Fn-Fn 区块系统技术白皮书

Fission and fusion network

版本 0.3

Fission and fusion fund limits

目录

一. 系统描述.....3
二.系统参数.....5
三.树状区块结构.....5
四.安全主链.....7
五.业务分支.....7
六.用户密钥与地址.....8
1. 密钥和公钥地址.....8
2. 模板地址.....9
3. 带参数模板.....9
七.区块与交易.....10
1. 区块结构.....10
2. 交易结构.....10
八.跨分支交易.....11
九.共识机制.....12
1. DPOS 节点协商过程.....12
2. 打包出块权权分配.....14
十.IOT 数据业务模型.....14

一. 系统描述

Fission and fusion network（后简称”Fn-Fn“）是构建于 P2P 网络的区块系统，同目前流行的 P2P 虚拟货币系统类似，以去中心化方式维护透明账本，实现用户虚拟资产自主安全管理和高效流动。Fn-Fn 系统针对 IOT 数据业务需求设计，利用区块技术为 IOT 数据业务提供去中心化安全管理平台，实现 IOT 系统所需高并发低延迟等性能要求。

和以往区块系统类似，Fn-Fn 通过安全共识组织用户交易（transaction），按时间顺序形成数据区块。同 Bitcoin 等单链系统不同，Fn-Fn 采用树结构来存储排列区块，可以根据业务类型和数据负载进行分叉形成多个分支。分支之间区块相互独立，新增区块只与自身分支数据相关。在多重分支的情况下，根据业务数据流量，可以分布到多个分支区块中，由此产生的可扩展性和高并发性正是 IOT 系统所需的基本性能。

Fn-Fn 的多重分支结构由唯一安全主链分支和众多业务分支构成，主链分支用于支撑全网共识机制，业务分支用于实际业务。在业务分支可以提供最低 2 秒的低延迟交易确认，用户可以指定交易紧迫性，支付相应交易手续费，以此实现低延迟业务。

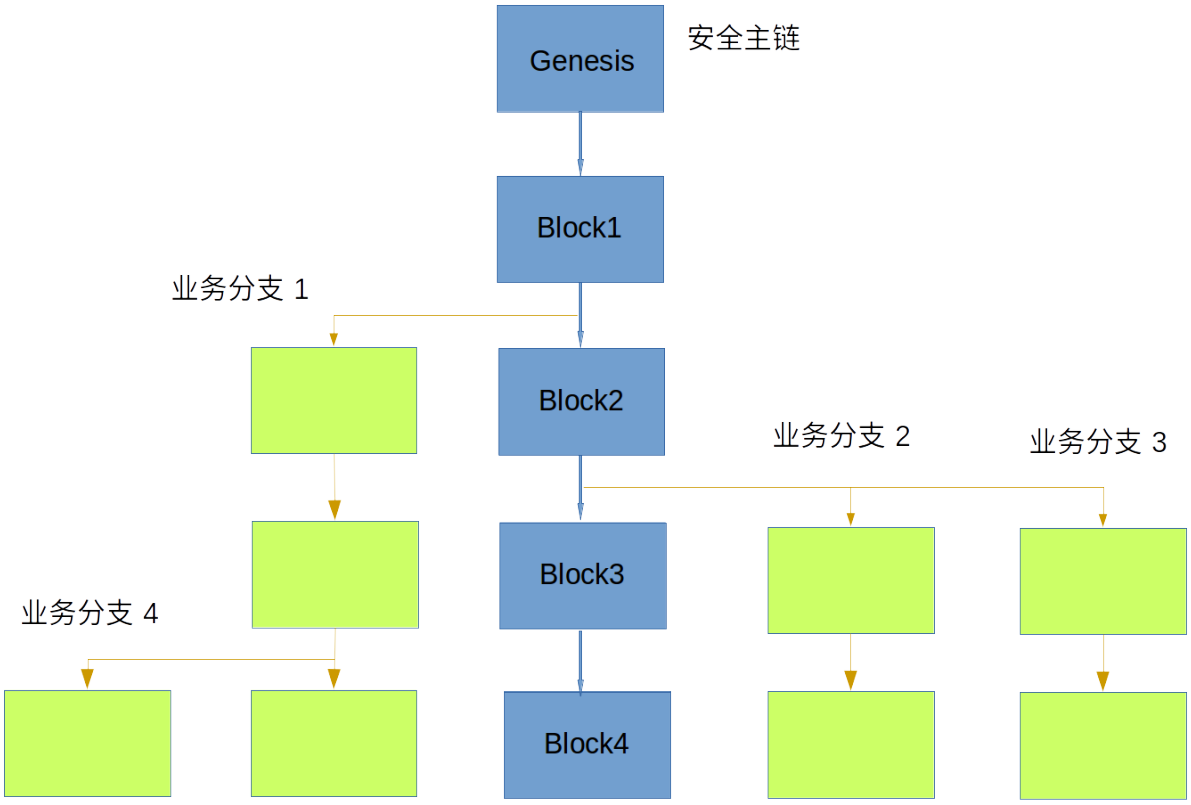


图 1.1 Fn-Fn 多重分支结构

Fn-Fn 网络由运行 Fn-Fn 软件的节点构成 P2P 网络。为了支撑庞大的 IOT 业务，Fn-Fn 核心网络由主干网和终端服务网构成。主干网节点进行共识组织区块数据；终端服务网形成分布式终端后台，同步校验区块和交易数据，并为 IOT 终端提供接口；IOT 终端包括智能传感器、控制器和移动终端，内嵌轻客户端程序，本地保存私钥完成交易构建和校验。

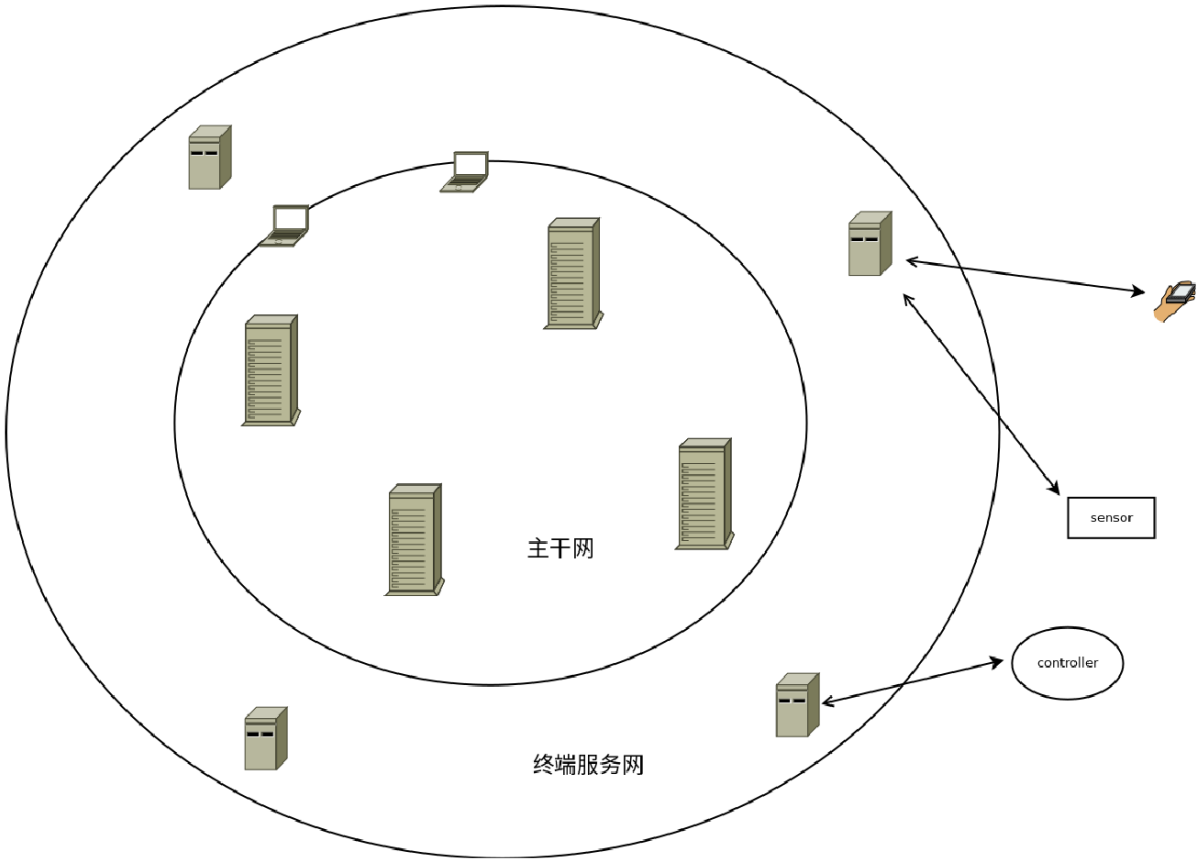


图 1.2 Fn-Fn 物理网络结构

Fn-Fn 系统软件包括核心钱包程序、轻钱包后台服务系统、移动端轻钱包程序、嵌入式系统轻钱包 SDK 和在线区块浏览器几部分。核心钱包程序用于主干网络节点和普通用户，对运行环境和硬件有一定要求，可以完整使用区块系统所有功能模块； 轻钱包后台服务系统用于终端服务网络后台服务器，为轻钱包终端提供必要的接入服务； 移动端轻钱包程序用于 IOS 和 Android 移动终端，在网络带宽和硬件性能都有较大限制的情况下，为用户提供安全钱包服务；嵌入式系统轻钱包 SDK 为 IOT 智能硬件提供轻钱包 API，可以通过终端服务器接入 Fn-Fn 网络，不需要在本地进行繁重的区块同步和区块数据存储，专注与业务相关的交易数据构造和鉴权；在线区块浏览器配合钱包节点实时展现区块系统状态，查询历史区块交易数据。

Fn-Fn 的安全共识机制为 DPOS+POW，节点收益为出块奖励息加上块内交易总交易费。用户可以用 token 为 DPOS 节点进行投票，投票为 DPOS 节点增加出块概率。当 DPOS 节点成功产生新区块，

对应投票用户也按投票额度分享出块奖励。节点需要筹集超过 token 供应总数 2%投票才能成为 DPOS 节点。POW 作为 DPOS 共识的补充，每轮 DPOS 协商过程有一定概率将首要出块权交给 POW 共识。参与 DPOS 过程的 token 越少，说明 DPOS 共识的安全性和可靠性越低，这种情况下，通过 POW 共识获取出块权概率越高，混合 POW 机制增强系统安全性和可靠性。

Fn-Fn 的树状结构中，除了一条分支外，其余分支地位对等且相互独立。这条特殊分支被称为安全主链，DPOS 节点群通过安全计算共同建立出块序列，同时产生真随机数信标。业务分支出块系列分配由安全主链的随机数信标计算产生。

根据 BA 原理，恶意节点少于 1/3 整个安全计算过程就不会被干扰；合理选择协商算法和参数，可以实现非 51%攻击情况下，安全计算过程就不会被控制。在 Fn-Fn 系统中，共识机制可以达到有较高的一致性，系统性分叉非常罕见，在恶意节点所持 token 少于参与 DPOS 总数 50%情况下，3 个确认可保证主链历史数据不可回滚。

二.系统参数

Fn-Fn 系统中业务分支的区块产生间隔需要和安全主链一致，其它主要参数可以在创建分支初始化过程中由创建者配置，可配置参数包括 token 总量和分布、出块奖励和增发方式等。

安全主链系统参数如下表所示：

初始 token 总量	745000000
token 年膨胀率	1%
区块产生间隔	60 秒
区块最大字节数	2MB
初始出块奖励	15
最大 TPS	156
DPOS 节点最大数量	50
POW 难度调整周期	1 同算法 POW 区块

三.树状区块结构

Fn-Fn 系统的区块按时间顺序连接在一起，多分支形成树状结构。分叉点后第一个区块的 hash 作为子分支 ID 被用于标识不同分支。

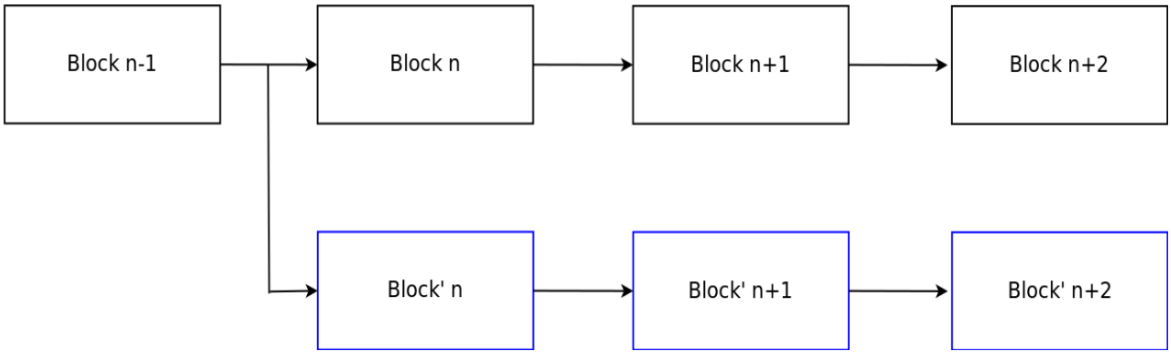


图 3.1 Fn-Fn 多重分支标识

如图 3.1，子分支 ID=HASH(Block'n)

在分叉之前，父分支和子分支拥有完全一致的链结构和交易；分叉点之后则相互独立，互不干扰。出现在分叉点前的同一笔 token 在父子分支中可以创建不同的交易发送到不同的地址；也可以通过相同交易发送到同一地址，只要该交易出现每个分支的区块中。用户在创建交易的时候需要指定一个锚定区块，标定在此区块之后的所有分支有效。在上图中，如果锚定区块设定为 Block n-1，创建的交易会被包含到两个分支中；如果设定为 Blockn，则该交易只在父分支有效，子分支中可以创建新交易将 token 发送其它地址。

通过在父分支发送一个分叉交易，抵押一定额度父分支 token，用户可以自由创建子分支。

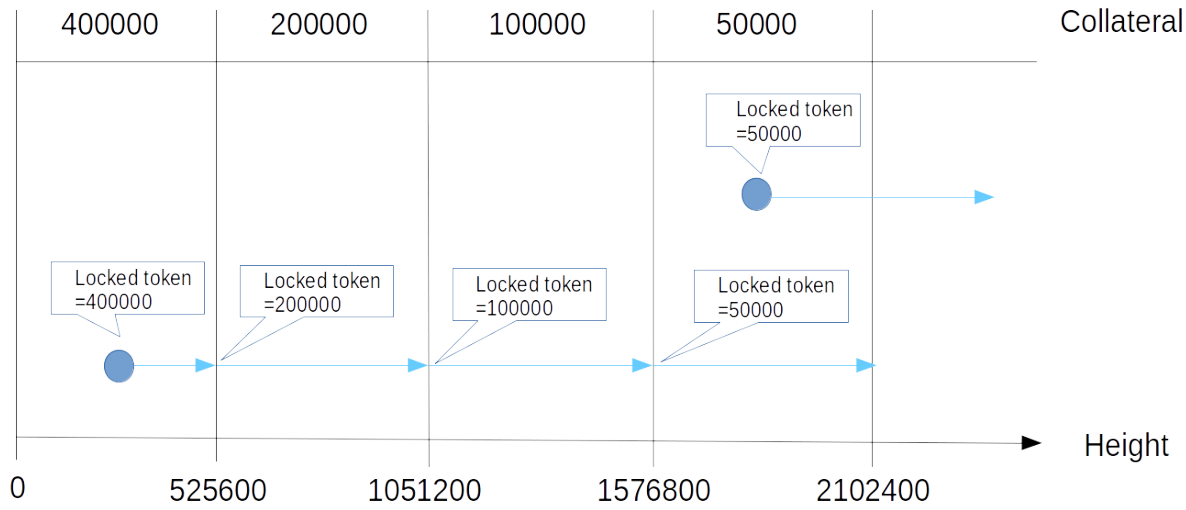


图 3.2 创建分支 token 抵押解冻

创建分支需要使用父分支 token 进行抵押，分叉交易中用于抵押的 token 被发送到一个特殊地址进行冻结。抵押 token 根据父分支区块高度分阶段解冻，创建者使用自己私钥进行签名后可以将解冻部分 token 转移到其它地址。创建分支所需抵押 token 随区块高度递减，每隔 525600 区块完成一次减半。

分叉交易中包含了子分支分叉高度和第一个区块数据，指定子分支 token 分布，可以继承分叉点父分支 token 分布也可以定义全新 token 分布，或者在父分支基础上进行增发。自分叉点之后，子分支 token 和父分支是完全隔离的。

四.安全主链

安全主链除了记录主链 token 转移，还保留 DPOS 节点协商关键过程数据。安全主链的区块之间不能插入子块，只能按照既定出块间隔增长。由于会有相当部分容量记录共识协商过程数据（50 个 DPOS 节点数据每区块～200KB），安全主链的交易容量低于业务分支。

安全主链以区块系统创世纪块为起点，通过 DPOS+POW 共识顺序产生区块。安全主链被用于支撑全区块系统的安全和共识，所有业务分支用户都需要同步和校验主链区块头信息，在 P2P 网络中主链的同步广播消息转发优先级高于业务分支。新节点接入网络后，首先完成主链同步，才开始进行对应业务分支同步。

鉴于功能特殊性，有三类与共识机制相关交易是安全主链独有的：1)DPOS 节点投票交易；2)DPOS 节点登记交易；3) POW 出块奖励交易。

DPOS 节点投票交易：

DPOS 节点产生一个 Delegate 模板地址，首次需要自己发送 token 到该地址，完成 Delegate 地址链上发布；用户创建投票地址将 token 寄存于 Delegate 地址，完成 token 投票，并锁定 10080 区块。DPOS 节点可以使用 Delegate 地址的投票作为权重参与 DPOS 协商过程。

DPOS 节点登记交易：

DPOS 节点在每轮协商需要筹集足够 token 投票，并以此创建登记交易提前在链上进行登记和发布自己初始协商参数，只有协商轮次开始前完成登记的节点才允许进入协商过程以及获取出块权。

POW 出块奖励交易：

POW 共识缺省情况下只用于主链共识出块，对应出块奖励通过这类交易提供给参与者。作用和类似 Bitcoin 中 coinbase 交易。

五.业务分支

业务分支有通过在父分支发送分叉交易创建，分支的第一个区块（分支创世纪块）被保存在分叉交易。子分支的 token 分布可由创建者定义，有三种方式：1）创建独立分支，分支创世纪块重新设置 token 总数和分配方式；2）完整继承分叉点 token 分布；3)继承分叉点 token 分布，并在此基础上进行增发，增发部分的分布方式在分支创世纪块中定义。

业务分支安全性依赖于安全主链的共识机制，可以不设立出块节点，由 DPOS 节点在获得主链出块权同时为分支产生新区块；也可以借用安全主链产生的随机信标设立本分支的出块机制。这两种应用分别对应公开和封闭业务模型。

业务分支和安全主链相比，在正常每分钟出块间隔中，可以产生子块，用于打包低延迟交易。子块间隔不低于 2 秒，且不可以产生空块。产生子块的节点由安全主链同高度区块块独立随机信标决定，子块没有额外出块奖励，但可以获取高额交易费收益。

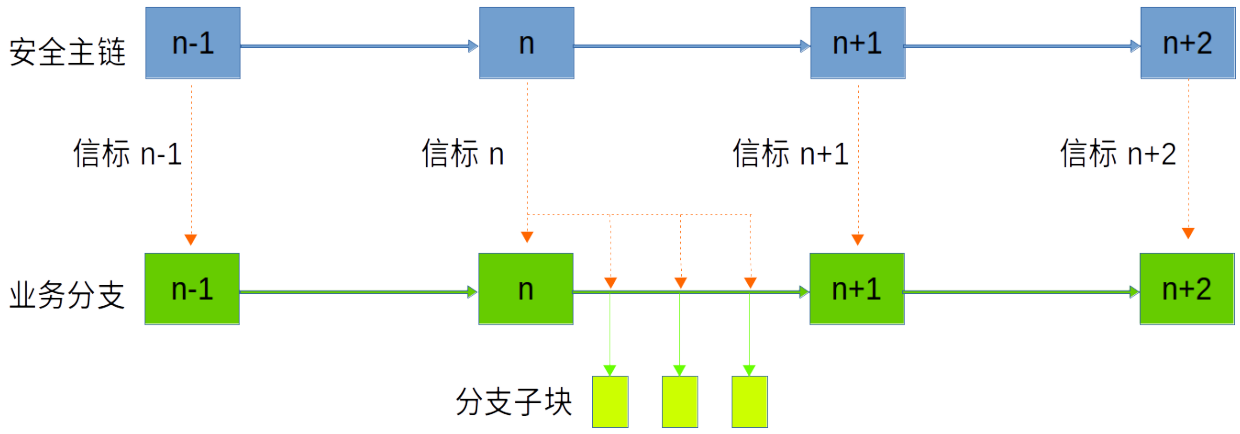


图 5.1 业务分支区块/子区块产生过程

考虑业务分支中的子块，每个业务分支的交易容量可以提高 30 倍，TPS 可达到 5200。当数据业务需要更高交易容量和并发性时，可以对针对当前业务分支创建多个分支，以此实现高量级 TPS。

六.用户密钥与地址

1. 密钥和公钥地址

Fn-Fn 系统采用 curve25519 作为基本安全算法，用户私钥和公钥均为 32 字节，私钥签名为 64 字节。curve25519 安全性和 P256 相同，同安全性算法中是目前效率最高的非对称安全算法。以类型前缀＋公钥作为钱包公钥地址。

例:

secret key :

8fca989d6eb659f87ab53c0527e3d1be4b6017a79a5a3740feef0312e1c804a9

public key:

a1184b98307b5a2483d2b12adf73eef4d9003953518bab8825dbb4d26f8e1c3c

address:

01a1184b98307b5a2483d2b12adf73eef4d9003953518bab8825dbb4d26f8e1c3c

为了保证用户私钥安全，在本地存储采用 chacha20+poly1305 算法加密，需要用户输入密码才可以恢复可用密钥。

2. 模板地址

模板地址由类型前缀+模板 ID 构成。模板 ID 由 2 字节模板类型+参数 Hash 低位 30 字节构成。例如一个 3-5 多重签名模板，参与五个公钥分别为：

fcd74aa82a1eb098830a2fcc877735a60152b441c16b2212157c4215db074e88

f1a1ced60a7ecdf83735a3380765f2ef77221f367da05bd901e885b9d799aec5

c2885254a2acefaeb05bd94b0e73e483bded994b02ebd0bc6b3523c2dde558dd

e2de897ad0935bbfd6cca48da2ee285c87ae784285df35513180143ec55c8450

b1f1ce918f30b46aa3d2648810f6153410e44122c042998699323b982664a16f

tempate ID:

000244c03d536e6175912b3040aa876388b197c21ae55c283f182403ab610852

address:

02000244c03d536e6175912b3040aa876388b197c21ae55c283f182403ab610852

3. 带参数模板

时下流行的区块系统都提供运行于不同 VM 之上的脚本或智能合约，对区块系统基本账本进行强大灵活的功能扩展。尽管发展数年，在区块系统中的 VM 模块目前还处于起步阶段。除了存在内在安全漏洞等问题外，运行效率和使用费率也在一定程度上限制了智能合约适用范围。Fn-Fn 系统不提供脚本和智能合约系统，而是采用带参数过程模板实现常用的脚本和智能合约功能。采用对应模板地址为用户提供功能调用。

Fn-Fn 系统提供以下模板

类型标识	*名称*	*参数*	*描述*
0x0001	带权重多重签名模板	签名所需权重，公钥和对应权重列表	可分别配置参与公钥签名权重，分配不同权限，公钥数不大于 16
0x0002	简单多重签名模板	签名所需数量，公钥列表	参与公钥签名等权重，公钥数不大于 16
0x0003	创建子分支模板	分支创世纪块 hash，创建者解冻抵押 token 地址	创建者可从模板地址取回解冻 token
0x0004	工作量证明共识模板	区块签名公钥，出块收益接收地址	采用出块签名公钥和花费地址分离机制，支持安全冷钱包挖矿
0x0005	DPOS 代理节点模板	区块签名公钥，节点所有者地址	采用出块签名公钥和花费地址分离机制，支持安全冷钱包 DPOS 过程

类型标识	*名称*	*参数*	*描述*
0x0006	跨分支交易模板	交易双方地址	用于进行跨链交易进行身份识别和条件判断
0x0007	订单交易模板	采购方的公钥和出售方公钥	用于支持数据交易中的订单交易

七.区块与交易

1. 区块结构

Fn-Fn 区块包括以下数据：

名称	*数据类型*	*描述*
nVersion	uint16	版本号
nType	uint16	类型，区分创世纪块、主链区块、业务区块和业务子区块
nTimeStamp	uint32	时间戳
hashPrev	uint256	前一区块 hash
txMint	CTransaction	出块奖励交易
vchProof	vector<uint8>	用于校验共识合法性数据
vTxHash	vector<uint256>	当前区块包含交易 ID 列表
vchSig	vector<uint8>	区块签名

目前区块版本为 0x0001。时间戳采用 UTC 以秒为单位。vchProof 包括了合法性证明系列化数据，在安全主链中，包括 DPOS 节点广播的计算结果（包括各节点签名），POW 区块中还包括工作量证明参数；在业务分支中，包含同高度主链区块 hash 和共识计算结果。区块在网络传输过程中只包含交易的 ID 列表，减少重复传输交易数据造成的网络带宽浪费。区块签名 vchSig 使用 txMint 输出地址进行签名，签名数据段包含除 vchSig 以外所有字段。

2. 交易结构

Fn-Fn 采用 UTXO 模型记录交易，包括以下数据：

名称	*数据类型*	*描述*
nVersion	uint16	版本号

nType	uint16	类型,区分公钥地址交易、模板地址交易、即时业务交易和跨分支交易
nLockUntil	uint32	交易冻结至高度为 nLockUntil 区块
hashAnchor	uint256	交易有效起始区块 HASH
vInput	vector<CTxIn>	前序交易输出列表，包含前序交易 ID 和输出点序号
addrTo	CDestination	输出地址
nAmount	int64	输出金额
nTxFee	int64	网络交易费
vchData	vector<uint8>	输出参数（模板地址参数、跨分支交易共轭交易）
vchSig	vector<uint8>	交易签名

目前交易版本为 0x0001。hashAnchor 用于指明当前交易适用于特定一个或多个分支。输入列表中的前序交易要求输出地址相同。 交易包括两项输出，一项为表中所列（addrTo/nAmount），另外一项是隐含的找零输出，地址同输入地址，金额为（Total Input - nAmount - nTxFee）。交易签名用输入列表统一地址，签名数据段包含除 vchSig 以外所有字段。

八.跨分支交易

Fn-Fn 不同分支虽然相互独立，但各分支处以高度同步，可以安全引用其它分支数据作为有效证明，实现快速跨分支交易。跨分支交易需要双方在自己分支上创建交易，交易数据中包含对方交易证明，把对应 token 发送到双方一致的跨分支交易模板地址。正常情况下，双方交易会在同一区块高度记录到不同分支区块，双方可从交易模板地址取回交换后的 token。

跨分支交易证明：假设已创建交易 tx，对 tx 除 vchData 和 vchSig 以外其他字段进行 hash 计算，结果为交易证明。交易证明被用于验证双方交易是否被正确记录到各自分支区块中。

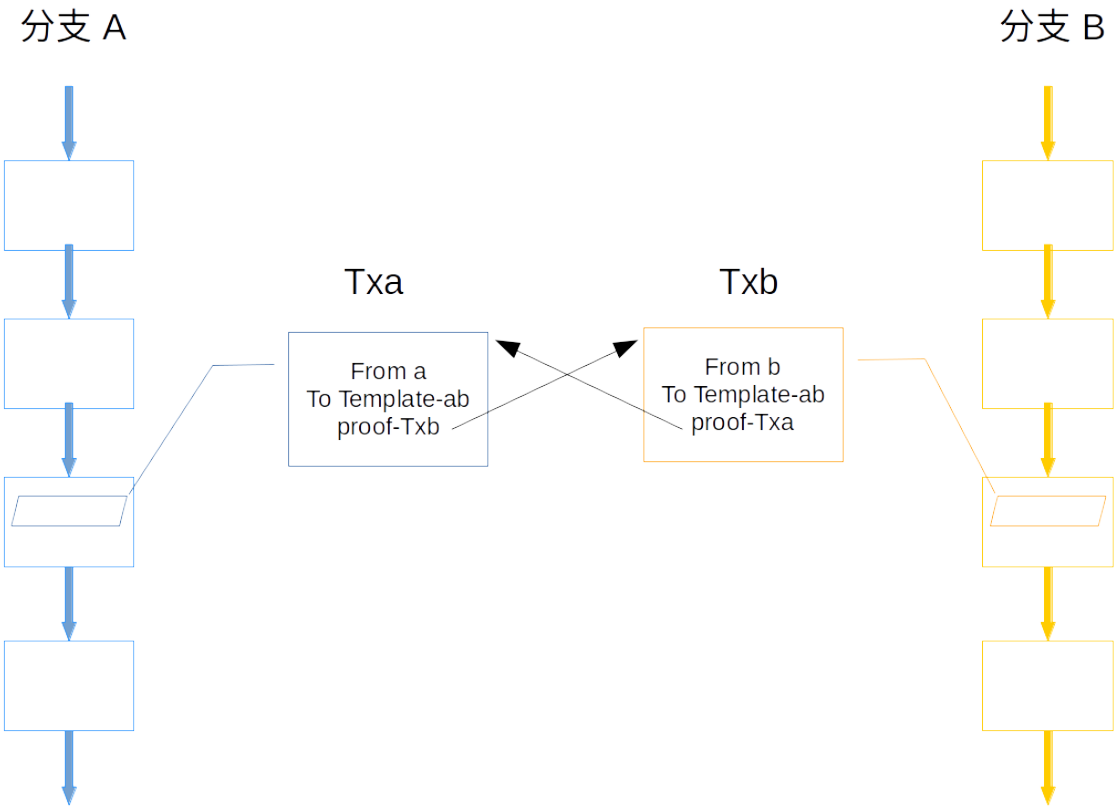


图 8.1 跨分支交易

九.共识机制

Fn-Fn 共识机制为 DPOS+POW，以 DPOS 为主导，决定下次获得打包出块权的节点或者指明下一区块由工作量证明共识产生。在 DPOS 机制未能有效建立时，例如启动初始阶段，POW 成为唯一的出块共识机制。

1. DPOS 节点协商过程

DPOS 节点以所持 token 投票数作为出块权重，通过随机数计算产生固定出块节点系列。DPOS 机制建立后，通过 DPOS 节点之间协商产生随机数。协商过程每分钟进行一轮，通过加权 VSS+BA 方式进行公平随机计算。

每轮协商都包括以下几个过程：1)节点登记；2)加密分片数据分发；3)秘密分片公布；4)数据重构和随机信标计算。

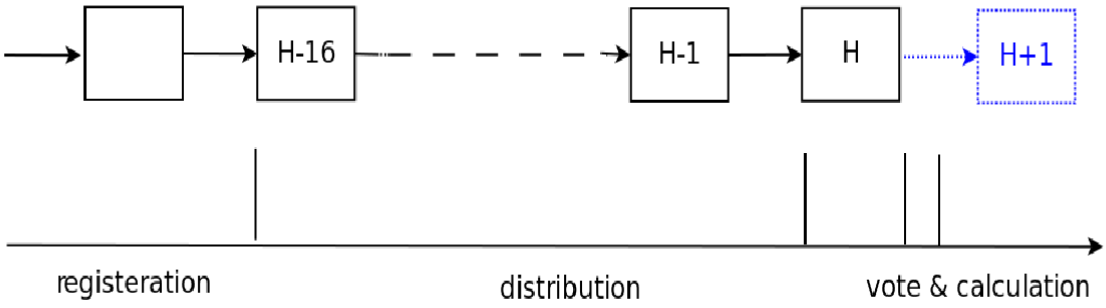


图 9.1 DPOS 协商过程

在每轮协商之前，每个 DPOS 节点需要利用 ECC 算法产生一组私钥： $\{a_0,a_1,\ldots,a_{t-1}\}$ 以及对应公钥: $\{A_0,A_1,\ldots,A_{t-1}\}$，满足 $A_i = a_iG$ 其中 $i = 0,1,\ldots,t-1$。 t 为重构数据的门限值，根据对有效 DPOS 节点设定，t 最大值为 50。

1) 节点登记

DPOS 节点在本轮协商对标区块 16 个区块之前将登记信息广播上链，包括加密后的多项式系数 $\{A_0,A_1,\ldots,A_{t-1}\}$,$A_0$ 作为节点协商公钥。

2) 加密数据分发

分发开始于协商对标区块之前 16 区块止于前一区块。分发过程开始时，根据登记节点的顺序和权重分配计算序号，每个节点分配到的计算序号数量= [token vote/（total supply x 2%)] 。节点 i 根据其它节点 j 发布的协商公钥创建共同密钥 K_{ij}，将秘密分片 s_{ij} 以 K_{ij} 加密后广播全网，对应节点 j 解密后可以用节点 i 的登记信息对 s_{ij} 进行校验。其中 s_{ij} 下式计算：

$$s_{ij}=\sum_{k=0}^{k<t} a_k \times j^k$$

由于节点 i 的加密公钥 $\{A_0,A_1,\ldots,A_{t-1}\}$ 在登记过程已公布，节点 j 通过下式进行校验：

$$sij \cdot G=\sum_{k=0}^{k<t} j^k \cdot A_k$$

若上式成立，说明节点 i 发送了正确秘密分片。

3) 秘密分片公布

当前一区块广播后，每个节点将通过校验的所有秘密分片广播全网，全网节点在收集到解密的节点分片，也可以通过上面公式进行校验，最终剔除恶意节点数据后将有效数据进行计算。

4) 数据重构和随机信标计算

全网节点在收集节点 i 的 t 个秘密分片就可通过拉格朗日方程重构 $\{a_0,a_1,\ldots,a_{t-1}\}$，不能收集到 t 个通过校验秘密分片的节点会被剔除，不能进入下一阶段计算。重复上述计算过程，最终可获取所有有效节

点数据。此过程中，所有可靠节点计算结果将一致，通过组合计算，得到全网一致的随机信标。由于用于计算的数据分别由各 DPOS 节点随机提供，在进行到最后一步计算前，都无法获知其它节点的数据。作弊节点在校验和重构阶段就会被剔除，在不考虑 51%攻击的情况下，没有节点可以控制最终计算结果，因此可以认为产生的随机信标具备真随机属性。

2. 打包出块权权分配

在 DPOS 机制没有有效建立起来的情况下，当前区块由 POW 共识产生。当 DPOS 协商成功完成，就会用随机信标进行掷骰过程，假设 DPOS 节点 i 的 token 投票为 V_i，总的 DPOS 投票 $V_d = V_0+V_1+...+V_n$，总 token 供应量为 S。

POW 等效投票为 V_{work} = S X (1 - V_d / S)^3

节点 i 获得打包权的概率 $P_i = V_i / (V_d + V_{work})$

POW 获得打包权概率 $P_{work} = V_{work} / (V_d + V_{work})$

重复上过程，就可以得到确定的出块序列。按照出块序列，对应节点完成当前区块打包，并将解密后的协商最后一步计算过程记录进区块，自证出块合法性。

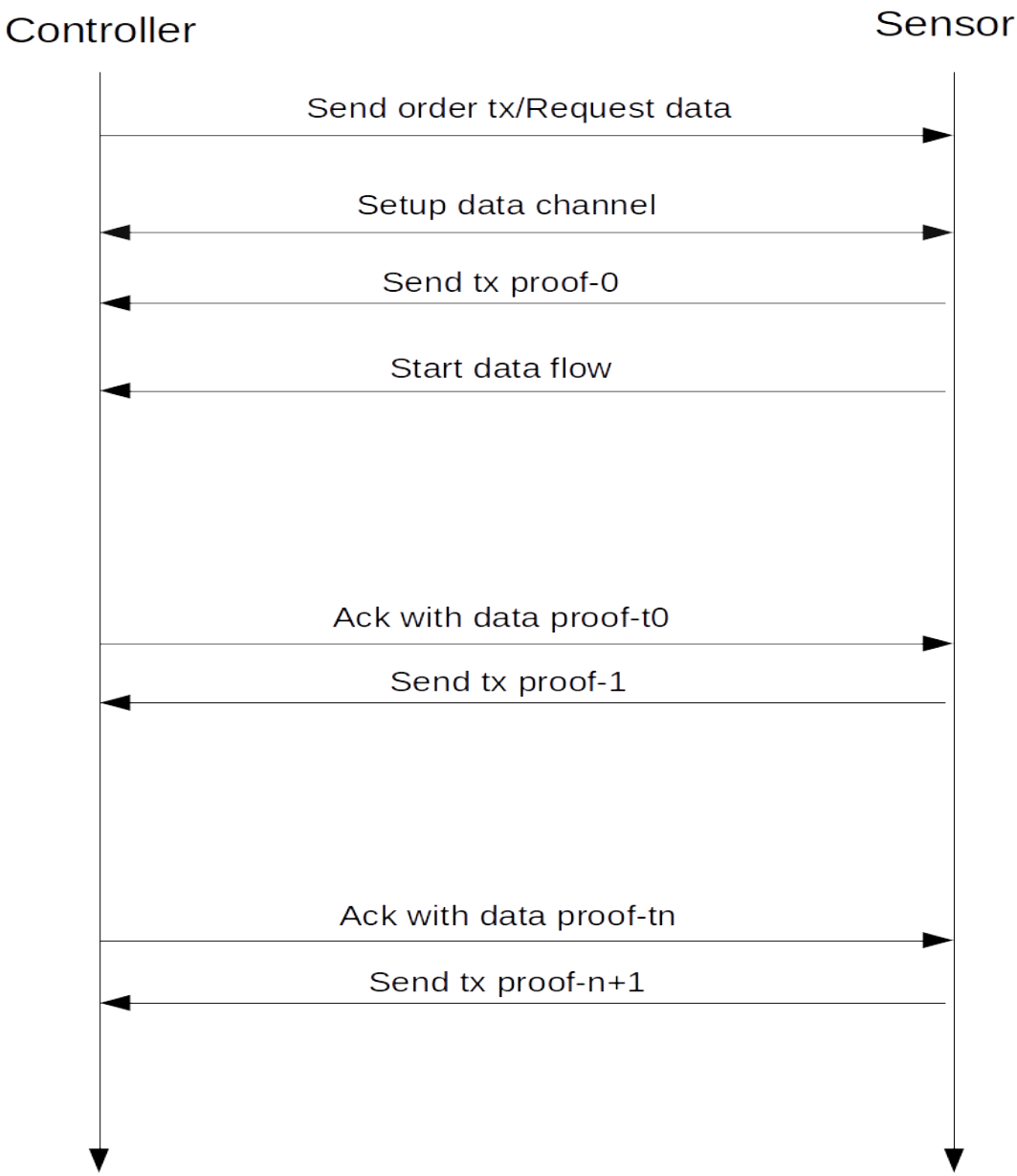
在经过 DPOS 协商，确定的出块系列可以被所有节点一致计算验证，除了指定确定节点进行出块，有一定概率指定 POW 出块。如上面公式，POW 区块被选中的概率和参与 DPOS 协商总 token 数量相关：

V_d / S	P_{work}
0	100%
0.25	62.8%
0.5	20%
0.75	2%
1	0%

在起始阶段，参与 DPOS 的节点和 token 比较少，共识机制退化为以 POW 为主，当越来越多 token 参与到 DPOS 过程，POW 出块几率会迅速降低。

十.IOT 数据业务模型

IOT 实时数据交易业务以交易订单形式构建，由数据需求方发起交易，将 token 发送至订单交易模板地址。一旦订单交易上链确认，数据提供方校验交易合法性后建立实时数据通道，并且立即发送一个带时间戳、有效期以及当前消费 token 数量的交易证明给数据需求方。在此之后，每当交易证明超过有效期，数据提供方应更新交易证明。假设双方约定以 t 为数据结算周期，每经过 t 间隔，数据需求方以签名证明作为 ack 发送给对方；任何时候交易中断或结束，数据提供方以最后的签名证明从链上对应订单交易提取消费 token。



图

10.1 IOT 数据交易过程

当数据提供方先从订单交易提取 token,需求方可以随后立即取回剩余 token。如提供方没有转移对应 token，需求方也可用一个包含有效交易证明的交易取回 token，该交易会被广播但会被打包节点锁定 30 区块高度。如不包含有效交易证明，会从订单交易所在区块开始锁定 2880 区块高度。锁定期间，数据提供方如有争议，可以发送自己有效交易优先取回 token,争议交易会被丢弃。