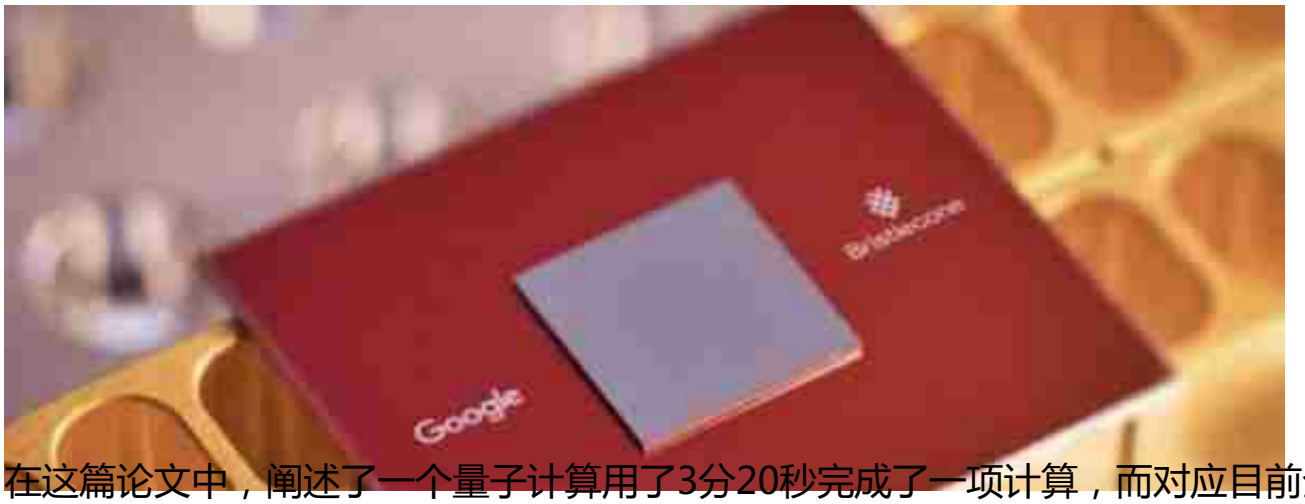
创立DigiCash的创始技术团队

在DigiCash发展得红红火火时，不少投资机构都寻求与DigiCash合作和投资的机会，比如美国的马克吐温银行、瑞士信贷、科技巨头网景公司等。甚至Chaum因为微软报价过低拒绝了与微软合作的机会。



在这篇论文中，阐述了一个量子计算用了3分20秒完成了一项计算，而对应目前全球最强大的超级计算机Summit，这项任务需要计算一万年。

这本来只是一个计算机行业更该关心的话题，但很多加密货币的爱好者开始意识到：

如果量子计算机的计算能力能够像谷歌论文中描述的那么快，那么加密货币赖以存活的私钥加密体制是不是就会轻易被量子计算机所攻破？

事实的确如此。只要通用型量子计算机确实能够搭建起来，现有的加密方案将被量子计算短时间攻破，那么比特币等加密货币将变得一文不值。

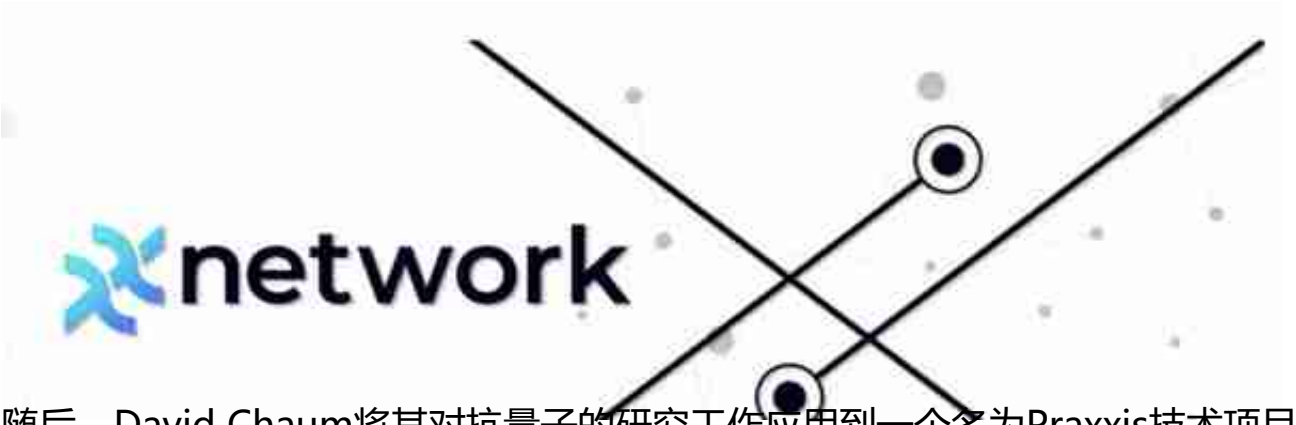
所幸的是，目前《量子霸权》论文描述的量子计算机仍然只能完成特定任务，还不能做通用性运算。所以，目前仍然没有威胁。

你我总只关心现在，但加密专家已然关心未来技术。

所谓道高一尺魔高一丈。假以时日，如果通用型量子计算机能够面世，唯一能让区块链技术继续长久存活下去的方案，就是设计能够抵御量子计算机攻击的机制。

这就是David Chaum现在非常关心的、也在专注解决的问题。

xx网络集毕生之大成



随后，David Chaum将其对抗量子的研究工作应用到一个名为Praxxis技术项目上。Praxxis协议使用基于大随机数的抗量子签名，这将使得区块链能够有能防御量子计算机攻击加密签名的方案。目前加密签名大多主要基于SHA256、ECDSA（椭圆曲线数字签名算法）等，有可能在量子计算机达到一定性能就会被攻破。大随机数算法则基于无法预测的随机数算法，能够真正防御量子计算机带来的破解危机。与此同时，基于高效量子安全的紧凑背书签名情况下，节点才能够在安全的环境下达成有效的共识。目前xx网络基于Praxxis提供的签名与共识技术，提出了xx共识、它引入了几个关键的突破，包括支持快速、单轮共识的背书采样、抵御网络攻击的承诺随机性，以及提供高效量子安全的紧凑背书签名。

有了Elixxir能够确保用户元数据得到足够强大的隐私保护后，David Chaum则为这些数据提供了抗量子的Praxxis技术用来验证、达成共识、上链的流程，从而构成了

xx区块链网络。这样的网络，是David Chaum倾注毕生所学所构造的，也站在了这个时代的最前沿。

目前基于xx网络发行的xx币，主要为维护xx网络的节点运营商、开发者以及使用者提供激励，使得xx网络能够在分布式社区的运营下健康发展。目前xx币也在sale.xx-coin.io进行提供售卖活动，为社区爱好者提供投资机会。

也许，我们仍然满足于目前区块链足够安全的架构，更希望看到的是新功能的出现。但大师的眼光总是看得比我们更远。这一次，他回归到区块链最核心的地方——用户隐私和性能安全。他希望在量子危机还没出现之前，就能够设计出抵抗、防御这个攻击的区块链网络，确保区块链网络在未来世界不会被轻易击垮。这样的深谋远虑，使得David Chaum为这个行业带来了能持续走向未来的xx网络。希望这个xx网络也会为行业带来新的设计灵感，一同走向更远的未来。

注：本文仅为个人投资思考，不作为投资建议。市场有风险，投资需谨慎。