比特币侧链Liquid及其底层强同盟技术方案解析！比特币，作为世界上首个对等式(也被译作点对点)电子现金系统，其为无需许可、私密的以及无需信任的交易敞开了大门。由于比特币的底层区块链技术遇到了隐私性、正确执行及交易终结时间方面根本性的限制问题，为试图重新定位比特币的底层区块链技术，我们提出了强同盟方案，这是一种公开可验证的拜占庭鲁棒交易网络，其可促进不同市场间的任意资产流动，而无需信任第三方。

强同盟方案可促进商业隐私(可支持隐藏资产类型和交易金额)，同时保持网络的公开可验证特性。就像比特币一样，该系统的执行是通过密码学强制完成的，然而，强同盟通过减少交易等待时间以及提高系统互操作性，显著降低了市场参与者的资本要求。

为了展示这一创新解决方案，我们会具体描述Liquid：第一个部署于金融市场的强同盟实现方案。

一、 引言

比特币，最初由中本聪于2008年提出，其基于的是称为区块链的想法 [1]。而区块链是由一系列区块串联组成的，其中每个区块，都由交易的时间戳集和前一区块的哈希所组成，正如图1所示：

(图1:默克尔树(Merkle tree)，负责将区块交易连接到区块头默克尔根)

比特币设计的基本原则是，网络当中的所有参与者皆处于平等的地位。他们共同信任工作量证明 [2]，以验证和执行网络的规则，这就消除了对中心权力机构的需求(例如票据交易所)。作为结果，比特币便准许大范围的参与者建立自己的银行：存储、交易以及为自己清算，而不需要用到第三方中介。

比特币的网络，使用公开可验证的算法，自动强制结算参与者的交易，这就避免了安全妥协、昂贵的(或难以获得的)法律基础设施、第三方信任要求或者货币的物理运输要求。由此，人类第一次有能力对其他参与者的行为进行密码验证，强制执行基于数学的规则，任何人皆可对此检查，而没有人能够破坏它。

由于这种设计，比特币的特点使得它成为了一种价值工具，它不同于以往任何存在的事物。

第一，它消除了交易对手的大多数风险 [3];

第二，它提供了资产所有权的密码证明(由于密码密钥的知识定义了所有权)[4];

第三，它是一种可编程的资产，其提供了支付一个程序(或一个“智能合约”)的能力，而不是被动的账户或单个公钥 [5];

第四，也是最后一点，它对于点对点实时传输、加速跨境支付、B2B汇款、资产转移以及小额支付 [6]这些应用而言，会是一种颠覆性的市场机制。

A.问题描述

由于比特币是一个全球共识系统，其去中心化网络和公开可验证性是需要成本的。而执行速度慢以及隐私保护不足问题，正是比特币的两大局限所在。比特币的工作量证明机制，被设计用于处理平均每隔十分钟确认一次交易。因此，从实时交易处理这一角度来看，比特币的确是慢的。这就自发地导致，使用比特币作为交易媒介的各方出现流动性不足的问题。即使在处理交易之后，对手方一般需要等待多次区块追加确认后，才会真正认可一笔交易。这是因为，比特币的全球账本的确存在着重组的风险(虽然很低)，其中最新的交易历史，理论上是可被修改的。这种潜在因素破坏了很多商业应用，因为这些应用需要的是实时的，或几乎即时的交易执行。

在今天，这需要一个中心化的对手方，而这就引入了第三方的风险。

尽管因为短期验证的问题，比特币在结算最终性方面是有优势的，在经过适当数量的区块确认之后，其为交易提供了强有力的安全保证(无法反转)。以传统支付网络为例，通常它们留出的最终结算时间最高能达到120天，而扣款则被允许推迟到8年的时间 [7]，当然，这取决于中心化网络拥有者强加的政策 [8] [9]。人们普遍认为比特币是匿名的[10]，但其隐私属性对于很多商业应用而言其实是不够的。

因为它的每笔交易都发布在一个全球公开账本上，这就允许少量关于用户财务活动的信息(例如，参与单笔交易的身份)可通过统计分析
[12]进行放大。这就限制了网络的商业用途，同时也伤害了个人的隐私 [13]，因为很多用户经常会假设：比特币是一个匿名系统。此外，它会破坏系统的可互换性，正如：具有不同历史的比特币，相应地它们是可被识别和评估的。

而克服这两大问题，会是很有意义的，这对于比特币行业以及更广泛的全球经济 [12]而言会产生积极影响。不幸的是，先前试图解决类似任务的电子货币们，它们遭遇了各种各样的问题：无法扩容(例如，比特金-BitGold
[14]);它们都是中心化的(例如，自由储备(the Liberty Reserve)或戴维的B-money [15]);或者它们会引起其他的安全问题 [16].

此外，依赖于一个中心控制的系统或单一的组织，通常对信任具有更高的要求。这通过建立具有高度许可的环境，这里具有实质性监管劣势及用户成本(造成了摩擦)，引入了对系统用户和运行者的限制
[17]，从而有效地复制了这些“比特币前辈”系统的问题。

如果一个解决方案是由一个中心机构运行的，那它就会不可避免地造成单一故障点风险[18]。这种情况的例子，包括最近发生的瑞波攻击。这已经表明，尽管瑞波和恒星网络在表面上都是成功的，但它们都存在着单一故障点(SPOF)风险 [19]。

同样的，引入更强的信任需求，可能会导致共识失败的风险，正如Tendermint以及以太坊已被证明的共识方法
[4]。最后，还有交易所和经济商，它们依旧明确依赖于第三方这种机制 [20]。这样的系统，会将它们内在的不安全性植入到任何建立在其顶部的解决方案当中，而任何底层系统的不稳定性，都可能会导致相依安排的坍塌。

B.贡献

本文介绍了一种旨在解决这些问题的新区块链系统，其会通过下列方式有助于该领域：

1)公开可验证：相比完全去中心化的系统，这种系统是分布式的、公开可验证的，它允许用户拥有最终资产的支出权限。

2)流动性：用户可自由地将资金存入这个系统，同时也允许他们随时从中退出;

3) 没有单一故障点：该系统维护了比特币的免许可特性，同时避免引入单一故障点风险，同时还提供了新颖的特征;

4)多资产类型转移：该系统支持相同区块链上的多资产类型转移，甚至是在同一原子交易当中;

5)隐私：通过扩展早期的保密交易[21]技术(即保密资产(Confidential Assets))，该系统支持几乎即时的、无需信任的、任意商品的原子交易，并且是公开可验证、私密的方法;

6)具体实施方案：Liquid，强同盟技术方案的一种具体实施案例;

论文的其余部分，将按如下方式进行组织：

在第二章节内容中：我们讨论了解决上述问题的强同盟方案的总体设计;

而第三章节内容：我们将深入到强同盟方案的技术细节;

第四章节内容：将讨论强同盟解决方案在不同领域的应用，而本文主要提到的Liquid，则是这一解决方案的第一个实施对象。强同盟方案在很多方面都是非常新颖的，因此需要花一些时间进行讨论。

而第五章节内容：我们将讨论各种创新;

然后第六章内容：会完全转向系统安全性评估及比较方面;

而在第七章节内容当中：我们会讨论进一步改进的方法论;

最后一章内容：则是给出相应的结论;

二、强同盟作为一种通用解决方案

正如我们在第一部分内容当中所述，基于工作量证明的共识机制会引入时间延迟问题。

然而，转移到一种中心化的系统，会创建出重大的风险。为了解决这些问题，本论文基于Back等人提出的“同盟锚定：一种比特币与侧链之间资产双向流动的方法论”[22]这一设计，而侧链是比特币区块链的平行网络，其允许各方通过提供交易占有的明确证明，从而实现在链之间的资产转移，过程正如图2所示。

(图2：锚定侧链，可允许各方通过提供明确的交易持有证明，在不同区块链之间转移资产)

A.侧链

侧链允许用户在不同的区块链之间进行资产转移。而更专业的说法则是：这些资产转移，通过将资产锁定在其中一条链的一笔交易当中，使得它们在当中不可用，然后在侧链创建一笔描述这个锁定资产的交易。从而有效地将这些资产从父链转移到侧链。

其工作原理如下：

1)用户将他们的资产发送到一个特殊的地址(会导致这些资产暂时冻结)，直到收到侧链资产返回信号

之后，这些资产才会得到释放;

2)使用一个同盟锚定的“in通道”，用户嵌入侧链的信息，表明这些资产在主链上已经冻结了，并请求在侧链上进行使用;

3)等额资产会在侧链上进行创建或解锁操作，这样参与者就可以在侧链规则下参与替代性交易方案，其与父链是不同的;

4)当用户希望移动他的资产或其中一部分资产时，他可以通过“out通道”进行返回操作，他把信息嵌入到侧链当中，以在主区块链上描述一个输出。

5)强同盟会在交易发生时达成共识;

6)达成共识之后，同盟锚定会创建一个输出，以解冻主链上的资产，并在侧链上进行相关指定。

B. 利用强同盟改进侧链

比特币展示了一种签署区块的方式：使用一种动态的签名者集方案(即矿工)，实现了动态成员多方签名(DMMS) [22]。而动态的集合就会给比特币引入延迟问题。而同盟模型则提供了另一种解决方案，其通过固定的签名者集合，替换掉了动态成员多方签名(DMMS)模型。这种解决方案减少了需要扩展的参与者数量，并增加了系统的速度及可扩展性，同时各方的确认，确保了交易的完整性。

强同盟是一种联合侧链，其中同盟成员充当了主链与侧链之间的协议适配者。可以说，从本质上讲，它们共同形成了一个拜占庭鲁棒智能合约。在一个强同盟当中，私钥的知识部分对于“花费权”而言就是足够的了，它不需要任何第三方的许可，并且该系统具有允许结算返回主链的机制(当同盟出现完全失败的情况下)。

其代码更新不仅是开放的、可审计的，并且在遇到强制行为的情况下是可被拒绝的，并且系统提供的是始终可靠的日志，保持状态的不可变性。最重要的是：同盟成员不能直接控制其他用户在系统内的任何资金。强同盟的网络运营者包括两种类型的工作者。这些工作者是那些满足特定条件的实体 [23]。

为了增加安全性，在实体之间，某些操作将被拆分开来，以限制攻击者可能造成的破坏。在一个强同盟系统当中，工作者有权控制区块链之间的资产转移，并强制执

行侧链的共识规则。在下一节内容当中，我们将提供关于划分这些责任是至关重要的具体原因。这两种类型的工作者分别是：

1)区块签名者(Blocksigners)：他们会负责侧链上交易区块的签署工作，定义网络的共识历史。

2) 看守者(Watchmen)：负责在主链上签署交易，将资产从侧链转移到主链。

这两类工作者可以是相互独立的。区块签名者对于产生区块链共识以及促进侧链账本而言是必要的。当资产在区块链之间进行传输时，看守者只需要处于在线状态即可。

作为一个极端的例子，我们可以想象这样一个方案，其中看守者每天只在线一次，来解决预先批准的进出境交易。这两个功能是通过单独的专用强化盒(dedicated hardened boxes)来执行的，并由拥有操作所需密钥材料的所有者进行配置。

网络元素之间的相互作用，正如图3所示。在区块签名者与看守者之间，只有前者是需要产生区块链共识的，它们是通过下一章节内容中描述到的协议进行的。

(图3：关于强同盟链与其他区块链之间进行互动的示意图)

三、技术细节

在技术层面，支持强同盟方案，需要发展两种类型的同盟：同盟锚定(Federated Peg)和同盟区块签名(Federated Blocksigning);

A. 同盟锚定(Federated Peg)

《启用锚定侧链区块链创新》[22]的作者提出了一种部署同盟侧链的方法，它不需要对比特币区块链的共识规则进行任何改动。在他们的方法论中，一个侧链使用了3 of 5(即5个当中要求至少3个)互不信任的同盟参与者，称之为工作者(functionaries)，他们负责分别确认和签署链区块(区块签名者)以及锚定操作(看守者)。而同盟锚定(Federated Peg)则是一种工作者在两条区块链之间进行资产转移的机制。

工作者至少会观察两条链(比特币区块链和侧链)，以验证它们之间的资产转移。为了符合强同盟的标准，工作者就需要使用一套分布式服务器(分布在不同的管辖区)，以此创造出一个妥协主义者工作者网络。这个网络保留了完全去中心化安全模型的部分有益性质。

同盟锚定(Federated Peg)的成员各自经营一个(运行比特币和侧链节点，以及用于创建和管理跨链交易的)安全服务器。每个服务器包含了一个(管理密码学密钥及签名的)硬件安全模块。该模块的主要工作就是保证网络的安全，如果被检测到危险，根据设计，系统会删除掉所有密钥，致使网络被冻结。

如果一个或少数几个工作者(机构)遭受到了攻击(即使他们的防篡改硬件完全受损)，系统也不会受到影响，只要有足够的其他工作者是完整的。而成功篡改这种同盟锚定系统，至少要求攻破大多数工作者(区块签名者和看守者)。

即使这样，篡改也是很容易检测到的，例如，当不相容的区块出现时，大多数区块签名者的妥协情况就可以观察得到。如果大多数看守者仍然是安全的，侧链持有的价值就无法在主链上赎回。

B. 拜占庭鲁棒性

比特币挖矿方案最重要的方面之一，就是拜占庭鲁棒性，这意味着任何缺少多数恶意成员的情况，都无法重写历史或审查交易[24]。这种设计的目的，就是创建鲁棒性，即使是在“次多数”算力长期进行攻击的情况下。比特币允许所有矿工同等地参与，并简单地宣布获得多数算力的的链为有效链。

也就是说，攻击者若无法掌握多数算力，就无法重写历史记录(最近的几个区块，并且概率非常低)，而这样做，最终其实是在浪费资源。这就鼓励矿工加入诚实的多数队列，从而增加了攻击的难度。但是，正如第一章节A部分内容中所讨论的，这个设置由于网络数十分钟的心跳而导致延迟问题，并引入了重组风险(即使当各方都是诚实的时候)。

C.在强同盟中达成共识

很显然，工作者的经济利益与同盟的正确运作相一致，将是至关重要的。显然，依靠随机分派的志愿者来支持具有重大价值的商业侧链是错误的。而激励措施的加入，就可以让强同盟参与者达成共识，这在商业当中是一个普遍存在的模式 [25]。激励可通过托管、代理分配或外部法律构造的方式(如保险政策和履约保证)实现均衡分配。

1)强同盟中的区块签名操作：为了让一个强同盟系统成为低延时的，同时消除少数敌对方重组攻击风险，其通过固定签名者集，从而取代了动态矿工集。类似于私链[26]，脚本的验证(可以把subject改变成固定规则或者静态规则)代替了工作量证明共识规则。

在同盟链中，这个脚本实现了一个k of n的多重签名方案。这个机制需要达到某个阈值数量的签名者签名区块;也就是说，在n个签名者当中，至少需要有k个签名者同意。因此，它可以模仿比特币的拜占庭鲁棒性：少数受妥协的(非诚实)签名者将无法影响系统。

(图4：在强同盟网络中的同盟区块签名过程)

图4展示了强同盟链如何达成共识。这个共识过程被称之为同盟区块签名，其包括以下这几个步骤：

步骤1：区块签名者为其他所有签名参与者提出候选区块;

步骤2：每个区块签名者通过预先承诺，对给定候选区块进行签字，以此来表明他们的意图;

步骤3：如果满足阈值X，则每个区块签名者会签署这个区块;

步骤4：如果满足阈值Y(可能和X是不同的)，区块则被接受，并发送到网络。

步骤5：下一名区块签名者提出下一个候选区块，然后重复以上过程。

当然，和任何区块链协议一样，人们可以想象其它协调工作的签名方式。然而，这一提出的方案改善了现有比特币共识机制的延迟和流动性问题，同时不引入单节点故障或在I-A章节内容中提到的更高的信任要求。

2)安全改进：由于比特币当中区块生成的概率，因此其存在最近区块发生链重组的倾向 [27]。由于强同盟的区块生成并不是概率分布的，它是基于固定的签名者集生成的，这可以让重组发生的可能性变为零。这可以显著减少确认交易的等待时间。

拜占庭鲁棒性针对两类攻击向量提供了保护。在第一种情况下，重要部分的节点可以从网络中分离出来，以此断开可用性。在第二种情况下，大多数节点可以受到攻击者的破坏和操控，从而破坏系统的完整性。

在一个强同盟系统的区块签名，最多可抵抗 2k − n −
1个攻击者。也就是说，只有2k − n个拜占庭攻击者将能够在同一高度的冲突区块被签名，从而分叉这个网络。举例来说，5-of-8的阈值将会是1级拜占庭鲁棒，而6-of-8的阈值就会是3级拜占庭鲁棒。另一方面，如果至少有n − k + 1个签名者无法签名，区块就无法产出。因此，提高k的阈值就对分叉提供了更强的防御，但减少

了对不可用签名者的网络恢复能力。

在论文第七章节D部分内容，我们解释了相同的策略如何可被用于工作者更新，这方面是未来的计划工作。

四、应用案例

强同盟被用作一种解决区块链交易延迟时间、商业隐私、可替代性和可靠性问题的技术解决方案。很多区块链应用可通过强同盟技术解决方案避免这些问题，这里强调两个主要应用：

A. 国际交易所和Liquid

比特币目前可用于汇款和跨境交易支付，但其性能受到技术和市场动态 [29]的限制。公共比特币网络的高延迟问题，要求比特币和多个交易所以及经济环境绑定在一起，同时比特币有限的隐私性增加了运营成本。

由于交易所市场之间是不相连的，这些交易所的交易可能会出现流动性不足的影响。因此，很多商业实体会选择明确高频次的交易
[20]方法。这些围绕比特币固有局限性的尝试，由于中心化和其它缺点
[29]而引入了弱点。

我们已开发出了一种称为Liquid的特殊解决方案，其通过利用比特币，可促使国际交易所变得更为有效。图5当中，展示了这种解决方案的大致原理，并且它也是第一个强同盟实现方案。作为一个强同盟，Liquid具有新的安全性及信任假设。这种系统的等待时间要比比特币区块链更少，同时它的信任模型要比其它更中心化的系统要更健壮(但肯定不如比特币本身)[30]。

(图5：通过Liquid系统进行的国际交易流程)

今天，这种Liquid实现方案允许一分钟出块。它将有可能减少预提交所需的时间，以及网络穿越的约定阈值时间(正如第三章节B部分内容中提到的)。这种权衡，对于实现新的服务于商业需求的行为而言，是值得的，而这恰恰是完全去中心化的比特币区块链，或中心化的第三方解决方案所无法提供的。

Liquid作为一个强同盟方案，其中的工作者就是参与网络的交易所，而资产就是从爱丽丝转移到鲍伯的某些密码货币。如图5所示，当爱丽丝想把钱转给鲍伯时，她会联系自己所喜欢的交易所。该交易所的当地节点会仔细寻找合适的交易所节点，

通过Liquid强同盟系统将资产转移到鲍伯。他们会谈判条件，例如交易汇率、执行时间，以及通知爱丽丝有关结果(如果她同意把资产转让给鲍勃)。

由于Liquid是在侧链上运行的，我们使用了多重签名方案，如果11个参与者当中有8个参与者同意一笔结算，那么鲍伯就可以收到他的钱。而Liquid的存在，就可以加速交易确认的过程。反过来，这又降低了交易结算期间比特币估值变化的风险，这对于成功套利和汇款操作而言是非常重要
[31]。汇款接受者最终会收到最初发送者的比特币，但将减轻波动带来的风险。

由于转移时间的减少，套利成本因此而降低， Liquid参与者市场将表现为一个统一市场。此外，因为Liquid资产拥有了多个法币进出口，且延迟较少，汇款人可实现结算多种法币。本质上，Liquid降低了关于货币的资本约束。

通过增加资金的安全性，Liquid 可改善整个比特币市场的潜在可靠性。而隐私方面的改善，得益于保密交易技术的采用，关于这一技术，我们将在第五章部分作进一步的讨论。这为系统用户提供了更强的商业隐私保护。

例如Liquid这样的强同盟方案改善了隐私、交易延迟以及可靠性，而不会让用户暴露于第三方信任方所引入的风险。通过将业务流程移动到Liquid，用户可提高他们的效率及资本储备要求。

B. 其它金融技术

当前金融服务产品的重要部分，在于依赖可信中介(以及当这种信任破裂时，需要依赖的法律基础设施)或中心化操作系统 [32]。而新的、公开可验证的共识系统(例如比特币)则具有潜力替代它们，因为这些共识系统提高了安全性和可靠性 [33].例如，流动性供应是主要券商和投资银行的基本业务模型[34].基金经理们，会在降低投资管理相关成本的前提下，将资金投入到一个单一的监护地点，同时可改善对投资机会的访问及流动性。

第三方券商然后让每个参与者获得各自对手方的流动性;聚焦的资本将在一个受信任的第三方保管人的管理之下[35]。通过让客户买入、卖出和对冲交易，这一制度为投资者提供了访问流动性的优先选择手段。

这些中心化的系统，为市场参与者提供了便利，但它们并非没有风险。一个现实的例子是：全球金融危机之后出现的欧元体系。欧元体系的资产清算努力，通过抵押33个复杂的证券来完成，但其造成的损失却超过了10亿欧元
[34].而类似这样的问题，就可以通过一个强同盟系统来解决。

当遇到所有权声称，以及防止未抵押资产的交易时，强同盟系统可以移除掉信任元素，同时允许系统的现有成员和新成员进行审计。此外，资产的所有权可以得到公开核实。

五、创新

在本章节内容当中，我们主要讨论以下这些设计亮点：(1)对交易延迟和可靠性的改进;(2)对隐私性的扩展;(3)硬件安全模块的创新;(4)以及对原生资产有趣的修改;

A. 对确定性、交易延迟以及可靠性的改善

比特币的工作量证明是一个随机过程，而强同盟方案则是确定性的，其中每个区块预计将由单方生成，因此重组就无法发生。在一个强同盟链中，区块签名者需要在扩大历史之前获得共识，因为它们是一个小而定义明确的集合，其网络心跳可能比比特币快很多。这意味着强同盟的用户可考虑单个表示不可逆性的确认;当信息在同盟成员之间传播并添加到区块当中时，该确认便发生了。这也意味着这些区块将可靠地按计划生成，而不是一个随机的过程。

B.隐私和保密

虽然在很多用户的认识当中，区块链会固有地提供强大的隐私性，但这一点一再地被证明是错误的 [36] [37] [38] [39] [40]. Liquid的强同盟方案，使用了保密交易 (CT) [21]技术，通过密码学的方式验证用户的行为，而不会提供交易的具体细节。

因此，强同盟链的资产转移可在对手方之间保持私密性，同时对网络参与者而言是可验证的。为了保护隐私，保密交易 (CT) 技术会遮蔽所有输出的数量，以避免关于交易的信息泄露给第三方。我们也可以使用传统的比特币隐私技术(例如CoinJoin [41])来合并输入与输出。在通常的应用当中，这样的机制会因为公众数量因素 [12]的存在而被大大削弱，而Liquid所使用的方案，其交易图表不再公开这些相关性[42]。保密交易 (CT)
技术作为Liquid当中重要组成部分的两大原因在于：商业可用性和可替代性。

当谈到前者时，如果大多数公司的内部账本和财务行为是完全公开的，那它们就无法经营下去，这是因为私密的商业关系及商业秘密是可以从交易记录中推断出来的。而引入保密交易 (CT) 技术，这些就不再是问题了，因为关于交易的信息已经被隐藏起来了。而另一点，对可替代性的改进也是很重要的，不然的话，资产的历史是可以通过公共记录进行追溯的，对于“问题资金”的情况，这可能是有问题的，当局可能会将其定义为非法或可疑交易[43]。

如果一个资产的历史可以被追溯，那么网络用户可能会发现，他们有义务确保自己没有收到这些问题资产。而这样的司法鉴定工作，会给网络用户和运营商带来巨大的技术负担，如果多个司法管辖区的定义冲突或不明确 [43]，这种辨别工作也就成为了不可能。这对于任何能够来回传递有价值历史的系统而言，都会具有潜在的风险。而通过改进可替代性，这是可以得到纠正的。

不幸的是，保密交易 (CT)
技术的使用是有代价的：这使得交易数据会变得更大，且需要更长的时间来验证。

在 Liquid系统当中，所有交易都会默认使用保密交易 (CT)
技术，这使得网络操作计算变得密集型。而Mimblewimble [44]这种方案，也是完全安全的，它也不需要完整的历史链数据，因此它也是一种可行的方案，其能够提供的隐私性，甚至比保密交易 (CT)方案更佳，且其扩容效果也是非常好的。关于Mimblewimble技术方案，我们将进行进一步的调查研究。

C.硬件安全

在强同盟方案中，k of n多重签名方案就需要用到足够安全的硬件，这就需要跨越多个未知的位置及条件。签名密钥需要存储在设备上，而不是服务器上，它的原因很简单：即使应用程序代码是无疵可寻的，为了获取访问主机和任何密钥的权限，攻击者也是可以利用网络堆栈漏洞的。

虽然多年来，人们通过虚拟化、内存保护等手段来保护网络，该领域仍然无法有效做到成功防御 [45]. 今天，最好的解决办法就是使用简化的接口和物理隔离方案;而Liquid特别创建了一种用于密钥存储和签名的单独硬件设备，以显著减少攻击途径的数量。

虽然密码算法的公开验证及协议改善系统安全性，已然是事实，但我们无法将这种说法放在硬件设备身上。事实上，任何措施，最终都有可能被拥有无限样品硬件供应的攻击者所攻破。然而，如果这种硬件要求昂贵、高度专业化的设备，并且需要很高的技能要求，它就降低了攻击者的可能人群。

当用于破坏系统的技术是破坏性的情况下，这就更是如此了，这要求任何给定硬件[46]需要多个副本。不幸的是，用于安全目的的硬件混淆方法，其价值只有在系统被破坏之前才是成立的。在遭遇攻击之后，保护硬件的唯一方法就是改变它的设计。

因此，强大的同盟硬件还应包括一个应对系统，当硬件遭受攻击时，这种应对系统要么发出警报，或者简单地删除可能被针对的信息。传统上，硬件安全模块(HSMS

)当记录到一个重大的环境变化时(例如突然过热或冷却，温度超出运行操作范围，或其它环境波动 [47])，便会这般应对。

D.支持多种原生资产

强同盟系统除了支持比特币，其还支持其它数字资产的会计处理。这些原生资产可以由任何用户发行，并与基础的比特币分开核算。参与者通过资产生成交易发行这类资产，可选的设置条件(例如增发)可在未来进行扩展：

1) 资产发行人决定资产生成的政策，包括用于赎回的带外(out-of-band)条件;

2) 发行人创建一笔带有一个或更多特殊资产生成输入的交易。注意，最初的资金可以发送到多个不同的输出。

3)资金生成交易是由一个强同盟参与者确认的，经过确认后，这个资产就可进行交易了。资产发行人使用标准强同盟交易，按客户基础分配其资产;

4)希望赎回其资产通证的客户，可将他们的资产股份归还给发行人，以换回带外(out-of-band)商品或所代表的服务。然后发行人就可以销毁通证
(即将通证发送到不可花费的脚本，例如OP-RETURN).

在今天，用户只能与一种资产类型进行交易，但系统设计是允许多种资产参与单笔交易的。在这种情况下，共识规则会确保会计等式适用于每个单独的资产分组。这就允许资产交易是无需信任的，并且是在没有任何中介的单笔交易中进行的。当第二种情况发生时，希望交易资产A和资产B的两位参与者，将联合达成一项带外汇率的协议，并产生一笔带有“甲方拥有A输入，以及乙方拥有A输出”的交易，然后，再产生另一笔带有“乙方拥有B输入，以及甲方拥有B输出”的交易。这将导致具有相等输入和输出量的一笔交易，因此，只有当双方签名时，这笔交易才会生效。

令人惊奇的是，这种创新不仅可用于货币交换，它也可以用于任何其它数字资产，包括：数据、货物、信息。

该协议可通过更先进的签名哈希机制做进一步的改进。

E. 锚定退出授权(Peg-out Authorization)

从任何带有固定成员集的私密侧链(其隐私性要比比特币更强)中移动资产时，目标比特币地址可控制侧链的一些用户，是可取的。这可以防止侧链上的恶意或错误行为(可由参与者解决)影响到更广的比特币网络，这个过程是不可逆的。

由于将资产移回到比特币区块链是由看守者集在负责把关的，他们就需要一个授权密钥的动态私密白名单。也就是说，用于固定签名密钥的看守者成员，需要能够证明一些比特币地址的控制权，而不会把自己的身份与它联系起来(除了他们属于这个团体的事实信息)。我们把这种证明称为锚定退出授权证明，并通过以下设计来完成它：

1)设置：每个参与者i 选择两个公私钥对 (Pi, pi)以及 (Qi, qi)。这里的Pi是一个“在线密钥”，而qi是一个“离线密钥“。参与者把Pi和qi这两个密钥交给看守者。

2)授权：为了授权一个密钥W(将对应一个单独控制的比特币地址)，参加者需要进行以下的行为：

a) 她计算

Lj = Pj + H(W + Qj )(W + Qj )

对于每个参与者索引j，这里的H是一个将组元素映射到标量的随机预言哈希。

b) 她知道Li的离散对数(因为她知道Pi的离散对数，并选择了W，所以她对W + Qi也是了解的)，因此可以产生一个覆盖每个Li的环签名。她这样做后，便签署了在线和离线密钥以及W的完整列表。

C)她把最终的环签名发送给看守者，或者将其嵌入到侧链;

3)转让：当看守者产生一笔将资产从侧链转移到比特币区块链的交易时，他们需要确保交易的每一个输出都是 (a)由他们所拥有，或者 (b)
具有关联其地址的授权证明;

这个方案的安全性，可以用一个直觉论证来证明，首先，由于授权证明是覆盖密钥集的环签名，对于生产它们的参与者而言，便相当于零知识 [48]。第二，密钥方程

Lj = Pj + H(W + Qj )(W + Qj )

是有结构的，这使得任何签署Li的人都知道：

1) W、pi 以及 qi的离散对数，或者

2) pi，但不是qi或者W的离散对数。

换句话说，攻破在线密钥pi，就允许攻击者授权(无人知道离散对数的)“垃圾密钥”。只有同时攻破pi以及qi密钥，攻击者才可以授权任意密钥。然而，要想攻破qi密钥是很困难的，因为这一方案的设计是：qi不需要在线授权W，在签名时只需要计算W + Qi。之后，当i想要使用W时，她会使用qi来计算其离散对数。这可以离线完成，并且具有更昂贵的安全要求。

六、评估

通过强同盟系统进行移动的信息，将是非常敏感的。因此，深入了解潜在的安全威胁是至关重要的。对于处理比特币交易时，尤其如此(交易不可改变)。换言之，网络的持续运行是次要优先级，很少有人会因为延迟问题而愿意把资金放到小偷唾手可得的地方。

当强同盟系统中累积的资金总价值增长时，攻击者的动机也就随之增加，重要的是，我们不能让攻击者成功地瞄准任何代码库的维护者。值得高兴的是，当参与者不断增加强同盟系统资产总价值的同时，参与者自然会受到激励，因此他们会更加小心地访问同盟签名者。因此，同盟安全模型会与参与者的利益对齐。

A. 与现有解决方案的对比

为比特币这类系统形成共识的现有方案一般分为两类：

一类是尝试保留比特币去中心化特性的同时，提高效率或交易吞吐量;另一类是采用不同的信任模型。第一类方案有GHOST [49],区块DAG[50] [51]以及Jute [52]。这些方案保留了比特币由动态匿名矿工集生成的区块模型，并且依赖于复杂而微妙的博弈论，以确保共识维持一种去中心化的方式。而第二类方案应用者，包括恒星Stellar [53] 以及Tendermint [54]。

这些例子存在着与可信方相关联的故障风险，当扩散到复杂的网络拓扑结构时，会导致严重且难以分析的失效状况 [55]。而我们的提议是在一组固定的、彼此间互不信任，但可识别参与者的集合下工作的，因此只需支持简单的信任模型:只要有足够数量的参与者继续诚实工作，则系统就可继续运作。

平行共识系统，是指寻求使现有共识系统实现更快、更便宜交易执行的系统。主要的例子就是闪电网络[56]，这允许各方通过之间的相互作用进行交易。我们观察到，这些系统依附于现有的区块链，它们是作为补充的新共识系统，包括本论文当中描述的强同盟方案。

最近，Eyal 等人提出了一个非常新颖、有趣的称为Bitcoin-NG的方案 [57]，虽然

这种方案还没有应用到市场上，但它是一种新的区块链扩容协议。根据实验，这一方案的带宽限制仅限于单个节点的能力，而延迟时间则受限于网络的传播时间。

B.保护机制

攻击者想要攻击一个系统，必须先与系统进行通信，因此，强同盟系统的通信策略，已被设计为将其与普通攻击向量隔离出来。

我们可采取几种不同的措施，以防止不可靠的各方与工作者通信：

工作者通信，受限于已知对应于对等工作者的硬编码Tor隐藏服务地址。

工作者间的通信，是通过使用硬编码的公钥，以及每个工作者签名密钥来进行认证的;

远程程序调用(RPC)的使用，受限于工作者硬件，以及Liquid钱包的部署(只针对本地系统的访问者)

除此之外，关键的政策是保护网络。而区块签名者的密钥设计，是在任何情况下都是不可恢复的，而看守者的密钥，必须在密钥恢复过程中创建。区块签名者的密钥丢失，需要强同盟共识协议的一次硬分叉，虽然这是很难的，但其还是存在着可能，并且不会冒任何损失资金的风险。然而，损失足够多的看守者密钥，会导致比特币的丢失问题，而这必然是不可接受的。

虽然强同盟的设计是拜占庭鲁棒性的，工作者依然要注意避免被恶意者控制，这是很重要的。而设计用于检测攻击工作者的防篡改传感器，当确定攻击正在进行时，它们需通知网络中其它工作者关于其无法保证数据完整性的信息。在这种情况下，可依靠的方案，就是关闭个别的系统，而在最糟糕的(即网络拜占庭鲁棒性遭到潜在威胁)情况下，网络本身应以关闭处理。

这可以确保受损系统不会对比特币区块链造成影响。即确保用户资金的直接安全性，以及用户对系统持续正确操作的信心。

C. 备份撤回

Liquid这一强同盟链是公开可验证的，从原则上讲， Liquid系统中的比特币持有者应可以把他们的资产从Liquid侧链移回到比特币主链(即使是在Liquid网络遭到DoS攻击，或因其它原因而停滞的情况下)。

要做到这一点，最直接的方法是：看守者提供时间锁定的比特币交易，将币退还给它们原来的主人。然而，这也会遇到一些延迟问题(数小时甚至数天)，在这个时间间隔内，币的实际拥有者可能会发生多次变化，因此，这种解决办法就不起作用了。比特币无法提供一种好的办法。但是，我们可以设置一个“备份撤回地址”，它是由大多数网络参与者(工作者以及外部审计员)共同控制的。通过这种方式，如果Liquid发生了停滞的情况，受影响方有可能集体决定适当的行动。

D.可用性和拒绝服务

在一个强同盟系统中进行区块签名操作时，会有两个独立的阈值：签名阈值和预提交阈值。前者代表着网络不可更改的性质，并可设置为具有恢复性，它也可以调整到支持备份区块签名者(通常是不在线的)更为先进的政策。

而在另一方面，预提交阈值，仅仅是由签名者决定的，它们可以被设定为高水平(甚至需要签名者的匿名性)，并根据网络条件要求而改变。这意味着，即使网络区块签名者规则，原则上允许拜占庭攻击者引发分叉，在实践当中，恶意用户(最坏的情况下)仅能造成网络拒绝服务，只需要区块签名者设置足够高的预提交阈值就可以防止。而软件错误或硬件故障，可能会导致网络在单个工作者的情况下出现故障，致使暂时无法提供功能。

而这样的参与者，将无法再次参与共识协议或批准提款到比特币网络。除非有足够多的工作者失败，导致签名阈值是不可实现的，否则网络就会继续正常运行。在这种情况下，资金将在一定时间内无法移动(无论是在侧链内部还是返回到比特币主链)。一旦工作者恢复至完全运作状态，网络将继续运行，而资金则不会受到威胁。

E. 硬件故障

如果区块签名者遭遇到硬件故障，并且加密密钥出现不可恢复的情况，则整个网络必须同意更改签名规则，以允许替换区块签名者。

一个更为严重的场景，涉及到了看守者的失效，由于其密钥是在比特币网络当中使用的，因此无法通过硬分叉的方式从当前比特币签名集中恢复过来。如果单个看守者失效了，它可以被替换掉，而另一个看守者可以把锁定的资金移动到新看守者所持有的密钥下。然而，如果太多的看守者同时失效，并且他们的密钥丢失了，这些比特币就是不可挽回的了。

正如第6章节C部分内容提到的，这种风险可通过备用撤退机制得以减轻。预防机制包括提取与备份看守者密钥材料，如此，在发生这样的故障时，比特币资金就可以得到恢复。而对提取密钥进行加密，可确保它们只能通过原持有者或独立审计师访

问。这就防止了个别看守者提取密钥材料，并用于恶意操作的情况。

F.重写历史

有可能的是，区块签名者可通过分叉一个强同盟区块链，来尝试重写历史。相比比特币，如果某人持有一个签名密钥，那么签署一个冲突的历史，其实是相当便宜的。然而，重写链的历史，就需要攻破存储于安全保护状态下的区块签名者密钥。这种攻击是不太可能的，因为这需要确定几个签名者的位置，而这些签名者分布在全球多个国家的不同区域。此外，这种攻击是可检测的，并且任何人都可以发布出一个证明(包含冲突区块的区块头信息)，然后进行自动停止网络操作，直到问题得以解决(即被攻破的签名者被替换掉)。如果网络以这种方式分叉了，主动攻击者通过向两条分叉链提及冲突交易，以此扭转自己的支出交易，这是可能的。因此，任何不具有高度唯一性的有效区块，都应该被认为是无效的。

G.交易审查制度

通过攻破阈值数量的区块签名者，攻击者可潜在地强制执行选择性交易签名。这种情况，可在合法签名者之间发生冲突等情况下看到。这种类型的审查，是无法通过机器来检测的，尽管它可能是明显的。而在这种情况下，强同盟网络可使用其它攻击的相同应对机制，来替换或删除掉攻击签名者，

H.锁定比特币的没收场景

如果有足够多的看守者进行勾结，他们可以克服多重签名阈值，并没收目前侧链上所有的比特币。针对这样的情况，我们可以设置关于锁定比特币的高阈值签名。这是最为极端的一种串谋情景。然而，这样的方式会削弱看守者密钥材料丢失的恢复能力。对于这种情况，在同盟签名技术成熟时，我们必须要进行成本效益分析。

七、 未来的研究

虽然强同盟方案引入了新的技术解决方案，以解决各类长期存在的问题，但创新之路是没有尽头的。我们最终的设计目标，是实现一个广泛分布的网络，其中操作者是在物理上无法被干扰的，或者可通过任何方式与应用层进行交互，而在完全停止运作的情况下，我们可用备份计划将资金返回到比特币主链。

A. 进一步加强工作者

我们需要做更多的研究，以确保工作者无法被物理篡改，并保证网络交互是合法的、可审计的。未来的工作包括具体的设计改进或者进一步的密码学改进。在一个强

同盟系统中，被控制的(或恶意)工作者无法窃取资金、重写交易，或以任何方式影响系统的其他用户。

然而，足够多的恶意工作者总是可实现拖延网络的(通过拒绝与其他工作者合作，或完全关闭运行)。这可能会冻结资金，直到自动退出机制启动。因此，研究创造一个激励机制可能是有益的，这可以鼓励工作者节点在遭受攻击时仍然保持在线状态。这些激励措施可以防止某些拒绝服务攻击。

B. 加强Liquid

强同盟网络的隐私性和速度，可通过和闪电网络结合得到进一步改进[56]。正如比特币网络一样，初始系统的吞吐量是有意进行限制的，区块中发布的交易，是必须要对网络所有参与者可见的。这个阈值是根据(让每个人看到并验证每个操作的)需要来设定的。而有了闪电网络，个人交易只需要由参与方验证
[56]。这戏剧性地减少了所有参与者的验证负载。

因为终端网络速度是唯一的限制因素 [58], 它也大大减少了网络延迟的影响。此外，强同盟中的节点可通过闪电网络(双向支付通道智能合约网络)实现route支付。这可能会使Liquid网络可实现更高效的进入和退出操作。此外，闪电网络可以替换掉链间的原子交换智能合约，以及可能的混合多链传递性交易 [26]
，而不会有单一动态成员多方签名(DMMS)链的限制。

C.保密资产 (CA)

保密交易(CT)技术可隐藏交易资产的金额，但无法隐藏掉资产类型，因此它的隐私性并没有那么强。

然而，保密交易(CT)技术是可以扩展到隐藏资产类型的程度的。对于任何交易来说，除了交易方之外，其他人是无法确定哪些资产并且有多少金额的资产在被交易。这种技术方案，我们称之为保密资产 (CA)，该技术可提高用户的隐私性，并允许非相关资产类别的交易在单笔交易中秘密进行。然而，这种方案给予资产的隐私性与保密交易(CT)，在性质上是有差异的。假设一笔具有资产类型A和资产类型B输入的交易。所有的观察者都知道具有资产类型A和B的输出，但他们无法确定哪些输出具有什么意义(或者他们是如何分裂的，以及有关他们数量的任何事情)。

当交易发生时，输出(关于资产类型)会变得越来越模糊，除了个别交易者之外，其他人就无法知道这些输出的真正类型。如果发布的交易总是有多种资产类型，那么非参与者观察者就无法得知关于输出的真实类型。

D. 拜占庭鲁棒性升级路径

大多数加强方法依赖于中心化的、可信第三方，而这对于强同盟系统而言是一个威胁模式，因为任何单一故障点都可能被攻破。在任何大的系统当中，我们必须假设其中一部分可能处于故障状态或在任何时间点会遭受攻击。这意味着对于中心机构而言的简单程序，会变得更加复杂。

不幸的是，创建一个敏捷的网络或可升级的系统，是需要权衡安全性的，而理想的平衡是难以达成的：随着网络独立性的增长，成本和升级难度也会随之增长。因此，代码中的所有更改都应适用于所有方，并且过程应该是在工作者集当中(K of N)共识驱动的。这些改变也应该是完全可审计的，且在应用前是透明的。

最后，新成员的增加，或对网络的严格改进等维护过程，也必须确保整个系统的拜占庭安全性。对于比特币而言，这是通过长尾上游方式实现的，这是一个可审计和开源的程序，最终每个用户来自行决定验证的共识规则(也就是说，有争议的更改，可能会导致永久性的链分裂)。

(图6：为强同盟网络计划的拜占庭鲁棒性升级模式)

对于强同盟系统而言，这将通过一种升级程序的设计与实现来完成，它允许对系统进行迭代改进，而不会让攻击面生效(通过模仿比特币的软分叉升级路径)，正如图6所示，这遵循以下这些步骤：

1) 上游软件提供商(USP)编写工作者网络的软件更新，并为工作者提供相应的更新;

2)外部安全审计员可审阅软件更新和文档的正确性，验证文档及代码库本身的准确性;

3)每个工作者验证上游软件提供商(USP)以及可能的第三方审计师的签名，如果愿意的话，也可以进行审查或审计这些更新;

4)每个工作者在服务器上签名更新，并把结果签名返回给上游软件提供商(USP);

5)一旦大多数工作者签署了更新，上游软件提供商(USP)会把他们的签名和更新图像化为一个单独的package文件。这个文件，包含了更新图像、文件以及绝大多数工作者签名，然后将其分发给每个工作者;

6)每个工作者会在自己的服务器接受到上游软件提供商(USP)以及绝大多数工作者

的签名;

7)工作者验证这些package文件内容，然后应用更新;

请注意，这种情况假设了多数诚实参与者。在其他场景下，例如，一组协作的恶意工作者可集体拒绝任何给定的升级路径。对抗这类情况的方法，将有待于我们做进一步的研究。

八、结论

比特币的普及，表明了工作量证明这种无需许可的机制对发展基础设施而言是有效的。数十家公司投入了数亿美元的巨资，用于比特币的芯片及网络设计(包括数据中心管理，以及冷却系统 [60])。这些资源团体所提供的安全价值是巨大的。然而，比特币的工作量证明机制也会带来明显的缺点：增加了区块的等待时间，以及建立广泛分布的、共享当前账本状态的检查点。

本论文介绍了一种强同盟系统：其同盟共识机制显著缓解了使用工作量证明机制在真实世界可能引起的系统风险。这种解决方案，通过具体的实施决策以及最小化攻击面，可抵抗广泛的攻击种类。强同盟方案利用了侧链技术，以及保密资产技术，可有效改进区块链技术。目前的硬件安全模块(HSM)，对于只用于不和过去签名发生冲突的有效历史区块签名而言，只有有限的验证能力。

这不仅仅是因为安全硬件的性能局限性，还因为任何进入硬件安全模块(HSM)的东西，都会变得不可更改，这使得复杂规则集变得更困难，也难以去部署。改进的验证，需要硬件安全模块(HSM)支持一个有足够能力的升级路径，同时反对未经授权的升级尝试。或者，每一次软件部署，都意味着一个新的硬件安全模块(HSM)部署，但这种方式显然是不具备成本效益的(即费钱的)。

而第一个能够应用的强同盟系统就是Liquid：这是一个绕过比特币固有局限性，同时利用其安全属性的比特币交易和经纪多重签名侧链。Liquid的系统，通过一种k-of-n的多重签名方案，以替代比特币的SHA256工作量证明机制。

在这种模型下，共识历史即是一个区块链，其中每个区块，是由大多数确定的、全球分布的工作者集来完成签名的，并且这个过程将通过直接激励参与者的方式，来加强系统的安全性。强同盟方案在很多通用行业都将是有用的。尤其是那些试图数字化资产，同时需确保安全，并且需要保持私密性的行业。