申万宏源研究 SWS RESEARCH

2016 年 06 月 30 日

量子计算来了，区块链还安全吗？

——量子技术应用专题系列报告之一

看好

相关研究

"中国电信（728：HK）-发展战略" 2016 年 1 月 18 日

"2015 下半年通信行业投资策略" 2015 年 7 月 24 日

证券分析师
何俊锋 A0230515110002
hejf@swsresearch.com
顾海波 A0230515090007
guhb@swsresearch.com
联系人
何俊锋
(8621)23297818×7422
hejf@swsresearch.com

本期投资提示：

- **量子计算是对传统计算的革命，当前已经从实验室初步走向商业化应用。**量子计算与传统计算的最大区别在于量子计算采用量子比特（qubit）作为最小的运算单元。传统计算机采用二进制比特，即“0”和“1”，而量子比特可同时存在两种可能的状态，这种新状态被称作“叠加态”。因此，对量子比特的操作可以让许多计算工作并行进行。目前计算机领域所谓的并行计算只是从效果上来看形成问题的并行解决，实际从 CPU 的运行来看，CPU 依旧是一次只能处理一个计算。量子计算将会是真正意义上的并行计算，计算速度大大提升，对 1000 位的大数进行因数分解只需要几秒，而传统的计算机则需要 1025 年。目前量子计算已经从实验室初步走向商业化应用。量子计算已成为 IBM、微软和谷歌等信息产业巨头竞相逐鹿的战场。由于量子位在普通环境下难以制备，并且多量子位之间的协调控制较难，因此目前的量子计算机量子位数较少，导致量子计算机只能处理特定的问题，通用性差。此外量子计算机的制造维护成本特别高。量子计算机的成熟和大规模应用还需要突破很多技术瓶颈。

- **量子计算对现有通信安全系统形成挑战。**非对称加密基于数学难题——大数的因子分解，非对称加密不能破解的理论依据是计算机不能在合理的时间内计算出密钥的值，使得破解成本高于被破解的信息所带来的价值。按现在的算法，破解 1024 位密钥的非对称加密可能需要超级计算机运算数十年至数千年，因而从当前的计算水平来看，非对称加密方式有较高的安全性，也是当前应用范围最广泛的加密方式。量子计算从理论上说可以实现任意大整数的快速分解，这导致非对称加密算法不能破解的理论依据不再成立，量子计算对现有通信安全系统构成巨大威胁。

- **量子计算威胁区块链安全性。**区块链技术采用非对称加密算法保障数据库的可信赖性，使用户在互联网无实名制的背景下防止诈骗。每一个区块的数据中，包含了所有交易的记录以及账户身份信息，交易信息在区块链中是公开的，但是账户身份信息是通过非对称加密算法加密的。区块链是去中心化的，所有节点都保存有相同的交易数据，对单个节点数据的篡改会导致该节点被其他节点排斥，这样的攻击是无法成功的。但是，如果通过密码破解看到某个人的用户信息（得到其私钥），从而可以以此人的名义进行操作，这种情况对数据的安全和个人的隐私造成了威胁。

- **量子计算时代的通信安全解决方案：量子密码通信（技术成熟）和抗量子密码（尚在研发），看好量子密码通信行业发展前景。**量子密码的安全性由量子力学的物理原理保障，采用量子态作为信息载体，经由量子信道在合法的用户之间传送密钥。当没有监听者时信息传输的误码率在正常范围内，一旦信息通道中存在监听情况，误码率将高于阈值。现有通信加密算法存在量子计算等潜在威胁，未雨绸缪，大国纷纷大力研发量子密码通信，目前技术已经成熟，国内外都有试点网络建成，量子密码通信的发展领先于量子计算。量子密码通信在军事、金融等行业信息安全领域有着重大的应用价值。看好量子密码通信行业发展前景。除了量子密码通信，另一种加强信息安全性的技术方案就是抗量子计算密码设计。量子计算可以轻易地求解大数的因数分解，但是它并不是万能的。量子计算对非线性方程组求解、背包问题等难题并不擅长，针对量子计算难以求解的问题设计密码，成为了抗量子计算密码的设计思路。抗量子密码目前尚处在研发阶段。

申万宏源研究微信服务号

目录

图表目录

1.量子计算——革命性计算

1.1 量子计算是对传统计算的革命

量子计算与传统计算的最大区别在于量子计算采用量子比特（qubit）作为最小的运算单元。传统计算机采用二进制比特，即“0”和“1”，而量子比特可同时存在两种可能的状态，这种新状态被称作“叠加态”。因此，对量子比特的操作可以让许多计算工作并行进行。

表 1：量子计算与传统计算存在质的区别

项目	量子计算	传统计算
计算单元	量子比特	二进制比特
可计算量	2^N	2N
计算方式	并行计算	串行计算
计算结果	概率结果	确定结果

资料来源：申万宏源研究

根据量子计算的原理，量子计算具备三个特点：

- **并行计算、速度快**：目前计算机领域所谓的并行计算只是从效果上来看形成问题的并行解决，实际从 CPU 的运行来看，CPU 依旧是一次只能处理一个计算。而量子计算将会是真正意义上的并行计算。对 1000 位的大数进行因数分解只需要几秒，而传统的计算机则需要 1025 年。
- **微型化、集成化**：随着信息产业的高度发展，所有的电子器件都在朝着小型化和高集成化方向发展，而作为传统计算机物质基础的半导体芯片一直是这场运动的领先者，但由于晶体管和芯片受材料的限制，体积的减小存在极限，最终不能达到原子水平。而每个量子元件尺寸都在原子尺度，由它们构成的量子计算机，将会微型化与集成化。
- **能耗低**：计算产生的能耗主要是由于计算过程中不可逆操作引起的，传统计算机模型的计算操作是不可逆的。而对于量子计算由于叠加态的存在，计算过程可逆，因此只会产生较低的能量损耗。

1.2 量子计算初步走向商业化应用

量子计算的革命性引起了人们广泛的关注，也促使着量子计算技术从理论走向现实。随着第一台商用量子计算机的问世，量子计算从实验室走向了商业化应用。量子计算已成为 IBM、微软和谷歌等信息产业巨头竞相逐鹿的战场。IBM 推出一款 5 量子位的量子计算机平台，供用户进行算法或实验模拟；微软研究院借助量子计算，让半导体实现了衔接，使得半导体材料可以像超导一样运行；谷歌注重于量子计算机构架的研究，并提出了构建量子计算机的更简便方法，有可能大大提前新一代量子计算机问世的时间。然而我们也看

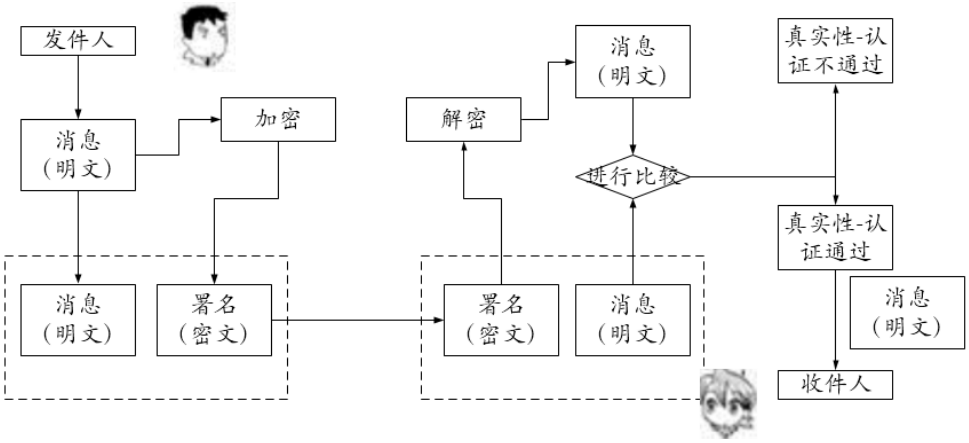
到，由于量子位在普通环境下难以制备，并且多量子位之间的协调控制较难，因此目前的量子计算机量子位数较少，导致量子计算机只能处理特定的问题，通用性差。此外量子计算机的制造维护成本特别高。量子计算机的成熟和大规模应用还需要突破很多技术瓶颈。

2.量子计算对现有加密算法形成挑战

2.1 量子计算强大的计算性能能对现有加密算法强力破解

非对称加密简单来说，它让我们在“加密”和“解密”的过程中分别使用两个密码，两个密码具有非对称的特点：（1）加密时的密码（在区块链中被称为“公钥”）是公开全网可见的，所有人都可以用自己的公钥来加密一段信息，保证信息的真实性；（2）解密时的密码（在区块链中被称为“私钥”）是只有信息拥有者才知道的，被加密过的信息只有拥有相应私钥的人才能够解密，保证信息的安全性。

图 1：非对称加密过程

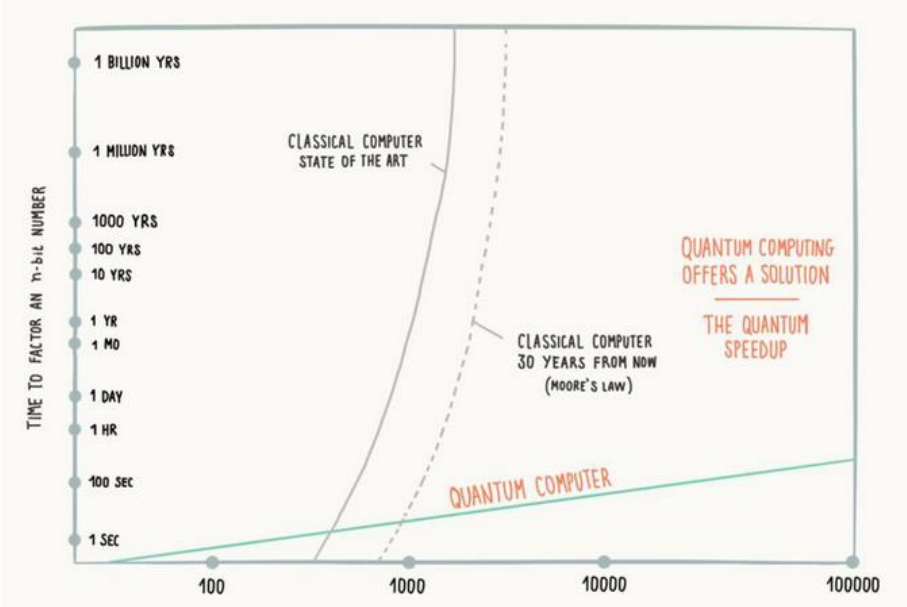


资料来源：申万宏源研究

非对称加密基于数学难题——大数的因子分解，非对称加密不能破解的理论依据是计算机不能在合理的时间内计算出密钥的值，使得破解成本高于被破解的信息所带来的价值。按照现在的算法，破解 1024 位密钥的非对称加密可能需要超级计算机运算数十年至数千年。因而从当前的计算水平来看，非对称加密方式有较高的安全性，也是当前应用范围最广泛的加密方式。

量子计算从理论上说可以实现任意大整数的快速分解，破解 1024 位密钥的非对称加密只需要几秒钟，这导致非对称加密算法不能破解的理论依据不再成立。

图 2：量子计算能实现对非对称加密的快速破解

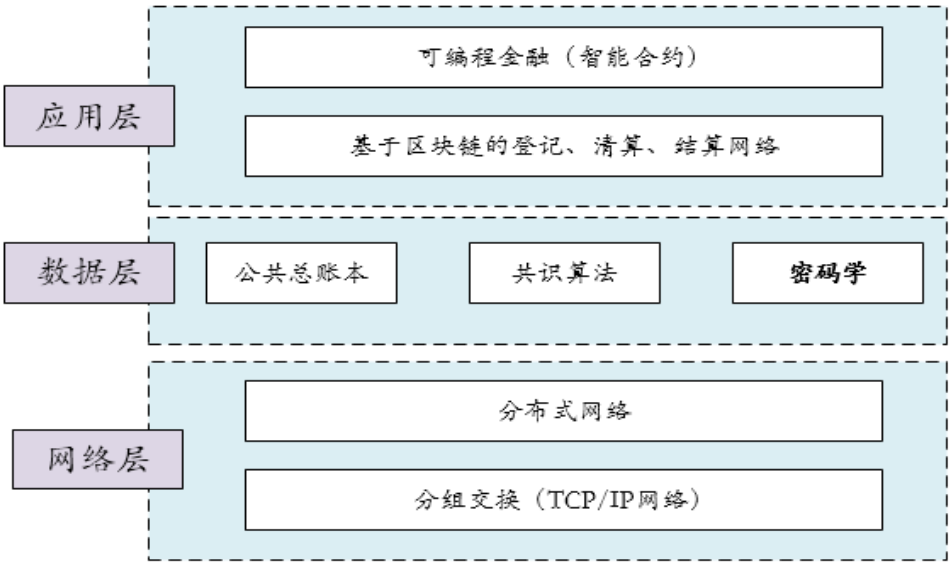


资料来源：申万宏源研究，钛媒体研究

2.2 量子计算对区块链安全性产生威胁

区块链技术是新发展起来的一种去中心化存储技术，本质上讲它是一种互联网协议，它建立了去中心化数据库结构，并保证数据的完整性以及安全性。在数据安全性方面，区块链技术采用非对称加密算法保障数据库的可信赖性，使用户在互联网无实名制的背景下防止诈骗。

图 3：密码技术是区块链协议的支柱性技术

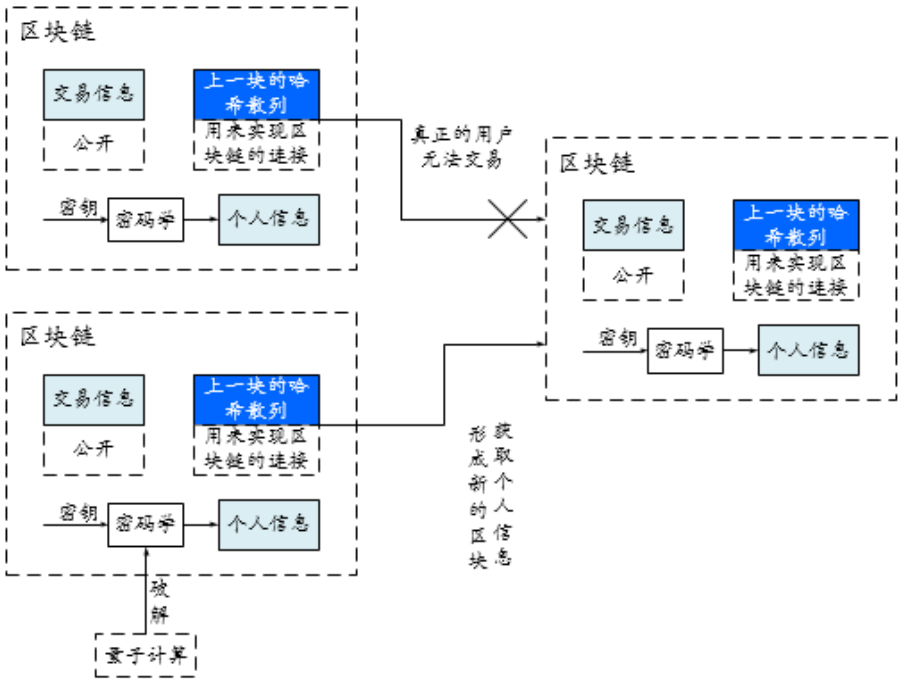


资料来源：申万宏源研究

每一个区块的数据中，包含了所有交易的记录以及账户身份信息，交易信息在区块链中是公开的，但是账户身份信息是通过非对称加密算法加密的。区块链是去中心化的，所

有节点都保存有相同的交易数据，对单个节点数据的篡改会导致该节点被其他节点排斥，这样的攻击是无法成功的。但是，如果通过密码破解看到某个人的用户信息（得到其私钥），从而可以以此人的名义进行操作，这种情况对数据的安全和个人的隐私造成了威胁。

图 4：量子计算通过密码破解威胁区块链安全



资料来源：申万宏源研究

区块链的数据安全性是基于非对称加密算法，而当前常用的 1024 位非对称加密通过量子计算在几秒内即可破译，这大大地威胁到了基于区块链技术的数据库可信任性，采用区块链技术的金融基础架构的安全性也因此受到影响。

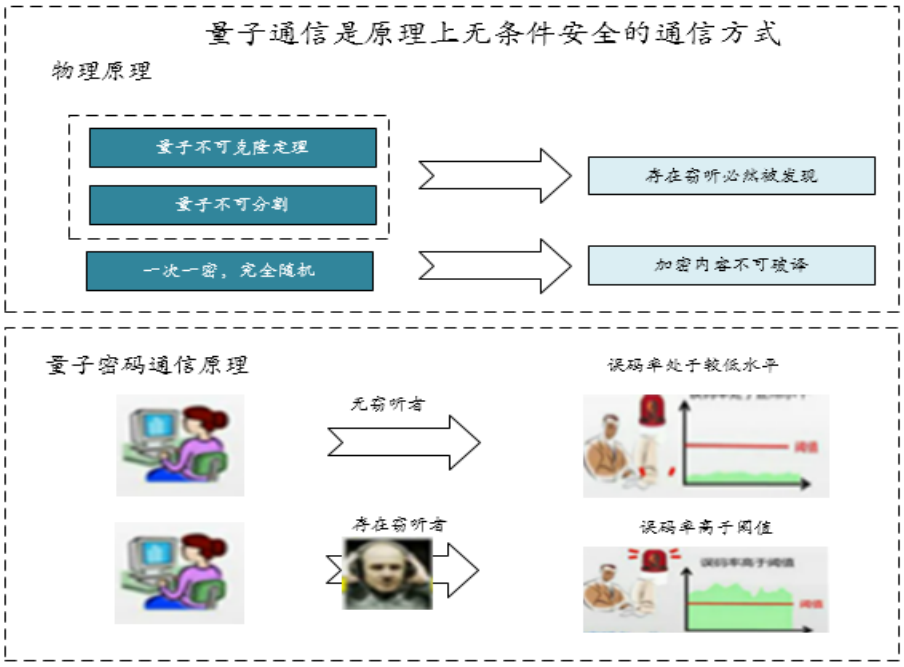
3.量子计算时代信息安全解决方案

解决量子计算所带来的信息安全问题的方法，主要是量子密码通信和抗量子计算密码。量子密码通信是在物理设备层面的加密方法，而抗量子计算密码是在软件算法层面的加密方法。

3.1 量子密码通信——技术成熟

量子密码术与传统的密码系统不同，它依赖于物理学作为安全模式的关键方面而不是数学。实质上，量子密码术是基于单个光子的应用和它们固有的量子属性开发的不可破解的密码系统，因为在不干扰系统的情况下无法测定该系统的量子状态。理论上其他微粒也可以用，只是光子具有所有需要的特性，它们的行为相对较好理解，同时又是最有前途的高带宽通讯介质光纤电缆的信息载体。

图 5：量子密码通信是原理上无条件安全的通信方式



资料来源：申万宏源研究

量子密码的安全性由量子力学的物理原理保障，采用量子态作为信息载体，经由量子通道在合法的用户之间传送密钥。当没有监听者时信息传输的误码率在正常范围内，一旦信息通道中存在监听情况，误码率将高于阈值。

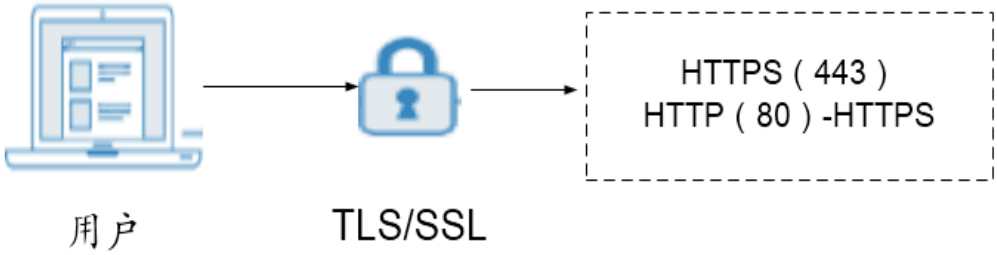
现有通信加密算法存在量子计算等潜在威胁，未雨绸缪，大国纷纷大力研发量子密码通信，目前国内外都有试点网络建成，量子密码通信的发展领先于量子计算。量子密码通信在军事、金融等行业信息安全领域有着重大的应用价值，看好其发展前景。

3.2 抗量子密码——尚在研发

除了量子密码通信，另一种加强通信安全的技术方案就是抗量子计算密码设计。量子计算可以轻易地求解大数的因数分解，但是它并不是万能的。量子计算对非线性方程组求解、背包问题等难题并不擅长，针对量子计算难以求解的问题设计密码，成为了抗量子计算密码的设计思路。

一个由微软、芯片制造商 NXP 和昆士兰科技大学组成的团队正在朝这个方向努力，该团队基于新的数学问题研发了一个用于抵御量子计算机的传输层安全协议(TLS)，网络银行等网站可以利用该 TLS 来加密网络数据，目前正在测试中。

图 6：抗量子计算 TLS 加密用于抵御量子计算机的攻击



资料来源：申万宏源研究，TLS 协议格式

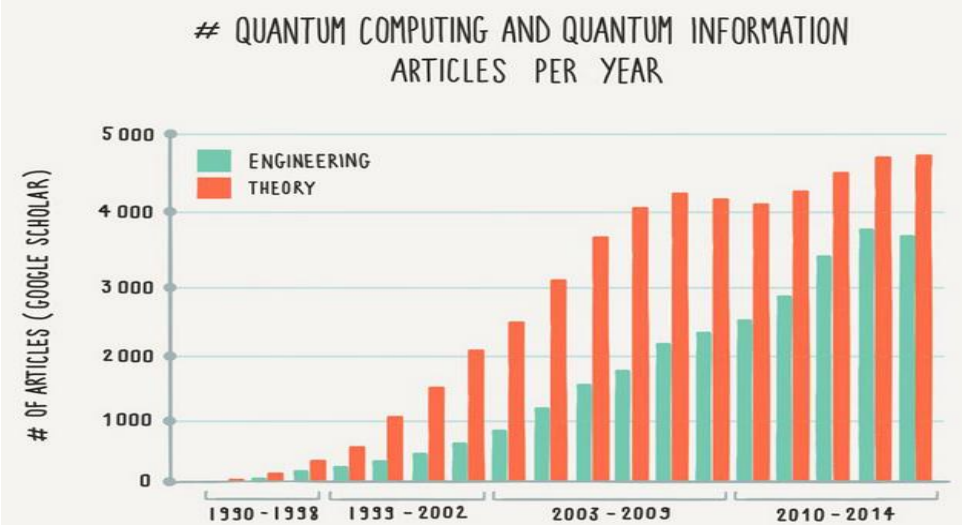
中国、韩国和日本等亚洲国家在 2016 年举办了第一届“亚洲抗量子密码论坛”，该论坛意在讨论量子计算对信息安全产生的影响以及新型密码的标准化工作的制定。会上研讨了与抗量子密码密切相关的量子计算复杂度的最新研究成果，亚洲相关各方共商了抗量子密码标准化工作的策略和方法。

附录量子计算发展现状

1. 量子计算逐渐从理论走向实践

经过几十年的研究与实践，量子计算不再仅仅停留在理论研究，而是不断的走向工程应用。从量子计算理论和工程论文发表的情况可以看出，这种转变并不是空穴来风。人们将重心转移到了量子计算机的研发上。

图 7：量子计算工程论文数量逐渐追上理论论文数量

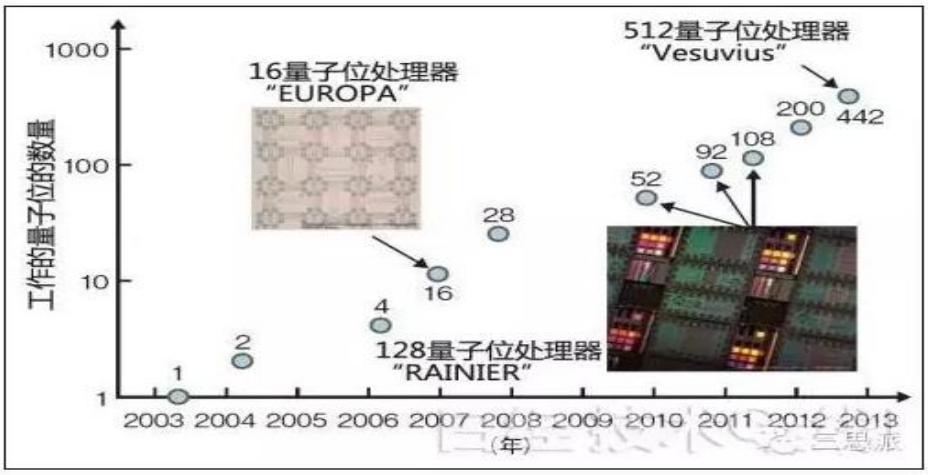


资料来源：申万宏源研究，钛媒体研究

2. D-wave——第一家商用量子计算机厂商

D-Wave Systems 成立于 1999 年，是一家来自加拿大、主打量子计算机研发的技术公司，并于 2011 年发布了全球第一款商用量子计算机“D-WaveOne”，它的处理器达到了 128 量子比特，一台售价高达 1000 万美元。2014 年，D-Wave 公司成功研制出 512 量子位的处理器。2015 年，D-Wave 2X 诞生，该计算机的每颗芯片上有超过 1000 个量子位。需要指出的是，D-Wave 利用量子隧道穿透效应实现计算，并没有利用量子门电路控制量子位来进行计算，因而对其是否称得上是真正的量子计算机存在争议。当前的量子计算机还只能处理经过优化的特定任务，通用任务方面还远不是传统硅处理器的对手。

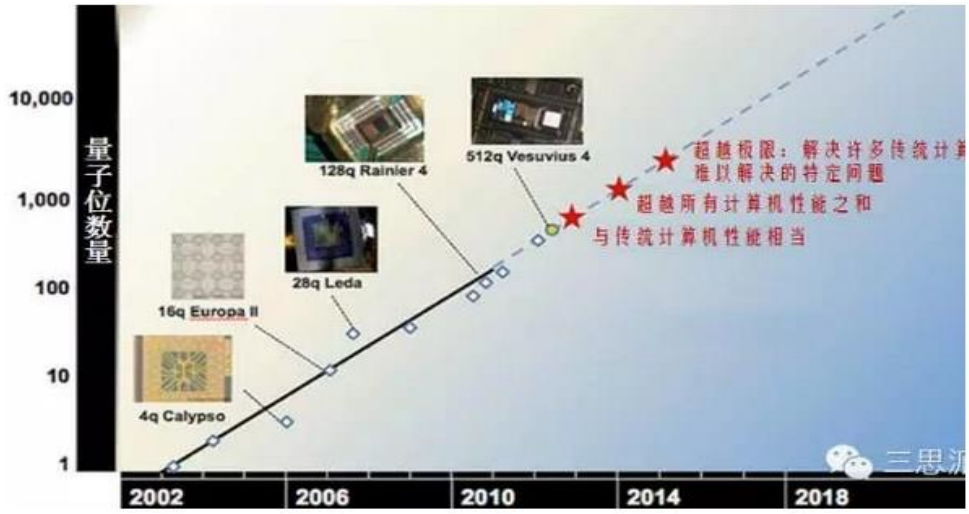
图 8：D-Wave 量子计算机量子位数量快速提升



资料来源：申万宏源研究，三思派研究

与摩尔定律相近，量子计算的计算速度也会随着量子位的增加而增加，但是是以指数的方式增长。以 D-Wave 公司创始人罗斯名字命名的罗斯定律认为：D-Wave 量子计算机的量子位数量每年翻番。每增加一个量子位，D-Wave 处理器的计算能力就会翻番，很快将接近释放计算潜能的边缘。根据这种趋势的发展，量子计算速度将打破摩尔定律极限。

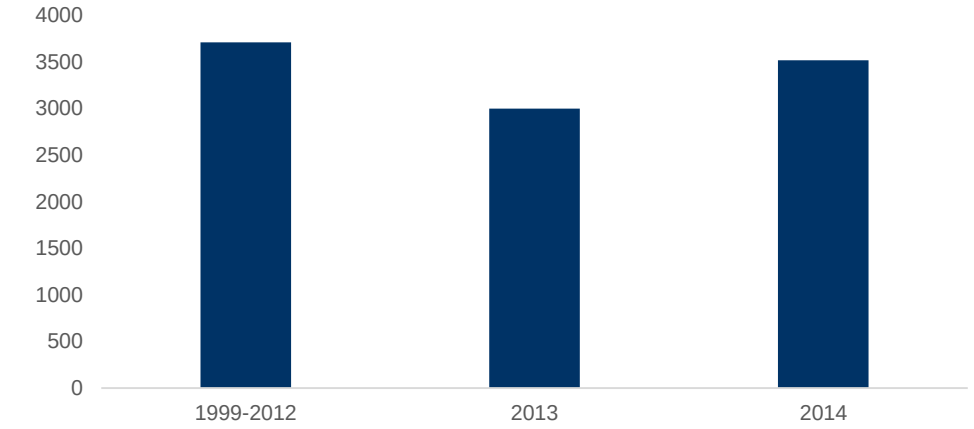
图 9：D-Wave 提出的罗斯定律将打破摩尔定律极限



资料来源：申万宏源研究，三思派研究

D-wave 公司在资本市场也持续保持着较高的被关注度，2014 年该公司进行了 2840 万美元的 F 轮融资，这笔资金由高盛、德丰杰及加拿大商业开发银行联合提供，该轮融资后其总融资额已达 1.02 亿美元。

图 10：D-Wave 累计融资 1.02 亿美元（单位：万美元）



资料来源：申万宏源研究

图 11：D-wave 投资者包含高盛等知名金融机构

资料来源：D-wave 官网

图 12：D-wave 客户包含 Google 等知名机构

资料来源：D-wave 官网

3.IT 巨头竞相布局量子计算

量子计算作为未来计算机发展的必然趋势，IBM、微软和谷歌等信息产业的巨头已经展开了明争暗斗，在量子计算领域提前布局。

表 2：IT 巨头竞相布局量子计算

公司	技术产品	研究方向
IBM	量子计算平台	推出一款 5 量子位的量子计算机平台，供用户进行算法或实验模拟。虽然该电脑目前仍不能实现通用，但用户可以通过对单个量子的操控学习和理解非二进制码计算系统的工作原理。
微软研究院	半导体研究	借助量子计算，让半导体实现了衔接，使得半导体材料可以像超导一样运行。简单来说，半导体可以实现极高的时钟频率，但发热量却很低，甚至不发热。
	量子计算模拟器	量子模拟器是量子计算软件架构和工具套件，将会被用于将采用高级语言编写的量子算法转换为量子设备的机器指令。

谷歌	D-wave X2	已成功证明于 2013 年采购的一台 D-waveX2 能基于量子技术进行数学计算，这种量子算法可以以比传统过程快 1 亿倍的速度解决问题。并且最近谷歌发现了构建量子计算机的更简便方法，将大大提前新一代量子计算机问世的时间。

资料来源：申万宏源研究

表 3：通信行业重点公司估值表

证券代码	证券简称	投资评级	2016-06-29		PB	申万预测 EPS				PE		
			收盘价(元)	总市值（亿元）	2015A	2015A	2016E	2017E	2018E	2016E	2017E	2018E
300213	佳讯飞鸿	买入	28.38	74	7.80	0.32	0.46	0.69	0.75	56.90	41.75	35.73
002583	海能达	增持	11.92	183	8.10	0.16	0.27	0.38	0.51	45.15	31.07	23.40
600050	中国联通	中性	3.86	818	1.00	0.16	0.19	0.21	0.23	20.05	16.65	17.24
002467	二六三	-	14.85	119	5.40	0.07	0.21	0.27	0.28	76.91	62.93	52.15
300250	初灵信息	-	29.75	68	3.70	0.73	0.53	0.67	0.77	57.47	46.38	38.83
300292	吴通控股	-	33.26	106	4.40	0.52	0.96	1.35	1.75	37.86	26.74	18.96
300252	金信诺	-	33.45	137	15.30	0.34	0.61	0.95	1.31	49.19	33.63	23.74
600498	烽火通信	买入	24.54	257	3.70	0.63	0.85	1.08	1.36	27.48	21.88	17.27
002017	东信和平	中性	14.38	50	5.90	0.19	0.00	0.00	0.00	0.00	0.00	0.00
600522	中天科技	买入	24.37	254	2.40	0.95	1.21	1.54	1.89	20.24	15.67	12.38
300467	迅游科技	-	59.71	99	21.30	0.37	0.52	0.68	0.94	110.22	80.53	57.26
000851	高鸿股份	-	12.73	75	2.80	0.14	0.00	0.00	0.00	0.00	0.00	0.00
600775	南京熊猫	中性	14.93	136	4.10	0.16	0.16	0.18	0.19	79.67	70.57	73.81

资料来源：Wind 资讯、申万宏源研究

信息披露

证券分析师承诺

本报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并注册为证券分析师，以勤勉的职业态度、专业审慎的研究方法，使用合法合规的信息，独立、客观地出具本报告,并对本报告的内容和观点负责。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

与公司有关的信息披露

本公司隶属于申万宏源证券有限公司。本公司经中国证券监督管理委员会核准，取得证券投资咨询业务许可，资格证书编号为：ZX0065。本公司关联机构在法律许可情况下可能持有或交易本报告提到的投资标的，还可能为或争取为这些标的提供投资银行服务。本公司在知晓范围内依法合规地履行披露义务。客户可通过 compliance@swsresearch.com 索取有关披露资料或登录 www.swsresearch.com 信息披露栏目查询从业人员资质情况、静默期安排及其他有关的信息披露。

机构销售团队联系人

上海	陈陶	021-23297221	18930809221	chentao@swsresearch.com
北京	李丹	010-66500610	18930809610	lidan@swsresearch.com
深圳	胡洁云	021-23297247	13916685683	hujy@swsresearch.com
海外	张思然	021-23297213	13636343555	zhangsr@swsresearch.com
综合	朱芳	021-23297233	18930809233	zhufang@swsresearch.com

股票投资评级说明

证券的投资评级：

以报告日后的 6 个月内，证券相对于市场基准指数的涨跌幅为标准，定义如下：

买入（Buy） ：相对强于市场表现20%以上；

增持（Outperform） ：相对强于市场表现5%～20%；

中性（Neutral） ：相对市场表现在－5%～+5%之间波动；

减持（Underperform） ：相对弱于市场表现5%以下。

行业的投资评级：

以报告日后的6个月内，行业相对于市场基准指数的涨跌幅为标准，定义如下：

看好（Overweight） ：行业超越整体市场表现；

中性（Neutral） ：行业与整体市场表现基本持平；

看淡（Underweight） ：行业弱于整体市场表现。

我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。申银万国使用自己的行业分类体系，如果您对我们的行业分类有兴趣，可以向我们的销售员索取。

本报告采用的基准指数 ：沪深300指数

法律声明