尔格平台项目概况

(“The Ergo Platform Project Overview”)

尔格开发者团队

2019 年 3 月 20 日

1.1 版本

摘要

这篇文章的内容包括了尔格（“Ergo”）平台的主要理念，并且高度概括了该平台的主要特征。有关该平台的更多细节在白皮书中有详述，也可以在其他有关平台介绍的专业文献及文章中获取。

1 愿景

经过几年的研究和原型实践后，尔格平台于 2017 年开始发展壮大。尽管加密货币一直被夸大宣传，但该技术本身已经接近其初始阶段。为了追求高利润和高声望，开发人员宣称区块链 2.0,3.0 等的应用，主要针对加密货币的主要优势，即“去中心化”，团队只是承诺将在未来的某个时间内将实现去中心化。

相比之下，尔格平台的理念是去执行随时可用的想法，从而使网络实现真正的去中心化。尔格可以被称为“区块链 1.1”的实践-这是区块链技术的重大更新，而不是革命性的突破性变化。尔格的目标是作为对需要区块链去中心化应用真正有用的平台，并且能够长存，从而使其成为一个强大的价值存储。以下各节总结了实现这一目标的技术层面和经济层面的解决方案。

2 共识机制

尔格的共识协议：奥托吕科斯（“Autolykos”），是基于众所周知的工作量证明(“PoW”)一致性算法。选择 PoW 有几个原因，其中包括 PoW 协议已被广泛研究，具有高安全性保证，并且对轻客户端友好。

然而，现有的 PoW 协议有几个周知的缺点：配备 ASIC 的矿工生产的区块比 CPU 或配备 GPU 的矿工生产的区块要快几个数量级，并且，它们会在采矿池中联合起来，结果就是仅有几个矿、池操作员控制了整个网络，有时候还是以一种不透明的方式。这可能代表网络的单点故障，并对长期生存能力构成严重威胁。

减少 ASIC 支配作用的一般方法是使用内存困难计算。奥托吕科斯是基于 k-和问题，类似于已知的内存困难的 Equihash 的 PoW [1]。另外，奥托吕科斯是 Schnorr 签名的变体，因此如果不访问私钥就无法进行挖掘，从而使基础拼图不可外包。

尔格平台的这两个属性阻止了围绕池运营商和 ASIC 制造商网络的中心化，并让尔格回到原来比特币白皮书中一个 CPU 一个投票权的理念[10]。

3 客户端

没有受信第三方的帮助，几乎不可能使用现有的加密货币。以不受信的方式收取即使是非常少量的币，客户端也必须下载并处理数十亿字节的数据以与网络同步，这即使在高端硬件上也可能需要数周时间，更不用说移动设备了。因此，不出意外，大多数用户更喜欢需要信任的解决方案来用于钱包，交换机，区块浏览器等。

尔格的设计在去中心化理念下，最大程度地方便用户使用，PoW 的一个重要特性是它可以在不用下载完整链的情况下验证所完成的工作。尔格大区块头支持工作量证明的非交互式工作量证明的证明（”NiPoPoW”）[7]，轻量客户端可以通过下载少于 1 兆字节的数据与网络同步。此外，尔格是使用认证状态[11]，对于任何交易，客户端都可以下载其正确性的证明。因此，

无论区块链大小如何，具有智能手机的普通用户都可以加入网络，并开始使用具有与完整节点相同安全保证的尔格。

4 生存性

如果尔格或任何其他加密货币要作为一个价值的存储，那么长期生存性和用户对平台长期生存性的信心就是至关重要的。

尔格更倾向于提供经过充分测试的解决方案，以实现长期生存。如果某些问题还没有经充分测试的解决方案，我们会进行自己的研究，而且尔格开发团队的同行评审文章数量已经很多了：[11, 9, 4, 3, 5, 6]。

为了生存，网络应该适应变化的环境而不受受信方（例如“核心开发者”团队）的干预。尔格的链上矿工投票协议允许逐步改变大量参数，这些参数包括：

- 最大区块大小
- 区块的最大累计计算成本
- 协议的计算成本
- 存储费变量(详情请见第五部分)

更根本的变化在于，尔格将遵循软分叉方法：如果绝大多数网络接受新功能，则会激活它，同时，不升级的旧节点将继续正常运行并且跳过此功能验证。

5 经济

为了获得生存性，尔格除了提供技术改进之外还提供经济改进，其中最重要的是滞期特性，它对尔格的稳定性起着重要作用：如果交易输出尔格币 (“Erg”) 保持 4 年而没有被动过，矿工可以对该状态下保留的每个字节收取少量费用。如果发币低于要支付的费用，那么所交易输出将从状态中被删除。

因此，滞期特性类似于常规的云存储服务，然而，它对于加密货币来说是全新的，并且具有几个重要的影响。首先，与比特币和其他 PoW 币在发行后就可能变得不稳定不同的是，尔格挖矿将始终保持稳定[2]。其次，状态规模增长变得可控和可预测，降低了对尔格矿工的硬件需求。第三，通过从过期的箱子中收取存储费用，矿工将币重新循环，防止由于丢失密钥而导致的循环供应的稳定减少[8]。

最后，它可以很快停止发行。尔格发行将持续 8 年，在最初的 2 年内，每个区块将发出 75 个尔格币（尔格币是平台的原生币），每隔 2 分钟一次，之后每 3 个月区块奖励将减少 3 个币（见图 1）。为了助力尔格的发展，在最初的 2 年半期间，超过 67.5 的区块奖励的部分将给到金库而不是矿工。尔格发行将从零开始，为了证明没有预先开采，我们会像中本聪（“Satoshi”）一样，运用一些新闻头条，同时，我们也会用比特币和以太坊的最新区块 ID。

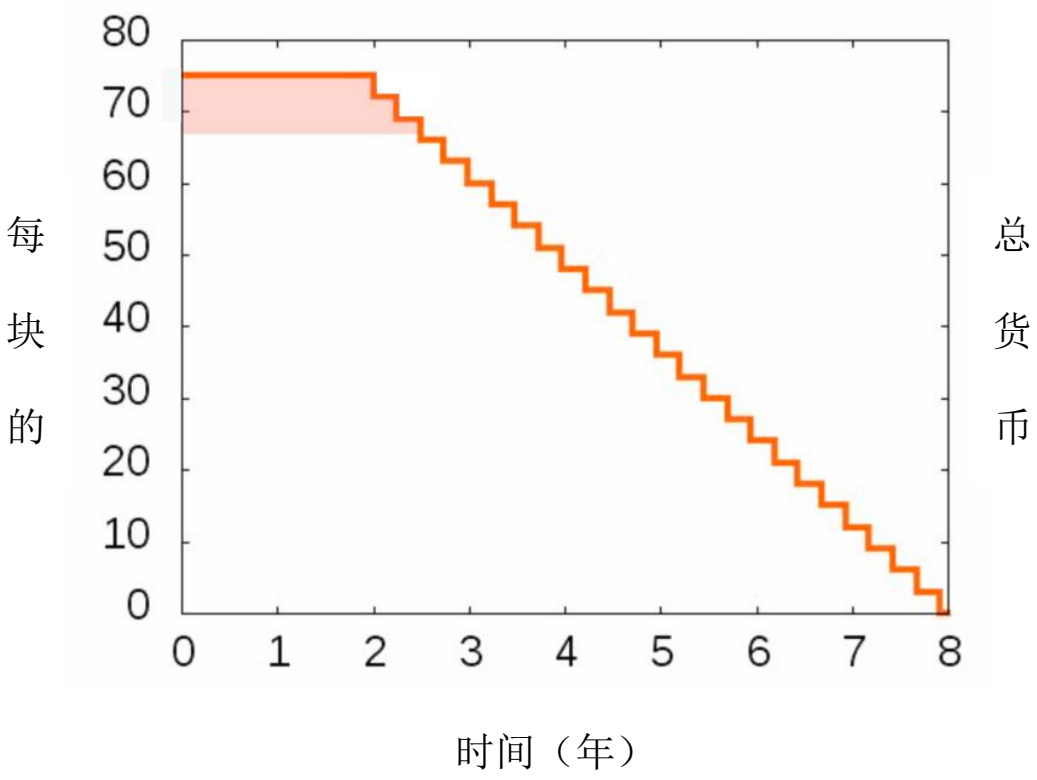

图 1：尔格的发布曲线

6 适用性

为了生存，区块链必须具有用户群。由于轻客户端，去中心化应用和链下协议可以真正去中心化的方式实现，但是，它们还需要一个有用且安全的智能合约语言。尔格智能合约是基于比特币未花费的交易输出（“UTXO”）模型，其中每个输出都受到某些脚本的保护。如果脚本语言足够丰富，它就可以编写图灵完备合同[3]，同时避免像以太坊中的瓦斯一样暂停程序的临时解决方案。虽然尔格脚本具有比比特币脚本更多的多功能性，但是尔格脚本只包含允许在运算前估计脚本复杂性的操作，这可以防止各种分散式阻断服务攻击（DDoS）。同时，这个指令集足以轻松编写任何可能的程序 - 尔格脚本（“ErgoScript”）被证明是图灵完备的[3]。尔格脚本的加密部分是基于 Sigma 协议的，自然也支持阈值 m-of-n 签名，环签名等。

7 结语

在这份精炼介绍尔格平台的文章中，希望我们已经突出了这个新平台最显著的特征、尔格平台开发团队的理念、以及为什么多样化的客户群、矿工、交易员及加密货币的长期投资者会对这个平台产生浓厚兴趣。

参考文献

[1] A. Biryukov and D. Khovratovich. Equihash: Asymmetric proof-of-work-based on the generalized birthday problem. *Ledger*, 2:1-30, 2017.

[2] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan. On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 154-167. ACM, 2016.

[3] A. Chepurnoy, V. Kharin, and D. Meshkov. Self-reproducing coins as universal turing machine. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 57-64. Springer, 2018.

[4] A. Chepurnoy, V. Kharin, and D. Meshkov. A systematic approach to cryptocurrency fees. *IACR Cryptology ePrint Archive*, 2018:78, 2018.

[5] A. Chepurnoy and M. Rathee. Checking laws of the blockchain with property-based testing. In *Blockchain Oriented Software Engineering (IW- BOSE), 2018 International Workshop on*, pages 40-47. IEEE, 2018.

[6] T. Duong, A. Chepurnoy, and H.-S. Zhou. Multi-mode cryptocurrency systems. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, pages 35-46. ACM, 2018.

[7] A. Kiayias, A. Miller, and D. Zindros. Non-interactive proofs of proof-of-work. Technical report, Cryptology ePrint Archive, Report 2017/963, 2017. Accessed: 2017-10-03, 2017.

[8] E. Krause. A fifth of all bitcoin is missing. these crypto hunters can help. 2018.

[9] D. Meshkov, A. Chepurnoy, and M. Jansen. Short paper: Revisiting difficulty control for blockchain systems. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 429-436. Springer, 2017.

[10] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[11] L. Reyzin, D. Meshkov, A. Chepurnoy, and S. Ivanov. Improving authenticated dynamic dictionaries, with applications to cryptocurrencies. In *Inter- national Conference on Financial Cryptography and Data Security*, pages 376-392. Springer, 2017.