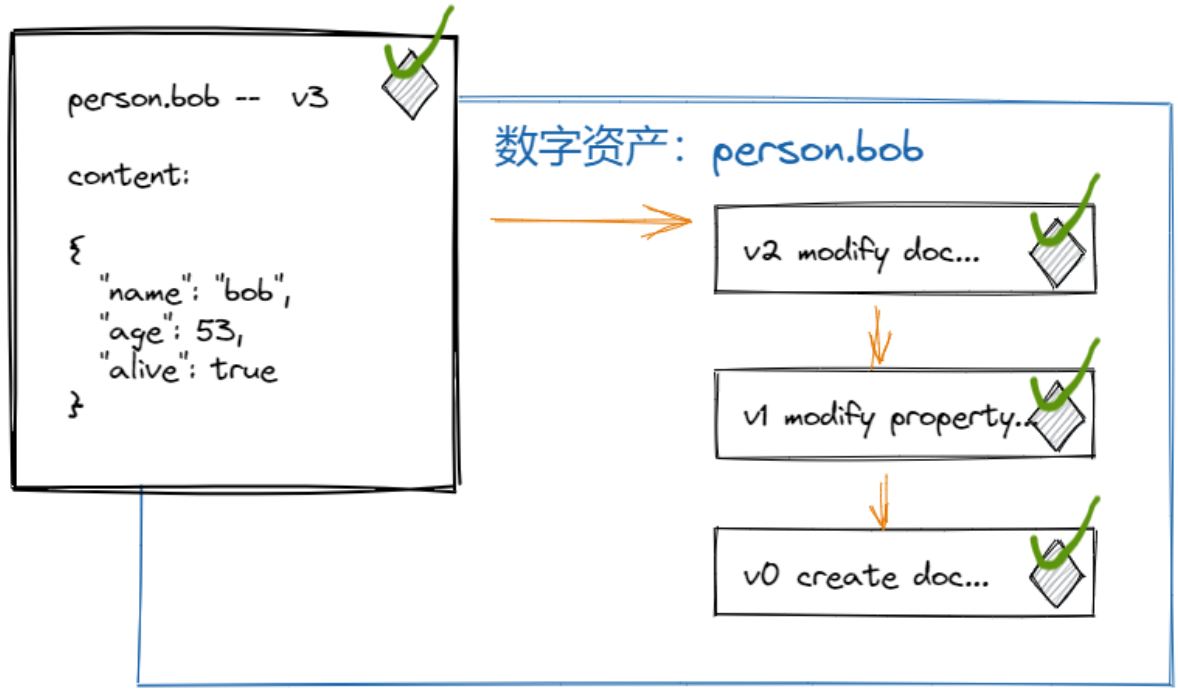
Paimon 快速入门手册

本文介绍Paimon核心概念和主要工作原理，具体操作和详细接口请参考《安装部署手册》、《开发人员手册》等详细文档。

数字资产

Paimon是以数字资产为核心的分布式账本系统

Paimon中的数字资产，是一个由文档内容、变更记录、数字签名共同构成，不可替代、不可篡改、可操作、可流转的最小数据单元。



文档内容是一个JSON格式文本，用于描述特定资产的属性特征，一个数字资产中包含了当前文档内容和所有的变更历史，每个变更记录都包含了由上一版本内容加上当前变更生成的特征值和数字签名，环环相扣，无法篡改。

- 不可替代性：每个数字资产拥有自己的唯一标识，即使属性完全一致的两个资产也不能相互替代
- 不可篡改性：数字资产自身的变更记录环环相扣，修改任一内容都会导致整个记录无效，再加上底层区块链对数据存储本身不可篡改性的保证
- 可操作性：支持数字资产和文档内容的创建、修改和删除，提供高性能的复杂查询能力
- 可流转性：每个数字资产在系统中作为一个完整单元进行交换、流转，不可拆分，不可复制

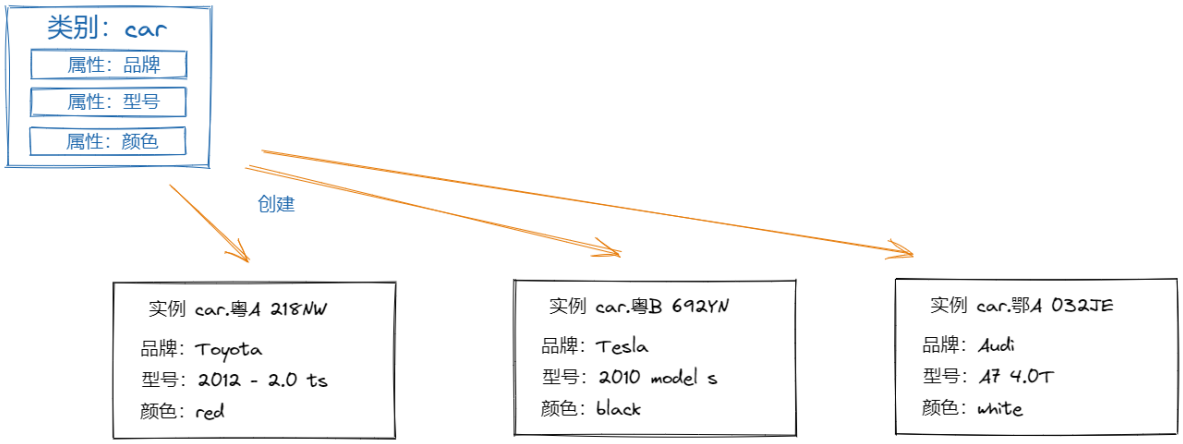
Paimon的数字资产是一个具备自描述性、可证伪性的独立文本文档。数字资产的文本文档无需依赖其他文件，独立存在，文档内容含义一目了然，无需翻译，文档真实性可以轻易验证。

对数字资产的操作由Paimon底层架构保障原子性、有序性：

- **原子性**：对数字资产的一个或者多个操作，不可中断，要么全部成功执行，要么全部不执行
- **有序性**：操作按照请求顺序执行，所有对数字资产的操作在集群各节点都根据相同的请求顺序执行

资产类别

每个数字资产都归属于一个资产类别（Schema），类别使用名称标识，账本系统中除了默认的系统资产类别（名称以'_'开头），用户还能根据业务需要自行定义资产类别。



资产类别定义资产必须拥有的属性清单，属性**有序**排列，属性定义如下：

参数名	值类型	默认值	说明
name	字符串		属性名称
type	字符串		属性的值类型，定义见后
indexed	布尔	false	该属性是否索引，索引属性变更后，需要重建整个资产类别的所属索引

目前支持以下属性类别：

属性值类型标识	名称	说明
string	字符串	字符串属性
bool	布尔类型	true or false
int	整型数字	实际类型int64，支持负数
float	浮点数字	实际类型float64，支持负数
currency	货币	浮点数，不允许出现负数
collection	集合	系统内部保留，保存数据集合
document	文档	系统内部保留，保存复杂文档内容

创建数字资产时，必须指定归属的资产类别，Paimon会对文档进行格式检查，格式匹配的文档才允许进行处理。

数字资产创建后，会根据资产类别在不同路径存储，如果标记了需要索引，则会同步更新索引数据，便于快速查询。

资产类别定义变更时，已经创建的资产不受影响，依然可以访问和操作，但也不会调整已有文档内容，需要调用者自行处理。

资产类别拥有版本记录，定义版本从1开始，每次变更后加1。类别数据会记录所有历史变更，每次变更记录也会使用上一版本定义和本次变更生成特征签名进行链式存储，防止篡改和数据毁损。

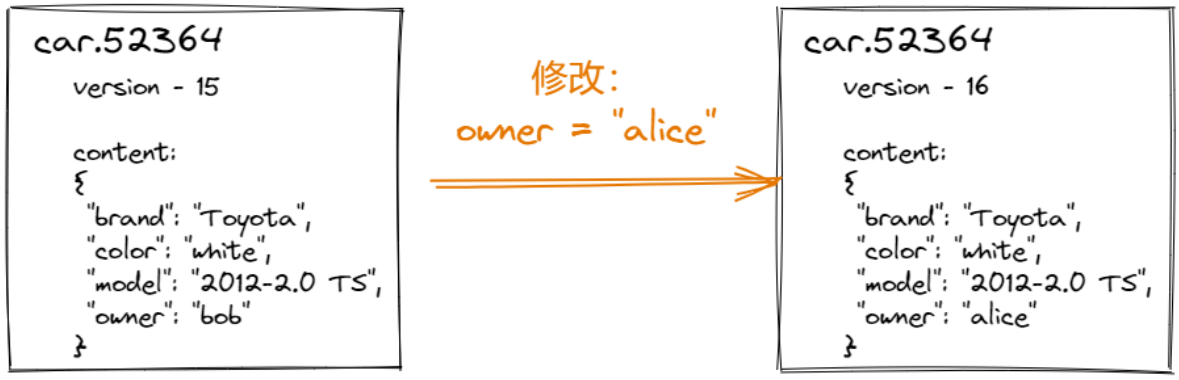
当资产类别要索引的属性发生变化时，原有索引数据全部失效，必须重建之后，才能继续在查询中使用。

资产实例

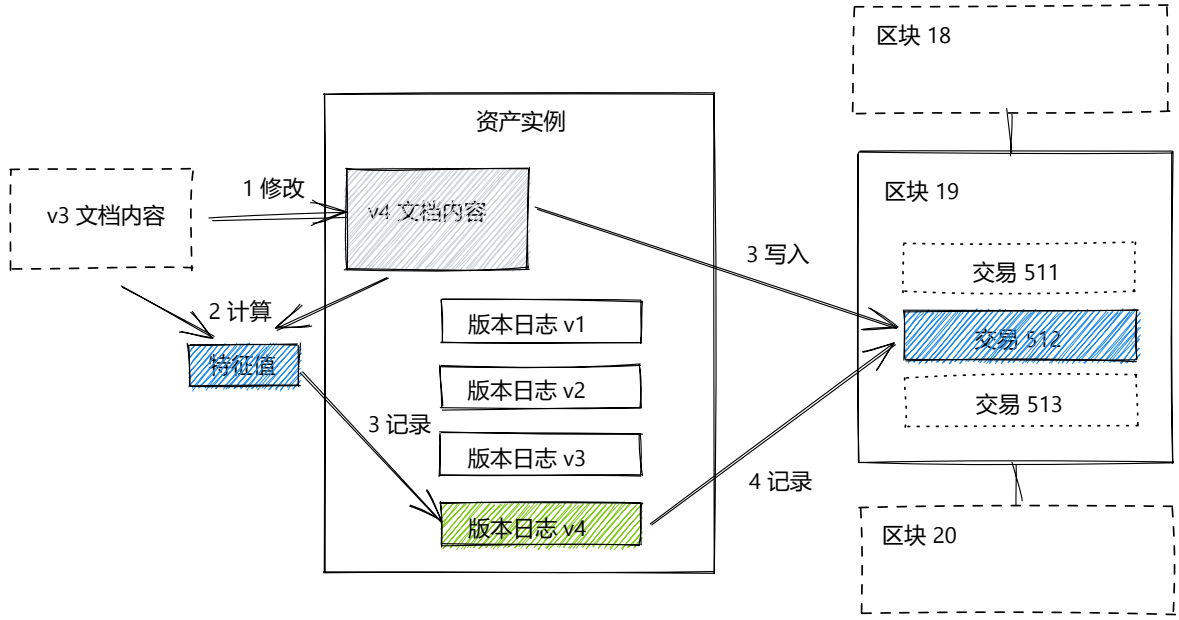
创建数字资产时，指定归属类别和文档内容，就会创建一个全新的数字资产实例，也称为文档（Document）。

每个实例使用"类别名.文档ID"进行标识，每个类别下文档ID都是唯一的，文档ID可以由创建者指定，如果不指定，则由系统生成唯一ID。

对用户和开发者来说，资产实例跟JSON文档一样读取，也能直接修改内容或者变更特定属性的值。



实例包含了文档内容的版本，初始版本为1，每次内容变更会使版本号加1。资产实例内置版本记录能力，除了最新版本的文档内容，资产实例还会根据上一版本内容和本次变更操作，生成特征签名，共识通过后，连同各版本变动关联的区块与交易信息，作为变更日志，持久化存储在实例中。



版本变更日志也是一个环环相扣的验证链条，系统能够非常容易地根据资产实例本身的记录验证文档内容是否被篡改，数据异常时也能快速进行修复，从而保证数字资产的状态和数据可靠可信。

数据域与世界状态

paimon的链上数据可以划分为叫做**数据域**的逻辑分区，域和域之间数据相互隔离，互不影响，链构建完成时会自动创建默认数据域**system**，所有数据类别和资产都默认创建在system域。

数据域内当前时刻所有类别、资产的状态集合，称为**世界状态。**世界状态是持续变化的，每个时刻的世界状态使用版本号标识，从1开始，任何一个交易成功提交（意味着有类别或者资产的状态发生变化），版本号加1。

世界状态的版本是节点间同步状态的重要参考，当节点出现数据不同步的时候，首先要对比各节点世界状态版本是否一致。

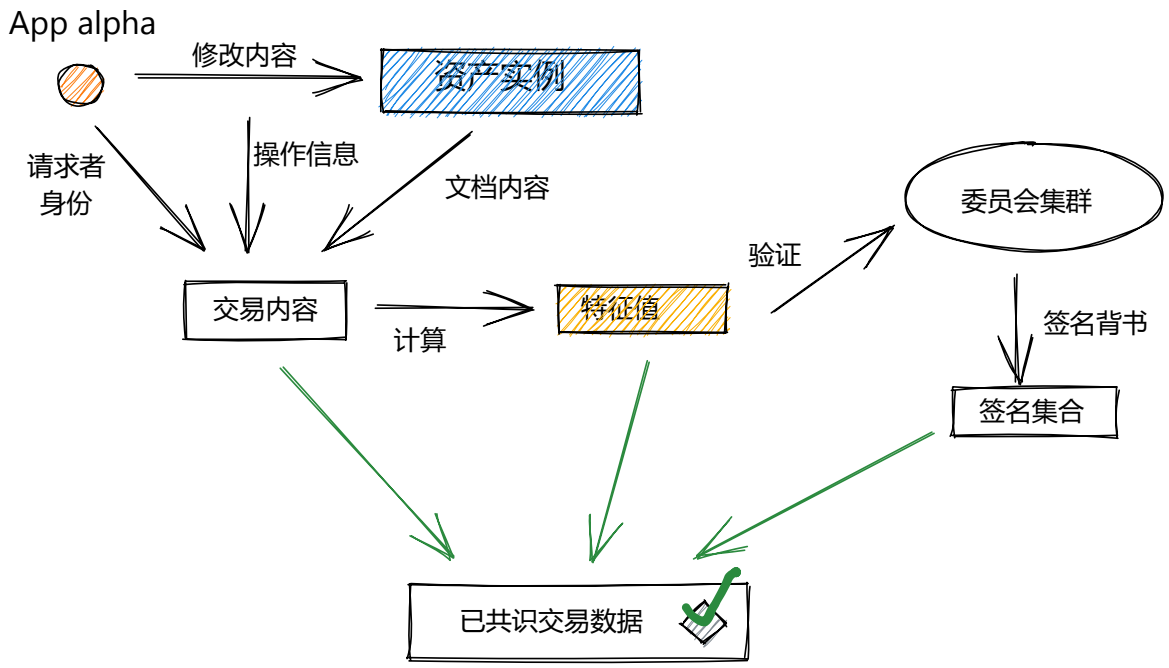
区块存储

除了数字资产以外，Paimon的交易数据也会以区块形式进行持久化存储。

交易

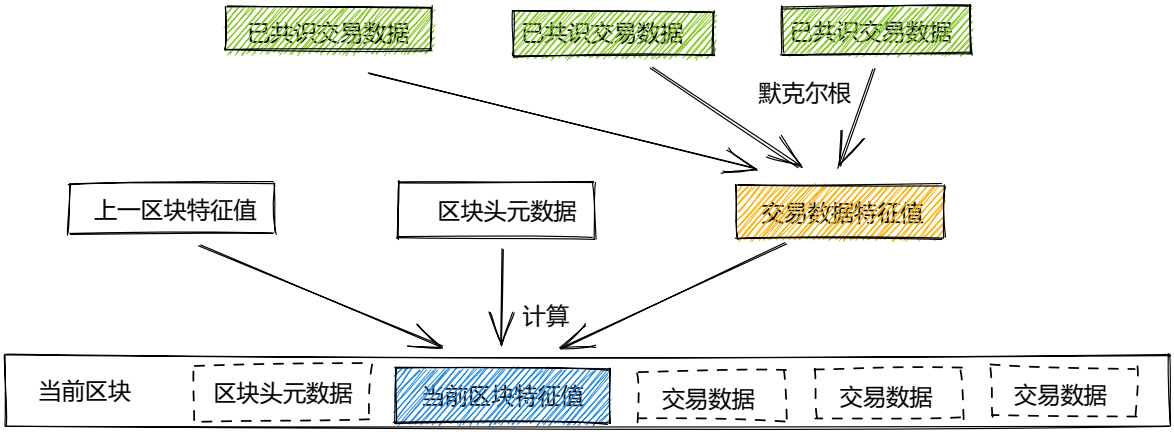
Paimon的交易由数字资产变更驱动，交易数据包含资产变更时间、发起者、世界状态版本、变更涉及的读写结果集等内容。

各节点接收到对数据资产操作请求后，在本地世界状态执行，产生交易内容，再根据交易内容生成特征值并使用自己的数字私钥背书签名。各节点独立执行相同的交易，产生相同的结果，然后对结果签名，委员会通过验证收集到签名，检查集群是否对于该交易结果达成共识，共识后的交易数据会在出块时写入区块中。



区块

出块时，Paimon会选择一定数量**已达成共识**的交易数据，加上上一区块特征值，再连同发起者、创建时间等标准元数据，构建区块内容，并且背书签名。



委员会通过验证有效签名数量，判断是否达成共识并持久化存储。由于每个区块都包含上一个区块的特征信息，要篡改数据，需要修改所有前置区块数据，并且需要全集群共识，技术上非常难以实现，所以能够有效防范恶意篡改。

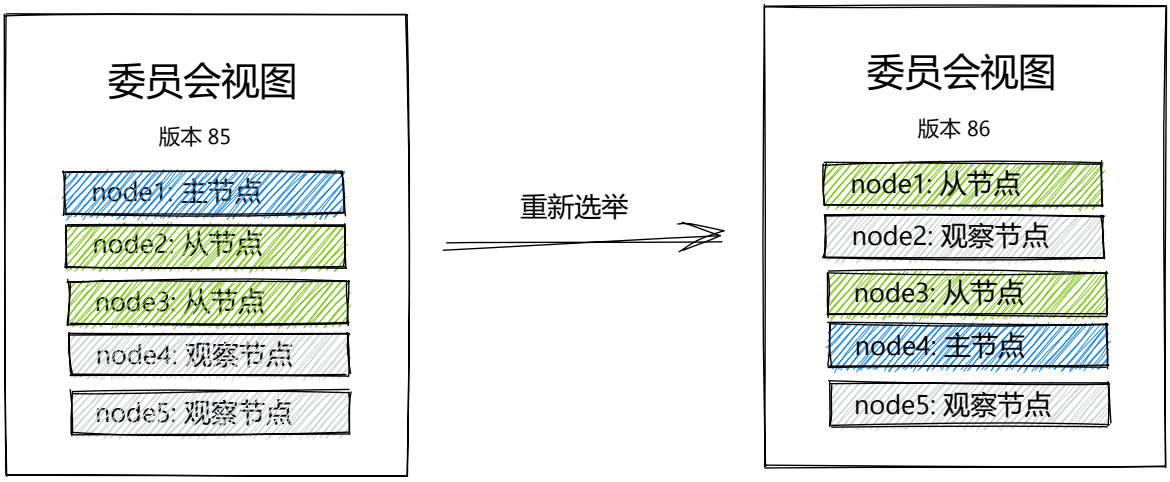
共识机制

委员会与视图

Paimon是分布式账本，意味着所有变更操作必须得到集群共识确认，才能持久化存储。

Paimon从集群节点中选出特定数量节点作为委员会节点，其中一个主节点，负责分配交易序号和判别何时出块，其余为从节点。为了让集群共识的时间复杂度和空间复杂度都保持为常量（O(1)），Paimon委员会节点数量为可配置的固定值。选举时，集群所有节点都平等地参与选举，选举完成后，委员会节点之外的节点，作为观察节点，持续从委员会节点同步最新的链状态，而不参与共识过程，直到下一次选

举。

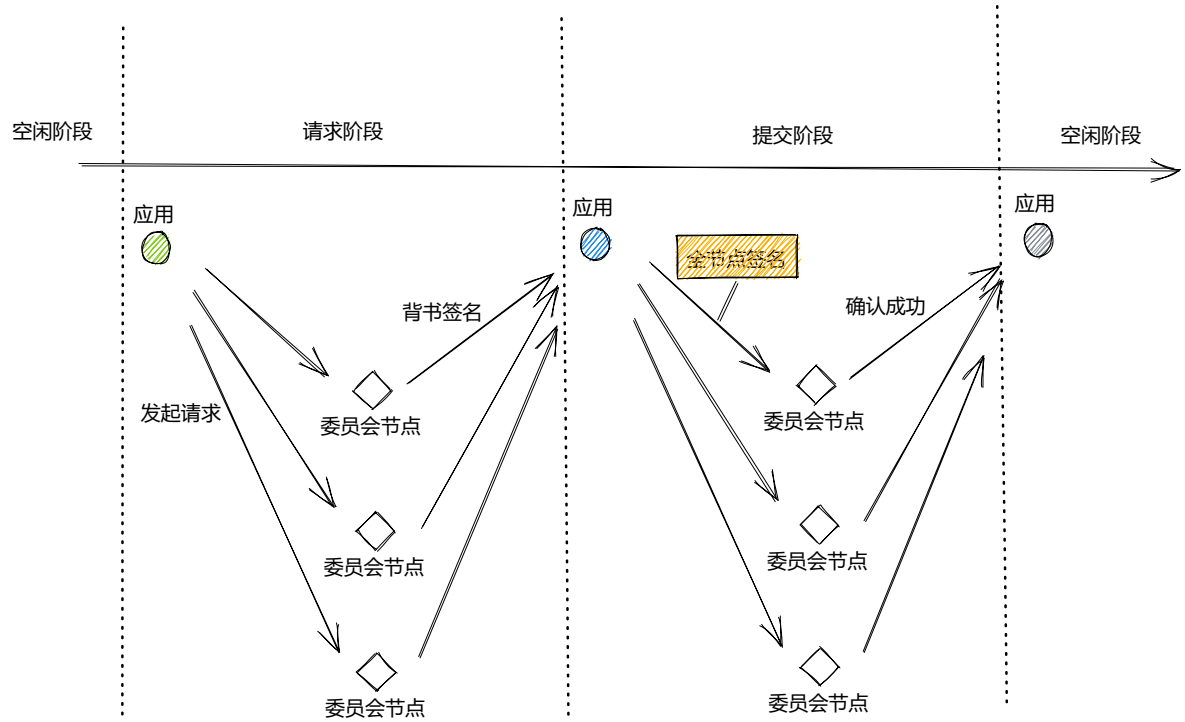


Paimon的选举算法是基于Raft的改进算法，其中加入了世界状态版本和区块高度等特征信息，用于提高选举效率和准确度。

任一时刻，委员会节点信息集合称为当前视图（Consensus View），视图使用版本号标识，每次从1开始，选举完成后，视图版本加一。视图版本信息会携带在操作请求中，节点发现收到请求的视图版本与本地不一致时，会认为请求失效，进行抛弃。

交易共识

请求交易时，首先向当前委员会的主节点分配交易ID，然后将请求内容加上ID发给所有委员会节点。各节点在本地根据交易顺序执行，并结果签名背书后发回请求者。请求者收到的共识响应数量达到预设阈值（可配置）时，视为满足提交条件，将所有收集到的签名连同提交请求发给所有委员会节点。



委员会节点接收到提交请求时，验证各节点签名有效性，如果有效签名数量满足条件，则接受交易提交，并进行持久化存储。

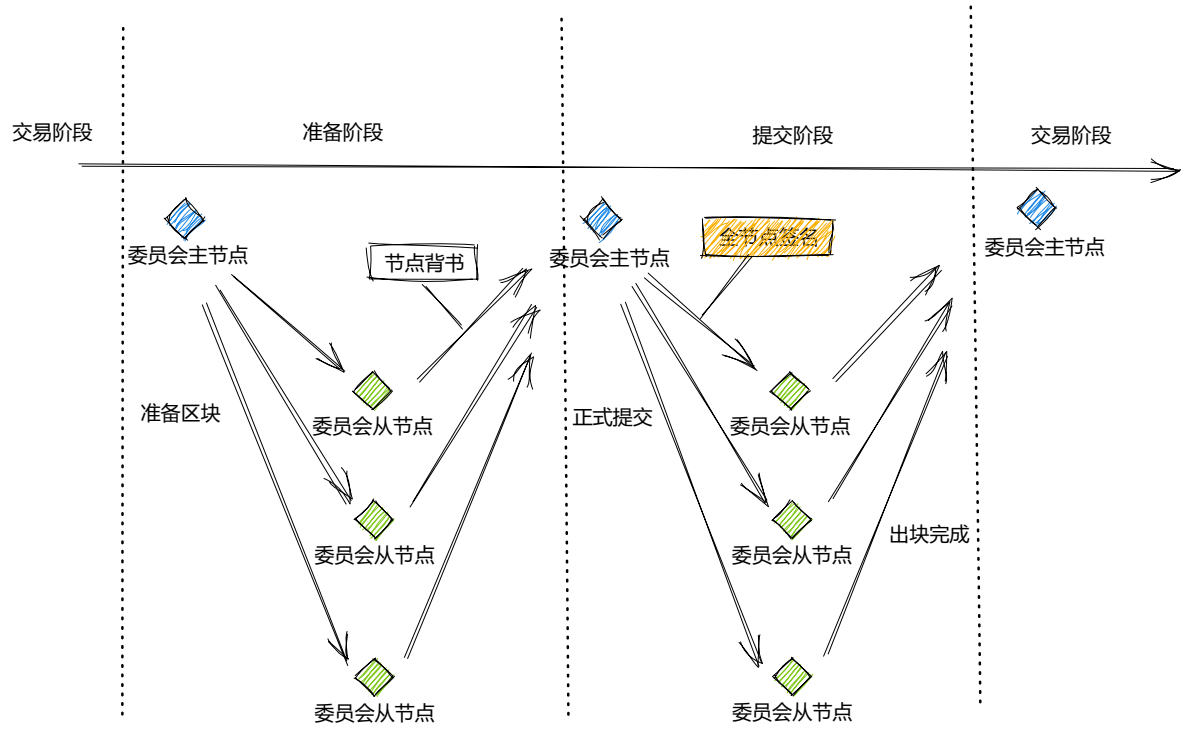
出块共识

委员会主节点会持续关注链的状态，当满足下列任一条件时会触发出块操作：

- 已确认的交易数量超过阈值
- 已确认的交易内容大小超过阈值
- 有已确认交易，且超过特定时间没有新交易请求

条件满足时，主节点进入预备出块状态，会选定要保存到区块的交易清单，准备好区块内容并且签名背书，向其他委员会节点发送准备出块请求。

其他节点收到准备请求后，也切换到预备出块状态，根据交易清单，独立生成区块，检验结果是否与主节点一致。如果验证通过，则签名背书，通知主节点同意出块。



主节点收集到足够的支持响应后，确认达成共识，将本地区块持久化存储，并将所有的签名连同出块请求发送给其他委员会节点，自己回到日常交易状态。

其他节点收到出块请求后，验证所有签名，如果内容无误，则确认出块并持久化存储，回到日常交易状态。