DBB

DOCUMENT BILL BIT

DOCUMENT BILL BIT

白皮书

前言

随着互联网金融向纵深发展，区块链技术及其应用成为人们日益关注的热点，开放、可信、去中心化、共享，区块链的这些核心思想被大家广泛认可，区块链技术被视为继互联网之后又一次计算范式的颠覆性科技创新。

本白皮书主要介绍了 DBB（Document bill bit）跨境贸易、跨境结算的发展初衷、产品架构、技术特点、产品优势以及行业应用方向。DBB 跨境贸易、跨境结算是基于区块链技术，服务于“一带一路”沿线国家和地区的跨境贸易、跨境结算解决方案。

DBB 联合全球著名的经济界、金融界以及区块链行业的技术资源、资本、人脉资源，计划打造一条全球跨境贸易、跨境结算通用的区块链服务网络。项目立项之初，咨询了国际知名的专家、学者、企业家以及区块链行业的知名人士。我们认为，基于区块链的一带一路跨境贸易、跨境结算项目具有无穷的应用场景、广阔的发展空间。

目录

第一章：市场背景 5
1.1 跨境贸易 5
1.2 “一带一路”丝绸之路经济带 6
1.3 市场痛点 8
第二章：DBB 简介 11
2.1 DBB 项目 11
2.2 DBB 使命 11
2.3 DBB 愿景 11
第三章：DBB 项目技术架构 12
3.1 基于基础协议交易信任的区块链系统 12
3.2 DBB 架构概要 13
3.3 DBB 底层架构 13
3.4 DBB 自治域 15
3.5 DBB 自治域间通信 17
3.6 DBB 参与方 18
3.7 DBB 共识机制 20
3.8 智能合约 22
3.9 网络安全 22
第四章：DBB 账户管理 23

4.1 DBB 账户管理 23
第五章：DBB 技术架构安全与网络安全防护 25
5.1 区块链本身具备的安全优势.....25
5.2DBB 的安全防护 25
第六章：DBB 优势与应用.....28
6.1 DBB 优势.....28
6.2 DBB 应用.....31
第七章：DBB 团队及资本.....34
第八章：代币发行与市场规划.....37
8.1 DBB 代币发行 37
8.2 DBB 市场规划 38
免责声明.....39
风险提示.....40

第一章：市场背景

1.1 跨境贸易

人类使用货币的历史产生于最早出现物质交换的时代。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，比如一头羊换一把石斧。但是有时候受到用于交换的物资种类的限制，不得不寻找一种能够为交换双方都能够接受的物品，这种物品就是最原始的货币。牲畜、盐、稀有的贝壳、珍稀鸟类羽毛、宝石、沙金、石头等不容易大量获取的物品都曾经作为货币使用过。

目前在市场经济发达的国家，实际上并存着两种不同的交易方式，即常规交易（或称货币经济）和跨境贸易，跨境贸易已成为货币经济重要的、有益的补充交易形式。从 20 世纪 80 年代起，现代跨境贸易交易公司在美国、加拿大、澳大利亚等国普遍兴起，成为这些国家减少现金用量、增加销售、减少库存、开发新客户、开辟新市场、促进经济发展的重要产业。现代跨境贸易在发达国家的发展表明它有存在和发展的客观基础，同时在很多发展中国家也一定有广阔的发展空间，我们正面临着一个巨大的商机。

跨境贸易、跨境结算从开始的那天起，就和库存商品结下了不解之缘。近年来，全球经济滑坡，通货紧缩，企业间三角债现象普遍存在。企业一方面无法回笼销售款采购原材料、扩大再生产，一方面市场疲软导致库存急剧增加。根据相关统计数字显示，全球的库存积压商品高达 6.4 万亿美元。在此情况下，国家不得不对一些产品实行限产压库。当时，一批经济学家经过调研认为，商品最原始的交易方式是“以物易物”，比如一个企业的彩电卖不出去，另一个企业

的煤炭卖不出去，那么企业间可以用彩电来换煤炭进行再生产，这就是跨境贸易交易，并早已在欧美兴起。经济学家们在此基础上确立了跨境贸易理论，认为“点对点”的跨境贸易很难推行，“点对多”、“多对多”是跨境贸易的必然选择。也就是说，大家把商品放到一个网络平台上，通过互联网挑选自己需求的商品，从而完成易物交易。据此，经济学家们一致认为，解决库存的最好办法是跨境贸易交易，即把数万亿商品同时放在一个大平台上进行跨境贸易，既解决了企业再生产而无现金的难题，又解决了商品的积压问题。

1.2 “一带一路”丝绸之路经济带

“一带一路”（The Belt and Road，缩写 B&R）是“丝绸之路经济带”和“21 世纪海上丝绸之路”的简称，2013 年 9 月和 10 月由中国国家主席习近平分别提出建设“新丝绸之路经济带”和“21 世纪海上丝绸之路”的战略构想。它将充分依靠中国与有关国家既有的双多边机制，借助既有的、行之有效的区域合作平台，一带一路旨在借用古代丝绸之路的历史符号，高举和平发展的旗帜，积极发展与沿线国家的经济合作伙伴关系，共同打造政治互信、经济融合、文化包容的利益共同体、命运共同体和责任。

图：一带一路沿线国家的范围

一带一路沿线国家的范围包括：

中蒙俄经济带：中蒙俄经济走廊属于一带一路丝绸之路的一部分。主要包括北京、乌兰巴托、乌兰乌德、伊尔库茨克、克拉斯诺亚尔斯克、新西伯利亚、欧姆斯克、别米尔、莫斯科等。

新亚欧经济带：新亚欧经济带也属于一带一路的一部分。东起中国连云港，贯穿西安、兰州、乌鲁木齐，西至哈萨克斯坦、乌兹别克斯坦、俄罗斯和荷兰。

中国—南亚—西亚经济带：南亚、西亚经济带是重要的政治、经济走廊，包括了喀什、德黑兰、意大利等重要的商业经济地带。

海上战略堡垒：主要指海上丝绸之路，东部包括中国连云港、福建、广西，东南亚地区包括南太平洋地区、新加坡、雅加达、加尔各答、斯里兰卡，西部包括瓜达尔港、坦桑尼亚、波斯湾、希腊等。

1.3 市场痛点

纵观上述一带一路整个经济带可以看出，大部分沿线国家和地区的经济发展都相对滞后，经济体量偏低，GDP 略低，通货膨胀率较高，外汇储备较低，这直接导致了各国之间的大宗贸易受制于政府的外汇储备量，导致交易困难，也暴露出跨境贸易目前的痛点，具体表现在以下方面：

痛点一：通货膨胀率高，导致他国不愿接受本国货币

对于跨国跨境贸易、跨境结算项目大都是中大型项目或产品为主，往往存在交易周期长，涉及资金量大等特点。但一带一路沿线大多数国家的货币存在较高的通胀率，这样会导致在很多项目或交易还未完成时，其交易的法币已经大幅贬值，直接影响了跨国贸易。

痛点二：外汇储备低，缺乏硬通货，贸易困难

对于一些相对较落后的国家和地区，缺少足够的美元、欧元或者人民币的外汇储备。因此，当需要购买他国商品时，他国更愿意接受美元、欧元等货币支付，但这些国家或地区缺少足够的外汇储备，导致了贸易困难。

痛点三：信任缺失

信任是跨境贸易中举足轻重的要素，业务中的物流、资金流和数据流都需要依靠信任来维系。但在目前的跨境贸易环境中，能够用以支持信任的技术相对较少，而是大量通过传统的纸质文件、手写签名、第三方托管等模式，不但无法有效降低欺诈风险，也在一定程度上影响了跨境贸易的处理效率。

数据源真实性难确认。跨境贸易中各数据源即参与方不仅数量众多、类型复杂，还因跨境的业务特点，分布在不同国家和地区的管辖区，在没有可靠电子化流程系统的情况下，业务链中任意一方想要确认其他各环节的参与方身份的真实性，避免贸易欺诈风险都面临着巨大的挑战。

层层传递影响数据可信度。当前跨境贸易业务中，业务链上单环节的数据来源往往较为单一 。 以海关为例，其监管所需的大部分数据通常来自于报关行等贸易服务商，或经认证经营者企业（即 AEO 企业）。然而这些企业的数据也并非全为一手获得，数据经过层层传递，其可信度势必大打折扣，导致跨境贸易过程中仅信息核实环节便需要投入大量的时间和人力成本。

痛点四：中心化平台瓶颈

在目前未使用区块链技术的环境前提下，几乎所有能够实现跨境贸易数字化的技术方案所提供的，均为中心化的服务或平台。这类系统在技术层面和治理层面都具有高度集权的特点，每一个使用者都与中心相连，中心拥有远高于一般参与方，极不对称的权利和义务。同时，这类系统还存在着中心透明度低、对中心依赖性强的问题，一旦中心违约、丧失或连接丧失，整个系统都会遭受巨大的破坏。中心的确立也是此类中心化系统在应用过程中面临的最大挑战之一。

在一般业务中，出于普通商业机构间的竞争关系及其对各自利益的考量，系统中心的角色通常由拥有强制手段和权力的监管机构来担任。但跨境贸易因其业务特点，商品流、资金流和数据流势必都将跨越至少两个不同国家或地区的管辖主体，任何一个管辖主体都几乎不可能将自身对数据流的控制权和拥有权交由其他主体。此外，不同交易跨越的主体具有非常强的多样性与非规律性，从而使类似局部协议或联盟的方案也几乎无法实现。来自商业与政治的压力与制约，使得任何试图整合跨境贸易数据流的中心化平台，都几乎不可能具备其实现目标所需要的相应统治力。

根据上述的主要问题，我们提出通过跨境贸易方式解决，主要可服务以下方面:

一是政府为保证国内基本生活物品的供应，在外汇短缺、贷款无着落时，通过寻求跨境贸易解决。如政府进口小麦、进口铁路车厢，基础设施建设等。在这种情况下，政府会主动帮助解决跨境贸易物品的交易难题。

二是在外汇管理体制下，有些实体有投资能力，通过进口设备进行技术改造，项目能获得政府批准，但政府不负责解决外汇资源。这些单位每年都有相当可观的本地收入，项目单位愿意支付本币。在这种情况下，需要交易双方企业自己解决跨境贸易物品问题（购买方用本币购买该国特色产品，以特色产品交换对方的设备）。

三是交易的部分货款以本外币分期付款形式支付。如一笔交易，双方商定买方先以美元结算 40% 的货款，剩下部分实行收益分成制，并以本地货币进行支付。在这种情况下，由卖方通过与其他本地企业之间进行兑换调剂，只有在经济落后的国家设立了分支机构的单位才可开展贸易。一些金额较大的交易最终还是需要通过跨境贸易、跨境结算方式进行。

第二章：DBB 简介

2.1 DBB 项目

作为一家国际化、集团多元化发展的新型技术企业，DBB 着力搭建全球贸易智慧生态圈，采用了基于商用、政用、民用的区块链技术打造的区块链跨境贸易网络，通过跨境贸易，区块链提供了跨境贸易、跨境结算记账、征信、业务关系、政府监管、多边贸易撮合的综合服务。通过区块链的开放账本，可支持多国、多企业、多用户接入，支持不同终端设备、不同平台间共享跨境贸易账本信息，提升资产流通性，提高一带一路沿线国家的经济实力。

2.2 DBB 使命

DBB 以服务“一带一路”国家战略和探索制定“贸易新规则”为使命，通过跨境贸易在交易、支付、物流、通关、退税、结汇等环节的技术标准、业务流程、监管模式和信息化建设等方面先行先试，逐步形成一套适应和引领全球跨境电子商务发展的管理制度和规则，抢占全球跨境电子商务发展的制高点和话语权。

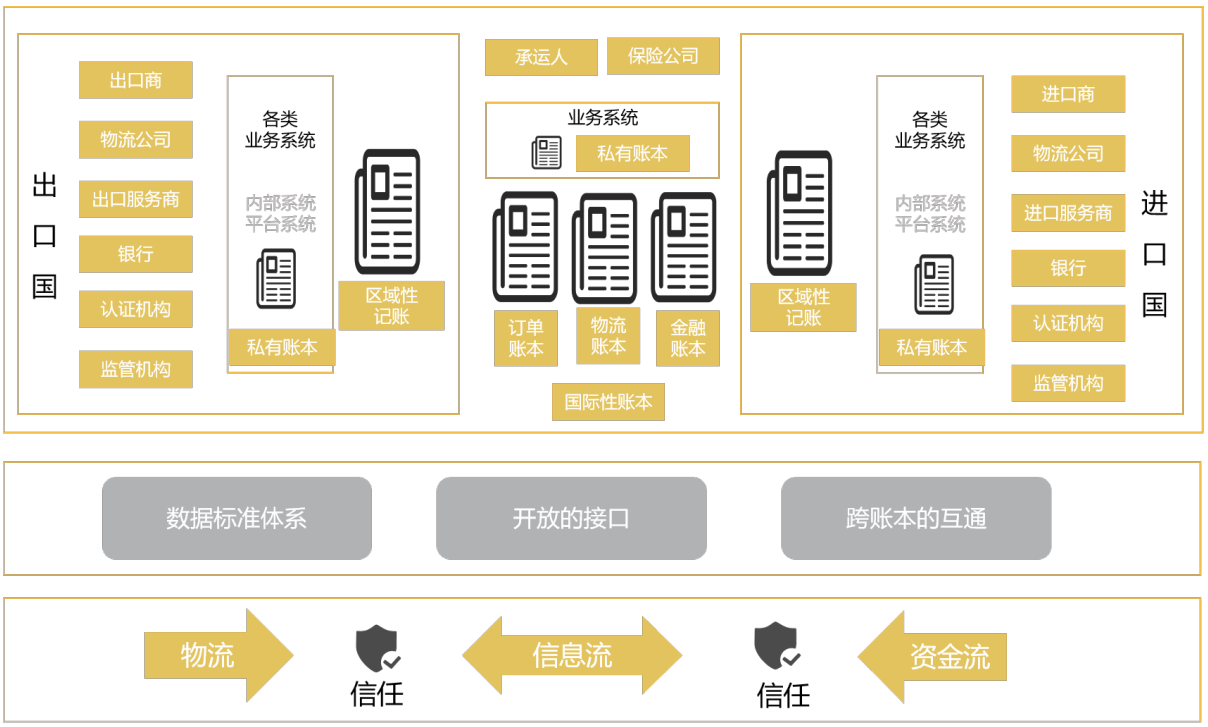
2.3 DBB 愿景

DBB 集结各地的优势，构建世界级的城市群，旨在成为环球创新、金融及贸易中心。DBB 跨境贸易平台将成为巨大的经济增长引擎，旨在结合各城市的优势也有利于促进贸易，刺激全球的经济增长。

第三章：DBB 项目技术架构

3.1 基于基础协议交易信任的区块链系统

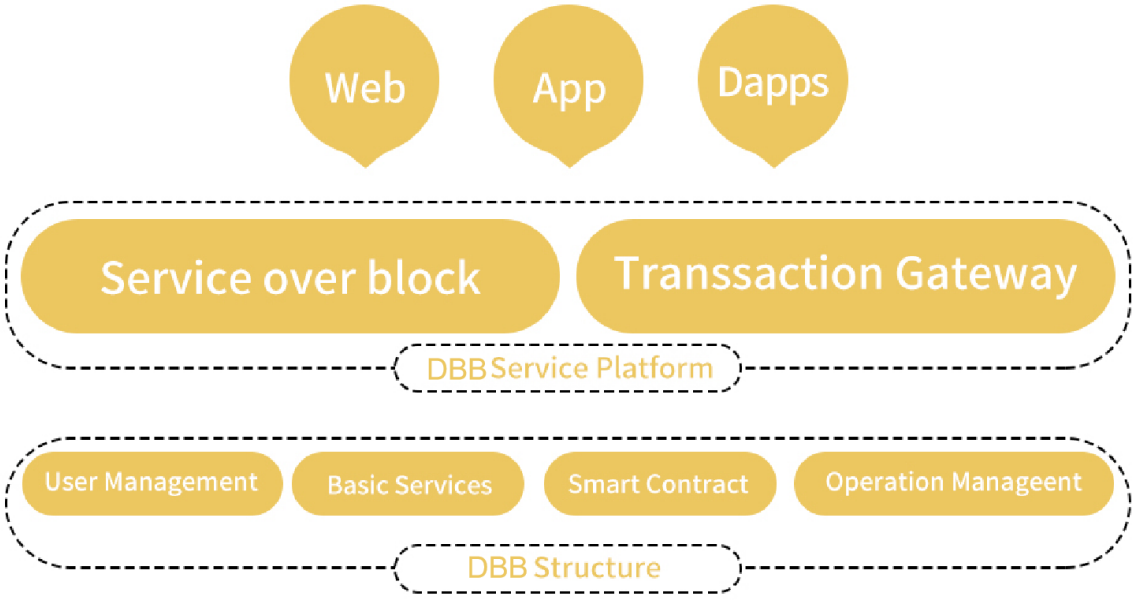
DBB 是基于以太坊开发，将包含协议的完整实现、基础工具和 API 接口。D 基于跨境贸易的交互业务逻辑相对简单，但对交易关系形态的变化较多，因此我们在底层基础协议方面提供更多灵活的空间和扩展性需求；但在工具和 API 接口方面，对一致性和安全性保持相对的强耦合状态。根据团队前期的 P2P 电商领域丰富的经验，市场需求非常旺盛，相信这两个方面的考虑会对 DBB 快速的大规模商用提供一定帮助。



3.2 DBB 架构概要

DBB 的整体架构分成三个层次：（1）DBB Structure；（2）DBB 服务层作为中间层，提供交易网关作用，用于链 WEB 协议等的交互；（3）上层是 DBB 应用服务层，提供 api 接口，并提供 web 应用开发和 DAPP 开发框架和底层应用能力。

整体框架结构如下图：



3.3 DBB 底层架构

（1）账户管理：负责区块链参与者的身份信息管理，包括维护公私钥生成、密钥存储管理、以及用户身份和区块链地址对应关系维护等。

（2）基础服务：基础服务部署在所有区块链的节点上，用来验证业务请求的

有效性，并对有效请求完成共识后记录到账本上。对一个新的业务请求，基础服务先对接口适配解析及鉴权处理，然后通过共识算法将交易或者合约加上签名并加密之后，完整一致地存储到共享账本上。共识机制可自适应，网络异常或者节点欺骗的情况下具有强容错性。

（3）智能合约：负责交易的区块链合约的生成以及合约的触发和执行。用户通过简单操作即可完成 P2P 电商合约逻辑，发布到区块链上之后，根据合约条款的逻辑，由用户收款签名等其他的事件触发执行，完成交易结算等合约的逻辑。

（4）运维管理：负责区块链发布过程中的部署、配置修改、合约设置以及产品运行中的实时状态可视化的输出，如：告警、交易量、网络情况、节点健康状态等。

3.3.1 DBB 服务层

DBB 服务层提供链内链外交易网关和信息服务层的中介。交易网管协助用户进链下电商购买操作到链上的交互接口，并提供鉴证服务：让卖家和买家通过一个简单的 API 接口就可以把交易信息等发布到区块链上，让所有记账节点共同为自己作证。在本质意义上是交易信任与买家对交易标的个性化体验差异解耦。DBB 体系功能实现的是在链内的信任关系机制，因此将链外部的商品标的信息与交易信息分离。在交易关系收敛周期内，如果双方没有进一步的交易完成，

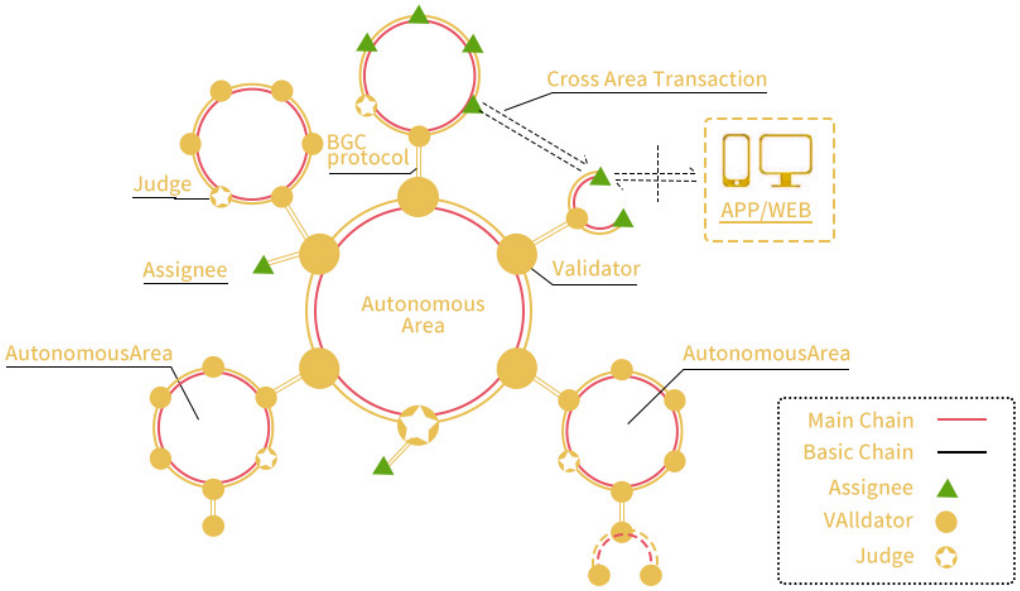
则认为双方信任关系解除；而交易关系的收敛周期根据所自然形成的自治域的链的交易速度和广度有关。信息服务层则抽象底层区块链多种信息，提供上层应用开发框架所需要的底层信息和消息对话机制。

3.3.2 DBB 应用层

DBB DAPP 应用服务层提供简单应用开发的框架，应用类型包含了数字资产、共享账本、鉴证证明、产品追溯及所有权交易等基本应用模型。用户可以基于这些应用开发框架进行业务开发。开放区块链底层结构（DBB structure）和应用层（SEC）的能力，协助社区开发新的 DBB 电商应用服务、匹配对应的应用场景，共同维护区块链生态

3.4 DBB 自治域

DBB 是一个涵盖众多独立区块链的网络，多域自治的域，叫做自治域（Autonomous Area），即把整个 DBB 网络划分为许多较小的网络单位，频繁的交易关系和信任关系的节点自动生成并收敛在同一个自治域内。DBB 自治域是一种社交关系权益证明加密货币网络，它通过类似路由简单的管理机制来实现网络的改动与更新。DBB 自治域还可以通过连接其他链通过跨链来实现扩展。



DBB 的自治域

通过域间通信（BGC）协议进行交易，BGC 协议就是通过不同域兼类用户数据报协议（UDP）和类传输控制协议（TCP）进行通信。Tokens 可以安全快速在域间转移，两者之间无需体现汇兑流动性。同一自治域内部所有 Tokens 的转移都会通过 SEC 关键节点，它会记录每个自治域所持有的 Tokens 总量。这个自治域会将每个资质与其他故障自治域隔离。

DBB 被设计成一个自治域的集合，可以向外扩展，会有非常大数量的自治域。每个自治域通过相同的网络模式进行平行管理，因此系统具有可伸缩的能力。在 SEC 调度内核支持下运行，是一个类似异步拜占庭容错的安全共识引擎，兼具一致性等特点，而且在其严格的分叉责任制保证下，能够防止怀有恶意的参与者做出不当操作。采用 DBB 模式，区块链计算可以合并或分开进行，进而实现了负载均衡 （loadbalancing）。

DBB 网络通过 DPOS 机制来运行众多区块链自治域。负责管理众多独立区块链（称之为“自治域”，参考路由协议）。自治域会不断地提交最新区块，

这可以让自治域跟上每个节点状态的变化，之后信息包就会从一个自治域传递到另一个自治域，并通过发布梅克尔证明（Merkle-proof）来说明信息已经被传送或接收 。这 种机制叫做 “ 自治域间通信 ” ，或者简称为 “Border Gatewa Communication” 机制。

任何区块都可以自行成为验证人，从而形成非循环图。DBB 自治域是独立的区块链，能够和其他自治域进行 BGC 信息交换。从 DBB 全网络的角度看，自治域是一种双链形成，它可以通过 BGC 信息交互进行 Tokens 和账户信息发送与接收。

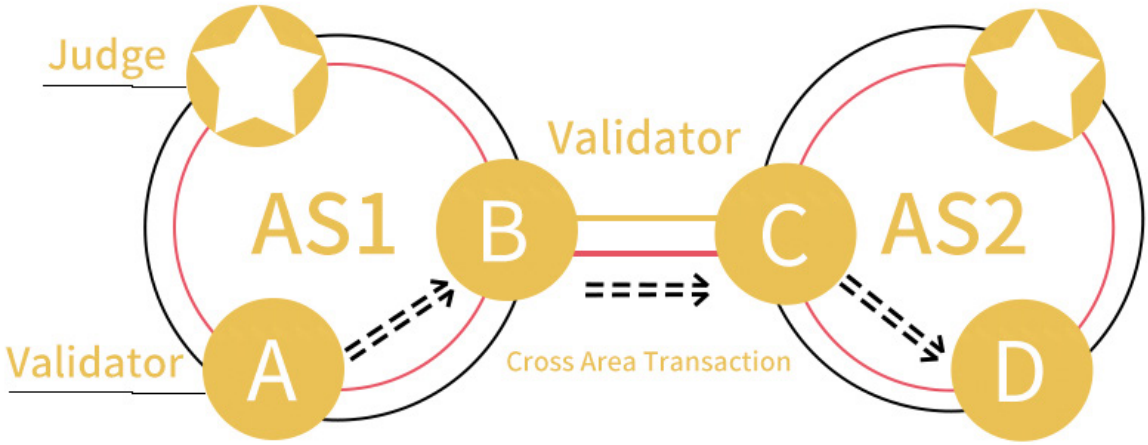
设置自治域中心的信任验证人。虽然验证人出现重复而引起的攻击行为会导致 DBBtoken 数量减少，但是如果自治域中有超过三分之二的选票都出现拜占庭问题那这个验证人就可以广告无效状态。其他自治域的验证人不会验证或执行提交到其它自治域的交易，DBB 的管理系统可能会通过改善协议，来解决自治域故障问题。比如：在检测到袭击时，可以将有些自治域发起的 Tokens 转移实现紧急中断。

3.5 DBB 自治域间通信

DBB 最关键的部分之一是跨域通信。因为在自治域之间可以存在某种信息交易，因此是可伸缩的区块链系统。为了保证最小的实现复杂度、最小的风险和最小自治域架构束缚，这些跨域交易会有个发起方字段，用来辨别自治域的身份。跨链交易使用简单的队列机制解决，该队列用梅克尔树（Merkle tree）来保证数据真实。验证者的任务是把交易从发起自治域的出口队列转移到接受自治

的入口队列。

现在我们来看一个实例，假如现在有两个 DBB 自治域，分别是“自治域 1”、“自治域 2“，自治域 1 内一个节点 A 和自治域 2 内节点 D 生成一个交易。为了能够让 Tokens 和信息从一个区块链节点 A 转移到另一个区块链节点 D，需要在接收方区块链节点 C 上发布一个证明，来明确发送方 A 已经发起了交易到指定地点。



DBB 自治跨域交易示例

DBB 的自治域可以在保持一致性的前提下，通过优先交易关系链，划分自治域加快交易，自治域域内因长期经常发生交易，因此双链账户信息和交易关系变动有限，进而实现交易的快速完成——针对双向订单交易，及 BGC（跨自治域通信）Tokens 与其他自治域的交易。

3.6 DBB 参与方

DBB 有三个基本的角色在维持：受托人（Assignee）、法官（Judge）、证

人（Validator）。在交易信任关系上三者具有相同权限和功能，在打包利益和确权下三者分工角色不同。

1、 验证人

验证人有最高权限，职责是在 DBB 自治域里打包新区块。验证人需要抵押足够多的押金，且必须在高运算能力和高带宽的机器上运行一个节点的客户端。每个区块上，节点都必须准备接收一个已提交的新区块。这个过程涉及接受、验证、再发布候选区块。验证人的任命是确定性的，但运作逻辑导致的结果实际上很难预测，进而提升了安全性。

不同自治域的验证人一旦都确定性地批准了自己所属自治域的新块，他们就必须开始更新交易队列的状态。也就是从一条自治域的出口队列转移到另一条自治域的入口队列，进而处理已批准交易集合、批准最终的区块、吸收自治域的

最终状态。在共识算法约束下，会惩罚一个没有履行职责的验证人。第一次错误，就会扣留他们的奖励，但如果是重复的错误会扣减他们的押金，会导致他们丧失全部的押金（一小部分烧毁，其余奖励给法官和诚实的验证人）。验证人唯一有权限可以创建有效的自治域区块。

2、受托人

受托人有两个角色，第一个是受托人是帮助验证人制造有效的自治域内区块的群体。他们会运行一个特定自治域的全节点，他们有自治域全节点的必要信息，可以打包新区块并执行交易；受托人群体为了获得更多手续费，竞争性地去收

集交易信息，推动信任交易的产生，同样地，去中心化的提名人群体也会允许多个有抵押的参与者来协调和分担验证人的职责。这种能力保证了参与的开放度，有助于成为更加去中心化的系统。

第二个是，受托人为信任传递角色。受托人信息字段中自动 trust index，初始值为 1，当受托人完成交易 TI 值会增加，最高 100。同样如果未完成交易，或卖家售卖假冒伪劣或买家恶意投诉，则 trust index 会减少；当 trust index 减为 0，则账户禁用。Index 越大，根据交易额，交易提交的押金越多。

3、法官

法官并不直接和区块打包的过程相关。他们是独立的“赏金猎人“，激励他们的是一次性的大额奖励。法官及时举报并证明至少一个有抵押的参与方存在非法行为，他们就能获得奖励。为了预防由于私钥泄露给法官所导致的过度奖励。法官所需要的资源相对较少，也没必要承诺稳定的在线时间和大的带宽。法官

只需要提交很少的押金，这个押金用于预防浪费验证人计算时间和计算资源的女巫攻击。它是立即可以提现的，但如果监测到一个不当行为的验证人，可能会收获很大的奖励。

3.7 DBB 共识机制

我们选择使用以 DPoS 为基础的共识算法。在共识上，在有任意网络缺陷的架构下，只要大部分验证人是诚实的，就能提供一种高效的容错算法，可以在大

概率层面保证数据的真实性和准确性。DBB 在初始时刻即被创建，在应用场景中不断被分发。根据不同的要求定制 DBB 的细节功能和 DBB 所提供的服务和 DBB 的 Tokens 具体信息，不同链之间建立一部分同步共享账本。这些定制信息形成 DBB 的数据结构，以类似 DBB 交易记录的方式，被记账节点记录在当前时段的区块中。至此自治域将作为一条独立的区块链，记录自治域 Tokens 的交易。

（一）双链共识算法

通过团队成员研发生成的“Ω 算法”，作为一种严格基于区块链的密码及共识基础而被开发，与现有算法所不同的是对电商领域所需要的极速共识、安全性、超低算力需求，该算法均可满足。利用双线性映射函数的性质，在不泄露因变量的情况下来验证“函数”有效性，避免一个区块的生成者预测以后生成者的概率时候的天然优势的影响程度，而实际通过网络延迟（即牺牲速度）实现算法有效性。同时构建 DPOS 共识机制，同样通过密码学的方法，通过封装函数非规律性决定下一个区块的生成者，在不牺牲速度情况下，实现共识机制。算法关键点：（1）为保证完全随机，在区块中引入 X block（第 X 个块）且仅当前区块的潜伏者在整个网络中被揭晓时才能最终确认，从数学逻辑上阻断入侵阻断可能性。（2）同时构建并发机制，多个潜在的潜伏者所在的区块也完全独立，通过公网进行统一汇集，优先进行区块数据广播，之后进行揭晓环节，从而保证了篡改失去意义。（3）算法支持播放器更换机制，从而使任何节点都可以随时被其他节点接管，综合提升算法时效优势、提升经济性。综上所述，

Ω 算法涵盖了如下优点：可控制的分叉风险、需要很少的计算量、节点离线容忍度扩容、单向不可逆密钥高安全级、复合验证投票机制。

3.8 智能合约

DBB 中的智能合约基于计算机代码形式实现合约参与方达成的条件型协议，当条件被触发时区块链系统执行该协议。根据应用场景的不同需求，跨境贸易区块链可有选择性地提供智能合约功能。在使用智能合约的系统中，需提供如下功能支持：

●提供编程语言支持及配套开发环境；

●支持 合约内容静态和动态检查；

●支持运行载体， 如虚拟机；

●支持向账本中写入合约内容，防止对合约内容进行篡改；

●支持多方共识下的合约内容升级；

●支持监管方统一 部署或参与方自行部署的方式，以满足监管要求；

● 对于与区块链系统外部数据进行交互的智能合约，外部数据源的影响范围应仅限于智能合约范围内，不应影响系统的整体运行；

●涉及变更区块链账本信息的智能合约，必须有相应的差错处理约定，确保数据的正确性；

●区块链系统中实现的智能合约也应考虑智能合约的生命周期管理，包括：订立、履行、变更、中止、审查、监督等。

3.9 网络安全

DBB 会基于以太坊 devp2p 协议系列的延续，包含 libp2p 和 IPFS 标准，将有效改善隐私性、强健性、延迟及模块化。

在 DBB 网络中，我们专注解决电商交易信任问题，售卖产品的文字、图片或视频信息存储不做考虑，因此基于 devp2p 协议对 DBB 是足够使用的。当然在现在网络架构和电子商务中，服务器或云服务器都成为垄断性能力，即使简单的云服务器使用，对于普通个体电商参与者都可能成为一种障碍。DBB 基金会，将关注 p2p 网络服务，去中心化算力项目等有助于降低个人搭建 web 应用的项目，当然卖家商品信息存储在中心化机房，并不影响 DBB 网络的使用。

第四章：DBB 账户管理

4.1 DBB 账户管理

（1）用户管理。用户管理主要解决用户身份到区块链地址的映射关系、用户隐私的保密性。

（2）账户管理。账户管理负责用户的账户管理，包括账户的注册、登录、注销以及账户跟密钥的不相关性处理。账户注册时，将原来用户习惯的用户名、密码等身份信息映射到区块链地址。

（3）密钥管理。在全托管的模式下，密钥管理系统负责用户密钥跟账户的关联、密钥安全管理和丢失找回。用户密钥在客户端生成，用户可以选择将密钥保存在钥保险箱或者委托给关联账户的方式以便密钥丢失后找回。

（4）权限管理。权限管理模块负责用户账户、密钥系统、节点加入和退出、数据访问等权限的控制和管理。包括账户委托权限、节点共识权限以及用户数据访问权限等。审计权限是为监管机构提供审计的功能，对访问权限和数据范围做严格的控制，对共享账本上交易不相关性的用户可以做到用户关联。账户委托权限用来控制用户账户委托关系的访问控制。共识权限对参与或者新加入节点进行共识权限管理，访问权限用来管理客户端对区块链上的数据查询权限。

（5）用户信用风控管理。风控模块负责对区块链中用户交易行为进行风险控制 DBB 初始用户采用。

第五章：DBB 技术架构安全与网络安全防护

5.1 区块链本身具备的安全优势

如今黑客可以破坏整个网络、篡改数据或诱导粗心的用户落入安全陷阱。他们窃取盗用身份信息，并通过对中心化数据库的攻击及单点故障引发其他安全威胁。但区块链技术中的数据存储和共享数据的模式，与目前信息安全是截然不同的做法。比特币和以太坊都使用相同的密码学技术来保障安全交易，但现在也能够作为一种防范安全攻击和安全威胁的工具。

区块链在信息安全上的的优势主要在于以下四个方面：

●利用高冗余的数据库保障信息的数据完整性；

●利用密码学原理进行数据验证，保证不可篡改；

●权限管理方面，运用了多私钥规则进行访问权限控制；

●区块链上的交易数据全部都附有交易者的数字签名，不可伪造；

●利用区块链的安全优势可以进行多重安全应用的开发。

5.2DBB 的安全防护

5.2.1 以身份验证保护边界设备安全

正如 IT 关注数据和连接向“智慧”边界设备的迁移，安全同样关心这种转变。

毕竟，网络的扩展可能会提升 IT 效率、生产力并降低耗电量，但也给 CISO、CIO 和整个公司带来了安全挑战。很多公司因而寻求应用区块链来保护 IoT 及工业 IoT(IIoT) 设备安全的方法——因为区块链技术可增强身份验证，改善数据溯源和流动性并辅助记录管理。

5.2.2 提升机密性和数据完整性

尽管区块链最初创建时是没有特定的访问控制机制的（源于其公开分发的属性），有些区块链实现如今却在解决数据机密性和访问控制问题。在当今数据极易被篡改或伪造的时代，确保数据机密性和完整性问题无疑是巨大的挑战。但区块链数据的完全加密特质确保了这些数据不会被非授权方染指，但又仍具有流动性（中间人攻击几乎没有成功的可能）。

5.2.3 更安全的 DNS

DBB 是一个探索分布式 DNS 概念的新项目，理论上分布式 DNS 可以应付访问请求洪水，不会因响应过载而宕机。DNS 之类互联网关键服务可被黑客利用来制造大规模掉线和攻击公司企业，因使用区块链方法的可信 DNS 基础设施，将能大幅增强该互联网核心信任基础设施。

5.2.4 网络层访问控制

在 DBB 中允许节点自由进出网络，且区块链的网络层没有登记用户身份。金

融行业的风险和安全性相对更高，未登记身份的节点自由进出网络为系统安全带来很多不可控性。DBB 区块链技术在金融行业应用时，应结合业务需求，分析必要使用公有链，并登记网络中节点的身份。此外，还应采用 VPN 专网、防火墙、物理隔离等技术对节点，特别是矿工节点的物理网络和主机进行保护。

5.2.5 共识层安全

DBB 使用分布式共识协议来防止单点故障等问题，有效防范了双重花费、矿工恶意封锁某个用户的交易等攻击。但这都建立在区块链网络节点的权利分布均匀、不存在 51% 攻击的前提下。很大程度上取决于区块链的一致性不被破坏。因此，设计合适的共识算法对于区块链应用的安全性至关重要。

5.2.6 智能合约层安全

区块链 2.0 版本中引入智能合约层，提出区块链即服务（BaaS）的概念。智能合约层提供了自动化脚本代码组成的智能合约来开发应用、操作数据。智能合约本质上而言仍然是编程语言，如果它是图灵完备的，支持循环指令，攻击者就可能构造带有死循环代码的交易对网络中的矿工发起 DoS 攻击。

第六章：DBB 优势与应用

在跨境贸易融资的业务领域内，无论是信息化前所使用的纸质单证还是信息化后所使用的基于 EDI 或基于互联网的电子单证都是存在于不同的层次，如：

1）国际性数据标准体系，如 UN/CEFACT 从 1981 年到目前为止共发布的 35 份建议书 7 套标准和 5 套技术规范；

2）区域性数据标准体系，如中国所制定的由通用信息类标准、数据元类标准、以及单证格式与数据元布局类三部分组成的中国国际贸易单证标准体系；

3）企业内部数据标准体系，作为企业连接业务与数据的纽带，帮助企业打通内部各部门间的数据，提升企业生产和运营效率，甚至全面实现大数据战略。

运用区块链网络是期望通过分布式账本技术打破不同系统间的数据孤岛，但如果数据在不同的区块链网络中以非标准、不统一的形式进行呈现，那么这些更多、更精细化的数据只会给其他参与方在实际业务中进行理解带来更大的挑战。所以各个层面的区块链网络应当自上而下地根据上述不同层次的数据标准体系制定其自身账本的数据标准。

6.1 DBB 优势

优势一：开放的接口

DBB 通过对现在已有的区块链应用网络的研究，通常可以从两个维度对账本进行归类：

1）基于所覆盖的地域范围进行归类，如：

私有账本；

区域性账本；

国际性账本；

2）基于所侧重的细分业务进行归类，如：

订单和商业发票可能记录在贸易融资业务账本中；

提运单和运输数据可能记录在物流业务账本中；

各类许可证和申报单据可能记录在行政监管业务的账本中；

因此，一笔跨境贸易的各项子流程数据在初始状态下很可能散落在各个层次的各类账本中那么无论是对于希望使用数据推进业务流程的贸易或服务参与方，还是对于希望使用数据验证交易的金融或监管参与方，都希望能够找到一种跨账本整合数据的方法，这样才能使各个层次以及各个细分领域中各账本的数据能够相互融合，进而催化出更广泛、更深刻的应用价值。

优势二：信息安全

在跨境贸易的场景下，跨账本的互通通常意味着信息存在跨国的流转。然而在当前这个信息技术高速发展的时代，信息安全是保障国家安全的重要组成部分，所以，在进行区块链技术应用的整体设计时，如何处理好信息的隐私与共享、封闭与开放、应用与保护、安全与发展的关系，是各国所面临的共同挑战。

可以从以下 3 个方面来应对信息安全的挑战：

制定跨国的区域性或国际性信息安全标准及行为准则；

制定跨国的区域性或国际性信息安全法律法规或国际公约；

在区块链技术的选型上应满足保密性、完整性、可用性、可控性和不可否认性等 5 大信息安全的基本特性。

优势三：优化流程协同

DBB 借助区块链技术的数据一致性特点，使得区块链系统有能力覆盖跨境贸易流程中各个环节的参与方，打通贸易数据流，为各参与方深层次的协同合作提供最重要的基础。

此外，在部分标准化环节中引入智能合约的应用，在前序数据满足条件时自动触发执行后续相关业务，在提高自动化程度，增加效率的同时，也能在一定程度上规避信用欺诈风险和操作风险，对于建立跨境贸易参与方与参与方之间、参与方与海关之间、甚至海关内部的协作和交流机制都有非常广阔的应用场景。

优势四：高吞吐量

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，DBB 的处理性能已经能满足万级 TPS 的需求。如果再引入 Off-Chain 等机制，还能进一步大幅提高交易吞吐量。

优势五：快速交易验证

通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，DBB 可以实现秒级的快速交易验证，满足绝大部分区块链应用场景的用户体验。

6.2 DBB 应用

6.2.1 金融领域

DBB 在国际汇兑、信用证、股权登记和证券交易所等金融领域有着潜在的巨大应用价值。D 将区块链技术应用在金融行业中，可省去第三方中介环节，实现点对点的对接，从而在大大降低成本的同时，快速完成交易支付。

6.2.2 跨境支付

DBB 利用区块链技术建立的分布式网络，让 DBB 的用户可以实现跨境汇款低费用甚至是零费用，并且能以极快的速度完成跨境转账。DBB 的点对点支付方式去除了第三方金融机构中心，不但可以全天候支付、瞬间到账、提现容易及没有隐形成本，解决了跨境汇款手续费成本高、效率低、操作不方便等痛点问题，也有助降低跨境贸易资金风险及满足跨境贸易对支付清算服务的便捷性需求。

6.2.3 供应链管理

供应链金融

传统供应链金融领域，核心企业的信任背书只支持一级供应商或一级经销商，无法扩展到二级、三级供应商，因为核心企业的绝对优势地位，常常导致二级、三级供应商存在较大的融资需求。基于 DBB 的供应链金融，可以将核心企业的信任背书传递到二级、三级甚至更远层级的供应商，使围绕核心企业的生态链系统可以健康发展。同时，对于金融机构，也可以通过作为节点方式，回放相关供应商的历史数据，降低金融风险，提升金融信任。

供应链清结算

对于传统的复式记账而言，最大的问题莫过于供应链的清算过程。基于 DBB 区块链的解决方案，可以围绕着核心企业的多个供应商，当交易完成后，通过供应商和核心企业确认的交易签名信息，同步在区块链上，使相关的交易记录无法进行任何篡改。实现交易即清算，令牌即结算等高效的供应链清结算服务。

6.2.4 溯源领域

DBB 区块链可应用于各类物品的溯源领域，主要采用了区块链的“链”特性。溯源领域包括食品溯源、产品溯源、奢侈品溯源、珠宝玉石溯源等。将代表实物资产的资产代码在区块链的各个环节流通，保证溯源的信息不可篡改，且可完整追溯。DBB 在溯源领域，可通过其自身具有的备注字段，为每个溯源环节加多自定义的溯源信息（如资产故事等），以实现资产价值的提升。

6.2.5 高安全领域

区块链是由不同的组织、不同的机构或个人组成的价值网络，任何个体对账本的修改均不会造成数据的篡改。区块链自身具备金融级的签名算法，且采用了分布式存储的技术，在一定意义上讲，区块链的安全等级高于现有金融系统。因此，区块链非常适合高安全等级的军事领域、金融领域。

6.2.6 自征信领域

随着国家推行实名制模式，逐步建立诚信社会，使个人、机构的不诚信成本提高，但目前大多数征信信息掌握在 BAT 中，对于广大中小企业或组织是难以涉足的。DBB 通过开放式接入原则，支持各个组织、个人对每个人的征信进行写入，并提供给全社会进行征信调阅，为建立自征信社会提供了行业标准。

第七章：DBB 团队及资本

Mohsen Ahmadi/CEO

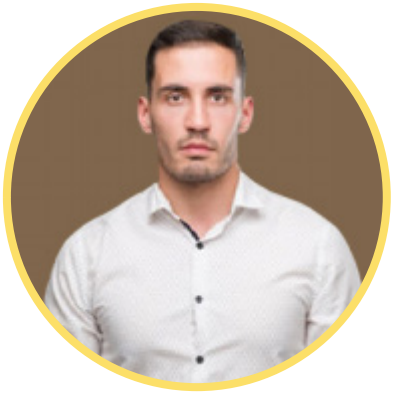
曾任美国富国银行公司核心项目负责人，15 年中国及北美银行应用系统、金融软件系统设计和研发经验，新加坡南洋理工大学计算机博士。

Tom Radionov/CTO

毕业于杜克大学，并取得计算机科学学士学位，毕业 7 年内，取得哈弗大学计算机科学博士学位。Tom Radionov 在技术领域拥有超高的学识，在甲骨文、微软集团工作期间将个人价值集中化提现。Tom Radionov 成功开发和部署了新加坡首个将金融技术应用到商业的产品，其技术证明了技术开发的更多可能性。

Vong Pham/ 核心开发者

资深后端开发工程师，为多个区块链产品开发了网页钱包和区块链浏览器。并开发了基于多种加密货币的 RPC 协议，此协议可以和多个交易应用端口互换市场数据。



Mark Prugh/ 核心开发者

毕业于新加坡国立大学，并取得电脑科学学士学位。曾就职于微软亚太区总部、脸书亚太区域总部，并在团队中担任重要角色。Mark Prugh 也是数字货币资深爱好者，2013 年开始研究与区块链技术，并多次参与至项目开发中，经验非常丰富。

Justin Aggarwal/CMO

Justin Aggarwal 拥有十多年的营销管理经验，曾带领部下多次创造月度业绩第一、季度业绩第一的成绩。在 DBB，Justin Aggarwal 负责制定亚太及大中华区域的营销战略，以及公司整体走向的把控。

DBB 资本

Halodata 于 2006 年创建，主要业务在信息安全、企业移动性、业务连续性 3 个领域。Halodata 向东盟市场推出了数据安全、企业移动性和业务连续性方面的下一代创新解决方案，Halodata 拥有久经考验的业绩记录，以及在金融、能源、政府、教育、制造业、媒体等多种行业的杰出终端用户基础。

Fortune Capital Management Pte Ltd(富 鑫 集 团) 自 1995 年于新加坡设立至今，已有 22 年历史，过去总管理资产约美金 5 亿元，总共投资 302 个项目，累积了丰富的投资、投资后管理及并购经验。富鑫过去 22 年的投资遍及美国 (尤其是硅谷)、台湾、中国、香港、新加坡、印尼、马来西亚、澳洲、越南。

DeClout 是下一代信息和通信技术的全球建设者，DeClout 投资、孵化和扩展公司，总部位于新加坡，在亚太地区和非洲拥有庞大的网络。

Golden Gate Ventures 是一家在东南亚投资的早期风险投资公司。自 2011 年，公司已在亚洲 7 个多国家 / 地区投资了 30 多家企业。公司投资涉及到许多不同领域的互联网和移动初创企业，包括电子商务、支付、市场、移动应用和 SaaS 平台。

第八章：代币发行与市场规划

8.1 DBB 代币发行

通证全称： Document bill bit

英文简称： DBB

发行数量： 2 亿枚

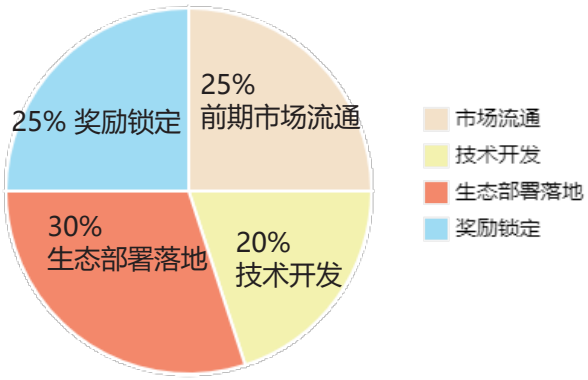
分配比例： 前期 25% 用于市场流通（5000 万）

20% 用于技术开发

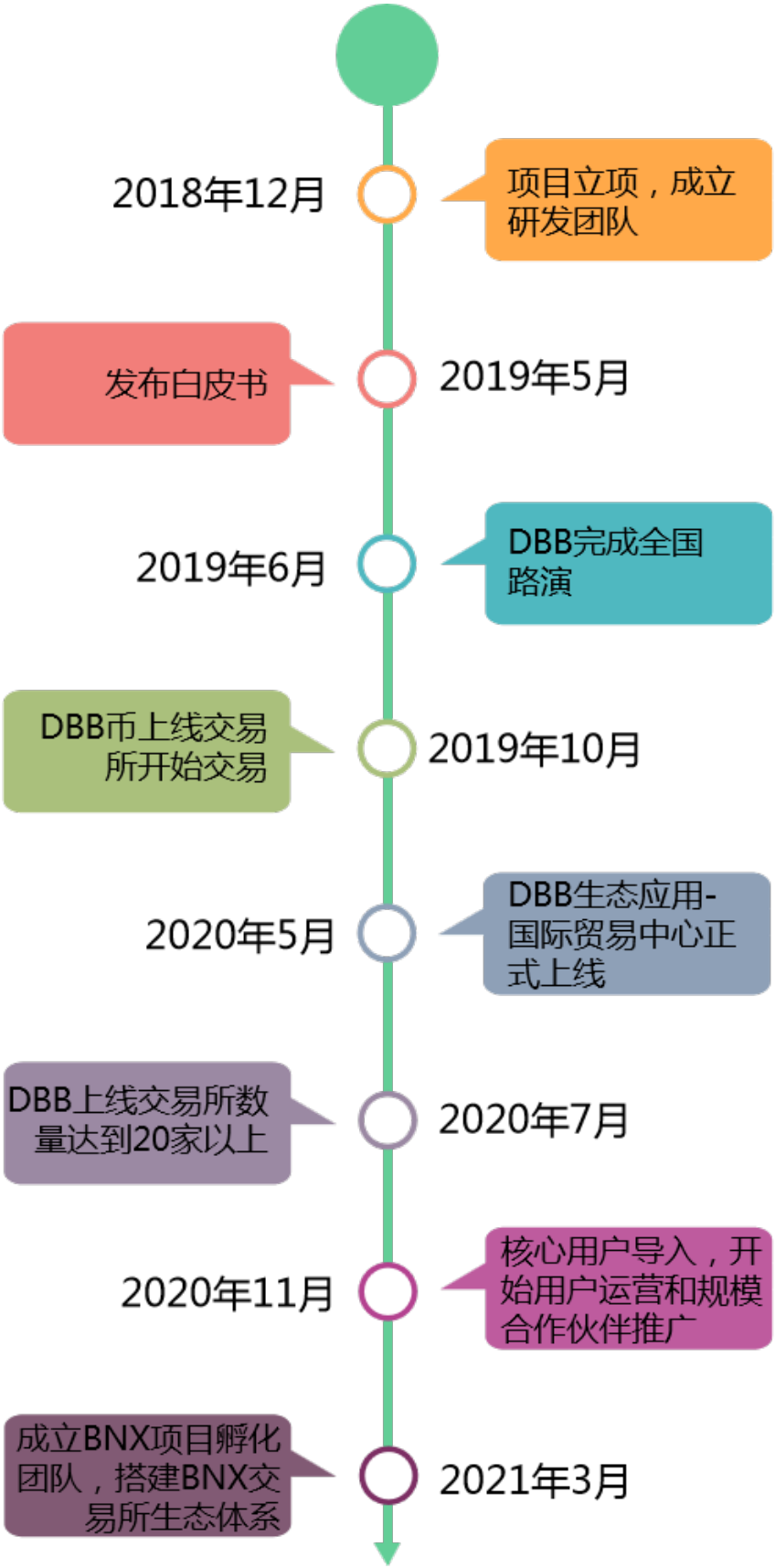
30% 生态部署落地

25% 奖励锁定

DBB代币发行分配



8.2 DBB 市场规划


2018年12月
项目立项，成立研发团队
发布白皮书
2019年5月
2019年6月
DBB完成全国路演
DBB币上线交易所开始交易
2019年10月
2020年5月
DBB生态应用-国际贸易中心正式上线
DBB上线交易所数量达到20家以上
2020年7月
2020年11月
核心用户导入，开始用户运营和规模合作伙伴推广
成立BNX项目孵化团队，搭建BNX交易所生态体系
2021年3月

免责声明

本白皮书只用于传达信息之用途，并不构成买卖 DBB 股份或证券的相关意见。以上信息或分析不构成投资决策，或具体建议。

本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖、任何形式证券的行为，也不是任何形式上的合约或者承诺。

DBB 明确表示相关意向用户明确了解 DBB 平台的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意为此承担一切相应结果或后果。

DBB 明确表示不承担任何参与 DBB 项目造成的直接或间接的损失，包括：

（1）本白皮书提供所有第三方信息的可靠性

（2）由此产生的任何错误，疏忽或者不准确信息

（3）或由此导致的任何行为

DBB，是一个在 DBB 平台使用的数字加密货币。在写这段文字时 ,DBB 币尚且不能用来购买相关物品或者服务。我们无法保证 DBB 币将会增值或贬值，那些没有正确使用 DBB 币的人将有可能失去使用的权利，甚至会有可能失去他们的 DBB 币。DBB 币不是一种所有权或控制权。控制 DBB 币并不代表对 DBB 或 DBB 应用的所有权，DBB 币并不授予任何个人任何参与、控制、或任何关于 DBB 及 DBB 应用决策的权利。

风险提示

1、证书丢失导致的丢失 DBB 币的风险

购买者的 DBB 币在分配给购买者之后会关联到购买者的 DBB 账号，进入 SEC 账号的唯一方式就是购买者选择的相关登录凭证，遗失这些凭证将导致 DBB 币的遗失。最好的安全储存登录凭证的方式是购买者将凭证分开到一个或数个地方安全储存，而且最好不要储存在公开场所或者会有陌生人流出现的地方。

2、以太坊核心协议相关的风险

DBB 币基于以太坊协议开发，因此任何以太坊核心协议发生的故障，不可预期的功能 问题或遭受攻击都有可能导致 DBB 币或者 DBB 应用以难以意料的方式停止工作或功 能缺失。关于以太坊协议的其它信息 http://www.ethereum.org。

3、购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制购买者的 DBB 币，为了最小化该项风险，购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

4、司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体施加影响则 DBB 应用或 DBB 币可能受到其影响，例如法令限制使用，销售，电子 Tokens 诸如 DBB 币有可能受到限制，阻碍甚至直接终止 DBB 应用的发展。

5、DBB 应用缺少关注度的风险

DBB 应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对 DBB 币和 DBB 应用造成负面影响。

6、DBB 相关应用或产品达不到 DBB 自身或购买者的预期的风险

DBB 应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何 DBB 自身或购买者对 DBB 应用或 DBB 币的功能或形式 (包括参与者的行为) 的期望或想象均有可能达不到预期，任何错误地分析或者底层设计的改变等均有可能导致这种情况的发生。

7、黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 DBB 应用或 DBB 币功能的可能性，包括服务攻击，Sybil 攻击，游袭，恶意软件攻击或一致性攻击等。

8、漏洞风险或密码学科突飞猛进发展的风险

密码学的突飞猛进的发展或者其他相关科技的发展诸如量子计算机的发展，或将破解的风险带给加密 Tokens 和 DBB 平台，这可能导致 DBB 币的丢失。

9、缺少维护或使用的风险

购买 DBB 币应该被认为是一种对于下一代电商应用开发的支持和投资，而不是一种投机行为。虽然 DBB 币在一定的时间后可能会有相当的市场价值，导致早期投资者产生较大的收益，不过如果 DBB 平台缺少维护或没有足够的应用，这种升值并没有太多的实际意义。

10、未保险损失的风险

不像银行账户或其它金融机构的账户，存储在 DBB 账户或以太坊网络上通常没有保险。任何情况下的损失，将不会有任何公开的组织或者个人为你的损失承保。

11、应用存在的故障风险

DBB 平台可能因各方面的原因故障，无法正常提供服务。

12、无法预料的其它风险

密码学 Tokens 是一种新兴的技术，除了本白皮书内提及的风险外，此外还存在着一些区块链业内以及 DBB 团队尚未预料到的风险。