# Plasma设计

可扩展的多方计算平台

假设我们有某种状态，如两个不同用户的余额，经历了许多频繁的小变化。如果我们可以完全在链下协商并且快速交易，然后只有在各方满意时才提交最终状态，这就是状态通道（针对支付的用例被称为“支付通道”）。

状态通道的主要缺点是，它要求你与所有想要进行状态转换的人“打开一个通道”。 因此，如果我想付钱给你，我必须开一个状态通道，这需要质押金钱（还是加密经济安全性），然后关闭通道（成本还更高）。在简单的情况下，额外工作并没有提供任何好处，但它确实提高了效率，将多个状态转换压缩到单个状态转换，可以支持小额支付或点对点游戏逻辑。你也可以像雷电或闪电网络那样通过中间人使用状态通道，这可能会缓解大部分不利因素。

一般而言，状态转换具有最终确定性，但该确定性是以“质疑期（Challenge period）”为代价的（仅在单边退出的情况下）。质疑期让一位参与者有时间窗口提交另一位参与者的欺诈证明，从而使双方提议的状态变化无效。从用户体验的角度来看，这个质疑期非常烦人，因为要渡过质疑期，状态通道关闭的最终状态才能实际使用。

## 子链的树形结构

子链周期性提交状态迁移到父链，提交到父链的状态为finalized状态。

树形结构可以无限扩展。从根上来看，只有周期性状态迁移提交到链上，由智能合约确保基于权益的共识和业务逻辑的执行。

由于不是所有数据都全网广播，相关方需要持续监控对应的子链，当发现欺诈行为时，及时提出挑战。

## 子链的权益证明

白皮书设计中，每个Plasma子链采用PoA的方式，即有一个operator负责创建区块，所有链的参与者都是验证者，当operator生成了一个无效的区块，所有其他人都可以构建对应的欺诈证明，从而对operator进行惩罚，并获得奖励。

为防止隐藏区块的攻击方式，Plasma也可以基于权益证明的共识方式。

借用Nakmoto共识的思想，通过权益保障共识安全的同时，激励网络中验证者之间进行高效的区块广播。

Fee的分配给所有的区块的创建者，同时考虑区块创建者抵押的Stake占Stake总数的比例。比如，一个创建者的Stake占比为3%，在每100个区块中平均应当有3个区块由他创建的，当他创建的区块的比例>=3%时，将可以收到3%的手续费；但是如果创建区块的比例<3%，将不能和同比的获得3%的手续费。

由此带来两个效应：

1. 估计所有验证者相互合作，使所有验证者都参与到链的构建中
2. 由于每个区块的构建都需要历史100个区块的完整信息，所以也激励区块验证者之间互相传递区块，从而使每个区块都能快速得到所有验证者的验证。

## 激励子链的持久运行

每个子链由一系列的智能合约实现，在白皮书的设想中，每个plasma子链都有一种token，基于此token实现PoS，通过这个子链上的token价值激励子链的validator。

validator通过抵押ETH参与到子链中，然后接收子链上的token作为手续费，如果子链上的经济模型比较合理，validator将持续对子链上的区块和交易进行验证，从而保证子链的持久运行。

## sharding的refuse to disclose information问题

白皮书设计中，提出以下三种策略：

1. 通过增加PoS机制，激励节点广播自己的区块
2. 增加withdrawal证明和延迟时间
3. 子链上的交易可以通过提高手续费直接广播到父链，参与方将更倾向于将交易发送到子链上，从而降低成本

## 无欺诈证明

白皮书设计中，子链上的所有状态都附带无欺诈证明，在区块完成finalize之后，就无需向parent chain提交无欺诈证明。

每个区块都需要的内容：

1. 当前状态的Merkle证明
2. 输出UTXO的Trie树
3. 交易的Merkle树
4. 向前一个state的hash链接

如果parent chain上监测到子链上的区块欺诈，子链的无效区块将被回滚。

## 合约锁定的规则

1. 钱支付到主链
2. plasma链上收到支付证明，完成初始化
3. 各方在plasma链上确认参与后，钱真正完成锁定

## 状态迁移的压缩

plasma中的状态主要是指utxo的状态，可以通过bitmap表示输出。（参考意义不大）

提款请求：

签名交易的bitmap

bitmap中纪录了哪些utxo将被支付

# Plasma MVP设计

链的状态数据：

1. 链的owner
2. 区块链表
   1. 每个区块中
      1. Merkle root
      2. Merkle root的提交时间
3. 请求退出的交易列表
   1. 每个请求退出交易
      1. 交易提交者的地址
      2. UTXO位置（对应的区块号，交易Index，out index）

区块的创建有两种方式：

1. 链的operator可以创建区块
2. 在主链上将ETH抵押到合约中，当抵押完成，plasma自动创建一个新的区块，区块中只包括一个交易，交易中创建的UTXO和抵押的金额相同。

合约的接口：

1. submitBlock (bytes32 root)

提交一个新的区块，区块中只包括Merkle root

1. deposit ()

生成一个新的区块，区块中只包括一个交易，交易生成msg.Value等值的UTXO

1. starExit (uint256 plasmaBlockNum, uint256 txindex, uint256 OutputIndex, bytes tx, bytes proof, bytes confirmSig)

指定UTXO的退出请求，需要UTXO生成的区块号，包含此UTXO的交易，交易的Merkle证明，创建此UTXO交易的所有者的签名等。

1. challengeExit(uint256 exitId, uint256 plasmaBlockNum, uint256 txindex, uint256 oindex, bytes tx, bytes proof, bytes confirmSig)

对某个UTXO的退出请求提出挑战，需要提供：退出请求的Id，TXO的对应的花费证明，花费所在的区块号，TXO的owner所做的签名。

所有的startExit保存在一个优先级队列中，优先级表示为：（区块号，交易ID，output Index），当调用退出时，如果创建Utxo的区块已经超过7天，可以使用7天内最早的区块替代。退出申请超过14天后，将按照优先级依次完成退出。

通过退出的顺序性，也可以保证先提出的退出请求会被先处理，在攻击者伪造无效区块包含无效的UTXO的时候，对应UTXO的持有人可以比攻击者提前退出Plasma。

交易的格式

［blknum1, txindex1, oindex1, sig1, # input-1

blknum2, txindex2, oindex2, sig2, # input-2

newowner1, denominations1, # output-1

newowner2, denominations2, # output-2

fee]

用户交易流程：

1. 获得对方的地址
2. 构建交易，发送自己的UTXO到对方的地址
3. 等待交易包括到区块中
4. 发送确认消息，并使用和UTXO相同的密钥签名

challenge周期为7天，所以plasma上的所有用户都必须7天内对plasma链做一次验证，确保及时对无效的退出请求提出challenge。