trend CQIU

2017年4月17日星期一

目 录

[1. 模板标题1 3](#_Toc480191340)

[1.1 模板标题2 3](#_Toc480191341)

[1.1.1 模板标题3 3](#_Toc480191342)

[1.1.2 模板标题3 3](#_Toc480191343)

[1.1.2.1 模板标题4 3](#_Toc480191344)

[1.1.2.2 模板标题4 3](#_Toc480191345)

[2. 模板标题1 3](#_Toc480191346)

[2.1 模板标题2 3](#_Toc480191347)

[2.1.1 模板标题3 3](#_Toc480191348)

[2.1.1.1 模板标题4 3](#_Toc480191349)

## 背景

区块链，大数据，人工智能，量子力学，计算机未来的一些联系

知识点链接：张首晟教授，

张首晟演讲：量子计算、人工智能与区块链

对话新时代，2018中国（深圳）IT领袖峰会

<http://www.p5w.net/live/lthyzb/zglxfh02_2662/201803/t20180325_2098638.htm>

## 未来发展方向

对未来发展方向的一些判断，

### 量子计算

从粒子说起

#### 粒子有正也有反

中国哲学观点，万事万物都是对立存在的，有正必有反，有阳必有阴。在量子物理世界中，也是一样的。

曾经有一位非常伟大的理论物理学家狄拉克，他跟爱因斯坦、杨振宁是我认为20世纪做出最伟大贡献的三位物理学家，他把爱因斯坦的狭义相对论和量子力学统一起来，在统一的过程中他要做一个非常简单的数学运算，就是开一个根号。在开根号的时候始终会出现正负两个解，一般人可能只关心正解，不关心负解。但是狄拉克很聪明，他把负解解释成所有的粒子必然有反粒子。这些本来是负能的解，大家觉得非常奇怪，为什么粒子可能有负能，他就把负能的解释为所有的基本粒子有粒子必然有反粒子。他当时这个是非常惊人的预言，1928年的时候并没有发现有反粒子的现象，大家都对他提出非常大的质疑，说他这个方程肯定不对，在世界上肯定没有看到反粒子。他说我的方程实在是太美了，你们继续去寻找。过了5年，他也是非常幸运，果然在宇宙辐射的射线里面，大家找到了电子的反粒子，就是正粒子，命名为狄拉克海。从此之后基本粒子物理了有质子找到了反质子，有中子也找到了反中子。比如正电子对生活当中医疗领域里面已经有广泛的应用，有一种医疗测试叫PET，就是用正电子的产生，和正电子和负电子可以成像，比如我们要测阿兹海默症，最好的办法就是做PET。

#### 好看的电影《达芬奇密码》《天使与魔鬼》

一定要看的好电影

#### Majorana费米子先生提出质疑有粒子没有反粒子

出来另外一位理论物理学家他完全出于好奇心，他问世界上会不会有一些粒子并没有反粒子？他果然有找到了一个方程，现在叫Majorana方程，这个方程也是奇妙地描写了有一种粒子没有反粒子，或者它自己就是自己的反粒子。他的文章发表之后没人理他，因为所有的反粒子都找到了，所以他没有像狄拉克那么幸运，他也感到自己的人生非常失落，在意大利的一个港口城市上了渡轮，本来想去西西里岛，但是他从来没有下过。这个就成了整个物理学的两个大迷，一个是粒子有没有存在，我们称它为Majorana费米子，它是没有反粒子，只有它自己一种或者它自己就是自己的反粒子。另外就是Majorana本人也是非常大的迷，他好像泄露天机之后就被天使叫去了。

#### 寻找Majorana费米子

寻找马约拉那（Majorana）费米子

基本粒子有正面和反面，但是费米子只有一面，他可能是通常粒子的一半，通常粒子在电导是台阶性的量子化，是0,1,2等等，张首晟的观点，费米子电导率是0.5的台阶。

我们定义这个粒子是天使粒子

#### 小插曲天使粒子-费米子和玻色子

这两种粒子都是天使粒子，标准模型中的基本粒子可以分为费米子和玻色子。

费米子是构成物质的粒子，

玻色子是传递物质间作用力的粒子。

简单例子，物质和辐射可以同时表现出粒子和波的行为，这叫波粒二象性。

#### 马约拉那费米子制作量子计算机

计算机已经分成两类了，有经典计算机和量子计算机。有些问题经典计算机就很容易解决，比如把两个大的数乘起来，经典计算机可以算得很快。但是一个数看能不能拆成另外两个数的乘积，比如15可以写成3乘以5，这个数比较小的话你自己也可以算出来。但是给你一个很大的数，经典的计算机要算这个数到底是不是两个数的乘积需要花很长的时间，因为它用的算法是穷举法，把所有可能被除的数一个个除过来，最后才能确认这到底是不是两个数的乘积，经典计算机算起来非常慢。今天人工智能要做的事情，整个人类所有计算的事情最终能转化为优化的问题，很多的可能性，我们要找到最佳的可能性，经典计算机只能用穷举法，最后才算出一个答案。但是量子世界是非常神奇的世界，是平行的世界。比如一个著名的试验，如果我放出一个粒子，比如光子，它有两个孔，要不是左边，要不是右边。比如我打一个炮弹过去的话，要不就是从左边穿过，要不就是从右边穿过，不可能同一个时间既穿过左边，又穿过右边。但是量子世界有一种本真的平行在里面，一个基本粒子在某一个瞬间同时穿过了两个孔，只有这种行为才能解释在后面形成的干扰条纹。假定要么是左，要么是右的话，看起来的图像就不是这个显示的图像。量子的世界本身就是平行的。如果用量子世界来做计算的话就能够秒算，把所有的可能性一下子算出来，因为量子世界有它本真的平行性，这是量子计算最基本的概念。

　　但是要真正造出这个量子计算机是非常困难的，比如最基本的单位，经典计算机最基本的单位是比特，就是信息要不是0就是1，用0、1就能够表达所有的信息，这是经典计算机的概念。但是在量子世界里面，一个粒子同时穿过左孔，又穿过右孔，处在某一种叠加的状态。一个量子比特讲不请是0还是1，它是处在0和1叠加的状态里面。大家听一个比喻，薛定谔猫就处在死和活的叠加状态里面。这是一种非常奇妙的现象。但是由于这种基本的现象，说明一个量子的比特本身是不太稳定的，你去观察一下周围就知道它要不就是在左边，要不就是在右边，要不是0，要不就是1，任何一个噪声就会对量子比特产生很大的干扰。

　　最近量子计算机成为全球和美国著名公司特别关注的，谷歌也在这方面做投资，微软也在做投资，IBM也在做投资，因特尔也在做投资，但是根本上不能解决这个问题，一个量子比特是非常不稳定的，如果哪天告诉我们做了50量子比特，但是关键的问题是有用的比特是多少，如果只有一个有用的比特，往往在这种量子计算的框架下需要10个、20个甚至40个、50个纠错的比特来为它服务，使得量子计算很难真正实现。但是天使粒子的发现根本改变了，这是量变到质变的过程，并不是把量子比特做得越多越好，量子比特本身自带纠错的能力，就是我把通常一个量子比特能够拆分成两个天使粒子的。我刚才一直在讲基本的概念，通常的粒子有两面，天使粒子只有一面，所以天使粒子通常只相当于一个粒子的一半。所以通常一个量子比特就可以用两个天使粒子来储存它。一旦用了两个粒子储存它，它们在遥远的地方，它们相互是有纠缠的。但是在经典世界里面的噪音，它们相互之间是没有纠缠的，这样的话就没法用噪声来破坏由天使粒子所储存的量子，所以这是一个革命性的改变。所以我在两周之前在美国物理学会作的演讲，首先天使粒子的发现是激动人心的发现，但是用量子做量子计算机是多少比特就多少比特，不用附加纠错的比特，自带纠错功能，这会对量子计算达到突飞猛进的发现。

#### 量子计算机个人总结

基础技术的发展需要更长的时间，这块东西与我专业关系不大，关注进展即可，可以看出10年之内不会有重大商用突破。

### 人工智能

人工智能的发展，目前还处于早期阶段

#### 人工智能发展还处于早期阶段

现在人工智能是在简单地模仿人的神经元，但是我们更应该思考的，在这里面有一个基础科学重大突破的机会，就是我们真正去理解那个智慧和智能的基本原理，基本的数学原理，这样真正能够使人工智能有突飞猛进的变化。

#### 人工智能脑动大开的想法-做科学实验

最近我在人工智能里面写了一篇文章，将会在美国的科学院杂志上发表，题目叫“Atom2Vec”，人类最伟大的科学发现之一，有相对论、量子力学，在化学里面最伟大的发现就是元素周期表的发现。今天的机器假定我们根本不知道元素周期表这件事情，今天的机器在没有任何辅导的情况下，他自己能不能自动发现元素周期表？我们输入的就是所有存在的科学元素的名字，把这些化合物的名字输入这个算法里面，结果这个机器自然地发现了元素周期表，它可以做出人类认为最伟大的科学发现。然后我们这个程序可以帮助我们发现新药，也可以用机器学习的办法发现新的材料。

#### 人工智能发展个人总结

目前人工智能是大家能看到容易落地的方向，比量子计算要容易些，发展前景广阔，值得一辈子研究学习的方向。

### 区块链-利用数学建立信任

In Math we trust，人与人之间的信念建立在数学上。

#### 数据的保护，隐私的保护，区块链的使命

接下来我会再跟大家分享我最后一个题目区块链，人工智能在突飞猛进发展，但是人工智能最缺少的是数据，恰恰今天数据是处在完全中心垄断的状态里面，不能帮助机器合理地学习。大家听说在一个星期之前Facebook很多个人的数据被盗一样，至少在没有被允许下就用。在今天的世界个人会产生出很多的数据，个人的基因数据、医疗数据、教育数据、行为数据等。但是很多这些数据都是掌握在中心机构里面，没有达到真正的去中心化。但是区块链的产生就是能够产生一个数据市场。所以我理想的世界，未来每人拥有自己所有的数据，这是完全去中心化的储存，这样黑客也不可能黑每个人的数据。然后用一些加密的算法在区块链上真正能够达到既保护个人的隐私，又能够做出良好的计算。

所以我把今后区块链的整个理念用一句话来描写，叫“In Math we trust”，我们的信念建筑在数学上。这张表大家应该记得，我看到很多人在照相，某一天它肯定会为整个区块链和整个IT领域里面最基础的，它既是最基础的数学，又是能导致数据市场里面保护个人隐私，又能够做出合理的统计性的计算。比如有一种非常神奇的计算方法叫零知识证明，它能够向你证明我的数据是非常有价值的，但是又不告诉你真正隐私的数据在哪。

我今天报告的题目主要是有一个核心的理念，就是要使得IT真正能够发展，既需要物理学，又需要数学。深圳在应用方面做得不错，但是由于大学还不是在全世界范围里面最领先的大学，但是我建议最核心的投资，这一类的数学和物理，跟IT领域真正有紧密的联系。

有了区块链之后，这个数据市场的产生，我们也真正能够使得社会变得更加公平，我们现在社会最大的不公平是我们容易歧视一些少数派。但是在机器学习的过程中最需要的就是那些少数派所拥有的数据。如果今天机器学习的精准率达到90%了，我要使90%达到99%，它需要的不是已经学过的数据，而是跟以前最不一样的数据。往往是少数派拥有的数据对机器学习来讲是最有价值的。一旦我们建筑在区块链的基础上，再加上这些奇妙的数学算法之后，我们就能够真正达到数据市场，在这个数据市场里面，这些少数派所拥有的数据是最可贵的。这样的话我们真正能够把一个丑小鸭变成一个美天鹅，因为丑小鸭并不是丑，只是跟别人不一样而已，在这个世界里面真正达成区块链和人工智能互相共存的世界理念，它们是会最有价值的。

整个区块链，大家对它的认识还不是最根本的第一性原理的认识。用最基本的物理学原理来讲，达到共识就是大家都同意同一个账本，就相当于在物理学里面，比如磁铁本来是杂乱无章的，但是到了铁磁态里面它们指向的方向都是同一样的。所以达到共识在自然世界里面有，在今天的人文世界里面也有。但这种现象是叫熵减的现象，达到共识，大家都朝一个方向的话，这个状态的熵是远远比杂乱无章的熵要小。达到这个共识是非常难的，因为熵总是在增的，今天你要把它减是很难的事情。在区块链上能达到一个共识系统都是用一种算法，在这上面是需要消耗能量。大家可能一开始不太理解为什么这件事情听起来不合理，一些账户为什么要耗费能量。从物理学第二定理来讲，这是非常合理的一件事情，因为达到共识本身是熵减，但整个世界的熵一定要增加，所以在达到共识的同时一定要把另外一些熵排除出去。这种没有中心化的机制跟自然世界里面磁铁从杂乱无章的状态达到有序的铁磁状态非常相像，这付出的代价也是必然的趋势。

我在这里跟大家分享，我除了做斯坦福大学教授之外，也是丹华资本创办人，我们主要的核心理念就是要把今天最前沿的科技和投资要紧密联系起来，要用第一性原理的思维方式来理解今天的世界。

我另外想讲的是我是来自学界，我们在整个人工智能领域里面需要做两个大的桥梁，一个是要学界和产业界做紧密的联系，在学界有最好的物理、最好的数学和算法的发现和发明。在今年1月8日，我非常荣幸在人民代表大会堂受到习总书记给我授予的中华人民共和国国际科技合作奖。我们整个世界科学是最无止境、最没有国界的，科学能真正把人类带到超越国界的，今天我们所要解决的人工智能、量子计算都是整个人类的问题。所以我们一定要把我们的眼光不要放在自己的局部，而是放眼整个全球和整个世界。在这个过程中，中国也是一个非常大的机遇，大家都想回答的问题，我们中国除了把应用科技做得好，能不能在中国有真正原创科技的产生。我今天跟大家介绍的这些都是最基本的物理和最基本的数学原理，我们这方面能够做好的话，而且这些原理听起来比较抽象，比如熵增原理，正负电子。但是在最基本的层次上，这是我们今天这个世界的奇妙，它真正能够给整个IT行业提供最基本的科学技术发展的前景。

#### 区块链个人总结

区块链的发展，使得人和人之间的沟通建立在数学基础上，而不是权利，政府，这个非常重要，长期的发展必然是这个结果。

短期之内，可以在小规模应用领域，比如数据加密，隐私保护等等，未来数据爆炸性的增长，但是如何保护隐私呢，利用数学，区块链技术，值得钻研的方向。

## 模板标题1

模板标题1正文

### 模板标题2

模板标题2正文

#### 模板标题3

模板标题3正文

##### 模板标题4

模板标题4正文

###### 模板标题5

模板标题5正文

模板标题6

模板标题6正文

模板标题6

模板标题7

模板标题7正文