BLOCK CHAIN

区块链风暴

区块链3.0时代的商业经济重塑

戴永彧 林定芃 ○著

去伪存真，透析资本与技术的临界点

颠覆与革命，“大数据+人工智能”

区块链3.0时代，你该何去何从？

企业管理出版社
ENTERPRISE MANAGEMENT PUBLISHING HOUSE

区块链风暴

戴永彧 林定芃 著

企业管理出版社

图书在版编目（CIP）数据

区块链风暴 / 戴永彧，林定芃著. -- 北京 : 企业管理出版社，2018.10

ISBN 978-7-5164-1796-6

Ⅰ. ①区… Ⅱ. ①戴… ②林… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字(2018)第 233692 号

书　　名：区块链风暴
作　　者：戴永彧　林定芃
选题策划：周灵均
责任编辑：周灵均
书　　号：ISBN 978-7-5164-1796-6
出版发行：企业管理出版社
地　　址：北京市海淀区紫竹院南路 17 号　　邮编：100048
网　　址：http://www.emph.cn
电　　话：编辑部　（010）68456991　　发行部　（010）68701073
电子信箱：emph003@sina.cn
印　　刷：北京华创印务有限公司
经　　销：新华书店
规　　格：165 毫米×235 毫米　16 开本　15.25 印张　150 千字
版　　次：2018 年 10 月第 1 版　2018 年 10 月第 1 次印刷
定　　价：68.00 元

序

区块链热延烧的日子，戴永彧院长喊出："凡不以真实消费或落地应用为目的的区块链项目，通通都是耍'流氓'。"这既需要洞察的智慧，更需要说真话的勇气。我是最早看过本书初稿的少数几位之一，深感作者见解独到、鞭辟入里，链上原风景跃然纸上。

因为工作的关系，我所在的中科星泰公司和中科院海西研究院，与戴教授任职院长的海西创业大学有较多交集。对我们开发中国版基础链 Token String 的初衷，戴院长高度赞赏。上线后，Token String 在国际国内发布悬赏，经受饱和黑客攻击测试，基于 Java 的区块链程序安然无恙。和马云不懂 IT 技术一样，同为"60 后"的戴院长也不会编程，但他们对互联网思维和区块链精神的理解，透彻且具有前瞻性。

戴院长创作伊始，在了解他想解构区块链技术的意愿后，我们进行了多次交流与沟通，并且给予了一些个人的见解与意见。戴院长如斯形容区块链技术 1.0 和 2.0：比特币好比没有窗户和楼梯，只有 2100 万套高耗能空调房间的不实用的空中摩天大厦；以太坊则好比一个广袤的开发园区，但入园条件模糊、基础设施不全、建设没有规划。戴院长高度认同 Token String 是真正的区块链技术 3.0。

由衷感谢戴院长能够将这本书写得如此无懈可击，书中所著述的区块链应用场景，全部可基于 Token String 而完美实现！我希望在业内我们能起到抛砖引玉的作用，在日后的落地应用中能引起更多业内人士尤其是应用企业的重视，从而使得这项中国原创技术能够在区块链全球风暴中有更多的建树。

这是一个弯道超车的绝佳时代。以太坊创始人 V 神确实是一个天才，他的创新给了我很多启发，在 Token String 的底层设计上我学习、借鉴了比特币和以太坊技术，同时也做了漏洞修补和关键创新。

中国技术，中国声音，中国规则，中国力量；国际视野，国际领先，国际布局，国际合作。

Token String 从诞生之初即已注定不凡。在戴院长促成下，我们正选择优秀的区块链企业进行混合所有制改造，形成 TOK 产业集群，未来将有大批传统实体产业完美链上 Token String。

让风暴来得更猛烈些吧！

中科星泰数据科技有限公司 CEO/CTO　罗马（Rome）

2018 年 8 月

目录

第九章

chapter ONE

第一章

探寻区块链的源头："重回拜占庭"

在原始的战争年代，将军与将军、将军与下属之间的联系只能采用最原始的方式——"出行靠走，通信靠吼"的口头传输。在已知有成员谋反的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，这就是"拜占庭将军问题"。

1. 古老的“拜占庭将军问题”

让人生，让人死，让人痴迷，让人疯狂。这就是传说中繁华与没落、绝望与救赎并存的东罗马帝国首都——拜占庭。

想象一下，在拜占庭时代有一个强大的城邦，它拥有巨大的财富，它的周围有 10 个城邦，它们都觊觎拜占庭的财富，想要侵略并占领它。

它们各自组织了一支军队，这 10 支军队之间彼此独立、各自为营，且各自派出一个联络员互相联系。在这种情况下，“中心”是不存在的，信息传递可以在任意两支军队之间进行。也就是说，此时的信息传递是“点对点的”。

假设这 10 支军队必须同时进攻才有胜算，那么要做到同时进攻，就必须确保所有的“点对点”信息传递都是正确无误的。但是，这一点在实际操作中很难。因为在战争中，要做到信息同步几乎不可能，而且存在“他们当中有叛徒，故意传递错误信息”的可能。

这就是信息传递中的“拜占庭难题”。

2. 国家、组织与个人之间的不信任

简单地讲，"拜占庭难题"指的就是去中心化信息传播中的"同步"和"互信"的难题。

我们进一步往深处探讨一下"拜占庭难题"，很显然，这 10 支军队是一个由互相不信任的各方构成的网络，是一个去中心化的网络，但它们又必须一起努力完成共同的使命。它们之间唯一的联络方式就是信使。

如果每个城邦都向其他 9 个城邦派出 1 名信使，那么每个城邦会派出 9 名信使，共 10 个城邦，也就是说在任何一个时间总计有 90 次的传输，并且每个城邦分别会收到 9 个信息，而每一个信息都可能传达着不同的进攻时间。

假设这当中有几个城邦故意同时答应几个不同的进攻时间，或者它们重新向网络发起新的信息，都可能造成进攻时间上的混乱。这种国家、组织与个人之间的不信任，解决的难度会更大。

现在这个网络里只是 10 个人，那么假如是 20 个、30 个人呢？

我们稍加计算就可以发现：随着人数的增加，达成共识的希望会变得越来越渺茫。

如果把上面例子中的城邦换成计算机网络中的节点，把信使换成节点之间的通信，把进攻时间换成需要达成共识的信息，我们就可以理解“去中心化传播中的共识问题”是一个怎样的难题了。

达成共识对于信息传播的重要性是不言而喻的。

例如，我们在一个去中心化（没有第三方做信用背书）的网络里交易，核实的时候系统告诉你“关于你的上一笔交易情况，我们的系统里有三个版本的记录”，那么这个系统显然是不可信的。在区块链出现之前，去中心化的共识问题是很难被完美解决的，要保证达成共识就必须采取中心化的系统。

再如，两个不认识的人在网络上交易，A 付了钱，B 却不承认，说自己没有收到，A 几乎是一点儿办法也没有。在淘宝上交易，因为有了第三方——支付宝的存在，有支付宝做信用背书，交易才能顺利进行。

我们会发现，在区块链出现之前，绝大多数商业行为都是中心化的系统。

3. 构建人类命运共同体最大的挑战

区块链的出现，其实与信用是必不可分的。为什么呢？

这还要从货币的产生说起。

在原始社会，人们使用以物易物的方式，交换自己所需要的物资，比如一头羊换一头牛。后来发展到用一种大家都能接受的物品作为交换物，于是就有了实物货币的出现——贝壳。

比如，甲有一头羊，乙有一头牛，那么，甲用一头羊换了贝壳，再拿着贝壳去换乙的一头牛。这个交换过程的前提就是，贝壳是甲、乙两人都认可的"实物货币"。

随着商品交换的迅速发展，对货币的需求量越来越大，海贝已无法满足人们的需求，于是人们开始用铜仿制海贝。铜贝的出现，是我国古代货币史上由自然货币向人工货币的一次重大演变。

随着人工铸币的大量使用，海贝这种自然货币便慢慢退出了货币舞台。经过长年的淘汰和选择，金属逐渐取代了其他物品，并成为交换中的固定媒介。

古希腊哲学家亚里士多德认为，货币必须具有实质价值，这种价值由其金属价值决定，货币的实体必须由贵金属构成。在这个相当漫长的时间里，我们发现货币的发展始终停留在“价值货币”的层面上，也就是说，货币本身是有其自身价值的。

随着经济的进一步发展，金属货币同样暴露出使用上的不便。在大额交易中，金属货币的重量和体积给人们增添了很多麻烦，而且金属货币在使用流通的过程中会有磨损，这几乎是不可避免的，在这种情况下纸币应运而生。

纸币的出现，这个时候的货币本身已经没有任何的价值，它只是一种价值的符号。但是人们为什么愿意接受它呢？为什么愿意用自己的大米、猪、牛、羊、衣服等有实际价值的东西，去交换一张自身没有任何价值的纸币呢？

这就是信用问题。

当解决了信用问题，货币就可以完成从“价值货币”到“记账货币”的转变。这其实就是信用共识的问题，纸币天然地把货币的实用价值降到最低，同时纸币天然地带有信用的色彩，即一种被信任的能力。

为什么人们对纸币能够达成信用共识呢？是因为有个“中心（国家）”的存在。人们相信国家，相信政府，所以相信它印刷的纸币。

纵观整个货币发展史，我们不难发现，人类的货币发展史实

际上也是人类对信用机制探索的过程。

继续延伸下去，这不只是货币，在人类社会的方方面面，无论是商业还是生活，其实都有"信用"的难题存在，如果不能解决信用问题，人类将寸步难行。目前，商业社会中各个领域的信用机制都是"中心化"的，所以有各种中介的存在。

例如，人们怕对方借钱不还，所以出现了担保人和担保公司；人们网购怕付了钱对方不认，所以有了"支付宝"；人们在交易房屋等贵重物品时，怕对方赖账，所以会让房地产中介充当中间人，以起到监督的作用。

有了这些中介还不够，仍然会出现各种各样的纠纷，所以还有公证处、仲裁中心、法院等机构来解决纠纷。

有没有一种方法，能够在去中心化的前提下（没有第三方监管），让两个完全不认识的人之间达成互信呢？区块链就是在解决这个难题的过程中诞生的。它创造了智能信用，对人类意义非凡。

信用、信任对人类社会有多重要，答案是不言而喻的。很多时候，商业活动中的一切曲折和难题都是信任的问题，而其中无数的低效行为和资源浪费，也都是为了解决信任的难题。

（1）人与人之间的信任

一个人能记住多少张脸？

有一个人类学家，他研究部落的时候，发现每一个部落都控制在150人左右。因为人再多一些的话，就记不住了，记不住脸就感受不到亲近，连亲近都没有了，信任就更无从谈起了。没有信任，部落之间的战斗和争端就永远不会停止。

人与人之间点对点的信任，其极限也就是150人——这个理论由数学家邓巴提出，也称“邓巴数”。虽然这个世界上有一些人，他们的社交范围非常广，但总体来说，一旦一个群体的人数超过150人，成员之间的关系就将开始淡化。

邓巴写道：“150人似乎是我们能够建立社交关系的人数上限，在这种关系中，我们了解他们是谁，也了解他们与我们自己的关系。”

中国人也有一句老话：“好事不出门，坏事传千里。”

当一个客户对你的服务满意时，他会告诉身边的5个人；而当一个客户对你的服务不满意时，他会告诉身边的20个人。

当一个销售人员去拜访他的潜在客户时，即使可以很快断定这个不可能是你的客户，你也不能让他感到你冷热无常。生意可以不做，但是朋友不可不交。否则，这一趟你就白跑了。即使他不可能和你做生意，但是不要忘记他后面还有150个人，如果他把你当成了朋友，并且了解了你的生意，他就有可能帮你介绍生意。要知道一个人能够信任的人是非常有限的。所以，在过去的经济活动中，第三方信任背书是必不可少的。