅助链消失，也可使清算得到顺利执行，因为KanBan及存储系统保存完整的交易数据及状态信息，而由于SCAR机制的设立，任何辅助链交易均转化为用户与SCAR之间的交易，而SCAR是由基础区块链控制的，所以无需其它交易方的同意即可执行清算。

清算完成后，辅助链上对应地址清空，KanBan中对应的记录也删除。

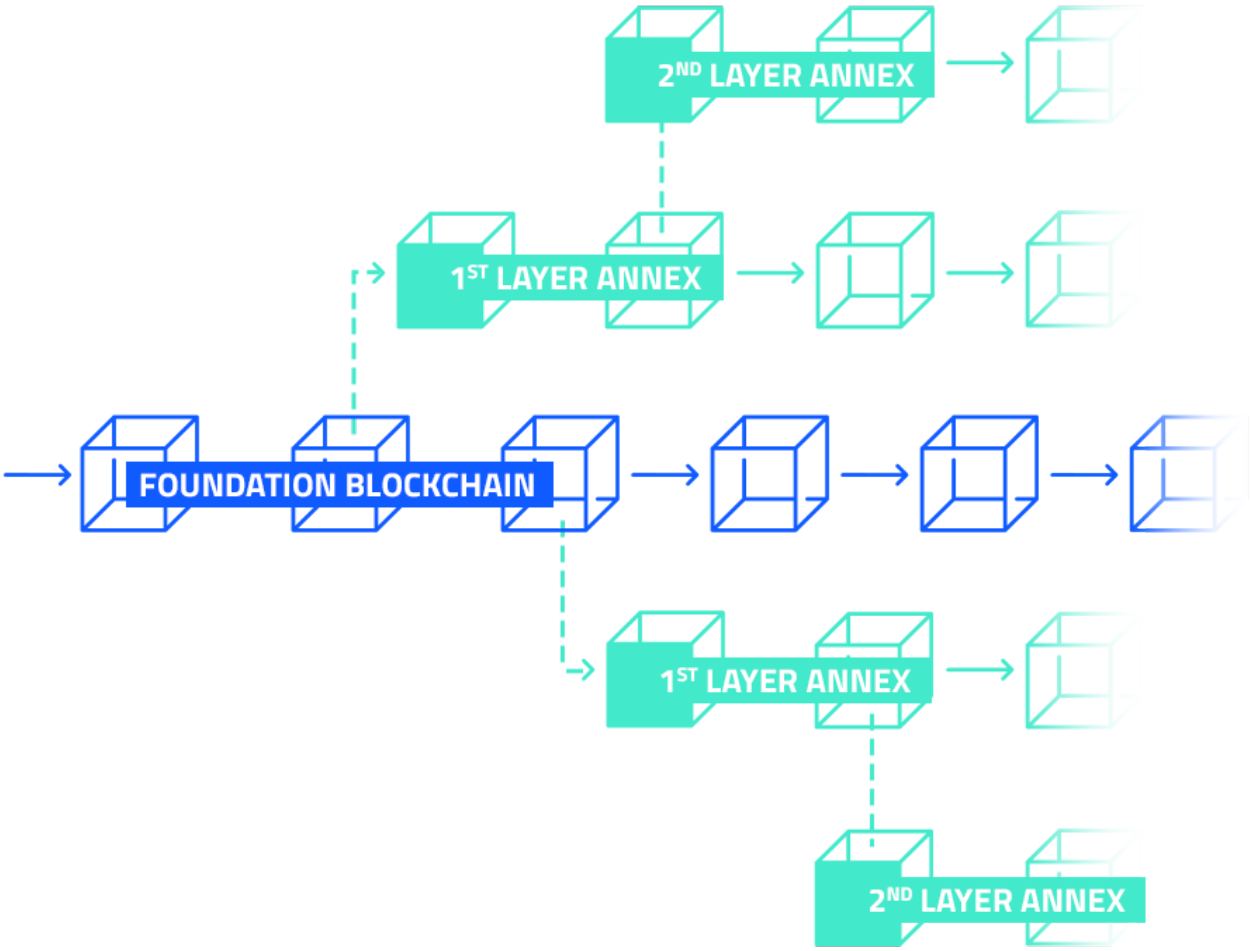

图16. 分层辅助链结构图

2．3．12 辅助链分层架构

辅助链在系统设计原理上并不限于一层，而是可以建立多层次链。如下图所示：

所谓的多层辅链结构，就是从辅助链上再衍生出下一级辅助链，上一层链称为父链，衍生出的链称为子链。

在分层辅助链系统中，子链的KanBan由父链节点维护，因此，辅助链核心也具有KanBan模块，在必要时配置激活。

由于本系统跨链统一地址规范中区块链编码部分四个字节中第一个字节用于表达深度，其余三个字节作为链编号，因而整个系统最多可以有256级辅助链，每级最多可以有16,777,216个辅助链。

2．3．13 辅助链价值体系与共识机制

通常情况下，辅助链采用基础区块链同一价值体系，即在辅助链直接执行基础链货币交易，其条件是，该辅助上级所有链均采用基础链价值体系。

本系统支持辅助链用户自定义价值体系与共识机制，其目的是增强系统灵活性与适应性。基于业务需要的理由，一个辅助链可以发行自己的币，维护自己独立的价值体系。

父链KanBan仍然维护子链交易状态，如果子链与主父链为同一价值体系，子链与父链间可以自由交易，如果子链与父链间为不同价值体系，则只能通过兑换机制同级交易实现价值转换。

2．4 开放存储架构

快捷区块链系统的开放存储架构是系统的三大组成部份之一，开放存储机制对构建去中心化的商业应用具有非常重要意义。

2．4．1 开放存储架构设计

开放存储架构全面支持快捷商用区块链的价值交易及事务交易记录的存储，并利用MapReduce技术构造映射精简函数模型，以支持大数据快速查询。

开放存储架构不仅支持面向区块链交易的快速查询，也支持对事务区块链相关的基于内容的开放商业信息快速查询，在服务于本系统的同时，为建立区块链时代的搜索引擎打下基础。

系统设计以利益激励机制吸引服务提供者主动加入，主要有三个方面: 一是系统支付存储费用收益；二是支持通过MapReduce函数，参与辅助链的POS共识机制决策，获取挖矿收益；三是公共开放商业数据，是区块链时代搜索引擎的基础。

为了支持大数据并发，系统架构设计方案为在数据库口层采用Sharding技术，支持数据库的水平扩展。

存储系统总体逻辑架构如下:

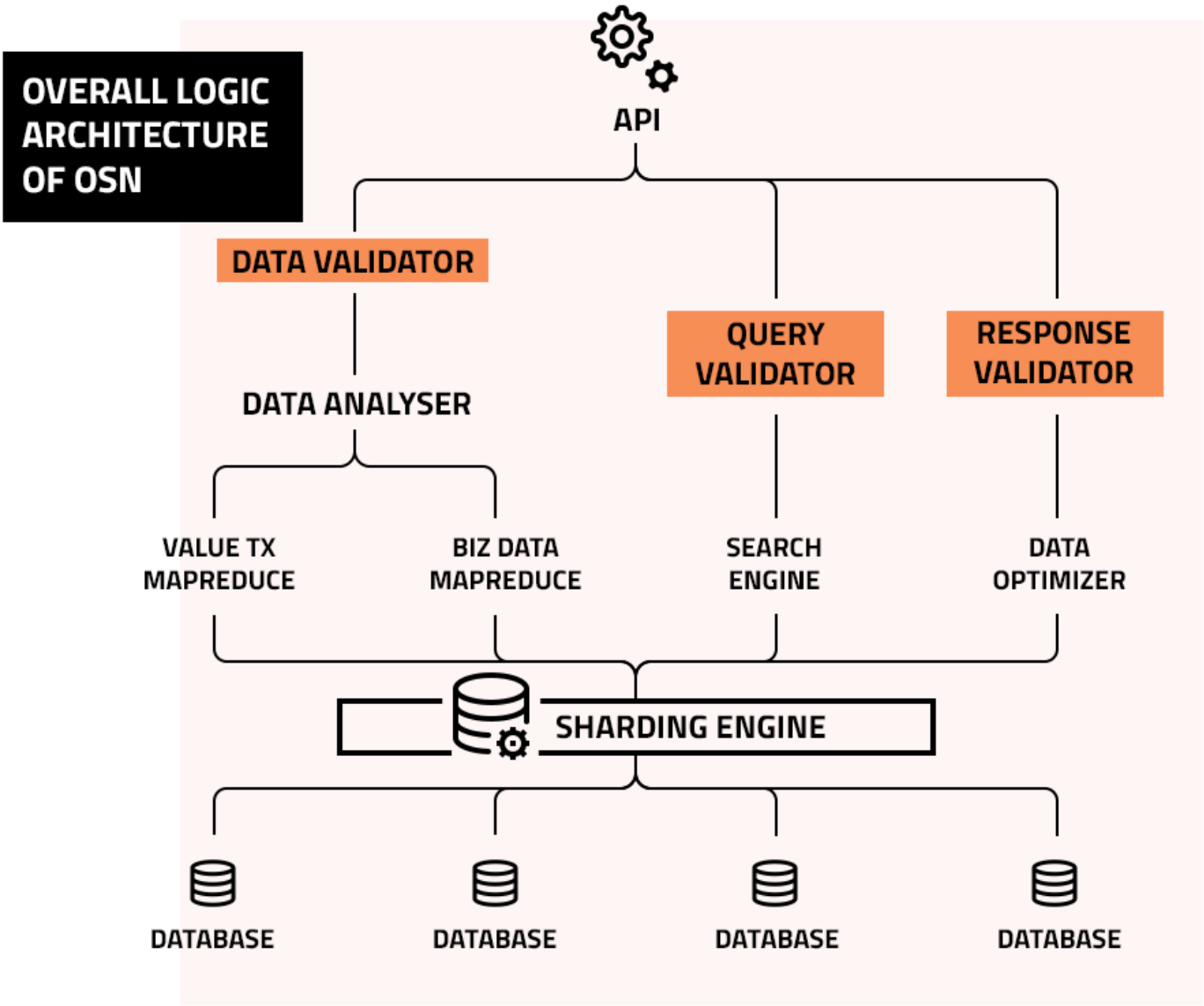

图17. 存储系统总体逻辑架构

整个存储系统的设计与公共区块链系统一样，采用开放的架构，服务提供商及用户均可自由加入。

2．4．2 存储节点的内核架构

开放存储架构的节点除具有数据存储架构外，还具有与区块链系统兼容P2P协议及联接管理与通讯接口，可以方便地加入区块链网络。

存储节点也是通过P2P网络参与各辅助链共识机制的。

一个开放存储节点可能与多个辅助链相联，为多个辅助链提供数据存储服务并参与多个链的共识机制。

存储节点架构图如下：

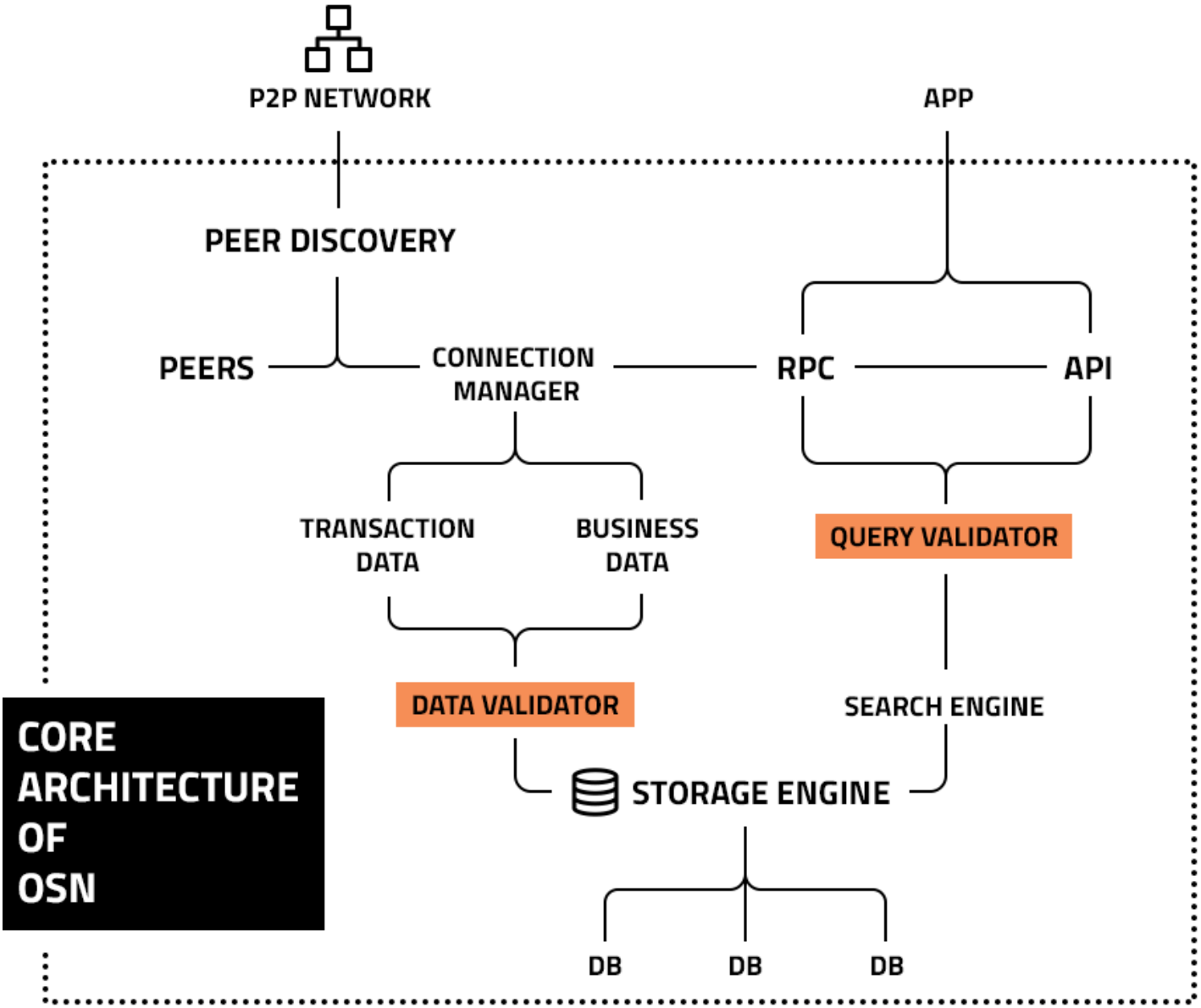

图18. 开放存储节点内核架构

2．4．3 存储节点的费用激励机制

存贮节点的费用机制由基础区块链智能合约制订，原则上，存储节点可以自由制订存储费用，但费用作为参数加入POS共识机制规则的确定，费用越高，POS的投票权越低，投票权的计算公式为：

$$W = V / R$$

其中： W － 投票权重；

V – 投票权值；

R – 存储 费率。

存储节点的直接收入包括存储费用及POS采矿收入，潜在的收入包括数据搜索服务。

3. 价值体系

快捷商用区块链体系采用统一基础货币体系 - 发币(FAB Coin)，是英文Fast Access Blockchain的缩写。发币作为本系统的价值基础，通行于系统三大组成部份的所有环节，是一切费用与价值交换的标准价值单位。

发币采用定量制，固定2亿枚，其中8百万枚保留供开发及推广激励，2千4百万枚通过ICO方式发行，其余1亿6千8百万枚通过挖矿产生，发币的采矿机制与比特币相同，

参考文献

1. A method of validating external data block by Bitcoin transaction to construct new blockchain, Paul Liu

2. Using Smart Contract Account Routing (SCAR) to Streamline Transactions, Paul Liu

3. A method of constructing scalable blockchain by using KanBan to update off-chain state, Paul Liu

4. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto

5. The Business Blockchain - promise, practice and application of the next internet technology, William Mougayar

6. Omni Layer Specification, https://github.com/OmniLayer/spec

7. Enabling Blockchain Innovations with Pegged Sidechains, Adam Back et al

8. Blockchain - Blueprint for a new economy, Melanie Swan

9. Mastering Bitcoin, Andreas M. Antonopoulos, O'REILLAY, First Edition, December 2014