MULTICOIN CAPITAL

Delegated Proof of Stake: Features & Tradeoffs

委托权益证明：特点和权衡

文 Myles Snider, Tushar Jain, & Kyle Samani

译 June Chan

Multicoin Capital is a thesis-driven cryptofund that invests in tokens reshaping entire sectors of the global economy. We rigorously research blockchain protocols, teams, and market opportunities to deliver venture capital economics with public market liquidity.

Multicoin Capital是一个论文驱动的加密基金，投资代币重塑全球经济的整个部门。我们以极其审慎的态度研究区块链协议、团队和市场机会，以提供具有公共市场流动性的风险投资经济学。

Report Disclosures

报告披露

***Disclosures**: As of the publication date of this report, Multicoin Capital Management LLC and its affiliates (collectively "Multicoin"), others that contributed research to this report and others that we have shared our research with (collectively, the "Investors") may have long or short positions in and may own options on the token of the project covered herein and stand to realize gains in the event that the price of the token increases or decreases. Following publication of the report, the Investors may transact in the tokens of the project covered herein. All content in this report represent the opinions of Multicoin. Multicoin has obtained all information herein from sources they believe to be accurate and reliable. However, such information is presented "as is," without warranty of any kind – whether express or implied.*

***披露**：截至本报告出版之日，Multicoin资本管理有限公司及其附属公司（统称"Multicoin"）、对本报告做出贡献的其他人以及我们与之分享研究成果的其余人士（统称为"投资者"）可能持有本报告所涉及项目的多头或空头头寸，或拥有相关代币期权，在代币价格上涨或下跌的情况下实现收益。本报告发布后，投资者可就本报告所述项目的代币进行交易。本报告所有内容均代表Multicoin的意见。Multicoin获取的所有信息均来自其认为准确可靠的来源。但是，此类信息"按原样"呈现，不作任何形式的保证，无论是明示还是暗示。*

This document is for informational purposes only and is not intended as an official confirmation of any transaction. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, and reflect prevailing conditions and Multicoin's views as of this date, all of which are accordingly subject to change without notice. Multicoin has no obligation to continue offering reports regarding the project. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances.

本文件仅供参考之用，不作为任何交易的正式确认。所有市场价格、数据和其他信息均不保证其完整性或准确性，它们都基于选定的公开市场数据，并反映截至发表之日的普遍情况和Multicoin的观点，上述所有信息都可能发生变化，恕不另行通知。Multicoin没有义务继续提供有关该项目的报告。报告是按所标明的日期编制的，可能因随后的市场或经济情况而不再精准可靠。

Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. This report's estimated fundamental value only represents a best efforts estimate of the potential fundamental valuation of a specific token, and is not expressed as, or implied as,

assessments of the quality of a token, a summary of past performance, or an actionable investment strategy for an investor.

任何投资都存在相当的风险，包括但不限于价格波动、流动性不足和潜在的本金完全损失。本报告的基本价值估计值仅代表对特定代币潜在基本价值的最佳努力估计值，并不明示或暗示为对代币质量的评估、对过往业绩的总结或对投资者提供的可操作投资策略。

This document does not in any way constitute an offer or solicitation of an offer to buy or sell any investment or token discussed herein.

本文件不以任何方式构成买卖本文件所述任何投资或代币的要约或邀请。

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond Multicoin's control. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on all tokens discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.

本文件所含信息可包括或引用前瞻性陈述，其中包括任何非历史事实陈述。这些前瞻性陈述可能被证明是错误的，可能受到不准确的假设、已知或未知风险、不确定性和其他因素的影响，其中大多数超出了Multicoin的可控范围。投资者应在专业财务、法律和税务专家的协助下，对本文件中讨论的所有代币进行独立的尽职调查，并在作出任何投资决策前对相关市场做出独立判断。

Note: Most of this analysis refers to DPoS as implemented in BitShares, Steem, and EOS. Other platforms use a similar DPoS framework but alter certain features. Much of this analysis will focus specifically on EOS's consensus algorithm. We will publish a full analysis and valuation of EOS in the future.

注意：本分析主要指在Bitshare、Steem和EOS中实现的DPoS。其他平台使用类似的DPoS框架，但会更改某些特性。本分析主要将特别关注EOS的共识算法。我们将在未来发布对EOS的完整分析和评估。

Introduction

介绍

Distributed ledgers don't easily scale. That fact has become readily apparent in the last few years as Bitcoin, Ethereum, and others have faced serious challenges as they attempt to increase the speed and throughput of their platforms.

分布式账本不容易扩展。这一事实在过去几年显得尤为明显，因为比特币、以太坊和其他公司在试图提高平台的速度和吞吐量时，都面临着严峻的挑战。

This problem can be best understood as a scalability trilemma (this idea was first formalized by Vitalik Buterin and Trent McConaghy). The scalability trilemma posits that any blockchain system in which every node validates every transaction can have only two of three potential properties: decentralization of block production (DBP), safety, and scalability. These properties can be defined as follows:

想要理解这个问题，最好的办法是将它视为一个可伸缩性三难困境（Vitalik Buterin和Trent McConaghy率先就这个想法撰文）。可伸缩性三难困境假设任何区块链系统（其中每个节点都验证每个事务）只能具有区块生产(DBP)去中心化、安全性和可伸缩性这三个潜在特性当中的两个。这些属性可以定义为：

- DBP can be quantified as the number of block producers.
- Safety can be quantified as the cost of mounting a Byzantine attack that affects liveness or transaction ordering. Note that safety does not refer to the integrity of cryptographic signatures, or the ability of a 3rd party to derive a set of private keys from public keys.
- Scalability can be quantified as the number of transactions per unit of time that the system can process.
- DBP可以用区块生产者的数量量化。
- 安全性可以用发起拜占庭式攻击的成本量化，这种攻击会影响活动或事务排序。注意，安全性不涉及加密签名的完整性，也不涉及第三方从公钥派生一组私钥的能力。
- 可伸缩性可以用系统每单位时间内处理的事务数量量化。

While projects like Ethereum, Dfinity, Polkadot, and Kadena are attempting to solve the scalability trilemma via sharding, alternative consensus schemes, and other techniques, we don't yet have a live platform that has solved this trilemma. Even if one of these projects does manage to solve the scalability trilemma, the market may not care. It is entirely possible that users are willing to accept tradeoffs in decentralization of block production or safety in the name of better performance and easier user experience for certain use cases.

虽然像以太坊、Dfinity、Polkadot和Kadena这样的项目正试图通过分片、替代共识方案和其他技术来解决可伸缩性三难问题，但是我们还没有一个已在解决该问题的实时平台。而且即使当中有项目能够解决可伸缩性的三难困境，市场可能也不会在意。用户为了某些用例获得更好的性能、在体验上更简单易用，而接受在区块生产去中心化或安全方面的妥协，这是完全有可能的。

Decentralization is valuable to ensure that any given party cannot alter the database. More decentralization means it is harder to collude to alter the database. There are different levels of protection which are necessary for different use cases. Bitcoin, being censorship-resistant money, is designed for sovereign-grade protection; it is designed to withstand an attack by a large nation-state. However this isn't necessary for most decentralized applications (dApps). These dApps need platform-grade protection; global, neutral databases uncontrolled by any one party.

去中心化对于确保任何一方都不能修改数据库是很有价值的。去中心化程度越高，就越难以串谋修改数据库。不同的用例需要不同级别的保护。比特币作为一种抗审查性货币，旨在提供主权级的保护；它在设计之初就考虑到如何抵御一个大型民族国家的攻击。然而，对于大多数去中心化应用程序(dApps)来说，这并不是必需的。这些应用程序需要的是平台级保护；不受任何一方控制的全球中立数据库。

Delegated Proof of Stake (DPoS) concentrates block production in the hands of just a few, known, semi-trusted entities in order to achieve orders of magnitude more scalability than proof-of-work (PoW) or other proof-of-stake (PoS) blockchains. In this analysis, we'll examine the features and tradeoffs of DPoS.

委托权益证明(DPoS)将区块生产集中在少数已知的半可信实体手中，以便实现比工作证明(PoW)或其他权益证明(PoS)区块链更大的可伸缩性。在此分析中，我们将研究DPoS的特性和权衡。

Delegated Proof of Stake

委托权益证明

Delegated proof of stake (DPoS) is a consensus algorithm invented by Dan Larimer in 2013. DPoS was originally invented to power BitShares, Larimer's first blockchain project. He refined it in his second project, Steem, and is refining it further in EOS, which he's been working on for about one year. While Larimer invented DPoS and continues to evolve the algorithm, several other projects have adopted DPoS and made changes. Current blockchains utilizing DPoS include:

委托权益证明是Dan Larimer在2013年发明的一种共识算法。DPoS最初是为了驱动BitShares而发明的，这是Larimer的第一个区块链项目。他在第二个项目Steem中对其进行了改进，现在则在已经深耕了一年半的EOS中再做进一步改进。当Larimer发明了DPoS并继续改善其算法时，其他几个项目也采用了DPoS并进行了修改。目前使用DPoS的区块链包括：

- EOS, BitShares, Steem, Golos, Ark, Lisk, PeerPlays, Nano (formerly Raiblocks), and Tezos

- Cosmos/Tendermint, Cardano, and a few others use consensus algorithms loosely based on DPoS

- EOS、BitShares、Steem、Golos、Ark、Lisk、PeerPlays、Nano（其前身是Raiblocks）和Tezos

- Cosmos/Tendermint、Cardano和其他一些松散地使用基于DPoS的协商一致算法的公司

In DPoS, those who hold the network token are able to cast votes to elect block producers; votes are weighted by the voter's stake, and the block producer candidates that receive the most votes are those who produce blocks. Users can also delegate ("proxy") their voting power to another user who can vote on their behalf. **DPoS is a liquid, representative democracy with token holder suffrage.** DPoS can also be thought of as a formalized, digital version of a traditional organizational hierarchy that operates in a completely transparent way. While there are problems with both democracy and corporate governance that are beyond the scope of this paper, one compelling features of DPoS is that the open-source nature of these protocols means that users can fork if they disagree with the majority. The same cannot be said of democracies, corporations, and other organizational structures. DPoS adopts ideas from many traditional governance models, but is ultimately far more flexible and transparent.

在DPoS中，持有网络代币的用户可以投票选举区块生产者；选票是由选民 所持的保证金来加权的，获得最多选票的区块生产者候选人负责出块。用户还可以将本人的投票权委托给能够代表自己投票的其他用户。**DPoS是一种流动式的代议制民主，代币持有者拥有投票权。**DPoS也可以看作是传统组织层次结构的形式化、数字化版本，以完全透明的方式运行。虽然民主和公司治理存在的问题超出了本文讨论的范围，但DPoS的一个引人注目的特性是，这些协议的开源性质意味着，如果用户不同意多数派的意见，他们可以进行分叉。民主国家、公司和其他组织结构就不是这样了。DPoS借鉴了许多传统治理模型的思想，但最终更加灵活和透明。

Block producers can be voted in or out at any time, so the threat of loss of income and reputation is one of the major incentives against bad behavior. Additionally, slashing conditions can be implemented in DPoS rather trivially. Most traditional PoS implementations allow users to produce blocks proportional to their stake in the network. DPoS allows users to cast votes proportional to their stake to decide who produces blocks. Block producers themselves do not necessarily need to have a large stake, but they must compete to receive votes from users.

区块生产者可以在任何时候当选或被投票出局，因此防范不良行为的主要动机之一是来自收入和声誉受损方面的威胁。此外，在DPoS中可以相当简单地实现削减条件。大多数传统的PoS实现允许用户生成与他们在网络中的权益成比例的区块。DPoS允许用户根据自己的权益比例投票，决定谁来生产区块。区块生产者本身并不一定需要拥有大量保证金，但他们必须通过竞争来获得用户的投票。

DPoS can power entire blockchains, or it can be used as a consensus algorithm for child chains, sidechains, private blockchains, and more. DPoS could be used to power consensus within Ethereum Plasma chains, and DPoS bears many similarities to the "Proof of Authority" consensus mechanism formalized by Parity. It could also be a solution for application-specific chains like those in Cosmos zones.

DPoS可以驱动整个区块链，也可以用作子链、侧链、私有区块链等的共识算法。DPoS可以用来在以太坊Plasma链内部为共识提供动力，它与由Parity提出成型的"权威证明"共识机制有许多相似之处。它也可以作为面向特定应用程序特定链的解决方案，比如Cosmos中的链。

For other in-depth documentation on DPoS, see this link and this link from BitShares, and this white paper from Larimer.

有关DPoS的其他深度文章，请参见Bitshares中的这个链接和这个链接，以及Larimer的白皮书。

DPoS Features and Tradeoffs

DPoS特性和权衡

The core elements of DPoS are the following:

DPoS的核心要素如下：

BLOCK PRODUCERS

区块生产者

Like other PoS chains, DPoS doesn't include miners who run hashes to produce blocks. Instead, an elected subset of users is chosen to perform the work of validating the chain. We'll simply refer to these users are block producers, though they are sometimes called delegates, notaries, validators, forgers, or witnesses.

与其他PoS区块链一样，DPoS不包括使用哈希生成块的矿工。相反，它会选择一个用户子集来执行验证链的工作。我们将简单地将这些用户称为区块生产者，尽管他们有时还会被称为委托人、公证人、验证者、铸币者或证人。

Because the token holders decide on a elected subset of users to produce blocks, mechanisms to allow a wider group of computers to participate in block production (which ultimately slow down block production) can be removed. DPoS can be seen as a form of "controlled semi-centralization" that gets the benefits of semi-centralization (efficiency and speed) while still maintaining some calculated measure of decentralization (X # of independent block producers that can be voted in and out by token holders).

由于代币持有者决定由一个选定的用户子集来生成区块，因此可以删除允许更广泛的计算机组参与区块生产的机制（这最终会降低区块生成的速度）。DPoS可以被看作是"受控半中心化"的一种形式，它获得了半中心化的好处（即效率和速度），同时仍然保持一些经过计算的去中心化度量（X # 可以由代币持有者投票决定是否加入的独立区块生产者）。

The multi-billion-dollar question then becomes "How many block producers are necessary in order to be sufficiently decentralized?" This is a loaded question and one that divides the crypto community. It's also the single feature that is often presented as a game-ending criticism of DPoS: DPoS is not decentralized enough.

这个价值数十亿美元的问题因此变成了"为了充分去中心化，需要多少区块生产者？"。这是一个意味深长的问题，而且在加密界存在分歧。这个特性也经常作为对DPoS盖棺论定的批评：DPoS不够去中心化。

Importantly, decentralization is a spectrum, and increased decentralization often also incurs higher costs. There are many different measures of decentralization. Some like Balaji Srinivasan have attempted to quantify decentralization, but even he admits that his proposals need more work. He breaks down networks into subsystems, each of which can be measured differently and each of which contributes to an overall notion of system-wide decentralization. Some people may have opposing views about which subsystems to include and how much weight to assign to each. Ultimately, measures of decentralization can produce different results when different variables are examined, and they don't produce a binary result. Systems are not decentralized or not; rather, some are more decentralized than others, though this measure can be somewhat subjective.

重要的是，去中心化是一个范围，去中心化越多，成本也就越高。去中心化有许多不同的措施。Balaji Srinivasan等人曾试图量化去中心化，但就连他自己也承认，他的提议尚需要做更多工作。他将网络分解为子系统，每个子系统都可以用不同的方法度量，并且每个子系统都有助

于系统范围内去中心化的总体概念。对于应该包含哪些子系统以及应该给每个子系统分配多少权重，有些人可能持有相左的观点。最终，当检查不同的变量时，去中心化的度量可以产生不同的结果，并且它们不会产生一个二元的结果。系统并非只可能是中心化或去中心化的；事实上只能说，有些系统比其他的更加去中心化，尽管这个指标可能有些主观。

The goal is not decentralization for its own sake. **Decentralization is a feature of systems that allows them to achieve other goals: censorship resistance, open participation, immunity from certain attacks, and elimination of single points of failure.** While some features that contribute to decentralization can be quantified, the phenomenon as a whole cannot be. The number of block producers is just one metric, but it fails to capture all of the relevant subtleties. It also doesn't describe how much decentralization is necessary to accomplish the underlying goals, or how to think about theoretical vs practical decentralization.

其目标不是为了去中心化本身。**去中心化是系统的一个特性，它允许它们实现其他目标：抵制审查、公开参与、免受某些攻击、消除单点故障。**虽然有助于去中心化的一些特性可以量化，但整个现象却无法量化。区块生成者的数量只是一个度量标准，但它不能捕捉所有相关的细微差别。它没有描述完成基本目标需要多大程度的去中心化，也没有描述如何考虑理论与实践上的去中心化之分。

DPoS doesn't attempt to "find" a balance between the number of block producers needed to ensure that control is sufficiently decentralized and the number of block producers that can easily be monitored for bad behavior. Rather, it explicitly sets the balance, though it can be modified later.

DPoS不会试图在确保充分去中心化所需的区块生产者数量和易于监控不良行为的区块生产者数量之间"寻找"平衡。相反，它显式地设置了平衡，尽管稍后可以修改它。

There does not seem to be a single number that encapsulates this. In our view, 20 block producers all located in China is less decentralized than 10 block producers spread across various jurisdictions around the globe. Cornell's IC3 team recently wrote a paper that attempted to quantify decentralization in Bitcoin and Ethereum. They ultimately found that block production in Bitcoin and Ethereum was far more concentrated than commonly thought. They noted:

似乎没有一个数字可以概括这一点。在我们看来，与分布在全球不同司法管辖区的10家区块生产者相比，全部位于中国的20家区块生产者的去中心化程度较低。康奈尔大学的IC3团队最近写了一篇论文，试图量化比特币和以太坊的去中心化。他们最终发现，比特币和以太坊的区块生产比人们通常认为的要集中得多。他们指出：

> "These results show that a Byzantine quorum system of size 20 could achieve better decentralization than proof-of-work mining at a much lower resource cost. This shows that

> further research is necessary to create a permissionless consensus protocol without such a high degree of centralization."
>
> "这些结果表明，规模为20的拜占庭法定人数制度能够以低得多的资源成本实现比工作证明采矿更好的去中心化。这表明，在没有如此高度集中的情况下，有必要进行进一步的研究以建立一个无许可的共识协议。"

DPoS is one potential solution to this problem; we look forward to more research on this front. The benefits of decentralization can't be accurately measured by a single number—they are emergent properties that must be observed in an iterative, dynamic, unpredictable, real-world environment. **Token voters in DPoS systems will have to take into account not just how many block producers there are, but also in which jurisdiction they are located, with whom they are affiliated, and more. If voters do enough due diligence to ensure that 21 individual entities located in different jurisdictions are producing blocks, then validation in DPoS has the potential to be far more decentralized than almost any other blockchain.**

DPoS是解决这一问题的一个潜在方案；我们期待着在这方面出现更多的研究。去中心化的好处不能用一个数字精确地衡量——它们是必须在一个迭代的、动态的、不可预测的、真实世界的环境中观察到的突现特性。**DPoS系统中的代币投票人不仅要考虑有多少区块生产者，还要考虑它们位于哪个司法管辖区、与谁有关联，等等。如果选民做了足够的尽职调查，以确保位于不同司法管辖区的21个单独实体正在生产区块，那么DPoS验证去中心化的程度可能远甚于几乎所有其他区块链。**

For an argument of why DPoS is more decentralized in practice than PoW, see this excellent post from Ian Grigg. In it, he describes how the Chinese government could launch an attack on Bitcoin miners within the country, either by directly taking them over, forcing them to shut down, or exploiting the great fire wall that controls the in/out pipes of the internet in China. This would be hugely disruptive for the Bitcoin network, and would render it severely compromised for a period of time, even if it were eventually able to recover. DPoS, on the other hand, could easily avoid this problem by voting out Chinese block producers and replacing them with block producers in other jurisdictions as soon as (or even before) the government took action.

关于为什么DPoS在实践中比PoW更加去中心化的争论，请参阅Ian Grigg的这篇精彩的文章。在文中，他描述了中国政府如何对国内的比特币矿工发起攻击，要么直接接管他们，迫使他们关闭，要么则是间接利用控制中国互联网进出管道的防火墙。这将对比特币网络造成巨大的破坏，哪怕它最终能够恢复，也会在一段时间内使其受到严重损害。而DPoS可以很容易地避免

这个问题，只要能在政府采取行动之时（甚至赶在那之前），就把位于中国的区块生产者排除在外，用其他司法管辖区的区块生产者取而代之就行。

One interesting feature of DPoS is that while block producer candidates compete for token holder votes, elected block producers actually cooperate to secure the network during rounds. Block producers share block rewards (from inflation) equally, and they are only allowed to produce one block per round. There are no incentives for block producers to compete to try to produce more blocks than the other producers, since this is impossible. In EOS and Steem, block producers are funded entirely by inflation; there are no transaction fees. Block producers aren't incentivized to order transactions based on who pays the highest fee; rather, priority is given relative to overall stake—ownership in the network gives users a claim to bandwidth within the network when the network is at capacity. Block producers compete o-chain to get votes, but once they are voted in they cooperate to secure the chain. And since the number of block producers is fixed, block-producing power doesn't concentrate, even with economies of scale.

DPoS的一个有趣的特性在于，当区块生产者候选人竞争代币持有人的选票时，获选区块生产者实际上会在各轮间合作以确保网络的安全。区块生产者平均分享（来自通货膨胀的）区块奖励，并且他们每轮只能出一个块。区块生产者没有动机去竞相生产更多的区块，因为这根本不可能。在EOS和Steem中，区块生产者的资金完全来自通胀；不存在交易费用。区块生产者没有被鼓励根据支付的费用高低来订购事务；相反，优先级是相对于网络的整体风险所有权而给出的——当网络处于容量状态时，网络中的所有权赋予用户对网络带宽的所有权。区块生产者相互竞争以获得选票，但一旦他们当选，他们就会合作来确保区块链的安全。而且，由于区块生产者的数量是固定的，即使经济实现规模化，区块生产能力也不会集中。

CENTRALIZATION OF BLOCK PRODUCTION

区块生产中心化

The most notable feature of any DPoS-powered protocol is that the number of block producers is explicitly limited. The number of block producers varies in different implementations—101 in Lisk, 21 in EOS, etc. Often the number itself is a parameter that can be changed by a token holder vote.

任何DPoS支持的协议最显著的特性都是显式地限制了区块生产者的数量。区块生产者的数量在不同的实现中是不同的——Lisk中有101个，EOS中有21个，诸如此类。通常，数字本身是一个参数，可以通过代币持有者的投票进行更改。

DPoS validation happens in rounds; each round consists of a period in which each block producer is given one slot to produce a block. In Lisk, for example, a round would consist of 101 blocks. At the

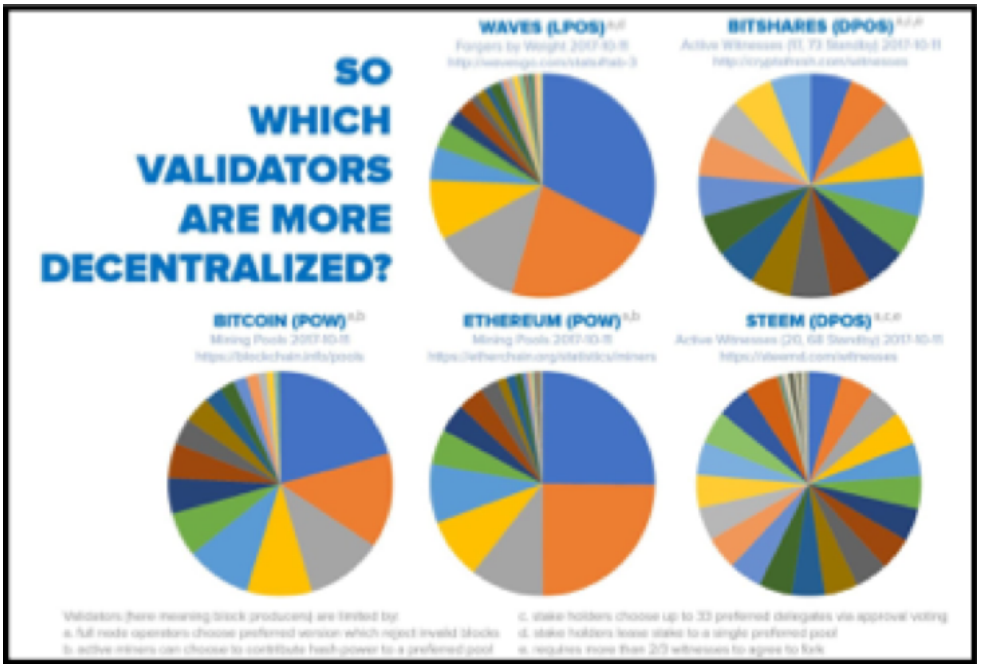
beginning of each round, each block producer is assigned a slot. Each slot corresponds to one block and is the only time in that round in which the assigned block producer can produce a block. If a producer fails to create a block during their slot, then that block is skipped and the transactions from that slot are included in the next block. Token holder votes are tallied each round, and block producers can be voted in or out each round. In every DPoS implementation, the number of potential block producers is always greater than the number of producers allowed in each round. Thus, there are always block producers ready to step in if a malicious producer is voted out. It is also possible to configure DPoS parameters to compensate backup block producers in order to incentivize them to be ready to fill the spots of producers that are voted out (see total witnesses in Steem).

DPoS验证以轮为单位进行；每轮由一个周期组成，其中每个区块生产者都有一个时段(slot)来生成块。例如，在Lisk中，一轮将包含101个区块。在每一轮的开始，每个区块生产者都被分配一个时段。每个时段对应一个块，并且是在该轮中指定的区块生产者可以生成一个块的唯一时段。如果生产者未能在其时段期间生成一个块，则跳过该块，并将来自该时段的事务包含在下一个块中。代币持有者的投票将在每一轮中统计，而区块生产者可以在每一轮中被投票选入或被踢出局。在每个DPoS实现中，潜在区块生产者的数量总是大于每轮允许的生成者总数。因此，如果恶意生产者被淘汰，总会有区块生产者适时补入。也可以配置DPoS参数来补偿候补的区块生产者，以激励它们随时准备好填补被淘汰的生产者的位置（参见Steem中的全职见证人）。

Collusion and censorship by validators is always a concern with any blockchain protocol. If three of the largest Ethereum mining pools colluded, it would be possible for them to pierce the safety of the network. DPoS is aware of these risks and attempts to mitigate them through transparency. In DPoS, token holders are directly responsible for deciding who controls validation. While this puts more responsibility on individual token holders, it also means that the owners of the network have recourse if validators behave badly. If Ethereum mining pools colluded, individual miners participating in the pool would have to point their miners elsewhere, or the community would have to hard fork the network. Both scenarios require some form of off-chain coordination. If DPoS block producers colluded, the community could vote them out within a single round and replace them with honest block producers. This still requires a form of ex-protocol coordination (token holders deciding how to re-allocate their votes), but it is more formalized and arguably more trivial to enact. This architecture allows DPoS to introduce a form of centralization while still maintaining security. The implications of this (as well as potential attack vectors) will be explored later in this document.

在任何区块链协议中，验证者的合谋和审查始终是一个问题。如果三个最大的以太坊矿池串通一气，他们就有可能破坏整个网络的安全。DPoS意识到了这些风险，并试图通过增加透明度来减轻这些风险。在DPoS中，代币持有者直接负责决定谁控制验证。虽然这让单个代币持有

者承担了更多的责任，但这也意味着，如果验证者表现不佳，网络所有者可以求助。如果以太坊矿池串通一气，参与矿池的单个矿工将不得不将他们的矿工派向其他地方，否则社区将不得不硬分叉网络。这两种场景都需要某种形式的离链协调。如果DPoS区块生产者串通，社区可以在一轮投票中将其淘汰，并用诚实的区块生产者取而代之。这仍然需要某种形式的前协议协（代币持有者决定如何重新分配他们的选票），但它更加正式，而且可以说更容易实施。这种体系结构允许DPoS在保持安全性的同时引入一种中心化形式。本文稍后将探讨这一点（以及潜在的攻击向量）的含义。



图片来源

SCALABILITY

可伸缩性

Known and limited block producers means that blocks can be propagated through the network much more efficiently, enabling significant scalability increases. Blocks can also be consistently and reliably produced in a much smaller time frame (BitShares currently produces a block every 3 seconds). Furthermore, finality can be reached as soon as of the block producers have confirmed a transaction, with strong guarantees that a transaction is on a valid chain even before that.

已知有限的区块生产者意味着可以更有效地通过网络传播区块，从而显著提高可伸缩性。区块也可以在更短的时间内稳定可靠地生成（Bitshare目前每3秒出一个块）。此外，只要区块生产

者确认了一个事务，就可以达到最终性，并且在此之前就可以确保一个事务处于一个有效的链上。

While DPoS is certainly more scalable than PoW, exactly how fast it can go depends on a variety of factors. EOS is attempting to optimize for extremely high throughput by using the WASM virtual machine and employing a message-based architecture instead of a state-based one. Early results showed 50,000 tps on an EOS smart contract, but those results are not indicative of full-scale main net performance. Recently, the community-run EOS test net hit 600 tps with beta software and non-specialized machines, and Larimer recently claimed in an update that the software could be set to debut with 5,000 tps in its single-threaded architecture before moving to parallel execution.

虽然DPoS确实比PoW具有更强的可伸缩性，但是它的速度取决于多种因素。EOS在优化极高的吞吐量方面，试图通过使用WASM虚拟机和基于消息的体系结构，而不是基于状态的体系结构。早期的结果显示EOS智能合约上有50,000个tps，但这些结果并不能代表其全面的主网性能。最近，社区运行的EOS测试网在使用beta软件和非专用机器时速度达到了tps 600次/秒，Larimer近期在一份更新中声称，该软件可以在进入并行执行之前，在其单线程体系结构中以5000 tps的速度首次发布。

It is worth noting that three of the top 5 blockchains with the most operations performed daily are DPoS blockchains, according to Blocktivity.info. And while Ethereum is consistently operating at near capacity, both BitShares and Steem have no pending transactions and plenty of bandwidth to spare. Smart contract platforms that host large-scale dApps need to be able to handle many thousands of operations per second, whether they are simple likes or million-dollar value transfers. This chart provides a great breakdown of operation type and count for BitShares, while this link provides statistics for Steem. For more information on how BitShares achieves its performance, see detailed explanations here and here.

值得注意的是，根据Blocktivity.info，在每天执行最多操作的前5个区块链中，有3个是DPoS区块链。尽管以太坊一直在以接近容量的速度运行，但BitShares和Steem都没有待处理的事务，而且有足够的带宽可供使用。承载大规模去中心化应用程序的智能合约平台需要能够每秒处理数千次操作，无论是简单的点赞还是百万美元的价值转移。这个图表提供了Bitshares操作类型和计数的详细分类，而这个链接提供了Steem的统计数据。欲知有关BitShares如何实现其性能的更多信息，请参见这里和这里的详细说明。

NETWORK INFRASTRUCTURE AS A SERVICE

作为服务的网络基础设施

Every blockchain network can be divided into two major subsets of actors—those who perform operations on the network and those who validate the operations. We can refer to the first group as users and the second group as validators.

每个区块链网络可以分为两个主要的参与者子集——在网络上执行操作的参与者和验证操作的参与者。我们可以将第一组称为用户，将第二组称为验证者。

In Bitcoin, Ethereum, Monero and other proof of work-based blockchains, the validators are miners. Miners race to solve computationally intensive puzzles, and the first to solve the puzzle is allowed to produce a block (and collect transaction fees and the block reward). In traditional PoS, users must bond their tokens, and they are awarded the ability to produce blocks proportional to their bonded stake.

在比特币、以太坊、门罗币(Monero)等基于工作证明的区块链中，验证者是矿工。矿工竞相解决计算密集型的谜题，第一个解决谜题的人可以生成一个区块（并收取交易费用和区块奖励）。在传统的PoS中，用户必须以其代币作保，并按提交的保证金比例获得相应的生成区块的能力。

In each of these scenarios, validators are providing key network infrastructure: They are collecting transactions, ordering them, and preventing double-spends. In PoW, validators are those with access to the best hardware and cheapest electricity. In PoS, validators are those with large ownership stakes in the network. In DPoS, however, the validators can be thought of as contractors that are hired by the owners of the network (token holders). They are hired (voted in), given a job (to produce blocks), paid (through inflation or transaction fees), and can be fired (voted out) for not performing their duties.

在这些场景中，验证者都提供了关键的网络基础设施：他们收集事务，对事务进行排序，并防止双花。在PoW中，验证者是那些能够使用最好的硬件和最便宜的电力的人。在PoS中，验证者是那些在网络中拥有大量所有权的人。然而，在DPoS中，验证者可以被看作是由网络所有者（代币持有者）雇用的承包商。他们被雇佣（通过票选），获得一份工作（生产区块），取得酬劳（通过通货膨胀或交易费用），并且可能因为不履行职责而被解雇（投票被踢走）。

This structure means that DPoS network token holders, as the owners of the network, ultimately have control over who provides infrastructure, while Bitcoin and Ethereum give token holders no choice. If miners misbehave, as they have incentive to do, users have no recourse. DPoS is the only algorithm that allows infrastructure providers to be easily fired (no slashing required) and replaced for not providing a good service. Reasons for firing could include any of the following:

这种结构意味着DPoS网络代币持有者作为网络的所有者，最终控制谁提供基础设施，而比特币和以太坊的代币持有者则没有选择。如果矿工行为不端——他们有这么做的动机，用户也没

有追索权。DPoS是唯一一种能轻松解雇并替换未能提供良好服务的基础设施供应者（不需要削减）的算法。解雇的理由可包括下列任何一项：

DISHONESTY

不诚实

- The appearance of dishonesty, or even a mere lack of sufficient transparency compared to other candidates
- Greed (e.g. trying to demand higher block rewards than other producers)
- Censorship
- Malicious collusion
- Support of controversial or malicious changes to the network
- Failure to support community-backed changes
- Regulatory fear based on jurisdiction (for example, Chinese block producers could be voted out if China announced a crackdown on crypto)
- 与其他候选人相比，候选人表现得不够诚实，甚至缺乏足够的透明度
- 贪婪（例如，试图要求获得比其他生产者更高的区块奖励）
- 审查
- 恶意串通
- 支持对网络进行有争议或恶意的更改
- 未能支持社区推动的变革
- 基于管辖权的监管恐慌（例如，如果中国宣布打击加密货币，中国的区块生产者可能会被投票选出去）

ON-CHAIN GOVERNANCE

链上治理

DPoS is inheherently a form of on-chain governance; it uses stake-weighted voting to allow the owners of the network (token holders) to make decisions about the network. DPoS is a form of liquid representative democracy where voting power can be allocated to other participants and votes can be changed at any time. While voting for block producers is the primary governance use case, token holder voting can also be used to decide on things like development funding, monetary policy, network parameters, hard forks and more.

DPoS在本质上是一种链上治理形式；它使用保证金加权投票允许网络所有者（代币持有者）对网络做出决策。DPoS是一种流动式的代议制民主，在这种民主制度下，投票权可以分配给其他参与人，投票可以随时改变。虽然为区块生产者投票是主要的治理用例，但是代币持有者投票也可以用于决定诸如开发资金、货币政策、网络参数、硬分叉等等。

Blockchain governance is still very much a nascent field, and there exists a lot of disagreement over which approach to blockchain governance is the most promising. Some, like Ethereum researcher Vlad Zamfir, have argued that on-chain governance is a bad idea because, among other reasons, it negates the role of non-block-producing full nodes in the governance process. Analyst Nic Carter similarly concluded that Bitcoin's informal off-chain governance, which consists of several different social and technological layers, is the ideal form of governance for a decentralized network. Fred Ehrsam, co-founder of Coinbase, argued for on-chain governance as a way to bring formal structure to these messy interactions. Many point to the Bitcoin scaling debate, the Ethereum DAO fork, and the recent Parity wallet bug debate as three examples of situations where on-chain governance could have more easily rectified very messy and uncertain situations.

区块链治理在很大程度上仍是一个新兴领域，对于区块链治理的哪种方法最有前途，存在着许多分歧。有些人，比如以太坊的研究人员Vlad Zamfir，认为链上治理是一个坏主意，其中一个原因在于它否定了非采矿的完整节点在治理过程中的作用。分析师Nic Carter也得出了类似的结论，认为由几个不同的社会和技术层面组成的比特币的非正式链下治理，应该是去中心化网络的理想治理形式。Coinbase联合创始人Fred Ehrsam则支持将链上治理作为为混乱的交互带来正式结构的方式。许多人指出，比特币扩容之争、以太坊硬分叉出DAO，以及最近的Parity钱包漏洞之争，这三个例子表明，链上治理可以更容易地纠正非常混乱和不确定的情况。

DPoS chains embrace the fact that all blockchain networks are inherently political and seek to formalize the political process. While there are certainly issues with on-chain governance and token voting (which we'll explore later), both are key features of DPoS. DPoS is a community-owned operational hierarchy that operates in a fully transparent, decentralized way. While it is not clear that

on-chain governance is better than other forms of blockchain governance, it certainly isn't clear that it is worse. We believe strongly that this approach should be tried and tested.

DPoS区块链接受这样一个事实，即所有区块链网络本质上都是政治性的，并寻求将政治过程正式化。虽然链上治理和代币投票肯定存在问题（我们将在稍后对此进行讨论），但它们都是DPoS的关键特性。DPoS是一个社区拥有的操作层次结构，以完全透明、去中心化的方式运行。虽然目前对于链上治理是否优于其他形式的区块链治理还得打个问号，但对于它是否就比其他形式更差，同样也是未知之数。我们强烈认为，这种方法应该得到试验和检测。

SELF-FUNDING THROUGH INFLATION

通过通货膨胀自筹资金

Almost every major blockchain pays for infrastructure with inflation. In the case of Bitcoin and Ethereum, miners receive block rewards as compensation for validating the blockchain. When block rewards run out in the future, infrastructure will have to be supported through fees alone. This raises questions about how high fees will get in the future, how that will affect incentives to mine, and whether that will affect the security of the chain.

几乎每一个主要的区块链都用通胀来支付基础设施。在比特币和以太坊中，矿工通过验证区块链获得区块奖励。当区块奖励在未来耗尽时，基础设施将只能通过收费来支持。这就提出了一系列问题：未来的费用会有多高？这将如何影响对采矿的激励？

EOS and Steem, because they have no transaction fees, use an entirely different model. Not only do they use inflation to pay block producers to provide infrastructure, but they also use inflation to fund the development of the platform itself. Token holders can vote on a maximum annual inflation rate, initially set at 5%. This number can be changed, as it has been several times in Steem. Token holders also vote on how much of the annual inflation is paid directly to block producers. If the token price increases, users can decide whether to keep block producer pay steady (by lowering block rewards) or to allow block producers to capture additional profits that can be used to scale up their infrastructure. That which is not paid to block producers can be paid to a set of community smart contracts that can be used in a wide variety of ways. A contract could be a development fund that pays out developers based on community votes; it could go directly to a company that is actively working on development; it could be used to fund hackathons; it could be burned; and more. DPoS actually makes it possible for developers, marketers, and others building community tools to be funded by the blockchain itself.

EOS和Steem因为没有交易费用，所以使用完全不同的模型。他们不仅利用通胀来支付区块生产者提供基础设施的费用，而且还利用通胀来为平台本身的开发提供资金。代币持有者可以投

票决定最高年通胀率，最初设定为5%。这个数字可以更改，在Steem中就已经更改了好几次。代币持有者还将投票决定每年有多少通货膨胀是直接支付给生产者的。如果代币价格上涨，用户可以决定是保持区块生产者支付稳定（通过降低区块奖励），还是允许区块生产者获取额外的利润用于扩大其基础设施。没有支付给区块生产者的那部分利润可以支付给一组以多种方式使用的社区智能合约。合约可以是一个开发基金，根据社区投票支付给开发人员；它可以直接流向一家正在积极从事开发的公司；它可以用来资助黑客马拉松；它可以被烧掉；用法不胜枚举。DPoS使得开发人员、营销人员和其他构建社区工具的人员能够获得区块链本身的资助。

Many people struggle with the concept of inflation and are adverse to relying on inflation funding. This shouldn't be the case. Inflation is perhaps the only method by which blockchains can be funded in a fair way because it solves the tragedy of the commons problem. Some blockchains, like Monero, rely entirely on community crowdfunding of development initiatives. While the generosity of the Monero community is remarkable, it remains unclear whether that is a sustainable way to fund development. Everyone benefits from the development advances made, but only a minority of users are willing to contribute their own money to funding. With inflation funding, all users collectively fund development and security ratably, and they all *collectively* reap the benefits. As Fred Ehrsam points out, inflation funding can actually be a net positive for token holders:

许多人不太能接受通货膨胀的想法，反对依靠通胀筹集资金。情况不应该如此。通货膨胀可能是区块链以公平的方式获得资金的唯一方法，因为它解决了公共问题的悲剧。一些区块链，比如门罗币，完全依赖于社区众筹的发展计划。虽然门罗币社区的慷慨颇为引人注目，但尚不清楚这种资助发展的方式是否有可持续性。每个人都从所取得的开发进展中受益，但是只有少数用户愿意自己出钱来资助。而在通胀资金的支持下，所有的用户都可以为开发和安全提供可靠的资金，并*共同*获得收益。正如Fred Ehrsam所指出的那样，对代币持有者而言，通胀融资实际上可以带来净收益：

> "If Ether holders believed an upgrade (ex: sharding) would make the price go up by >10%, they'd be happy to pay close to 10% of their tokens for it. That means Ethereum could crowdfund a $3bn feature bounty by inflating the number of ETH by 10% and pay the newly created tokens to the creator(s) of the upgrade. This is somewhat analogous to taxes: everyone in the community chips in to fund common infrastructure (ex: roads) which no one would build alone."
>
> "如果以太币持有者相信升级（例如分片）会使价格上涨10%，他们会很乐意多买近10%的代币。这意味着以太坊可以通过将ETH的数量增加10%，众筹30亿美元的功能奖金，并将新创造的代币支付给升级的创建者。这有点类似于税收：社区里的每个人都为公共基础设施（比如道路）出资，这些基础设施是没有人可以独自建造的。"

Every blockchain must pay to secure its network through either transaction fees, inflation, or both. Transaction fees force active users to pay, while passive users (hodlers) don't. A user could secure her

entire life savings in Bitcoin or Monero without almost ever contributing to the security of the platform through transaction fees. This creates a free-rider problem. Transaction fees are also variable and unpredictable, and may need to be astronomically high in order to pay for network security. Inflation is a more equitable and user-friendly way of securing the network.

每个区块链必须通过交易费用、通货膨胀或两者兼而有之的方式来支付网络安全费用。交易费用迫使主动用户付费，而被动用户（持有者）则不会。用户可以用比特币或门罗币来保障自己的毕生积蓄，而几乎无需通过交易费用为平台的安全性做出任何贡献。这就产生了搭便车的问题。交易费用也是可变和不可预测的，而且可能需要有天文数字那么高才能支付网络安全费用。在确保网络安全方面，通货膨胀是一种更公平、更用户友好的方法。

Similar approaches have been tried by other projects in a number of ways. Zcash collects a "Founders' Reward," that sends 10% of the total money supply to the Zcash Company and its shareholders. Dash collects a portion of block rewards for a masternode-vote development fund. DPoS formalizes these arrangements, bakes them directly into the protocol, and allows for maximum flexibility and accountability.

类似的方法也在其他项目中以多种方式进行了尝试。Zcash收取"创始人报酬"，将总货币供应量的10%发给Zcash公司及其股东。Dash收取了区块奖励中的一部分资金，作为主节点投票发展基金的一部分。DPoS将这些安排正式化，将它们直接放入协议中，并允许最大程度的灵活性和可靠性。

DPoS Attack Vectors

DPoS攻击向量

Below, we'll outline the major DPoS attack vectors and evaluate the threat they present.

下面，我们将概述主要的DPoS攻击向量，并评估它们所带来的威胁。

NOTHING-AT-STAKE

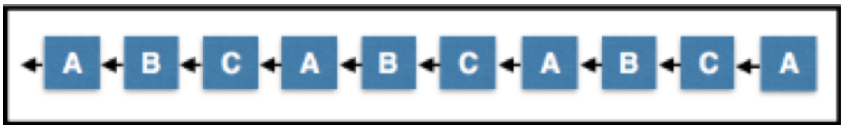
不承担任何风险

The "Nothing at Stake" problem is a flaw in some PoS schemes. Specifically, it refers to the fact that in the case of a fork, there is very little additional cost to the validator to validate on both chains. This is the optimal strategy for validators, since it is likely the most profitable.

"无利害关系"的问题是一些PoS计划的缺陷。具体来说，它指的是在分叉的情况下，验证者在两个链上验证的额外成本非常小。这是验证者的最佳策略，因为它可能是最有利可图的。

DPoS does not suffer the nothing-at-stake problem in practice. Token holders in DPoS are using their stake to vote on validators, not on blocks. DPoS is a longest-chain-wins algorithm. Because the number of validators is fixed and the order is decided each round, it would be impossible for a minority subset of validators to produce a fork that overtook the main chain.

DPoS在实践中并没有遇到无利害关系问题。DPoS中的代币持有者使用他们的保证金对验证者、而不是对区块投票。DPoS是一种最长链为赢家的算法。因为验证者的数量是固定的，并且每轮的顺序是确定的，所以一小部分验证者不可能产生取代主链的分叉。

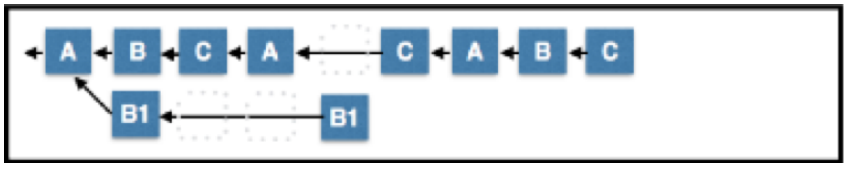


DPoS block production under normal network conditions (source)

正常网络条件下的DPoS区块生产（图片来源）

If a single block producer were to produce blocks on multiple forks (as shown below), the main chain would still advance with the rest of the honest block producers. The longest chain is considered the canonical chain, so the producer is unable to do any harm.

如果一个区块生产者要在多个分叉上生产区块（如下所示），主链仍然会与其他诚实的区块生产者一起前进。最长的链被认为是标准链，所以生产者不能对其做出任何伤害。



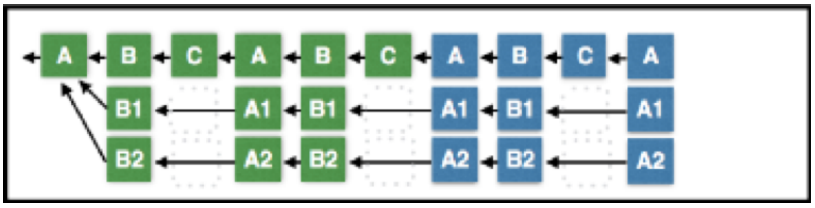
Source

图片来源

Even if a majority of block producers colluded to produce blocks on several forks (as shown below), the honest minority would still determine the longest chain. In each of these instances, there would be

clear cryptographic evidence that block producers had created blocks on multiple conflicting chains, and they could be voted out for doing so. It would also be possible to introduce slashing conditions and other protocol-level punishments based on cryptographic evidence of Byzantine behavior, but these additional features aren't always necessary.

即使大多数块生产者串通起来在几个分叉上生产区块（如下所示），诚实的少数人仍然可以确定最长的链。在每种情况下，都有明确的加密证据证明区块生产者在多个相互冲突的链上生成了区块，他们也因此可能被投票否定这么去做。基于拜占庭行为的加密证据，也有可能引入削减条件和其他协议级的惩罚，但这些额外的特性并不总是必要的。



Source

图片来源

It is possible for block producers to create blocks on multiple forks at little additional cost, but they do have some things at stake—their job, reputation, and future income stream. Because Byzantine behavior can be detected, it is a risky move. To actually corrupt the integrity of the chain would require collusion among a strong majority of delegates—at that point the attack becomes less about "nothing-at-stake" and more about traditional Byzantine fault tolerance.

区块生产者有可能以很少的额外成本在多个分叉上生成区块，但他们确实面临一些风险——他们的工作、声誉和未来的收入流。因为拜占庭式的行为是可以检测到的，所以这是一个冒险的举动。实际上，要破坏这条链条的完整性，就需要绝大多数代表相互勾结——到那时，攻击就不再是"无厉害关系"，而更多的是传统拜占庭式的容错。

For a detailed explanation, see Dan Larimer's DPoS white paper.

相关详细说明，请参阅Dan Larimer的DPoS白皮书。

EXPLOIT LOW VOTER TURNOUT

利用低投票率

This is the most obvious attack against a DPoS blockchain. The core of this attack is the fact that in any voting system, very few participants actually show up and vote. In blockchain token voting

systems, anyone with a small stake is unlikely to actually influence the direction of the platform with their vote. The time spent researching on how to vote may not be worth the eort for what they view as a minimal impact. Voters with a small stake may practice rational ignorance— the time spent researching how to vote may be more costly to them than the value that voting brings. DPoS attempts to at least partially rectify this by allowing proxy voting, in which a user can lend their voting power to another user who they consider more informed. In this case, the effort of deciding to whom to delegate voting power is likely less than the value gained. Still, the natural result of these systems is often that overall voter turnout is low, and voting is mostly done by whales, exchanges, and wallet providers. This problem has been explored by Vitalik in his blog post on blockchain governance.

这是对DPoS区块链最明显的攻击。这种攻击的核心是，在任何投票系统中，真正出现并投票的参与者都非常少。在区块链代币投票系统中，任何押下少量保证金的人都不太可能通过他们的投票实际影响平台的方向。花时间研究如何投票可能不值得，因为他们认为带来的影响微乎其微。押下少量保证金的选民可能会实践理性的无知——研究如何投票的时间对他们来说可能比投票带来的价值更昂贵。DPoS试图通过允许代理投票，在一定程度上纠正这一点，在代理投票中，用户可以将自己的投票权出借给他们认为更熟悉情况的其他用户。在这种情况下，决定将投票权委托给谁的努力可能比获得的价值要小。尽管如此，这些系统的自然结果往往是总体投票率很低，投票主要由鲸鱼、交易所和钱包提供商完成。Vitalik在他关于区块链治理的博文中探讨了这个问题。

Say, for example, that only 10% of the total supply of tokens was being used to vote. A whale (or group of whales) with more than 5% of the total supply could step in and take over governance. For context, the top block producer on BitShares has about 33% approval. Most DPoS systems use approval voting in which users split their votes among all candidates, and the top candidates by total approval become the block producers. This makes it much more difficult for a whale to take over the voting process.

例如，只有10%的代币被用于投票。占总供应量5%以上的一只巨鲸（或一群鲸鱼）可以介入并接管治理。具体来说，BitShares上最大的区块生产者获得了约33%的认可。大多数DPoS系统使用的是认可票制，用户将他们的选票分配给所有候选人，获得认可最多的候选人成为区块生产者。这使得鲸鱼接管投票过程变得更加困难。

One important caveat is that attacks on the voting system are bad for the network as a whole, and successful ones will likely result in a decrease in the price of each token. Anyone with a significant stake in the network should be incentivized to vote to protect the value of their tokens. While it is entirely possible that the percentage of token holders who vote may be small, the ones who do will be those with the largest stake. That means that an attacker would still have to purchase a very significant

stake in order to take over governance. Like all other PoS systems, DPoS will likely find follow the Pareto Principle, where a small subset of large stakeholders does most of the work related to decision making. This is not necessarily a bad thing, as large stakeholders have incentives to improve the network.

一个重要的警告是，对投票系统的攻击对整个网络是有害的，成功的攻击可能会导致每个代币的价格下降。任何与该网络有重大利害关系的人都应该被鼓励投票以保护他们的代币价值。虽然代币持有者投票的比例有可能很小，但真正投票的将是那些拥有最多权益的人。这意味着攻击者仍然必须押注购买为数不少的保证金才能接管治理。与所有其他PoS系统一样，DPoS可能会遵循Pareto原则，即一小部分主要利益相关者完成与决策相关的大部分工作。这未必是件坏事，因为主要利益相关者有动机改善网络。

In fact, participation is a problem that plagues all proof of stake systems, including Ethereum's proposed Casper PoS. Because ETH has utility outside of just staking, it is likely that only a fraction of all ETH in circulation will actually be staked to secure the network. If this is a very small percentage of total ETH, then an ETH whale could step in at any time, stake their tokens, and take over the validation process. This threat is described well in this Cosmos blog post. One advantage to the DPoS model is that, in most designs, DPoS tokens can delegate their voting power (either directly to a block producer or to a proxy voter) and still retain all of their utility. So participation in the voting system has no cost other than the time spent deciding how to allocate one's voting power. While small stakeholders in Ethereum may use staking pools to earn a passive return on their assets, the process of joining a staking pool may not be super easy, and there are capital lockup costs associated with doing so. DPoS token holders can quite easily delegate their voting power to someone they trust to do proper research into block producers, and they are still free to utilize their tokens in any way they choose to do so.

事实上，参与是一个困扰所有PoS系统的问题，包括以太坊提议的Casper PoS。因为以太币除了押注外还有其他用途，所以很可能只有一部分流通中的以太币会被押记以确保网络的安全。如果这只占到整个以太币中很小的一部分，那么以太币巨鲸可以随时介入，抵押其代币并接管验证过程。这篇Cosmos博客文章对这种威胁做出了很好的描述。DPoS模型的一个优点是，在大多数设计中，DPoS代币可以将它们的投票权委托给区块生产者或代理投票人，同时仍然保留它们的所有实用程序。因此，参与投票系统除了花时间来决定如何分配自己的投票权外，并没有其他成本。虽然以太坊中的小型利益相关者可能会使用押注池来获得被动资产回报，但加入押注池的过程可能不会特别容易，而且存在与此相关的资本锁定成本。DPoS代币持有者可以很容易地将他们的投票权委托给他们信任的人，让他们对区块生产者进行适当的研究，并且他们仍然可以自由地以任何方式使用代币。

Some models do require DPoS voters to lock up their tokens for a period of time when voting in order to incentivize votes that have some "skin in the game." This pushes users to cast more informed votes that take into account the long-term success of the platform, but it also limits the number of participants willing to vote. This is currently a subject of debate within the EOS community.

有些模式确实要求DPoS的投票者在投票时将他们的代币锁定一段时间，自个儿有利益在其中，这样更能激励投票。这促使用户了解更多信息，在考虑平台长期成功的前提下投票，但这也限制了愿意投票的参与者数量。这是目前EOS社区中争论的一个主要话题。

Voter participation will likely depend on a few things—voting participation as part of the social contract, how well the community encourages it, how easy it is for users to vote or delegate voting power, and more. Education and easy-to-use voting interfaces will be especially important in this regard.

选民的参与可能取决于几个因素——作为社会契约一部分的投票参与、社区对它的鼓励程度、用户投票或委派投票权的难易程度等。在这方面，教育和易于使用的投票界面将尤为重要。

BRIBING ATTACKS

贿赂攻击

Another attack, and one that has been observed in practice, is that of block producers paying for votes. This issue has affected Lisk and Steem recently. Whether this should be considered an attack depends on perspective and may hinge upon what the elected block producers do with their purchased validation power. Still, this situation is not desirable, so it will be examined in the context of maliciousness.

另一种攻击，也是在实践中观察到的一种攻击，是区块生产者为选票付费。这个问题最近影响到了Lisk和Steem。这是否应该被视为攻击，取决于各人的视角，也可能还取决于所选区块生产者如何运用其购买的验证权。然而，这种情况是不可取的，因此应在恶意的背景下加以审查。

Lisk, for example, has two pools (LiskElite and LiskGDT) that promise a portion of block rewards will be paid back to the users who vote for their delegates. There is even a website dedicated to helping users find the delegates with the best payouts and encouraging users to vote out those that don't share rewards.

例如，Lisk有两个池（LiskElite和LiskGDT）承诺将向投票给其代表的用户返还部分区块奖励。甚至有一个网站专门帮助用户找到奖金额最高的代表，并鼓励用户将那些没有分享奖金的代表淘汰出局。

The sustainability and efficacy of these attacks depends on other elements of the protocol. The attack is possible in any implementation of DPoS (or any implementation of on-chain voting, in general), but other features can make it much less likely. In system where the requirements for a block producer are simply to run a cloud instance that does the validation work, profit sharing is an easy option. Blockchains like Lisk, which are still in their infancy and don't have much usage, don't require a lot from block producers.

这些攻击的可持续性和有效性取决于协议中的其他内容。这种攻击在DPoS的任何实现（或者一般来说，链上投票的任何实现）中都是可能的，但是其他特性使这些攻击的可能性大大降低。在系统中，对区块生产者的要求只是运行一个执行验证工作的云实例，因此利润共享是一个简单的选择。像Lisk这样的区块链还处于起步阶段，没有太多的用途，不需要从区块生产者那里得到太多。

In EOS, however, the requirements for block producers go far beyond just running software. EOS block producers are also expected to provide storage, participate in governance, and gradually use their profits to scale up their hardware in order to increase the total capacity of the network. Larimer has even said that eventually EOS will scale to 21+ data centers with gigabit connections speaking directly to one another. The operational costs for block producers will be much higher than in other systems, and paying for votes will cut into profit margins. Block producers who pay for votes will also have less resources to scale up their systems, so the network itself will suffer. Voters who care about the long-term health of the network (and price of the token) will prefer block producers who contribute to increased network capacity rather than providing short-term kickbacks. It will be in the interest of businesses built on top of EOS (who will likely be among the largest token holders) to do vote for block producers who don't pay voters.

然而，在EOS中，对区块生产者的需求远远不止运行软件。EOS区块生产者还需要提供存储，参与治理，并逐渐使用他们的利润来扩大硬件规模，以增加网络的总容量。Larimer甚至表示，EOS最终将扩展到21个以上的数据中心，这些数据中心之间将有千兆连接，可以直接相互通信。区块生产者的运营成本将比其他系统高出许多，而为投票付费将削减其利润率。为投票付费的区块生产者扩展其系统的资源将相应减少，所以网络本身也会受到影响。关心网络长期健康发展（以及代币价格）的选民将更青睐那些为提高网络容量做出贡献、而不是提供短期回扣的区块生产者。建立在EOS之上的企业（他们很可能是最大的代币持有者之一）将票投给不向选民付费的区块生产者，这符合它们的利益。

If a block producer offers nothing but a share in the block reward, it is unlikely that he or she could complete for very long without becoming a tax on the network. In Steem, for example, witnesses campaign with plans about how they will work to improve the network. Similar campaigns are already happening in EOS (see EOS New York, EOS SoCal, EOSYS, and more). Token holders should realize that the network would stagnate with vote-bribing block producers essentially taxing the system, and eventually they should be voted out. Further, EOS also implements a vote decay system, whereby more recent votes carry more weight. Voters who recast their votes every month will have the full weight of their votes counted, while older votes will slowly decay until they have minimal impact after 2 years. This will encourage participation and also slowly discount those who simply cast votes once. In the case of block producers offering reward sharing, this means that those who simply cast votes one time and expect to earn passive income will gradually have their voting power removed. Other methods, like requiring voters to lock up their tokens for a period of time, could discourage vote bribing, as well.

如果一个区块生产者能提供的仅仅是区块奖励分成，那么他或她不可能在长期保持竞争力的同时，仍然能对网络有所贡献。例如，在Steem，证人运动就提出了改善网络的计划。类似的活动已经在EOS中展开（参见EOS New York、EOS SoCal、EOSYS等）。代币持有者应该意识到，网络会因为贿赂投票区块生产者而停滞不前，这本质上是对系统征税，最终他们应该被投票淘汰出局。此外，EOS还实现了选票衰减系统，越是近期的选票具有越大的权重。每个月再次投票的选民，其选票将获得完整权重，而老选民的选票将会慢慢衰减，直到两年后影响力降到最低。这将鼓励人们参与投票，同时也会慢慢降低那些只投过一次票的人的影响力。在区块生产者提供奖励分享的情况下，这意味着那些仅仅投了一次票，并希望获得被动收入的人将逐渐失去投票权。其他的方法，比如要求选民把他们的代币锁定一段时间，也可以阻止贿选。

Because DPoS is a community-driven consensus algorithm, the response to block producer bribes will ultimately be in the hands of the community. One option for the community would be to incorporate a ban on bribes and profit sharing directly into the EOS constitution. The constitution has been described as a “peer-to-peer terms of service agreement or a binding contract among those users who sign it.” Every transaction contains a hash of the constitution and expresses the user’s endorsement of the contract (the full implications of this digital constitution will be examined in our upcoming full analysis and valuation report on EOS). In Lisk, profit-sharing block producers had to make their intentions very public, so it would be very easy to identify offenders.

由于DPoS是一种社区驱动的共识算法，对区块生产者行贿的回应最终将掌握在社区手中。社区的一个选择是将禁止贿赂和利润分享直接纳入EOS宪法。该宪法的定义是“点对点服务协议条款或合约，该合约对所有签署者具有约束力。”每笔交易都包含宪法的一个散列，并表达了用户对合约的认可（我们将在即将发布的EOS全面分析和评估报告中分析这一数字宪法的全部

含义）。在Lisk中，利润分成的区块生产者必须公开他们的意图，因此很容易识别出不守规矩的人。

Ultimately, we believe that block producers paying for votes is a bad thing. It encourages voting based not on what is best for the network but rather who pays the highest returns. This does not align with the long-term incentives of the network, or even the long-term incentives of token holders. We hope that the communities that emerge around DPoS chains create norms where paying for votes is very much frowned upon, and we plan to encourage such a norm ourselves. We also encourage further research into in-protocol mechanisms, like voting lockups and voting decay, that might discourage such behavior.

说到底，我们认为区块生产者为选票付费是一件坏事。它鼓励人们在投票时不是基于什么对网络最有利，而是看谁给的回报最高。这与网络的长期激励不一致，甚至与代币持有者的长期激励也不一致。我们希望围绕着DPoS区块链出现的社区能够建立抵制贿选的规范，我们本身也计划鼓励这种规范。我们还鼓励进一步研究协议内机制，如投票锁定和投票衰减，这可能会阻止这类贿选行为。

ATTACKS AT SCALE

大规模攻击

One interesting attack vector that has not yet been observed in practice involves assumptions about what an industrial-scale DPoS blockchain looks like. Larimer has said that EOS is likely to scale in a way such that large data centers act as block producers in order to provide the level of bandwidth and speed the network requires. This outcome may be several years away, but the implications are worth considering.

一个尚未在实践中观察到的有趣的攻击向量涉及到工业规模DPoS区块链的假设。Larimer表示，EOS很可能会以这样一种方式扩展，即大型数据中心充当区块生产者，以提供网络所需的带宽水平和速度。这一结果可能还需要几年时间，但其影响值得考虑。

If block producers are expected to be in dedicated data centers, this limits the number of potential block producers and especially limits the number of entities that could step in to replace block producers that are voted out. Validator churn may be quite low as a result. If there aren't any block producers with sufficient resources to replace block producers that have been voted out, then the network may suffer as a result. Voters would have to decide between punishing a misbehaving block producer and lowering the overall resources of the network.

如果要求区块生产者身处专门的数据中心中，这将限制潜在区块生产者的数量，特别是限制可以随时介入以替代被淘汰的区块生产者的实体的数量。因此，验证者的更迭流失率可能相当低。如果没有手握充足资源的区块生产者来替换已被选举淘汰的区块生产者，那么网络可能会因此受到影响。选民将不得不在惩罚一个行为不端的区块生产者和降格网络的整体资源之间做出选择。

Importantly, DPoS networks can continue to run with a smaller number of validators until a new peer is ready to join the block producer quorum. This is not ideal, but it at least allows network operations to continue as normal during the transition period. New block producers may not have the same resources as existing producers, but they can campaign for election on the promise to use their block rewards to quickly scale up their efforts.

重要的是，DPoS网络可以继续使用更少的验证者运行，直到一个新的对等点做好成为区块生产者的准备，满足出块人法定人数。这并不理想，但至少可以保证在过渡期间网络操作能正常进行。新的区块生产者可能没有与现有生产者相同的资源，但他们可以在竞选时承诺利用区块奖励迅速扩大自己的努力。

BLOCK PRODUCERS COLLUDE

区块生产者勾结

In any blockchain system, the threat of block producers colluding is looming. In DPoS, this threat is often presented as especially dangerous; because the number of validators is small, it should theoretically be easy to organize collusion among them. While block producer collusion is obviously not desired, it is important to think about what kind of damage colluding block producers could do, and what the recourse is in the case that they attempt to do so.

在任何区块链系统中，区块生产者串通的威胁都是迫在眉睫的。在DPoS中，通常认为这种威胁尤为危险；由于验证者的数量很少，理论上他们之间应该很容易勾结一气。区块生产者串通显然是不可取的，但重要的是要考虑区块生产者的这种做法可能造成何种损害，以及在他们试图这样做的情况下能有怎样的追索权。

In DPoS systems, there are three major attacks that colluding block producers (meaning more than of all block producers) could launch:

在DPoS系统中，有三种主要的攻击是合谋的区块生产者（意味着超过所有区块生产者相加）可以发起的：

1. Censorship

2. Changing System Parameters

3. Double Spends

1. 审查

2. 改变系统参数

3. 双花

Censorship in the context of DPoS means that a block producer refuses to process valid transactions. If a single block producer censors an individual or entity, it will be futile. Not only will the next block producer validate the transaction in the following block, but the single block producer's censorship attempt will be visible on-chain, and repeated infractions would get the producer voted out. For individual block producers (or even a minority group of block producers), the most damage they could cause is delaying transactions by not processing them in their blocks. Those transactions will still be processed by the honest majority, so it is unlikely that block producers will even attempt censorship since it won't amount to much (they'd simply delay a transaction for a few seconds until the next block producer's turn). And while it is certainly possible to do damage by delaying transactions, block producers are risking their reputation, future income stream, and possibly even arbitration every time they attempt to do so (see page 6 of this paper). An effective implementation of DPoS will likely see block producers quickly voted out for any attempt at censorship.

在DPoS的上下文中，审查意味着区块生产者拒绝处理有效的事务。如果只有一个单独的区块生产者审查某个个人或实体，这将是徒劳的。下一个区块生产者将在下一个区块验证交易，而且上一个区块生产者的审查尝试将在链上可见，这种违规行为反复出现，生产者就会被投票出局。对于单个区块生产者（甚至是一小部分区块生产者）来说，它们可能造成的最大损害是由于不在块中处理事务而导致事务延迟。这些事务仍将由诚实的多数人来处理，因此，区块生产者甚至不太可能尝试审查，因为这根本不会产生多大影响（他们只会将交易延迟几秒钟，很快就能轮到下一个区块生产者来处理）。虽然延迟交易确实有可能造成损害，但区块生产者每次试图这么做时，都会冒着声誉、未来收入流受损甚至仲裁的风险（见本文第6页）。DPoS的有效实施很可能会导致区块生产者迅速投票否决任何审查尝试。

Another attack that block producers could launch would be an attempt to change the protocol parameters. This could mean many things—changing the constitution, increasing their block rewards, forking out certain stakeholders, and many other options. Luckily, DPoS is designed in such a way that these attacks are not possible without implicit voter approval. In EOS, for example, changes to

system parameters have time delays before they are actually incorporated. Changes to the constitution require approval by 17/21 block producers, and they must maintain that approval for 30 consecutive days before the changes take place. If users disagree with the changes, they can vote out those block producers during that time and replace them with producers that don't support the changes. More information on EOS protocol updates can be found here. Ultimately, changes to the system must be endorsed by token holders through, at the very least, passive approval. Parameter changes cannot be enacted without a time delay during which they could be negated. This severely limits the damage that malicious block producers could cause.

区块生产者可能发起的另一种攻击是试图改变协议参数。这可能意味着很多事情——修改宪法，增加他们的区块奖励，为某些利益相关者提供资金，以及许多其他选项。幸运的是，DPoS在设计时就已经确保，如果没有选民的默许，这些攻击是不可能的。例如，在EOS中，对系统参数的更改在实际合并之前存在时间延迟。对宪法的修改需要在21个区块生产者中，得到17个的批准，而且他们必须在修改发生前连续30天保持该批准不变。如果用户不同意这些更改，他们可以在这段时间内投票淘汰这些区块生产者，并选出不支持更改的生产者取代他们。可以在这里找到更多有关EOS协议更新的信息。最终，对系统的更改必须得到代币持有者的认可，至少要通过被动批准。参数更改不能在没有时间延迟的情况下执行，而在此期间可以对其进行否决。这严重限制了恶意区块生产者可能造成的破坏。

Finally, block producers may be able to coordinate double spend attacks by majority collusion, though these situations are highly unlikely in practice. DPoS uses a concept of "last irreversible block" that provides finality once more than two thirds of block producers have built on the same chain. Users who need strong guarantees of finality for their transactions can wait for this confirmation.

最后，区块生产商可能能够通过大多数人合谋来协调双花攻击，尽管在实践中这些情况极不可能发生。DPO使用了"最后一个不可逆块"的概念，指的是一旦超过三分之二的区块生产者在同一个链上构建，它就提供了最终性。需要对其事务的最终性获得强有力保证的用户可以等待此确认。

DISTRIBUTED DENIAL-OF-SERVICE ATTACK (DDOS)

分布式拒绝服务攻击(DDOS)

In most DPoS implementations, block producers are known entities. In some implementations they may even be highly public individuals or organizations whose whereabouts and IP addresses are known. Because the order of block production is fixed during each round, attackers could identify who will be producing blocks at a given time and launch DDoS attacks on the producers.

在大多数DPoS实现中，区块生产者是已知的实体。在某些实现中，它们甚至可能是高度公开的个人或组织，其位置和IP地址是已知的。由于每轮出块顺序固定，攻击者可以确定谁将在给定的时间生成块，并对出块人发起DDoS攻击。

Such an attack would be difficult to pull off in practice. While an attacker may be able to target a single block producer, targeting several different block producers simultaneously would be unlikely. The network may suffer temporary delays, depending on how many producers the attacker was able to target, but it seems near impossible that an attacker could simultaneously DDoS the majority of the nodes. Further, block producers can campaign on their ability to resist DDoS attacks by using backup servers in other locations and a variety of other means. Finally, if a single block producer (or even a few) were consistently failing to produce blocks because of such an attack, they could be voted out and replaced by backup producers within a single round.

这样的攻击在实践中很难成功。虽然攻击者可能只针对一个区块生产者，但是同时针对几个不同的区块生产者是不太可能的。网络可能会遭受暂时的延迟，这取决于攻击者能够针对多少生产者，但是攻击者几乎不可能同时对大多数节点进行DDoS。此外，区块生产者可以通过在其他位置使用备份服务器和各种其他方法来宣传他们抵抗DDoS攻击的能力。最后，如果一个区块生产者（或者甚至几个）由于这样的攻击而始终不能生成块，那么它们可以在一轮投票中被淘汰，由候选生产者取而代之。

Conclusion

结论

DPoS is an elegant, robust, and most importantly, practical and proven solution to the blockchain scalability problem. It also offers solutions for blockchain governance, funding, the nothing at stake problem, and more.

针对区块链可伸缩性的问题，DPoS是一个优雅、稳健——最重要的是实用且经过验证的解决方案。它还为区块链治理、资金、无利害关系问题等提供了解决方案。

Blockchains based on DPoS architecture achieve high scalability by compromising on the “decentralization of block production” in the context of the scalability trilemma.

基于DPoS架构的区块链在可伸缩性三难困境的背景下，通过牺牲“区块生产的去中心化”来实现高可伸缩性。

Of the three properties comprising the trilemma, two are ends in and of themselves: scalability and safety. These are essential features of any blockchain. Decentralization, on the other hand, is a means to an end. Therefore, it makes sense to compromise on decentralization of block production if the desired ends can still be achieved. The goals of decentralization are censorship resistance, openness, and no single point of failure. We believe that DPoS still achieves all of these goals.

在构成三难困境的三个属性中，有两个属性本身就是目的：可伸缩性和安全性。这些是任何区块链的基本特性。另一方面，去中心化是达成上述目的的一种手段。因此，如果仍然希望达成预期的目标，就有必要在区块生产的去中心化方面作出妥协。去中心化的目标是抵制审查、开放和没有单一的失败点。我们相信DPoS仍然实现了所有这些目标。

Some but not all aspects of decentralization can be quantified; the number of validators is simply one aspect. There are other factors outside of the number of individual entities that must be considered, and DPoS token voters will have to vote to ensure that the system retains all of the desired effects of decentralization.

去中心化的某些方面是可以量化的（但不是所有方面）；验证者的数量只是其中一个方面。除个别实体的数量外，还必须考虑其他因素，而DPoS的代币选民必须投票，以确保该制度保留去中心化的所有预期效果。

There are some drawbacks to DPoS—mostly that it places more requirements on token holders to monitor the health of the network, watch for bad behavior, and decide upon what makes for sufficient decentralization. In exchange, however, DPoS gives huge performance enhancements and has other very advantageous attributes. We believe that DPoS has a very compelling set of features and tradeoffs that make it a great solution for many types of decentralized applications.

DPoS也有一些缺点，主要是它对代币持有者提出了更多的要求，以监控网络的健康状况、监视不良行为，并决定如何进行足够的去中心化。然而，作为交换，DPoS提供了巨大的性能增强，并具有其他非常有利的属性。我们相信DPoS有一组非常吸引人的特性和权衡，这使得它成为许多去中心化应用程序类型的优秀解决方案。

DPoS recognizes that decentralization has a cost—both economically and in terms of performance—and it opts for semi-centralization in exchange for scalability. If DPoS systems can still offer the requisite levels of censorship resistance, permissionless-ness, and trustlessness, then DPoS is better for a huge range of decentralized applications. For certain use cases—absolutely censorship-resistant digital gold, peer-to-peer digital money, etc., a tradeoff in favor of

decentralization at the expense of performance may make sense. For the vast majority of applications, scalability is far more pragmatic.

DPoS认识到为了实现去中心化，在经济上和性能上都要付出代价，于是它选择了半中心化以获得可伸缩性。如果DPoS系统仍然能够提供去中心化数据库所需要的抗审查性、无许可性和去信任性的必要级别，那么DPoS更适合广泛的去中心化应用程序。对于某些用例（完全抗审查的数字黄金、点对点数字货币等）来说，以性能为代价而支持去中心化的折衷可能是有意义的。对于绝大多数应用程序，可伸缩性要实用得多。

DPoS is not the only consensus algorithm that could succeed at scale. It may not be the right fit for every type of decentralized application, but it is highly likely to have a place in the world. Even if we assume the worst—that 21 known entities control the database, or that a concerted international government effort could result in censorship—DPoS still provides a set of features that may be highly desirable for certain use cases. Businesses want a neutral database that offers scalability, low latency, and maybe even desire some notion of government endorsement. The size of this market could be measured in the trillions.

DPoS并不是唯一能够在大规模应用中取得成功的一致算法。它可能并不适合所有类型的去中心化应用程序，但是它很可能获得一席之地。即使我们假设最坏的情况是21个已知实体控制数据库，或者一个协调一致的国际间政府行为可能导致审查——DPoS仍然提供了一组对某些用例非常有用的特性。企业希望有一个中立的数据库，提供可伸缩性、低延迟，甚至可能希望得到政府的某种认可。这个市场的规模可以用数万亿美元来衡量。

Still, we estimate that DPoS, in practice, will be far more resilient than described above. We look forward to learning from the incredible social experiment that is DPoS.

尽管如此，我们估计DPoS在实践中会比上面描述的更有弹性。我们期待着从DPoS这个令人难以置信的社会实验中学习。

Thanks to Jesse Walden, Denis Nazarov, Trent McConaghy, Sam Kazemian, Malcolm Mason Rodriguez, Thomas Cox, Ian Grigg, and others for their input and feedback.

感谢Jesse Walden、Denis Nazarov、Trent McConaghy、Sam Kazemian、Malcolm Mason Rodriguez、Thomas Cox、Ian Grigg和其他各位的意见和反馈。