、Plasma：可扩容自主智能合约

Joseph Poon
joseph@lightning.network

Vitalik Buterin
vitalik@ethereum.org

2017 年 8 月 10 日
工作草案
https://plasma.io/

摘要

Plasma 是在激励下强制执行智能合约的框架提案，该框架可扩容，令每秒钟的状态更新达到极高水平（可能数十亿），从而赋予区块链反映全球海量去中心化金融财务应用的能力。这些智能合约在网络交易费的激励下持续自主运行，最终依赖底层区块链（例如以太坊 (Ethereum)）来执行交易状态转变。

利用我们提出的这个方法，去中心化自主应用可以通过扩容，处理财务活动并且为全球持续的数据服务建构经济激励。这个方法或许能取代中心化服务器群。

Plasma 包含两个关键的设计要素：一是将所有区块链计算重构成一个 MapReduce 函数集，二是一个基于“中本聪共识”激励反对扣块的认知，在现有区块链上用权益证明保证代币的可选方案。

这个结构是通过使用欺诈证明在主链上编写智能合约完成的，借此，可以在父区块链上执行状态转变。我们用区块链组成树结构，并将其各自视为一个单独的支链，该支链带有已执行区块链历史和提交到梅克尔证明中的 MapReducable 计算。通过父链执行，将某人的帐本送入子区块链，可以基于最小的信任实现超大扩容（假设根区块链有效且正确）。

实现非全球数据的全球执行最大的困难在于数据的有效性和扣块攻击，Plasma 的应对方法是保留现有错误链，并且创造机制以激励并且强制数据不断纠正。

由于非故障状态期间，周期性广播梅克尔提交，交易和计算的扩展性和成本优势达到难以置信的程度。非错误状态下，只向根区块链（即以太坊）周期性广播通过梅克尔证明的结论，从而实现大规模扩容并且降低交易和计算成本。Plasma 令大规模持续运行式去中心化应用成为可能。

1 可扩容的多方计算

区块链确保正确性的方法大致可以归结为让每个参与者自己验证链。要接受一个新的区块，必须充分验证此块以确保正确性。很多扩展区块链的交易能力的方法（如 Lightning Network[1]）都需要使用时间承诺来建立一个保真保证（或断言/质疑协议），从而送断言数据进入争议期，供区块链上参与者判断状态真伪。此断言/质疑结构允许一人断言某状态属实，如果此值不真，则进入争执期；争议期内，另一名观察员可以在约定时间之前提供质疑此断言的证明。若出现欺诈或错误行为，区块链将惩罚违规者。通过这种方式，形成鼓励参与者在当且仅当不实状态被断言时才执行的机制。通过这种断言/质疑－证明结构，感兴趣的参与者可以向根区块链（例如以太坊)[2] [3]）上的不感兴趣的参与者断言本底真相。

此结构不仅可用于支付，还可以扩大到计算本身，从而令区块链成为合约的评审层。然而，必须满足一个前提，即假设各方皆是计算验证活动的参与者。例如，在闪电网络中，这个结构允许人们做出关于计算合约状态的承诺（例如，借助条件化状态的多签名交易预签树）。

这些结构支持十分强大的规模化计算，但是有一些问题需要总结大量外部状态（即总结整个系统/市场，计算大量共享/不完整数据，大量贡献者） 。这种形式的多方链下状态（“状态通道” [4]）承诺要求参与者充分验证计算，否则就必须对计算本身投注大量信任，即使是在单回合环节中。此外，通常还有一个“回合”假定，经由这些回合，执行路径必须在合约启动前完全展开，从而让参与者有机会退出并且强制费用不菲的计算上链（因为无法证明停止的是哪一方）。

相反地，我们希望能设计出一个可以让计算在链下发生但最终可在链上执行的系统，这个系统只需要最低限度的链上更新就能支持每秒数十亿次计算。这种状态更新发生在一个权益证明验证人自主集上，这些验证人被鼓励采取以欺诈证明证伪的正确行为，从而允许计算发生并且不允许单个行为人轻易中断此计算服务。为此，必须尽量遏制因数据可用性问题（即扣块）产生的弊端，令根区块链在出现拜占庭行为人时能够最大限度地减少必要的状态更新以防止根链上出现风险折现交易费，此外还要采取一个机制来执行状态变更。

以闪电网络类似， Plasma 是一系列在现有区块链顶层运行的一系列合约，它在保证执行的同时，确保了人们可令资金处于合约状态，也可以在日后完成净额结算/取款。

2 Plasma

Plasma 是一种可以对区块链进行可扩容计算、并且通过其结构创造经济鼓励，无需合约创建者主动实施状态转变管理就能令链自主持续运行的方法。有激励机制驱使这些节点本身维持链运行。

此外，Plasma 具有极强的可扩容性，做法是从一个合约到位图中单个比特，将一笔支出反映的资金最小化，这样一来，一个交易和签名就反映了涉及众多参与者的一笔聚合交易。我们将此机制与 MapReduce [5] 框架相结合，进而构建出由已保证的智能合约来执行的可扩容计算。

基于这个结构，人们可以让外化方代表自己，以类似于矿工的身份来持有资金并且计算合约，但 Plasma 是在现有区块链上方运行的，所以聚结状态更新时链上数据最小，人们不需要在每次状态更新后在底层链上创建交易（包括添加新用户的帐项）。

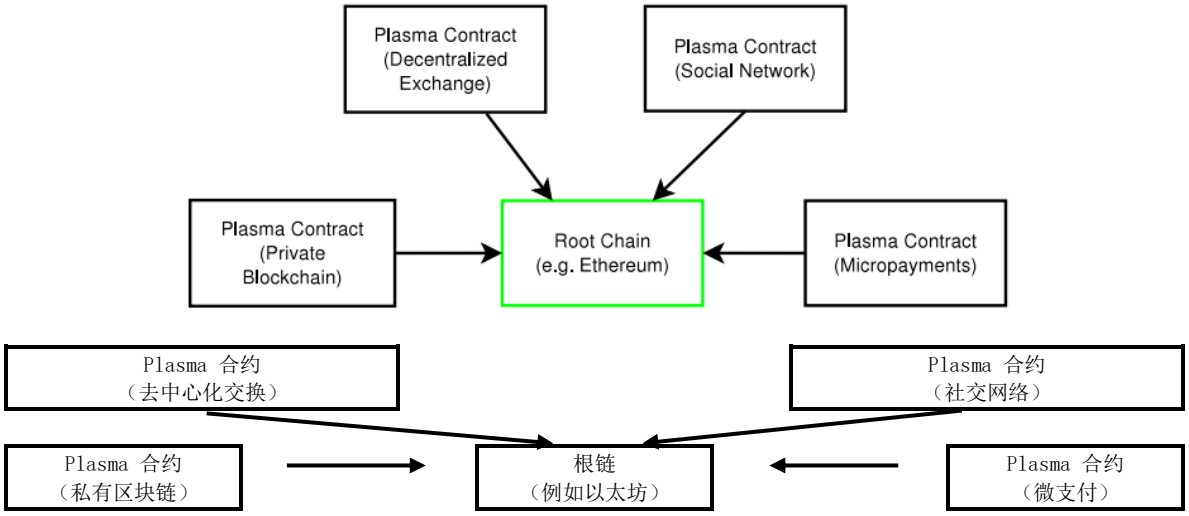

图 1：任何人都可以创建自定义 Plasma 链以实现众多不同用例的智能合约扩容。Plasma 是允许根区块链内有众多区块链是一系列智能合约。根区块链令状态在 Plasma 链中生效。根链负责执行全局范围内的所有计算，只有在欺诈证明的情况下，才被计算并且受处罚。许多 Plasma 区块链可与自己的业务逻辑和智能合约条款共存。在以太坊中， Plasma 会由在以太坊上直接运行的 EVM 智能合约组成，但只处理微小承诺，这些承诺可以反映数量极为庞大的计算和非拜占庭用例中的财务账项。

Plasma 由五个主要组件构成：一个激励层，以经济高效的方式持续计算合约；一个结构，将子链部署成树结构从而最大限度地优化成本效率和交易净额结算；一个 MapReduce 计算框架，用于在这些嵌套链内构建状态转变欺诈证明，以令其与树结构兼容，同时重建状态转变以令其高度可扩容；一个共识机制，此机制依赖根区块链，后者试图复制中本聪[6]共识激励；一个位图 - UTXO 承诺结构，它的作用是确保根区块链下的状态转变准确，实现集中退出成本最小化。Plasma 运行机制的一个关键设计点是允许遇到数据不可用或出现其他拜占庭行为时退出。

2.1 Plasma 区块链，或外化的多方通道

我们提出一个让多方链下通道可以代表他人保持状态的方法。我们称此框架为一个 Plasma 区块链。对于 Plasma 链中持有的资金而言，这个框架允许 Plasma 链中存入和提取资金，通过欺诈证明执行状态转变。因为支持资金存取，所以可以保证可执行状态和可替代性，Plasma 区块中的账目与根链持有资金一致（Plasma 的设计与部分准备金银行制度不兼容）。

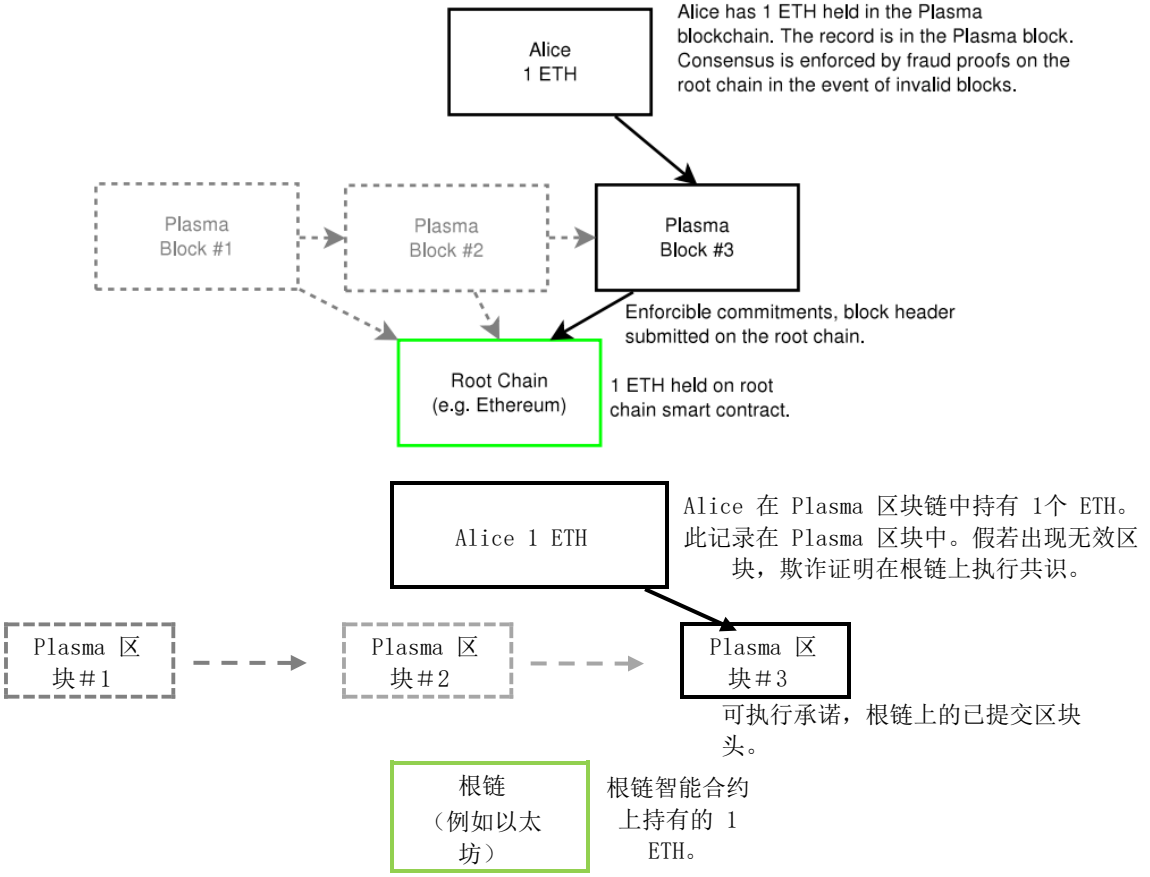

图 2： Plasma 区块链是一个区块链内的一个链。此系统由已保证的欺诈证明执行。Plasma 区块链不在根链（例如以太坊）上披露区块链的内容。事实上，提交到根链上的是区块头哈希，如果欺诈证明被提交到根链上，则区块回滚，区块创建者受处罚。这个方法的效率非常高，因为一个哈希（加上少量相关数据）反映了很多状态更新。此更新可反映未反映在根链上的余额（Alice 的总账余额不在根链上，她的账本在 Plasma 链上，根链中的余额反映的是一个执行 Plasma 链本身的智能合约）。灰色区块是旧区块，黑色区块是已被传播并提交到根链上的最近一个区块。

只需用极少的数据击打根区块链，就能提交大量交易到这条 Plasma 链上。参与者可以向任何人转移资金，包括不在现有参与者集中的参与者。此类资金转移活动可以是存入资金或从根区块链的本币/代币中提取资金（有一定延时并且需要提交证明）。

Plasma 允许某人（或由权益证明网络中的参与者组成的一个网络）在根区块链上没有关于帐本的全部持续记录且未向单个或多个第三方授予监管信任的情况下管理区块链。最坏的情况是资金被锁定，区块链上发生集中退出，损失时间价值。

我们在根区块链上以智能合约［7］形式构建一系列欺诈证明以在此通道中执行状态，从而大量削减欺诈或非拜占庭行为企图。

这些欺诈证明执行一个交互式提取资金协议。与闪电网络类似，取款需要退出时间。我们构建了一个交互策略，要求退出方证明安置在一个请求取款的 UTXO 模型中的参与者帐本输出位图。网络上的任何人都可以提交用以证实是否已发生资金支出的替代性*已保证*证明。假若这样做不正确，则网络上的任何人都可以证明欺诈行为，削减保证以回滚证明。经过足够时间之后，第二个*已保证*回合允许取款发生，这是一个在已承诺的时间戳
* 之前*的状态上的绑定。这个设计允许全部取款，从而令错误的 Plasma 链可以迅速退出。在协调集体取款事件中，参与者可以在父链上只消耗不超过 2 比特的区块空间的情况下退出（最糟情况中，根以太坊上链）。

发生扣块攻击时，参与者可以快速且廉价地完成集中退出，耗用的成本比过去的下链方案少得多。此外，这个方法还不需要向验证节点联盟（侧链工作人员、渔民）提供任何信任。

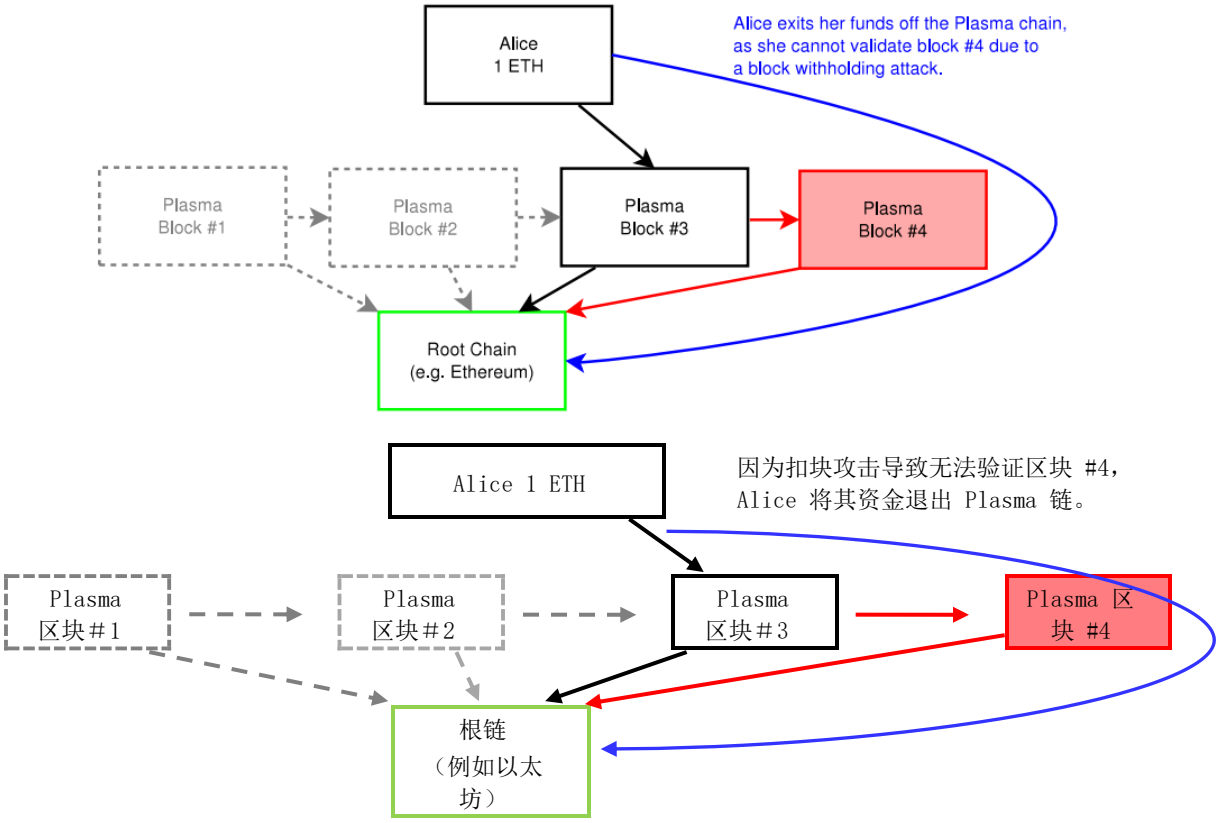

图 3：扣块时资金退出。红块（区块＃4）是被截留并承诺的到根链上的区块，但是 Alice 不能够提取 Plasma 区块＃4。她在根区块链上广播资金证明以退出，她的取款操作在经过争议延时后被处理。

与闪电的结束机制类似，利用两个参与者之间的互动机制，激活二者之间的可执行无限支付，进而允许 n 个参与者之间存在互动机制。主要的区别在于并非所有参与者都需要上线更新状态，参与者不必在根区块链上有录入记录就能参与 — 可以在不进行链上直接互动的情况下在 Plasma 上放置资金，在以树的形式构建这些 Plasma 链时，只需极少数据就能确认交易。

2.2 区块链中的可执行区块链

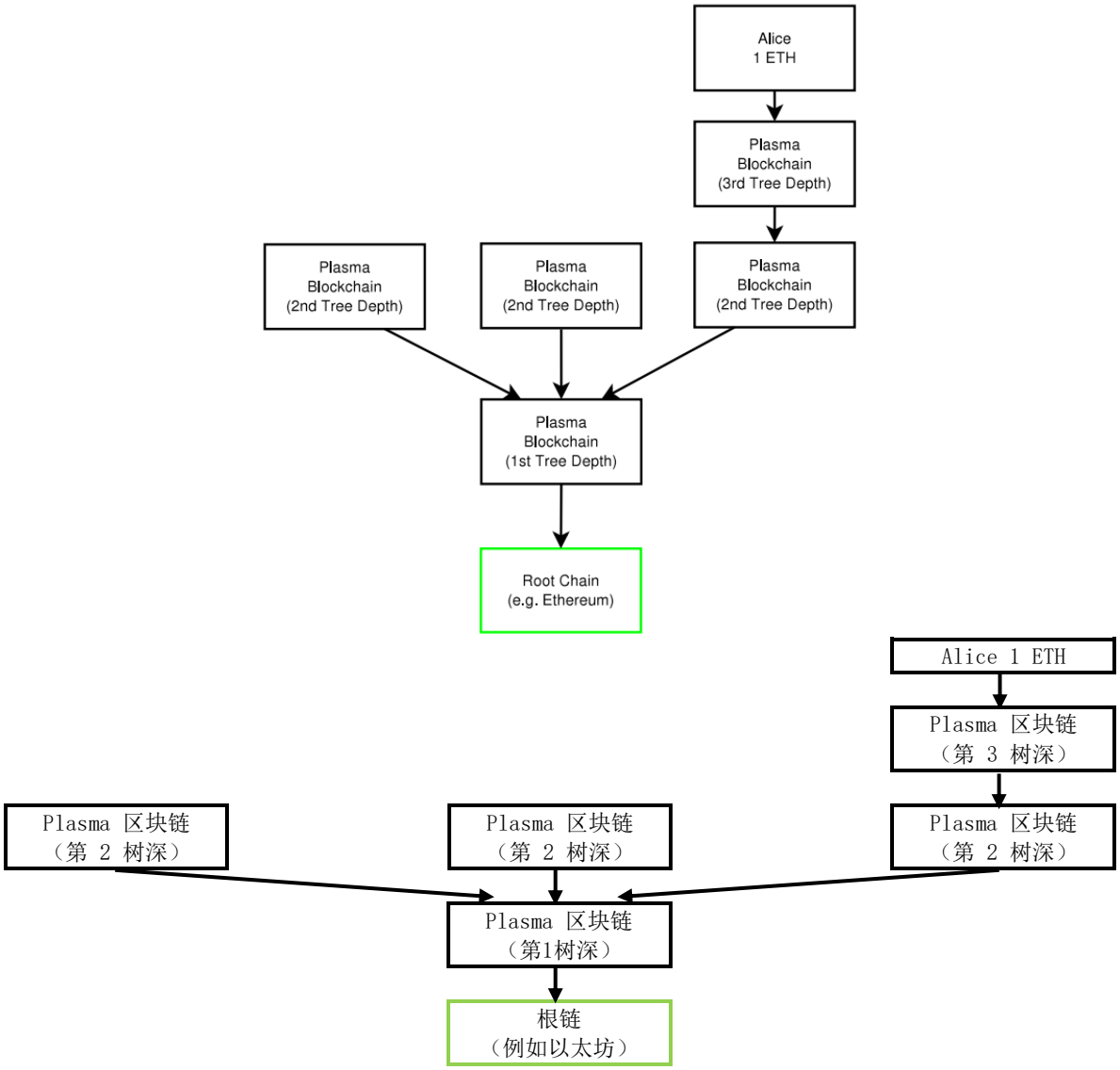

图 4： Plasma 将区块链组织成树。区块承诺向下流动，退出可以提交到任何父链，最终被提交到根区块链。

我们建构的这个机制类似于法院系统。如果闪电网络对最终在根区块链上可执行的支付使用裁定层，则我们创建较高和较低的法院系统，在非拜占庭状态下，实现可用性最大化和成本最小化。如果链是拜占庭 ，则可以选择前往其任一父链（包括根区块链）以继续运行或以当前已承诺状态退出。我们没有（通过撤销）执行递增的当前状态，而是构建了一个欺诈证明系统以执行余额和这些链级的状态转变。

实际上，我们可以创建只会周期性承诺给父链（然后流到根区块链）的状态转变。因为可以在拜占庭条件下只提交原始数据给父（或根）链，所以极大地扩大计算和账户状态的规模。从局部拜占庭条件下恢复的成本被降至最低，因为可以前往 Plasma 父链以执行状态。

这个子区块链在根区块链（例如以太坊）之上运行，从根区块链的角度看，只看到周期性承诺，代币保证在合约中以执行权益证明共识规则和区块链的业务逻辑。

这对于区块可用性最大化和某方货币验证风险最小化极为有利。然而，由于不是所有的数据被传播到所有参与方（只传播到那些希望验证某特定状态的参与方），参与方要周期性监控他们感兴趣的特定链，并且在出现扣块攻击时，迅速自行退链。

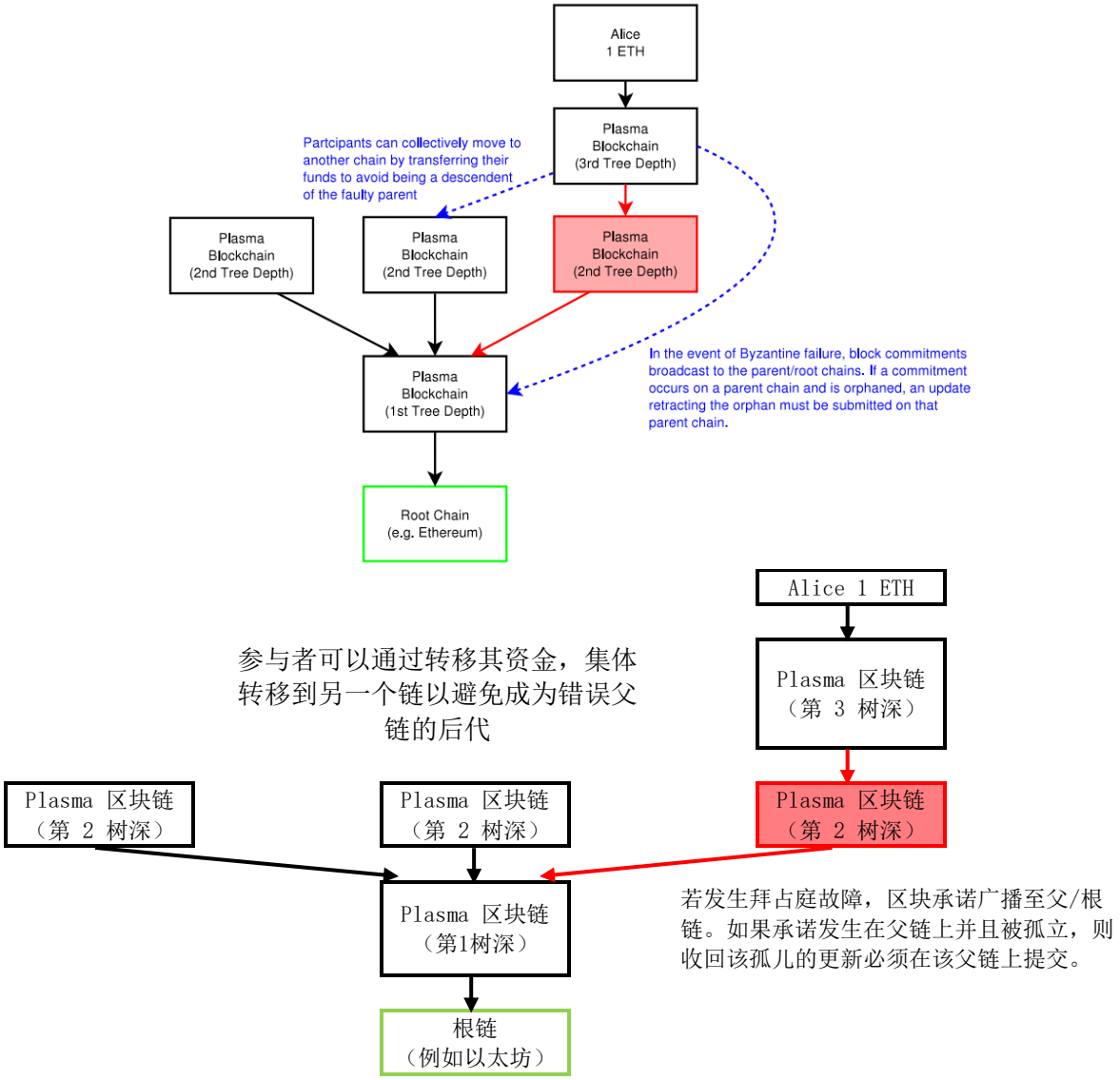

图 5：通过广播一个承诺至其父 Plasma/根链（右蓝色虚线），令错误区块链（有红色阴影的区块链）沿路线传送。第 3 深 Plasma 链中的参与者，在一定时间后，集体迁移至另一个链（左蓝色虚线）。

在非拜占庭环境中，这种结构联合区块链状态树并更新所有子 Plasma 链。所有链上的整个更新集可用一个带签名的 32 字节哈希值来证明。

2.3 Plasma 权益证明

虽然单验证人代表他人持有资金的做法相当有趣，但是我们采用的方法却是允许单方运用一个验证人集来执行状态的方法，这种情况常见于要求 ETH 保证或代币保证（例如 ERC-20）的权益证明框架中。

这个权益证明系统的共识机制是在一个区块链上智能合约中执行的。

我们试图使用权益证明保证，围绕中本聪共识复制激励。我们认为运用中本聪机制构建的一个比较有用的激励机制，能够通过极有效的激励来最大限度地减少扣块攻击。。这是因为领导者都是概率当选的。领导者是随时间推移，基于概率选出的（初始实现中，是 6 个确认）。当人们发现一个区块时，人们相当确信他们有可能是领导者，但是尚且无法肯定他们就是领导者。为了确保他们就是领导者，他们将自己的区块传播给网络上的所有参与者以实现其当选几率最大化。我们认为这是中本聪机制的一大贡献或者说是主要贡献，于是尝试复制此激励。

权益证明联盟面临这个问题，因为如果某人执行直接领导者选举，源自大多数卡特尔的扣块攻击可能（也被概括为“数据可用性问题”）会被放大。

我们可以通过允许利益相关者在包含一个关于他们的新区块的已承诺哈希的根区块链或父 Plasma 区块链执行发布操作，来减轻 Plasma 权益证明中的这个问题。验证人只能在经过他们充分验证的区块基础上实施建构。他们可以在区块上进行并行建构（以鼓励信息共享最大化）。我们的激励很有创造性，通过将更多的交易费支付给准确反映，让验证人反映过去的 100 个区块以匹配当前权益人比例（即若某人投资了 3% 的币，他们就占过去 100 个区块的 3%）。（权益人的次优行为导致的）盈余费用将转到池中以支付未来费用。一个承诺存在于每个包含来自过去的 100 个区块（带随机数）的数据的区块中。一个正确链端是带有最高费用合计权重的链。一段时间后，区块定局。

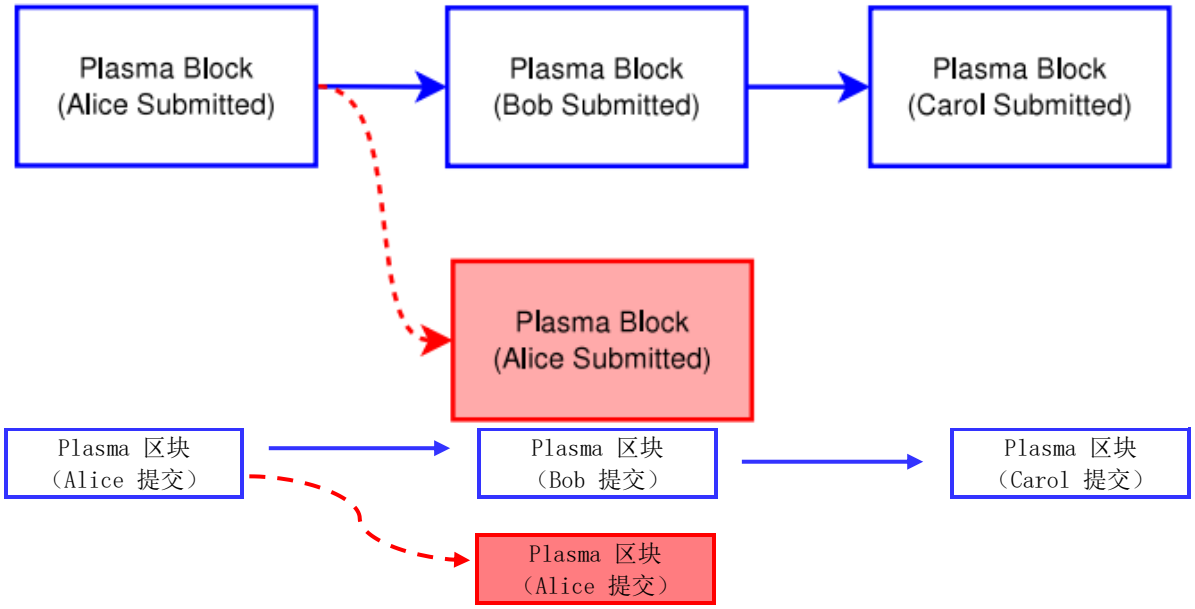

图 6：假定 Alice、Bob 和 Carol 是 3 名权重量相当的验证人。他们都受到构建循环结构以追求最大回报的激励。这些承诺被提交到父/根链。链端视最大权重得分而定，要在 n 个周期中正确分配区块（蓝色是当前候选链端，红色是孤儿）。次优链端有盈余费用进入一个池中以等待未来正确性超过一定阈值（例如 90%）的验证人。n 个周期后，假定蓝色链端已定局。

这鼓励参与者在中本聪共识中参与并复制 51% 的攻击假设。若因扣块或其他拜占庭行为导致链受到攻击，则非拜占庭参与者将在父/根区块链上执行集体简约取款。如果最高父 Plasma 链的保证以代币形式存在的，则该代币的价值很可能会因为集中退出而大幅贬值。

2.4 区块链作为 MapReduce

区块链 : git :: Plasma : Hadoop (MapReduce)

通过构建 MapReduce 格式的计算，也容易完成基于分层树的计算和状态转变设计。

MapReduce 提供了一个跨数千个节点的大规模计算框架。该区块链在计算规模方面也面临类似的问题，在计算证明生成方面还有额外的要求。

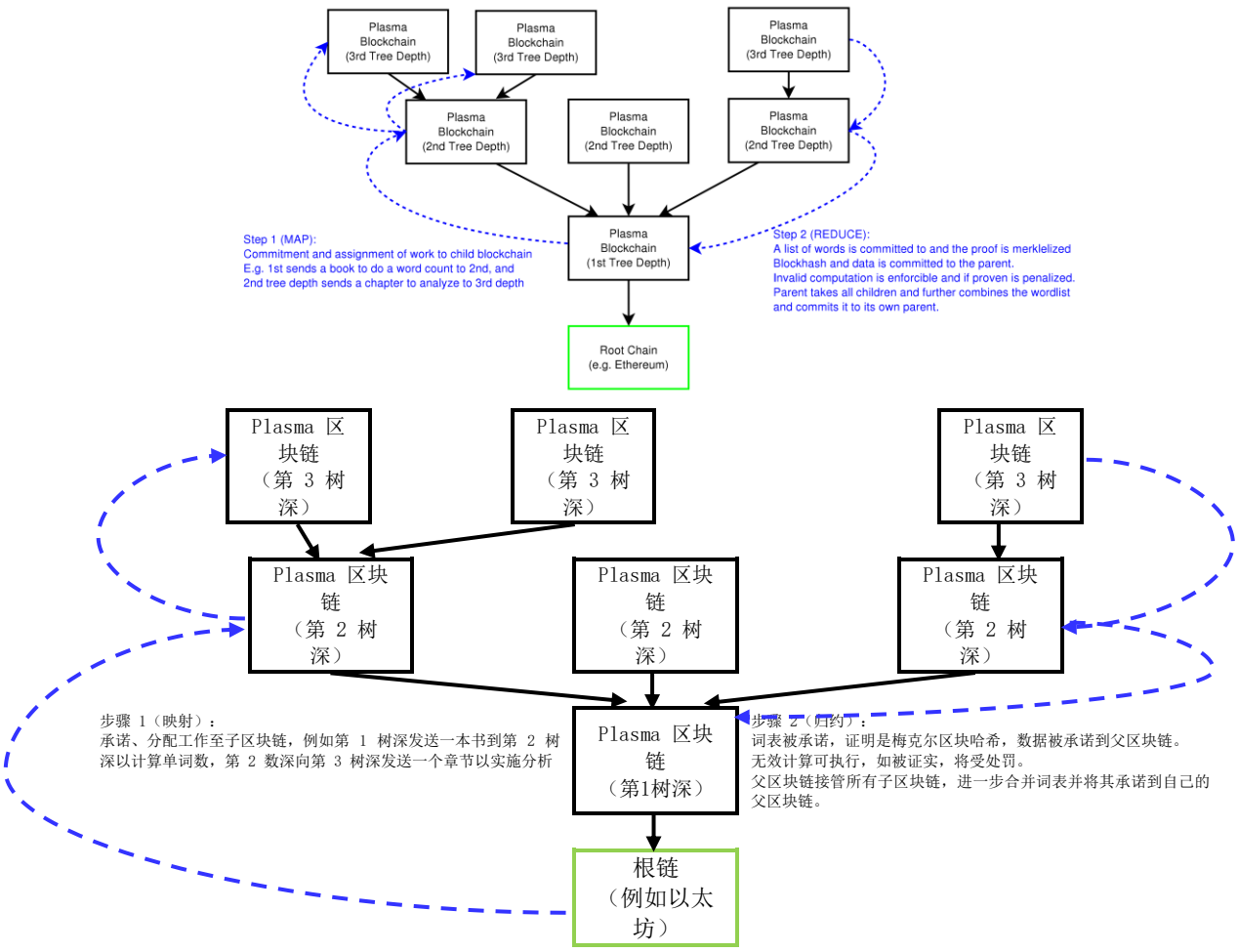

图 7：蓝色是包含在父区块中的、要传递到子区块的消息。子区块必须向一定块数内的父块做承诺，否则将面临跛链。区块数据向用于计算的子区块分配工作。第 3 级子区块链执行计算并返回一个词表（例如，在他们负责计算的章节中，单词“你好”出现了3次，“世界”出现了 2 次）。词表的数据返回到父区块链作为承诺的一部分，子区块链的此表合并后提交给父区块，最终完成全球词表（如整个文集包含 100 个“你好” 实例和 150 个“世界”实例）。由此可以创建经济的规模化可执行计算，只用提交到根链上的一个区块头/哈希就能包含非常多的数据和工作。只有当一个区块是错误的，才会发布无效证明，否则周期性地在根链上提交数量极微的数据。

我们提出的方法是，让映射阶段包含计算用数据作为输入，在归约阶段，在返回结果时包含一个梅克尔化状态转变证明。梅克尔化状态转变是通过在根区块链上构建的欺诈证明执行的。也可以构建关于状态转变的 zk-SNARK 证明。对于某些计算结构而言，归约步骤中可能还需要关于一个关于状态转变的位图（因此这些用例的每个 UTXO/账户可能要使用不止一个位）。

我们的结构在有时间或速度取舍的情况下实现了极高规模的计算。这些取舍产生了一个网络，网络中的节点断言计算和参与者负责验证它们。如此不会产生一个不支持无信任完全外包计算的系统，只是激活了将计算压缩到保证证明中的能力。这些保证证明鼓励参与者只诚实证事。这也遵循闪电网络中的评语，如果一棵树倒在森林中并且无人倾听它发出的声音，则假定无论此树是否发出声音都不要紧。

同样，如果没人监督/执行运算，则假定运算是正确的或者结果如何根本没关系。开放网络中的任何参与者都可以监督计算，但周期性监督链以确保正确性的则是持有余额和/或要求正确计算的参与者。之所以具备扩容优势，是因为它允许人们不监督对其不造成经济影响的链，只需监督其想要对其执行纠错行为的链即可。在其他 Plasma 链上的行为可以作为归约步骤的组成部分被一起扣除，于是可用最小状态表达对某人有影响的计算。例如，在一个去中心化交换中，人们不关心哪个对手下了什么订单，他们只需要看到一个聚结订单簿，于是他们只需要将所有其他链视为一个对手，他们自己的链被充分验证以执行交易并且向正确的人（包括他们自己）按单供货。另一个例子是人们可以在 Plasma 链树上构建 BBS 并且不需要接受关于自己不关心的主题的更新。

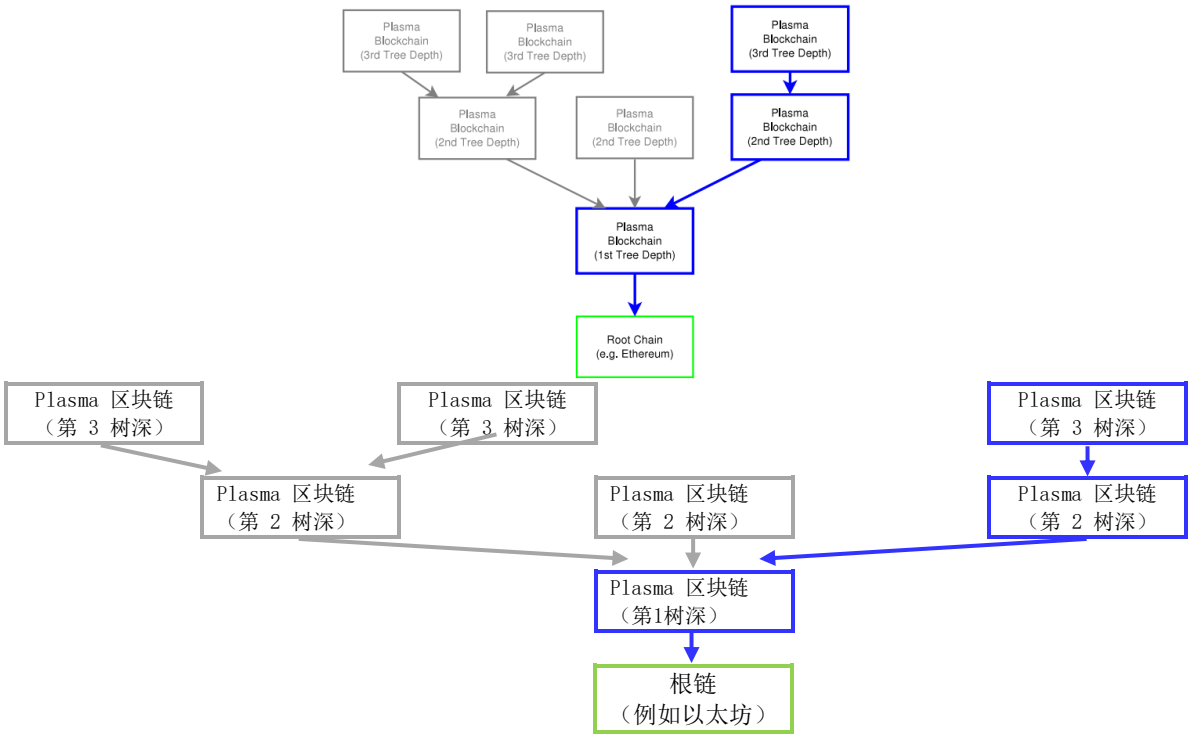

图 8：人们只需要监督其想要执行的数据。如果其它 Plasma 链上发生了不必执行（灰色）的经济活动或计算，可以将所有其它链当作一个对手对待。例如，在一个 Plasma 去中心化交换中，人们只需要监督可影响其承诺的链（加粗蓝色）。

2.5 关于持续去中心化区块链的经济激励说明

利用我们设计的结构，人们可以创造经济激励以持续驱动子区块链运行。对于不需要状态转变高度复杂或依赖的状态，原生代币（例如，ETH 反映以太坊）可被用于保证状态。然而，对于复杂合约而言，因为有旨在确保系统活跃性和订单公正性的激励，所以可能存在很强的、可以驱动链继续运行的激励 [8] [9]。

每个 Plasma 链以一个合约集表示。这些合约执行链共识规则，且若可出具欺诈证明，欺诈行为将招致严重处罚。

然而，为激励人们规避拜占庭状态，特别为了保证正确性和活跃度，为每个合约创建一个代币可能是理想之选。此代币反映网络运行合约的效力，创建激励以实现合约的安全性最大化。因为 Plasma 链需要代币来保护权益证明结构中的网络，所以权益人受到抵制拜占庭行为或错误的激励，因为后者会导致代币价值损失。代币的作用是确保如果验证人经由反映价值下降行不义之事，则存在对其本地化的成本。

利用简单的合约和业务逻辑，诸如基本合约帐户代表其用户持有资金，以太坊的保证可以在Plasma 链中反映权益。

挂出保证（无论是代币还是 ETH）的权益人有继续运行网络的动机，因为他们收取交易费用以运行网络。然后，这些交易费被支付给网络的权益人，进而鼓励非拜占庭行为且为代币创造长期价值。

由于权益人有继续运行此网络以收取交易费的动机，他们将持续运行链，并受到根区块链合约定义的欺诈证明的制约。

3 设计堆栈和智能合约

历史上，许多人认为区块链最好的用途是充当交易性支付的全额结算系统。然而，全额结算系统扩容困难。净结算设计，如闪电网络，作为一个支付通道网络，通过改变结构允许参与者之间发生近乎无限的支付。因为通道是在区块链上净结算的，所以交易能力大幅提升。支付可以在这些通道网络上沿路线传送。

该结构还支持有效的瞬时付款。这不但对高度时敏的支付至关重要，对合约也是。

Plasma 的设计不求快速达到有保证的定局，即使交易在子链中被快速确认，它要求其在底层根区块链中定局。通道有必要具备快速对支付和合约定局（链上可执行）的能力。

在智能合约中存在“自由选择问题”，即需要智能合约要约的接收人（第二或最后一个签字人）签署并且广播此合约以令其执行 - 在此期间，合约的接收人可能会将此视为一家可以自由选择的事情，可能因为自己对此活动不感兴趣而拒绝在合约上签字。智能合约在对待不可信任的对手的时候最有效（因为这会导致对手风险最小化，进而导致信息成本最小化），因此加剧了这个问题的严重性。

Plasma 自己无法解决这个问题，因为区块链中交互协议的第一和第二签名步骤的原子性是没有保证的。

借助闪电（包括在 Plasma 上方的闪电），可以在保证合理的本地化终局感的基础上，执行快得难以置信的更新。没有给予最后方余地的单笔支付，一笔支付被分成许多小支付。此法解决了每个切分片段的金额的自由选择最小化问题。由于智能合约的第二方只对切分片段中金额有自由选择权，所以自由选择权的价值被降至最低。

在上述的用例中，闪电可以是位于 Plasma 上方的快速金融支付/合约主接口层，因为 Plasma 允许只用最小的根链状态承诺进行帐本更新。

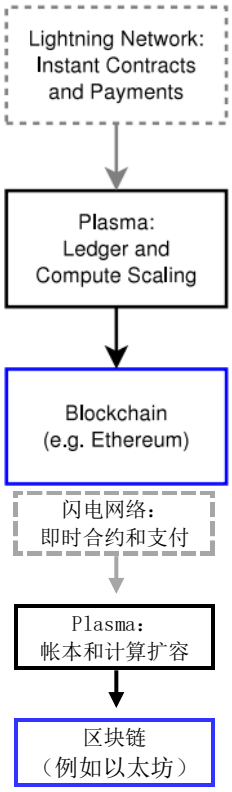

图 9：位于根层的是区块链，它是合约和支付的判决层。合约本身位于根区块链。Plasma 链包含当前帐本状态，后者可以在根区块链上结算和赎回。欺诈证明的存在目的是允许资金被赎回。Plasma 反映一个嵌套 Plasma 链集以创建通过最小区块链交易，以可扩容方式提取资金的场所。顶层是闪电网络，它允许跨 Plasma 和区块链实施瞬时支付。

3.1 分片最严重的问题是信息。

数据集被切片之后，碎片个体拒绝披露信息的风险很大。这将导致欺诈证明无法生成。

我们尝试用 3 个策略来解决此问题：

1. 采用一个新的权益证明机制来鼓励区块传播。底层机制并完全依赖激励的纠错功能，但是这应该能显著减少错误行为。

2. 取款延迟明显，确保取款证明的准确性。个人无需如此频繁地监督 Plasma 链，任何位于相同 Plasma 链上的、以用户身份存在的诚实行为人，都可以在跟区块链上预防更高 Plasma 链上的欺诈。若发生扣块事件，Plasma 链可以立即凭借证明来锁定资金，防止攻击者提交伪造的取款证明。若攻击者试图提取高于其限额的资金，则更多的资金会被锁定，发起攻击的 Plasma 链将失去其存款。

3. 创建子链，让交易可以在任何父链中传播。出于这个原因，网络上的参与者将希望将交易提交到深子链。这样可以为没有经济实力支付根区块链上高额交易费的较小余额创建经济效率，因此可用很多小余额来实现资金移动。因此，鼓励人们创建反映显著价值的、深度嵌套子链。注意，有些人在选链方面的名声有待商榷，他们持有非常小的、无法位于根区块链上的余额；不过交易费却因为拥有深嵌链而缓解。Plasma 链的新颖性主要体现在这个安全模型上。

4 相关工作

有些相关项目使用梅克尔树，将归约步骤作为计算证明，然而这种方法主要关注的是数据可用性并且鼓励以欺诈证明为中心实现成本最小化，通过一个协议，经由有经济激励的、持续的切碎链组管理这些问题。

其他相关项目提出子区块链系统，但方法差异较大。

Plasma 使用梅克尔证明以执行子链。

4.1 TrueBit

Plasma 在欺诈证明的依赖方面与 TrueBit 有很大的相似性 [10]。欺诈证明结构与 TrueBit 类似，几乎所有由 TrueBit 执行的工作都可以直接应用到 Plasma，特别是关于状态转变的梅克尔化证明工作。

TrueBit 的设计允许创建简约证明以提交给 Plasma 区块链，这对 Plasma 而言是有必要的，所以几乎所有由 TrueBit 文书和团队承担的重吊工作都可以直接应用在此设计中。使用能生成梅克尔化证明的验证环节 (Verification Game) 能够降低计算规模，算是锦上添花。与 TrueBit 类似的假设应用，即计算状态必须是可计算的并且是可在线广播的（大片数据必须经过多回合拆分），数据可用性问题需要缓解，失败必须披露。我们试图弱化这些问题，特别是后两者。

Plasma 试图在 TrueBit 上构建的主要事物是需要在共享状态下计算的多方参与者概念。例如，一组参与者仅关心一个子集的数据和计算，只需要计算与自身相关的方面（例如 BBS 或交换）。我们还试图经由链下执行场所来弱化计算回合的执行问题。

4.2 区块链分片

当前区块链分片工作 [11] 使用类似的技术和目标，例如以太坊分片方案。此结构作为较高层，可能兼容。如果根区块链被分片，那么 Plasma 链可以在其上运行以提高可扩容性且发挥其他优势。这样也可以作为不同分片技术的测试平台，因为在以太坊和其他富状态区块链在开始基本操作之前不必改变共识。

4.3 联合侧链

Plasma 不是联合侧链[12]，因为它不依赖联合会以实施诚实活动，也不完全依赖受信任行为人在链中执行状态。Plasma 还将帐本状态外部化到另一个区块链上，允许使用相同的币/代币，但是，如果欺诈证明可用，Plasma 会实施可执行验证。Plasma 并不依赖强大的行动人联合会，因为这些行动人的正确性有重大承保风险，因此 Plasma 不是与联合会挂钩的侧链。

驱动链 [13] 与联合侧链有相似性，但验证人是一个未知的、不断变化的参与者（矿工）集，去中心化程度更高。

4.4 合并采矿区块链

例子包括 Namecoin，它用父区块链创建并发区块 [14]。这个做法假设对区块链完全验证，因此没有可扩容这一优点。扩展区块就属于合并采矿链，后者允许资金在主区块链和合并采矿链之间移动（有全矿工集的执行机制，作为根链上的共识规则）。合并采矿链允许新建共识规则和选举用户，从而允许用户只验证他们关心的链，但矿工/验证人必须验证所有链。Plasma 的目标是确保只有用户和矿工才需要验证与自己相关的链。

4.5 树链

树链 [15] 主张使用树结构区块链，使用工作证明在子区块中对其进行验证。根链拥有所有子区块链的总计工作证明。堆栈较下层有更高的安全性，堆栈高层是否取决于验证和工作的级别则不一定。虽然树链的拓扑结构是树结构，但其结构依赖于经由分支求和的采矿安全性。在这个安全模型中，叶子上的安全水平较低，因为它是受工作证明保护的。采矿时，只有根是完全安全的，安全性和证明从根流出，Plasma 则正好相反。构建树形图中所示区块的证明做法类似。

4.6 zk-SNARK 和 zk-STARK

非交互式计算证明提供可扩容计算的巨大优势[16]。zk-SNARK/STARK 和其他形式的非交互式简约证明与 Plasma 互补。可以随梅克尔计算结果一起提供证明。另外，其他优势包括，可以减少子 Plasma 链中持有小余额遭受的系统性攻击。关于 MapReduce 功能的 SNARK 研究已经开展 [17]，我们希望这种利用该研究和 Plasma 可以通过使证据在一组区块链中可以排序和执行来扩展。

进一步好处包括计算证明，计算证明可加快同步速度并且验证链本身。请注意，zk-SNARK 不能解决有关数据可用性的问题，只能减少数据要求量和计算量。zk-SNARK 可以充当任何基于断言/质疑时间的机制的替代或补充，特别有用。 zk-SNARK 可以发挥深入防守的作用。如果最后一道防线是在不用酷炫加密术的情况下使用区块链，则第二道防线可以是 zk-SNARK，第一道防线是受信的计算硬件。

从 Plasma 链取款时可以利用 zk-SNARK 来提供保护，好处在于可以选择不用位图，从而可以转移非常小的余额。

4.7 Cosmos/Tendermint

Cosmos [18]在 Cosmos“中枢”中排列区块链，并且通过权益证明系统对子区块“区域”进行验证。与子区块链结构存在显着的相似性，但是 Plasma 依赖施工欺诈证明来执行子链中的状态，并被泛化以应用于许多链。Cosmos 的权益证明结构假定验证人中诚实的大多数占 2/3，其中包括其 Cosmos 区的验证人。

4.8 Polkadot

Polkadot [19] 也构建了一个区块链层级结构。与 Polkadot 的设计有一些相似之处。我们构建了一系列通过梅尔克证明执行状态的子区块链，而不是一个通过“渔民”验证人来确保区块正确性的结构。Polkadot 结构依赖于由渔民执行的子区块链（“parachains”）状态和信息可用性。

4.9 Lumino

Lumino [20] 是一个 EVM 合约的设计，区块链上有压缩更新。这允许参与者只更新最小承诺状态。Plasma 的输出管理设计的进步在于只用一个位元来代表一个特定的输出。出现子 Plasma 链故障时，这种设定可以支持快速的、低成本的集中取款协调。

5 多方下链状态

目标是构建一种方法，使参与者可以在没有有效上链状态时，持有位于区块链的原生底层币/代币中的资金。Plasma 开始模糊上链和下链之间的界线（例如是链上分片还是链下分片）。

建立跨区块多方通道有两个共同的问题。第一个问题是在需要对系统进行更新（或对全局状态更新的可用性进行折中）时，需要同步所有参与者之间的状态更新，因此必须在线。第二个问题是添加和删除通道中的参与者需要大规模区块链上更新，穷举所有被添加和删除的参与者。

相反，最好的方法是建构一个机制，可以在不需要大量根链状态更新和内部状态更新的情况下，就添加和删除许多参与者，而且不用所有方都参与，参与者只有在自己的余额被调节或侦查到拜占庭行为时才有必要参与。

一般结构是一个子区块链，它允许在根区块链（例如，以太坊）上持有智能合约中反映的余额。智能合约的余额被表示并分配到子 Plasma 区块链中已完结区块的余额中。这样就可以让子区块链持有本币，在根区块链上充分反映余额，支持争议调解期后取款。

为了达到这些目的，我们为帐本构建了 UTXO（Unspent Transaction Output，即未支出的交易输出）模型。虽然这不是一个明确的要求，但是通过快速取款更容易理解。UTXO 模型的原理是要简明地反映某特定状态是否已经被支出是很容易的。这可以表示在前缀树内作梅克尔化证明，以及作为其他人解析的简约表示的位图。换句话说，智能合约是在根链上的帐户上进行的，但是 Plasma 链则维持了一个 UTXO 的一组余额，用于分配在根链帐户中持有的余额。有些子链对于状态转变没有明显的要求，所以可以使用帐户模型来处理更为复杂或频繁的状态转变，但是对父区块链的区块空间可用性的依赖性较大。

现在，可以假设一个单独的领导选择一个子级别的链。可以将其构造为标记证明集或已命名的预设 n/m 验证人，但在这些示例中，为简单起见，我们使用单个已命名验证人。验证人的作用是提供用于排序交易角色的块。验证人/提出者受到根区块链合约中构建的欺诈证明的限制。如果他们传播一个无效的状态转变的区块，任何其他接收该区块的参与者都可以在父区块链上提交一个梅克尔化欺诈证明，无效的区块带着经过减刑的处罚回滚。

这些区块被传播给希望观察这些区块的参与者，包括持有余额或希望在单个 Plasma 链上观察/强制计算的参与者。

尽管维护下链状态的存款复杂性很小，但状态转变和取款却令复杂性增大。

5.1 欺诈证明

该子区块链中的所有状态都通过欺诈证明执行，允许任何一方执行无效区块，并假定块数据可用性。

然而，这种结构中最大的困难是数据/块可用性没有明确的保证。

根区块链（例如以太坊）中有一组欺诈证明，这些证明可以确保有块数据可用时，所有状态转变都是有效的。对于复杂的计算，状态转变必须被梅克尔化以实现有效的验证。

另外，状态转变也可以通过 zk-SNARK/STARK 来执行，后者杜绝了不当退出。zk-SNARK 结构可能需要递归的 SNARK 以发挥最大功效，因此可能需要对可能性做进一步研究。然而，按照设计，此系统不需要搭配 SNARK 就能独立工作。

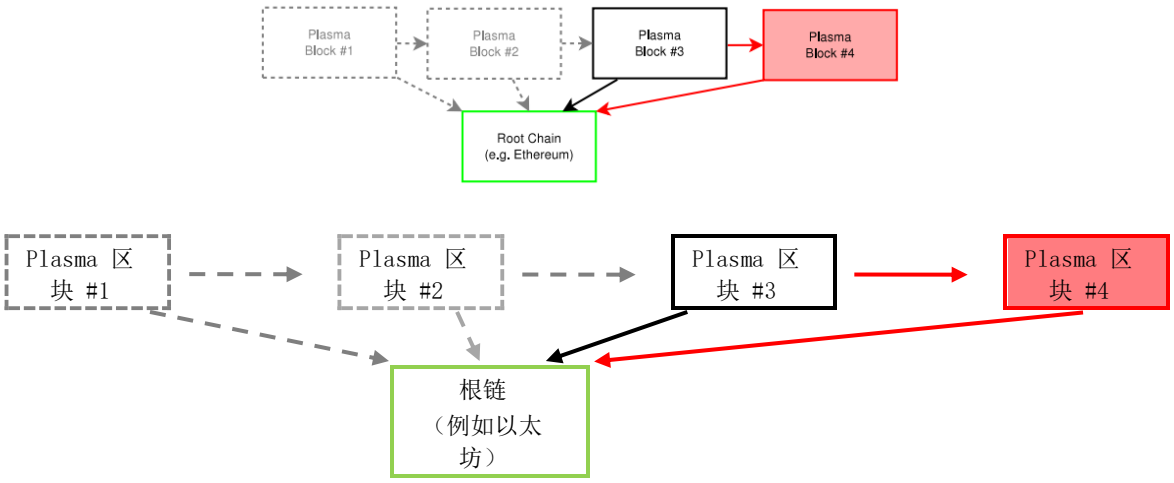

图 10：每个人都有区块 1-4 的块数据。区块 4 中的梅克尔化承诺和来自前一个区块的数据可以证明区块 4 的承诺化状态转变具有欺诈性。

欺诈证明确保所有状态转变都得经过验证。示例欺诈证明是交易支出的证明（资金在当前的 UTXO 中可用），状态转变证明（包括检查签名可以支出输出的能力，跨块的纳入/排除证明以及存款/取款证明）。有些较复杂的证明需要一个互动环节。一般结构是采取函数性方法来处理区块验证。如果以固态编写这种共识机制，则被验证区块的梅克尔证明的每个函数都有一个额外的输入，输出将返回验证是否有效。然后，只需复制共识验证码，就可以简约的梅克尔化证明的形式对其进行处理（从而不需要处理整个区块以生成欺诈证明）。

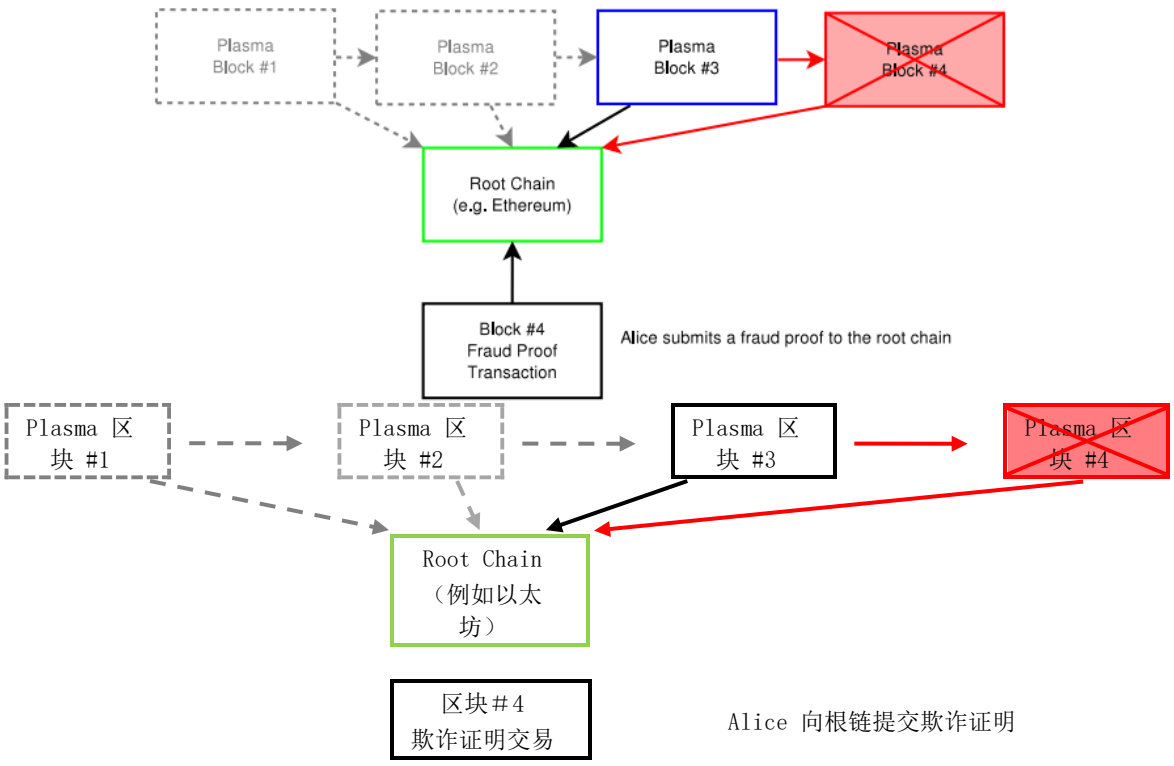

图 11：Alice 拥有所有区块数据的副本，因此她在根链上提交欺诈证明。区块 4 无效并回滚。区块 4 的提交者因失去智能合约中的保证而受到处罚。当前区块变成了区块 3（蓝色）。约定的时间过去之后，区块被定局，无法提交欺诈证明。建构活动只能发生在不能通过完全验证区块来证伪的区块上。

为了让这个结构具有最小证明，所有区块必须提供一个承诺到当前状态的梅克尔前缀树、已支出输出的前缀树、交易梅克尔树和被改先前状态的索引。

欺诈证明确保参与者联合会无法在不受处罚的情况下创建欺诈区块。如果欺诈区块在根区块链（或父 Plasma 链）上被检测出且被证实，则无效区块被回滚。此机制鼓励个体参与者抵制拜占庭行为，从而解决了与联合会挂钩的比特币侧链中存在的状态转变脆弱性问题。

结果是 Plasma 区块链中可执行高度可扩容的状态转变，同时确保了有权访问区块数据的观察者能够证明（并因此能够阻止）无效状态转变。换句话说，只要根链上有周期性承诺，支付就可以发生在这个链中。

5.2 存款

来自根链的存款直接发送到主合约中。此合约负责跟踪当前状态承诺，使用欺诈证明对无效承诺进行处罚以及处理取款。由于子 Plasma 区块链是根区块链的完全验证人，所以必须使用两阶段锁定来处理传入交易。

存款必须包括目的地链区块哈希以指定目标子链，利用多步骤过程实现以确保币不可恢复。

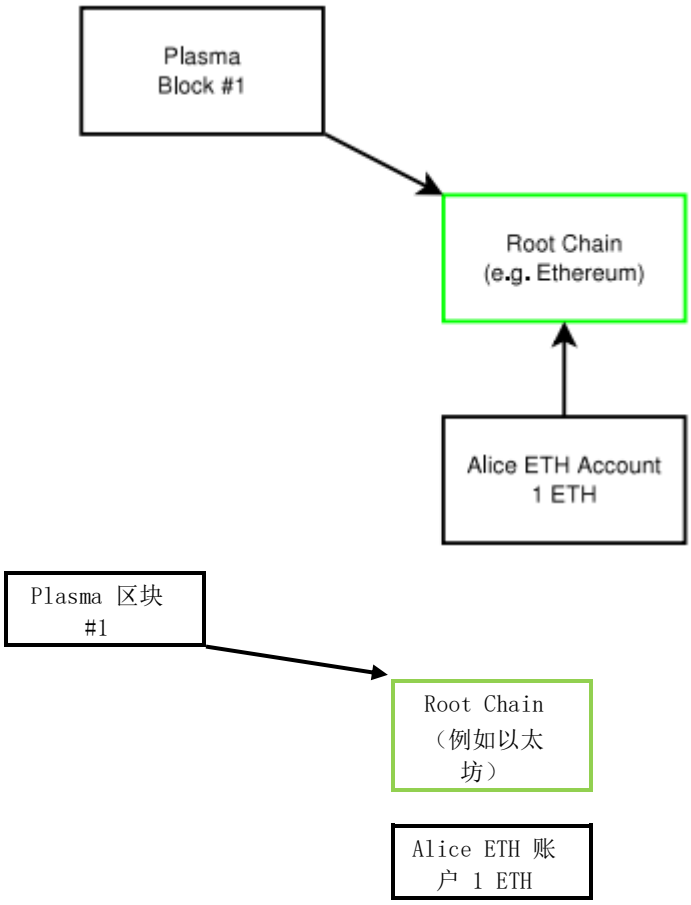

图 12： Alice 拥有 1 个 ETH 账户。她想把它发送到 Plasma 区块链中。她将其发送到 Plasma 合约中。

1. 将币/代币（例如 ETH 或 ERC-20 代币）发送到根区块链上的 Plasma 合约中。币可以在为质疑/响应而设定的时间段内被回收。

2. Plasma 区块链包含一个进入的交易证明。此时，Plasma 区块链承诺交易是进入的，它将在存款人发起锁定交易或支出的情况下变得可支出。当其被包含在内时，区块链承诺其将履行取款请求。但是，因为尚且没有确认存款人有足够的信息可以生成欺诈证明，所以尚未有来自存款人的承诺。此区块包含状态树、位图和交易树中的添加，因此存在正确纳入的紧凑证明。

3. 存款人签署子 Plasma 区块交易上的交易，激活此交易，其中包含一个承诺，声明基于链的第 2 阶段承诺，他们已见过此区块。这个阶段的作用是让存款人证明他们有取款资金所需的、足够的资料。

在此过程后，链已经承诺他们将处理这些币并给予分配，所以取款可以被简约地证明。在第 3 阶段，用户证明了他们可以取款的事实。

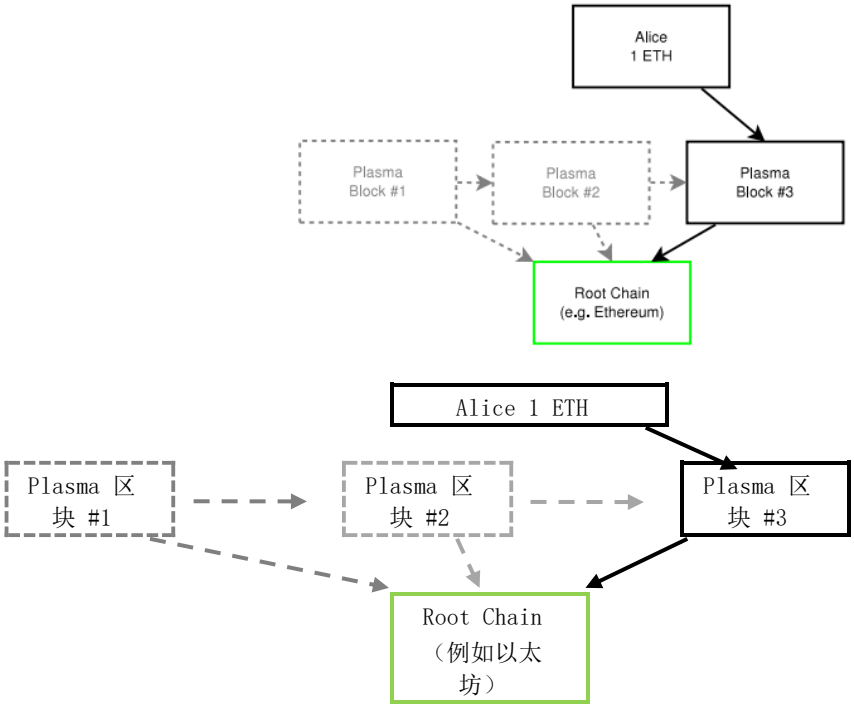

图 13：Alice 现在在 Plasma 区块中有 1 个 ETH。她已承诺她看到了资金，而且资金现在被锁定了。这些资金被保管在根链上的一个智能合约中，但帐本记录是在这个特定的 Plasma 区块链中，（因此，状态转变，即发送资金给他人或智能合约）可能可以在不产生高额的根区块链路费用的情况下产生。

如果存款人没有通过第 3 阶段，那么存款人可以尝试在根区块链上取款。存款人提交未确认的取款请求，必须多等待一段时间以便网络上有人出示证明存款人已经签字并且锁定 Plasma 区块中资金的欺诈证明。如果没有证明，存款人可以取款未确认的资金。这种取款需要相当大的根链联结以确保非拜占庭行为。

5.3 集中取款和位映射状态

该系统的主要问题在于无法验证状态。

为了能够进行状态交易的最大压缩，可以选择在位图中表示输出。这对于因为过于昂贵而无法在根链上执行的取款证明是必要的。这种结构旨在允许在 Plasma 链上保持小余额。这些余额在根区块链上的合约中全额保留，但全帐本不在区块链。需要缓解的主要攻击是被扣留的无效区块（对根链的承诺）。若系统观察到无效状态转变，参与者执行集中交易退出。

利用位图结构，取款包含一个希望退出的已签名交易的位图。构建环节/协议，由智能合约执行以确保信息无误。此位图确保每个人都能够明白支出了什么输出。

由于这是一个位图，因此需要在未支出的交易输出数据结构 (UTXO) 中表示状态，以发挥小价值余额的最大功效。支出性可以简约地证明，大量状态转变可以干净地执行。在预定义的结算时间段之后，这些位可以重新被使用。

昂贵的高保证到廉价的低保证之间存在一个梯度：

1. 帐本状态在根区块链上
2. Plasma 上的帐本状态，执行单笔交易在经济上可行
3. Plasma 上的帐本状态，使用位图（1-2 位成本）执行在经济上可行
4. Plasma 上的帐本状态，使用根区块链上的位图执行在经济上不可行。1-2 位集中取款费用太高。

持有可在根链上执行的余额者，不需要执行 UTXO 位映射格式。但是，对于持有余额的人而言，只有当根区块链的 1-2 位交易气体/费用足够低时才可执行。

对于第 4 类（1-2 位链上集中取款的成本太高），系统依然要保留弹性（尽管有一些假设称已命名实体是可靠的）。本文的后面部分描述了一种层级化的区块链结构，可以创建许多可以经济地进行集中提款的场所。另外，如果第 4 类交易的总价值明显低于代币价值，由于代币持有人名誉受损，所以按照博弈理论可以推断攻击这些余额代价太大。

5.4 状态转变

默认情况下，Plasma 链中的状态转变按照与存款类似的多阶段过程运行。这是为了确保用户有可用的信息来提供状态转变。然而，与存款结构不同，一旦交易被签名并包含在一个区块中，就有承诺以参与。为此，状态转变应包括签名、状态更新（例如目的地、数量、代币和任何其他相关联的状态数据）以及某种类型的、过期用 TTL 和一个对特定区块的承诺。此 TTL，虽然不是必需的，但应低于构建退出证明的时间以确保对抗退出条件已知。预签名的交易当然不应该包含 TTL。这种结构有弱活跃性假定，因为退款已经有了关于深层次的取款活跃性假设。对区块的承诺是支出者所做的承诺，在 Plasma 链中广播交易的实体已经观察到了上至此点的链，能够执行证明并且必须位于已发生支出的区块之后。

快速定局的多阶段的承诺如下：

1. Alice 希望将她在 Plasma 链中的输出支出给位于相同 Plasma 链中的 Bob （没有在区块链上提交完整的交易记录）。她创建了一个交易，将她的其中一个输出支出在Plasma链中，签名并广播交易。

2. 交易被 Plasma 链的验证人包含在区块中。头部作为区块的组成部分，被包含在父 Plasma 链或根区块链中，最终被提交且密封在根区块链中

3. Alice 和 Bob 观察交易并签署承认书以确认他已经看到了此交易和区块。此承认书被签名且包含在另一个 Plasma 区块中。

对于慢速定局，只需要进行第一步。

承认书发生后，交易被认定为已定局。第 3 步之所以存在，是为了确保参与者（Alice 和 Bob）具备区块可用性。步骤 3 不是必需的，但没有步骤 3 会导致定局严重延迟。理由是在区块的有效性和信息的可用性可以被交易相关的所有各方证明之前，交易不应被视为已定局。

若区块在第 1 步之后被扣留，Alice 不清楚她的交易是否已被支出。如果交易已被包含在一个区块中（无论是否被扣留）并且步骤 3 尚未定局，则将其视为未确认。因此，如果 Alice 还没有签署承诺，她仍然可以取款这些资金，只要她在根/父区块链上的提款消息发生在区块定局之前。Alice 不能在区块定局后取款资金，区块被推定发送给 Bob。如果在定局之前区块被扣留（在步骤 1 和 2 之间）并且 Alice 和/或 Bob 观察到了这一点，则 Alice 可以取出她的未定局资金。如果区块在步骤 2 之后、步骤 3 之前被扣留，那么推定 Bob 有足够的信息来取款资金，但由于 Alice 和 Bob 都没有完全承诺支付，所以被认为不完整，根据信息的可用性，任何一方在理论上都可以申请资金。如果双方在第 3 步签字，则认为是真正定局。支付到合约哈希 (Pay-to-contract-hash) [21] 执行发生在此步骤定局之后，具体时间是当签名在链上被可证地观察到时。如果一方拒绝签字或区块被扣留，则须以兑现证明为条件。由于所有状态最终经由梅克尔证明被承诺到链上，对支付到合约哈希的依赖性较少，因为在定局之后，支付是可证且可执行的。

注意，步骤 3 执行与否可以取决于智能合约而非双方签名，即状态以 HTLC 释放原像为条件。因此，有多链或多交易原子性可用。合约创建的复杂性可能会增加，如果需要这些特征，可能需要编写更高级别的语言/工具。

5.5 对根链的周期性承诺

Plasma 链必须能够创建区块链序列。在 Plasma 链中，区块内有排序，但是区块未被证明并且自行排序。因此，有必要在根区块链上创建一个承诺。Plasma 链在根链上发布其区块头，其区块头被欺诈证明执行。如果发布对其他人有数据可用性的欺诈区块头，则任何其他参与者可以发布欺诈证明和承诺，区块被回滚，发布者受到处罚。

这些承诺允许真正地排序，而不需要稍后等待。如果尝试疑义，就存在充分的欺诈证明，可以被处罚。在一段时间之后，区块被定局，因此只要根区块链也达到足够终局性，就不能被重新排序。

5.6 取款

Plasma 允许人们脱离根区块链存入本币和代币（即 ETH 和 ERC-20 代币）资金。只要有信息可用性，它还允许状态由根区块链执行的 Plasma 区块链内发生状态转变。如果发生信息可用性失败，需要在此 Plasma 链执行集中退出。最后，也可以简单地取出 Plasma 链中持有的资金。

但是，在正常运行中，可以执行简单取款操作。

5.6.1 简单取款

执行简单取款时，只能取出承诺在根区块链中并且最终在 Plasma 链中定局的资金。

我们描述了存款设计、简约分配了帐本状态和状态转变。直到这个阶段，除了欺诈证明之外，根区块链上还没有发布当前的 Plasma 帐本状态。但是，取款时，需要一个反映 Plasma 链中持有资金而且是流动资金的具体证明。

取款是最关键的组件，因为它确保了根区块链与子级别链之间存在币的可替代性。如果能够将资金存入 Plasma 链中，则可以进行状态转变（即向其他方转移币），其他方能够取出资金，然后其价值应密切映射到根链上的币价值。在某些情况下，Plasma 的资金可以变得更为有用，因为它具有更大的交易能力，安全性则最终取决于根链。

简单取款时，所有资金都需要大保证，所有取款请求都必须包含大保证作为欺诈证明。如果当前区块数据可用，则第三方可以非常低的成本提供此证明，因为第三方服务可以验证 Plasma 区块链活跃并确保取款证明有效。

Plasma 链的所有参与者必须验证所有父 Plasma 链和根区块链，以确保在更新状态时特定帐户/输出中不存在正在进行的提款。如果取款正在进行中，后续的区块将不能支出币/代币，这里的任何拜占庭行为都违反了共识并且要遵照根区块链中的 Plasma 合约出示欺诈证明、接受处罚和区块逆转。

取款发生在以下步骤中：

1. 已签名的取款交易被提交到根区块链或父 Plasma 链。被取款的金额必须是全部输出（无部分取款）。多个输出可能被取款，但它们都必须位于同一 Plasma 链内。输出位图位置作为取款的一部分被公开。附加保证作为取款的组成部分置入，用以处罚虚假取款请求。

2. 存在预定义的超时期限以允许争议。这与闪电网络的争议时期相似。在这种情况下，如果任何人可以证明被取款（至区块链，很多情况皆如此）链中的输出已被支出，则取款被取消并且绑定取款请求丢失。任何观察链的人都可以提出争议。如果提供了支出输出的欺诈证明，则保证将丢失，取款被取消。

3. 存在第二次延迟以等待任何具有较低区块确认高度的其他取款请求超时。这是强制在特定 Plasma 链或根链中的有序取款。

4. 如果 Plasma 智能合约中定义的约定争议期限已经过去，但根链或父链上没有提供欺诈证明，则推定取款是正确的，取款者将能够在根链/父链上赎回他们的资金。根据 UTXO /帐龄，取款按旧到新的顺序处理。

请注意，只要经济上可行，Plasma 链中发生扣块攻击时也可以取款。

欺诈证明仅要求网络上的人证明同笔输出有重复签名的支出，这一点可以被简约证明。对于闪电和其他状态通道，额外的要求还必须证明较高随机数。对于通道，如果尝试较低随机数取款，则资金将保留在 Plasma 链中，可以接受正确签名取款。其他结构也是可能的，但设计可能需要作为为 Plasma 链创建智能合约欺诈证明的组成部分而被前端加载。

由于正常的取款是一个缓慢而费钱的过程，它们很可能被聚结成一个取款或者其他人愿意使用闪电或原子交换 [22] 来交换其他链的币。

5.6.2 快速取款

快速取款与简单取款的结果相同，但资金会被发送到进行原子交换的合约。被交换的资金是根链/父链上的、带低时锁的资金，用于交换带高时锁的退出 Plasma 链的资金。

快速取款不是即时取款。然而，如果 Plasma 链不是拜占庭式（包括进行扣块），快速取款可以显著缩短取款时间，取款时间相当于提供交易终局性所需的时间。因此，扣块攻击期间无法进行快速取款交换，反之有必要发出缓慢的集中取款请求。

快速取款发生在以下步骤中：

1. Alice 想把资金取款到根区块链，但不想等待。为了方便，她愿意支付时间价值。Larry（流动性提供者）愿意以服务形式提供这种便捷。Alice 和 Larry 协调以撤回至根区块链。该 Plasma 区块链被假设为非拜占庭式的。

2. 资金被锁定到 Plasma 链的特定产量的合约。这出现的方式与标准的转移的相似之处在于，双方播送交易之后承诺其在 Plasma 区块中已看到了交易。合约的条款是，若合约在根区块链上被播送并且已经终止，则付款将通过 Plasma 链。若无交易证据可以提供，则 Alice 可以赎回资金。也可通过让 Alice 生成一个原像，且仅在她认为可接受后发布来将此构建为 HTLC

3. 在上述 Plasma 区块定型，并且 Larry 有信心在满足合约条款的情况下能够赎回资金之后，Larry 创建关于链的合约，使指定数额的款项（他将会收到的数额减去他为此服务支付的费用）被支付给 Alice

在我们的示例中，流动资产提供者 Larry 必须处于活跃状态并且充分验证 Plasma 区块链才能接受该交易。若 Larry 不能充分验证 Plasma链（或者不熟悉根链中所定义的智能合约欺诈证据），他就不该进行撤回。若 Larry 不想要该链中的资金而宁愿要根区块链上的资金，则其可以在此完成之后发起撤销，或者进行原子交换作为撤回本身的一部分。

在多数情况下，与流动资产提供者结算的 Plasma 区块链之间的转移可能更具成本效益。转移可以通过允许快速定局的闪电或原子交换在 Plasma 链之间发生。

由于这是一种链间的原子交换，Alice 和 Larry 并未给予对方资金的保管信赖。Alice 将她的资金置于根/父链之上，而 Larry 将能够在今后的某个时刻完全访问根/父链。假如低成本的区块可用，而根区块链的非拜占庭式的行为已尘埃落定，那么即使 Larry 不信赖 Plasma 区块链本身，他也可以对其将获得资金持有相当的把握。

5.7 对抗性的大规模撤回

尽管对抗性的大规模撤回交易在 Plasma 的框架之内，协议对此并无要求，其设计主要是为了扣块情况下的状态经济稳固（较少的气体/费用）。若某人希望使用 Plasma 链内部的账号状态，则其也可以依托其他设计，如付款的等级。此外，注意此处使用了 UTXO 模型，但该系统仅在根链使用账户模型的情况下才能有效工作。再者，若大规模撤回不是必要或想要的特性，可以将账户模型用于持有 Plasma 链中的资金且仅顾及简易的撤回（随着递增序号）。

由于 Plasma 设计的首要考虑涉及到扣块攻击以防止欺诈证明（等数据可用性缺乏的暗示），需要迁移用于检测到的数据无效性。当用户在 Plasma 链上检测到区块无效时，参与者在特定日期离开该链显得十分重要。在未及时退出链的情况下，后果类似于未抗拒闪电中的错误撤回。该机制是正确操作 Plasma 区块链的关键。Plasma 赖以存在的事实是，若用户通过扣块检测到拜占庭式的行为，则该用户负有退出 Plasma 区块链的责任。其中的基本原理是，根区块链上不可能检测出某一区块是否正在被扣押（要么用户能够断言其从未获得区块，要么 Plasma 链能够断言该用户拒绝承认该区块可用且在说谎）。结果，用于已断言区块无效性的成本已按照惯例被推定为揭露了当前的链上状态（也就是闪电所做的）。然而，对于大区块和状态过渡而言，这可能贵得难以置信，而 Plasma 并不使用该结构，毕竟谁负责支付这些费用尚不明确。相反，Plasma 假定，若用户认为 Plasma 区块链在对抗性地扣押区块并且可能影响今后执行状态过渡的性能，则人们就应当尽快退出该 Plasma 链并进入下一条 Plasma 链。

因此，只要某一区块不可用，则假定 Plasma 链为对抗性或拜占庭式的，这就被定义为对抗性的大规模撤回。大规模退出确保了 Plasma 链的拜占庭式行为不在重要的延时以及停止链之外影响一个人的资金。

假定使用 SNARK 的附加安全缓解将在今后使用，但具体设计仍为开放性问题。假如观察者有周期性的活跃度，该结构并不有赖于用于撤回的 SNARK，然而通过在 Plasma 链内实施状态过渡，使攻击性或拜占庭式 Plasma 链能够进行对抗性的扣块以从那些并不周期性地观察 Plasma 链的观察者窃取资金的能力可以被 SNARK 回路的安全性能尽可能地削弱并施行。在那种情况下，它将需要 SNARK 证明进行状态过渡以及用于撤回的 SNARK 证明，以获得状态过渡的更大把握。然而，假如用户正在观察链，Plasma 的目标并不依赖于 SNARK 以做出状态过渡的正确行为，智能合约正确地对这些机制作了编码，并能够在根区块链上撤回。通过确保链下状态仅在由第三方提交的关于支持智能合约的链的递归性 SNARK 证明中可行，在确保正确的当前状态中，类似的效益可以为闪电网络而存在。

Plasma 链的安全性可以通过深度防卫得以保证，需经过具有安全要素/硬件的第一防线、具有 SNARK/STARK 的第二防线、以及终极防线（即链上交互式游戏）。其中，第一防线可能失败，但第二防线使用新颖的密码术确保其安全，而终极防线采用具有公众透明度的交互式游戏。我们最初认为 Plasma 是使用终极防线的系统。

通过创建交互式游戏来实现大规模撤回，从而退出以如下方式发生：

1. Alice 与其他人在 Plasma 链上配合执行大规模退出。众多的大规模退出可能会立即发生，但其不应具有重复的撤回。在其具有重复撤回的情况下，大规模退出将更新其余额，这些退出将被依次处理，并且造成重复的个人将被处罚。各方应当配合将其资金直接发送到另一条 Plasma 链中。

2. 退出处理器 Pat 愿意组织该退出。Pat与目的 Plasma 链配合发送资金，并已承诺当大规模退出终了时，自动地将资金识别为可用于新链中。

3. Pat 验证 Plasma 链，直至具有信息可用性的点。该点须位于可接受的争辩及 Plasma 结束期间（不同于根区块链结束），且符合智能合约的各项条款。Pat 对参与者显示新的 Plasma 链中待定的目的账户。Pat 从希望退出的参与者（包括我们的示例 Alice）中取得所有的签名。Pat 证实了直到数据之前所有参与者均有权退出的区块链。Pat 用大规模保证创建退出交易（如根区块链智能合约中所定义）。Pat 可以收取参与者退出的费用。

4. 用户下载完所有的签名后再次签字保证大规模撤回。这容许用户了解 Pat 将不受处罚，而其现在不能更改。尚未提交第二签名的用户，其份额将不被纳入。

5. 然后，Pat 观察是否存在任何其他退出交易，在必要时去掉副件，签署退出交易，并在根区块链或父 Plasma 链上播送。在重复的情况下，链的父代获得优先权（取决于作为最高优先级别的根区块链）。越早的交易获得的优先权越高。在播送大规模退出启动交易 (MEIT) 时，Pat 以其将以下信息更正的证据为保证：区块有效性、区块高度处的 UTXO 集，非终结、从位图到 UTXO 的梅克尔映射、承诺的金额（以用于快速证明的梅克尔总和树的形式），若/当受到质疑时，Alice 等人的签名可用。作为 MEIT 的一部分，Pat 发布了正在退出状态的完全位图。正是如此，其他观察到根/父链的参与者才能证实什么正在遭受撤离和质疑，如果它被看出是错误的。MEIT 的终止是一个非常漫长的过程，恐怕需要很多星期的时间，因此 MEIT 是不得已而为之的交易（今后的加速也许有了SNARK 是可行的）。

6. 若有重复的撤回，则 Pat 可以选择在较短的宽限期间更新位图及正在取出的余额。

7. 网络上的任何参与者可以凭有争议的大规模退出交易 (DMET) 对 MEIT 中所验证的数据提出质疑。然而，由于 Pat 无法获知今后的区块是否取代输出，若交易已耗费在某一未来的区块上，Pat 不得受到处罚（但用户却可以）。若提出了质疑，则资金将被锁住，直到该挑战游戏结束。这些质疑必须出现于较早的宽限期内，若某一质疑有效，则 Pat 必须更新待取出的余额。

8. 若无质疑，则在预先定义的 MEIT 终结期过后，用户获得其资金。

Plasma 链的终结空窗时间也就是某人必须至少周期性地观察链的时间。在终结空窗过后，推定每个人均有直到该窗的 Plasma 区块链区块数据可用性。

实际上，在 MEIT 被 Pat 创建时，Pat 也证实了直到特殊的 Plasma 区块高度的正确记录，并证实了其具有用于撤回的签名及各输出的事实。若证明期过后某一输出已被重复耗费，则 Pat 不受处罚（正如扣块不应使 Pat 受到处罚）。

5.7.1 大规模撤回争议：不正确的撤回质疑

在某一用户（如 Alice）发现 Pat 正在未经其同意而尝试大规模撤回的情况下，她可以通过提出质疑使该撤回无效。

1. Alice 发现 Pat 已尝试在 Plasma 区块链中的大规模撤回她的某一输出，由于某一位图领域被激活。Alice 用大规模保证播送一条质疑。该保证证实了某一质疑将不会产生的事实。她在区块链上播送此内容。

2. 若在设定的时期过后该质疑并未遭受争议，Alice 将其保证退回，而整个 MEIT 被取消。若该质疑经证明因 Pat 或任何其他方面产生了关于她的不正确的撤回质疑的证据而遭受争议，则 MEIT 仍然有效，且她的保证将被削减。

参与者们确信的是，由于 MEIT 中有第二阶段（第 4 个步骤），签名可以用于证明，所以他们有足够的信息争论某一质疑是否具有欺诈性。激励措施是反对提出欺诈性质疑的，在假定区块有用性和根链的非审查性质的前提下，这些质疑将受到处罚。

5.7.2 有争议的大规模退出交易

在输出从后期区块的大规模退出启动交易中已被耗费的情况下，Pat 可能不知道此事，于是他不应该受到处罚，因为无法提供扣块。

可能存在针对类似的位图集合的多种争辩，但所有这些争议须附有大的债权。

任何参与者可以用大的保证表达耗费的位图/范围。大的保证是货币在后期区块中已被花费的证明，含有对区块头的承诺。

然而，无法严谨地证明该争辩，故有可能出现另一种反复的质疑，对有争议的大规模退出交易 (CDMET) 发起挑战。

关于该争端的质疑如下：

1. Alice 注意到某人（如执行扣块的链运营商）试图抗拒她正在参与的大规模撤回。她提出关于该争议的质疑，用大的保证证实了争议提出者不能产生有效预算的事实。

2. 争议的提出者必须在某个时期内对质疑做出响应。若提议者不能产生预算的证据，即本质上后期交易的签名，则Alice将被证明无辜，而整个争议将被取消（这就是重复争议被受理的原因所在）。若提议者能证明货币已被花费，则 Alice 将失去她的保证而争议将持续不休。

5.8 回收 UTXO

预算输出完成之后，可以再次将 UTXO 位图用于严实性。

5.9 总结

作为该大规模撤回博弈的结果，对于撤回的很多参与者来说，在最佳情况下按每次消耗 1-2 比特的信息进行大规模撤回是可行的。

大规模退出在扣块的情况中是必要的。然而，这样代价或许仍然过于高昂。鉴于此缘故，我们可能还需要不依赖于使根链负荷过重的替代性策略。

该结构容许很多参与者在某一子区块链中持有其资金，若区块信息可用，则状态无效通过欺诈证明发生，状态过渡能够发生（即付款），撤回有效，且大规模退出（虽然存在一定的延迟）在扣块的情况中是可能的。

6 区块链中的区块链

如我们已描述过的，Plasma 在其核心处构建一种方法进行可扩展的计算，然而我们需要应对围绕产生欺诈证明的扣块的问题以及区块空间可用性的问题。针对 Plasma 中扣块的解决方案是构建一个系统，使得人们能够在 Plasma 扣块的链终止的情况中进行大规模退出。

然而，区块链上的大规模退出交易可能非常昂贵，特别是当 UTXO 集较大而位图需要发布时。此外，只发布单一退出可能会令人满意。大规模撤回交易需要复杂的包括众多参与者的交互式游戏。其应当在万不得已时才使用。

相反，我们构建的系统具有高级和低级法院，特殊的审判地可以存在以证明状态。人们可以将根区块链视为最高法院，各附属法院由此获得其权力。正是根区块链的法律才容许所有低级法院获得其司法权。这考虑了审判地的可扩展性，仅当低级法院的状态受到争议或终止时，人们才需要转移到高级法院争取更受代表的审判地。在高级法院播送状态的证明总是可行的，但可能更昂贵。

所有的状态均为梅克尔的并承诺至根区块链。在最佳情况下，区块头被发布在直接父链中，而父链又被发布到其父代中，以此类推直到到达根链。头的内部是对区块的梅克尔承诺，人们已在父代中见到。

交易可以提交给 Plasma 链及任何 Plasma 父链、以及根区块链。这样规定的目的是确保可替代性和抗审查性。特别地，在区块移动终止及未披露的情况中，人们同样能够撤回资金。

当区块承诺递交时，其须等待反映在根区块链中的一定金额的确认才能批准。在此期间，欺诈证明可能被递交到根区块链或任何中间的 Plasma 链（然后通过区块根效忠于根链）。

各 Plasma 链运行一个将承诺捆绑入 Plasma 区块的状态机。各 Plasma 链能否内省到 Plasma 子链的详细信息中皆有可能。相反，它们具有 Plasma 链的价值的运行确认的余额。当 Plasma 子链更新其状态时，它们将其 Plasma 区块头的哈希表递交到任何一个 Plasma 父链或根区块链。

这意味着特殊的根区块状态能够被递交到多个父链。在重复的情况中，则可能不存在缺陷（但根据应用情况，在一定的合意规则下可能受到处罚）。另一方面，若状态有含糊性，如忠于父代 1 的状态不同于忠于父代 2 的状态，则 Plasma 链的见证人可以将其存款削减。

新的子状态更新可以使用其状态更新消息中的以下字段进行：支付的费用（及面额）、所效忠的根区块哈希、上一个区块哈希、所效忠的父代区块哈希、存款证明、撤回证明。

不论当前效忠的是哪个父代区块链，该链总是假设子链已看见直到该点的一切，递归地包括其上的所有父代。这是为了忠于其所拥有的将不会含糊不清的证明以及双重预算交易（因此在含糊不清的情况中将其暴露于削减）。

在含糊不清的情况中，父链状态始终取得优先权。建立了激励措施以通过知晓内幕的当事人披露含糊不清的情况。

存、取款在父链和根区块链上均有可能发生。

假如有足够的流动资产且另一方愿意在别处承担资金，取款还有可能发生于 Plasma 链之间。这可以通过链间的原子交换实现。

若某人希望使用主区块链清算，可以在链间构建看似链上闪电支付的 HTLC。

所有的欺诈证明必须出具链承诺的梅克尔证明。虚假证明处罚为欺诈区块负责的特殊 Plasma 链。

首要的设计复杂性在于以抗审查性的利益表示多个父链间的交易状态播送。较早的迭代可以推定状态过渡/交易只能在各条 Plasma 链中进行，并且与其他链的唯一交互是传递给亲/子及存/取款的提交的消息。那样的话，首要的复杂性是有关存、取款的唯一凭据。

数据承诺被假设为纳入证明的一部分。

6.1 链内接收资金

在区块链中链的该分层框架中，当一用户收到来自另一用户的资金时，若 Alice 欲在深度为 3 级的 Plasma 链中将资金发送给Bob，该过程如下：

1. Alice 就其欲将资金发送给Bob一事与Bob协调。Alice 向 Bob 透露他将从中得到资金的 Plasma 链。Bob 决定是否接收付款，特别地，Bob 应当保证关于根区块链的智能合约中提到他愿意接收付款（智能合约代码/机制，以及可接受的合意退出延迟等）

2. 若这是某商品的付款，他们预先签订定义了付款条件的声明，在多数情况下，其为将区块纳入具有充分成熟度的区块链的付款证明，然而在某些情形中，其还可以是向合约哈希的支付。这不是链上的，但仅为附加一些条款，以便将结算证明给他人。

3. Alice 在 Plasma 链内部进行支付。区块被验证程序签字保证生效，而对区块头的承诺被发布到父代的区块当中。对于Plasma子链的梅克尔承诺被纳入一切父代区块且最终被纳入到根区块链当中。

4. Bob 与根区块链完全同步，然后证实资金正在其中被接收的链及其任何父代。Bob 不需证实其他 Plasma 链，其资金不是这些链的一部分。Bob 可以充分证明，在最坏情况下 Alice 已在具有充分成熟度的 Plasma 链中进行了付款。然而，若需要迅速定局，Alice 可以在新的区块中被履行的付款上签字保证（见之前关于接收 Plasma 链内部付款的声明）。若 Alice 愿意在付款上签字保证，并且 Bob 接受之（因其能证明取款），则推定已达到该定局。Bob 能够从该 Plasma 链中撤回资金。

本设计的关键方面在于，某人完全负责证实子区块链。若 Bob 不证实 Plasma 链及所有父代（最终定期的承诺被发布到根链当中），则其不应被视为已经履行。同闪电网络中的构造相似，Bob 无需关心其他 Plasma 区块链中所发生的情况。他只需观察这些链的正确性，这对于他而言至关重要。一旦他有能力使用货币，他就有信心能花费这些货币。

6.2 从父链中获得资金

从父链中获得资金类似于来自根区块链的存款，唯一的区别是接收者需要核实所有的 Plasma 父链（而不仅仅是 Plasma 链本身）。进入 Plasma 子链的存款是迅速的。

6.3 从树到网

尽管以上描述是关于单个父链的，但 Plasma 链有可能观察多个根区块链。这容许人们用子链更新余额。必须留意的是，某一父代上的故障可能不为所有参与者立即识别，而级联式的系统故障必须经过延时和最小化链间流动资产的假设得以缓解。对此的正确结构是一开放性问题。

6.4 缓解扣块问题

通过构造许多现场让人们可以播送撤回交易，现在可以存在很多可从链中退出的已终止或使扣块的地点。若某一子链发生故障，则即使交易在根链上变得昂贵，单独的退出也可在父链上处理。

这允许人们在 Plasma 链上保持小额付款输出中拥有一定的信心，前提是他们拥有其中某一 Plasma 父链运行正确的把握。该目标是其首要原因，其次是缓解级联式故障的影响。

若人们让充分大的输出余额得以保持，在没有重要时间价值的情况下，他们无需做出重要的承保，然而，若人们持有低价值的单一输出（其中支付交易费用变得过于高昂），则人们应当拥有其中某一 Plasma 父链具有可用性的一定把握。若人们想要更大的把握，则可以深度地运行嵌套链，同时让独立的多方在各层次上运行各 Plasma 链。不过，通过这样的方式操作，会存在一些折衷，就像特殊的 Plasma 链变为拜占庭式，然后每个人将需要向新链进行大规模撤回。不过，若存在非拜占庭式的父代，在父代拒绝处理拜占庭式链的承诺的情况下，可以继续运行并促进向另一链的迅速转变。

服务可能出现，从而在子链发生故障的情况中，其除了处理交易外不做任何处理。该业务的操作员无需做任何事，除非某一子链发生故障（到了它们可以为其可以假想地关闭其服务直到故障发生而感到充分被动的地步，区块头自动地跳过它们，以待在被动操作员上一等级的链上播送）。

我们期望父链中的多次撤回将是简单的撤回，而不是大规模的撤回，因为父链可以拥有高得难以置信的交易额（区块大小/气体限度）。

6.5 退出

大规模的退出对于父链或根链而言是可能的。若子链开始模仿拜占庭式的行为，则推定任何状态可能无效，类似于无嵌套父链的一条 Plasma 链。类似地，大规模退出是快速从拜占庭式父链退出的一条途径。可以不经过父链（或子链本身）而到达其父链或根链。

尽管设计中看似好像有一定复杂度，但其中的假设是如果任何链是拜占庭式的，则其所有子链须表现同样的行为。存在可行的优化使得退出无需经过心跳的协调而可行（退出在默认情况下无需在用户端将其撤销的签名，也无需 Plasma 链本身做出已收到的承诺，但可能是过早的优化）

该结构基本上与简易退出或大规模退出相同，然而设计中存在一些支持嵌套链的次要改变。退出可以重复，但父链上的退出始终占有优先权。若某一父链开始模仿拜占庭式的行为，则退出也可以在根链上进行。反映并更新其父/根链重复退出的状态并取消其自身链中的重复退出是（被认为是）拜占庭式 Plasma 链的责任。然而，若其不这样做，用户的资金将在根链上可用。

若父代是拜占庭式的，而某人持有其中资金的子链正在正确地运行，则可以避免进行复杂的大规模退出交易。参与者发现了发送其资金并进行简易退出的一条新链，从而流动资产提供者在该子链中获得资金，其他用户则在新链上获得资金（无需拜占庭式父代）。子链区块的承诺被发布到根链或更高级别的父链上（避免拜占庭式结点）。用户快速拥有新链中的资金，随后流动资产提供者将其资金退至根链或最高级别的父链上。这样设计的目的是新的资金可以快速的分配到新链当中，而退出能够迅速地发生。

6.6 可扩展性

这考虑到 UTXO 位图可扩展性，在位图太大的情况中，人们只需将位图分解为多条子链。对于子链，假定其表示为具有区块高度随机数（及候选链尖端）而没有输出的账户余额。类似地，对于喜欢使用账户而非 UTXO 的状态，假设人们愿意仅对支持简易撤回做出权衡，则其也是可能的。

这样的最终结果对于用户而言是相当大的可扩展性。他们只需观察其资金被持有的 Plasma 链（及其父链）。这有效地将数据集粉碎为影响自身的验证。

7 Plasma 权益证明

我们提出简易的权益证明结构。这或许不是最佳的权益证明结构，但可以说明Plasma链中什么是可行的。

直到现在，我们已经假设了 Plasma 链的操作员是负责签字保证区块的单个实体。若他们创建了无效的区块，拥有区块数据的其他任何人能够产生欺诈性证明并通过对操作员加以处罚退回区块。这是可以证明的，因为操作员已经用其签名在区块上做了签字保证。在根链中的 Plasma 区块的梅克尔承诺的发布（由于最高级别的 Plasma 父区块包括对其子区块的状态更新的承诺），因此状态更新是有序的，并与正确的行为结合。

然而，在多数情况下更为可取的是构建权益证明链取代单方的权威证明链。这样可以尽可能降低有关扣块的风险（通过将某一链嵌套入单方权威证明以及公开的多方权益证明链，可以获得两个命令的最佳者）。随着标记的价值从拜占庭式行为中降低，标记化的权益证明链同样给予了激励，鼓励标记持有者正确地操作。关于标记化的潜在价值的更多细则在下一节中提出。

权益证明构造在 Plasma 中较容易构建，因为它同样取决于基本的根区块链的鲁棒性。关于扣押、定局等因素的问题被推向根链的可靠性。Plasma 充其量仅能具有与根链相当的安全性。若根链正在运行工作量证明，则这是工作量证明上的权益证明（根区块链上的 Plasma）若根区块链是权益证明，该构造便是权益证明上的权益证明，然而权益证明机制可以更简单或相异于运行在根区块链上的情形。

7.1 中本聪共识激励

我们试图从中本聪共识中复制主要的激励（工作挖掘证明）。待复制的最为重要的激励之一是鼓励区块向其他掘进者传播的激励。

许多现有的已提出的权益证明机制有赖于领导人选举，某一领导人在时刻 t_0 被选举，而该领导在时刻 t_1 有权产生区块。这并不围绕传播复制中本聪共识激励。中本聪共识并不从事领导人选举，而是从事概率性的领导人选举。若某人发现一区块，则其认为其有可能成为领导人，但又不完全确信。其他某些人本可以在恰当的时机采掘区块。最大化某人成为领导人的几率的最佳途径是尽可能深远、广泛、快速地播送该区块，使得其他区块能够在其上发展。这位信息可用性创造了激励措施。

Plasma 的权益证明构造需要做一些类似的事情。

我们想要鼓励每个人尽可能深远而广泛地传播他们的区块，在此意义上我们进行了权衡。可能存在其他的构造（特别是一些通过对特殊分支分配随机分值并将链尖端确定为具有最高分值的分支而严重依赖于事实背后的随机选择和概率性的领导人选举的构造）。

7.2 简易权益证明模型的示例

尽管这是建立权益证明模型的简单提议，其可能在任何方面并非接近最佳方案。目标是构造一些简单的便于 Plasma 使用的对象。

该方法不是创建实施机制，而是仅仅创建激励措施鼓励适当的协调和正确的行为（区块传播）。

费用由根合约指定和分配，并在需要的情况下定期支出，但会计在链本身的内部完成。

作为赌注合约的一部分，利害关系人分配的资金被过户给经授权的利害关系人。该利害关系人负责代替用户行事，如果利害关系人出现差错，则用户将受到处罚。赌注的承诺将持续一定的时间（如 3 个月）。各赌注的最低金额为各代币的百分之一，最高为百分之五封顶。若人们想分配多于百分之五，则他们应当使用多个赌注身份（目的是最大化数据分布而最小化低于 51% 的同业联盟的效率）。

资金的分配取决于过去的 100 个 Plasma 区块是否对所有的参与者具有代表性。例如，若某人以利害关系人的 3% 被下注，则资金应为前 100 个区块的 3%。若高于此金额，个别利害关系人不因发布额外的区块承诺而获得附加报酬。若过去的 100 个区块中有低于 3 的，则当前区块创建者获得较少的报酬。只有一个区块可以在根链上按块分配。

这样便鼓励所有的参与者对等地协调和包含每个人的区块。其假设是，某人无需建立实施机制，参与者将协调并保证某个类型的机制（如循环投注），以保证最大回报。

若他们由于不当的区块量而得不到最大交易费用，则资金被分配给某一资金池以支出日后的区块。

结果是一人推出来自每个人的参与的经济鼓励。

然而，这还不完整，因为我们只是在鼓励来自各利害关系人的准确参与。每个区块中有一个对来自之前 100 个区块的任意部分区块中的数据的梅克尔承诺。这迫使利益关系人拥有充分的区块数据，结果又迫使区块创建者将其传播给所有的利益关系人。

链尖端由最大回报确定，若有平行分支，则取胜的分支也就是从最大限度的协调中拥有最大费用回报的分支。

该构造并非受任于停止 51% 的攻击，但相反却受任于鼓励区块传播（若某人致力于被扣押的区块，则威胁是对等的）。此外，该构造有赖于根链上区块包含中的信息可用性和公正性；不可能由于数据可用性和审查激励方面的假设而在根链上构建这种类型的权益证明。

8 经济激励

在权益证明验证模型内，可以构建与合约条款的正确操作相符的激励。尽管忠诚保险契约确保了针对链的准确性，我们需要围绕数据可用性创建进一步的激励措施并阻止挂起。由于代币的价值来自所有今后的赌注回报的净折现值，通过仅允许使用针对 Plasma 链的代币下注，人们能够确保有待持续运作的激励。 结果，网络故障降低了当前持有的代币的价值，而个别代理人可以最佳的利益对网络的持续运营享有大量的激励。

Plasma 链的操作员从播送链上交易中获得费用。经计算，不同的运营可能有不同的资费，并且费用可能下跌，特别是对于复杂的运营。尽管有激励让更多的交易在深度的子链中进行，可以在子链中为转移的资金创建承诺或估算，再传播开来。这允许父链在子链中收取估算费用，并且若有错误保证，则区块数据将失效且不可执行。这并非必要之举，在多数情况下，人们宁愿在子链上选择更多具有较低必要性的估算，以分配资金直到父链。

对于系统升级，可以通过创建另一份接受相同代币的合约并公告过渡时期来升级系统（或由团体在分散体系中共同决定）。

这可能创建自我运行的系统。尽管人们过去需要对从事数据存储和计算的主站点支付和操作云计算方面的业务，如今可以构建一套（具有欺诈证明的）智能合约，代币，靠充分数量的参与者支付费用，从而系统能够自我运行，同时有一群利益关系人继续正确地操作网络和计算基础设施，在真正意义上使计算在无定形的云上发生。

8.1 代币与货币的较量和经济安全

这些根区块链上最终持有的欺诈证明和契约可以是本地代币，如用于以太坊的以太币 (ETH)，也可以是维护基本区块链的合意规则的单独代币。

表面上看，使用根区块链的本地代币（如 ETH）最简单不过，然而有一些有趣的经济安全含义。

若目标是防止链终止及错误行为（取决于区块链应用），只要 ETH 被使用过，激励就有可能不足以防止错误行为。若链终止或为拜占庭式，则代币的价值将会降低。此外，代币价值大约是未来交易费用的 NPV，其可使代币成为有价之物。若某人对 ETH 下注，则相对于所得费用的金额而言，该人所下注的是来自债券的时间价值的价值。该保证的价值有望将远低于代币的净折现值。此外，难以证明和阻止的是链终止和扣块，并且若某人保证 ETH 并于赌期过后取回资金，没有足够的激励可以非拜占庭式的方式生效，而有了代币，该代币的价值将会随着广泛的拜占庭式行为而降低。

9 用于区块链的 MapReduce

几乎任何可在 MapReduce 上计算的对象也同样应在该链上可计算。这需要对我们关于区块链上的计算和编程的思路进行深度重构。这是 MapReduce，但含有欺诈证明。各节点表示一条区块链。这与前一节所描述的 Plasma 区块链树结构高度兼容。

例如，若某人想要做标准的字数统计，您可以创建一颗由链构成的梅克尔树操作 reduce 函数。若欺诈的证据存在，则产生欺诈的节点将受到处罚。如果您能够产生关于求和的 reduce 函数，那么您也能够产生平均值。例如，平均价格等映射函数仅向各链发送计算，然后传递结果。显然，存在围绕数据吞吐量的约束条件，也就是减少欺诈证明之所以有必要的原因。各种类型的任意计算是不可能的，但可以解决许多类型的问题集；通常，受内存约束的问题集可以通过先运行排序算法而得以解决，对 Plasma 链内流量进行权衡。

若节点不能产生实际的区块来证明计算，则其结果应当丢弃并重新运行。注意到这并不保证 MapReduce 所能保证的计算可扩展性（因为您需要观察链以维护共识），然而，它确实给予了活动的实施并赋予了代理人向上扩展的能力。结果，主要局限围绕着一个事实，即受特殊计算影响的当事人应当遵守该套计算。若某人仅需要遵守某一小部分，则应该没问题，但是若某人需要遵守整个计算，则其并不给予可扩展性的好处（只有围绕可扩散的保证的好处）。即便如此，许多问题可以这样解决，例如分散的交换（您的映射集合关注您自己的交易，若其他每个人的网状执行可以实施，则您不用关注具体细则）等

区块格式必须与可在 TrueBit 构造中计算的数据兼容。存在对状态的承诺（将能构造容许容/斥上状态过渡的证明的 UTXO/状态特里结构），账户特里结构（对子链和复杂的状态过渡）、费用方面的承诺（致力于费用方面的状态过渡的树）、梅克尔交易、对从父/子区块传递而来的数据的保证，对见到的父/子区块的保证（以避免重排序）、以及任何业务逻辑（如字数统计示例将会对文字及其所见之处产生梅克尔分类的承诺）。通过构建梅克尔承诺，人们可以在能够证明错误状态过渡的根链或父链上创建可证明的智能合约。存在一些可能不兼容该格式的问题集，但无重要记忆要求的一般计算是可行的。用于此目的的思想框架将用于计算的最大存储空间看作相当于欺诈证明中所允许的最大数据。

一系列的映射与 reduce 函数以某种方式考虑了待操作的区块链，根据该方式有义务处理数据。这要求父代与子代创建处理的义务。子代必须包含传递数据的父代，否则该链将终止。父代可以在子代中执行计算，并且若子代终止，计算的执行可以通过在父链中广播数据并在此核实证据而发生。TrueBit 构造中的主要威胁与围绕终止的问题有关，因此若子链停止，应当注意考虑继续的运行，虽然这要求大量的复杂度，特别是随时间推移（数据集可以改变，而具有时间一致性因某些问题更难以推出）。

通过在带有子链的映射和 reduce 框架中构建区块链计算，可以采用现有的计算机科学研究并直接将其应用于为区块链而存在的分布式系统问题集中。可以构建以可扩展方式产生许多有用的业务应用的 Solidity 合约。人们只需计算并验证与其相关的活动。

10 示例应用

分散应用可被再构造为 MapReduce 问题，用经济激励鼓励由代币作保证的正确活动。

10.1 区块链上的 Reddit 克隆

这主要是关于数据存储 (CRUD)。首先，计算和证明是围绕访问控制、身份（选举和帖子）和适度的。很多网络应用实际上只在后端从事 CRUD。

根区块链包含智能合约合意规则及欺诈证明。最顶端的父代包含子版块的账户。各子版块是居于最顶端的父代的 Plasma 区块链子代。在各子版块内有一条帖子的 Plasma 链。该帖子的子链也包含评论。共识机制执行访问控制。对之前块数据的随机化承诺（含父链提供的随机数）在一切区块头中得到保证。定期地计算 reduce 函数，用于置顶发帖和其他统计数据。

个人用户的计算机下载数据和软件，该数据和软件对于机器格式而言是本地的。提交数据要求支付交易费用以激励数据的包含，根据可用性可能产生下载旧的区块数据的费用。

要浏览具体的帖子，用户在根链上检验承诺，再前往最顶端父代的链尖端（往回走 n 个区块到达终结时期，也许为一周的价值），找到用于相关子版块的状态账户特里结构。连接到 DHT 网络以发现子版块上的节点，下载子版块的链尖端（再往回走 n 个区块以检验），并查阅帖子列表，下载状态特里结构作为用于带有评论的相关帖子的轻客户端和原始数据。用户只需观察仅与自身相关的部分Plasma 链（仅下载与自身相关的帖子和子版块）。

这是数据存储的简单示例，在区块链上具有一定的计算。验证程序充分验证各个节点是可行的，然而，还有可能将其分片出来。不过，一旦分片过远，就会产生信息可用性的考虑。缓解此情况一种办法是给予子版块主对子链的完全控制权。

10.2 分散交换

尽管区块链上的 reddit 克隆使 CRUD 网络应用的可能影响变得显著，但除现场统计数据外，其并不显著利用 MapReduce 操作。

分散交换表明，可以用较低的潜在性换取较高的计算性能。由于存在许多状态，可以在账户而非 UTXO 中定义输出，或者对于状态机中的各个步骤，可以使用较大的位图来表示各个状态，而不用单个布尔值表示位图中的花费。

类似于子版块，存在一颗子链树，其中各链表示一个交易对。在各自之内有一颗由链构成的树用于最大化可扩展性（对于低活性的交易对来说，其只可能为一条 Plasma 链，但对于高活性的链来说，其可能拥有更加多的子代）。这些链中的每一条均有联结的活性，并且能够按轮交易的份额受限于联结的份额。

第一步是在子链中拥有余额，所以这就像作为基准的 Plasma 支付链。

接下来，直接将订单发送至子链当中。作为对父代的承诺的一部分，各订单聚结为单个订货薄的梅克尔承诺，由链本身表示为一份订单。该步骤以递归的方式将各子代的订货薄还原为由该链表示的单个订货薄，直到到达最高等级的 Plasma 链父代为止。在收到订单之后，订单窗口关闭，并且交易成批地执行。

在该还原步骤完成并递交到根区块链中之后，各链通过映射步骤被通知其分配。父代以明确的方式告诉子代其订单的什么分配被填充。假如子代能够见到其他订单（暗示着该子代能够在该步骤期间观察到父链），这些订单在该映射步骤中将能够被证明为正确的执行分配。接收分配之后，映射步骤继续以递归的方式到达该链的子代。

当此完成时，通过将所有的资金更新递交到一个区块当中而将区块头递交给某一父代，进行最终的还原步骤。

在重要的价格运动的情况中，通过允许多轮 MapReduce 回合（允许高精度的定价）而做进一步的优化，然而这种一般的构建开启了极高的容量。 在该框架中，理论上可以进行世界上的所有交易活动，通过将该活动转变为完全致力于并受根区块链绑定的批执行交换而带有速度上的某些权衡。

这种类型的构造对于许多类型的财政活动和计算是有用的。

10.3 分散邮件

要创建 D-Mail，可以表示 Plasma 链中某人的账户并要求付款以接收邮件（在链中插入消息）。提交的内容用个人的公共密钥进行加密。强制执行可以确保未知的实体必须支付，可以使用 zk-SNARK 做进一步的优化。父链包含链的目录并执行付款。简易设计

10.4 分散的 CDN

可以拥有分散的 CDN。类似的构造如以太坊分片提案。将各条子区块链看作分片。具有随机性信标（可以是根区块哈希或别的内容）。将数据在每隔 n 个区块的分片之间来回挪动。父链负责对挪动的保证。其他链可以懈怠地保留档案，数据损失会被通告，而保留档案的人会得到回报。由于人们在其他分片拥有数据的情况下才得到回报，故为传播采用激励措施。鲁棒性取决于对流量“长度”的要求；鲁棒性越高，在任意时刻需要拥有副本的分片数量越多。此处的重要见解是，存储量是带宽的函数。数据不被看作盘上的平稳数据。各数据实际上在朝着其下一个目的地流动和运动；正符合道教的观点。

为下载数据，个人验证父链的分片和随机信标，以便了解哪个分片含有数据，进而通过识别对等实体的 DHT 与之连接，并下载数据。

10.5 私有链

参与者无义务向其他人披露链中的数据（虽然没有阻止数据被公开的机制），并且作为结果，只要链上的参与者想让根链实施某个私有的区块链网络，他们就可以这样做。这就好比内联网/互联网的区别。交易可以发生于本地的私有链上，但也传达财政活动并使之受到公共链的约束。

11 攻击、风险及缓解

11.1 智能合约代码

书写优良的智能合约代码是有难度的。安全性完全取决于对欺诈证明的正确处决。可能的情况是，一些欺诈证明可能不被采纳，而无效的状态过渡在根链中可能有效。

11.2 在主链上关闭交易过于昂贵

存在一种风险，即交易可以在主链上被关闭，但这样做在经济上并不可行。这样可以创建某些类型的退出骗局，从而使某人将大量的价值积少成多。

通过设置退出规定，根据退出规定对各交易进行分类，并在某个争端调停期过后允许从整条链中立即退出，这种情况可以得到缓解。这又允许第三方观察者代为某人进行观察。然而，该构造显著地增加了复杂度。根据链的哪个部分发生故障或最终取决于根网络，这些预先签订的聚结的交易能够传播到其他父代网络上。然而，这还取决于正确行动的任命当事人，这就是之所以个人应当对单个输出或输出集聚结所有未花费的付款，从而使退出的交易在经济上可行。

此外，人们可以将小额付款留在估价甚高的代币联结的链上，并盗用该价值（由于存在充分的抑制因素阻止完全扼杀 Plasma 链）。

若广义的递归性 SNARK/STARK 变得可行，则理论上可以保证实体撤回无权做出未经授权的退出，即便具有被扣押的区块。

11.3 定局

用于退出的争端窗口本质上在创建定局假设。若基本链有一些与重组联结的重要成本来促成定局，则其可以显著回避造成链间同步性缺乏的深度链重组风险。缓解的示例是有计划的 Ethereum CASPER 结局诡计。

11.4 根链缺乏容量或增加成本

若无缓解到位，在费用或气体变得过于昂贵的情况中，在设定的时期内将难以退出交易。例如，若费用/气体成本增加 50 倍，或者没有足够的空间来退出交易，并且采掘者不增加容量或气体限值。

通过延长退出延时、暂停允许有序退出的退出计数机制，有几种缓解方式。这可以通过暂停退出来实现，只要存在之前 x 个区块中发生的退出交易。这允许每个人随着时间的推移而离开，前提是近期至少存在一个退出交易。若退出发生早于某人的退出，则计数器复位。结果将会是其遭到破坏，不论某人必须等待多久才能收到资金返账，这增加了流动资产提供者估价的费用。若平均区块链气体/费用成本高于非常高的特殊量（以某个合理的上界时刻为门限，其中该暂停的状态能够持续），简易的机制将在撤回时刻暂停时钟。

持有资金的用户应当确保至少有一个 Plasma 父区块链对信息可用性拥有较高程度的信心（理想情况下多个独立的父代）。

11.5 根链审查

本设计假设超过 51% 的根链是诚信的。若根链上的参与者通过审查区块配合攻击网络，则可能因强制执行退出交易或状态更新而产生显著困难，可能会产生围绕资金损失的严重问题。审查制度是安全性的首要因素，风险价值以及结局诡计（如 CASPER 结局诡计）可能需要被束缚于未来的链中。

这可以通过添加 zk-SNARK/zk-SNARK 资金证明而得到缓解，但需要重要的新工程和研究。

作为各退出交易一部分的大额债券的使用怂恿了欺诈证明，因为采掘者可能会获得该欺诈证明相当一部分的回报，而审查制度将备受抵制。

为该网络所给予的安全性是某一 Plasma 父链、根区块链诚信度和正确性以及资产规模的函数

全局转移金额的系统局限性（速度限制按块退出）并确保其低于结局诡计

11.6 链终止

若链终止，在设定的时期过后可以呈递预先保证的状态过渡。然后接管交易的消耗链可以播送对该事件的接受，整条链移动。只有在某条链不再向前移动一段设定的时间之后（忽略父代上的交易广播），才允许这样。欺诈证明能够争辩链尖端。

可能有针对链终止的更大激励鼓励包含复杂状态过渡的财政活动。

11.7 改变合意规则的无能为力

由于本设计是前载型的，无法改变合意规则而不对此能力预编程序。这可以通过创建升级路径作为系统的一部分来得到缓解（如在某个日期后被强制的终止）。由于存在针对代币持有者的经济激励以继续操作系统，这种无能还能产生无法终止链的社会意义，因而在其启动后可能会变得难以终止 Plasma 链。

12 未来的研究

还有未来研究的更多领域，包括与这些链的安全性相关的利益。当前的一个研究领域是广义的递归性 SNARK/STARK，其会显著提高退出交易的安全性。具有深度防卫同样是人们所期望的，因此防卫的最后底线将是容许有争议的证明的直接分散退出机制，而前线则是新奇的密码术和安全的硬件元件。配对密码术等各种形式的同态加密术的创新使用方面的进一步发展可能也会是有帮助的。

对立即观察多条根链而同时保持同步的能力提出了较高专一性要求（不仅仅是促使硬同步）。

围绕定局及其在多条链间的交互需要进一步的研究，区块链退出风险也需要进一步减小（SNARK/STARK 在此能够起到帮助）。

13 结论和小结

Plasma 这种设计的主要焦点在于确保具有数据压缩的信息可用性（特别是关于扣块攻击）。

我们提出了一种机制，使得人们可以提交允许人们持有区块链中的资金（其状态由根区块链强制执行）的可实施承诺。

这容许跨越广泛无定形的计算机网络进行重要的计算和存储。活动由施行承诺的经济代理人联结，最终可以在各父链间执行，而实施向下流动至持有执行事实的智能合约的根区块链。该构造容许人们进行状态过渡，否则其在根链上不会具有成本效益。

由此结论，区块链可以处理世界范围内近乎所有财务计算上的承诺（只要其每次不占有过多工作内存）。只有当计算无效时才提交证明并回滚那些承诺。人们无需对链的操作员给予监管上的信任。

为减少围绕链终止等拜占庭式行为的激励，费用产生激励以鼓励链继续运作。若 Plasma 链由针对该链的代币中的活动联结，则终止受到阻止。若链终止，则链的价值降低，为继续运作创造显著的经济激励。

该激励和结构容许人们创建分散式自治程序，在交易费的资助下连续运行。这些分散式自治应用程序创建真实的云计算，从而处理并验证数据，但其成员集处于不断改变中，且是无定形的。Plasma 能够让区块链纵向扩展以服务拥有大量用户的广义应用程序而不受重要限制。应用程序创造者仅能编写智能合约代码，然后将代码提交到区块链，激励能够持续以继续运行这些合约的计算，只要人们使用 Plasma 链支付其费用。

14 致谢

非常感谢 TrueBit 作者的对梅克尔证明的设计和实现，包括感谢 Chrstian Reitwießner 的评审。感谢 Vlad Zamfir 多方面的的点拨及其促使这些思想形式化的总体思想框架搭建。感谢 Thomas Greco、Piotr Dobaczewski 和 Pawe~l Peregud 的反馈和贡献。

待办事项：要求他人的承认。

待办事项：提高参考书目并取得更多引用 待办事项：完成

框图

参考文献

[1] Joseph Poon 和 Tadge Dryja闪电网络https://lightning.network/lightning-network-paper.pdf，2015 年 3 月。

[2] 以太坊。以太坊。https://ethereum.org.

[3] Gavin Wood.以太坊：一种安全、分散、广义的交易账簿。http://gavwood.com/paper.pdf，2015 年 2 月。

[4] 雷电。雷电网络。https://raiden.network/.

[5] Jeffrey Dean, Sanjay GhemawatMapReduce：大集群上简化的数据处理*OSDI*中的页码范围：137-150USENIX 协会， 2004

[6] 中本聪比特币：一种点对点的电子现金系统https://bitcoin.org/bitcoin.pdf，2008 年 10 月。

[7] Nick Szabo《公共网络形式化与安全的关系》http://szabo.best.vwh.net/formalize.html，1997 年 9 月。

[8] Fred Erhsam《区块链代币和分散商业模式的黎明》https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f.

[9] Naval Ravikant《用于众筹的比特币模型》https://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/.

[10] Jason Teutsch, Christian Reitwiessner《一种针对区块链的可扩展验证解决方案》https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf，2017 年 3 月。

[11] Vitalik Buterin以太坊分片常见问题https://github.com/ethereum/wiki/wiki/Sharding-FAQ.

[12] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timn, Pieter WuilleEnabling Blockchain Innovations with Pegged Sidechainshttps://blockstream.com/sidechains.pdf，2014 年 10 月。

[13] Paul SztorcDrivechain - The Simple Two Way Peghttp://www.truthcoin.info/blog/drivechain/.

[14] 比特币维基Merged mining specificationhttps://en.bitcoin.it/wiki/Merged_mining_specification.

[15] Peter Todd树链https://github.com/petertodd/tree-chains-paper.

[16] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Mardas VirzaSuccinct Non-Interactive Zero Knowledge for a von Neumann Architecturehttps://eprint.iacr.org/2013/879.pdf，2015 年 5 月。

[17] Alessandro Chiesa, Eran Tromer, Madars VirzaCluster Computing in Zero Knowledgehttps://eprint.iacr.org/2015/377.pdf，2015 年 4 月。

[18] Jae KwonCosmos: A Network of Distributed Ledgershttps://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md，2016 年 9 月。

[19] Gavin Wood.POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORKhttps://github.com/w3f/polkadot-white-paper/raw/master/PolkaDotPaper.pdf；2016 年 11 月。

[20] Sergio Demian Lerner. lumino transaction compression protocol (ltcp)https://uploads.strikinglycdn.com/files/9dcb08c5-f5a9-430e-b7ba-6c35550a4e67/LuminoTransactionCompressionProtocolLTCP.pdf，2017 年 2 月。

[21] Ilja Gerhardt, Timo HankeHomomorphic Payment Addresses and the Pay-to-Contract Protocolhttp://arxiv.org/abs/1212.3257，2012 年 12 月。

[22] Tier NolanRe: Alt chains and atomic transfershttps://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949.

声明：

本译文纯属个人兴趣爱好，仅供参考，如有疏漏，请海涵！

后续将邀请业内人士审校、润色和排版。如需探讨翻译问题或业务，请加微信号 Ron1378 并说明来意。