百科 | 七个不可不知的加密术语

作者：Robert D. Knight，Cointelegraph；编译：白水，本站

掌握加密货币并不容易。即使你已经了解了比特币和以太坊以及工作量证明和权益证明之间的区别，仍然需要学习和理解一大堆新术语。

但即使是对相当资深的加密货币爱好者来说，仍然有一些术语难以理解。以下是区块链领域几乎没有人能够完全或深入理解的七个术语。

## Blobs

在 1958 年由史蒂夫·麦奎因主演的电影和 1988 年的翻拍版中，Blob 是一个类似变形虫的果冻怪物，它恐吓小镇的居民，在吞噬他们时变得越来越大、越来越红。

在加密货币中，尤其是以太坊中，blob（二进制大对象）是以太坊电子虚拟机 (EVM) 不需要的大量数据块。Blob 数据在链上保存约 20-90 天，然后被删除。



资料来源：John Irving

结果是更具成本效益和可扩展性的区块链。作为以太坊 Dencum 更新的一部分，blob 经常与此列表中的下一个术语同时讨论。

blob 也可能指存储在去中心化存储系统（如 IPFS 或 Filecoin）上的数据块。这些 blob 经过加密并存储在多个节点上。

最后，blob 还可以指 Monero 上的交易 blob，即交易在广播到网络之前的二进制数据。由于 Monero 是一条隐私链，因此这些 blob 的结构可以保持匿名。

而这就是大量的 blob。

## Rollups

Rollup 是一种在 Layer 2 协议上处理交易的方式，可以释放基础层的宝贵空间。Rollup 会在第二层上逐笔折叠交易，有时会折叠数十次，然后将它们滚动在一起，再将数据发送回 Layer 1。

Rollup 主要有两种类型，optimistic和零知识 (ZK) 证明。

OptimisticRollup 是一个相当明确的术语。这意味着 Rollup 采用“optimistic”方法运行，假设交易有效，除非验证者证明其错误。只有在存在争议时，他们才会检查交易的有效性。

ZK Rollup 会在不透露任何交易数据的情况下证明交易。因此，称为“零知识”。

ZK Rollup 提供即时终结性，因为加密证明保证数据有效。

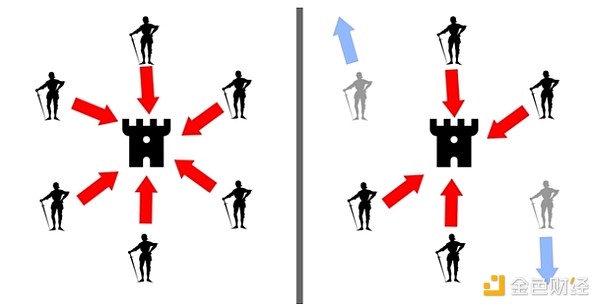
在许多方面，Rollup 之于您的标准区块链交易就像 Calzone 之于普通披萨片。通过滚动，您可以放入更多东西。

## 拜占庭容错

这是区块链的经典术语之一，也是该技术的一个关键特征，但对于大多数人来说，他们根本不会花时间去思考它。

拜占庭将军问题是一项理论练习，描述了在没有可信的集中实体的情况下，分散各方达成共识的难度。也就是说，它努力解决坏人制造虚假信息在特定情况下产生不良结果的可能性。

具体来说，没有直接沟通的将军必须同时攻击拜占庭才能取得胜利。如果其中一名将军撤退，或者发出攻击信号但随后撤退，战斗将以溃败告终；比所有将军协调撤退更糟糕。



在左边，如果所有将军同时进攻，他们将获胜。在右边，如果两名将军错误地发出进攻信号，然后撤退，其他人就会被击溃。来源：Lord Belbury

中本聪通过使用工作量证明共识机制解决了比特币的拜占庭将军问题。创建区块需要花费大量的时间和精力，因此他们有动力提供准确的信息。

拜占庭故障是去中心化计算系统中的错误，它会向不同的参与者显示不同的错误或结果，就像拜占庭将军问题一样。

因此，拜占庭容错是该计算系统对产生此类故障的弹性。

我们希望这不是一个太过拜占庭式的解释。

## 原始 Danks 分片

分片是一种将账本分割成更小的部分（称为分片）的方法。

但 proto-danksharding 是加密世界词汇中最不透明的术语之一。这个术语并没有特别的指导意义。proto 是原型的缩写吗？这是你最喜欢的 meme 文件夹中的同一个 dank 吗？这两个假设可能都相当合理，但都是错误的。

protolambda 和 Dankrad Feist 首次提出了这一想法，他们以自己的名字命名了这一想法，proto-danksharding 是一种接受上述 blob 的交易类型。使用 blob 的解决方案旨在克服以太坊长期以来的高 gas 费用和低交易吞吐量问题。

第 2 层汇总使用 blob 来捆绑交易并将其提交给以太坊基础层，而不会使其不堪重负。

但如果 proto-danksharding 看起来像一个令人困惑和神秘的措辞，您可以选择使用更具指导意义的名称来表示该过程； EIP-4844。

再想想，proto-danksharding 这个术语并没有那么糟糕。

## DVT——分布式验证器技术

大多数加密货币领域人士都已经熟悉在权益证明共识模型中批准交易的验证器。

DVT 采用了这一概念，并将流程分散到多个验证器中。正如 Lido 所描述的，DVT“作为一个系统，其运行方式类似于运行验证器的多重签名 (multisig) 设置。”

他们称之为“简单的 DVT”，但它的简单性仍然是个谜。

最终，DVT 利用多个操作员而不是依赖单个操作员，从而增强了弹性并减轻了单点故障。

## 动态重新分片

动态重新分片并不是你祖母时代的旧分片。动态重新分片是一个相对较新的术语，Near Protocol 的营销团队将其称为“分片的圣杯”，但它也创造了一个无法立即理解的新词汇。

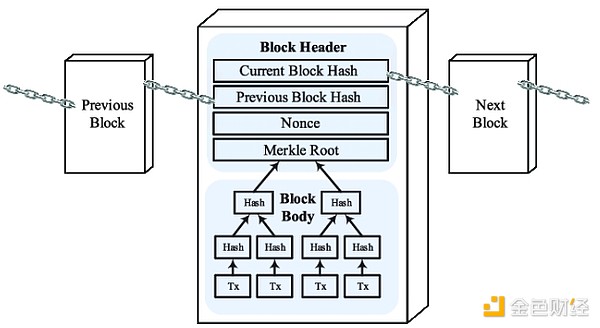
基于区块链分片的概念，当网络根据负载调整分片数量时，就会发生重新分片。

超载的分片可以变成两个分片，而两个未充分利用的分片可以变成一个。

## Nonce

Nonce 是大多数人在早期发现加密货币时会遇到然后就完全忘记的术语之一，就像你在聚会上刚遇到的一大群人的个人名字一样。

在比特币区块链中，随机数是区块头中使用的数字，然后对其进行加密哈希处理。这是通过反复试验猜测的数字，用于决定哪个矿工生成下一个区块链。



包含随机数的比特币区块的数据结构。资料来源：Research Gate

随机数生成使挖矿过程更加公平透明。这需要大量的计算能力和能源，在某些情况下，矿工可能需要多次调整随机数才能解决一个区块。