悠唐天下区块链技术应用

白皮书

v 1.0

悠唐天下

2017 年 6 月 26 日

目录

1. 序言 1

2. 悠唐区块链系统简介 4

3. 传统区块链系统的问题 5

4. 悠唐区块链系统的解决方案 8

悠唐社会化网络中的虚拟社会结构分为三个分支 8

悠唐的社会化网络结构与区块链技术的结合具体表现 9

悠唐区块链系统的架构 11

5. 悠唐区块链系统的发展 14

悠唐天下区块链技术应用 v 1.0

序言

据最新数据统计 ,基于区块链技术在全球范围内的应用和普及目前最为主流的区块链电子币市场已经超过 1000 亿美元，包括比特币（BTC）、莱特币（LTC）、以太坊（ETH）、瑞波币（Ripple）这些电子货币都在区块链技术基础上发展而来，在保持区块链技术的去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively maintain）、可靠数据库（Reliable Database）的四个基本特征前提下产生的更适合于未来商业行为所需要的商务合约、众筹募资、跨境支付、域名系统、交易市场、身份管理等业务，此外还有诸如去中心化交易所、金融衍生品、对等投注和基于块链的身份和信誉系统之类的更高级的应用。可能所有这一切之中最具雄心的概念是自治代理或者去中心化自治机构-资源和资金被密码学块链上的自我强制的智能合约以自治方式管理 ,从而避开了对于法律合约和组织规章的依赖，且没有任何中央控制的在块链上运行的自治实体。

区块链就是分布式认证协议。区块链技术的首个软件实现就是比特币，即区块链 1.0 实现的是数字电子货币功能。区块链 2.0 本质是个所有权登记认证系统，致力于实现一切市场交易和商业信用行为，包括债券、保险、外汇、股票、期货、期权、期钱等金融活动，和租当、众筹、信用物联网等需要征信和智能合约的场合，可参照软件有以太坊等。区块链 3.0 是个网络化计算机协同的人工智能操作系统，其目标是实现自组织机构、分布式节点互信社交网络及蕴含的相应经济社会制度，乃至去中心化政府其配以建国方略实现的乌托邦。

目前全球基于区块链技术而产生衍生技术超过百种，形成了诸子百家的形态，基于上述同一基础理念而形成不同的方向 ,随着时间的推移必定会因为传统商业和传统金融的逐步应用和认可而形成电子货币的统一，才能形成全球市场的合理流通，如同秦一统七国，电子币

不可能长期出现兑换关系，在未来只有一种电子币成为唯一全球电子币而统一全球货币，实现全球更有效的经济发展。

区块链目前分为三类，在货币发行的《区块链：定义未来金融与经济新格局》[2] 一书中就有详细介绍，

其中混合区块链和私有区块链可以认为是广义的私链:

公有区块链（PublicBlockChains)

公有区块链是指：世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。公有区块链是最早的区块链，也是目前应用最广泛的区块链，各大 bitcoins 系列的虚拟数字货币均基于公有区块链，世界上有且仅有一条该币种对应的区块链。其特点是任何人都可以成为矿工，并以算力竞争记账权，用户匿名使用，没有国界限制 ,典型代表有比特币及以太坊，公有链的应用依托平台上的各类智能合约，提供众筹募资、跨境支付、域名系统、交易市场、身份管理等业务。

联合（行业）区块链（ConsortiumBlockChains)

行业区块链：由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程(本质上还是托管记账，只是变成分布式记账，预选节点的多少，如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的 API 进行限定查询。其特点是有授权中心，一些节点获得授权成为记账节点，记账节点通过投票共同维护账本，系统用户通常是实名且获得授权后准入。联盟链是当前政府、金融行业应用较为集中的方向，典型代表有 Hyperledger，EEA 和 Corda。

私有区块链（privateBlockChains)

私有区块链：仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，

独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。目前(Dec2015)保守的巨头（传统金融）都是想实验尝试私有区块链，而公链的应用例如 bitcoin 已经工业化，私链的应用产品还在摸索当中。

悠唐区块链系统简介

悠唐的区块链技术实际上是介于 2.0 系统和 3.0 系统之间的一个创新的分支系统，悠唐区块链系统自 2015 年 9 月启动规划，2016 年初正式启动开发，自 2017 年 1 月开始测试已持续近半年，计划于 9 月 1 日上线试运。悠唐区块链系统定义为：联合（行业）区块链（ConsortiumBlockChains)。同时，悠唐区块链不同于传统区块链在保留了区块链技术的必备特征以及安全特点的前提下，结合社会化网络的复杂需求，形成了适合于实现自组织机构、分布式节点互信社交网络及蕴含的相应经济社会制度的社会化区块链系统。把个体的人和商品、贸易和货币、组织和社会全部通过区块链体系融合在一起。

悠唐区块链技术所代表的电子货币名称为“唐卡”英文“Tangka coin”缩写 TKC。大唐王朝在人类发展过程中是当时全球科技、政治、经济、文化、军事的霸主地位，对日本、西亚乃至欧洲的社会文化、经济、军事都产生了巨大影响。因此，唐卡借大唐盛世之意表一统天下之心，所以悠唐电子币定义为“糖卡”。糖卡的实物设计沿袭“币”的圆形将 TK 的字符衍生，同时将唐朝的天元通宝所代表的中国古币天圆地方的设计理念融合，形成唐卡的实物定义。

传统区块链系统的问题

比特币（BTC）和以太坊（ETH）代表着两种区块链技术，两种技术代表着不同区块链版本，比特币(BTC)代表着区块链技术的 1.0 版本（以虚拟货币交易为重，后来通过侧链技术衍生到不同的商业合约的应用），以太坊（ETH)从诞生起目标就明确为：通过去中心，去信任化，提供更为丰富的社会商业应用。所以代表着区块链 2.0 版本。

这两种区块链技术也都遇到了安全和流量危机：

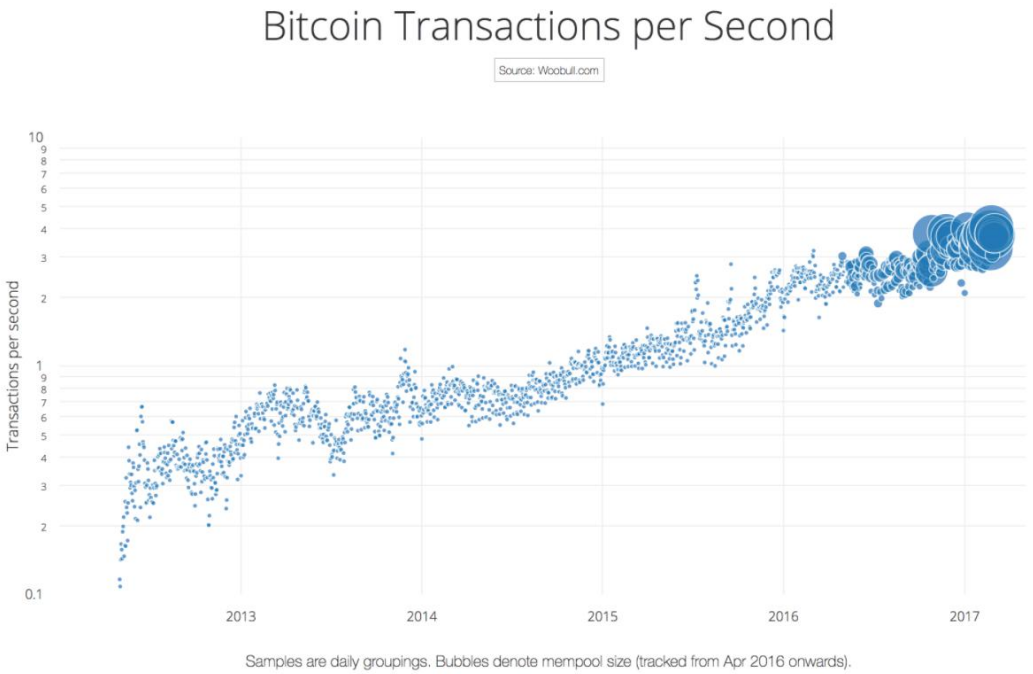
安全危机：

2014 年 2 月 7 日 ,因遭到网络攻击 ,世界最大规模的比特币交易所运营商 Mt.Gox2014 年 2 月 28 日宣布，因交易平台的 85 万个比特币（按目前市价计算为约为 170 亿人民币）被盗一空 Mt.Gox 临时停止比特币提取业务，引发交易混乱和用户不满。2014 年 2 月 25 日午间起，用户无法登录 Mt.Gox 交易平台。网站首页随后贴出“告顾客书”，称为保护用户和交易平台，将暂停所有交易。

2016 年 6 月 17 日发生了在以太坊区块链历史上留下沉重一笔的攻击事件。由于其编写的智能合约存在着重大缺陷,区块链业界最大的众筹项目 TheDAO 遭到攻击,目前已导致 300 多万以太币资产（按目前市价计算约为 69 亿人民币）被分离出 TheDAO 资产池。

流量危机：

随着交易量和节点的增加，比特币和以太币的都会出现流量危机。



上文中的图表显示了比特币网络近年来处理交易（每秒）的能力

比特币的交易计算方式以及每个区块 1M 的容量会逐步成为瓶颈。假设我们只是想要实现全地球人一年两次的链上交易 ,那就需要大约 126MB 区块以及 6.7TB 一年的理论上的最大化区块链增长。长远来看的话，运行一个完整节点很明显会成为一件很严重的事情。如果我们想要全人类能够实现一日两次的链上交易（如还账单、买食品杂货、买咖啡）的话，我们需要接近 46GB 的块大小，这是很惊人的。运行一个完整存档节点每年需要 2.4PB 的存储，这是一个让 btc 走向终点瓶颈，需要有合理的方法去解决，区块过大会导致中央集权的发生，过小会无法适应快速的流量增长。

以太坊（ETH）合约所能提供的业务，几乎是无穷无尽的，它的边界就是你的想象力，因为图灵完备的语言提供了完整的自由度，让用户搭建各种应用，这是以太坊的核心。随着用户搭建的应用的增多 ,每种应用都存在大量的交易。如前述所提到的 The DAO 攻击案例，The DAO 就是一种基于以太坊合约的一个应用。因此，以太坊的网络里充满了大量的垃圾交易，造成所有的交易所和钱包服务商无法提供提币业务。和比特币不同，最让以太币持有人郁闷的是，无论怎么提高手续费，很多交易都会被弹回（rejected）。比特币还可以提高

手续费得到快速确认，以太坊拥堵似乎无解。

上述问题以及更多发现但本文未阐述的问题，在很长一段时间都会伴随者这两种不同方向的区块链技术形影不离，需要在成长的过程中不断与魔鬼搏斗，毕竟都还在取经路上。

悠唐区块链系统解决方案

悠唐的区块链技术从开始就选择的是 :联合(行业)区块链(ConsortiumBlockChains) 技术。从逻辑角度理解，相对于公有区块链（ PublicBlockChains) 没有那么全面的开放，会带有一定来自核心的管理规则和认证，避免了公有区块链的完全自治而导致的不可控风险。同时，悠唐的区块链技术源于其在近三年时间建立的虚拟社区网络所组织的社会化网络结构而实现的有组织的去中心化管理机制。这种机制与区块链技术结合，形成基于人类社会的去中心化+基于区块链的货币的去中心化，这两个去中心化的同步实施，达成两条腿前进，缺一都会成为去中心化进程的瘸腿状态，必然难以为继。因为这个社会是人的社会，不仅仅是货币，当然科技、文化、商业等进程依然需要货币的参与，所以社会化网络和区块链技术的结合，两个去中心化的结合，相辅相成才是区块链技术的未来，才是社会化网络的未来！

悠唐的社会化网络是通过构建一个庞大的虚拟社区并逐步引入现实社会中所涉及的各种商业、生活、娱乐需求，形成一个去中心化的虚拟与现实相结合的、水乳交融的、不可分割的去中心化的社会网络，一个去中心化的乌托邦。目前已开发并上线内容包括：电商（ bestkeep)、影视(xweed)、创业(xunoins)、游戏(悠唐天下)、服装工业(Tailorx)、体育（ 黑晶、非常果岭)、医美（ u 美)、娱乐（ 千寻)、演艺（ 芊雨 ）等涉及社会需求的各个方面，同时随也影响力的扩大也按计划逐步开展各行业、企业进入悠唐生态，提供社会化网络更全面的服务内容。

悠唐社会化网络中的虚拟社会结构分为三个分支：

1. **创世：**悠唐网络+诸侯国，随着社会化网络去中心化的发展最终形成一个概念而无权力;

2. **会员：**社会化网络的人口，每个会员都是现实社会中的真实个体，通过一定规则相

组合形成社会化层级概念，形成虚拟的立体结构。商业行为、市场行为、社交行为、等都以这个分支为唯一分支，也就是这个分支是正常的全社会形态的网络化；

3. **门客：**也是会员，同时具有相对于会员更高的建议权和参与权，相对于会员来说其有更好的在不同行业、学科的经验、能力和学术理论。这个分支代表着社会化网络发展中的决策建议功能。

这三种社会结构分支，代表三种力量相互制衡，相互发展，以去中心化为发展方向，通过健全的、高效、安全的票权系统（以区块链技术为基础）形成最终的去中心化组织结构。

悠唐的社会化网络结构与区块链技术的结合具体表现如下：

创世+区块链：

创世是指悠唐社会化网络发展的初期由悠唐网络所以公司行为来辅佑其初期稳定发展的悠唐网络的代称。在悠唐区块链上线后，国王出现，其所管辖的诸侯国接手原悠唐网络的部分权利，如唐卡发行权，所辖社群 192 万人的管理权，等等。国王也就成为创世的成员。

会员+区块链：

悠唐的社会化网络的会员的组织结构分为：布衣、百夫长、知府、刺史、太守、国王，6 个主要类型。同时社会化网络赋予除布衣、百夫长之外的 4 个类型的会员不同的人口的管辖权（包括人口数量和社会内容）分别对应 4 个人口单位：府（500 人口）、郡（1 万人口）、州（16 万人口）、诸侯国（192 万人口）。

区块链技术结合主要体现在与这 4 个单位的结合，悠唐区块链技术直接摒弃了区块链技术的串行链技术，而是将网状 P2P 和串行链技术相结合，形成层级传递结构，不仅有效的避免了前述所论述到的 BTC 和 ETH 所遇到安全和流量问题，而且大大提升了交易效率，能做到毫秒级的交易达成，并大家降低节点记账和验证压力，这也是分级所带来的优势。这

也是中国文化所讲求的自然，毕竟世间万物，无论花草、动物、星系都是层级相生。在自然界有食物链系统层级，在宇宙中有恒星系、银河系等的层级，从微观到宏观层级无所不在。所以区块链不可避免的要依存于自然规律才能得到更好的发展。

回溯 20 年前网络传输技术的发展，可以惊人的看到区块链技术的现在和未来竟然与网络传输技术的发展如此的相似。当网络传输技术在开始初期具有三种主流协议：令牌环（token-ring）、IPX（ipx/spx）、TCP（tcp/ip），这三种协议在 2000 年前还在讨论谁最终一统天下，当时认为 TCP 技术必然消亡的专家学者占大多数，但结果是其它两种技术已经消失了。为什么呢？当时互联网带宽还是以模拟拨号和 isdn 为主流技术，所能承载的带宽在 64kb 和 128kb，虽然 tcp 协议简单方便，但是有冗长的报头，占用大量的带宽，所以当时得出这个结论，谁能想到 2000 年之后的快速以太网技术的发展，光传输技术的发展，导致目前家庭带宽都到了 100Mb，达到了当初带宽速度的 1000 倍。

当然，以太网交换和路由技术的发展也有类似的过程，最开始在局域网中还存在大量的 HUB（冲突域），导致每个网段的互联电脑的数量很少，也较为复杂（5-2-3 原则）。紧接着交换机（广播域）的普及可以让一个局域网轻松接入上百台设备，同时通过路由器形成不同广播域的路由关系（当然路由协议也同样有类似的进程，这个好奇者可以百度，本文不再论述）

而现在的区块链技术与互联网传输技术的早期很相似，不同的协议版本百家争鸣，所有的区块链技术都处于串行和全广播技术层面。试想，如果数 10 亿人，每天都交易两笔，这个层面的技术如何撑住如此天量的传递和验证，更不用说保证安全。就如同 10 亿人在同一个房间每个人都拿着一个喇叭开会，如此的广播量不死即伤，何况有效传递。

所以区块链的立体化结构势在必行，悠唐区块链系统正是通过其社会化网络的立体结构与区块链立体结构的全融合的解决方案。从而能应对天量级的各类交易和社会服务。

门客+区块链：

门客是会员的另一种身份，其本身也是会员。门客与区块链的结合是通过悠唐的票权系统通过区块链技术实现在投票过程的中的身份验证、匿名投票、隐私保护、票权计算等稳定与有效，实现区块链技术为基础的票权系统，能够强力促进社会事物的大众方向，是社会化网络去中心化进程的基础。

基于上述悠唐网络区块链技术的社会化特点：将社会的人和区块链技术紧密结合。形成如下运行逻辑（细节见后续版本）

悠唐区块链系统的架构

悠唐区块链不同于传统区块链在保留了区块链技术的必备特征以及安全特点的前提下，结合社会化网络的复杂需求，形成了适合于实现自组织机构、分布式节点互信社交网络及蕴含的相应经济社会制度的社会化区块链系统。把个体的人和商品、贸易和货币、组织和社会全部通过区块链融合在一起。

悠唐天下中的国定义为诸侯国，国的形成基本要素是最大人口数满足 192 万人（192 万人的有效注册信息）。在人口达到 192 万之前，可以具备国的结构，王的选举是通过创世、门客、会员通过票权系统推荐产生的。王在达到管理 192 万人口 60%之前按执政期来计算，每个执政期为 1 年，可以连任，最多连任 2 界。当超过 60%人口后，王为终身和世袭制。两种方式都会有一定的执政管理考核方式，从而期望对诸侯国合理的管理，刺激人口的增长和业务市场的发展。

诸侯国（王），作为区块链的最高级节点（一级记账区块），具备唐卡（TKC）的发行权（TKC 的发行不是依照传统区块链的挖矿方式，而是依据于诸侯国内有效会员的人口数量为参照作为发行数量。按每个府为 500 人口为计算，每个府具备 1 万 TKC，那么平均

每个新增有效注册，就会增加 20TKC 的发行量，同时获得 5 倍的预发行量，即 100 个 TKC。王可以与国内的太守、刺史、知府、百夫长、布衣按一定的比例规则去扩大该国会员数量的增长从而获得 TKC 的销售数量和销售额。销售收入由诸侯国和创世钱庄 1：1 分配，同时在悠唐数据可视化系统网站公开数据，并按一定规则给予王本人和在人口增加的过程中，每增加一个人都会按一定比例奖励一定数量的 TKC，如同比特币挖矿后奖励的 BTC。奖励的 TKC 激活后，可以直接参与交易。

诸侯国所发行的 TKC，为防止 TKC 在不同诸侯国的币值不统一，所以所有 TKC 不分国属性，统一币值，统一交易市场，统一发行价 30 元每 TKC。按 192 万人口最多可发行收入 11.5 亿人民币。

诸侯国（王）不仅作为 TKC 的发行单位同时还作为全账本，并保持与其他国账本的同步及验证、信任关系。当此诸侯国（王）失去区块链全体信任后，其州（太守）节点会自动跨越国账本而直接获得其他国账本的同步，同时自动推举出一个州（太守）作为临时的国账本。国账本需与州账本保持实时在线，且根具相关参数决定失效后的代替机制（如上线总时长，掉线概率，稳定性，计算力，带宽质量，全网信任度，等等）

州（太守），作为 TKC 的二级区块链记账系统，能够有效的屏蔽区块链在某一个瞬时交易的糖卡而产生的全网同步而而产生的广播风暴，当一个交易产生时，系统会自动在主干全网广播，由主干形成交易的全网记录，同时本次交易会在该主干所辖的所有节点同步记账。作为国区块链记账系统的二级备份，州（太守）保持本州内所有交易的全账本记录并收取 TKC 交易的管理费用，同时保持与本国内的 12 州的验证与交易的记账同步，并随机与非本国的按一定规则随机挑选的 128 个州的互联验证与交易记录的记账同步，每 3 个月按一定规则随机更新 128 个州的互联，且对上次 128 给予相关规则下的系统自动评分，确保每个州的区块能够在全网监督下稳健运行。

州（太守），同时全权管理所辖郡的虚拟社群的管理和运营，通过对 16 万社群人口的管理，形成稳健的人口市场效率，增加社群纽带关系，建立强势的商品贸易，电商购物，情感交流，创业服务，等等涉及社会人口服务的方方面面的支持。

郡（刺史），作为三级记账点（收取糖卡交易的管理费用），也是区块链电子币交易平台（btc 有 1 万多个交易平台）。发起 p2p 交易的两个端点，交易记录的记账内容一定在交易平台做交易记录，同时该笔交易的所属郡也会同时做一次记录。如果 p2p 直接无平台交易，那么该笔交易的所属郡做一次记录。

郡的交易记账同步仅仅在本州内实现为主。郡作为三级区块，每笔交易都会有其 TKC 所属的区块，或者所在交易平台发起验证和记录。每个区块与其他区块保持国内的全网状链接关系。

这种立体分级化的记账同步管理优于，传统的区块链技术实现的平面化同步管理，避免了整个链系统的频繁的大规模的广播风暴。提升了记账效率，和交易效率，能够真正意义上实现社会化网络所需求每用户每日无限次数的高效交易和各类合约服务。

悠唐区块链系统的发展

悠唐区块链系统实际是区块链技术的混搭的综合解决方案,这种混搭的解决方式将区块链的直链方式改为分级全网状互联，将社会的人和区块链技术的数字货币和数字合约相结合，从目前的区块链行业所遇到的瓶颈来看具有绝对的发展优势。

区块链技术是继工业革命和互联网革命之后有可能引发技术和产业变革的颠覆式创新，但在实践中仍存在着处理性能、隐私保护和升级修复机制不足等一系列问题。任何一种技术都不能包治百病,在新技术高速发展过程中,如单纯为了区块链而区块链,反而是削足适履；雾里看花更需保持清醒,区块链技术应用应契合其技术特点,找到明显优于传统技术的适用场景，与其他技术结合，发挥改良作用，进而实现架构最优。

目前有人大力推崇“去中心化”，大多是对一些中心化运行模式的协作效率、数据一致性及可靠性有所担虑,还有少数人曲解区块链的分布式架构等同于去中心,简单分析,物理分布与逻辑统一并不矛盾,有管理的分布式架构系统才有充分的运行责任兜底,比特币表面上看去中心化,实际上少数矿池拥有大多数算力,无管理状态下也存在较大道德风险和隐患。单从技术价值分析，区块链作为一种技术不是为了“去中心”而存在，而是提供了一种对原有“中心化”重新定义及优化的途径，所谓“去中心化”分布技术体系与传统“中心化”技术体系在架构复杂度、资源投入产出比、数据一致性、效率等方面各具优势，因此，对于一些规模较大、以中心化管理为主的主辅式多元业务生态，要兼顾运行效率、多点数据一致、失效恢复及业务补偿等特性,可将区块链作为原有中心化架构有益补充去分层混合构建整个可信环境，而不是简单的“去中心化”走向另一个极端。在日常技术实践中也往往将两类架构混合使用，如涉及大量信息读写，为提升效率控制成本，往往将关键信息或密钥上链，海量信息还存在中心化管理节点上,这种机制也能较好的保护信息安全,回避敏感信息全网分布带来的泄露风险，实现两全。

从应用层面来看，数字化资产（如比特币）从产生开始就一直在链上，区块链可以覆盖其业务全生命周期，区块链建立的这个技术上的可信环境天生是数字化的封闭系统，但现实大多数业态涉及的还是线下实物资产，如果这个封闭系统没有可信机构或某种机制来背书、管理，就无法保证实物资产进入这个封闭系统之前的真实性。有些业务场景要时刻做到“账实相符”，链上链下随时同步，难度将更大，这也是悠唐区块链系统能够带来的改变，能够结合多种技术及机制组合并用。这种复杂场景下，实现链上链下的集成与交互，可以算是另一种形态的 O2O（onchain　2 offchain）。

因此，区块链技术与其它技术的组合应用，实现链上与链下信息同步和可信入口，能够解决目前区块链接技术所遇到的所有瓶颈，形成未来新兴商业模式或技术风口。

通过悠唐区块链技术的不断演进与发展，下一步将与物联网、智能化、大数据等技术深度融合，成为互联网时代的新引擎，会给世人不断的超预期体验与惊喜，值得我们积极拥抱、共同见证。

悠唐天下 TKC

常常

18621802600