LEXEL 链锁

基于区块链的芯片级
数字身份认证硬件基础设施

白皮书 V2.0

www.lexel.io

LEXEL

提供完整的个人数字资产

安全保值与增值解决方案

www.lexel.io

概述

当前互联网的验证操作，无论是登录密码、资金密码亦或是短信验证码等等，黑客都可以通过程序截取甚至模拟。很多硬件层面的加密也只是内存级别，同样可以截取并模拟。互联网、物联网、区块链等多领域都存在严重的安全问题，且形势越趋严峻。

LEXEL 是数字身份认证与数字资产安全解决方案提供商，基于区块链技术为用户提供个人身份认证与信任公链，并提供完整的个人数字资产安全保值与增值解决方案。可应用在个人可信数字身份，数字资产钱包与数字货币交易所等场景。

当前互联网与金融行业数字认证（CA）应用广泛，但传统数字认证基于中心化企业作为认证机构，面临信息滥用、内部管控等各种风险，也造成各家认证机构各自为政，无法被完全信任。

当前区块链技术引领的价值互联网，需要一个可信的个人身份识别体系作为价值交换的底层基础，基于这个基础，才能进一步拓展个人与机构，个人与个人的可信价值交换，LEXEL致力于成为价值交换的底层基础，为区块链应用场景的繁荣，提供可信的底层身份认证信任公链。

基于 LEXEL 的身份认证信任公链，还为用户与机构提供完整的数字资产安全解决方案，保证数字资产的安全。更进一步，LEXEL将面向未来，发展数字资产增值生态，在公链上建立智能合约，完备的解决数字资产交换问题，促进个人与个人，个人与机构之间信贷，投资生态建立。

目录

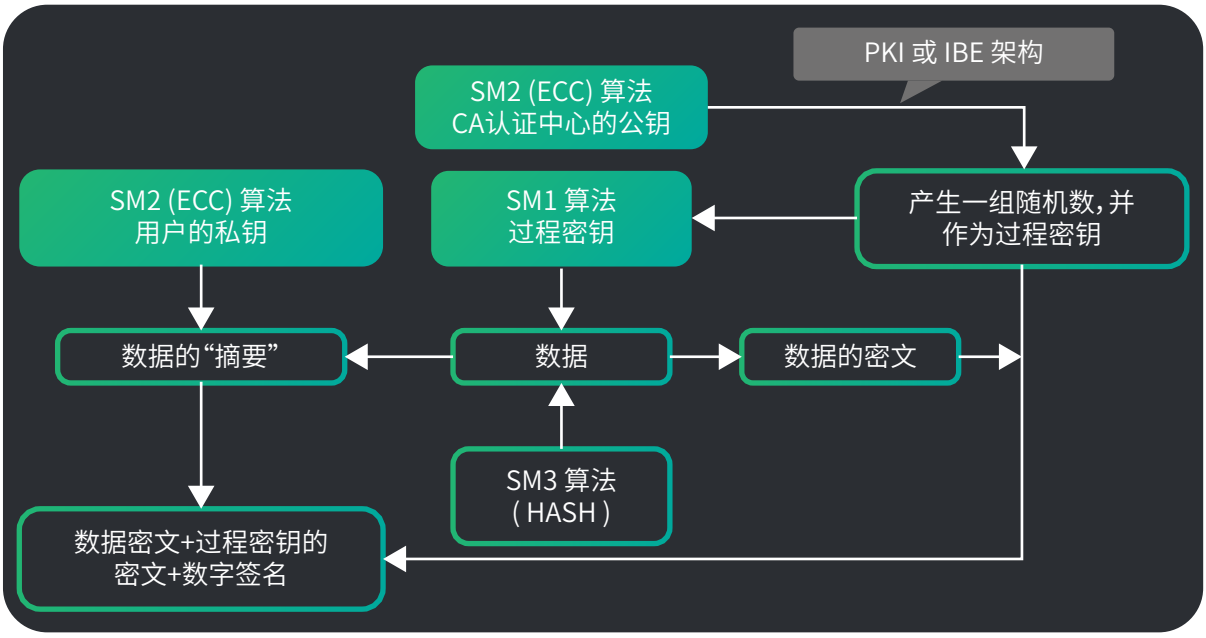
1. 市场概述

1.1 市场背景

20世纪80年代，美国学者提出了PKI（公开密钥设施）的概念。为了推进PKI在联邦政府范围内的应用，美国在1996年成立了联邦PKI指导委员会;1999年，PKI论坛成立;2000年4月，美国国防部宣布要采用PKI安全倡议方案。2001年6月13日，在亚洲和大洋洲推动PKI进程的国际组织宣告成立，它就是“亚洲PKI论坛”，其宗旨是在亚洲地区推动PKI标准化，为实现全球范围的电子商务奠定基础。

什么是PKI?

PKI是Public Key Infrastructure（公开密钥基础设施）的缩写，是一种普遍适用的网络安全基础设施。一些美国学者把提供全面安全服务的基础设施，包括软件、硬件、人和策略的集合叫做PKI，但我们的理解更偏重于公开密钥技术。



▲ PKI 认证架构逻辑图

数字证书是PKI中最基本的元素，所有安全操作都主要通过证书来实现。PKI的部件还包括签署这些证书的认证机构(CA)、登记和批准证书签署的登记机构(RA)以及存储和发布这些证书的电子目录。除此之外，PKI中还包括证书策略、证书路径、证书的使用者等。所有这些都是PKI的基本部件，它们有机地结合在一起就构成了PKI。

可提供的服务

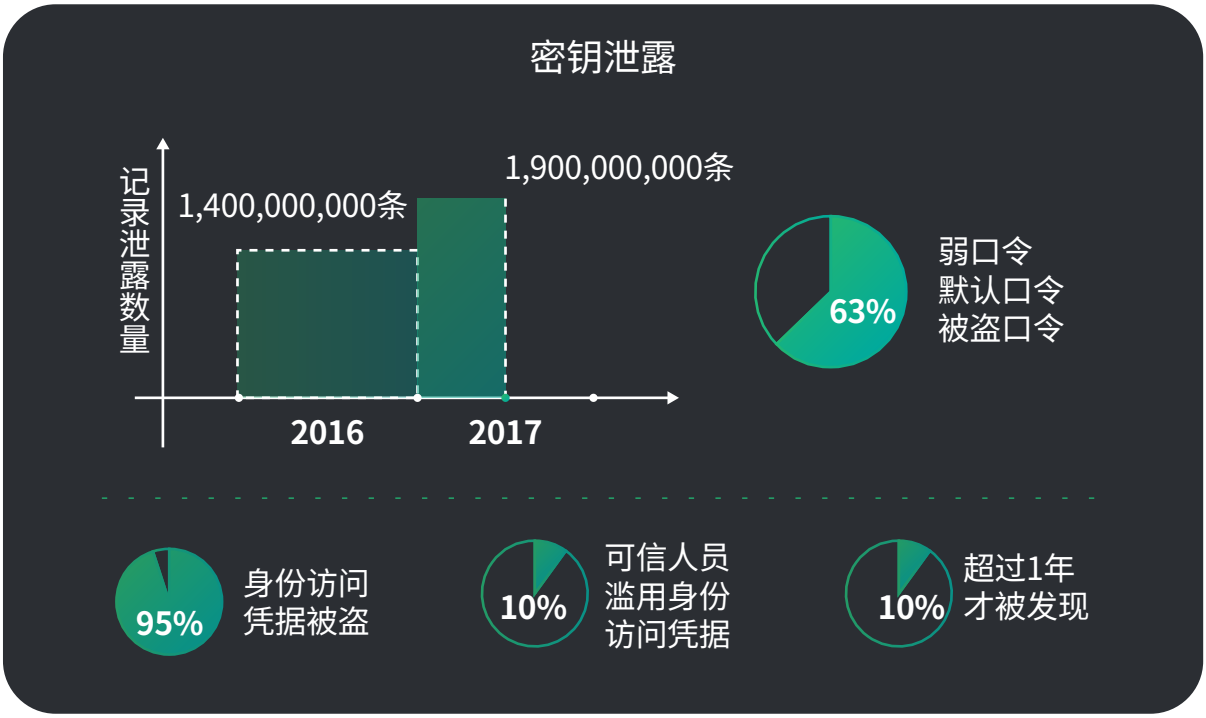
PKI已经广泛应用在金融、电子政务等领域，如网上银行使用数字证书确定使用者身份、企事业单位信息系统使用基于硬件的USBKEY或IC卡进行身份鉴别及其他信息保护等。其中在安全电子邮件、web安全应用（SSL/TLS）、VPN、IP/sec与电子商务上的应用尤为突出。

1.2 存在的风险

PKI的安全包括太多的方面，包括设备安全、运行安全、协议安全等。尽管PKI有如此多的应用场景，但PKI存在几大致命问题：

• 安全性低

在当今的互联网中，服务器认证用户的主要方式是密码系统。用户在首次使用网站时创建密码，以便在随后的访问中确认其身份。市面上数字签名认证大都属于软件级别与内存级别的加密，密码容易被黑客模拟或者盗取，用户信息与资金存在较大风险。包括密码较弱，密码过于复杂，每个站点需要一个唯一的密码，以及恢复被遗忘密码的不便。



• 性能不足

PKI技术是基于RSA加密算法，需要建立CA数字认证中心，采用第三方参与的方式，密钥采用分散生成集中存放方式。随着用户的增长，与满足加密安全性的要求，PKI只能延长RSA算法的密钥。陷入数据库数据量愈发庞大，运行速度愈发低下的死循环。

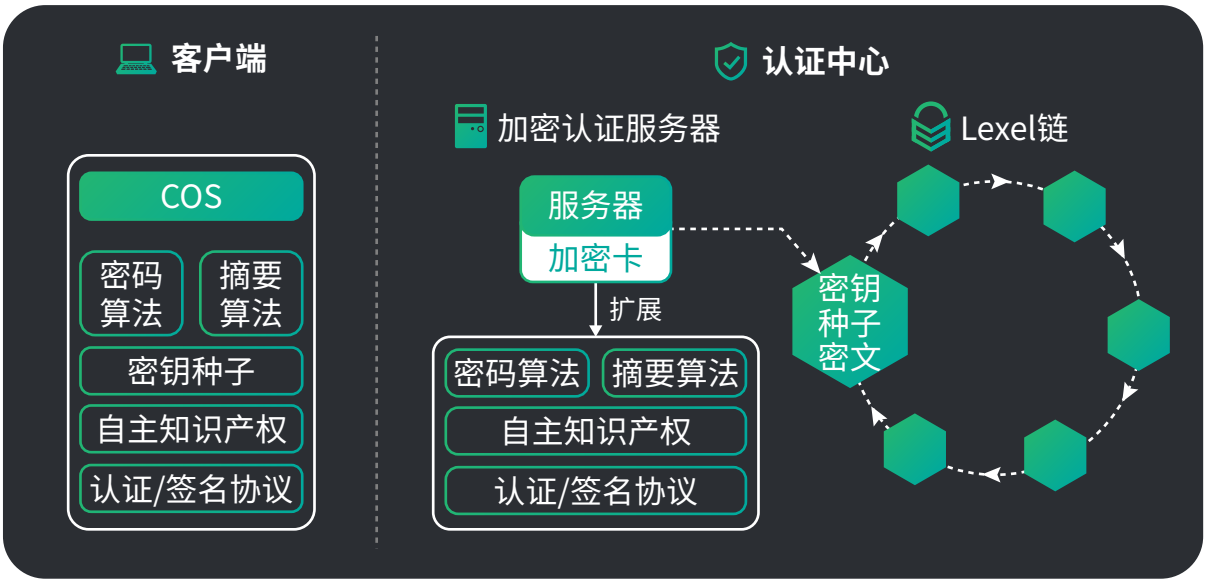
• 成本偏高

PKI的认证过程需要庞大的证书数据库进行在线比对认证。每 1000多用户，就要建立一级CA及一套数据库存放证书与密钥，数据库在线比对认证速率低，管理用户量小。同时由于庞大的数据库与服务器架构，需要大量的运维人员去保障设备的安全，运营负担沉重。

2. 关键技术优势

2.1 LEXEL 数字加密与安全认证技术

LEXEL 体系是由身份认证、数字签名、密钥交换和数据加密协议组成。通过采用自主产权算法（如：密码算法、摘要算法），完成身份认证、数字签名、密钥交换和数据加密等4种功能。



▲ 加密芯片架构

其中的技术关键在于，如何解决单钥密码算法的密钥管理世界性难题。主要具备以下特性：

2.1.1 自主可控性

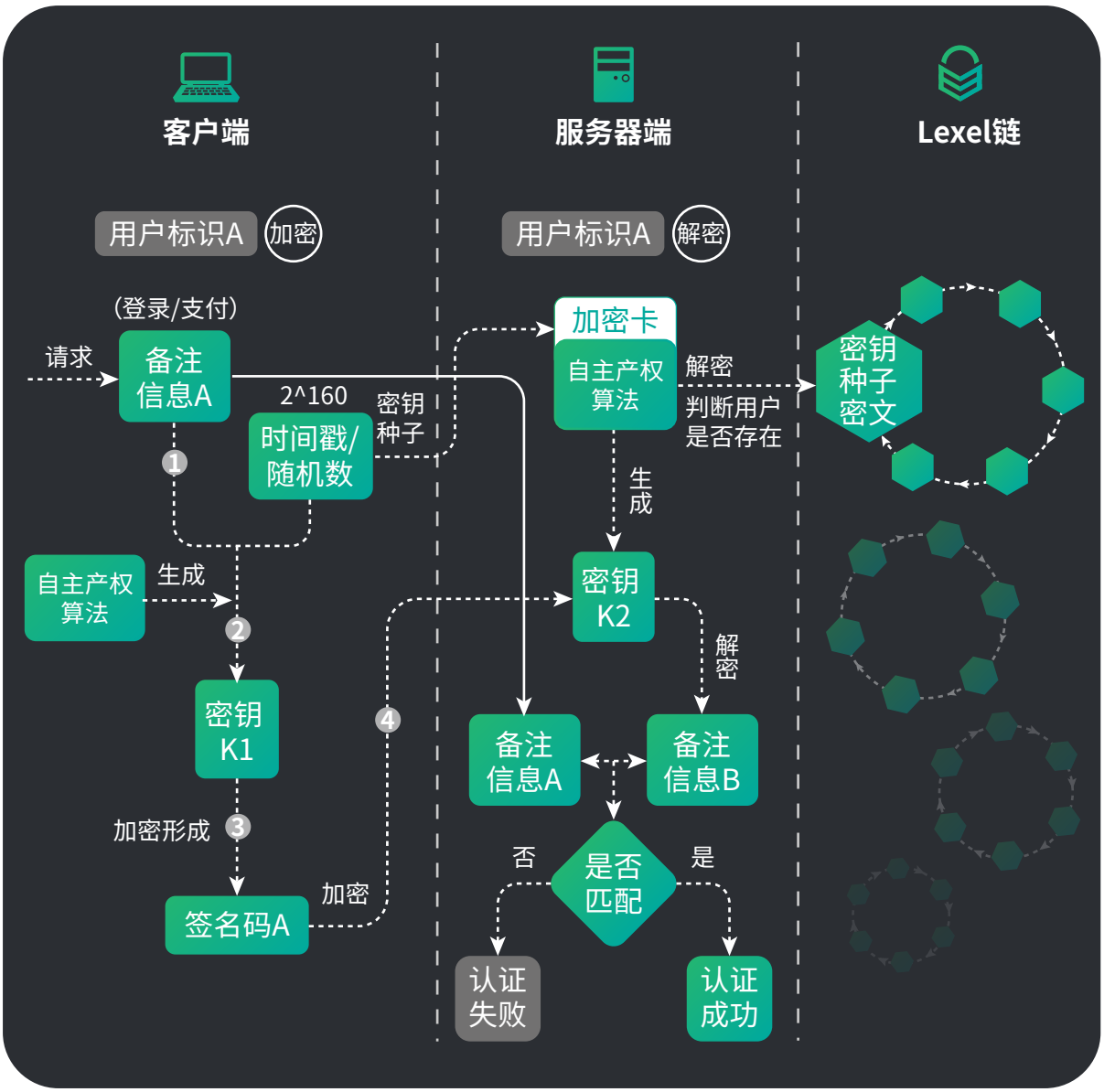
自主可控就是依靠自身研发设计，全面掌握产品核心技术，实现信息系统从硬件到软件的自主研发、生产、升级、维护的全程可控。LEXEL 100%采用自主开发技术，从加密设备到算法，操作系统到数据库，均采用国家级标准，是真正实现产品从硬件到软件等个个环节都做到自主、可控。

2.1.2 与传统认证技术对比的先进性

(1) 架构对比

PKI等传统认证技术采用需要用2套算法，2+3次算法及调用，完成标准认证流程，密钥与设备固定匹配；而 LEXEL 调用1次单钥算法，即能完成所有认证流程，并且通过芯片计算，做到密钥一次一变。

LEXEL 不仅简化了认证过程，大大提高了认证速度和并发量，更保证了认证安全性。



▲ 加密与解密过程原理图

(2) 参数对比

性能/认证模式	LEXEL	PKI或IBE（国外技术）
安全性	高（芯片级认证）	低（内存级认证）
认证\签名速度	比PKI或IBE快100倍-200倍	慢
认证中心管理用户量	已证实案例达3亿， 理论可达十几级	无法保证千万数量级 以上的良好运作
认证中心建设成本	比PKI或IBE少80%	高
系统维护人员	比PKI或IBE少70%	多
核心技术	自主可控	半自主，不可控

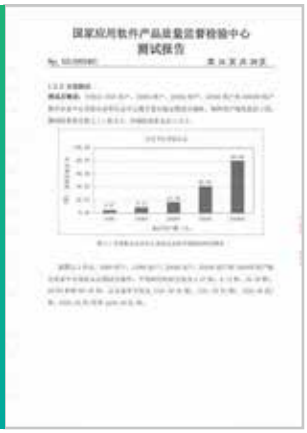
(3) 国际对比

2011年初，奥巴马政府为实施“网络身份证”国家战略，拨款5.63亿美元新技术研发经费（比15年用于航天发动机研发费用高一倍多）。期望研发新技术建立美国3亿人口体量的网络ID，但至今，新认证技术仍未问世，由于传统认证技术的代表PKI/CA及IBE体系无法做到大并发量的商用要求，美国这一国家战略受到传统技术“短板”的制约而失败。

通过 LEXEL 技术，以3亿用户为基础，建立一套 LEXEL 系统。经《软件产品质量检测中心》检测，该系统运行良好，足够支撑3亿用户使用，并发认证达到1228.50次/秒，并发签名验证达到823.93次/秒，各项指标均优于传统认证中心的上限指标。

足够支撑 3 亿用户使用

并发认证 1228.50 次/秒



并发签名认证 823.93 次/秒

2.1.3 技术评价、技术奖项与技术专利

LEXEL 技术已获得13项发明专利，系统检测结果均为国际领先水平，并获得中科院院士高度书面评价，通过专家组论证获得密码学顶尖专家团队的高度认可，并给予 LEXEL ——“技术领先欧美至少十年”的评价。

业内国际大奖

《英国金皇冠奖》
英国国际发明博览会最高荣誉

《韩国国际发明铜奖》
韩国国际发明展大会铜奖

《中国国际发明金奖》
中国国际发明展览会最高奖

专利资料

LEXEL 加密技术所获得的发明专利清单，共13个如下所示：

No.	专利内容	数量（个）
1	密码算法发明专利	2
2	数字签名发明专利	1
3	密码防盗发明专利	2
4	数据传输发明专利	1
5	网络身份认证发明专利	1
6	手机认证发明专利	1
7	物联网认证、加密传输和控制发明专利	3
8	银行卡防盗加密发明专利	1
9	VPN加密发明专利	1

2.2 LEXEL 的区块链核心技术

LEXEL 的区块链核心组件包括区块链基础设施、区块链协议、密码学算法等，具体而言有P2P网络通信协议、分布式计算技术、分布式存储技术、加密算法和隐私保护算法、密钥管理机制、共识机制、智能合约、标准代币协议、钱包SDK等技术。以下，我们将挑选LEXEL的重点创新模块进行阐释。

2.2.1 DPOS+BFT并行

（1）现有区块链底层的性能无法支撑商业级应用

区块链作为一套去中心化的解决方案，其核心在于共识与治理方式。比特币诞生时间较早，估计发明者本人最初也未曾考虑过比特币的流通范围竟然能遍及全球，因此采用的POW工作量证明机制，要求每个节点都参与竞争式记账（挖矿），每一个记账节点都需要通过处理交易、维护全系统的备份，且节点还无限制地开放，导致区块链的节点网络逾日臃肿。

区块链网络拥堵造成三个显而易见的恶果，其一，吞吐量极低。比特币形成一个区块的时间是10分钟，以太坊形成一个区块的时间是14秒左右。例如在以太猫应用上线的高峰期，以太坊积累了数百万条未确认交易，仅仅一个智能合约的小应用已经无法承载，这也是公有链应用迟迟未见落地的主要原因。其二，手续费极高。由于记账节点（矿工）处理能力有限，只能优先处理支付了高gas的交易，竞争之下，每笔交易的手续费水涨船高，导致高频率的应用丧失成本优势。其三，实质形成财力中心化。由于挖矿难度增加，算力逐渐集中，能源被大量浪费，记账者开始以财力换取算力，矿机集中形成矿池，本意是去中心化的比特币已沦为大矿池垄断的工具。

因此，公有链在2018年的最关键需求便是性能的提升。一方面，既要求新一代的公有链基础设施能像Google、Facebook、阿里巴巴一样，能支持千万级乃至亿万级的活跃用户，支持并行计算及实现高效率低延迟的交易；一方面，又要求能低成本甚至零成本地让个人用户享受到区块链应用的好处，从而帮助Dapp生态发展出更大的用户规模、扩大用户使用频率、提高商业利

润;另一方面,还要求能让区块链生态的创建者与最初的加入者受益最大化,而非被富有财力的后来者轻易掠夺。

(2) LEXEL 的共识设计

共识机制是区块链系统中各个节点达成一致的策略和方法,是商定确定性交易顺序和过滤无效交易的过程。可类比现实社会中,通过全民通过逐级的投票和评选,最终选出国家或企业领导人的过程。

在共识机制的设计层面,需要重点考虑公平与效率的均衡。公平性要确保所有的参与者都拥有记账的权利,效率要求并不是所有的参与者无时不刻都要参与记账,而是可以通过投票方式选择代理人。最终,共识机制需要满足业务场景对资源利用性、响应时间、处理时间、吞吐率和最大极限负载容量的要求。因此,LEXEL 在比较了POW、POS、BFT、DPOS等多类主流共识算法后,最终选择采用DPOS共识。

DPOS全称股份授权证明机制(Delegated Proof of Stake),通过引入“受托人”这个角色,降低过度竞争带来负面影响,将记账能力赋予专业化机构。LEXEL 赋予了给持币人的持币份额对应的表决权,而不是直接进行挖矿的记账权。通过每个人持币的比例与其拥有影响力的映射,体系的去中心化与民主得以达成。每个持币人可以将其投票权赋予一名记账代表(在项目前期,基金会将对记账代表节点进行认证及甄选),获得票数最多的前一百位代表按照既定时间表轮流产生区块。

LEXEL 的DPOS共识算法旨在将主流主权国家的决策机制(如众参议院、人民代表大会制等)引入区块链系统,优点在于可以大幅缩小参与验证和记账的节点数量,实现几秒内完成共识,同时提升效率、节省能源和确保公平。

LEXEL 的DPOS的工作原理如下:

第一,在正常操作模式下,块生产者每3秒钟轮流生成一个块。假设没有人错过自己的轮次,那么这将产生最长链。块生产者在被调度轮次之外的任何时间段出块都是无效的。

第二,在少数分叉情况下,不超过节点总数三分之一的恶意或故障节点可能创建少数分叉。在这种情况下,少数分叉每9秒只能产生一个块,而多数

分叉每 9 秒可以产生两个块。这样，诚实的 2/3 多数将永远比少数（的链）更长。

第三，在离线少数人多重生产情况下，（离线的）少数人可以试图产生无限数量的分叉，但是他们的所有分叉都将比多数人的那条链短，因为少数人在出块速度上注定比多数人来的更慢。

第四，在网络碎片化情况下，导致没有任何分叉拥有多数块生成者。在这种情况下，最长的链将倒向最大的那个少数群体。当网络连通性恢复时，较小的少数群体会自然切换到最长的那条链，明确的共识将恢复。

第五，在在线少数的多重生产情况下，少数节点B在其时间段内产生了两个或更多可供选择的块。下一个计划生产者（C）可以选择基于B产生的任何一种方案继续构建链条。一旦如此，这个选择就成为最长的链，而所有选择B1的节点都将切换分叉。少数不良生产者企图广播再多的替代块也无关紧要，它们作为最长链的一部分永远不会超过一轮。

此外，在缺乏明晰的生产者法定人数这种低概率的情况下，少数人还是可以继续出块。利益相关方可以在这些块里包括更改投票的交易。这些投票可以选出一组新的生产者，并将出块参与率恢复到100%。一旦如此，少数链将最终超过所有其他以低于100%参与率运行的链。

归根结底，LEXEL 的DPOS甚至在面对相当数量生产者舞弊的情形时也是安全的。因为社区可以投票替换掉不合格的生产者，直到恢复100%参与率。这同时又能确保不断优化诚实节点的数量，从而使得DPOS有能力在平均只有1.5秒的时间内以99.9%的确定性确认交易。

LEXEL的BFT共识机制进行了定制，实现秒级出块，具备高一致性、高可用性，抗欺诈能力较强。

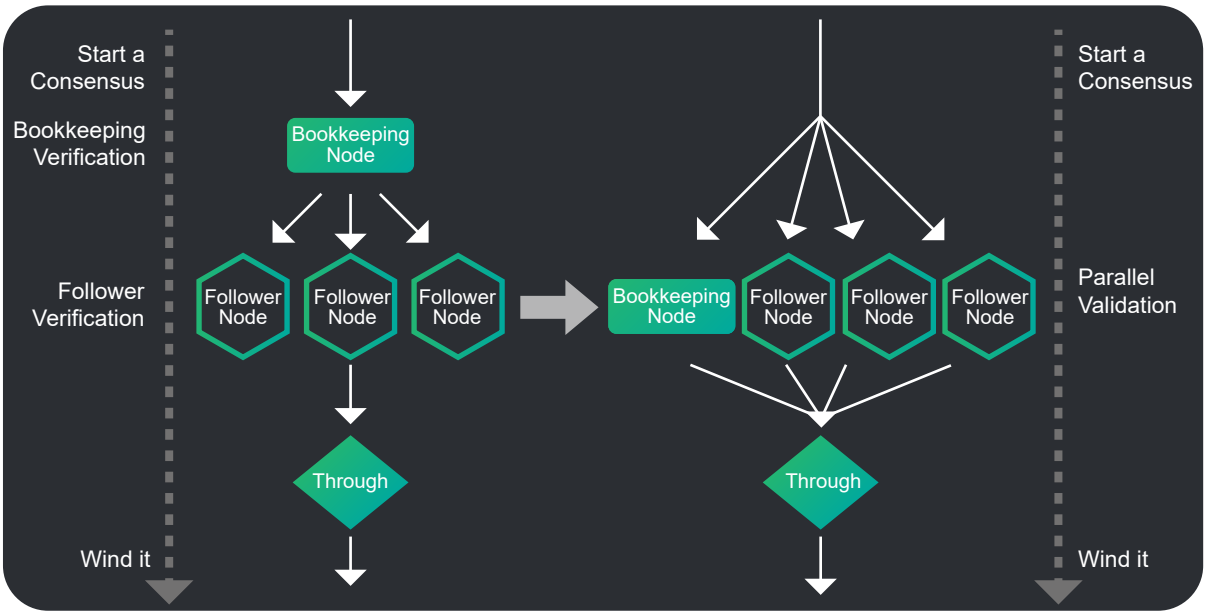
BFT算法的过程是一次提案，几步投票直到最终确认，在这个过程中有复杂的状态机维护过程，投票往返步骤较多，且部分流程在节点内部以及节点之间是串行进行的，每一步都会需要互相等待，在其他上一阶段的计算完毕或网络通信收集数据完成，达成阶段性确认后再进入下一阶段。

由于流程复杂，数据往返较多，共识过程也容易受网络波动影响，对网路

延迟和丢包比较敏感，在状况不理想的网络和计算环境可能需要多次共识的尝试才能达到最终一致性。

以上的技术挑战给系统带来的影响是，系统并行能力可能遇到瓶颈，或者交易的确认速度会偶发性延长。所以我们对BFT算法进行了深度的优化。

在LEXEL中，首先我们对共识过程进行了深入分析，按计算步骤，节点等维度进行分解，尽量让所有的节点在每个阶段的计算都是并行进行的，无论是议长节点还是投票节点，一个节点在运算验证一批交易的过程中，其他所有节点也在同步运算和给出投票，不需要互相等待。



▲ 并行BFT共识流程

然后，我们对耗时较高，有次数冗余的计算过程进行了精简，通过关键路径优化，重复计算结果进行缓存等方式减少了共识过程中的每一步的耗时。

同时，我们对网络健康度、节点存活等因素进行检测，当发现有的记账节点无法服务时，快速切换到下一个记账节点，避免出现全体节点出现空等待的状况。

最后，我们考虑到金融交易的场景常常有高峰期和空闲期的特点，在空闲期系统没有交易流量的时候，共识机制进入心跳状态，只维护网络的健康状态，不产生包含交易数为0的空区块数据，避免不必要的存储浪费，以及避免空区块的同步流量和时间消耗。

2.2.2 更安全的隐私保护算法—零知识证明

(1) 现有公有链的伪匿名及数据隐私泄露问题

比特币一直以完全匿名作为最大的卖点，但现实是，在大数据及监管科技工具之下，大部分的比特币账户也是可以被完全追踪的。虽然只要钱包地址不与个人法币账户连接在一起，一个人就可以一直保护自己的隐私，但只要一旦在中心化的交易所中进行交易或提现，这个秘密就暴露了。目前，美国的执法机构已能够在调查过程中识别特定的比特币用户。另一方面，由于数据在公共账本中完全暴露，导致例如电子病历、身份验证数据、凭证管理、财务文件等一些需要强隐私的应用场景无法在公有链网络中实现。

因此，在新一代公有链的隐私保护技术层面，需要重点考虑其安全需求。这可从保密性、完整性、抗抵赖性、可追溯性和真实性等角度入手。其中，保密性指区块链系统确保其数据只能被授权用户访问的能力程度；完整性指区块链系统防止未授权访问、篡改程序或数据能力程度；抗抵赖性指区块链系统针对活动或事件发生后可以被证实且不可被否认的能力程度；可追溯性指区块链系统对每一个使用者的活动可以被唯一地追溯到该使用者的能力权限的程度；真实性指区块链系统对目标或资源的身份标识确实能够证实该目标或资源的能力程度。

(2) LEXEL 的零知识证明隐私保护算法

零知识证明是证明者在不向验证者提供任何信息的情况下，使得验证者相信他们拥有一些秘密知识。换句话说，一个程序可以有秘密的输入，证明者不会向验证者揭示任何东西。零知识证明提供了可用于构建隐私保护机制的基础。零知识证明在区块链隐私保护中的作用越来越重要。目前，在数字货币中尝试使用零知识证明解决交易双方的隐私问题。但是在应用模型上，已有的零知识证明方案只针对比特币的UTXO模型，且很难推广到以账户模型为基础的新型区块链中，因此也制约了其对智能合约的支持。现有的零知识解决方案在生成证明时，先将证明内容转化成门电路的形式，该过程需要消耗大量的计算资源和时间，因此证明只能在计算能力充足的节点（比如矿工节点）才能生成，这大大限制了其适用场景。

为了加强匿名保护与隐私保护，LEXEL 拟将引进借鉴ZCASH的零知识证明技术以提升隐私保护强度。该零知识证明协议包含三个算法：KeyGen，Prove和Verify。KeyGen是一个随机算法，输入公共参数，输出证明密钥pk和验证公钥vk；Prove算法输入证明公钥pk,实例x以及证据a，输出一个零知识证明π；Verify算法则输入验证密钥sk,实例x以及证明π,输出一个判定比特。零知识证明协议可以说服系统中的所有人相信，交易是正确进行的。但在账本中不记录交易地址，而只记录由地址计算出来的序列号。这样就隐藏了交易的用户，起到保护隐私的作用。由于序列号是由交易地址经过哈希函数计算得到，根据哈希函数不可逆的性质，没办法逆推出交易地址，从而无法关联同一用户的两个或多个交易。

此外，在区块链本身的非对称加密方面，LEXEL 通过通用的哈希摘要算法，通过在区块中记录上一个区块的哈希值，确保了被记录数据的不可篡改，并对数据完整性给予保护。对于给定的数据明文和哈希，LEXEL 可以验证该数据明文是否被篡改。为了防止区块链的各方对记录的数据进行抵赖。LEXEL 强化了数字签名功能，用以确认数据单元的不可伪造性，即：确定消息确实是由签发方签署的。流程上，首先由签名者用私钥对信息原文进行处理生成数字签名值，然后验证者将利用签名者公开的公钥针对数字签名值和信息原文验证签名。

2.2.3 更丰富与多样化的智能合约应用

LEXEL 的智能合约参考了以太坊设计思想，提供一个图灵完备的智能合约平台，让开发者都可以编写任意逻辑的程序。LEXEL 将定制一个用于执行合约代码的虚拟机，智能合约的开发者可使用Solidity语言进行开发。LEXEL的CALL和CALLCODE指令的目标地址通过栈来传递，使得合约可以在运行时动态调用其它的合约代码，使合约的调用路径变为非确定性。而智能合约可以访问到的数据都是确定性的，使得所有节点在动态调用目标代码时一定会获得相同的目标地址，保证了系统的一致性。

针对目前智能合约较难进行形式化验证的问题，一方面，LEXEL 将尽可

能支持一些容易验证的编程语言，例如Haskell和OCaml这样的函数式语言会比C / C ++、Java和JavaScript等命令式语言更适合智能合约代码，因为它们的结构更容易推理和形式化验证。一方面，在智能合约的样板建议中，使用解释而非编译型语言，实际代码在区块链上可见，并且可以轻松检查。最后，代码永远是难以完美的，LEXEL 将加入一定的基金会层面的治理机制，为智能合约的升级、迭代、弥补漏洞提供一个合理的机制。

针对以太坊智能合约技术存在开发友好度不足的问题，LEXEL 将进一步深化开发出智能合约的管理器，并加入智能合约命名模块，从而更加便于开发者进行智能合约的版本升级及命名管理。

2.2.4 SDK工具

为了帮助更多的生态合作伙伴轻松接入LEXEL链锁使用，LEXEL还将提供SDK工具，同时支持java和node.js两种开发语言。在SDK基础上，合作伙伴的开发者可轻松开发DAPP。届时，生态合作的伙伴的客户只需调用链上节点的功能接口，在客户端上即可以访问链上部分或全部的数据，向区块链发起交易等。

在SDK的设计上，提供了简易的接口，开发者只需关注具体DAPP的数据字段以及调用返回结果，而并不需要了解区块链节点的具体部署情况，即可实现业务合约的管理、执行、交易查询功能。这样可以大幅度降低生态伙伴的开发门槛和成本，快速开发各种业务场景的应用。

2.2.5 LEXEL 的区块链技术先进性

LEXEL的技术先进性可以从业务场景适用性、架构设计合理性、计算能力完备性、高速共识效率、超强加密与隐私安全性、可追溯与可审计性等多个维度中体现。

业务场景适用性——LEXEL将以提供更安全的基础设施及原生币的广泛应用为核心，深度改变数字货币行业的安全痛点，与传统PKI不同，LEXEL将以真实的业务场景需求为导向，保障业务流程的可靠性、时效性、稳定性。

架构设计合理性——LEXEL未来拟对链上有价值的可信大数据进行容灾设计，实现系统、数据和链路的冗余备份，保证系统的可靠性和可用性，即便某个版本智能合约或DAPP的代码出现漏洞，也不至于受到毁灭性影响，保证项目的高可用性。

计算能力完备性——价值可编程是区块链技术的一个重要的本质属性，直接决定了技术对业务逻辑的表达能力，计算能力的完备性具体体现在“智能合约”上。

高速共识效率——采用了当前最为领先的高性能DPOS共识算法，基金会将对共识节点的配置建立高标准要求，实现秒级出块，最高可支持百万量级的交易并发。

超强加密与隐私安全性——涉及用户重要隐私的数据需经过隐私保护处理，区分为隐私敏感信息与公开信息。由于采用了硬件与软件加密技术相结合，真正确保了用户的信息隐私保护及资产确权，任何未受授权用户都无法将被保护的信息解密，而只能阅读公开信息。

可追溯与可审计性——通过区块链技术的不可篡改和时间戳特点，可支持基金会进行监督管理、核查审计全部记录并作为相关的法律纠纷证据。

2.3 数字加密与区块链的结合

传统PKI 技术中，CA中心（Certificate Authority，证书认证机构）是信任的起点，只有信任某个CA，才信任该CA给用户签发的数字证书。但在具体应用中，PKI 技术存在如下问题：

- 单点失败问题：处于核心的CA极易遭受攻击，一旦被控制，CA根证书以及该CA 已经签发的证书都不再可信。
- 多CA互信难问题：用户证书只能由所属CA的根证书进行验证，不同CA之间不能相互验证，现有CA互信解决方案适用性受限。

LEXEL结合区块链技术的分布式数据存储与共识机制等特点，实现去中心化认证的方式。因此，LEXEL与区块链结合有以下几点优势：

1) 验证节点如果遇到技术故障或遭受恶意攻击，LEXEL不可能遭受全系统服务中断。此外，用户不可能在单一机构的突发事件下将其账户全局暂停；

2) 企业或者个人在使用验证加密技术时，无需向传统PKI的第三方CA申请证书或者独立部署CA系统，只需要加入到LEXEL链的生态即可；

3) 结合DPOS+BFT共识，保障安全性，同时保证了TPS。

另外在当今的互联网中，服务器认证用户的主要方式是密码系统。用户在首次使用网站时创建密码，以便在随后的访问中确认其身份。缺点包括密码较弱，密码过于复杂，每个站点需要一个唯一的密码，以及恢复被遗忘密码的不便。保护网络连接的最常见机制是SSL。除了服务器证明其真实性外，SSL还在客户端和服务器之间建立加密连接。但是，如果攻击者可以通过使用假浏览器根证书将自己添加到用户浏览器的受信任用户列表中，则可以中断安全连接。在公司网络中，管理员可以将证书添加到受信任用户列表中，然后在https连接中组织一个“中间人”攻击。

LEXEL加密芯片是一个独立的系统，他采用其自主产权算法结合用户标识字段，以及行为备注信息来自动提取用户信息一填写网站上的用户配置文件，包括付款到客户制定的帐号。分布式的算法，通过允许网站配置文件自动填充来补充的无密码登录。实现所有帐号登录密码在安全的环境下一键式登录，用户无需记录任何信息——芯片在手，通行我有。

3. 商业模式与应用场景

3.1 商业模式

LEXEL 作为一个去中心化的解决方案，由 LEXEL 基金会主导项目进展与开发者社区维护，专注于身份认证信任公链的开发，并通过技术支持与投资的方式，推进基于LEXEL 链上的落地项目。

LEXEL 身份认证信任公链设计有自己的 Token ，除作为 GAS 消耗外，Token 可应用于身份认证信息修改、智能合约建立与维护、数字资产质押、数字资产纠纷申诉与仲裁等场景，对应场景产生的 Token 消耗将作为奖励提供给公链上的应用开发者，矿工，让 LEXEL 身份认证信任生态更加健康。

作为基础公链，公链上能够存储完备的身份信息，信用信息，提供身份认证解决方案，与基于场景的智能合约与图灵完备的合约编程语言言。此外作为一个见见证人网络，会设计完备的去中心化认证机制，防范网络被攻击的可能性。据此成为价值互联网个人身份认证信任的底层基石。

基于 LEXEL 身份认证信任公链，LEXEL 同时提供完整的数字资产安全解决方案，使用 LEXEL 独有专利的数字加密与安全认证技术，将传统的数字资产钱包私钥存储方式进行革新，软硬件结合为用户提供更安全有保证的数字资产存储、转账解决方案。

除资产保值外，LEXEL 致力于搭建数字资产增值生态，在链上对接开发者、服务提供商（如数字资产交易所，数字资产量化交易团队，P2P金融理财团队等），搭建个人对个人，个人对机构，机构对机构的数字资产借贷、投资与金金融互助等多种模式的数字资产金融生态。

简而言之，基于 LEXEL 公链，开发者与服务提供商社区，我们致力于成为未来价值互联网的身份认证信任基础链，同时提供最好的数字金融生态，让数字资产推动未来金融发展，具有坚实的基础。

3.2 通证设计

作为价值交换媒介的通证（Token），是 LEXEL 公链上必不可少的一个环节，通证以链上应用的广泛程度直接相关，另一方面也作为 LEXEL 生态通用货币为使用 LEXEL生态服务的人提供价值交换便利。通证的价值保证与应用来自于以下几个方面：

3.2.1 数字货币

- 可信任网络维护：针对见证人网络中的见证人节点进行奖励，保证可信任网络平稳运行；
- 链上价值交换：服务链上各个生态价值交换场景。

3.2.2 应用逻辑

- GAS消耗：网络转账等操作的 GAS 消耗；
- 硬件消耗：官方回收token，兑换成硬件发放给用户；
- 服务消耗：与LEXEL合作的机构/交易所定期提交token给予官方，作为技术服务费；
- 金融场景消耗：金融服务生态中各项资产交易产生的场景消耗。

3.3 应用场景

3.3.1 应用场景之一：个人可信数字身份

当前，全世界各国都在关注个人数字身份ID，如美国、德国、比利时，有些国家甚至有一个专属网络身份。但目前，只有爱沙尼亚基本实现了国家网络身份证体系，成为全球数字化程度最高的国家。但爱沙尼亚只是一个340万人口的小国，其他各国在个人数字身份ID过程中，都遇到了大量级并发的难题。而纵观全球，更是没有一个可以全球迅速认证检测的数字身份ID，因这意味着将实现全球各国的身份证颁发机构、护照颁发机构的统一联网，难度可想而知。

而区块链技术诞生之后，多样化的共识机制与治理验证机制，此前奢想的“让全世界的人来证明你的身份”变为可能。但即便如此，过去比特币、以太坊等公链处理交易的效率过于低下，以及RSA、ECC等非对称加密算法过于繁复缓慢，仍然没有真正可以商用的个人可信数字身份技术和应用落地。

身份的安全认证，就是要确保正确的人能够在正确的时间和正确的原因下正确访问正确的资源。需要通过对账号（Account）、认证（Authentication）、授权（Authorization）和审核（Audit）进行管理，即谁能够在什么时候获得怎样的授权来使用某一个应用或设备，如何去使用这样的应用或设备，以及知道谁在什么时候访问了某些应用或设备等，确保合法用户安全方便使用IT资源。

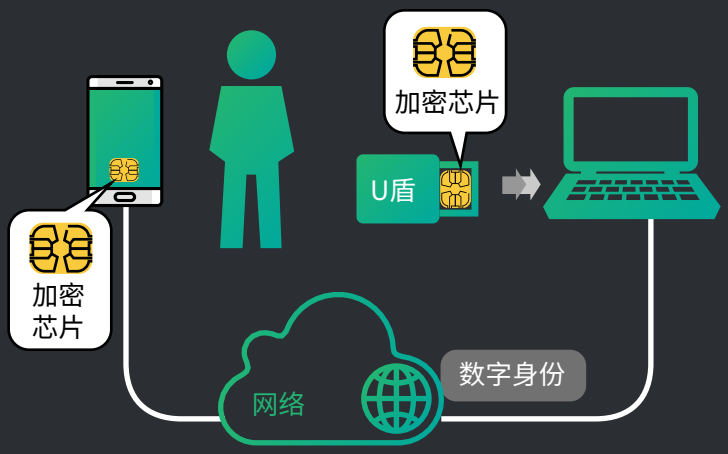
目前，LEXEL通过将加密技术与全新采用DPOS共识算法的区块链技术结合，能够完美的解决海量级交易的并发问题，并实现个人可信数字身份认证的三大功能：

一，实现个人数字身份的创建、上链存储、与数字身份查询验证；

二，将结合硬件设备，实现个人身份与数字资产的绑定，防止黑客盗窃身份，暴力破解数字钱包密码，盗取数字钱包账户资金，全面保护数字财产安全；

三，基于可信个人数字身份的电子签章（签名）、司法存证和证据保全等应用。

以达到万亿级体量的市场为例，即使传统的PKI/CA传统体系能够突破大量级并发和区块链技术落地的难题，其成本也是使用“LEXEL”的5倍以上。



3.3.2 应用场景之二：数字资产钱包

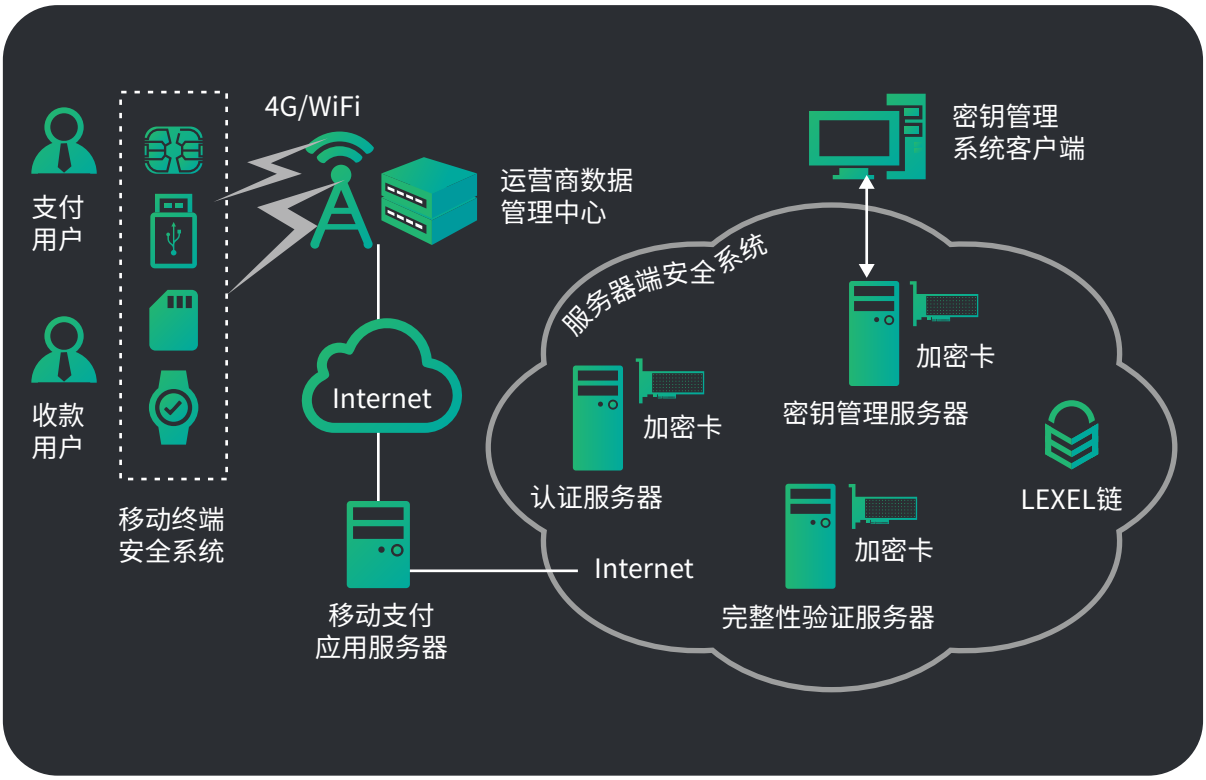
在传统金融场景中，网上银行、手机银行、移动支付已经如火如荼的进入我们的生活。但即便如此，传统金融仍然难以进行高安全级的支付，因此，国家通常采用限制支付的额度来控制风险。大额交易转账仍需通过网上银行及硬件设备来配合实现。

其背后的原理是，移动支付方法都是采用验证码（动态口令）认证模式，如：支付宝、微信、苹果PAY等。动态口令认证模式速度快，操作简单，成本低廉，但其缺少签名功能，黑客可通过截获并替换支付单的内容，实现对移动支付协议的有效攻击，盗取用户账户中的资金。但若采用传统PKI等传统认证技术处理数字签名，PKI/CA认证中心并发签名验证的速度较慢，加上CA认证中心建设成本偏高，市场无法接受。

而在数字货币的世界里，用户仅凭一串私钥，就敢全权管理成万上亿级的数字资产，不仅缺乏数字签名，甚至连动态口令认证的步骤也没有。如此不设防备，加之各类电脑、手机终端中存在无数的漏洞及木马后门，因此数字货币的投资者被黑客盗走数以亿计的资产也屡见不鲜了。

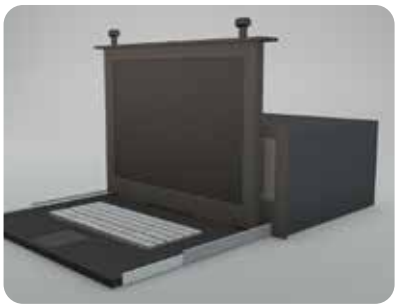
因此，LEXEL致力于改变此严重的行业安全痛点。

“LEXEL”技术本身在传统场景中，就已经实现一次一密和数据加密保证个人信息安全和资金安全，数据加密传输速度能满足2~3亿用户并发不延时。在数字货币场景中，通过与区块链技术结合，首先将个人可信的数字身份存储于区块链之上，再生成对应的密钥，部分存储于区块链账本、部分存储写入于LEXEL的专用硬件中（可支持sd卡、sim卡、u盘、智能穿戴等多类存储设备）。用户在支付转移数字资产时，需通过硬件设备进行验证，黑客即便盗取了数字钱包的密码，也无法将用户的数字财产转移。



3.3.3 应用场景之三：数字货币交易所

近期，数字货币交易所被黑客盗取数字货币资产的事件频繁发生。其大致原因是，黑客通过攻击交易所的大量用户，可以盗走交易所存放在“热钱包”中的代币。通常而言，除了比特币、以太币等大币种，绝大部分币种都没有被市面上的硬件冷钱包支持，一般只能通过普通的密码和多重签名钱包防护，盗取难度极低。


LEXEL通过加密技术，可以把关键的验密过程写入专用硬件中。与LEXEL合作的数字货币交易所，可以要求所有与热钱包有关的操作（包括但不限于管理员登录与操作权限变更、热钱包用户的访问登录、代币资产提取、币币交易等）都需要一步连接专用硬件进行验密的过程。由于黑客无法获得硬件信息，即便破解了交易所用户设置的所有密码，也无法将数字资产转移盗走。

3.3.4 应用场景之四：LEXEL 链锁生态

基于 LEXEL 安全与海量并发的基本特性，形成链锁的自由生态。通过智能合约形成信用机制，给予用户使用 LEXEL 生态的各种服务时享有“特殊待遇”（根据信用积分高低决定），如：

1. 使用 LEXEL 钱包，转账免 Gas Fee
2. 持有者的 LEXEL 会自动增值（数字资产银行）
3. 游戏或者应用特权

LEXEL 链锁生态务求打造一个既保障了用户的数字资产，同时能够给用户的数字资产带来增值的区块链生态。

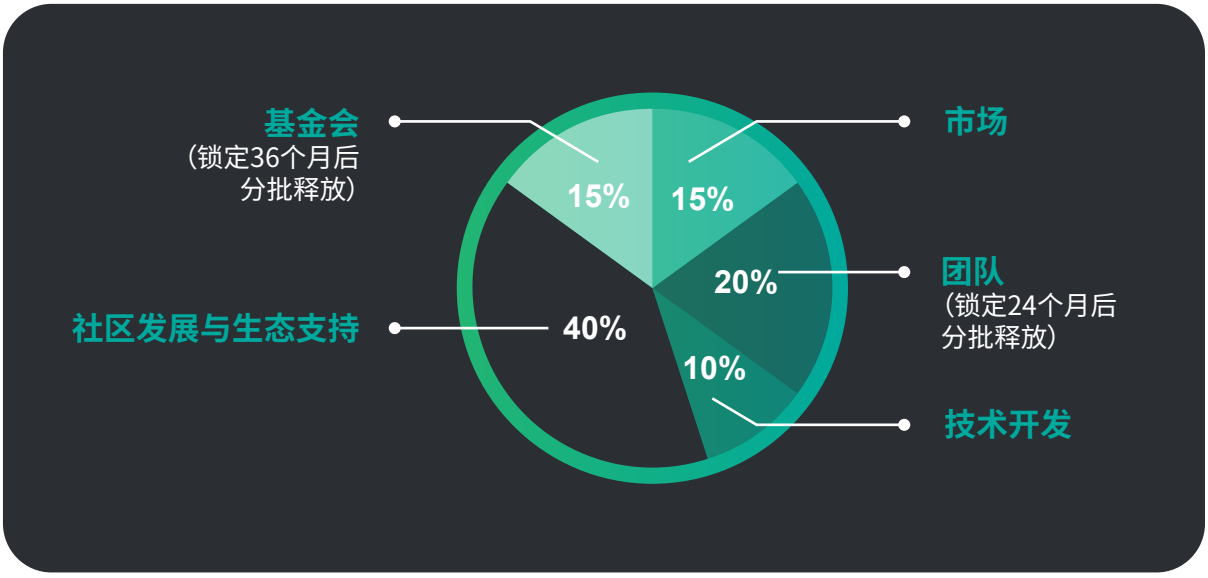
4. Token 分配

a) **代币总量：** 10,000,000,000 LEXT（永不增发）

b) **代币生成时间：** 2018年2月中旬

c) **交易所上线时间：** 2018年6月中旬

LEXEL 不会有任何形式的公募和私募，所有代币只对战略投资者、社区生态贡献者、商业合作伙伴赠送，以及基金会与技术开发团队保留持有。禁止中国人与美国人以任何方式购买及持有，否则一切法律后果自负！



LEXT 届时将在 LEXEL 生态体系中流通使用，包括但不限于交易（事务）的记账消耗（GAS）、个人数字身份的创建及查询费用、安全加密存储及支付相关服务费、可信浏览器广告收入、其他数字认证场景的服务费用等。

5. 发展路线图

2011~2017

- 2011年初-2017年11月 加密认证技术研发

2018

- 2018年2月中旬 生成代币
- 2018年6月中旬 代币交易所上线
- 2018年6月下旬 主网投入开发
- 2018年7月~8月 关键硬件研发
- 2018年9月 关键模块研发、主网基本完成
- 2018年12月 主网，钱包开发完成并上线

2019

- 2019年3月 智能合约应用模板推出
- 2019年6月 硬件设备接入主网开发
- 2019年8月 硬件接入主网完成
- 2019年12月 首个DApp试运行

2020以后

- 持续推进... 扩大硬件及主网的应用范围，建立主网生态

6. 核心团队

6.1 团队成员

Lewis Lo

CEO CTO

10多年IT开发经验，负责LEXEL的全局统筹与管理。近几年钻研区块链技术的落地及应用，曾成功帮助某珠宝公司开发了一个基于联盟链技术（PBFT共识机制）的珠宝销售及防伪追溯平台。

Evangelos Rekleitis

CSO

帝国理工大学高级计算机硕士学位，自2007年起一直担任ICT工程师和风险分析师，参与了塞浦路斯政府网络安全战略及其云安全战略的修订，并参与了希腊政府的多项安全研究和风险分析与管理项目。2015年受聘于欧盟网络和信息安全局；参与了大数据安全、网络威胁、安全标准化和密码学等项目。

Christine He

COO

毕业于北卡罗莱纳州立大学，曾就职于全球最大视频电商系统Cinsay公司，带领团队开展跨国业务。曾协助Cinsay合作方——Formula E车队Andretti Autosport开发定制页游及运营工作。精通多国语言，具有丰富的社区运营及公关宣传经验。

Alog Rana

毕业于帝国理工大学，在安全交易，AML以及诈骗检测解决方案方面有丰富的经验。同时具备在低延迟率，可扩展性以及高可用系统设计方面的实施经验。在金融IT方面具有贯穿整个项目生命周期的丰富的业务知识。

Soumil Verma

北卡罗莱纳州立大学计算机工程与电子工程双学位。曾担任康涅狄格大學研究员，曾就职于食品安全检验局USDA担任数据分析师，参与开展ArcGIS项目。

Anuj Sanghavi

现于Caterpillar Inc. / EASi LLC公司担任项目工程师，负责自动化测试项目，曾是Albright Entrepreneur Village公司成员，北卡罗来纳州立大学电气及电子工程师协会联合主席，及The Carrom Club 出纳。

Todd Downing

毕业于贝勒大学，拥有超过20年的IT从业经验，并具备多行业的业务知识，曾就职于Dell、Nexstar Broadcasting、Cinsay等知名企业。依靠丰富的技术及管理经验，多次参与企业发展战略的制定。在技术与业务发展方面有独到见解。

James Kersbergen

具有超过20年的开发经验，曾任职于Belo、Nexstar Broadcasting和Cinsay，负责技术开发及团队管理工作。在流媒体、云计算及数据库技术方面有深入研究。

Serge Kononov

在IT测试领域拥有超过15年的丰富经验，对测试技术有深入了解，擅长自动化测试。曾负责企业的自动化框架设计及搭建，确保产品快速迭代的可靠性。

Fadi el Hamdi

毕业于荷兰阿姆斯特丹大学国际商务理财学系，曾就职于荷兰银行（ABN AMRO Bank N.V.）的信息科技部门。负责网络银行金融安全漏洞分析。为工作人员提供网络安全工作环境与即时应对病毒木马入侵。

6.2 专家顾问

Richard Zhang

毕业于加州大学伯克利分校电子工程和计算机科学系。曾就职于BigFix和IBM，任高级软件工程师。现就职于AppDynamics的资深软件工程师。曾创立过一个网络图形计算器引擎和参与过文件加密软件TrueCrypt的开源项目。专注于用户体验、单页应用、加密技术、应用安全传输、应用安全性能管理等网络技术。

Riad Elmnebhi

毕业于法国国立应用技术学院，信息系统架构专业。在巴黎银行工作了11年。现在是银行区块链计划的总监，负责创立了巴黎银行私有区块链系统。

Khalil Najjar

云技术、企业ERP、企业数字化高级顾问；
物联网，区块链，微服务，人工智能等领域专家、架构师。

6.3 合作机构

创世资本

极点基金

链上资本

聚合资本

普渡大学区块链研究室

三链资本

Africoin

引力资本

天天交易所

6.4 合作媒体

金色财经

火讯财经

耳朵财经

币头条

TokenBook

牛X导航

One Top

3点钟财经

7. 风险提示

链锁团队郑重提示您：参与者应当知晓所有区块链项目皆具有风险，区块链项目的价值与项目发展状况及市场参与者的预期密切相关，参与者不应盲目相信任何区块链团队所作出的任何获利保证，也不应盲从跟风参与，而应对项目的技术及应用发展潜力、自身的经济承受能力和心理承受能力做出客观判断，一切责任、收益、损失最终均由参与者自行承担。

具体而言，链锁和LEXT将可能存在以下风险：

（1）信息披露不完备的风险

截至本白皮书发布之日，链锁仍处于开发阶段，其哲学理念、共识机制、算法、代码等技术规范和参数可能会经常且不断更新与变更。尽管本白皮书包含链锁的特定信息，但其并不绝对完整，且出售方可能会根据特定目的不时对这些信息作出调整与更新。出售方无法，也无义务随时告知参与者链锁开发中的每个细节(包括其进度和预期里程碑，无论是否推迟)，因此并不必然会让参与者及时且充分地获悉链锁开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

（2）监管风险

加密代币正在被或可能被各个不同国家的监管机构所监管。出售方可能会不时收到来自于一个或多个监管的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何与售卖、链锁开发或LEXT币相关的行动。链锁的开发、营销、宣传或其他方面以及售卖均可能会因此受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家之中现有的对于链锁或售卖的监管许可或容忍可能只是暂时的。在各个不同国家，LEXT币可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，LEXT币可能被禁止交易或持有。

(3) 密码学加速发展的风险

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步(例如密码破解)或者技术进步（例如量子计算机的发明/改良）可能给基于密码学的系统（包括链锁)带来危险。这可能导致任何人持有的LEXT被盗、失窃、消失、毁灭或贬值。在合理范围内，项目方将自我准备采取预防或补救措施，升级链锁的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的，项目方将和链锁社区其他成员一起尝试适应密码学和安全领域的不断变化。

(4) 项目失败或中止的风险

链锁仍在开发阶段，而非已准备推出的成品。由于链锁系统的技术复杂性，出售方可能不时会面临无法预测和/或无法克服的困难。因此，链锁的开发可能会由于任何原因而在任何时候失败或中止（例如由于缺乏资金)。开发失败或中止将导致LEXT无法交付给售卖的任何参与者。

(5) 收入被盗的风险

可能会有人企图盗窃出售方所收到的募集资金（包括已转换成法币的部分)。该等盗窃或盗窃企图可能会影响出售方为链锁开发提供资金的能力。尽管出售方将会采取最尖端的技术方案保护募集资金的安全，某些网络盗窃仍很难被彻底阻止。

(6) 源代码漏洞风险

无人能保证链锁的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能、暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害链锁的可用性、稳定性和/或安全性，并因此对LEXT的价值造成负面影响。

(7) 无准入许可、去中心化自治账本的风险

链锁底层的分布式账本是无准入许可的，这意味着它可被所有人自由访问和使用，而不受准入限制。尽管链锁初始时是由出售方所开发，但它

并非由出售方所有拥有、运营或控制。自发形成的链锁社区是完全开放、去中心化且无准入门槛即可加入的，其由全球范围内的用户、粉丝、开发者、LEXT持有人和其他参与者组成，这些人大都与出售方无任何关系。就链锁的维护、治理乃至进化而言，该社区将是去中心化且自治的。而出售方仅仅是社区内与其他人地位平等的一个活跃成员而已，并无至高无上或专断性的权力，不考虑其之前曾对链锁的诞生做出的努力和贡献。因此，链锁在启动之后，其如何治理乃至进化将不受到出售方的支配。

(8) 源代码升级风险

链锁的源代码将逐步开源且可能被链锁社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对链锁的运行或LEXT的价值造成重大不利影响。

(9) 安全漏洞风险

链锁区块链基于开源软件并且是无准入许可的分布式账本。尽管出售方努力维护链锁系统安全，任何人均有可能故意或无意地将弱点或缺陷带入链锁的核心基础设施要素之中，对这些弱点或缺陷出售方可能恰好无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的LEXT或其他数字代币丢失。

(10) “分布式拒绝服务”攻击风险

链锁被设计为公开且无准入许可的账本。因此，链锁可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使链锁系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入链锁区块链的区块之中，或甚至暂时无法执行。

(11) 节点处理能力不足的风险

链锁的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过链锁区块链网络内届时节点所能提供的负载，则链锁网

络可能会瘫痪和/或停滞，且可能会产生诸如“双重花费”的欺诈或虚假交易。在最坏情况下，任何人持有的LEXT可能会丢失，链锁区块链回滚或甚至硬分叉可能会被触发。这些事件的后果将损害链锁的可使用性、稳定性和安全性以及LEXT的价值。

（12）LEXT未经授权被认领的风险

任何通过解密或破解LEXT购买者的密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意认领在售卖中所购买的LEXT。据此，购买者在售卖中所购买的LEXT可能会被错误发送至通过购买者注册邮箱或注册账号认领LEXT的任何人士，而这种发送是不可撤销、不可逆转的。每一购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性：使用高安全性密码；不打开或回复任何欺诈邮件；以及严格保密其机密或个人信息。

（13）LEXT钱包私钥丢失风险

若丢失或损毁了存取LEXT所必需的私钥，这可能是不可逆转的。只有通过本地或在线LEXT钱包来占有相关的独一无二公钥和私钥，才可以操控LEXT。每一购买者应当妥善保管其LLEXT钱包的私钥。若LEXT购买者的该等私钥丢失、遗失、泄露、毁损或被危及到，出售方或任何其他人士均无法帮助购买者存取或取回相关LEXT。

（14）系统分叉风险

链锁是一个由出售方发起并由社区提供支持的开源项目。尽管出售方在链锁社区中具有影响力，但是其并不也无法独断链锁的开发、营销、运行或其他。任何人士均可以开发链锁代码的补丁或升级，而无需获得任何其他人士的授权。一旦部分的链锁区块链上验证者接受链锁的补丁或升级，这可能导致链锁区块链“分叉”，由此将会出现两条分叉的网络，直至分叉的区块链合并或者其中某一条终止出块（这两种情况可能永不会发生）。链锁区块链由于分叉而产生的每一分支均将有其自己的加密代币。因此，在两条分叉

的分支上会分别存在拥有几乎相同技术特征和功能的LEXT。链锁社区可能分裂成两批，分别支持两条分支。此外，分叉出的链锁区块链分支在理论上可以进一步无限次分叉。分叉区块链的暂时性或永久性存在可能对链锁运行及LEXT的价值造成不利影响。在最坏情况下，可能摧毁链锁系统的可持续性。尽管链锁区块链上的该等分叉有可能经社区牵头努力后将两条分支合并而解决，但并不能保证成 功且可能耗时很久。

(15) 平台合并的风险

技术角度而言，在特定情形下，为实现协同效应或基于其他有价值的对价，链锁可能与其他区块链项目合并。这种形式的合并可能导致链锁区块链被放弃或废弃，以换取新创建的其他区块链上一定数量的加密代币。该等新的加密代币将按一定比例分配并派发给合并前的LEXT持有者。在特定估值模型下LEXT持有者可能在该等合并中获得的补偿不足。

(16) 应用缺少关注度的风险

LEXT的价值很大程度上取决于链锁平台的普及度。链锁并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，链锁甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部LEXT需求可能具有投机性质。缺乏用户可能导致LEXT市场价格波动增大从而影响链锁的长期发展。出现这种价格波动时，出售方不会(也没有责任)稳定或影响LEXT的市场价格。

(17) 流动性不足风险

LEXT既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的货币，也没有任何硬资产或其他信用所支持。LEXT在市场上的流通和交易并不是出售方的职责或追求。LEXT的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从LEXT持有者处购买任何LEXT，也没有任何人士能够在任何程度上保证任何时刻LEXT的流通性或市场价格。

LEXT持有者若要转让LEXT，该LEXT持有者需寻找一名或多名有意按约定价格购买的买家。该过程可能花费甚巨、耗时长并且最终可能并不成功。此外，可能没有加密代币交易所或其他市场上线LEXT供公开交易。

(18) 代币价格波动风险

若在公开市场上交易，加密代币通常价格波动剧烈。短期内价格震荡经常发生，该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量(包括投机买卖)、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在LEXT交易的二级市场，出售方对任何二级市场的LEXT交易不承担责任。因此，出售方没有义务稳定LEXT的价格波动，且对此也并不关心 。LEXT交易价格所涉风险需由LEXT交易者自行承担。

(19) 竞争风险

链锁的底层协议是基于开源电脑软件，没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用链锁的源代码和/或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台或虚拟机从而与链锁竞争，或甚至赶超或取代链锁。出售方对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台与链锁产生竞争关系。出售方在任何情况下均不可能消除、防止、限制或降低这种旨在与链锁竞争或取代链锁的竞争性努力。

(20) 第三方开发者风险

链锁将提供一个开放平台适用于第三方（尤其是链锁社区成员）开发的任何类型的分布式应用和智能合约程序。所有这些应用和智能合约程序可以被接入或建立在链锁区块链上而不受限于审查制度、限制、控制、资格预审或准入要求。出售方既不意图也无法担当审查员在任何程度上对任何将要在链锁系统上开发或与之相关的程序进行审核。因此，在特定司法管辖

区域被禁止或限制的程序，如涉及赌博、投注、彩票、乐透、色情等等的程序，可能利用链锁区块链的无准入要求来开发、促进、营销或运营。特定司法管辖区域的监管当局可能对特定程序或甚至其开发者或用户采取相应行政或司法措施。任何政府当局的处罚、惩罚、制裁、镇压或其他监管措施，或多或少会惊吓或威慑到既有或潜在链锁用户使用链锁系统并持有LEXT，从而对链锁的前景造成重大不利影响。

(21) 其他加密资产的风险

链锁中将会创建或生产并流通着各种加密资产。这些加密资产中一部分可能是由特定人士发行的，发行人将对持有人负有特定承诺或义务。其他些加密资产可能是由链锁内的智能合约创建的。这些加密资产都不会带有和LEXT一样或类似的功能。这些加密资产既不是出售方所出售或提供的，出售方也不会对它们负责，除非出售方另有特别说明。

LEXEL

www.lexel.io