

Sagittarius 生态白皮书

基于区块链的金融流量集成解决方案



Sagittarius 生态® 2021 年 5 月

1.....第一章区块链技术概述.....	
2. 区块链技术的创新价值.....	2
3. 区块链系统性解决金融痛点.....	3
4.....第二章 Sagittarius 区块链生态.....	4
5. Sagittarius 生态.....	5
6. Sagittarius 模式.....	6
7.第三章 Sagittarius 与银行金融系统结合的重大场景.....	7
8. 数字货币.....	8
9. 跨境支付与结算.....	9
10.. ..第四章 Sagittarius 技术特点.....	10
11. Sagittarius 的 SHA512 算法加密技术.....	11
12. RING TOPOLOGY HUB 环状拓扑中继技术.....	12
13.. ..第五章 SGR 通证模型.....	13
14. SGR 的分配与奖励机制.....	14
15.. ..第六章 Sagittarius 生态应用.....	15
16. SGR 价值流通应用.....	16
17. SGRSwap 去中心化 Swap 协议.....	17
18.. ..第七章 Sagittarius 发展规划.....	18
19.. ..第九章风险提示与免责声明.....	19

摘要

自各主流经济体表态积极推进官方发行的数字货币之后，越来越多的金融机构开始关注数字货币背后的“区块链技术(blockchain)”。然而，对于什么是“区块链”，以及它将对银行业带来什么影响，大多数的银行高管和从业人员仍然心存诸多疑问。

区块链技术，是继蒸汽机、电力、信息和互联网科技之后，目前最有潜力触发第五轮颠覆性革命浪潮的核心技术。该技术在金融领域的应用将完全改变交易流程和记录保存的方式，从而大幅降低交易成本，显著提升效率。在过去几年中，区块链技术已成为全球创新领域最受关注的话题，受到风险投资基金的热烈追捧。国际各大领先金融机构也纷纷行动起来，组建了 R3 CEV 和 Hyperledger 这样的区块链技术应用联盟。一场技术标准的竞争和颠覆式创新浪潮正悄然袭来。

区块链的特性将改变金融体系间的核心准则；因其安全、透明及不可篡改的特

性，金融体系间的信任模式不再依赖中介者，许多银行业务都将“去中心化”，实现实时数字化的交易。区块链的应用在虚拟货币、跨境支付与结算、票据与供应链金融、证券发行与交易及客户征信与反欺诈等五大金融场景将能产生最直接与有效的应用。以跨境支付结算来说，区块链将可摒弃中转银行的角色，实现点到点快速且低成本的跨境支付；根据麦肯锡的测算，从全球范围看，区块链技术在 B2B 跨境支付与结算业务中的应用将可降低每笔交易成本约 40%。

面对区块链技术迎面而来的机遇与挑战，全球领先银行已经开始积极布局，以抢占先发优势。各大银行目前采取的策略不一，大致可分为三类：

1) 组建区块链大联盟，制订行业标准；如 R3 CEV 集结超过 40 家国际领先银行建立行业监管及相应的技术标准。

2) 携手金融科技公司，发展核心业务区块链应用；如 Capital One 及 Visa 通过战略投资金融科技公司，

紧抓区块链技术的突破口。

3) 银行内部推进局部领域的应用，快速实施试点;如 UBS、花旗、德意志及巴克莱都已经成立区块链实验室，自行研发或通过与金融科技公司的合作，针对不同的应用场景进行测试。

本白皮书分析了 Sagittarius 基于区块链技术打造适用于银行系统的基础公链，并形成系统性生态，以此为契机，可助力第三方机构在数字货币改革、跨境支付与结算、供应链金融以及证券发行与交易等领域的长足发展。


同时，Sagittarius 认为，就金融机构应如何把握机遇，抓住战略机会提出了三个行动建议：

1) 国内银行应尽快就参与区块链技术的应用的策略予以明确；



2) 快速推进业务应用场景的试点实施；

3) 积极投资布局，小投入，广撒网，合理布局。



区块链技术的应用将开启许多令人兴奋的可能性，颠覆银行业的游戏规则并可能重塑整个行业格局。谁将是这一场颠覆式技术革命的最终赢家，我们拭目以待。




上世纪 70 年代个人电脑问世，人们开始借助电脑阅读资料，编写文档，但人们仍通过书信往来沟通，去银行网点存钱、汇款和借贷。上世纪 90 年代中期，商业互联网出现，人们可以随时随地购买和阅读书籍，使用无

需下载的流媒体收听音乐，人们开始使用邮件、即时消息和实时视频进行无缝沟通，开始使用网上银行存钱、汇款和借贷。现在，一项名为“区块链”的重大技术正在起步。20 年后我们也许会这样描绘我们的生活：数字货币

成为主流货币，人们可以随时随地向身处世界任何地方的任何人进行资产转移交易，就好像发送邮件或打开流媒体播放音乐一样方便、快捷、实时。



区块链，是继蒸汽机、电力、信息和互联网技术之后，目前最有潜力触发第五轮颠覆式革命浪潮的核心技术。就如同蒸汽机释放了人们的生产力、电力解决了人们最基本的生活需求、信息技术和互联网彻底改变了传统产业（如音乐和出

版业) 的商业模式一样, 区块链技术将有可能实现去中心化的数字资产安全转移。

“区块链”听上去充满了未来感和技术色彩, 但本质上它是一个去中心化的分布 式账本。去中心化, 也就是说所有的交易都是点对点发生的, 无需任何的信用中介 或集中式清算机构; 分布式账本, 意味着当交易发生时, 链上的所有参与方都会在自己的账本上收到交易的信息, 这些交易记录是完全公开, 且经过加密、不可篡改的。正是基于区块链技术这样的特征, 当其被应用到不同的场景时, 将为交易参与方带来主要以下四个方面的意义:

◦ 消除交易中介存在的必要性, 从而降低交易成本: 因为实现了点对点的交 易, 中央处理或清算组织成为冗余; 因为交易的真实性是由区块链上所有参与者 共同验证和维护的, 所以作为第三方的信用中介也失去了存在价值。

⑧ 交易结算几乎是实时的, 从而提升了交易效率, 大大提高资产利用率。

⑨ 区块链上信息的不可篡改性, 和去中心化的数据储存方式, 使其成为数据和 信息记录的最佳载体

⑩ 可编程的区块链使交易流程实现全自动化: 通过在区块链中嵌入预设好的 交易规则, 达到预定条件则自动完成, 可提升交易的自动化程度区块链技术的 颠覆性主要体现在以下两个方面:

最底层技术的颠覆者



如果我们将银行商业模式层层分解，不同的新技术发展一直在推动各个层面的进步（如上图）。以信息时代为例，互联网带动了应用层面的无数创新应用——P2P 借贷、在线理财、众筹；云平台改变了业务处理和基础设施部署的模式，大大降低了银行的业务运营成本和 IT 投入；大数据分析技术将风险控制从以经验判断为主带入了以机器学习为主、用数据作为决策依据的时代，使得全自动的快速信贷模式成为可能。尽管金融上层应用和业务流程创新风起云涌，但信用中介的基本要求使银行在商业模式的底层逻辑和相关技术，例如系统间的信息交互方式以及交易清算的基础设施方面，并未有革命性的提升。区块链技术的出现恰恰要颠覆银行商业模式的底层技术基础。首先，“清算”这个概念在区块链网络中将不复存在，所有的交易都是“发生即清算”的，交易完成的瞬间所有的账本信息都完成了同步更新；其次，系统间的信息交互不再因为兼容性和互斥性而导致部署成本高且连接困难，因为所有系统都使用同样的技术协议；而各参与方之间的交易规则也依照协议共识写入区块链成为标准，不得篡改。

商业制度创新的推动者

区块链技术的出现是对现有商业模式的制度基础和参与者之间关系的重大挑战。现有金融体系是建立在三个基本制度框架之上的：商业信任是依赖法律条文而存在的；资产转移交易是以独立第三方作为信用中介来保障实现的；交易结算和清算是以集中式的清算机构为中心来处理完成的，然而人们习以为常的制度基础和商业流程都有可能随着区块链技术的广泛应用被颠覆。在现有制度框架下如鱼得水的金融中介机构，如何在这场模式变革中调整角色，将决定其未来的命运。

从银行的角度来说，在这一波新的技术革新浪潮中是成为技术受益者，还是被颠覆方，完全取决于银行如何审时度势，积极调整自身在未来商业格局和逻辑中的角色定位，不再只做信用中介‘被动依赖垄断地位收取息差和交易费用’而

要积极做技术应用的先驱者，不断提升高价值的金融月良务能力和内容，引领和参与新的商业格局形成。

其“系统性”主要体现在三个方面：

⑧区块链技术可以被应用在不同的银行业务，从支付结算，到票据流转和供应链金融，到更复杂的证券发行与交易等各核心业务领域，均已有金融机构和科技公司在积极探索和尝试。

⑨区块链技术带来的收益将惠及所有的交易参与方，包括银行、银行客户、银行的合作方（如平台企业等）。

⑩目前金融服务各流程环节存在的效率瓶颈、交易时滞、欺诈和操作风险等痛点，大多数有望在区块链技术应用后得到解决（如下图所示）。例如现有流程中大量存在的手工操作、人工验证和审批工作将得以自动化处理，纸质合同将被智能合约所取代，而在交易处理环节不再会由于系统失误而导致损失发生。举例来说，区块链技术的应用可以帮助跨境支付与结算业务交易参与方节省约40%的交易成本。



Sagittarius CLUB（Sagittarius 生态）是国际知名的区块链技术服务商，在全球区块链开发、资产管理、战略规划以及生态应用融合等领域有着丰富的经验。Sagittarius CLUB 所代表的不仅仅是一种技术创新，更是顶级商业模式之间通力协作实现自身以及行业转型的技术驱动力。Sagittarius CLUB 基于来自 Sagittarius 公链的优势，我们已经在全球金融领域启动了数百个项目及几十个活跃网络，它们无时无刻不在银行和金融体系创造着价值。

拥有多年行业经验的专业团队，ABC TEAM 于 2016 年开始进行区块链业务开发，随后于 2017 年开始进行 ICO 和区块链咨询，并于 2018 年成为 ABC 联合主席资格，充分发挥专业经验和知识，为全球提供高质量服务。ABC TEAM 已被邀请参加由 BDEX 交易所和 Trichanin Capital 主办的国际贸易竞赛。

未来，Sagittarius CLUB 将以 Sagittarius 公链为核心，面向全球金融机构提供优质服务，不断驱动行业向更加完善的价值互联网转变。

Sagittarius 针对包括银行在内的金融生态中存在的痛点，打造以区块链技术为应用模式的基础公链，将提供革新的解决方案，提供所有金融商品账户管理的专业平台服务。Sagittarius 利用安全分散型区块链技术，为生态体系打造数字货币 SGR，促进自有生态以及第三方银行机构的用户使用频率，在基于流通价值的基础上实现全生态下的价值的良性循环。同时打造 DAPP 应用程

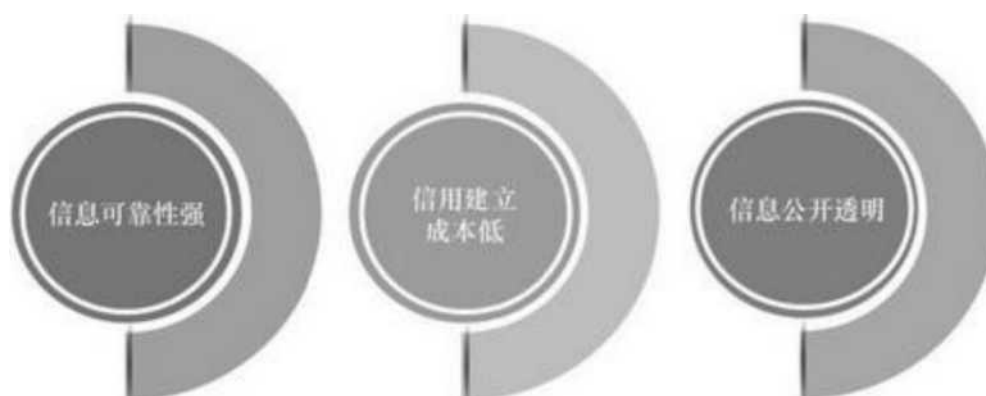
序，为全球用户提供一个快捷、安全、可信任的金融基础工具。

Sagittarius 公链在银行体系内容的运转，将为行业带来以下几个方面的改变：

形成新的混合型数字货币体系。Sagittarius 公链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。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，那些具有信誉度的银行基于 Sagittarius 公链推出数字货币并创造了虚拟交易场景，则可以让消费者能够体验到更好的创新性服务。

形成新的信用形成机制。信用体制一直以来都是银行发展的核心。在传统模式下，银行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。在客户申请贷款的时候，银行需要查询与客户相关的各种征信数据信息。在查证环节中，信息的收集链条环节比较多，所涉及的范围比较广，但依然存在信息不经、数据不准备等缺陷，同时还造成成本过高、决策程序冗长等问题，这样对银行高效完成业务操作具有极大的影响。

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。



Sagittarius公链的区块链技术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。

形成新的场景价值链。互联网的突飞猛进以及对金融市场的极大冲击，使得传统的销售模式已经不再适应现代经济的运行需求。场景金融成为当前互联网金融发展的重要支柱，使得银行从传统的单一的厅堂营销服务场景融入更多的场景当中，比如网购场景、社交场景、旅游场景等，这样不但可以增强客户的体验满意度，还可以形成一个依托场景的金融生态圈。

Sagittarius 公链技术本身架构灵活，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资金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：

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。

Sagittarius 公链技术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。区块链在银行支付结算方面的应用，使得银行新城了一种全新的支付结算方式。

Sagittarius 公链基于区块链特性和生态独有的创新 将在银行等金融系统中 实现五大场景应用，驱动传统金融机构转型发展。Sagittarius 公链“去中心化”的本质能让当今金融交易所面临的一些关键性问题得到颠覆性的改变，而其应用的 最佳场景将是在支付及交易银行、资本市场及投资银行业务等。

Sagittarius 公链将提高货币发行及使用的便利性！

比特币的崛起颠覆了人类对货币的概念。比特币及其数字货币的出现与扩展正在改变人类使用货币的方式。从过去人类使用实物交易，到发展物理货币及后来的信用货币，都是随着人类的商业行为及社会发展不断演进。随着电子金融及电子商务的崛起，数字货币安全、便利、低交易成本的独特性，更适合基于网络的商业行为，将来有可能取代物理货币的流通。

以比特币为代表的数字货币目前已在欧美国家获得相当程度的市场接受，不但能在商户用比特币支付商品，更是衍生出比特币的借记卡与 ATM 机等应用产品。数字货币与法定货币之间交换的交易平台也应运而生，例如美国最大的比特币交易平台 Coinbase 目前支持美金、欧元、英镑及加拿大币与比特币之间的兑换；比特币与法定货币之间的庞大交易量与流动性足以被视为一种国际通行货币。正是比特币网络的崛起，让社会各界注意到其背后的分布式账本区块链技术，并逐渐在数字货币外的众多场景获得开发应用。

国家发行数字货币将成趋势。2015 年厄瓜多尔率先推出国家版数字货币，同时，其他许多国家也在探讨发行数字货币的可行性。目前，包括瑞典、澳大利亚及俄罗斯正在研讨发展数字货币的计划。英国央行正委托伦敦大学学院设计一套数字货币 RSCoin 进行试验,预期通过央行发行的数字货币来提高整体金融体系的安全性与效率。依托 Sagittarius 公链打造的数字货币，能够替代实物现金，降低传统纸币发行、流通的成本，提高支付结算的便利性;并增加经济交易透明度，减少洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力;同时，通过发展数字货币背后的区块链技术应用，扩展到整个金融业及其他领域，确保资金和信息的安全，提升社会整体效能。

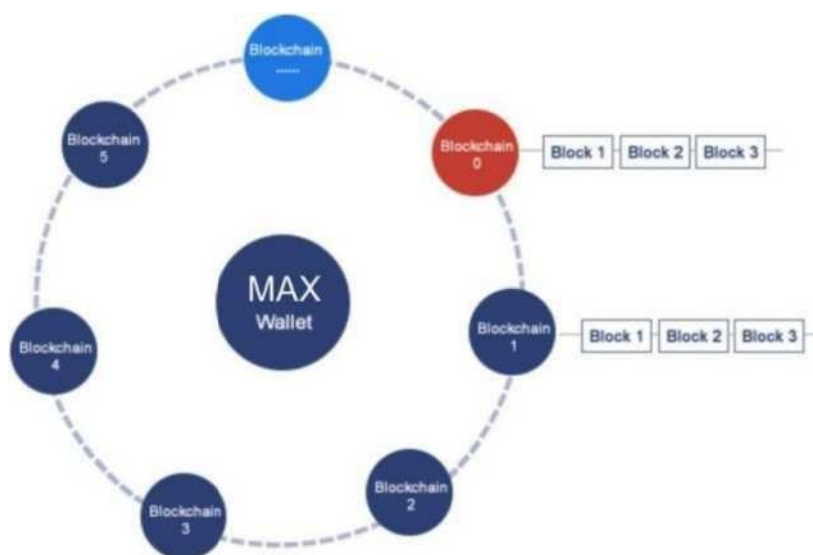
当前的跨境支付结算时间长、费用高、又必须通过多重中间环节。拥有一个可信任的中介角色在现今的跨境交易非常重要，当跨境汇款与结算的方式日趋复杂，付款人与收款人之间所仰赖的第三方中介角色更显得极其重要。每一笔汇款所需的中间环节不但费时，而且需要支付大量的手续费，其成本和效率成为跨境汇款的瓶颈所在。如因每个国家的清算程序不同，可能导致一笔汇款需要 2 至 3 天才能到帐，效率极低，在途资金占用量极大。



Sagittarius 公链将可摒弃中转银行的角色，实现点到点快速且成本低廉的跨境支付。通过区块链的平台，不但可以绕过中转银行，减少中转费用，还因为区块链安全、透明、低风险的特性，提高了跨境汇款的安全性，以及加快结算与清算速度，大大提高资金利用率。未来，银行与银行之间可以不再通过第三方，而是通过区块链技术打造点对点的支付方式。省去第三方金融机构的中间环节，不但可以全天候支付、实时到账、提现简便及没有隐形成本，也有助于降低跨境电商资金风险及满足跨境电商对支付清算服务的及时性、便捷性需求。

SHA（Secure Hash Algorithm，译作安全散列算法）是美国国家安全局（NSA）设计，美国国家标准与技术研究院（NIST）发布的一系列密码散列函数。通过对SHA512加密技术的定制，研发出属于Sagittarius使用的SHA512加密技术，保证对Sagittarius公链网络的数据安全。

Sagittarius的Ring Topology Hub技术将多条链连接到一个Hub上，让数字资产终端轻松实现一键跨链和转换。环状的优势在于拓扑结构对资源的消耗比星型、树形要小很多。节点少、距离近可能不明显，但是距离远、节点多，环网的这一优势会很明显。大体的设计结构如图所示：



SGR 是持 Sagittarius 生态系统的唯一的价值流通通证。在 Sagittarius 生态系统中，所有生态场景的流通支付、手续费、用户激励等均已 SGR 作为中介。

Sagittarius 发行的代币名称为 **SGR**，发行总量 **10 亿枚**，具体分配方案下：

分配情况	占比	说明
空投	1%	根据项目的进度不定期空投
流动性挖矿奖励	73%	85%挖矿奖励/15%分享奖励
流动性	2%	全部用于初始添加流动性
创始团队	10%	6 个月后，分十个月线性释放
基金会	9%	市值管理团队
私募	5%	分 5 期进行私募

SGR 激励：

- 1) 钱包持有 SGR 视为有效账号获取分享链接。
- 2) 每次交易扣 11%。
- 3) 7%添加流动性。
- 4) 转账销毁 1%（销毁剩 50"再销毁）。
- 5) 推荐被推荐人交易，一代推荐人可获得 2%交易奖励，二代推荐人获得 1%交易奖励。
- 6) 推荐流动性挖矿/质押挖矿奖励：第一代 10%第二代 5%。
- 7) 交易手续费会磚市场情况进行合约调整，直至最终上线主流交易所。（最终合约自动关闭）

1 SGRSwap 去中心化 Swap 协议

本项目实现一种基于 SGR-Rollup 技术的 Layer-2 AMM 去中心化交易协议 SGR-Swap，在 Layer-2 上实现了 uniswap 的所有功能，在保证去中心化交易的核心价值的同时，实现实时交易，把 Uniswap 的 TPS（每秒可以处理的交易数量）提升了多个数量级，同时交易的过程几乎不需要消耗任何 Gas 费用。

SGRSwap 系统框架

SGRSwap 系统由链上智能合约，链下 SGRSwap Server，零知识证明系统和前端用户界面组成。

Fig. 1.系统架构

SGRSwap 智能合约 SGRSwap 会在以太坊区块链上部署一系列智能合约，用于存储用户存入的代币，同时需要记录和验证 Layer-2 的状态更新和相关证明，是连接链上和链下的关键枢纽。

SGRSwap Layer-2 服务端 SGRSwap 服务端是在链下实际处理所有交易的模块。SGRSwap 服务端可以通过 WebSocket 接口和用户发生交互，同时还可以监听以太坊区块链上的交易。所有合法的交易请求将被放入 SGRSwap 内存池中，

最终由 Swap Engine 负责处理。内存池中的交易类型和上一节中 Uniswap 所有操作类型保持一致。Block proposer 对交易进行 Rollup 生成新'区块'并由 State Keeper 更新 Layer-2 中所有代币的状态。State Keeper 会把状态发送给

Committer，后者负责与 Prove server 通信，获得对应交易的证明，并最终将状态和对应的 SNARK 证明通过 Ethereum sender 发送到链上的SGRSwap 智能合约。

Plonk 零知识证明系 SGRSwap 的零知识证明系统采用分布式架构，并采用最新的零知识证明算法 PLONK[6]生成证明。Prove server 支持多个 Prover。多个 Prover 主动查询 Prove server 中的证明任务，生成证明后发回 Prove server。PLONK 的全局 trust setup 只需要生成一次，电路规模在一定范围内的应用都

可复用，极大地降低了零知识证明的使用门槛。

SGRSwap 状态树

SGRSwap 系统的状态树记录了当前系统中所有账户的余额状态。SGRSwap 的状态树是一棵高度为 34 的默克尔树。根节点 Root 的子节点为系统中所有账户节点（24 层）。

账户节点分为两种类型：

普通账户节点，用于记录账户内所有 Token 的状态。普通账户节点可以有任意多个叶子节点（10 层），每个叶子节点都代表一种类型的 Token 及其数量；同一账户下的 Token 类型不可重复；

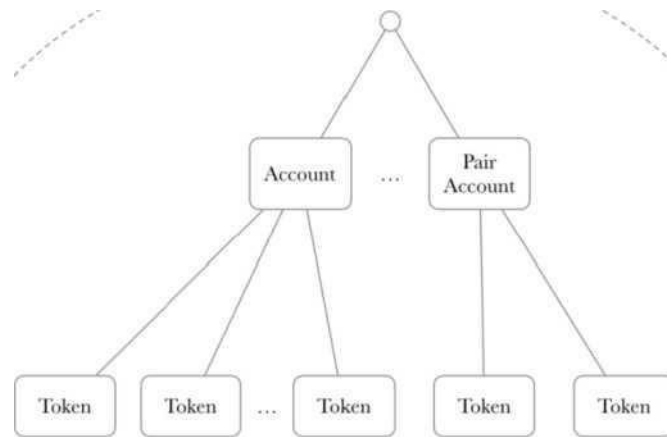
Pair 账户节点，用于记录 SGRSwap 中某个交易对资金池的状态。Pair 账户节点只包含两个叶子节点，每个叶子节点代表该资金池中一种 Token 的余额和类型。

SGRSwap 中交易的过程实际就是状态树更新的过程。下面介绍SGRSwap 中所有交易类型和对应的状态变化。

存币 (Deposit)

Deposit 是指用户把以太坊链上的代币存入 SGRSwap 合约，使其可以在 Layer-2 中使用的过程。Deposit 操作由用户从链上发起。当 SGRSwap Server 监听到用户在链上将 Token 转入 SGRSwap 智能合约的交易后'会根据交易详情更新状态树。首先，根据交易所属的账户找到对应的 Account，并根据Deposit 的金额更新 Account 下对应 Token 的状态。若该 Account 下没有对应 Token 的叶子节点，首先需要创建该 Token 对应的叶子节点，再进行状态更新。叶子节点的状态更新完成后，根节点的哈希也会随之更新。

更新后的状态树根节点哈希会和 Deposit 交易的 SNARK 证明一起被发送到链上的 SGRSwap 合约中。



取币 (Withdraw)

Withdraw 是指用户从 Layer-2 中将 Token 提出，并从 SGRSwap 合约中 解锁⁵ 发到对应 Layer-1 账户的过程。Withdraw 操作由用户从 Layer-2 发起，SGRSwap server 在收到用户对某一Token 的提币请求后，会更新对应账户下对应 Token 的状态，并把更新后的状态树根节点哈希和 Withdraw 操作 应用的证明发送到链上 SGRSwap 合约。合约验证通过后会 把合约中锁定的对应 Token 发送到对应链上账户。

转账 (Transfer)

Transfer 是指用户在 SGRSwap Layer-2 把某种 Token 发送给另一用户的过程。Transfer 由用户在 Layer-2 发起。当 SGRSwap Server 收到 Transfer 请求后，会根据请求详情找到对应的收发账户，并根据发送金额更新收发双方账户下该 Token 的状态。状态树根节点哈希也会随之更新，并和 Transfer 操作对应的 SNARK 证明一起被发送到 SGRSwap 链上合约。Transfer 不会改变链上对应 Token 的状态，因为 Token 仍然锁定在 SGRSwap 合约中，并没有在链上发生转移。

增加流动性 (Create Uquidity)

Create liquidity 是指用户在 Layer-2 完成创建或增加流动性的操作，其定义和uniswap保持一致。Create liquidity 由用户在 Layer-2 发起，当 SGRSwap server 收到用户创建某一对 Token 流动性的请求后，首先需要找到对应的发起人 Account 和这一对 Token 的 Pair Account（若 Pair Account 不存在，需要先创建 Pair 资金池）；然后把 Account 下两种 Token 按照 AMM 算法规定的比例要求 Transfer 到 Pair Account 下；同时系统会计算出用户可以获得的 LP Token 数量，并更新流动性提供者 Account 下对应的 LP Token 状态。所有状态更新完成后⁵ 状态树的根节点哈希将会和 Create Uquidity 对应的证明一起被发送到链上的 SGRSwap 合约。首次创建的 LP token 需要由 SGRSwap 合约在链上部署对应 LP Token 的合约。

减少流动性(Remove Liquidity)

Remove Liquidity 是指用户从 Layer-2 的某一 Pair 资金池中销毁 LP Token 并在 Layer-2 中取回相应比例的两种 Token 的过程。Remove Liquidity 由用户在 Layer-2 发起，当 SGRSwap Server 收到用户 Remove Liquidity 请求时，首先会找到对应 Account 销毁 Account 下对应数量的 Liquidity Token；接着会将 Liquidity Token 对应的 Pair Account 下的两种 Token 按照比例 Transfer 给销毁 Liquidity Token 的 Account。操作完成后状态树会做相应更新⁵ 根节点哈希和对应的 Remove Liquidity

Swap 交易

Swap 是指用户在 Layer-2 的资金池中完成交易的过程。假设用户需要在包含 TokenA -TokenB Pair Token 的资金池中进行 Swap 交易。用户首先从 Layer-2 将自己 Account 下的 TokenA 发送到对应的 Pair Account，SGRSwap 会根据 AMM 算法计算用户可以获得的 TokenB 的数量并发送给用户。状态树随之更新⁵ SGRSwap Server 会将更新后的状态树根节点哈希以及 Swap 操作对应的证明发送到链上的 SGRSwap 合约。Swap 交易不会改变链上 Token 的状态，因为 Token 本身仍然锁定在 SGRSwap 合约中。

提取流动性(Withdraw Liquidity)

Withdraw Liquidity 是指用户从 Layer-2 账户中的 Liquidity Token 提取到 Layer-1 的过程。Withdraw Liquidity 在 Layer-2 的发起过程和状态更新与上述普通的 Withdraw 完全一致，但在 Layer-1 中产生的结果不同。SGRSwap 合约收到 Withdraw Liquidity 请求后，会自动触发 Liquidity Token 的 mint 操作，在 Layer-1 中创造出额外的 Liquidity Token，并发送给指定账户。

总结与展望

SGRSwap 利用 SGR-Rollup 技术，在 Layer-2 实现了Uniswap 的完整功能，是一套去中心化的 Layer-2 代币 AMM 自动化做市商 Swap 协议。SGRSwap 协议可无限扩展，支持超高 TPS，且流动性提供者和用户不需要支付高昂的 gas 费用，并且具备实时交易性，用户不再需要等待区块确认，就可以在 Layer2 上面完成极速的交易，极大降低了DEX 的使用门槛，对现在所有的 DEX 和 CEX 都带来了巨大变革。

SGRSwap 由 L2 Lab 支持开发。在未来，L2 Lab 将继续推动 Layer-2 协议层的发展，结合 SGRSwap、Layer-2 隐私稳定币等一系列 Layer-2 基础协议 打造完整的 Layer-2 DeFi 生态。

通过打造用户体验极佳的 Layer-2 协议标准，L2 Lab 致力于推动区块链行业的范式转换，让 Layer-1 成为清结算的根基，Layer-2 成为连接区块链应用和 Layer-3 的桥梁和出入口。我们会致力于推动让所有的区块链应用都运行在没有任何限制的 Layer-3 的世界。我们会致力于让 SGRSwap 成为 DEX 中最好用的产品，时机成熟的时候，也会推出流动性挖矿计划和 DAO 计划，助力分布式金融 DeFi 的崛起，一起引领区块链应用的范式变革。

依托于 Sagittarius 公链发行的 SGR 数字货币，面向全球用户，将实现在旅游、美容、游戏、购物等支付流通。

- 8) 在旅游场景中，SGR 基于公链生态的应用，可以实现机票购买、酒店预订、跨境旅游支付等功能，同时，还能实现旅游置业、旅游健康产业投资等；
- 9) 在美容场景中，以韩国为例，美容机构和整形医院已经开始接受数字货币支付，用户使用 SGR 可实现美容消费、整形医院及机构的医美费用支付，解决先进支付和传统支付到账和汇率问题。



Sagittarius 生态白皮书

