Algorand：解决区块链“三元悖论”的分布式账本技术

时长：1 小时

去中心化、安全和高扩展性是区块链平台的三个主要目标。根据目前广为流行的的“区块链三元悖论”，任何技术解决方案最多只能兼顾其中的两项。幸运的是，我们可以证明这种说法是不准确的。

在这次演讲中，我们将向听众讲解 Algorand 的技术是如何解决这个所谓的三元悖论的。基于创新的隐秘自选技术，Algorand 采用开放参与的、纯粹基于权益证明的共识机制，能够在高度异步的网络环境中高效地工作。与之前基于工作量证明的分布式账本技术不同，Algorand 不需要“矿工”，所需要的计算量几乎可以忽略不计。此外，“软分叉”发生的概率也是几乎可以忽略不计的：Algorand 在交易进入账本的同时，就能够立即确保该交易的最终性。

凭借其独特的共识协议，Algorand 能够以非常平滑的方式持续演进，不需要“硬分叉”就可以满足区块链社区未来的需要。

Algorand:The Truly Distributed Ledger Solving The “Blockchain Trilemma”

Time：1h

Security, scalability, and decentralization are the three main goals of a blockchain platform. However, according to popular intuition, the famous “blockchain trilemma”, you could enjoy at most two of them. Fortunately, we prove this intuition not accurate.

In this talk, we will show how Algorand’s technology solves the trilemma. Based on our novel technique of cryptographic self-selection, Algorand is permissionless, is pure proof-of-stake, and efficiently works in a highly asynchronous environment. Unlike prior implementations of distributed ledgers based on proof-of-work, Algorand dispenses with “miners” and requires only a negligible amount of computation. Moreover, `”soft forks” occur only with negligible probability: that is, Algorand guarantees the finality of a transaction the moment the transaction enters the ledger.

Empowered by its unique consensus protocol, Algorand is able to evolve frictionlessly so as to meet the future needs of the community, without “hard forks”.