雪崩站台
2020/06/30

Kevin Sekniqi、Daniel Laine、Stephen Buttolph 和 Emin Gu–n Sirer

摘要本文提供了雪崩平台第一次发布的架构概述，
代号为北冰洋雪崩。有关标有$AVAX 的本地代币的经济性的详细信息，我们
引导读者阅读随附的 token dynamics 论文[2]。
披露：本文描述的信息是初步的，随时可能更改。此外，本文可能包含“前瞻性陈述”[1]

Git 提交：7497E4A4BA0A1EA2DC2A111BC6DEEFBFF3023708E

1 导言

本文提供了雪崩平台的体系结构概述。重点关注平台的三个关键区别：引擎、体系结构模型和治理机制。

1.1 雪崩目标和原则

雪崩是一个高性能、可扩展、可定制且安全的区块链平台。它针对三个 15 个广泛的用例：

–构建特定于应用程序的区块链，跨越许可（私有）和无许可（公共）部署。
–构建和启动高度可扩展和分散的应用程序（DAPP）。
–使用定制规则、契约和附加条款（智能资产）构建任意复杂的数字资产。

Avalanche 的首要目标是为数字资产的创建、转移和交易提供一个统一的平台。

通过构造，雪崩具有以下特性：

*可伸缩*雪崩被设计成具有大规模可扩展性、健壮性和高效性。核心共识引擎能够支持一个全球网络，该网络可能由数亿个连接互联网的低功耗和高功耗设备组成，这些设备可以无缝运行，具有低延迟和极高的每秒事务量。

*保护*雪崩的设计目的是强健并实现高安全性。经典的一致性协议设计用于抵御多达 f 个攻击者，当面对大小为 f+1 或更大的攻击者时完全失败，而中本一致性协议在 51%的矿工是拜占庭人时无法提供安全性。相反

当攻击者低于某个阈值时，雪崩提供了非常强大的安全保障，这

可以由系统设计器参数化，当攻击者超过此阈值时，它可以提供优雅的降级。即使攻击者超过 51%，它也能保证安全性（但不能保证活跃性）。这是第一个提供如此强大安全保障的无许可证系统。

*分散的*雪崩旨在提供前所未有的权力下放。这意味着要致力于多个客户端实现，而不是任何形式的集中控制。生态系统旨在避免

具有不同兴趣的用户类别之间的划分。至关重要的是，矿工、开发者和用户之间没有区别。

可治理和民主$AVAX 是一个高度包容的平台，任何人都可以连接到其网络，参与验证和第一手治理。任何代币持有者都可以在选择关键财务参数和选择系统发展方式方面投票。

*可互操作且灵活*雪崩旨在为众多区块链/资产提供通用且灵活的基础设施$AVAX 用于安全和作为交换的记账单位。该系统旨在以价值中立的方式，支持在顶部构建许多区块链。该平台从头开始设计，以便于将现有区块链移植到平台上，导入余额，支持多种脚本语言和虚拟机，并有意义地支持多种部署情节。

概述本文的其余部分分为四个主要部分。第 2 节概述了为平台提供动力的发动机的细节。第 3 节讨论了平台背后的体系结构模型，包括子网、虚拟机、引导、成员资格和锁定。第 4 节解释了能够动态改变关键经济参数的治理模型。最后，在第 5 节中探讨了各种

感兴趣的外围话题，包括潜在的优化、后量子加密和现实对手。

命名约定该平台的名称为雪崩，通常被称为“雪崩平台”，与“雪崩网络”或（简单地说）雪崩可以互换/同义。

代码库将使用三个数字标识符发布，标记为“v.[0-9].[0-9].[0-100]”，其中

第一个数字表示主要版本，第二个数字表示次要版本，第三个数字表示补丁。第一个公开版本代号为雪崩北风，是 v.1.0.0。该平台的本机令牌名为“$AVAX”。雪崩平台使用的协商一致协议系列被称为 Snow*系列。有三个具体的实例，称为雪崩、雪人和雪人

冷冰冰的。

2.发动机

对雪崩平台的讨论始于为平台提供动力的核心组件：共识引擎。

出身背景分布式支付和更普遍的计算需要一组机器之间的协议。因此，使一组节点能够达成一致的共识协议位于
区块链的核心，以及几乎所有部署的大型工业分布式系统。近 50 年来，这个话题受到了广泛的关注，迄今为止，这项工作只产生了两个协议家族：依赖于全对全通信的经典共识协议，以及依赖于工作证明挖掘和最长链规则的中本共识协议。虽然经典的协商一致协议可以具有低延迟和高吞吐量，但它们不能扩展到大量参与者，也不能
在成员资格变更的情况下，系统非常强大，这使得它们大多被降级为许可的、大多是静态的部署。另一方面，中本共识协议[5,7,4]是健壮的，但存在高确认延迟、低吞吐量，并且需要恒定的能量消耗来保证其安全性。

雪崩引入的 Snow*协议家族将经典共识协议的最佳特性与中本共识的最佳特性结合起来。基于轻量级网络采样机制，
它们实现了低延迟和高吞吐量，而无需就系统的精确成员身份达成一致。他们的规模从数千人扩大到数百万人，直接参与协商一致协议。此外，协议不使用 PoW 挖掘，因此避免了其过高的能量消耗和随后在生态系统中的价值泄露，从而产生了轻量级、绿色和静态协议。

机理与性质 Snow*协议通过对网络进行重复采样来运行。每个节点轮询一个小的、大小不变的、随机选择的邻居集，如果超级多数支持不同的值，则切换其提议。重复采样直到达到收敛，这在正常操作中很快发生。

我们通过一个具体的例子阐明了操作机制。首先，事务是由
一个用户，并发送到验证节点，该节点是参与协商一致程序的节点。然后通过八卦将其传播到网络中的其他节点。如果该用户还发布了一个冲突的事务，即 doublespend，会发生什么？为了在冲突事务中进行选择并防止双重花费，每个节点随机选择一小部分节点，并查询被查询节点认为有效的冲突事务。如果查询节点收到支持的绝大多数响应
对于一个事务，则节点更改自己对该事务的响应。网络中的每个节点都会重复这个过程，直到整个网络就其中一个冲突事务达成一致。

令人惊讶的是，虽然核心操作机制非常简单，但这些协议带来了非常理想的系统动力学，使它们适合大规模部署。

– *无许可证*、*易受搅动*、*健壮*.最近一批区块链项目采用了经典的
协商一致的协议，因此需要完全的成员知识。在封闭、许可的系统中，了解整个参与者集足够简单，但在开放、分散的网络中，了解参与者集变得越来越困难。这一限制对使用此类协议的现有公司构成了高安全风险。相比之下，Snow*协议即使在任何两个节点的网络视图之间存在充分量化的差异时，也能保持较高的安全保证。Snow*协议的验证程序
享受验证的能力，无需持续的正式会员知识。因此，它们非常健壮，非常适合公共区块链。

– *可扩展和分散*Snow 家族的一个核心特征是它能够在不产生根本性权衡的情况下进行扩展。Snow 协议可以扩展到数万或数百万个节点，而无需授权给验证程序的子集。这些协议拥有同类最佳的系统分散性，允许

每个节点都需要完全验证。第一手的持续参与对系统的安全有着深远的影响。在几乎所有试图扩展到大型参与者集的利害关系证明协议中，典型的操作模式是通过将验证委托给小组委员会来实现扩展。自然，这意味着系统的安全性现在正与小组委员会的腐败成本一样高。此外，小组委员会还受制于卡特尔的形成。

在 Snow 类型的协议中，这样的委托是不必要的，允许每个节点操作员在系统中随时拥有第一手发言权。另一种设计通常被称为状态切分，它试图通过将事务序列化并行化到独立的验证器网络来提供可伸缩性。不幸的是，在这种设计中，系统的安全性只有最容易损坏的独立碎片那么高。因此，无论是小组委员会选举还是分片都不是合适的缩放策略

用于加密平台。

– . 与其他基于投票的系统不同，Snow*协议在对手较小时可实现更高的性能，但在大型攻击下具有很强的弹性。*适应的*

– . 与最长链协议不同，Snow*协议不需要同步性才能安全运行，因此即使在面对网络分区的情况下也可以防止双重开销。在比特币中，*异步安全*

例如，如果违反了同步性假设，就有可能对比特币网络的独立分支进行长时间的操作，一旦分支恢复，任何交易都将失效。

– *低延迟*.如今，大多数区块链无法支持商业应用程序，如交易或每日零售支付。等待几分钟甚至几个小时来确认交易是不可行的。

因此，共识协议最重要但却被高度忽视的特性之一是最终性时间。Snow*协议通常在≤ 1 秒，这明显低于最长链协议和分片区块链，这两种协议的最终期限通常为几分钟。

– *高通量*.Snow*协议可以构建一个线性链或 DAG，可以覆盖数千个 transac-

每秒 5 万次（5000+tps），同时保持完全的权力下放。声称 TPS 较高的新区块链解决方案通常会权衡分散化和安全性，选择更集中、更不安全的共识机制。一些项目报告来自高度控制的设置的数字，从而歪曲了真实的性能结果。AVAX 美元的报告数字直接取自一个真正的、全面实施的雪崩网络，该网络运行在 AWS 上的 2000 个节点上，地理分布在全球各地的低端网络上

机器。通过为每个节点提供更高的带宽和用于签名验证的专用硬件，可以实现更高的性能结果（10000+）。最后，我们注意到前面提到的度量是在基础层。第二层缩放解决方案立即大大增强了这些结果。

共识比较图表表 1 通过一组 8 个关键轴描述了共识协议的三个已知系列之间的差异。

	中本	古典的	雪*
坚固（适用于开放式设置）	+	-	+
高度分散（允许许多验证器）	+	-	+
低延迟和快速终结（快速事务确认）	-	+	+

高吞吐量（允许多个客户端）	-	+	+
轻量级（系统要求低）	-	+	+
静态（未执行任何决策时不活动）	-	+	+
安全参数化（超过 51%的对抗性存在）	-	-	+
高度可扩展	-	-	+

表 1。三个已知的共识协议家族之间的比较图。雪崩、雪人和霜冻都属于斯诺家族。

3.平台概述

在本节中，我们将提供该平台的体系结构概述，并讨论各种实现细节。Avalanche 平台清晰地区分了三个问题：链（以及构建在上面的资产）、执行环境和部署。

3.1 架构

子网子网或子网是一组动态的验证器，它们协同工作，以就一组区块链的状态达成共识。每个区块链由一个子网验证，一个子网可以验证任意多个区块链。验证器可以是任意多个子网的成员。子网决定谁可以进入它，并可能要求其组成验证器具有某些属性。雪崩山麓

该平台支持任意多个子网的创建和操作。为了创建新的子网或加入子网，必须支付以$AVAX 为单位的费用。

子网模型有许多优点：

– 如果验证器不关心给定子网中的区块链，它就不会加入该子网。

这减少了网络流量，以及验证器所需的计算资源。这是在与其他区块链项目不同，在这些项目中，每个验证器都必须验证每一笔交易，即使是他们不关心的交易。

–由于子网决定谁可以进入，因此可以创建专用子网。也就是说，子网中的每个区块链仅由一组受信任的验证器进行验证。

–可以创建一个子网，其中每个验证器都有特定的属性。例如，可以创建一个每个验证器位于某个司法管辖区的子网，或者每个验证器受某个实际合同约束的子网。出于合规性原因，这可能是有益的。

有一个特殊的子网称为默认子网。它由所有验证器验证。（也就是说，为了验证任何子网，还必须验证默认子网。）默认子网验证一组预定义的区块链，包括$AVAX 居住和交易的区块链。

虚拟机每个区块链都是一个虚拟机（VM）的实例 VM 是区块链的蓝图，就像类是面向对象编程语言中对象的蓝图一样。区块链的接口、状态和行为由区块链运行的 VM 定义。区块链的以下属性和其他属性由 VM 定义：

– 块的内容
– 接受块时发生的状态转换
–区块链及其端点公开的 API
–保存到磁盘的数据

我们说区块链“使用”或“运行”给定的 VM。创建区块链时，需要指定它运行的 VM，以及区块链的起源状态。可以使用预先存在的 175 个虚拟机创建一个新的区块链，或者开发人员可以编写一个新的区块链。可以有任意多个区块链运行同一个 VM。每个区块链，即使是运行同一个 VM 的区块链，在逻辑上也独立于其他区块链，并保持自己的状态。

3.2 自举

参与雪崩的第一步是引导。这个过程分为三个阶段：连接到种子锚、网络和状态发现，以及成为验证器。

种子锚任何在没有许可（即硬编码）身份集的情况下运行的对等网络系统都需要某种对等发现机制。在点对点文件共享网络中，使用了一组跟踪器。在加密网络中，一种典型的机制是使用 DNS 种子节点（我们称之为种子锚），该节点包含一组定义良好的种子 IP 地址，其他成员可以从这些地址中访问网络可以被发现。DNS 种子节点的作用是提供有关系统中活动参与者集的有用信息。比特币核心[1]采用了相同的机制，其中 src/chainparams。源代码的 cpp 文件包含一个硬编码种子节点列表。BTC 和 Avalanche 之间的区别在于，BTC 只需要一个正确的 DNS 种子节点，而 Avalanche 需要简单的大多数锚节点才能正确。例如，新用户可以选择通过一组建立良好且信誉良好的交换来引导网络视图 190，其中任何一个单独都不受信任。然而，我们注意到，引导节点集不需要硬编码或静态，并且可以由用户提供，尽管为了便于使用，客户机可能会提供一个默认设置，其中包括经济上重要的参与者，例如客户机希望与之分享世界观的交易所。不存在成为种子锚的障碍，因此一组种子锚无法决定节点是否可以进入网络，因为节点可以通过连接到任何一组种子锚来发现雪崩节点的最新网络。

网络和状态发现一旦连接到种子锚点，节点将查询最新的状态转换集。我们称这组状态转换为可接受的边界。对于链，可接受的边界是最后一个可接受的块。对于 DAG，接受的边界是一组顶点，这些顶点已被接受，但尚未被接受

没有被录取的孩子。在从种子锚收集接受的边界后，大多数种子锚接受的状态转换被定义为接受。然后通过与采样节点同步来提取正确的状态。只要种子锚集中有大多数正确的节点，那么接受的状态转换必须被至少一个正确的节点标记为接受。

此状态发现过程也用于网络发现。该网络的成员集为在验证程序链上定义。因此，与验证器链同步允许节点发现当前的验证器集。验证程序链将在下一节中进一步讨论。

3.3 Sybil 控制和成员资格

共识协议提供了安全保障，前提是系统中最多有一定数量的成员可能具有对抗性。一种 Sybil 攻击，其中一个节点廉价地淹没网络

如果身份是恶意的，这些保证就很容易失效。从根本上说，只有在证明存在难以伪造的资源的情况下，才能阻止这种攻击[3]。过去的系统探索了 Sybil 威慑机制的使用，这些机制跨越工作证明（PoW）、利害关系证明（PoS）、经过时间证明（POET）、空间和时间证明（PoST）和权威证明（PoA）。

在其核心，所有这些机制都具有相同的功能：它们要求每个参与者一些“游戏中的皮肤”以某种经济承诺的形式出现，这反过来为参与者的不当行为提供了经济障碍。所有这些都涉及一种形式的赌注，无论是以挖掘钻机和散列能力（PoW）、磁盘空间（PoST）、可信硬件（POET）或认可身份（PoA）的形式。这些股份构成了参与者获得发言权所必须承担的经济成本的基础。例如，在比特币中，贡献有效块的能力与参与者的哈希能力成正比。不幸的是，共识协议和 Sybil 控制机制之间也存在着实质性的混淆。我们注意到，共识协议的选择在很大程度上与 Sybil 控制机制的选择是正交的。这并不是说 Sybil 控制机制是彼此的替代品，因为特定的选择可能会影响共识协议的基本保障。然而，Snow*系列可以与许多已知的 225 种机制耦合，而无需进行重大修改。

最终，为了安全和确保参与者的激励与网络利益相一致，AVAX 选择 PoS 作为核心 Sybil 控制机制。某些形式的股权本质上是集中的：例如，采矿钻机制造业（PoW）本质上是集中在少数人手中，他们拥有适当的专有技术，可以获得竞争性 VLSI 所需的数十项专利

制造业此外，由于每年都有大量的矿工补贴，PoW 采矿公司的价值流失。类似地，磁盘空间大部分由大型数据中心运营商拥有。此外，所有产生持续成本的 sybil 控制机制，例如哈希的电力成本，都会泄露生态系统的价值，更不用说破坏环境了。这反过来又降低了代币的可行性范围，其中在小时间范围内的不利价格变动可能导致系统无法运行。工作证明本质上是为

有关系购买廉价电力的矿工，这与矿工进行系列化交易的能力或他们对整个生态系统的贡献关系不大。在这些选项中，我们选择了股权证明，因为它是绿色的、可访问的，并且对所有人开放。然而，我们注意到，虽然$AVAX 使用 PoS，但 Avalanche 网络允许使用 PoW 和 PoS 启动子网。

赌注是参与开放网络的一种自然机制，因为它可以实现直接的经济利益论点：攻击成功的概率与定义明确的货币成本函数成正比。换句话说，利益相关节点出于经济动机，不参与可能损害其利益价值的行为。此外，该股份不会产生任何额外的维护成本（除了投资另一项资产的机会

成本），并且与采矿设备不同，如果在灾难性攻击中使用，其财产将被完全消耗。对于 PoW 操作，采矿设备可以简单地重复使用 245 次，或者——如果所有者决定——全部出售回市场。

希望进入网络的节点可以通过首先放置在网络参与期间被固定的桩来自由地这样做。由用户决定赌注的金额和持续时间。一旦被接受，股份就无法收回。主要目标是确保节点基本上共享相同的、基本稳定的网络视图。我们预计将最低下注时间设定为 250 周。

与其他也提出 PoS 机制的系统不同，$AVAX 不使用斜切，因此，当下注期到期时，所有的下注都会返回。这可以防止不必要的情况，例如客户端软件或硬件故障导致硬币丢失。这与我们构建可预测技术的设计理念相吻合：即使存在软件或硬件缺陷，下注的代币也不会有风险。

在 Avalanche 中，希望参与的节点向验证程序链发出特殊的股份交易。下注交易指定要下注的金额、下注参与者的下注密钥、持续时间以及开始验证的时间。一旦交易被接受，资金将被锁定，直到下注期结束。最低允许金额由系统决定并执行。如下文所述，参与者投入的股份数量对参与者在共识过程中的影响力以及回报都有影响。指定的锁定持续时间必须介于 δmin 和 δmax 之间，这是任何桩可以锁定的最小和最大时间范围。与赌注金额一样，赌注期限也会影响系统中的奖励。锁紧钥匙的丢失或被盗不会导致资产损失，因为锁紧钥匙仅在协商一致过程中使用，不用于资产转让。

3.4 美元 AVAX 智能合约

在发布时，Avalanche 通过以太坊虚拟机（EVM）支持标准的基于实体的智能合约。我们预计，该平台将支持一套更丰富、更强大的智能合约工具，包括：

- 具有链外执行和链内验证的智能合约。
- 具有并行执行功能的智能合约。在雪崩的任何子网中，任何不在同一状态下运行的智能合约都将能够并行执行。
- 一种改进的坚固性，称为坚固++。这种新语言将支持版本控制、安全数学和定点算法、改进的类型系统、编译到 LLVM 以及实时执行。

如果开发人员需要 EVM 支持，但希望在专用子网中部署智能合约，他们可以直接启动一个新子网。这就是 Avalanche 如何通过子网实现特定于功能的分片。此外，如果开发人员需要与当前部署的以太坊智能合约进行交互，他们可以与以太坊的子网进行交互。最后，如果开发人员需要与以太坊虚拟机不同的执行环境，他们可以选择部署

他们通过实现不同执行环境（如 DAML 或 WASM）的子网进行智能合约。子网可以支持 VM 行为之外的其他功能。例如，子网可以对持有智能合约时间较长的较大验证程序节点，或私下持有合约状态的验证程序，强制执行性能要求。

4 治理和$AVAX 代币

4.1 美元 AVAX 本机代币

货币政策本机代币$AVAX 为上限供应，上限设置为 720000000 代币，在 mainnet launch 上提供 360000000 代币。然而，与其他封顶供应代币不同的是，AVAX 的设计旨在对不断变化的经济状况做出反应，而其他封顶供应代币则会永久性地影响造币率。特别是，AVAX 美元货币政策的目标是平衡用户持有代币的动机
而不是使用它与平台上提供的各种服务进行交互。该平台的参与者集体充当一个分散的储备银行。关于雪崩的可用杠杆是赌注奖励、费用和空投，所有这些都受到可控参数的影响。赌注奖励由链上治理设定，并由一个永远不会超过供应上限的功能控制。赌注可以通过增加费用或增加赌注奖励来诱导。另一方面，我们可以通过降低费用和降低赌注奖励来提高 295 对雪崩平台服务的参与度。

使用

*付款*真正的分散式点对点支付在很大程度上是一个未实现的行业梦想，因为目前缺乏现有企业的业绩$AVAX 与 Visa 支付一样强大且易于使用，以完全不可信、分散的方式，每秒允许全球数千笔交易。
此外，对于世界各地的商家来说，AVAX 美元比 Visa 提供了一个直接的价值主张，即更低的费用。

*锁定：确保系统安全*在雪崩平台上，sybil 控制通过锁定实现。为了验证，参与者必须锁定硬币或赌注。验证者，有时被称为赌注者，根据赌注金额和赌注持续时间等对其验证服务进行补偿
财产。所选择的补偿函数应使差异最小化，确保大型桩不会不成比例地获得更多补偿。参与者也不受任何“运气”因素的影响，如战俘采矿。这种奖励计划也不鼓励形成采矿或赌注池，从而实现真正分散、不可信任的网络参与。

*原子交换*除了提供系统的核心安全外，$AVAX 代币还充当通用单元
交换。从那时起，Avalanche 平台将能够在平台上本地支持不可信任的原子交换，从而直接在 Avalanche 上实现任何类型资产的本地、真正分散的交换。

4.2 治理

治理对于任何平台的开发和采用都至关重要，因为与所有其他类型的系统一样，雪崩也将面临自然演变和更新$AVAX 提供链上治理
对于网络的关键参数，参与者可以对网络的更改进行投票，并以民主方式解决网络升级决策。这包括最低赌注金额、铸造率以及其他经济参数等因素。这使得平台能够通过群组 oracle 有效地执行动态参数优化。然而，与其他一些治理平台不同，Avalanche 不允许对系统的任意方面进行无限的更改。相反，只有一个

可以通过治理修改预先确定的参数数量，使系统更可预测，并提高安全性。此外，所有可控制参数都受到特定时间范围内的限制，引入滞后，并确保系统在短时间范围内保持可预测性。

寻找全球可接受的系统参数值的可行过程对于没有保管人的分散系统至关重要。雪崩可以利用其共识机制建立一个允许

任何人都可以提出实质上是全系统投票的特殊交易。任何参与节点均可发布此类提案。

名义报酬率是影响任何货币的一个重要参数，无论是数字货币还是法定货币。不幸的是，修复这个参数的加密货币可能会面临各种问题，包括通货紧缩或通货膨胀。

为此，名义报酬率受预先设定的边界内的治理约束。这将允许代币持有者选择 AVAX 美元最终是否有上限、无上限，甚至是通货紧缩。

交易费用（以集合 F 表示）也受治理约束。F 实际上是一个元组，它描述了与各种指令和事务相关的费用。最后，赌注的时间和金额也是可以控制的。这些参数的列表如图 1 所示。

–：赌注金额，以美元为单位。该值定义了在参与系统之前作为债券所需的最小赌注。Δ
–：节点进入系统所需的最短时间。δmin
–：节点可以占用的最大时间。δmax
–：(πΔ,τδmin）→R：奖励率函数，也称为造币率，确定参与者在 τ 连续 δmintimeframes 的一段时间内，根据其所有权下的一些 π 公开披露节点的数量，作为赌注金额的函数，可以获得的奖励，例如 τδmin≤ δmax。ρ
–F：费用结构，这是一组可管理的费用参数，用于指定各种交易的成本。

图 1。雪崩中使用的关键非共识参数。第一次使用时，所有符号都被重新定义。

根据金融系统的可预测性原则，$AVAX 的治理具有滞后性，这意味着参数的变化高度依赖于其最近的变化。每个可控制参数都有两个限制：时间和范围。一旦使用治理事务更改了参数，就很难立即对其进行大量更改。自上次更改以来，随着时间的推移，这些困难和价值约束会逐渐放松。总的来说，这可以防止系统在短时间内发生剧烈变化，允许用户在短期内安全地预测系统参数，同时在长期内具有强大的控制能力和灵活性。

5 讨论

5.1 优化

修剪许多区块链平台，尤其是那些实现中本共识（如比特币）的平台，遭受着持续的状态增长。这是因为——根据协议——它们必须存储 345 笔交易的全部历史记录。然而，为了使区块链可持续增长，它必须能够删减旧的历史。这对于支持高性能的区块链尤其重要，比如雪崩。

在斯诺家，修剪很简单。与比特币（和类似协议）不同，在比特币（和类似协议）中，根据算法要求不可能进行修剪，而在$AVAX 中，节点不需要维护 DAG 中深度和高度承诺的部分。这些节点不需要向新的引导程序证明任何过去的历史

350 节点，因此只需存储活动状态，即当前余额，以及未提交的事务。

客户端类型 Avalanche 可以支持三种不同类型的客户端：归档、完整和轻型。存档节点存储$AVAX 子网、锁定子网和智能合约子网的整个历史，一直到 genesis，这意味着这些节点充当新传入节点的引导节点。另外

355 这些节点可以存储它们选择作为验证器的其他子网的完整历史记录。存档节点通常是具有高存储能力的机器，在下载旧状态时由其他节点支付。另一方面，完整节点参与验证，但它们不存储所有历史记录，只存储活动状态（例如当前 UTXO 集）。最后，对于那些只需要使用最少量资源与网络进行安全交互的用户，Avalanche 支持可以

360 证明某些事务已提交，无需下载或同步历史记录。轻型客户端参与协议的重复采样阶段，以确保安全承诺和网络范围的共识。因此，Avalanche 中的轻型客户端提供与完整节点相同的安全保证。

切分切分是对各种系统资源进行分区以提高性能和降低负载的过程。有各种类型的切分机制。在网络分片中，参与者的集合

365 分为独立的子网，以减少算法负载；在状态切分中，参与者同意只存储和维护整个全球状态的特定子部分；最后，在事务切分中，参与者同意将传入事务的处理分开。

在北冰洋雪崩中，第一种形式的分片通过子网络功能存在。例如，可以启动一个黄金子网和另一个房地产子网。这两个子网可以完全存在于网络中

370 平行的只有当用户希望使用其持有的黄金购买房地产合同时，子网才会进行交互，此时 Avalanche 将启用两个子网之间的原子交换。

5.2 关注事项

后量子密码术由于量子计算机和算法的发展，后量子密码学最近得到了广泛关注。对量子的关注

计算机可以破坏当前部署的一些加密协议，特别是数字签名。雪崩网络模型支持任意数量的虚拟机，因此它支持具有合适的数字签名机制的抗量子虚拟机。我们预计将部署几种类型的数字签名方案，包括基于量子抵抗 RLWE 的签名。共识机制的核心操作不采用任何重加密。考虑到这种设计，可以直接使用提供量子安全密码原语的新虚拟机来扩展系统。

现实的对手雪崩论文[6]为强大且敌对的对手提供了非常有力的保证，在全点对点模型中称为圆形自适应对手。换句话说，对手可以随时完全访问每个正确节点的状态，知道所有正确节点的随机选择，并且可以在攻击前后随时更新自己的状态

正确的节点有机会更新自己的状态。实际上，这个对手是全能的，除了能够直接更新正确节点的状态或修改正确节点之间的通信。尽管如此，在现实中，这样的对手纯粹是理论上的，因为最强对手的实际实现仅限于网络状态的统计近似值。因此，在实践中，我们预计最坏情况下的攻击很难部署。

包容与平等无许可货币的一个常见问题是“富人越来越富”。这是一个合理的担忧，因为如果 PoS 系统实施不当，实际上可能会让财富的产生不成比例地归因于该系统中已经拥有大量股权的人。一个简单的例子是基于领导者的共识协议，其中一个小组委员会或指定的领导者在其运作期间收集所有奖励，并且被选择收集奖励的概率是有限的

与股份成比例，产生强烈的回报复合效应。此外，在比特币等系统中，存在一种“大变大”的现象，即大矿工比小矿工享有更高的福利，孤儿更少，失去的工作更少。相比之下，雪崩采用了一种平等的造币分配方式：每一位参与下注协议的人都会根据赌注获得公平和成比例的奖励。

通过让大量的人直接参与下注，雪崩可以容纳

数以百万计的人平等地参与赌博。参与协议所需的最低金额将由治理决定，但它将被初始化为一个较低的值，以鼓励广泛参与。

这也意味着代表团不需要参与少量分配。

6 结论

本文讨论了雪崩平台的体系结构。与今天的其他平台相比，

它要么运行经典风格的协商一致协议，因此本质上是不可扩展的，要么利用中本风格的协商一致协议，效率低，运营成本高。雪崩协议具有轻量级、快速、可扩展、安全和高效的特点。用于保护网络安全和支付各种基础设施成本的本机令牌简单且向后兼容$AVAX 拥有超越其他提案的能力，能够实现更高级别的分权，抵御攻击，并在没有任何法定人数 410 或委员会选举的情况下扩展到数百万个节点，因此不会对参与施加任何限制。

除了共识引擎，Avalanche 还进行了一系列创新，在事务管理、治理和一系列其他平台无法提供的其他组件方面引入了简单但重要的思想。协议中的每个参与者都有发言权，可以随时影响协议的发展，这是由强大的治理机制实现的。Avalanche 支持高度可定制性，允许 415 个几乎即时即插即用的现有区块链。

工具书类

1. 比特币：比特币/比特币（2018 年 10 月），https://github.com/bitcoin/bitcoin
2. Buttolph，S.、Moin，A.、Sekniqi，K.、Sirer，例如：Avalanche token paper-token dynamics（2019），https://files.avalabs.org/papers/token.pdf

420 3.杜瑟，J.R.：锡比尔袭击。主题：点对点系统国际研讨会。第 251-260 页。斯普林格（2002）

4. Eyal，I.，Gencer，A.E.，Sirer，例如 van Renesse，R.：比特币 ng：一种可扩展的区块链协议。参加：第 13 届 USENIX 网络系统设计与实施研讨会，NSDI 2016，加利福尼亚州圣克拉拉，美国，3 月 16 日至 18 日，2016 年，第 45-59 页（2016 年），https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal
5. 中本：比特币：一种点对点电子现金系统（2008）

425 6.T.Rocket.：雪花到雪崩：一种新的用于加密货币的亚稳态共识协议家族。知识产权 (2018), https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRVGV

14 凯文·塞克尼奇、丹尼尔·莱恩、斯蒂芬·巴托夫和埃敏·古恩·塞勒 7。Wood，G.：以太

坊：一个安全的分散式通用交易分类账（2014）

[11]前瞻性陈述通常与未来事件或我们未来的表现有关。这包括但不限于雪崩的预期性能；其业务和项目的预期发展；执行其愿景和增长战略；以及完成目前正在进行、正在开发或正在考虑的项目。前瞻性陈述仅代表我们管理层截至本报告日期的信念和假设。这些声明不是未来业绩的保证，不应过度依赖这些声明。此类前瞻性陈述必然涉及已知和未知的风险，这可能导致未来期间的实际表现和结果与本文中明示或暗示的任何预测存在重大差异。雪崩不承担更新前瞻性声明的义务。尽管前瞻性陈述是我们做出预测时的最佳预测，但由于实际结果和未来事件可能存在重大差异，因此无法保证这些陈述将被证明是准确的。提醒读者不要过度依赖前瞻性陈述。