本文将从一名区块链产品工作者的视角向大家说明，区块链并不止眼前的ICO和交易所，还有更多玩法有待发掘，过早地炒作可能是一种“捧杀”，希望更多人能静下心来挖掘实际应用场景下的可能性。

复杂的交易所参数

还有，随着交易所的数量增长，像比特币类似的区块链货币在不同交易所的价格是存在一定差异的，这也很正常，交易所中某个币种的价格受交易所交易撮合结果的直接影响，而谁也无法保证不同交易所中的价格认知都时刻保持一致。那么问题来了，哪个交易所的价格才可以用来代表比特币的最新价格呢？事实上，这个问题并不会对比特币的价格产生过大的影响，因为区块链货币的去中心化特质，一旦A交易所中比特币的价格高于B交易所中的，就会有人从B交易所购买比特币，并且转入A交易所中高价卖出，这会使得两个交易所中的比特币价格趋同，当然，还需要考虑到转币的手续费是否可以被利润cover掉。

交易所钱包

前面提到，交易所中的地址并非区块链上的公钥，而是使用了一种叫做钱包服务器的技术生成并分配给用户的，如果用户通过Txhash或者其他方式在区块链上查询从个人钱包转入到交易所钱包的一笔转账，就会发现区块上的转入地址并非交易所提

供的地址，事实上，这个地址是交易所的收款公钥（为了和大家所知的交易所地址区分）。实际的流程是，用户从个人钱包转帐给了交易所的收款公钥，交易所再将与这一笔转账的金额相同数量的虚拟货币分配到用户的账户下，这个时候，它又从一个区块链实体变成了一个数字，真正的区块链实体保存在了交易所的钱包中。

黑客通常喜欢将黑手伸向这些囤积有大量虚拟货币的交易所钱包，一旦交易所钱包失窃，那对交易所会是个莫大的打击，甚至万劫不复。为了应对这种情况，有人开发出了多种方案，其中还运用了许多密码学的知识。冷存储和热存储，是目前较为流行的做法。

冷储存与热储存

前面我们提到，交易所会把区块链货币放在自己的服务器中，把区块链货币放在电脑里就像把钱放在钱包里带着，这叫“热储存”，这很方便但不安全。而“冷储存”是离线的，把区块链货币锁在其他地方，不联入互联网，所以相对安全和保险，但显然是不方便的。这就像你带着一些零钱出去，但是把终身积蓄锁在保险柜里的道理一样。

要分开热储存和冷储存，你也必须要用不同的私钥，否则如果热储存被人破坏了，冷储存也会处于危险之中。你也需要把币在两边转来转去，这样两边都需要知道对方的地址或公钥。

因为冷储存是离线的，所以热储存和冷储存不需要上线就可以接收比特币——热储存端知道冷储存端的地址，所以它随时可以给冷储存转账。当你觉得你的钱包里的钱太多的时候，你可以把一部分的币转到冷储存，但不需要让冷储存上线而暴露自己。当然，只要冷储存上线，就可以接收到区块链的转账信息，然后可以随意处理这些比特币。

但管理冷储存有个小问题：一方面，为了私密性和其他考虑，我们希望使用不同的地址（这些地址有不同的密钥）收款。所以我们把比特币从热储存转到冷储存的时候，要用一个新的冷储存地址。但是由于冷储存不上线，所以热储存端必须要能找到这样的地址。

一个直接的方案是让冷储存一次性生成一批地址，然后把地址列表发送给热储存，热储存可以依次使用这些地址，当然，这个方法的缺陷是为了传送地址，我们不得不经常让冷储存端上线，上线的过程中就存在与热储存端一样的风险了。

分层确定性钱包

还有一个比较有效的方法是分层确定性钱包。这个方法可以让冷储存端制造无限量的地址数量，然后通过一个短暂的 / 一次性的交换，让热储存端知晓所有地址。但这需要使用密码学的技巧。在分层确定性钱包中，我们用“generateKeys”地址生成函数生成一个被称为“地址生成信息”的东西；我们也不只生成私钥，而是生成“私钥生成信息”。有了地址生成信息，我们就可以生成一系列地址。我们把地址生成信息和一个整数i作为地址生成函数的输入参数，就生成了i个对应地址。同样，我们用私钥生成信息来生成一系列私钥。对于每个i而言，第i 个地址和第i个私钥相匹配——换言之，第i个私钥控制第i个地址的区块链虚拟货币，这样一来，我们就有一组彼此配对的公钥和私钥。这种方式的好处是：地址生成信息不会泄露关于私钥本身的任何信息，这意味着你可以放心的把地址生成信息给任何人。

了解了这样的技术后，接下去的过程就显而易见：

1. 冷储存端生成和保存私钥生成信息和地址生成信息，然后将地址生成信息一次性转给热储存端，这个转的过程中，黑客即便获取到地址生成信息也不会暴露私钥；
2. 当热储存端要给冷储存端转账时，就通过地址生成信息和“generateKeys”地址生成函数按次序生成新的地址；
3. 冷储存端上线后，也会按顺序生成地址，然后查收相应地址收到的款项，直到某一地址没有收款为止；
4. 如果冷储存端需要向热储存端转账，它就会按顺序生成私钥序列。

分层确定性钱包有我们需要的所有特性：两方都可以生成公钥 / 私钥序列，而且这些公钥 / 私钥相互配对；而且，这种方法还具有另外一种我们尚未提及的特性：当你向外提供这些公钥时，这些公钥之间没有联系，也就是说，别人无法断定这些公钥来自同一个钱包。

分层确定性钱包的热储存端的安全性较低，但如果热储存端收到损害，私钥以及区块链虚拟货币仍然是安全的。通常，分层确定性钱包还支持任意多个安全等级，当一家公司内部存在多种授权级别时，就需要这种特性。

大脑钱包与助记词

除了分层确定性钱包外，还有一种通过密码就可以支取数字资产的方式，这被称之为“大脑钱包”。大脑钱包无需使用硬件 / 纸张或者其他长期储存介质，这在物理安全性较差的情况下（例如跨国出差 / 旅行时）非常有用。

大脑钱包的主要原理是用一个可预测的算法把一个口令变成一对公钥 / 私钥。但是，如果有黑客知道了猜到了你的口令，他还是可以偷走你大脑钱包里的所有私钥。在计算机安全领域，我们通常假定黑客知道你生成密钥的步骤，黑客不知道的只是你的口令。所以黑客可以尝试使用不同的口令生成地址，并在区块中查看这些地址上是否还存在未被使用的数字资产，一旦发现数字资产，黑客就可以迅速把这些资产转给自己，这种破解方式被称之为离线猜测或者密码破解。因此，设置口令密码的难度就大大增加了，又要容易记，又要不容易被猜中。

这也就是助记词的由来，从最常见的10000个英语词汇中，随机选择6个词，从而生成大致80位长度的字节。这种方式会比随机取字母容易记忆，因为这种方式生成的口令通常是这样的：

earth alloy dog okay till focusing

当然了，如果需要增加复杂度，可以选择12个词或更多。需要记住的是，一旦用户忘记大脑钱包的口令，钱包里的数字资产就永远取不出来了，除非用户还采取了其他措施来保管私钥。

风险

前面我们提到了交易所最重要的几个技术特点：

1. 数字资产存储
2. 撮合交易
3. 加密钱包

许多交易所在这三个方面还会有各自的创新和技术选型，我只是根据我所了解的程度介绍了最常见的几种。把交易所比作银行，交易所同样也需要面对和银行同样的风险问题：

- 第一类风险是挤兑。
  挤兑就是大家同时都去银行提款，由于银行只保留一部分存款，所以可能无法应付所有的提款要求。当银行无法兑现的谣言四起之时，大家开始恐慌，然后更多人去银行提钱，造成资金链断裂。
- 第二类风险是，银行本身可
  能就是庞氏骗局。
  庞氏骗局的做法是不断借新还旧，从储户吸收存款，答应日后提供一定的收益，但实际上这笔钱并没有用于投资，而是勇于支付先前储户的收益，

这类骗局最终必然会崩溃。
- 第三类风险就是黑客入侵。
  由于交易所储存大量数字资产，所以交易所需要非常小心地监控软件的安全性及其操作流程——例如，如何管理冷热储存等。如果某个环节出了差错，用户储存在交易所的数字资产就会被盗取。

在历史上，这三种风险造成交易所倒闭的案例都出现过。

监管方式

目前交易所还没有被纳入到政府的监管中，因此不免有许多投资人会对交易所感到不放心，但是银行却在政府监管下存在了很久，所以我们不妨站在政府监管银行的角度来考虑政府应该如何监管交易所。

政府会要求银行有一个最低准备金，在美国，银行随时要保留总储蓄量的3%～10%的现金来应付突发的提款要求。政府通常还会对银行的投资类别以及资金管理方法进行监管，政府要求银行的资产投向低风险资产。除此以外，当一个遵纪守法的银行濒临破产时，银行会偿还储户一部分存款，甚至有时候充当“最后借款人”的身份来给银行提供贷款，知道银行有足够的资金可以周转，从而渡过难关。

那么，交易所未来的监管方式是否会是这样的呢？也许不尽相同，相较于“政府背书”，交易所也需要寻求一种“共识背书”，接受包括政府在内的任何机构和个人的监督，例如实现去中心化的交易所，这将是一个类似比特币“自举”的过程。有一种相对简单的证明方式叫“准备金证明”。

准备金证明包括两方面内容：

- 证明交易所有多少准备金。
  这比较容易，交易所只需要发起一笔向自己转账的交易，转账的金额等于其公布的金额即可，然后向用户说明这笔交易的有效性；
- 用同一个私钥为一条查询命令签名，这个查询命令是公正的第三方随意发出的字符串，这样就能证明出具准备金证明的人至少知晓该私钥。

但仅仅这样，也只能证明交易所“至少”有多少准备金，按照严格的方式，交易所还需要公开储蓄规模（即交易所的负债规模），才能向投资人证明自己的准备金比例是一个比较合理的比例，所有人都可以通过交易所公开的准备金证明和负债证明来确认交易所的准备金比例。

这种方式虽然可以达到目的，但是由于会泄露许多交易所信息，所以通常很少有交易所愿意这么做，有一种叫“准备金”的协议可以解决这个问题，既可以证明有偿付能力，又不需要披露总负债和准备金规模。不过这个协议采用了更先进的加密技术，相对来说比较复杂，这里不作赘述。

MtGox曾经掌握比特币世界90%的交易量，但最终还是抵不住信任危机而倒闭，监管从某种长远意义上能够帮助合理运营的交易所减少风险，但这只是我个人的愚见。

尾记

区块链遇上交易所是“区块链遇上现实”系列的第一弹，后续不定期会更新我对区块链落地应用的一些想法以及方案，因为区块链技术每天都有巨大地进步与发展，希望通过更新文章督促自己不断学习。