彎曲評論

科技 · 人物 · 潮流

弯曲评论-硅谷科技月报(2013/12)

作者: 硅谷寒

科技一周~落花时节的比特币

2013/12/07

十二月，又是一年花落时，几人欢喜几人痴？这一周是2013年末月的开始，人们在为明年做准备的时候，也开始了对过往一年的总结与回顾，且看《时代周刊》对今年硬件产品的回顾，究竟“最佳硬件”的名誉，花落谁家呢？

本周，美国《时代周刊》总结了2013年的硬件产品（Gadget），并评出年度十佳[1]：

10. Nokia Lumia 1020；
9. LeapMotion Controller；
8. Nest Protect；
7. Amazon Kindle Fire HDX；
6. Microsoft Xbox One；
5. Apple iPhone 5s；
4. Pebble Smartwatch；
3. Oculus Rift 三维虚拟现实游戏设备；
2. Apple new iPads；
1. Google Chromecast。

Chromecast荣登榜首，颇为出人意料，竟然没有Nexus 5/7、PlayStation 4、Google Glass！毕竟与其它复杂的产品相比，Chromecast多少有点四两拨千斤的意味，难道是因为《时代周刊》的编辑更偏爱流媒体设备？值得注意的是，榜单上的Pebble和LeapMotion都是通过众筹平台Kickstarter募资的初创公司。有传言说，下一代的Chromecast将会开放SDK，让开发者们可以开发基于Chrome OS的Web-App游戏。如果此言成真，至少在我眼里，这应该算是Chrome OS一个里程碑式的进步。

- Amazon计划推出无人机送货服务（Prime Aire）。据CEO Bezos所言，无人机的软硬件技术已是万事俱备，只欠相关部门出台“低空飞行送货”的政策法规了。有趣的是，著名黑客Samy Kamkar在第二天就宣布推出“劫持战机”SkyJack，用以专门俘获Amazon的无人送货飞机。SkyJack造价约$400，基于开源硬件系统树莓派（Raspberry Pi）。且看，Amazon如何应对SkyJack？毫无疑问的是，无人机送货技术将会在黑客与反黑客的斗争中，向前迈进。
- 华为宣布放弃美国运营商设备业务。这一举措，实乃以退为进，既然美国政府重重设障，那么华为就先放弃之，等到一统美国以外的市场，成为其它各国运营商事实上的“标配”之后，拿下美国不过是举手之劳。这一出戏，似乎正在重复六十多年前某人所走的“农村包围城市”之路。
- 比特币（Bitcoin）成为本周最疯狂的虚拟货币，先是摸高到巅峰值$1240，之后急坠至$800，然后回调升高，再巨降而下。难道真地是：上帝欲使其灭亡，必先使其疯狂吗？在这个问题上，各人有各人的见解，至少赵东（车库咖啡CTO）敢于投入自己100万房产来玩比特币的勇气，是不得不令人敬佩的。

本期科技一周的科普焦点当然是火到爆表的“比特币”原理了。《弯曲评论》有意在未来做一个深度专栏来介绍比特币的全部密码学原理和分布式计算原理，此处，仅仅阐述一下比特币原理中涉及到的两个重要概念：比特币的帐户地址，比特币的加密交易。

就像每个人都用银行帐户来存钱一样，每个比特币交易者也需要比特币帐户来存储自己的比特币。每一个比特币帐户就是一个根据SHA256协议产生出来的160-bit的Hash地址，例如：1PC9aZC4hNX2rmmrt7uHTfYAS3hRbph4UN。这个地址里包含有一对“钥匙”（公钥和私钥）。

进行在线交易时，这对钥匙就起到至关重要的保护作用。举例来说，习大准备给老江发送2个比特币，整个交易过程如下：

- 1）老江把自己的Hash地址（比特币帐户）发给习大；
- 2）习大产生一个明文，包含了老江的Hash地址和比特币个数（2个）；
- 3）习大用自己的私钥对上面的明文进行加密，产生密文；
- 4）习大把生成的密文和自己的公钥，一同发送给老江；

- 5）老江用接收到的公钥把密文解密，看到明文里显示自己得到两个比特币，非常开心；
- 6）在老江接收到密文的同时，整个网络也接收到了密文，解密之后，网络知道“习大给了老江两个比特币”，并把这个信息产生成一个“区块”（Block），永久性地存储在网络里，用以记录该交易。至此，该交易结束。

在这个加解密的交易过程中，习大的帐户信息被保护起来（私钥并没有发送出去）。比如，胡哥虽然也看到了整个交易过程，但他无法盗取习大的私钥，因为从公钥破译出私钥是个极难极费时的过程，该过程一般都对应于一个NPC（NP-Complete）问题，就现有的非量子计算机的计算能力而言，破解一个NPC要数万年的时间。所以胡哥没有习大的私钥，也就无法伪造习大的签名来给自己发送比特币。

在上述过程的第6步里，整个网络在产生区块的时候，会耗费很大的计算量，这个计算量是由网络里所有的节点计算机共同承担，哪个节点首先产生出这个区块，就会被奖励一定数量的比特币，这也就是“挖矿”的由来：你的节点计算机性能越强，首先产生出区块的概率越大，你就越有可能“挖”出比特币来。看到这里，你是不是怦然心动？那就快去买一台“挖矿机”，一起来“挖矿”吧。

[1]. Time, Top 10 Gadgets, http://techland.time.com/2013/12/04/technology/slide/top-10-gadgets/ , Dec 2013.

图1. Google, http://www.google.com/intl/en/chrome/devices/chromecast/ .

图2. Amazon, http://www.amazon.com/b?node=8037720011 .

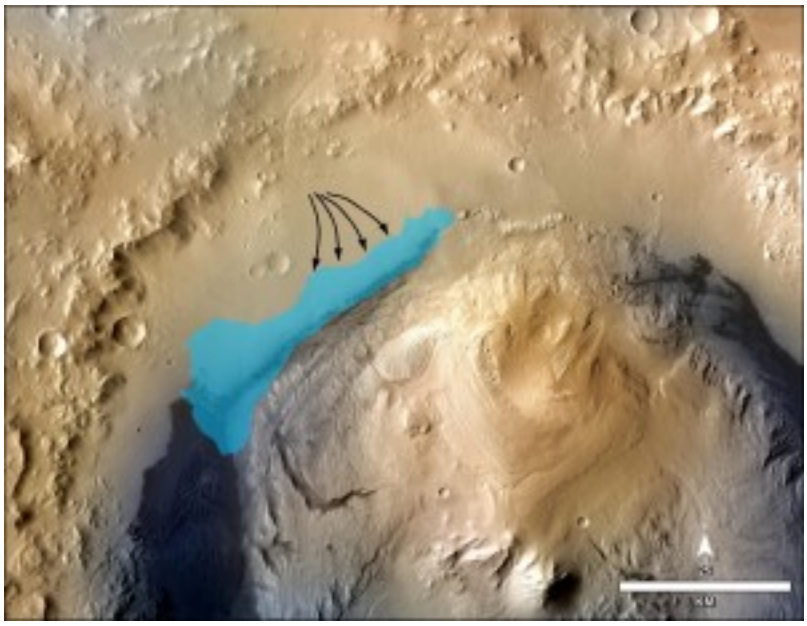
图3. Techinasia, Is bitcoin really illegal in Thailand, http://www.techinasia.com/bitcoin-illegal-thailand/ , Aug 2013.

科技一周~天才与人类的每一步

2013/12/14

“That’s one small step for a man, one giant leap for mankind.”这是1969年，当Neil Armstrong代表人类第一个登上月球时传回的第一句话。四十多年后的今天，每当我阅读

计算机科技史的文章，碰到那些震古烁今的天才科学家时，便又回想起Armstrong的话，



其对我内心之震撼，犹深不减。

- 本周最重大的新闻，无疑是NASA的“好奇号”（Curiosity）火星探测器，发现了火星上曾有淡水湖泊的明证，从而极大地提高了火星上曾有生物的可能性[1]。我一直觉得，科技的终极目标有两个：认识自我，认识宇宙。前者是人工智能技术要解决的问题，而后者则要依赖于像“好奇号”这样的宇宙航行器了。“好奇号”今天的发现，不过是它这个机器人在行进当中的小小一步，但却是我们人类认识宇宙的一大步。

- 本周五，Google宣布收购机器人公司，Boston Dynamics，由Anroid OS的发明人Andy Rubin统领[2]。这已是Google在2013年收购的第十家与人工智能或机器人技术相关的公司，难道机器人的时代真地为期不远了？现在的Google不光注重软件技术，更是开始进军芯片设计领域。最近，在Google的招聘栏里，出现了“数字芯片设计工程师”的职位，这说明Google已经不满足于软件层面的技术领先，更要从底层硬件的设计上拉大与竞争对手的距离。
- 在iOS 7.1 Beta版本里，出现了一项新功能“Car Display”[3]，标明了Apple下一代iOS进军汽车领域的决心。这一点我们已在前面的《科技一周~iOS in the car》有所描述[4].

本期科技一周的科普焦点，则是要探讨一下“好奇号”里面计算机控制系统的高可靠性问题。

当今的高可靠性计算机系统（比如，数据中心服务器、航天飞行器系统、“好奇号”机器人），对数据的正确性有着极其严格的要求，因为一旦出现传输错误，其结果之代价不仅昂贵，而且是致命的，轻则数亿美元的损失，重则数十亿美元，甚至会对很多人（宇航员、飞机乘客）的生命构成威胁。数据在稳态存储的情况下，其出错概率可以忽略不计，但在传输过程中，出错的概率就会大许多。这一点比较容易理解，就像，你把钱放在家里的保险箱中，几乎不会丢失，但你把钱拿出来随身携带，那么丢个三块两毛就是经常性事件了。

最简单也是最“笨”的方法，就是用两套相同的设备来传输，在接收端也用两套相同的设备来检测，并校正数据。打个比方来说，你要给家人写封信，为了保证可靠性，你把信复制了一下，寄出去两份相同的信件。当邮递员投递信件时，恰巧天有大雨，信上落满了斑斑点点的雨水，模糊了不少字迹。但你的家人阅读信件时，依然可以通过对比两封信件的内容来确认你的言词，即：如果一封信里某处词语模糊了，就阅读另一封信里同样位置上的词语。这种双信件高可靠性通讯暗含了一个原理：两封信都在同一个词语上出错的概率可以忽略不计。

然而，上述方法的缺点是，成本高昂：为达到高可靠性，花费了至少两倍于原来的成本。这个时候，就是“天才与奇迹”登场的时刻了。著名数学家，Richard Hamming，在1950年发明出以自己名字命名的编码格式：汉明码（Hamming Code），以极低的成本代价，达到了翻倍的校验可靠性。

汉明码现在被广泛地应用于高可靠性系统的内存模块上，即，带有ECC（Error-Correcting Code）功能的内存。Richard Hamming也因此获得了1968年的计算机界最高奖项，图灵奖（Turing Award）。

简单说来，如果一个传输数据拥有N比特，其中只要包含（logN+1) 比特的汉明校验码，就可以达到对一个比特错误进行自动校正的目的。例如，一个31比特的传输数据，其中只需要包含5比特的汉明校验码，另外26比特则是真正需要传输的有效信息。这样只需要花费5/26，不到五分之一的额外成本，就可以把出错概率降低一个幂次。也就是说，如果一个比特出错的概率为万分之一，原有系统的出错概率也是万分之一，但加入汉明码后，至少要两个比特同时出错，才会影响整个系统，于是整个系统的出错概率就降到了亿分之一！

Google的数据中心服务器里，飞机的计算机系统里，“好奇号”的控制系统里，中国的登月飞船里，无不使用了基于汉明码（或其衍生码）的高可靠性存储模块。That’s one genius’ small step, but one giant leap for science and technology。天才只迈出了一小步，就使人类的科技飞跃而前！

[1]. NASA, Possible extent of ancient lake in Gale Crater, Mars, http://www.nasa.gov/jpl/msl/mars-rover-curiosity-pia17596.html#.UqzFJWRDvnI , Dec 2013.
[2]. Josh Lowensohn, Google buys Boston Dynamics, http://www.theverge.com/2013/12/14/5209622/google-has-bought-robotics-company-boston-dynamics , Dec 2013.
[3]. Richard Nieva, Apple iOS 7 beta update hints upcoming “Car Display” feature,http://news.cnet.com/8301-13579_3-57615604-37/apple-ios-7-beta-update-hints-at-upcoming-car-display-feature/ , Dec 2013.
[4]. 硅谷寒, 科技一周~iOS in the car, http://www.valleytalk.org/2013/11/09/%E7%A7%91%E6%8A%80%E4%B8%80%E5%91%A8ios-in-the-car/ , Nov 2013.
图1. [1].
图2. [2].
图3. http://en.wikipedia.org/wiki/Richard_W._Hamming .

科技一周~色即是空

2012/12/21

“色不异空，空不异色，色即是空，空即是色。”《般若波罗蜜多心经》里的这句名言，并不是为了让我们联想起某些情色影片而存在，从计算机技术的角度来看，这句话竟然是虚拟现实（VR，virtual reality）技术所追求的究极之境：表象里美不胜收的“色”，均是由计算机生成的“虚拟之空”。虚实之道，真假之别，这一切看似互斥性的集合，很可能在未来的VR世界里不再有区分。换句话说，《Inception》绝非幻境，《The Matrix》终将来临。

- 初创公司Oculus本周从著名的投资人Andreessen Horowitz那里，融资7500万美元

[1]。Oculus是一家研制虚拟现实游戏设备的初创公司，其头盔式设备Oculus Rift刚刚荣获《时代》杂志评选的2013十佳硬件产品。此番再获风投认可，堪称锦上添

花。在机器智能浪潮再次袭来之际，虚拟现实技术作为增强人机交互体验之关键路径，也吸引了越来越多的高科技投资人。

- Facebook开始大力推出视频类广告，然而其面临的困难与挑战却一点儿也不少于希望。原有的电视广告世界并没有遭到破坏，甚至更加强大。现今的网络视频广告却已基本上成为Google YouTube的盘中之餐，Facebook要想横刀夺爱，绝非易事。从量级上来看，两者不相伯仲，均是十亿用户的量级，但从产品生态上来看，一在湖底一在天。当然，在这则新闻的背后，并不排除另外一种可能，Facebook在不远的将来，尝试推出硬件类产品来增强其生态。
- 惠普宣布自己旗下失败已久的移动操作系统WebOS，转战TV机顶盒市场[2]，第一个产品会在下个月的CES上展示。难道这就是Meg Whitman（惠普CEO）绸缪了三年的移动战略？要知道，TV设备市场因其固有生态之稳定，对于外来势力而言

，介入其中的壁垒并非如想像中那般容易。即便是如Google之强大，也曾在Google TV上连续失败了两代产品，直到今年推出超廉价的Chromecast，才出现转机。惠普的希望有多大？我的感觉是，微乎其微。

今天科技一周的技术关注点是“虚拟现实”。也许，虚拟现实的最高境界是摒弃了一切设备，直接对人体神经系统施以电脉冲刺激，从而使人脑产生相对应的虚幻印象。当然，这种最高之境界还有待生物学科的发展，从目前看来，其距离梦幻成真尚有时日。当下，在计算机界里最流行的虚拟现实，大多是一种视觉上的虚拟：通过特殊成像设备，在狭小的空间内虚拟出广阔的三维世界来。在这些虚拟现实系统里，最重要的一个组件，就是成像显示设备。微处理器经过复杂的计算后，都需要把生成图像信息传给显示设备，以此达成以假乱真的虚拟场景。

Oculus的显示设备并没有什么特别之处，依然是一个普通的LCD显示屏，7吋，分辨率1280×800。Oculus通过一对凸透镜来产生LCD画面到虚拟镜像，其原理类似于放大镜，可以使人们看到放大了许多倍的图像。Oculus的特别之处在于，利用双透镜，产生三维场景，并且在头盔上配备了运动传感器，可以实时检测到佩戴者的运动信息，从而反馈给处理器，做出相对应的场景切换。

相对而言，Google Glass的硅基液晶投影成像技术（LCoS，Liquid Crystal On Silicon）更先进一点。LCos并不需要笨重的LCD显示屏，而是直接将生成的图像投射进人眼的视网膜上，使人们产生“距离”的虚幻感觉。这样的眼镜，非常轻便，美中不足之处是，分辨率还没有LCD显示器高。确切地说，Google Glass还只是一种增强现实（Augmented Reality）技术，因为眼镜并不需要完全生成虚拟场景，否则佩戴者将会有安全风险。但是LCoS技术却有潜力在未来完全替代LCD技术，以LCos为基础的三维眼镜可以兼顾小巧轻便与细腻成像的有点。

在当前，最为逼真的虚拟现实技术要数美国伊利诺伊大学开发的CAVE（Cave Automatic Virtual Environment）系统了[3]。CAVE系统是一个以投影显示器为墙面的房间，实验者除了佩戴眼镜，还需在身上粘贴几片轻薄的传感器，走入房间后，便置身于巨大的虚拟幻境之中，自己的一举一动都被房间监测到，并反馈给计算机系统，从而对墙面上的显示图像做出调整，给人一种完全真实的“交互虚拟”。当然，这是非常专业级别的技术与设备，目前只有商业公司才会花费巨资来购买CAVE系统。希望，随着科技的进步，这类专业设备的成本降得越来越低，直到有一天“飞入寻常百姓家”。

[1]. Craig Manning, Oculus raises $75M to introduce virtual reality headset into mainstream marketplace, http://natmonitor.com/2013/12/16/oculus-raises-75m-to-introduce-virtual-reality-headset-into-mainstream-marketplace/ , Dec 2013.

[2]. webOS will reappear as a TV set at CES, Andrew Kameka, http://www.mobileburn.com/22353/news/webos-will-reappear-as-a-tv-set-at-ces , Dec 2013.

[3]. CAVE2: Next-Generation Virual-Reality and Visualization Hybrid Environment for Immersive Simulation and Information, Jason Leigh, etal. http://www.evl.uic.edu/core.php?mod=4&type=1&indi=424 , Dec 2013.

图1.
http://toucharcade.com/2013/10/29/oculus-rift-virtual-reality-headset-confirmed-for-ios-devices/
图2.
http://unwire.hk/2013/02/25/lg-acquires-webos-source-code-and-patents-from-hp-will-live-on-in-new-smart-tvs/news/attachment/lg-webos-smart-tv/
图3. [3]

科技一周~居里夫人的八百万比一

2013/12/28/

年年岁岁花相似，岁岁年年人不同。这是2013年的最后一个周末，对于高科技公司而言，无非是去年之回顾，来年之宏图，事程大同小异，然而，参与之人却可能多有不同。互联网、高科技，是个快速更迭的产业，这不仅仅指技术，也指从业人员，每一名高科技业者都随着行业的变化而变化：有人从传统软件转向移动应用，有人从互联网营销转向互联网煎饼，有人从网游转向掌游，还有人从网络黑客转向网络安全专家。当然，反之亦如是。

- 本周，美国著名加密实验室，RSA，否认其安全加密算法专门给美国国家安全局（NSA）留有后门的说法[1]。在今年8月份的时候，有多家科技媒体爆出，RSA每年接受NSA数千万美元的资助，从而专门给NSA留有解密后门，可以使其较为容易地破解所有采用RSA加密算法的密文。RSA本周虽然否认留有后门，但并未否认接受资助，其声明之可信程度仍有存疑。无论如何，这还是会给世界上其它国际带来安全性隐忧，毕竟RSA算法所用甚广，倘若其真有幕后之门，那么对于除美国外的所有国家而言，无异于把自己的“内裤”交给了美国。这是任何一个要与美国抗衡之大国所无法容忍的。
- “当红炸子鸡”初创公司，Snapchat，的API漏洞被澳大利亚黑客公开，虽然给Snapchat的用户带来了极大的安全问题，但却给全球的黑客们送来了一份圣诞节

大礼。黑客们凭此漏洞，可以轻松获取用户的电话号码，即使该用户在Snapchat里把自己的电话号码设置为“私密”等级[2]。

- 本周的12月26日，是镭元素被发现115周年纪念日。历史上第一个两获诺贝尔奖金的科学巨匠，居里夫人（1903年物理学奖，1911年化学奖），在115年前（1898年）的这一天发现了镭元素（Radium），之后又耗时四年从近8吨铀矿中提炼出来微似尘埃的1克镭[3]！精华的撷取，需要高达八百万倍的徒劳之功！每一个为人类文明做出了卓越贡献的人，都会被永恒地雕刻在空气与阳光里，我们每一次呼吸，每一次目视，都能体会到她（他）们给这个世界带来的震撼。

本期科技一周的科普焦点是第一条新闻里的加密算法~RSA。RSA算法是由三名数学家Rivest、Shamir、Adleman共同发明，现在已广泛应用于网络世界里，例如网络传输（https协议）、数据库加密存储。

RSA是一种非对称加密算法，即，采用两个不同的密钥来完成加解密：公钥加密，私钥解密。生成两个密钥，则需要使用到两个极大质数（Prime Number）的乘积。由于公钥会公开传输，可以被黑客截获，所以RSA的密钥生成算法要使得“从公钥计算出私钥具备极高的时间复杂度”。这一点是由质因数分解问题（Prime Factorization）的复杂度来保证，虽然质因数分解还没有被证明是NP（Non-deterministic Polynomial），但现存已知的算法复杂度要比多项式量级（Polynomial）慢很多，仅比指数量级（Exponential）略快。1999年，512-bit的RSA密钥被成功破解，之后又花了十年，才破解768-bit的密钥。现在流行的RSA密钥有1024 bits，但业界已经开始建议升级到更长的2048 bits，以确保加密的安全性。

理论上，RSA算法不存在所谓的“后门”，要想从密文破译出原始明文，必须要知道在加密过程中所用到的两个大质数，如果RSA不给NSA提供大质数的选择算法，NSA是无法在短时间内破密信息的。当然，所有一切的安全性假设都基于RSA实验室的独立性，如果RSA接受了NSA的金元资助，那么这种假设前提的安全性就要大打折扣。毕竟，互联网虽是基于计算机，但计算机却是受人所控。

[1]. Damon Poeter, RSA denies knowingly building NSA ‘back door’ into security software,http://www.pcmag.com/article2/0,2817,2428665,00.asp , Dec 2013.

[2]. Violet Blue, Researchers publish Snapchat code allowing phone number matching after exploit disclosures ignored,

http://www.zdnet.com/researchers-publish-snapchat-code-allowing-phone-number-matching-after-exploit-disclosures-ignored-7000024629/ , Dec 2013.
[3]. Aip.org, Maria Curie and the science of radiactivity, http://www.aip.org/history/curie/resbr2.htm.
图1. [1].
图2. [2].
图3. [3].