C3安全峰会
CYBER | CLOUD | COMMUNICATION

《安全简史》之区块链新视角

杨义先 教授
北京邮电大学信息安全中心主任

C3

《安全通论》《安全简史》作者

最近全力以赴，写了两本书

- 第1本：《安全通论》
  - 定位：顶天！为网络空间安全学科，建立一套统一的基础理论，改变安全界“盲人摸象、头痛医头，足痛治足”的现状。
  - 榜样：香农《信息论》，将通信领域的各个分支，统一起来；仅用区区两个定理（信源编码定理、信道编码定理），就为现代通信竖起了“指路明灯”。
  - 目的：刷新业界安全观！

最近全力以赴，写了两本书

- 第2本：《安全简史》
  - 定位：立地！外行不觉深，内行不觉浅。内容将涵盖信息安全的各主要分支。
  - 榜样：霍金的《时间简史》，布莱森的《万物简史》，格雷克的《信息简史》。它们不但出神入化，而且还能改变读者的世界观！
  - 目的：信息安全知识的全民科普！
- 两本书综合起来的梦想：为百姓明心，为专家见性；为安全写简史，为学科开通论！

《安全通论》与《安全简史》的关系

- 《安全通论》是用数学语言写成的《安全简史》；
- 《安全简史》是用文学语言写成的《安全通论》！
- 如果您不想陷入数学公式中，那么，建议您只阅读《安全简史》！
- 如果您想吃透《安全通论》，那么，也建议您先读《安全简史》！
- 下面用“诗和远方”来简介《安全简史》中的区块链部分。当然，您若想更爽，建议您直接阅读《安全简史》！

《安全通论》的第一个副产品

C3安全峰会
CYBER | CLOUD | COMMUNICATION

公众号： 亦仙亦凡

通过京东购买《安全简史》

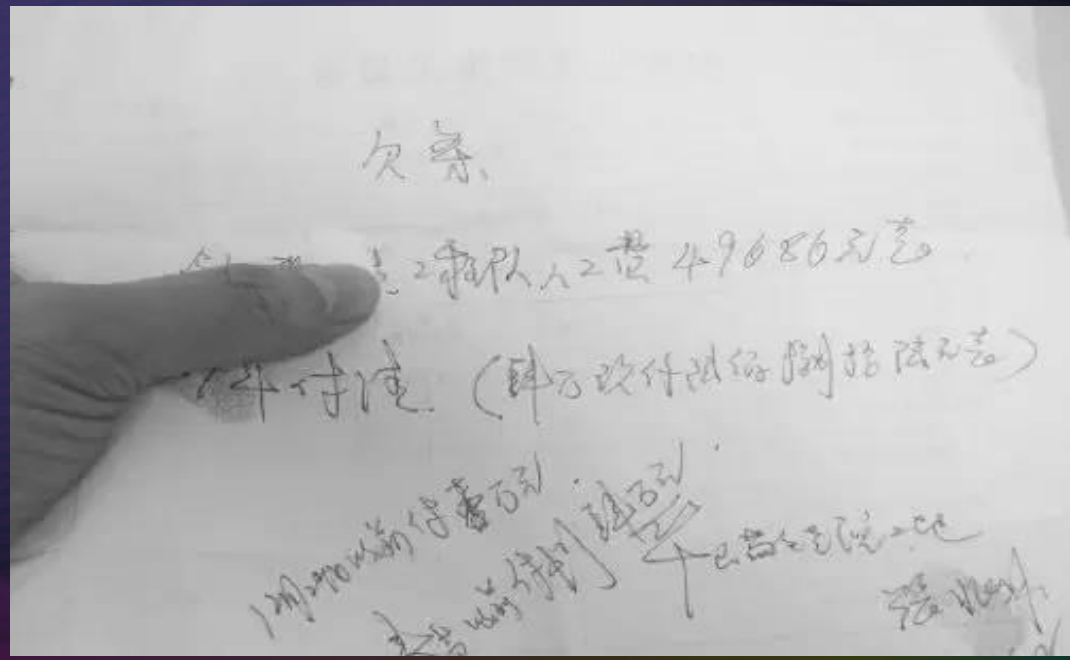
通过当当购买《安全简史》

第2回：牵着区块链，却道没看见

- 哥们儿，见过钱吗？别说你是千万富翁，甚至亿万富翁，你可能还真没见过钱；至少没用过钱，或很少用过钱；再保守一点，你可能不知道，到底什么才是钱，才是真正的钱！
- 请别在我面前拍出什么美钞呀，英镑呀，加币呀，日元呀等等；告诉你吧：它们仍然不是钱，而是“钞票”。**别急，且听我慢慢道来。**

第2回：牵着区块链，却道没看见

- 你当过民工吗？老板是不是经常给你发白条？如果你和工友们，对老板足够信任的话；那么，在你们眼里，白条几乎就等于钱了。彼此之间，既可以用白条来交易；又可以，在年底老板发财后，用白条去换钞票。



第2回：牵着区块链，却道没看见

- 退一万步说，如果老板破产了，还可以凭白条，去法庭打官司，讨回欠薪！理论上说，只要老板高兴，只要他不顾自己的信誉，那么，他就可以签发无数白条，直到东窗事发。
- 如果这个老板不是普通老板，而是大老板，甚至大到某个国家的“央行”；那么，他发的白条就叫做“钞票”了。如果你非要问我“钞票和白条有什么本质区别”的话，那我只好说：滥签白条后，有法院为你撑腰；滥印钞票后，你就自己找个地儿，哭去吧！

第2回：牵着区块链，却道没看见

- 若你没当过民工，那么，总用过单位发的饭票吧。饭票在单位内部，可以当钱花。用饭票，不但可从食堂买到窝头，还能与同事换擦脸油；部门领导年终发奖金时，也可以折合成饭票；在单位倒闭前，根本不用担心饭票会变废纸！

第2回：牵着区块链，却道没看见

- 从理论上说，单位的饭票也可以随便印，想印多少就要多少，直到公司破产为止。如果这个单位不是普通单位，而是大单位，大到是某个国家的“央行”，那么，它发的饭票就又成为“钞票”了。当然，在非常时期，钞票可以变得一钱不值，甚至出现“一袋子钱，买半袋子米”的怪事；如果遇到改朝换代，那就更惨了，因为，前朝的钞票就连废纸都不如了。

第2回：牵着区块链，却道没看见

- 所以，白条、饭票、钞票、支票、汇票等都是一回事，它们本身不是钱，但在平常，又确实可以当钱用；可在特殊时期，却可能变得一文不值！
- 为什么会出现这种翻天覆地的变故呢？关键就是信任基础不牢靠！你信老板吧，他可以跑路；信单位吧，它可以破产；信央行吧，可能改朝换代；信国家吧，却道是“天下大势，分久必合，合久必分”，国家也可能重组！

第2回：牵着区块链，却道没看见

- 真正的钱，应该以“最牢靠的东西”为信任基础！但是，什么东西才“最牢靠”呢？答案就是：除了上帝，就是自己！当然，这里的“上帝”，是会与时俱进的；这里的“自己”并不是个体的自己，而是“自己的群体”，或者说是“群体的绝大多数”。

第2回：牵着区块链，却道没看见

- 伙计，别急！我知道你想单刀直入“区块链”，但是，不先把“上帝”说清楚，你就无法洞察区块链的本质；除非你是安全专家，除非你能直接阅读《现代密码学》、《数字货币技术》、《安全协议设计与分析》等方面的学术专著或原创论文。
- 早期，由于人类对自己根本没信心，所以，肯定不敢想什么“基于信任自己”的真钱；而是，全力以赴，寻找“基于信任上帝”的真钱。

第2回：牵着区块链，却道没看见

- 于是，“齿贝”便成为了首个“基于信任上帝”的真钱。而且，这种真正的钱，在部落之间，也完全可以流通，因为，其它部落也造不出“齿贝”。

第2回：牵着区块链，却道没看见

- 请仔细想想，在无船、无潜水设备、无大型挖掘机，更无人工养殖技术的时代，部落所能获得的“齿贝”总数，显然是有限的；而且，该数量完全由上帝确定，即使是贵为酋长，他也没本事随意“印刷”或制造“齿贝”。而且，到遥远的海边去拾贝，并不比上山狩猎更容易；所以，不必担心“通货膨胀”。

第2回：牵着区块链，却道没看见

- “齿贝”被淘汰后，人类又开始寻找新的“真钱”。先是用铜当“真钱”，按其重量来代表价值；但是，由于冶炼技术越来越高，结果却发现，铜太多了；于是，铜就变成了“基于信任国家”的“假钱”了，并被铸成了“孔方兄”。

第2回：牵着区块链，却道没看见

- 经过无数次探索，无数次与上帝的讨价还价，人类终于发现了一种长期有效的“基于信任上帝”的真钱。只可惜，这家伙太沉，分割又不方便，携带也麻烦；于是，如今，包括你在内，大部分人都没把它当钱用，而只是将它打成小环，套在手指上；或将它熔成豆腐块，藏在保险柜里。国家们也并不更高明，它们也是将“真钱”锁在库房里，不但不用，还得派重兵把守，简直成了负担。也许你已经猜到了这个真钱是什么；对，它就是你朝思暮想的黄金。

第2回：牵着区块链，却道没看见

第2回：牵着区块链，却道没看见

- 为什么说黄金是“基于信任上帝”的真钱呢？这里主要有两个原因：
  - 首先，除了神话中的“点石成金”外，人类至今没办法，在可见的将来好像也没办法，无中生有地制造出黄金来；因此，任何国家或组织，都无法根据自己的意愿来随意“印钱”了。
  - 其次，黄金确实是上帝赐予的，是他老人家从遥远的外星，送给地球的：那已是45亿年前的事情了，当时，地球还是一个温度足以熔化一切的大火球，宇宙中的许多小天体，便带着黄金投奔了地球。

第2回：牵着区块链，却道没看见

- 到目前为止，好像还没有比黄金更理想的“真钱”，即使是曾经与黄金比肩的白银，现在也越来越不行了；因为，白银实在是太多，几乎快要被挤出“货币”江湖了。
- 看来，在“真钱”方面，上帝能帮人类的，也就只这些了。剩下的，只能依靠人类自己想办法，研制“自己信任自己”的“真钱”了。于是，**“区块链”就准备粉墨登场了。**

第2回：牵着区块链，却道没看见

- 那么，“真钱”到底都有哪些特性呢，从当年的“齿贝”和现在的黄金，我们可以归纳出：
  - 1）除上帝外，没发行机构，其发行数量也就不可能被操纵；用行话说，就叫“完全去中心化”。注意：上帝是与时俱进的哟，比如，当养殖业发达后，“齿贝”的“发行量”就可操纵了；万一今后某天，人类若能从太空带回更多黄金，那时，黄金数量就可操纵了。

第2回：牵着区块链，却道没看见

- 2）“真钱”的总量，既不能像白银那样过多，也不能像钻石那样太少。至于，到底多少才是最佳，可能与其使用人群的数量和财富有关。
- 3）能匿名，且保存方便。即，无法像支票那样，追踪出使用者，否则，人类就没隐私了。
- 4）很健壮，且合并、分割等使用也很方便，而且，不容易被毁掉。
- 5）可以跨国界流通、交易，甚至在全世界使用，既可以买，也可以卖；而且，操作还很方便。
- 6）无法造假，而且还具有专属所有权，即，“我的就是我的，不可能莫名其妙地变成了你的”。

第2回：牵着区块链，却道没看见

- 以上条件，听起来非常苛刻，好像很难达到。但到目前为止，至少比特币就声称能达到“真钱”的所有主要条件。
  - 比如，它没有货币机构发行，只能通过大量的计算产生；所有交易行为，都由全球的分布式数据库来确认并记录；网络本身的去中心化特性，确保了任何单位和个人，都无法“大量制造比特币，并以此来操控币值”。基于密码学的设计，又可确保“只有真正的拥有者，才能转移或支付比特币”，而且，还不影响其所有权和交易匿名性。比特币的总量非常有限，具有极强的稀缺性；它的数量永远不会超过2100万个等等。

第2回：牵着区块链，却道没看见

- 现在介绍设计比特币的最核心技术，区块链，的前世和今生。
- 如果你不懂数据库，不懂密码学，不懂算法理论，不懂网络……，反正，IT界的所有高精尖的东西，你全都不懂的话；没关系，只要继续听，你就能懂“区块链”。
- 如果你已经是“区块链”专家了，那么，也建议你继续听下去，因为，你将突然发现，哦~，原来我们过去只顾一心科研，竟然忘了玩！

第2回：牵着区块链，却道没看见

- 伙计，其实没那么玄！只要你是中国人，哪怕是文盲或半文盲，那么，对区块链的理解都再容易不过了。因为，区块链就是虚拟部落的“家谱”。除了读写、存储、传输、验证、安全、共识等雕虫小技的IT细节外，“区块链”与你我家中，压箱底的传家宝“家谱”，其实并无本质差别。

第2回：牵着区块链，却道没看见

第2回：牵着区块链，却道没看见

- 如果你不信，咱们就来逐一对比：
  - 首先是所谓的“去中心化”。你的“家谱”虽然作为宝贝，牢牢藏在箱底，但是，它的拷贝版，却在你七大姑、八大姨等家，每家都有一份，而且内容完全一样。
    - 每个小家在“家谱”的“核算”、“存储”、“维护”等方面的权利和义务，也都完全均等，都是通过家族开会，由“族长”领导大家，共同修订、补充新版本的。如果你偷偷修改了“自家的那份家谱”，当然不管用，只不过是自欺欺人而已：家族是不会承认的，甚至可能变成笑柄；严重时，还可能受到家法惩处。

第2回：牵着区块链，却道没看见

- （续1）再看“开放性”。有哪家的“家谱”是保密的！完全可以公开，而且，谁都乐意公开嘛，因为，那上面都记载着祖先们的光荣事迹呢。
- 第三，看看“自治性”。在同一家谱所系的整个大家族中，哪个成员会怀疑自己家谱内容的真实性？就算是在天涯海角，偶然遇到的陌路人，如果发现同为家谱成员，那么，就绝不仅仅是“老乡见老乡，两眼泪汪汪”了。至于外族人，他爱信不信，反正与他无关。

第2回：牵着区块链，却道没看见

- （续2）第四，看看“信息不可篡改性”。一旦相关事迹写入家谱，就会永久保存下去，除非某天召开家族大会，同意（或多数同意）某项修改，那么，仅对少数几本家谱的篡改是完全无效的
  - 就算是你要坚持做些修改，那么，后代通过对各家家谱内容的统计比较，仅仅采用“少数服从多数”的原则，就能轻松发现你的篡改。所以，“家谱”的数据稳定性和可靠性都极高。

第2回：牵着区块链，却道没看见

- （续3）第五，看看“匿名性”。家谱的每次修改和补充，都是经过大家讨论同意的结果。至于这些内容是由谁抄上去的，其实并不重要。甚至，对文盲家族来说，他们可能聘请穷秀才，即，大街上的那位写字先生，来帮忙抄写“家谱”新版本。所以，在“区块链”这本“家谱”中，每次交易（即，修改和补充“家谱”的工作），到底是由谁完成的，你永远不得而知！

第2回：牵着区块链，却道没看见

- （续4）第六，看看“历史可追溯性”。这恰恰是家谱最基本的功能，每个人通过自己的家谱，都能够将自己的祖宗十八代，查得清清楚楚、明明白白；就像“区块链”中“通过任意一个区块，都可以追溯出与之相关的所有区块，了解整个信息的演变过程”一样。
- 怎么样，请问区块链的哪条性质，家谱不具备！如果你还要坚持说，区块链还有什么“私有区块链”、“公有区块链”和“联合（行业）区块链”等的话，那么，别忘了，家谱也有“小家家谱”、“某地某姓族谱”和“全球某姓族谱”等等

《安全简史》这样讲“区块链”

- 寻寻觅觅，深深浅浅，区区块块链链。
- 乍暖还寒难辨，真币假钱。
- 饭票钞票白条，怎敌他换代改朝！
- 雁过也，正伤心，财富一夜丢尽。
- 满地黄金堆积，支票损，狂喜竟然哭泣！
- 守着齿贝，独自怎生得意！
- 真钱更像细雨，到黄昏，点点滴滴。
- 求上帝，早促成电子货币！

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You