

BSGX 白皮书

基于区块链技术的全球无障碍支付系统

目录

第一章 区块链技术与全球支付应用	4
1.1 支付行业简介	4
1.2 区块链与通证经济	6
1.3 区块链的价值应用	7
1.4 区块链正在改变全球支付格局	9
1.5 字节链通的诞生	11
第二章 BSGX 概述	13
2.1 BSGX 简介	13
2.2 设计原则	14
2.3 应用目标	15
2.4 核心优势	16
第三章 BSGX 应用功能模块	17
3.1 钱包系统	17
3.2 全球支付清算系统	18
3.3 多币种管理与交易系统	19
3.4 跨境金融服务	21
3.5 配套功能支持	22
第四章 BSGX 技术体系	24
4.1 技术概述	24
4.2 技术整体架构	25
4.3 共识机制	27

4.4 安全加密算法	29
4.5 P2P 协议	31
4.6 恶意攻击防范与惩罚机制	31
4.7 支付系统的风险控制	33
第五章 BSGX 通证经济模型设计	35
5.1 BSGX 代币经济学	35
5.2 BSGX 的价值属性	35
5.3 市场激励	37
5.4 BSGX 的应用价值	37
5.5 BSGX 流通场景示例	38
5.6 推动价值无国界流通	39
第六章 项目落地与发展	41
6.1 全球团队	41
6.2 项目落地支持	42
6.3 市场合作	42
6.4 BSGX 生态发展基金	43
第七章 风险提示与免责声明	45
7.1 风险提示	45
7.2 免责声明	45

第一章 区块链技术与全球支付应用

1.1 支付行业简介

支付交易是社会经济活动的基础，其职能主要由银行承担，并有银行、银保监会进行监管。随着信息技术的迭代更新、支付场景的移动端化以及线下支付的小额高频化，支付结算的各种场景及终端需求快速增长，银行体系已经越来越难以满足日益增长的支付需求，第三方支付通过承担大量小额高频的支付结算需求，与传统金融机构的大额低频的结算业务形成互补关系，为客户提供更加便捷、个性化的支付服务。

第三方支付的市场规模从 2013 年 16.9 万亿，快速增长到 2023 年 200 万亿，交易规模增长超过 10 倍，近三年复合增长率超过 80%。预计 2025 年将达到 400 万亿元的市场规模，而未来三年仍将保持较高的增长。

经历超过十年的行业发展后，互联网支付、移动支付的兴起，进一步推进超过百万亿元交易规模的第三方支付行业的发展，第三方支付的崛起在某种程度上大幅度第改善了转账手续费高、到账时间慢等传统银行问题。

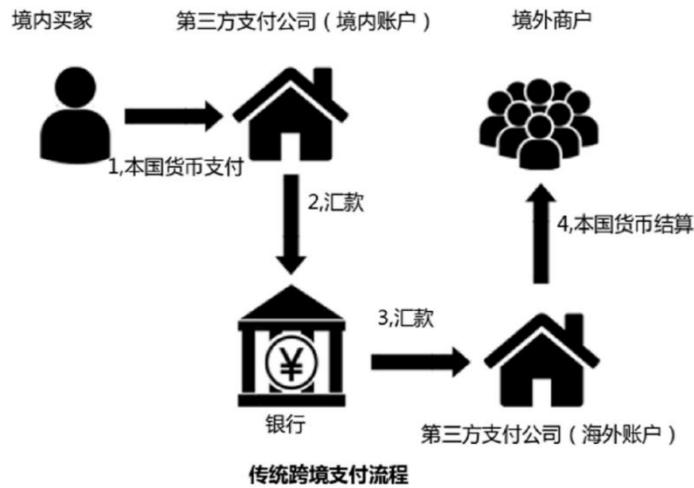
传统意义上的第三方支付包含网络支付、移动支付、银行卡收单业务、跨境电商等。第三方机构作为非金融机构在银行、商户、用户之间建立起支付结算通道，一方面与银行签订协议，搭建数据交换和信息传输网络；另一方面链接商家、整合用户，逐步形成以交易为核心的平台并建立起快速便捷而有效的交易结算服务。

当前，第三方支付市场已经成为互联网金融领域最为成熟的行业，并作为基础服务广泛应用于各类场景之中，支付是交易活动中信息流、资金流的重要停留节点，掌控支付就意味着掌握流量的入口，对于互联网企业而言，流量带来了用户、数据以及资金流，是万物物联时代的核心竞争力；对于区块链企业而言，流量的导入活跃了加密数字货币的应用场景，在区块链发展的早期阶段，掌握支付终端意味着掌握了渠道入口。

虽然第三方支付相较于银行清结算体系，有了很大进步，但第三方支付依然是基于银行的清结算体系而生，传统银行清结算体系依然存在诸多弊端，亟待解决，下面我们以跨境支付为例，可以清晰的看好其核心问题所在。

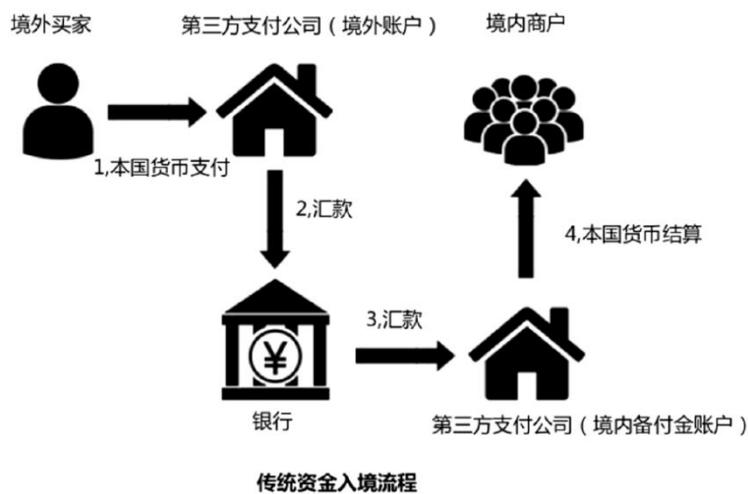
1) 效率低

传统跨境支付模式中银行会在日终对支付交易进行批量处理，通常一笔跨境支付需要至少 24 小时才能完成。而且传统支付模式中，银行间需要进行人工对账，这也会耗费一些时间。



2) 费用昂贵

传统跨境支付模式有四块成本：支付处理成本、接收费用、财务运营成本和对账成本。根据世界经济论坛报告《全球金融基础设施的未来》，一般而言，汇款人的汇款费用是汇款金额的 7.68%。银行使用代理银行完成一笔跨境支付的平均成本在 25 美元到 35 美元之间，该成本是使用自动交换中心 (Automatic Clearing House, ACH) 以日本为例完成一笔结算，支付成本的 10 倍以上。



3) 流动性差

传统跨境支付模式中，银行为了保持流动性，需要在银行账户中持有多个国家的货币，这种账户被称为“往来账户”。由于汇款行难以预知代理行具体何时会确认自己的转账信息，不得不在往来账户中持有一定量的外币。

4) 不可抗力因素

因某国家货币受到政策或战争的变动等外部不可抗力原因，很大可能丧失信任背书，导致所发行货币的国家货币贬值以及无法流通，而且传统跨境支付模式中，并不是所有银行才能加入 SWIFT，或者说加入 SWIFT 并不经济。

区块链技术的出现，对于数以百万亿计的支付产业产生巨大的冲击，网络支付、移动端支付以及更小额、更高频的 M2M（机器对机器）支付的理论和时间正在向泛中心化的网络支付聚焦，基于区块链技术的支付手段成为当前研究的热点和重点。同时，以区块链技术为依托，诞生的加密数字货币，为支付模式的变革，带来了强有力的变化。

1.2 区块链与通证经济

互联网经过 40 余年的发展，为人们带来了电子邮件、网络公司、社交媒体、移动网络、大数据、云计算以及物联网等新事物及新概念，极大地降低了搜索、协作和交换信息的成本，以及多领域准入门槛，促进了诸如新媒体业、新娱乐业、新零售业的出现，并在其基础上产生了全新的工作组织架构模式以及前所未有的数字化商业模式。然而对于商业和经济活动来说，仅仅是信息的分享和传输并不能满足经济社会的发展。当缺少第三方机构提供的检验信息时，人们无法快速确认交易方身份，也无法在彼此间建立商业往来活动所需的信任关系。

直至 2008 年，中本聪(Satoshi Nakamoto)首次发布了一种点对点的现金系统及其基础协议—比特币：白皮书《比特币：一种点对点网络中的电子现金》，比特币诞生。经过十余年的发展，比特币背后的区块链技术逐渐为更多的人所认识，并在其基础上继续发展创新。

得益于区块链技术的特性及优势：块链式数据结构来验证与存储数据、分布式计算机节点的共识算法来生成和更新数据、密码学保证数据传输和访问的安全、自化脚本代码组成的智能合约来编程和操作数据而形成一种全新的分布式基础架构与计算范式。此外，区块链技术能够在网络中建立点对点之间的可靠信任，使得价值传递过程脱离了对中介的依赖，既公开信息又保护隐私，既共同决策又保护个体权益，这种机制提高了价值交互的效率并降低了成本。

区块链在信任中发挥的作用正犹如互联网在信息中发挥的作用。基于在提高透明性及保护隐私方面的能力，区块链将“信任”这种最深刻的人类需求连接起来，为人们通向一个更公平、更高效及更四通八达的全球商业系统指出了一条前进的道路。区块链技术拥有极大的潜力，将为传统商业贸易、金融行业、政府部门，乃至人类社会带来巨大变革。

随着区块链技术的发展，依托区块链底层技术的通证经济也在高速繁荣。区块链让互联网从“信息”跃迁到“价值”，给互联网和数字世界带来两个独特的功能特性：

- 第一是技术性的区块链信用层，用于数字世界的“价值转移”；

- 第二是经济性的通证(Token)，用于数字世界的“价值表示”。

随着区块链技术特别是基础公链的大发展，各行各业对区块链应用进行了泛探讨与尝试，落地的可能性在逐步呈现。目前，各大应用平台和国际顶级机构均在区块链的价值表示和价值转移的基础上，利用通证的激励和治理功能，动员各类用户群体与合作伙伴，改造互联网平台，以期构建一个公平、公正、公开的去中心化价值生态。

但是，目前的互联网技术还不能实现点对点的价值传递。不同于信息传递的可复制特征，价值传递需要保证权属的唯一性，所以当前价值的传递仍然需要依赖中心机构承担记账功能。那么，如果网络本身能够提供可靠的记账功能，将使得价值传递不再完全依赖于中心机构，可以实现价值的点对点转移。

在区块链的分布式总账技术(DLT, Distributed Ledger Technology)和通证经济模型的支持下，能让参与各方在技术层面建立信任(Trust)，有潜力成为构建未来价值自由流通网络的基础设施，即形成价值互联网(Internet of Value)。

1.3 区块链的价值应用

通过对比分析、研究各领域的典型应用案例及相关参考文献，并结合自身研发和应用实践，我们获得了一些有助于在业务中推广应用区块链的经验，并推荐以下特点的应用场景或问题，应该积极考虑尝试区块链技术：

1) 业务开展需要进行跨主体协作

当需要为开展跨主体的业务建设 IT 系统时，传统的解决方案通常是两种思路。要么建立和运营一个中心化的系统来处理各个参与方的业务需求，业务数据由中心化的组织维护；要么采用 SOA 架构，由各个参与方发布服务接口，并相互调用，数据仍然维护在各个参与方。如果采用中心化的方案，若是业务的参与方之间是相对独立平等的，要开发建设一个中心化系统是很困难的，包括协调、立项、成本分摊等问题。如果采用 SOA 的方案，则技术实践上比较复杂，技术方案缺少通用性，难以支持复杂的业务。此外，从数据的角度来看，无论是中心化的方案还是 SOA，都难以实现数据防篡改。

在业务参与方之间相对独立平等的跨主体业务协作的场景下，利用区块链的共有数据、防篡改、分布式和数字化合约的特点，能够把一些以往需要在业务层面协调解决的问题，放到技术层面来解决，使得问题的解决过程更高效、灵活以及更具客观性。

2) 业务开展需要参与方之间建立低成本信任

大多数业务开展都需要建立一定的信任基础，尤其是跨主体的场景下。对信任建立困难、

信任维护成本高的应用场景，区块链可提供非常有效帮助。我们从三个方面来考察区块链如何建立低成本信任：

- 数据可信：传统的解决方案中，数据通常是以中心化的方式存储，本应共有的业务数据通常却被强势的参与方持有。这种模式下，数据的可信度是由数据持有者的商业/社会信用来保证的，只能建立主观的可信，对于一些重要的领域，仍需要付出额外的成本来防范数据被恶意篡改的风险。 区块链的解决方案是结合了密码学哈希和数字签名，以区块链条的形式将数据的变更历史按时间先后链在一起，并通过共识协议使得参与的各方都共同拥有这些数据。由于多方分别持有相同的数据副本，并且数据被签名确认，并记录数据的“指纹”(哈希值)，以密码技术保证了数据无法被篡改，数据因此变得可信。 区块链使数据持有变得去中心化，以技术手段实现数据客观“可信”。
- 合约履行：通常的合约(或者契约、协定、合同)的履行从根本上是由法律来保障的。合约被自觉履行一般都是因为有利益、道德或法律后果，受许多主观因素影响。商业活动中为了防止违约、或对违约进行追索，需要付出高昂的成本(担保、保险、律师费、漫长司法程序等)。区块链智能合约的本质是一套数字化形式的契约，由计算机确保严格执行。执行方式上，通常的合约是事后以人的主观意愿来执行；而智能合约是在触发条件被满足后，由计算机程序来保证合约及时地执行，具有客观性。我们把资产数字化到区块链或与区块链锚定，采用智能合约来描述对资产关系的承诺，同时智能合约的执行过程和结果被区块链严格记录，这样便可以降低履约成本和确保高效履约。区块链智能合约带来的是“契约”的一种新的更精确的表示形式，以及一种更客观、更严格的执行方式。由于契约是我们社会活动的基础，因此这种变化将会带来更广泛的社会影响。
- 历史可证明：区块链固化了交易历史，并提供对交易历史的追溯查询，保证交易的不可篡改和不可抵赖。如果某个事件发生时，这个事件连同时间戳一起被记录到区块链中，将来就可以通过区块链证明这件事确实在这个时间发生过。因此区块链为参与交易的各方保留了可信的历史记录。

3) 业务过程存在长交易、长周期链条

业务在多主体间流转时，难以确定间接主体的真实性和有效性，同时由于多主体间的业务隔离，难以延伸出多级业务。区块链从技术上保证整个长交易、长周期链条的各参与主体身份真实，数据可信，实现信用的多级传递，促进业务链条扁平化，提升业务效率。比特币作为区块链技术的一种典型应用，在交易市场上市值已达千亿美元，这样的一个高市值系统却是以开源的方式在公共网络上运行了多年，表现出了良好的安全性和健壮性。比特币系统的表现揭示了一个重要事实——以客观区块链技术为手段可以直接建立信任，而 不需中介背书。如果我们把区块链技术推广运用到更广泛的产业、金融、公共服务等场景，将使社会的生产分工方式产生巨大变化，这些变化包括：

- 商业交易过程更容易达成信任，降低风险，使交易更具确定性
- 商业交易中间环节被缩减，多方交易可直接达成
- 传统中介的中心化的服务模式将发生巨变

这种影响目前已经逐渐显现，随着区块链的逐渐成熟和应用的不断丰富，这种影响力将会像蝴蝶效应一般逐步放大和深入到整个社会，推动去中心化或多中心化主体间的高效协同和共识决策。人类因掌握“工具”而发展文明，我们相信区块链是一种新的“工具”，最终将促进人类社会的进步发展。

1.4 区块链正在改变全球支付格局

1) 传统支付体系的缺陷

传统支付体系的价值转移需要依托清算中心进行银行间的数据交互。随着互联网金融的发展，第三方支付（特别是移动支付）出现了爆发式增长，但它仍是依靠中心化的方案来解决价值转移。中心化方案是通过某个公司或者政府信用作为背书，将所有的价值转移计算放在一个中心服务器（集群）中，尽管所有的计算也是由程序自动完成，但却必须信任这个中心化的人或者机构。事实上，通过中心化机构的背书来解决信用问题，也只能将信用局限在一定的机构、地区或者国家范围之内。

在传统支付体系的运作流程中，甲银行的 A 客户向丙银行的 F 客户发起一笔支付，需要借助中介机构背书与清算。假设甲银行在央行没有开立清算账户，甲银行必须通过乙银行作为代理行，乙银行和丙银行之间的支付则通过央行的清算账户进行结算。最后，客户 F 收到 A 转移的货币。若涉及跨境支付，过程更为复杂。

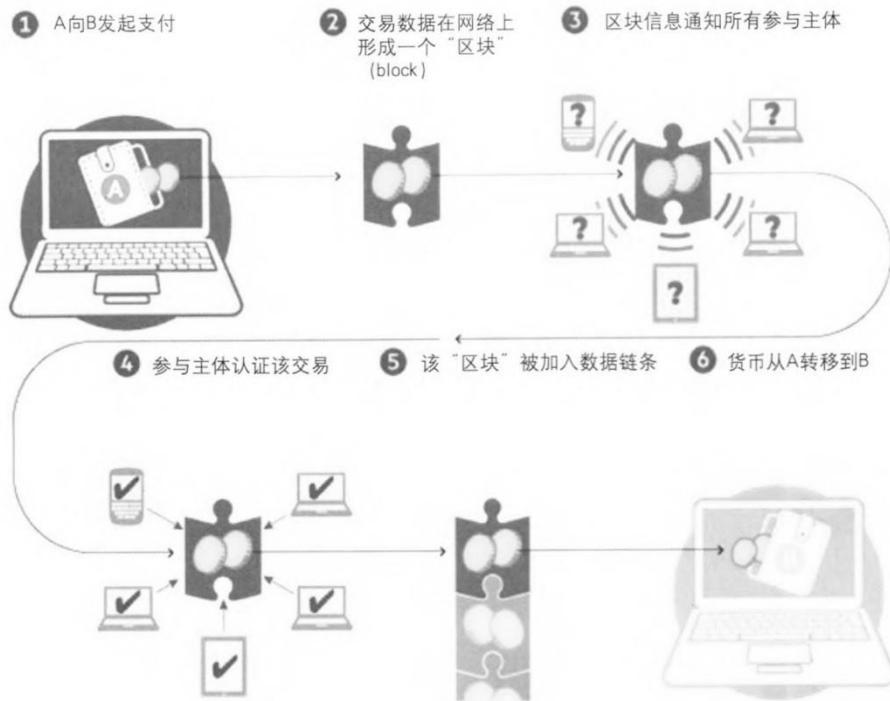
目前，跨境贸易交易清算支付都要借助第三方中介，要经过开户行、央行、境外银行（代理行或本行境外分支机构），每一机构都有自己的账簿系统且互相隔离，彼此之间需要建立代理关系，需要有授信额度；每笔交易需要在本银行记录，还要与交易对手进行清算和对账等，导致交易速度慢、成本高。众多的中小企业，特别是发展中国家的中小企业，在跨境支付上付出的成本更是高昂。

2) 突破互联网价值转移的局限

互联网诞生的最初，要解决的核心问题是信息制造和传输，但其无法解决价值转移问题，即在网络中以每个人都认可的方式，将某一部分价值（包括货币资产、有价证券、金融衍生品等）精确的从某一个地址转移到另一个地址。区块链技术能在信息不对称和信息不确定的环境下，建立起满足经济活动所需的“信任”生态体系，突破互联网价值转移局限。比特币

是区块链技术在金融领域的首个运用，但如果区块链上运行的不是比特币而是法定货币，商业银行形成联盟后建立起支付私链，货币只是作为区块链上的数字资产被登记、转让，不受比特币每秒 7 笔交易的限制，就能借助区块链技术迅速完成支付和清算。

区块链技术下的支付流程示例：



3) 区块链技术对支付体系的变革

与传统支付体系相比，区块链支付是交易双方直接进行数据交互，不涉及中介机构。即使部分网络瘫痪也不影响整个系统运行，极大地降低了中心化支付方式的系统性风险。从图上可知，区块链技术下完成一次支付不需要任何中心化机构的参与，市场中的银行和客户完全可以建立一个私链完成支付过程。

假设 A 向 B 发起了一笔超过其账户余额的支付，由于在分布式账簿中，每个参与主体都有所有历史支付的数据拷贝，那么在上图的第 4 步中就得不到其他主体的认证。而一旦交易得到认证，代表该交易的区块就将被永久地加入数据链条中，且该数据链条不能被修改。区块链上交易被确认的过程就是清算、结算和审计的过程，对优化金融机构业务流程具有重要意义。

基于区块链技术的支付网络有望能安全、快捷、低费用地解决全球支付问题。信任是信息交互时面临的难题，即在整个网络中的任意节点都无法信任与之通信的对方时，如何能创建出共识基础来进行安全的信息交互而无需担心数据被篡改。在没有任何中心化机构审核与背书的情况下，区块链技术能帮助市场主体解决互信问题。区块链使用算法证明机制来保证

整个网络的安全，整个系统中的所有节点能够在去信任 (truBSGXess) 的环境下自动且安全的交换数据。

通过采用区块链技术，能够实现点对点的实时交易并提升了交易效率，从而使得中央节点或是清算机构成为冗余，帮助商家节省 80%-90% 的交易费用，并且由于交易数据的真实性是通过全网节点的共同验证、是不可篡改的，因此能够消除交易中介存在的必要性、降低交易成本。除上述所列举的优势外，通过结合区块链技术还可以让支付方式更加碎片化，基于区块链技术支付手段具有更低的固定手续费成本，因此在线上、线下支付场景逐渐丰富的未来趋势下，达到满足用户日益灵活的付费需求。

1.5 字节链通的诞生

对比互联网技术的发展路径，我们发现不论是区块链技术、数字支付本身，还是基于区块链技术的支付应用，都处于行业发展早期有很多值得探索的方向。因此，我们希望可以构建一个全新的区块链支付生态系统，作为未来世界可选的互联网价值传输协议的可选项，并把整个区块链行业的易用性向前推进一步。因此，BSGX 打造了基于区块链技术的全球支付系统——BSGX 和无障碍支付媒介——BSGX 代币。

BSGX 认为，区块链和数字货币要有更长久的发展，就必须有更广泛的应用场景支持。目前随着区块链领域研究的深入，特别是针对智能合约方向的探索，逐渐有一些产品方案和实体经济生活相结合，在企业端谋求合作共赢。但真正落地并规模使用的还很稀缺，同时针对用户端的服务更是屈指可数。无论是比特币、以太币，还是基于智能合约平台新发行的各种代币，只有和实体世界有了更多的交互，才能增加数字货币自身的价值，进而促进数字货币的市场繁荣和实体世界的效率提升。

针对当前支付领域存在的痛点和挑战，BSGX 在技术和理念上进行了一系列的创新，提供完备的区块链+多场景应用的支付解决方案，使得 BSGX 有望成为区块链世界与现实商业世界的桥梁。BSGX 期望拓展区块链和支付系统的应用边界和技术边界，使普通互联网用户能感受到区块链技术的价值，并构建一个全新的基于区块链+支付技术的开发者和用户的生态系统。

BSGX 所构建的“区块链+数字货币+多元化解决方案”的支付底层体系，主要包括：

- 构建 BSGX 区块链的底层基础支付平台，为数字经济提供区块链支撑服务；
- 提供区块链+多行业应用解决方案，第三方可结合各产业实际情况，制定合理的区块链应用模型和代币发行机制；
- 打造 BSGX 生态圈，融合支付产业资产，实现产融对接服务。

未来，BSGX 将持续拓展区块链和支付系统的应用边界和技术边界，使普通互联网用户能感受到区块链技术的价值，并构建一个全新的基于区块链+支付技术的开发者和用户的生态系统。并在技术和理念上进行了一系列的创新，提供完备的区块链+实体场景应用的支付解决方案，使得其有望为成为区块链世界与现实商业世界的桥梁。

第二章 BSGX 概述

2.1 BSGX 简介

BSGX 是一家专注于为企业提供全方位虚拟货币支付解决方案的科技公司。我们利用区块链技术和智能支付系统，致力于为企业打造安全、高效的支付服务，促进企业数字化转型和商业发展。

BSGX 核心团队来自于花旗银行、苏格兰皇家银行、加拿大帝国银行、谷歌、IBM 等名企，拥有优秀的学术背景和丰富的金融产品、数字化平台搭建经验。管理团队拥有十年以银行、支付、金融及风控经验。目前，公司已在香港、东京、新加坡、雅加达和伦敦等多地开设分支机构，同时，法国，阿拉伯联合酋长国，美国，澳大利亚等地区的分公司正同步筹建中，全球覆盖的新型支付服务网络已然成型，可助力企业在 130+ 国家开展业务。

BSGX 的设计初衷是构建一个多维度的商业互通支付平台，通过区块链底层技术，构建一套完善的方案搭载在 BSGX 上，使用区块链技术产出的统一数字货币 (BSGX) 进行奖励：

- BSGX 通证经济解决方案
- 多产业互通解决方案
- 数字资产交易与流通生态体系
- 基于区块链技术的全球跨场景解决方案
- 全球无障碍跨链支付解决方案

在 BSGX，区块链和支付相融合的底层技术得到创新式应用，通过区块链技术来实现点对点的价值转移，并根据底层通讯协议，构建一个支持多个行业的去中心化的支付应用生态系统。这种分布式计算储存可以最大程度地保护系统免收攻击和故障造成的损害，去中心化的网络结构可以在短时间内解决大并发数据访问，适合未来的发展。这为 BSGX 支付系统赋予三大发展可能性：

- 点对点的商户支付方案：顾客正常的在商户平台充值，通过跳转到 BSGX 转账给商家，商家通过平台内置的 OTC 功能进行兑换货币，最终顾客充值到的金额会到商户平台上。
- 无障碍支付解决方案：支持跨场景和跨链支付，客户使用法币购买数字货币（如 BSGX），转入 BSGX 钱包，通过合作的支付机构向商户支付货款，支付机构在中间将客户

的数字货币快速转换为商户所在地法币后支付给商户。

- 第三方接口调用：基于支付接口形式，BSGX 将为全球企业和商业功能性场景提供支付服务。

未来，在各大解决方案和场景中，当 BSGX 的参与者作出了对生态的贡献，系统将根据贡献机制的计算，提供相应的合理回报 (BSGX)。而作为商业应用级区块链解决方案，未来，在公司全球的强大资本、业务网络、核心人才以及战略合作的支持下，BSGX 将形成多元化业务矩阵和通证激励生态系统，为价值无国界、无障碍流动奠定坚实根基。

2.2 设计原则

BSGX 围绕着驱动价值互联网（区块链加密支付）时代到来的核心价值，原则设计包含：

1) 价值传播原则

BSGX 以价值为导向输出结果，通过多维度展现出一个区块链支付应用和 BSGX 通证资产激励的立体模型。在模型中，所有的参与者都依附于整个载体，不再是单独的呈现结果，产业应用在一个领域里面通过不同的排列组合来体现多维度价值。

2) 自治原则

我们认为，去中心化应该更多的减少外部力量的干预，而是尽可能维持系统的正常运转。将权力释放到无数的载体上，才能进一步释放个体生产力。如果说互联网解放了生产力，那么去中心化进一步释放了生产力，让个体与个体之间达成共识，那么节点自治就是去中心化必须遵循的法则了。

3) 可持续原则

信息的传播可以创造价值，将加密资产的内在价值链路打通，实现可持续性发展，不断的催生出新的需求，诞生出新的产品和应用，促使信息不断地迭代，形成一个良性的循环。信息载体所增长的速度，不取决于起点的高度，而取决于迭代次数，随着需求的变化，迭代的次数越多，那么系统的成熟度越高，影响力越大，价值度越高，其内在价值链的可持续性就越强。

4) 高效率原则

BSGX 在区块链技术支持下，采用动态分片技术，将网络的节点根据交易请求的特点及节点资源的特点进行碎片划分，每个碎片节点仅处理对应特点的交易请求，这种分片机制提

高了节点交易的处理速度、提高了TPS；为了确保分片节点的可靠，分片将采用动态机制，每个碎片节点成员都不是固定的，将由选举产生。理论上，动态分片技术可使支付系统达到百万每秒的TPS处理能力。

5) 通证化原则

BSGX从节点记账资格竞选、数据记账打包、用户服务请求访问、分布式数据处理、分布式计算协同等各个环节确保其公平及可信程度，并从机制上实现网络生态真正意义上的去中心化通证激励。

BSGX希望可以构建一个全新的区块链支付生态系统，作为未来世界可选的互联网价值传输协议，并把整个区块链行业的易用性与实践性向前推进一步。真真正正将区块链与传统商业应用相结合，将这项技术带到人们的日常生活中去。同时，BSGX将首先通过对目标行业的渗透，获取市场份额，积累坚固的用户支持。并以此为基础，逐渐发展成为真正与现实商业应用相结合的区块链支付技术平台。

2.3 应用目标

BSGX将逐步实现以下目标：

- 打造便捷高效的支付体系：BSGX提供简单易用、安全高效的虚拟货币代收服务，实现一键代收、实时结算。BSGX中所有节点共享账簿，节点间点对点的支付通过用共识算法确认交易，并将结果广播到所有节点，不再需要支付双方建立层级账户代理关系，实现点对点价值传输，让支付更加便捷高效。
- 提升支付处理效率：BSGX通过智能化技术和区块链技术，实现支付处理的自动化和高效化，加快资金周转速度。虽然在当前的互联网时代，已经使得支付结算效率在很大程度上有所提升，但是在跨币种、跨国界、多种经济合约下，依然在多中心、多环节方面受到了限制。BSGX去中心化和点对点特征，能够减少中间环节、降低成本，在很大程度上提升交易效率，并形成一种新的支付结算方式，以驱动价值无国界流通。
- 降低支付处理成本：BSGX优化支付流程、减少人力成本和中间环节，降低企业支付成本，提高盈利能力。BSGX点对点直接交易不再依赖传统的中心金融进行信用背书和记账服务，减少支付中的中间关节，降低支付的成本。
- 实现数据透明与监管合规：BSGX利用区块链技术实现支付数据的实时记录和可追溯，满足监管要求，保障企业合规运营。通过分布式记账，使得每个参与节点都能对链上数据进行完整备份，支付数据丢失的可能性极小，部分节点数据丢失或损坏，对整个系统的运转、数据库的完整和信息更新没有任何影响。

- 提供多样化的支付解决方案：BSGX 覆盖数字货币、稳定币等多种支付方式，满足不同行业和企业的支付需求。同时，提供即时支付功能，让用户快速、便捷地进行支付交易，链上即时完成、省时高效。BSGX 还具备智能合约功能，可以自动化商家结算过程，让商家可以更快速地收到支付。
- 支持企业发行自有代币：BSGX 为企业提供发行自有代币的平台和服务，拓展企业数字化金融业务，提升品牌影响力和竞争力。

2.4 核心优势

BSGX 支付系统优势明显：

- 安全可靠：采用先进的加密技术和多重验证机制，确保用户资产安全和交易可靠性。
- 智能高效：通过智能化支付系统和智能合约技术，实现支付处理的自动化和高效化。
- 用户友好：提供简单易用的用户界面和操作流程，方便用户快速上手使用。
- 全球覆盖：支持全球范围内的支付服务，为企业提供跨境支付解决方案。
- 合规监管：严格遵守法律法规，确保平台运营合规，保护用户权益。

在应用上，BSGX 面对商家用户和个人用户提供了不同的服务及产品。面对商家用户，BSGX 将提供商用平台(Commercial platform)，可以实现一键接入 BSGX 以及应用支付解决方案等。面对个人用户，BSGX 将提供移动 DAPP 钱包、基于 RSA 算法加密的通讯模块、场外担保交易、极速交易等为加密数字货币用户定制的诸多功能。

在激励场景中，当参与者作出了对 BSGX 发展的贡献，系统将根据贡献机制的计算，提供相应的合理回报（奖励 BSGX 代币）。而作为商业应用级区块链支付解决方案，第三方商业机构的生态构建和转型升级问题也可通过 BSGX 的应用得到解决。

BSGX 完美地继承了传统支付技术和区块链技术的特性与优势，并解决了当前区块链的技术瓶颈，真正意义上将区块链与商业应用结合。并且，BSGX 大力且持续投入以区块链技术为代表的商业科技的研发和创新，将其运用于提升传统行业的价值以及促进区块链技术在各行各业中落地应用的蓬勃发展，以打造未来互利共赢的区块链支付生态系统。

第三章 BSGX 应用功能模块

3.1 钱包系统

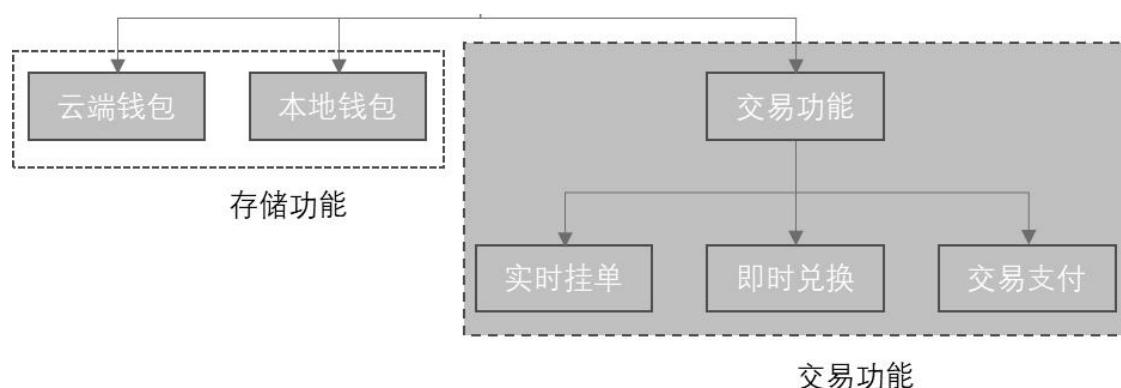
在 BSGX 系统中，钱包将承载关键作用。BSGX 钱包可用于数字资产的存储、管理、交易，用户不仅能够完全掌控自己的数字资产，而且极大的降低数字货币的使用门槛和管理负担，有效促进数字资产的灵活应用，未来，通过 BSGX 钱包进行交易，将成为全球支付用户的主要支付方式。

BSGX 钱包的核心价值正是落实及体现数字资产的市场真实性及流通力，打造个人用户更方便、快捷的实现全球加密货币产业真实性流通性能。在我们的规划中，任何加密货币只要是在 BSGX 钱包就可实现扫码即可支付，扫码即是安全地址。即使充币、提币或更多功能。BSGX 钱包具备以下几个特点：

- 更安全：路径安全、数据安全、防篡改以及无单点故障；
- 更快速：实时交易、无支付中介机构、跨境结算更快；
- 更便宜：低成本交易、低交易佣金、无中间商抽成。

1) 资产管理

通过 BSGX 钱包，为用户提供多区块链资产的统一管理，拥有本地钱包、云端钱包以及交易功能，实现资产管理一体化。



2) 多币种服务

BSGX 钱包系统可同时统一管理多种数字货币，不仅支持 BTC、ETH、以太坊等主流资产等存储和管理，还支持智能合约平台的标准协议，并快速增加基于各平台发行的代币。实

现多种数字资产管理一体化，减少用户操作成本。同时提供云端钱包和本地钱包，本地钱包私钥支持；云端钱包免交易手续费，实时到账，方便用户进行钱包内外转账。

3) 链上链下双存储理念

BSGX 秉持区块链核心要义，提供去中心化等数字货币存储方案，用户自持钱包密钥和所有类型货币等地址私钥信息，平台不触用户资产。同时，BSGX 提供便捷等密钥备份方案——用户只需进行一次备份，记下 12 个助记词，保存到安全的地方。即使后续增加数字货币种类，用备份的 12 个助记词即可恢复所有类别的数字货币资产。

4) 多重安全验证

除了让用户自持钱包密钥和私钥，还针对不同规模的数字资产管理，提供多重签名技术保证和两步授权验证，除此之外用户在转账交易时进行手机验证码、指纹、人脸识别等验证方式，全方位保证数字货币资产安全。

5) 多语言支持

BSGX 钱包将支持阿拉伯、中文、英文、俄罗斯、日、韩、德等主流数字货币市场等多种语言，提供更全面的全球化服务，打造世界级钱包运用。

6) 双钱包应用

为方便用户使用，BSGX 将开放云端钱包和本地钱包两种钱包形态，用户可自由选择其所需的钱包。

- 云端钱包：云端用户间转账秒级到账，无手续费；由云端保管私钥，储存用户的地址和交易记录，钱包不接触用户资产。用户可以通过用户名、密码、人脸识别的验证方式找回云端账号。
- 本地钱包：用户私钥自持，资产更安全。用户可以通过主密钥派生任意数量的子账户（也就是子密钥）在本地钱包为每个数字资产添加多个钱包地址，方便资产分离。

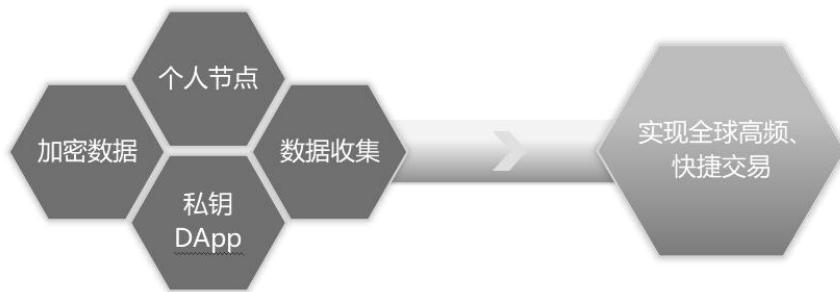
3.2 全球支付清算系统

除了对传统支付模式的变革，BSGX 还将通过闪电支付网络的应用以及高频支付的融合，实现基于区块链技术的全球支付清算系统的搭建。

1) 交易通道与闪电支付

BSGX 使用多重签名技术建立交易通道，实现堪比闪电网络的极速交易。BSGX 技术的核心是通过多重签名技术来实现极速交易，其安全度高于零确认，其简单程度和落地性优于闪电网络。

2) 高频支付清算系统



- 个人节点：BSGX 将基于区块链节点，为用户设计个人的分布式账号节点，也就是 BSGX 用户的唯一 ID，在通过平台内置的支付系统，基于以太坊技术基层的可扩展性和跨链技术，BSGX 用户将可以通过平台实现全球快捷支付系统。
- 数据收集：平台将通过数据收集，对于个人节点用户的数据得到分析，为用户建设信任体系，所有的数据信息将基于个人用户数据的私人数据。同时，在信任认证、广播、传输过程中，通过数据脱敏加密，充分保护个人隐私和数据。
- 私钥 DApp：BSGX 用户的金融交易数据都是通过个人私钥 DApp 流动数据。所有的数据将通过区块链技术的认证、以及智能合约的确认返还个人用户钱包，现实信任、公平、安全性。同时 BSGX 已经现实全球跨链衔接，所有的用户都可以基于 BSGX 享受全球金融提供的快捷交易、金融服务、金融应用数据等服务，也可以实现数字资产快捷换取其他区块链数字资产的长久保存，这样的模式将使得金融数据商业化变得更公平、更有持久存储以及长久增值效益。
- 加密数据：BSGX 的用户数据加密，是基于去中心化的存储技术，所有交易数据过程的安全性，平台会通过广播方式将以及隐私信息的脱敏。让 BSGX 用户在授权平台支付、金融服务数据使用时，没有后顾之忧。

3.3 多币种管理与交易系统

BSGX 通过钱包、支付清算体系，能为用户提供多区块链资产的统一管理，形成完整的资产管理体系，在该体系中实现了一站式、去中心化、多重安全保障和多语言支持等。

- 丰富多样的应用

- 追求易用而满意的用户体验
- 挖掘多样化的数字资产应用场景
- 全面掌控让价值更快更好的流通

BSGX 数字资产兑换网络，通过智能合约、跨链网关和跨智能合约技术，可以实现无风险的数字货币兑换服务。用户通过 BSGX 网络进行数字货币间的兑换，由平台方或其他第三方创建兑换的智能合约，由合约机制监控和执行兑换过程，规避了参与各方在交易过程中的违约风险。未来，BSGX 将打造包括多币种账户及兑换功能、点对点交易功能、点对公交易功能等在内的新型数字资产资管生态。

1) 多币种账户及兑换功能

- BSGX 计划为用户提供法币和数字货币中间市场汇率
- 通过当前最流行的社交媒体工具向其他用户免费转账
- 与其他持牌金融机构合作
- 努力为我们的用户提供更多服务

2) 点对点交易功能

全球价值转移应该像在聊天工具中打招呼一样简单。无论你住在哪里。BSGX 上的资金转移设计完全无障碍。通过我们支持的任何渠道，用户只需：

- 指定转账金额（例如: 0.1 ETH）
- 然后 BSGX 将返回一个“哈希值”，其形式是一个独特的 18 个字的十六进制字符串
- 第一个提交此“哈希值”给 BSGX 的用户，将获得该笔转账金额

用户可以通过在聊天工具中直接指定收款人的昵称或电话号码来转账，并即时完成交易。

3) 点对公交易功能

每个通过(KYC)身份验证的用户，该用户将获得 BSGX 所提供的虚拟借记卡。这一虚拟借记卡将让符合条件的用户可以在任何接受该卡支付的场所(包括线上和线下)使用该卡进行消费。

4) 安全及合规承诺

我们相信，合规及安全是主流加密货币被采用的基础。随着 BSGX 的业务及团队发展，合规及风险管理专业人士将遵循合规政策和程序，以确保完全遵守所有监管要求。

- BSGX 遵循“纵深防御”理念，安全及合规的心态与 BSGX 业务的所有方面相关。每个人都在安全方面发挥作用，我们将对网络安全采取全面措施。
- 随着项目的发展，BSGX 将实时完成详细的安全评估，包括外部渗透测试，威胁建模及风险控制审查。
- BSGX 将聘请领先的第三方安全专业人士进行彻底的外部安全测试，以确保安全控制的完整性。反洗钱，反恐怖融资，不断扩散大规模杀伤性武器及法规遵从性质制裁（合称“反洗钱/反恐怖融资”）对 BSGX 来说也非常重要。

3.4 跨境金融服务

1) 商业金融收付款

BSGX 可针对跨境业务的整体上下游环节，以 BSGX 代币为媒介，提供资金快速结算、周转、信贷、理财等综合金融服务。例如，为中小企业提供最优利率授信放款，支持基于收款、信用、抵押的多种标的灵活授信。BSGX 多样化的全球支付产品，将满足资金的不同增值需求。

2) BSGX POS 服务

BSGX 将打造基于 BSGX 代币的 BSGX POS 服务，以实现 BSGX 代币与包括 Visa、MasterCard、American Express、JCB、Diners Club、Discover 等在内的全球主流信用卡之间的交易。

未来，BSGX POS 可在全球商家用加密货币支付，只需将加密币转账到卡钱包。除了在全球各大经济地区推出实体卡外，BSGX 还将在加密借记卡上增加稳定币（如 USDT）支持，这样可以支持用户用其代币支付。

3) 全球商户收款服务

BSGX 可以满足企业在不同业态下的多样化收款需求：

- 多币种：美元、英镑、欧元等主流货币收款及印尼盾、泰铢等小币种；

- 多场景：支持 B2B 贸易出口、主流跨境平台及独立站；
- 企业账户：可为企业开设同名账户，同时支持创建多个账户；
- 全球本地收款账户：覆盖亚洲、欧洲、美洲、大洋洲、非洲等国家及地区。

未来，BSGX 的全球合作银行网络将遍布全球，用更有竞争力的手续费费率，有效降低企业成本，在多个主流国家及地区拥有本地收款能力，更快更省完成全球收款。同时，支持 7*24 小时操作提现，最快实时到账，可根据用户需求，灵活选择币种、金额、账户主体等。此外，自主研发的强大技术引擎也将为收款全流程加持，提供安全及时的响应。直接接入主流跨境平台，强大的数据同步机制，可一步获取订单数据，自动同步。

在以上收款后，商户/企业可以在钱包中把资金兑换成 BSGX 代币，以获取其他更多服务和支持。

3.5 配套功能支持

1) 资产登记确权

BSGX 针对资产登记和上链确权，提供全流程服务，过程由网关或者网关代理完成。所有网关登记的资产或者代理登记的资产，都需要获得资产拥有的信任，只有信任的双方才能交易同一种资产。登记的资产主要分作：货币类型资产和实物类型资产。

- 货币类型资产：货币类型资产主要用于网关与其他数字货币、数字资产平台进行对接，比如，网关可以登记 BTC 的资产代码，任何拥有 BTC 的账户都可以信任该网关，将 BTC 资产充值给该网关账户。货币类型的资产不限量，网关拥有多少实际的货币资产，就可以登记多少资产符号。
- 实物类型资产：主要指资产数字化，此类资产一般由企业或机构登记，并由网关代销。这类资产一般具有一定的额度，登记完毕后，将通过操作权限阈值自杀的方式，限制资产登记方不再增发。

2) 区块链浏览器

BSGX 提供了区块链浏览器，便于普通用户核对任何接入 BSGX 的资产数量。为确保账本的有效性，区块链浏览器支持链接不同的区块链节点查询账本情况，并可以实时观察每个区块、每个交易生成情况，输入相应账户时，可查询账户各种资产余额以及所有的交易记录。

3) 传统产业上链

BSGX 资产上链系统具备针对大额固定资产通证化（发行代币）的需求和广阔的应用场景，为企业提供发行自有代币的平台和服务，拓展企业数字化金融业务，提升品牌影响力和竞争力。BSGX 使用区块链作为底层技术，将固定资产上链，围绕核心企业进行估值，确权，抵押，交易，解决大额固定资产流通难的问题，促进金融流通效率提升。

- 借用第三方机构对有价值的资产进行资产登记、确权、评估、鉴定、估值、托管；
- 区块链存证，保证权证有效性：利用区块链技术特性，保证信息不可篡改性和透明性；
- 借助区块链通证经济学，实现实物资产通证化（发行代币），使固定资产实现价值分割，快速流通成为现实；
- 联合多家公信机构，将版权信息形成唯一有效的资产编码，链上确认权益；
- 使用技术手段保证通证化资产（发行代币）流转有效性，保障交易各方权益。

第四章 BSGX 技术体系

4.1 技术概述

BSGX 区块链底层在核心支持下，由参与方管理层、区块链层、应用层三个层级组成，其中支付系统由验证节点和投票节点两个子层级。

1) 参与方管理层

BSGX 系统参与方以超级节点的方式加入区块链网络。不同业务方可以根据需求加入和退出。超级节点之间信息互通，共同确保存证载体和存证数据的真实性。通过有效的制定统一适用的交易标准、STO 网关、智能合约等，从而有效的链接传递各个节点在不同事件中的身份职能与合同要素。

2) 区块链层

关键技术：该部分是应用服务部分各模块的基础支撑。

区块链技术：包括网络结构、数据结构、共识机制、签名验签等等，是系统运行的基础。

相关技术：

- 数据存储模块：基于内容的地址替代基于域名的地址，也就是用户寻找的不是某个地址而是储存在某个地方的内容，不需要验证发送者的身份，而只需要验证内容的哈希，通过这样可以让支付验证的速度更快、更安全、更健壮、更持久。同时提供存储安全防护措施，避免数据被强行盗取；而数据存取审计，便于追溯数据变化和流转情况。
- 身份模块：对用户、设备进行区块链认证、登记标识其有效性，同时对用户的标识即私钥进行管理，该系统也包含访问安全功能，作为系统安全的重要保证。
- 时间戳服务：为系统提供统一时间服务。
- 数据加解密模块：为系统提供数据加解密服务，该模块应支持国密算法，可支持可插拔的加解密算法。
- 客户端模块：客户端为用户提供了对账户，区块，节点和钱包的管理及查询功能，如新建账户，发送交易，生成随机种子，获取区块信息，获取钱包状态等。所有的支付交易都通过客户端，签名并加密后送入区块链。

- P2P 模块：P2P 模块连接各个节点，在全网广播交易，区块相关信息。
- Mempool 模块：交易缓存池，mempool 中存储从 RPC 接口来的交易，以及从 P2P 过来的交易。Mempool 的实现主要是解决共识模块的处理速度比 RPC 模块慢的问题。

3) 应用层

应用服务是在 BSGX 系统关键技术提供的支撑之上，针对各种服务模块进行实现和封装。每个服务是由一组相关的规范、流程和配套的交互接口构成。

可通过调用 BSGX 系统区块链层应用服务，经过二次开发对接特定业务场景。

4.2 技术整体架构

BSGX 系统是高速、安全、可扩展的数字货币支付基础设施，由超级节点和存储接节点两层构成。并通过区块链技术的支持，处理每秒钟数百万的交易服务，通过安全的去中心化云数据库，为 Dapp 提供无限扩展的存储能力。

BSGX 架构系统由以下几个部分组成，分别是：

- 同构多链的链系统，提供高 TPS 的访问能力、跨链支付能力等；
- P2P 的网络系统 BSGX P2P，提供网络层的寻址能力；
- 多数据库集群系统，提供可无限扩展的安全加密数据存储能力；
- BSGX 系统的底层结构支撑系统，包括一个块存储系统和一个分布式文件系统；
- 由多节点共识组成的属性基加认证访问系统，数据库的访问控制网关；
- 由多个验证人节点组成的数据完整性验证组织；
- 自适应的探针系统，提供内存数据存储、性能监控、安全监控和 Metrics 数据上传能力。

BSGX 系统核心是链库分离机制和功能子链设计。去中心化应用可以按照数据不同的信任和公开验证等级，将数据分别存放在链上和数据库系统中，BSGX 系统提供了不同类型不同层级的数据协同管理。并且，由于多数据库集群系统是一个 Permissionless 的环境。BSGX 系统还完成了基于多授权机构属性基加密的访问控制机制，以及完整的对存储数据的持有性证明。

链库分离设计的主要原因是系统未来的升级和更新考虑，由于区块链系统的更新会导致系统的分叉，总对整个经济系统造成不可逆的影响，因此，我们把主要的数据处理能力放在数据库系统之上，把对于数据库系统的访问控制体系通过功能子链来完成。功能子链设计一是为了未来的扩展性，更多是为了完成去中心化存储系统的两个核心功能：隐私保护和数据持有性证明。我们通过一种高效的多授权机构属性基加密方案实现了对云存储数据访问控制功能和加密功能。

1) 账户

BSGX 采用状态(state)的概念存储一系列账户，每个账户都有身份认证信息以及自己特有的数据。某些情况下，接受账户内有需要执行的代码，则交易会触发该代码的执行，那么账户的内部存储器可能就会发生变化，甚至可能会创建额外的信息发送给其他账户，从而导致新的交易发生。

2) 默克尔帕特里夏树

比特币是通过一种叫默克尔树的方式。IPFS 也是通过默克尔树的一个有向无环图数据结构来保存这个数据。默克尔帕特里夏树简单来说就是，当我们这个文件比较大的时候，别说有一两兆两三兆，甚至更大的，IPFS 的系统会在你上传文件到 IPFS 节点的时候，它会把文件分割，然后分割完以后每一个文件都是用一个哈希值作为它的文件名。然后这些文件是通过一种数的方式进行保存，而且总数呢，打个比方，这个数就好比有很多树叶，然后两片树叶相连的树枝其实是这两片树叶的一个哈希值运算，那么从树叶到树枝，然后从树枝的分叉一直到树根。

通过这种方式就可以确保，当某一个树叶上面的数据发生变化，直接体现在树根的哈希值也发生了变化。这种方式其实跟比特币的数据保存方式是一致的。它的目的就是为了让整个网络以最快的速度来验证一个数据的完整性。因为我们不需要去比较整个文件，我们只需要去看树根的值是否还是一样的。如果说一致的，不同的节点就可以证明这个数据没有被篡改。

默克尔帕特里夏树(Merkle Patricia tree/trie)，由 Alan Reiner 提出设想，并在瑞波协议中得到实现，是 BSGX 系统的主要数据结构，用于存储所有账户状态，以及每个区块中的交易和收据数据。MPT 是默克尔树和帕特里夏树的结合缩写，结合这两种树创建的结构具有以下属性：

- 每个唯一键值对唯一映射到根的 hash 值；在 MPT 中，不可能仅用一个键值对来欺骗成员(除非攻击者有~2A128 的算力)；
- 增、删改键值对的时间复杂度是对数级别。

MPT 为 BSGX 提供了一个高效、易更新且代表整个状态树的指纹。

3) RLP 编码

RLP 旨在成为高度简化的序列化格式，它唯一的目的是存储嵌套的字节数组。不同于 protobuf BSON 等现有的解决方案，RLP 并不定义任何指定的数据类型-如 Boolean、20floo、double 或者 integer 。它仅仅是以嵌套数组的形式存储结构，并将其留给协议来确定数组的含义。RLP 也没有明确支持 map 集合，半官方的建议是采用[[k1, v1], [k2, v2],...]的嵌套数组来表示键值对集合-k1,k2 ...按照字符串的标准排序。

与 RLP 具有相同功能的方案是 protobuf 或 BSON，它们是一直被使用的算法。然而，我们更偏向于使用 RLP，因为：

- 它易于实现；
- 绝对保证字节的一致性。

4.3 共识机制

共识算法作为区块链的基石之一，快速和不可逆是我们重点关注的目标。除此之外，为了更好地建设系统生态，我们认为公平性同样重要，如果大资本可以轻松占据系统中区块共识的话语权，那么会有很多系统上的开发者和用户的利益无端受损，一个不能保障系统建设者利益的生态，很难沉淀出价值深度，和 BSGX 设计原则相违背。所以我们在设计共识算法时，在优先保证快速和不可逆的情况下，将尽可能追求公平性，维护系统建设者的利益。BSGX 的共识为 PoD 共识算法机制。

1) 新区块产生

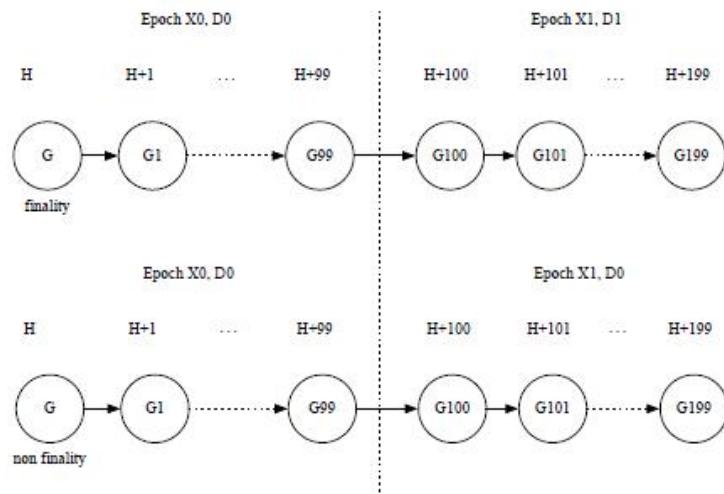
类似 PoI 共识算法选取重要性高的账户，PoD 将选取生态中贡献度较高的账户，不同之处在于，PoD 赋予选取出来的账户平等概率的记账权来参与产生新区块(block)，防止概率倾斜衍生垄断。

在选择贡献度较高的账户时，我们使用了 BSGX 原生普适价值尺度评估。在算法设计中，着重考虑了账户的流动性和传播性 (我们认为满足这些性质的账户对生态建设贡献度较高。所以在 PoD 中，部分账户自愿缴纳一定数量的 BSGX 代币作为押金后，则有资格成为新区块的验证者(validator)，参与记账。在给定验证者集合(validatorsset)之后，PoD 算法通过伪随机数来决定验证者集合中谁是新的区块的提议者(proposer)，提议者产生新区块。验证者集合不是固定不变的，有资格的账户可以选择加入或者退出验证者集合，而随着周期性 BSGX 孵化基石持有额变化，有资格的账户也会不一样。所以我们在 PoD 设计了验证者

集合动态变化机制，来实现验证者集合的更迭。

2) 验证者集合更迭

验证者集合的更迭就如朝代变更一样，于是我们将验证者集合按照朝代做划分，一个朝代内验证者集合不会发生变化。一个朝代不能更迭地过快，至少要保持一段时间不做变更，因此我们将每 X 个区块定义为一个 Epoch，在同一个 Epoch 中朝代不会发生变化。所以朝代的变更只会发生在 Epoch 交接时，在此时将会考察上一个 Epoch 的第一个区块，如果此区块到达了 finality 状态，那么当前 Epoch 进入下一个朝代 $D1$ ，否则延续上一个朝代 $D0$ 不变，如下图所示。



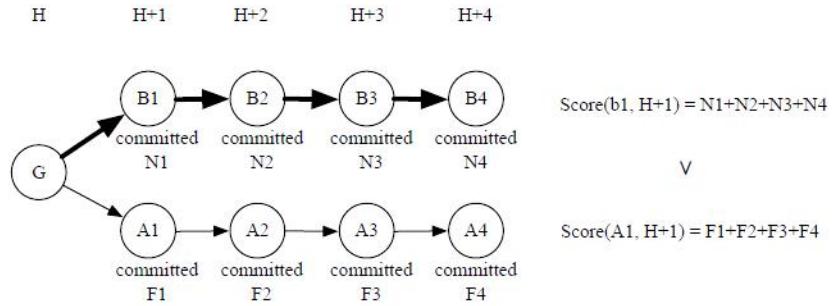
由于网络延迟，各个节点可能在朝代更迭时，看到的区块 G 是否 finality 的状态不一致，所以参考 Casper 的动态验证集策略，要求每一个朝代的共识过程将由当前朝代和上一个朝代的验证者集合共同完成。因此在任意一个朝代，有资格的账户只能申请加入或者退出 $D+2$ 朝代的验证者集合，当朝代变更到 $D+2$ 时，才可加入新区块的共识过程。

3) 分叉选择

PoD 算法以每个高度上区块的得分来选择权威链，总是选择得分最高的区块加入权威链，在高度 h 的区块 b 的得分如下，

$$Score(b, h) = \sum_{(b', h') \in \text{children}(b)} Score(b', h') + \sum \text{committed deposit in } b$$

即为该区块及其所有后代区块收到的 commit 票对应的押金总和



4) 投票规则

为了避免共识过程被恶意破坏，导致共识过程没法完成，阻碍生态发展，PoD 参考 Casper 的最小惩罚规则来约束验证者的共识活动。

假设共识过程中的 Prepare 和 Commit 票结构: $\text{Prepare}(H;v;vs)$ ，其中 H 为当前区块 hash， v 表示当前区块高度， vs 表示 v 的某个祖先区块高度 $\text{Commit}(H;v)$ ，其中 H 为当前区块 hash， v 表示当前区块高度。

PoD 算法为整个投票过程制定了如下 4 条基本规则：

- 单个区块的两阶段共识过程存在严格的先后顺序，只有在第一阶段 $\text{Prepare}(H;v;vs)$ 票总权值达到 $2/3$ 后，验证者们才可以投出第二阶段的 $\text{Commit}(H;v)$ 票，
- 多区块间不强制一个区块共识结束后才能开始后一个区块的共识，允许交织共识 (interwovenconsensus)，但是不能完全没有秩序，只有高度 vs 完成了第一阶段过程，拥有 $2/3$ 的 $\text{Prepare}(H_{anc};vs;vs')$ 后，才可以基于 vs 对其后代区块投 $\text{Prepare}(H;v;vs)$ 票，保证交织稳步向前
- 为了避免有节点利用交织共识恶意跨多区块投票，要求基于高度 u 投出了 $\text{Prepare}(H;w;u)$ 票之后，对于高度在跨度 u 和 w 之间的所有区块，不能再投出 $\text{Commit}(H;v)$ 票，保证共识过程的高效有序
- 为了制止节点用同一笔押金在多个分支上同时下注，导致 nothingatstake 的问题，要求在一个高度投出 $\text{Prepare}(H1;v;vs1)$ 票之后，不能再投出不一样的 $\text{Prepare}(H2;v;vs2)$ 票违反上述规则的验证者一旦被举报核实，将会被罚掉所有押金，举报者们将会共享罚金的 4% 作为奖励，罚金的剩余部分将会被销毁。

4.4 安全加密算法

BSGX 选择符合国内和国际标准的加密机制，对各项数据进行加密，用户间的支付数据

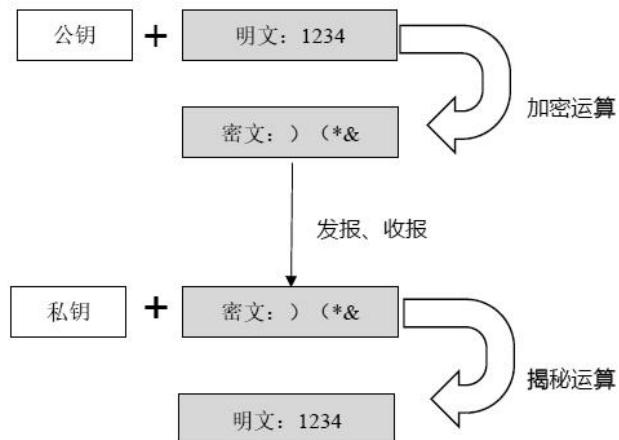
和交易信息仅交易双方和有相应权限的用户可以查看。

1) 私钥 (privatekey)

非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

2) 公钥 (publickey)

可公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，目前常用的方案包括：secp256r1（国际通用标准）和 secp256k1（比特币标准）。BSGX 控制链与初始数据链选择 secp256r1 作为密钥方案。

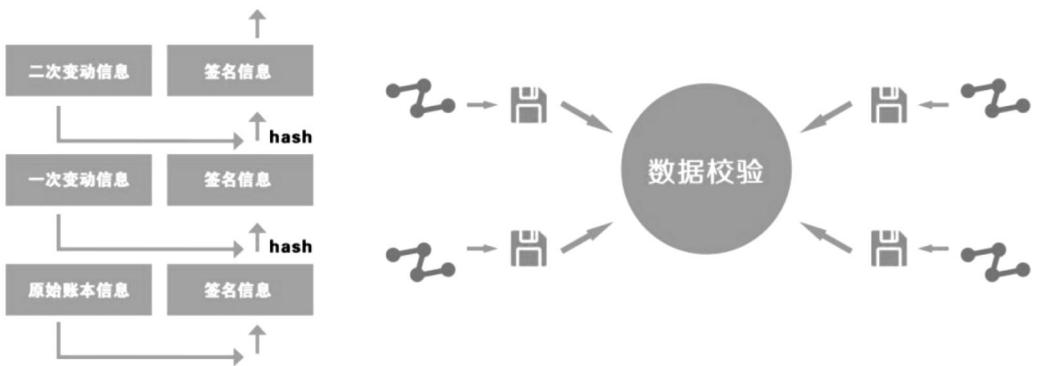


3) 加密

BSGX 通过非对称加密的数字签名的技术，做到了业务请求在传输过程中不被篡改，并且通过共识机制保证各节点的数据一致。对于已经存储的数据记录则通过节点内的自校验系统和准实时多节点系统来校验，以保证已经存储的数据记录同样无法篡改。

节点的自校验性是指 BSGX 采用块链结构存储数据记录，其中篡改数据会破坏块链结构的完整性，系统可以快速校验出来并从其他节点将数据恢复。另外 BSGX 每个记账节点都有自己的私钥，每个区块中记录了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。

准时多节点的数据校验是当节点的私钥被盗取，恶意用户是存在修改账本链上所有数据的可能性的，BSGX 提供了准时多节点的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。



4.5 P2P 协议

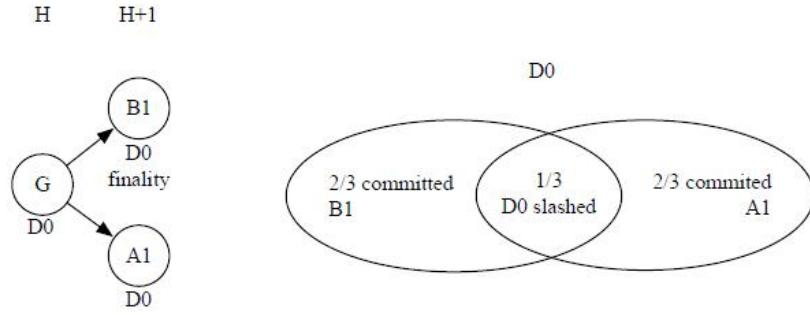
BSGX 上，每个节点（客户端）均采用 P2P 协议进行消息广播交互。对于 BSGX 的数据区块，采用的 P2P 协议是标准的加密货币协议，该协议的核心特点是引入“幽灵”协议。而 BSGX 的控制区块则采用标准的 P2P 协议，不支持“幽灵”协议。客户端通常工作于守护状态。该状态下，客户端执行的工作包括：

- 调用网络守护进程维护连接及定期发送消息；
- 获取当前区块信息以及关联区块信息；
- 获取工业制造参数，并对工业制造参数按照标准模型分析，确定是否提交更新的参数。

4.6 恶意攻击防范与惩罚机制

PoD 中的每个高度上的区块都有共识有效期，如果某个高度距离最新高度超过 100 时，该高度的所有区块在共识过程中将被视为过期，那么这些区块上的所有新的共识活动将将会被直接忽略。因此，要在 PoD 中完成长程攻击(long-rangeattack)几乎不可能，但是在有效期内依旧存在发起短程攻击的可能性。短程攻击者 Attacker 试图在高度 $H+1$ 的区块还没有过期的情况下，伪造 A 链来替代 B 链成为权威链，Attacker 需要让区块 A1 的得分比 B1 更高。由于多投会被严惩，所以 Attacker 将不可避免地要贿赂验证者，否则无法完成短程攻击。为了展现 PoD 共识算法的安全性，下面分别分析使不同数量的区块失效时，Attacker 需要付出的代价。

如果 Attacker 想要使 B1 失效，最小代价的情况如下图，就相当一次双重支付攻击，Attacker 幸运地成为了 $H+1$ 高度的区块提议者，那么至少需要贿赂朝代 D0 中 $1/3$ 的验证者多投使 A1 达到 finality，最小代价为所有押金的 $1/3$ 。

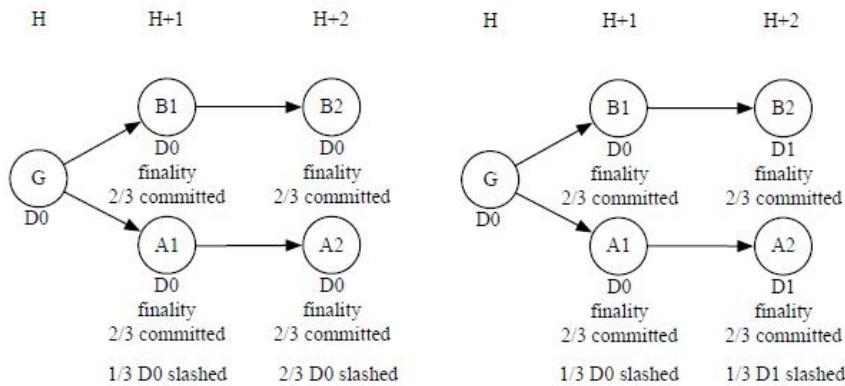


如果 Attacker 想要使 B1-B2 失效，假设 B1 和 B2 都已到达 finality，块中交易都已生效，为了让这些交易失效，这里考虑两种情况。

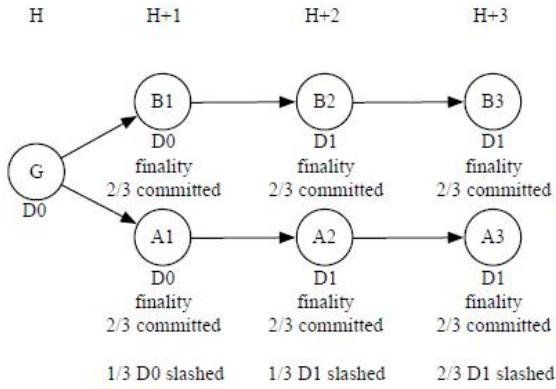
第一种如下图所示，高度 H+1 和 H+2 在同一个 Epoch 中，朝代相同，那么 Attacker 首先需要贿赂 D0 中 1/3 的验证者使 A1 达到 finality，此时这 1/3 的验证者将会被惩罚，押金被罚完。

在 A2 的验证中整体押金总和只有 A1 中的 2/3，此时 Attacker 想要让 A2 到达和 B2 同价值的 committ 票，需要贿赂剩下所有没有作弊的验证者，合起来至少需要损失总押金的 3/3，即使如此也不能保证 A1 得分比 B1 高，攻击失败风险高。

第二种情况如下图所示，高度 H+1 和 H+2 正好在不同的 Epoch 中，且朝代不相同，那么此时 Attacker 需要贿赂 D0 中的 1/3 来让 A1 到达 finality，然后贿赂 D1 中的 1/3 来让 A2 到达 finality，完成一次这样的攻击至少需要损失总押金的 2/3。综上，想要发起短程攻击导致两个 finality 区块失效，至少需要花费总押金 2/3 的代价。



如果 Attacker 想要使 B1-B3 失效，如下图所示，Attacker 首先需要贿赂 D0 中 1/3 的人完成 A1 的 finality，然后贿赂 D1 中 1/3 的人完成 A2 的 finality，最后需要贿赂 D1 中剩下 2/3 中的所有人来完成 A3 的 finality，综上至少要损失总押金的 4/3。要完成这些攻击准备将会十分困难，而且即使有幸做到了，也不一定能保证 A1 的得分比 B1 高，攻击也可能会失败。



4.7 支付系统的风险控制

无论是区块链，还是加密数字货币的流通、支付，都处于非常早期的阶段，因此，为了实现项目的安全发展，BSGX 提供完整的风险控制解决方案。

1) 系统风险控制

- 数据库读写分离机制：在初期，系统风险控制一般通过建立数据库主从复制、读写分离、Sharding 等机制来保证支付系统的数据库和风险控制系统数据的同步及读写分离。系统风险控制对所需要的客户/账户数据、交易支付数据一般都只有读取的权限，从而确保账户数据安全可靠。
- 缓存/内存数据库机制：高效的缓存系统是提升性能的有效措施，一般该机制会把频繁使用的数据存放到 Redis 等缓存系统中。例如风险控制规则、风险控制案例库、中间结果集、黑白名单、预处理结果、交易参数、计费模板、清结算规则、分润规则等数据。而对一些高频交易，基于性能考虑，则会采用内存数据库进行存储（一般会结合 SSD 硬盘）。
- RPC / SOA 架构：降低交易系统和系统风险控制的耦合度。在初期系统服务较少的情况下，一般直接采用 RabbitMQ / ActiveMQ 之类的消息中间件或 RPC 方式来实现系统间服务的调用。当系统服务增多，出现服务治理问题时，就会采用 Dubbo 之类 的 SOA 中间件来实现系统服务调用。
- 复合事件处理 (CEP)：实时/准实时支付风险控制，相对于纯粹基于规则的处理模式，采用复合事件处理 (CEP) 模式，其性能及扩展性更好。

2) 产品风险控制

第一阶段的产品风险控制主要集中于产品上市前的尽职调查，包括了针对数据库中的历史数据和参数的合理性检验，运用历史支付数据或标准化衍生品以及其市场价值对 BSGX

模型进行穿行测试，判断其设计合理性。

第二阶段的产品风险控制集中于产品稳定运行的阶段，通过制订各类支付和金融产品准入标准化的条款，以智能合约形式设立递次通过的锁件，所有通过审核的产品上线后，以区块链去中心化的数据形式上架发行销售，形成理财产品库。此阶段投资者可以自由选择产品，每种产品不会因为人为背景而误导投资者，所有上市产品的说明，都由经过严格的智能化审核后产生的数据来支撑，并且这些数据永久不能更改或删除。

第五章 BSGX 通证经济模型设计

5.1 BSGX 代币经济学

BSGX 将发行高价值代币——BSGX。BSGX 主要用于 BSGX 生态流通、跨境支付、全球金融以及各大实体场景下的价值流转等。例如，未来，BSGX 可在全球商业场景中流通使用。

代币名称：BSGX

发行总量：1000 万枚

发行价：1 BSGX = 1 USDT

总供应量：100,000,000 枚

公开认购量：16,000,000 枚

单笔认购价格：1.56 USDC

最低认购数量：500 枚

最大认购数量：500,000 枚

当 BSGX 支付生态系统形成后，通用支付和跨链支付变成高频事件，此时各方面对 BSGX 代币的需求量不断提升。BSGX 代币持有者拥有平台发展方向的原始分配权。BSGX 代币上线交易所之后，除了不断加强 BSGX 代币的激励模型的领先性以外，也会不断在链上发布新的技术和应用，全面拓展 BSGX 的生态结构和丰富 BSGX 代币的生命力。

5.2 BSGX 的价值属性

我们将通过 BSGX 代币在 BSGX 支付系统的流通，建立一个健康可持续发展的生态模型，把大部分收益全部给到项目投资者/社区成员，项目投资者/社区成员将更愿意支持和改善社区网络。社区成员能通过使用、普及和有效营销来帮助项目创造价值。

我们希望最大程度地将 BSGX 代币的价值观反映到金融支付经济体系的设计中：

- 独立生存：自身拥有清晰的商业模式，能够稳定存续，为 BSGX 创造流通基础；

- 自治与共识：社区与子社区逐步建立共同决策机制，并最终按照共识原则运行，建立以 BSGX 持有者参与投票为基础的发展决策体系；
- 共享：社区产生价值中的一部分作为共同财富，用于社区的生存和竞争力提升；
- 自我进化：建立 BSGX 奖励机制，鼓励成员对社区的技术和经济机制持续提出建议。

BSGX 的基础价值属性包含以下几个维度：

1) 物权属性

在明确的 BSGX 市场流通场景中，拥有 BSGX 的用户，享有代币的所有权与处置权，即享有了代币的物权，可在法律规定的范围内任意处置代币。

2) 货币属性

以加密货币为中心的 AP，可实现数据流转和代币的流通。在 BSGX 的流通场景中，用户行为数据、电子货币、消费都可记录在链上，而有效行为又可进一步转化成代币。每个成员有独立节点，共享账本数据，有效增强了代币使用的透明性。也就是说，代币建立一个“价值交换”的桥梁。

3) 股权属性

BSGX 是以 BSGX 全球支付网络为使用场景之一的数字代币，持有代币的用户拥有特定项目的股权。即持有 BSGX 达到一定的数量，表现为持币分红，但需要说明的是，代币并不是某种特定投资。

4) 治理属性

在去中心化治理系统中，任何决定都要在一个固定时间内完成投票，这个时间根据提议内容不同而发生改变。当且仅当收集到足够高权益的投票，提议才会执行，否则提议将会关闭。在去中心化自治系统中，并不是权益高者的一言决定，权益低者可以联合在一起制衡权益高者。去中心化自治内容包括但不限于用户注册、统计函数、抵押标记范围等，这些升级可以通过自治系统参与者共同投票参与决定。持有 BSGX 代币是具备治理资产的基础门槛。

5.3 市场激励

前期我们将通过空投/奖励等方式赠送 BSGX，更加吸引粉丝对 BSGX 全球支付网络的关注。在 BSGX 全球支付网络中，持有 BSGX 的用户能够享受代币升值，手续费抵扣，资产增值，收益返利，监督，投票选举，持币增值，NFT 奖励等系列权益。BSGX 全球支付网络通过各类激励措施将 BSGX 奖励给系统流动性做贡献的用户。平台通过激励机制回馈社区用户，通过持有 BSGX，从而享受 BSGX 社区各项权益。

BSGX 代币上线交易所初始，BSGX 将通过 kol，媒体新闻，社群领袖等多渠道宣发注册送币活动，招募合伙人活动，交易手续费减免活动，积极打造社区社群的运营建设。通过领袖的社区管理，全方位的社区推广活动，抽奖活动，问答送礼活动等，让全球 BSGX 布道者及新人看到平台锐意进取的决心。

5.4 BSGX 的应用价值

1) 基础应用价值

BSGX 作为高应用价值的加密数字货币，将实现类似于货币的功能。通常来说，货币有四大功能：价值贮藏、交换媒介、记账单位、延期支付标准，为了满足上述功能，BSGX 专门设计了以下特点：

- **价值贮藏物**: 价值贮藏物指的是能够保值的资产，不会随时间流逝而大幅贬值的资产。BSGX 是一种支付媒介，其设计使其在波动巨大的市场中也能保证价格稳定和稳步上升。
- **交换媒介**: 交换媒介指的是一切可代表价值标准、被用来促进商品或服务的出售、购买或交换（交易）的事物。在全世界不同类型的交易中，都能使用 BSGX 来达成交易。
- **记账单位**: 记账单位是一种标准化的价值度量衡，用于商品和服务的定价。虽然 BSGX 尚未在区块链外成为标准的价值度量衡，但是它在 BSGX 全球支付网络和一些合作 dApp 中将充当记账单位之用。

2) 多元支付应用价值

基于 BSGX 全球支付网络的基础功能设计，我们可以清晰的看出 BSGX 在交易、支付、投资领域将发挥较大作用，未来也将会进入到所有社会成员的方方面面：

交易领域

- 用户能够使用 BSGX 来代替法币进行交易，真正实现 P2P 现金；

- 用户能够使用 BSGX 来代替法币与其它数字货币进行交易；
- 用户可以将其它数字货币交易为 BSGX 来规避价格下跌风险。

支付领域

- 大大节省支付时间，尤其在跨境支付方面；
- 交易记录存储在区块链上，能更好地进行追踪；
- 有效降低加密货币支付情景下的支付成本。

投资领域

- 将其它加密资产抵押获得 BSGX 进行投资和理财，享受资产的双重增值；
- 交易记录存储在区块链上，不可篡改，免除了记账纠纷；
- 将 BSGX 和IDO、IEO 结合起来，降低 ICO 风险；
- 利用 BSGX 特性发展出基于区块链的贷款、衍生品、预测市场及其它需要价格稳定性
的长期智能合约。

5.5 BSGX 流通场景示例

BSGX 的流通场景包括但不仅限于以下几个：

- 生态流通：在 BSGX 生态基础上，将衍生出众多实体应用。当 BSGX 上线交易所后，可实现与所有数字货币的兑换，支持生态中各环节流通及支付，如收付款、转账、法币交易、充币、提币、上市投票、STO 网关、配币、借贷、公益、游戏、商城等所有流通交易以及与全球各国法币结算。
- 第三方生态：除了 BSGX 生态体系内的流通外，还将在基于 BSGX 全球支付网络开发的第三方应用内进行流通，并且作为唯一价值通证存在。这将加速 BSGX 的流通，为稀缺的 BSGX 增加更多流通价值属性，拉高整体价值和价格。
- 跨境支付：用户可以使用 BSGX 进行跨境购物，其中包括线上购物和线下实体店购物。同时还能作为跨国支付的基础手段。从而给自己带来更多实惠。当 BSGX 与全球主流平台实现打通后，用户可以享受 BSGX 带来的更广阔的全球全品类商品购买的便利。

- 全球贸易融资：在供货商、进货商、银行等贸易融资参与主体间建立联盟链，通过区块链记录贸易主体资质、多频次交易信息、商品流转信息等，使贸易双方及银行间公开透明安全地共享真实可信的信息。针对供应链中的大型企业，银行可以借此丰富融资风控模型，减少线下人工采集和确认信息真实性的工作量，开展动产评估下的融资服务。针对有融资困难的供应链上下游中小企业，可基于区块链提供的主体资质认证、与大型企业的多频次交易信息认证获得信用背书，缓解融资难题。而 BSGX 可以作为贸易融资的主体数字货币实现与全球主流法币之间的无障碍兑换，实现更加便利的贸易融资功能。
- 通用性方面：BSGX 能适应多样化的业务需求，满足跨企业的业务链条上的数据共享，这意味着 BSGX 对数据的记录方式有足够的通用和标准，能表示各种结构化和非结构化的信息，并能够满足随着业务范围拓展所需的跨链要求。而这就为 BSGX 的通用性提供了价值基础。让 BSGX 能更加从容的流通于世界各地的各个行业和各个场景之中。

5.6 推动价值无国界流通

在 BSGX 全球支付网络中，我们以 BSGX 代币为中心，充分发挥价值传输协议在支付领域的优势，实现全球化的、更快速、低成本的支付、清算、汇兑的金融系统的落地。这个系统支持各种类型的货币，将使得互联网支付就像 Email 一样简单便捷。

以该金融体系为基础，BSGX 将被引入三方实体产业，搭建“现实世界——区块链世界——现实世界”的桥梁，建立全球化的 BSGX 流通增值生态。在 BSGX 流通增值生态中，可以通过智能合约管理参与者的身份信息，为体系内的组织和个人提供更好的金融、交易支付、清算结算等服务。

在消费场景中，BSGX 将“区块链+金融+实体+消费”以新的方式紧密联结在一起，形成一个前所未见的数字世界应用生态。“区块链+金融+实体+消费”形成垂直整合的闭环生态链，区块链、金融、实体+消费各自形成横向扩展的开放生态圈，生态链与生态圈之间相互交错、形成矩阵结构，共同构成 BSGX 完整的价值循环闭环。

在金融场景中，BSGX 代币将以金融为核心，以无障碍支付、跨国交易结算、全币（包括数字货币与法币）汇兑为基础，从金融创新带动其他行业应用突破。随着 BSGX 代币应用普及和社会认知度的提高，将逐渐向社会各领域渗透，如区块链线上金融、企业期权分配、供应链金融、DeFi 等，实现无限的增值潜力。

1) 形成新的混合型数字货币体系

BSGX 站在事实的基础上对数字货币的跨国界应用的可行性进行了验证，同时也证明了区块链技术可以实现信息共享和透明化。由有影响力的银行发行，这样无论其发行规模和汇率都是由国家统一掌控的，从而形成一个以法币为基础，以数字货币为补充的多元化货币体

系。这催生了虚拟金融的交易规则的流程，从而为实体经济的繁荣起到巨大的推动作用。当然，那些具有信誉度的金融/企业/商业主体基于 BSGX 推出自己的数字货币并创造虚拟交易场景，则可以让用户能够体验到更好的创新性服务。

2) 创建新的信用形成机制

信用体制一直以来都是金融主体发展的核心。在传统模式下，商业主体是通过相关管理机构来维护信用、管理风控的，信用评级技术根据用户不同性质进行分类，如小额信用贷款的授信技术等。在大数据时代，各家企业往往采取多维度视角来挖掘和分析客户的行为特征，并以此分析客户的信用等级。虽然大数据可以对消费、小额贷款等进行批量授信，能够在一定程度上提升工作效率，使得数据信息具有一定的可靠性和较高的时效性，但是，这仅仅是实现了传统金融的电子化，并没有使得信用创造的方式发生根本性变化。

BSGX 全球支付网络系统本身是通过去中心化的信用创造方式来进行信用创造的，其具有信息可靠性强、信用建立成本低、信息公开透明等特点。

3) 形成新的场景价值链

互联网的突飞猛进以及对市场的极大冲击，使得传统的销售模式已经不再适应现代经济的运行需求。BSGX 技术本身架构灵活，能够根据不同的应用场景、不同的客户需求、不同的客户结构以及不同的价值运转流程而创造相对独立的、能够进一步强化金融和实体经济相互融合的场景价值链。具体表现在以下几个方面：

- 增加客户黏度和稳定性，使得交易更加依附于场景；
- 客户在应用中的所有交易信息都被记录到区块链上，更具安全性；
- 基于区块链这一“信任的机器”，场景客户的需求不再像以往一样依赖于第三方机构，甚至不再依赖于中心化大数据的支持，平台与客户之间比以往更具信任。

4) 形成新的支付结算方式

虽然在当前的互联网时代，已经使得支付结算效率在很大程度上有所提升，但是在跨币种、跨国界、多种经济合约下，依然在多中心、多环节方面受到了限制，从而使得支付结算的效率往往显得力不从心。

BSGX 代币的去中心化和点对点特征，能够减少中间环节、降低交易成本，在很大程度上提升交易效率，并形成一种新的支付结算方式，以驱动价值无国界流通。

第六章 项目落地与发展

6.1 全球团队

BSGX 的核心技术研发团队成员大多来自于硅谷技术精英团队、其他顶级区块链项目和知名互联网企业。汇聚了计算机、信息安全、支付、通讯、数学、金融、web 开发和高频算法交易等各个领域的行业最优秀的技术专家。同时，团队成员在 DAPP 开发、支付、大数据、钱包等方面具有市场和实践经验，不仅具备强大的技术能力，还拥有优秀的科研能力。

Rick Fishbune——新加坡计算机科学家，曾任职于 IBM 计算机研究中心。精通比特币、以太坊、HyperLedger 等主流区块链技术原理及实现，对区块链共识机制、智能合约、跨链技术、侧链技术、隐私保护等有深刻理解和丰富实践。

Richard Dobrow——硅谷著名区块链软件开发工程师，负责比特币、ETH 等虚拟货币的挖矿算法跨平台移植和矿机软件开发管理工作。在虚拟数字货币钱包和虚拟数字交易所技术架构方面，积累了丰富的产业经验。

Justin Drake——研究集中在大数据并行计算和分布式算法优化上，在区块链、密码学、及数据挖掘方面有着丰富的研究经验。将在区块链核心数学模型，人工智能核心算法、大数据并行计算层面为项目提供深度算法支持。

Jimmy Lee——新加坡国立大学电子工程与计算机科学硕士、博士。其研究涉及数据挖掘、电商数据及算法优化等方面。负责项目人工智能算法构建及优化工作。

Tony Wong——耶鲁大学计算机科学博士、博士后。10 年数据存储研发经验。先后任职多家大数据公司首席科学家。是商业智能系统专家，在数据挖掘方面拥有权威影响力，曾创立自己的大数据研究公司，负责项目架构与方案设计。

Maaghul Clinton——技术开发人员，哈佛大学计算机硕士，Python 语言专家，区块链技术工程师。其研究涉及数据挖掘、人工智能及算法优化等方面。负责项目人工智能算法构建及优化工作。

Matthew Walther——程序开发员，区块链技术应用资深工程师，在私密社交网络领域拥有资深开发经验。具有 15 年互联网从业经验，精通多种计算机语言，擅长海量高并发可用架构设计，拥有丰富的研发管理经验。

6.2 项目落地支持

得益于持续发展与创新的区块链技术、广泛的商业应用、精细化治理的优势，BSGX 项目的落地具备以下支持：

- 强大的团队：BSGX 具有十分成熟且强大的技术支撑，在供应链金融、跨境支付、物联网、信息技术、web3.0 等多个领域积累了丰富的行业与技术经验，在区块链技术开发和应用方面取得了业界领先的突破。BSGX 团队汇聚了多行业行业、多年实际运营经验、且对行业发展有深刻见解的资深人士。
- 资源丰富：BSGX 平台将与目标行业的顶级企业、银行、金融机构等签署战略合作协议，将会为 BSGX 切入目标行业提供强有力的支持，以此来真正推动支付应用的实际落地。
- 项目治理：与一般平台不同，BSGX 拥有对目标行业清晰且明确的战略规划。更为专注与专业地借助区块链技术的分布式去中心化、不可篡改和加密安全性及点对点传输价值的特性，针对支付行业进行渗透并快速取得市场份额。
- 资金管理：BSGX 的资金管理将严格遵守公平、公正、公开的原则，并以 BSGX 的发展为首要目的。我们将成立 BSGX 生态发展基金专项保管且确保资金的安全性及可持续性。BSGX 项目和基金会所有资金使用情况将会定期向所有投资者披露，保证资金使用的公开性。
- 未来空间：BSGX 的目标行业均为万亿级别的支付市场。开发团队通过拟定完善的治理架构，对一般议事、代码管理、财务管理、薪酬管理和特权操作范围等事务进行有效管理，以确保可持续性发展。
- 合规发展：BSGX 是由技术所决定的绝对安全，没有关网跑路的可能，因为 BSGX 是真正的去中心化的链上开放平台，开放源代码，无中央服务器，这保证了 BSGX 比现行的银行都安全。BSGX 没有资金池，完全的场外共识交易。扎根于互联网，存活于互联网，BSGX 的飞速发展，必将引领一个新的货币时代的到来。

6.3 市场合作

为了驱动 BSGX 代币用户和 BSGX 市场的发展，我们将通过社区、媒体和交易所等渠道，实现全方位宣发。

1) 社区

作为社区驱动型支付项目，BSGX 因中自带去中心化的价值观，目前，我们的合作伙伴遍布全球，尤其在社区领域，极具影响力，我们将通过社区渠道宣发。我们将在美国、澳大

利亚、新加坡、日本、法国、韩国、塞舌尔共和国等多个国家，120 个社区同时进行。

2) 媒体

随着 BSGX 更多应用功能的上线，BSGX 代币上线交易所，我们也将在全球媒体进行宣发。如，德意志财经、联合早报、每日新闻、BBC、华尔街日报、雅虎财经、谷歌新闻、Meta、CNN、彭博社、美国之音、世界报等。

3) 明星合作伙伴

为了保护 BSGX 的安全，我们从数学、计算机、人工智能、支付、金融、钱包、Web3 领域招募了一批全明星合作伙伴，作为 BSGX 代币网络的验证者。

4) 应用合作

BSGX 代币将与顶级应用达成战略合作:BlueMove、PancakeSwap、PONTEM、APOTOS、BINANCE、CoinMarketCap、crypto.com、coinbase、CoinGecko、nomics。

5) 上线交易所

未来，BSGX 立志在社区、媒体、交易所等的支持下，开发更多优质应用，携手全球用户共创辉煌，持续完善全球用户所有的去中心化支付基础设施和 BSGX 代币价值共识。

6.4 BSGX 生态发展基金

为实现 BSGX 在全球的快速落地，我们将联合全球顶级资成立 BSGX 生态发展基金，持续对平台生态进行优化。

基金会的职责是致力于 BSGX 的建设和治理透明度倡导及推进工作，促进开源生态社区的安全、和谐发展。同时，基金会将委托具有公信力的第三方机构，协助团队设立运营中心实体，并代为维护实体架构的日常运营与报告事务。通过基金会，选适当的社区参与成员，加入基金会职能委员会，共同参与实际的管理与决策。

1) 基金会组织架构

基金会组织结构提出专业委员会与职能部门相结合的方式，对日常工作和特殊事项予以应对。基金会的设立参考传统实体的运营，将设立各项职能委员会，包括战略决策委员会、技术审核委员会、薪酬及提名委员会及公共关系委员会等组成。

2) 风险评估及决策

区块链作为一项创新技术，不仅仅是在计算机核心技术上有颠覆性的突破，同时也是对个行业领域的革新。因而风险管理体系的重要性不言而喻。

基金会秉持建立以风险为导向的可持续经营的区块链社区。基金会将对基金会的运作进行持续性的风险管理。包括风险体系设立、风险评估、风险应对等一系列活动。对于重大风险，均需基金会战略决策委员会商议讨论并决策。基金会将根据事件特性，例如事件影响程度、影响范围、影响代币量和发生的概率进行分级，按照优先级进行决策，对于优先级高的事件，尽快组织基金会相关委员会进行决策。

第七章 风险提示与免责声明

7.1 风险提示

- 市场波动风险：虚拟化币市场波动较大，投资者需谨慎对待投资风险。
- 政策风险：政策法规的变化可能对项目运营产生影响，请投资者关注相关政策法规的变化。

BSGX 致力于为企业提供更高效、便捷的虚拟化币代收服务，并为投资者提供稳健的投资回报和参与项目治理的机会。

7.2 免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在 BSGX 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。

本文档内容不得被解释为强迫参与 Token 公开发行。任何与本白皮书相关的行为均不得视为参与 Token 公开发行，包括要求获取本白皮书的副本或向他人分享本白皮书。参与 Token 公开发行则代表参与者已达到年龄标准，具备完整的民事行为能力，与 BSGX 签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订合同之前对 BSGX 进行了清晰必要的了解。

BSGX 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。

BSGX 遵守任何有利于行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类 检查的所有信息必须完整准确。BSGX 明确向参与者传达了可能的风险，参与者一旦参与 Token 公开发行，代表其已确认理解并认可细则中的各项条款说明，接受潜在风险，后果自担。