BYSTACK

全球首创一主多侧架构

BUTXO模型BaaS平台

引言

自从 2015 年，人们发现了区块链巨大的潜在价值之后，区块链技术已经飞速发展了四年多，这四年中，区块链成为科技、金融、政府多方认可和推崇的创新技术，全球众多科技、金融巨头都投入了大量的人力物力进行研究，行业内初步涌现出了一批优秀的创业公司。然而，区块链技术发展还远没有达到成熟阶段，虽然整个区块链行业百花齐放却各有弊端，我们知道区块链行业的开拓者很难把区块链技术推向大规模的应用落地中。基于此，比原链团队从区块链架构和底层技术的维度出发，立足于区块链大规模落地场景，在共识机制、智能合约、可扩展性、隐私安全、跨链交互等几个方面对现有区块链进行优化，推出 Bystack 这一蕴含颠覆性理念和前沿技术的产品。

Bystack 是帮助用户快速创建，管理和维护企业级区块链网络和商业区块链应用的服务平台，具有开发成本低，部署快捷，性能高和扩展性强，安全可靠，方便易用等特性，为开发者或企业提供区块链能力的一站式解决方案。

Bystack 独创的主侧链模型和核心的 Blockcenter 系统通过将底层的区块链网络，共识，应用开发能力，区块链配套设施进行整合和抽象，转化为用户熟悉的可编程接口和操作界面，屏蔽底层的技术细节，让应用开发更加简单高效，让企业和开发者更加专注于区块链应用的开发。

1 序言

1.1 区块链技术的目标

自比特币白皮书中将区块链作为一种点对点电子现金系统底层技术概念首次提出以来，区块链作为一种综合性技术架构已衍生出了多种类型的技术结构，从开放程度上衍生出公有链、联盟链与私有链，从共识算法上衍生出 PoW，PoS、DPoS 和 PBFT 等，从底层模型上衍生出的 UTXO 模型和账户模型，从底层账本上衍生出区块链和 DAG，以及衍生出的跨链和侧链技术。

不论何种区块链，都想通过其独特的共识算法，密码学技术，分布式数据存储来构建一个去信任、高可靠、高可用、防篡改的商业系统，实现真正区块链应用落地。

1.2 当前商用区块链平台综述及问题

目前市场上出现了许多商用区块链平台，它们旨在突破商业与金融应用场景，具有可靠性、可运维性等优势，提供简单易用，一键部署，快速验证，灵活可定制的区块链服务。但是现在的商用区块链平台究其根本，提供的只是接口化的云服务，其底层实现一般都是闭源，不具有透明性和开放性，对用户来说完全是黑匣子，区块数据浏览器也一般不对普通用户开放，因此用户使用门槛较高且受制较大，不能为社区开发人员提供完全的自由的开源实践平台。

此外，为企业打造区块链解决方案，区块链不可能三角[①]是难以回避的第一性原理问题，即在去中心化、安全性、可拓展性（效率）三者之间，只能取其二。如果说安全是所有区块链即服务（BaaS）不可舍弃的属性，那么区块链不可能三角就简化为去中心化和效率的二元悖论。公有链的去中心化有保障，但 TPS 难以满足大型企业应用的需要。联盟链、私有链可扩展性高，但不具有去中心化、数据不可篡改性、交易不可逆转性等区块链属性，存在信用风险。

借鉴互联网 TCP/IP 协议栈经验，建立区块链分层模型或将解决区块链二元悖论，同时可以构建完整的商业应用架构。

分层的第一设计原则是，层次堆栈，每一抽象层创建在低一层提供的服务上，并且为高一层提供服务，即下层不关心上层的运行状态，但上层需要了解下层实现。 完成一些特定的任务需要众多的协议协同工作，这些协议分布在参考模型的不同层中的，因此可以称其为

① 《不可能三角形：安全，环保，去中心化》

一个协议栈。

分层的第二设计原则是层级之间独立，服务于不同功能需求，在 TCP/IP 协议中，IP 协议只关心如何使得数据能够跨越本地网络边界的问题，而 TCP 协议关心数据如何在各网络状态下可靠地传输，相对地在区块链模型中，需要有不同协议层去解决价值共识问题，交易效率问题，以及基于区块链的业务实现问题。

因此我们提出将区块链应用分为三层架构： 底层账本层，侧链扩展层，业务适配层 。其中核心是 Layer1（底层账本层）和 Layer2（侧链扩展层），Layer1 创造一个无需许可的共识环境，保障去中心化，侧重记账功能，是交易的安全性和数据不可篡改性的根基。Layer2 负责交易效率，侧重业务能力，提供快捷强大的业务接入能力，将 Layer1 的价值传递到实际业务中，也可以通过中继再回归到 Layer1 上。这样这两层优势互补，兼具去中心化和效率。

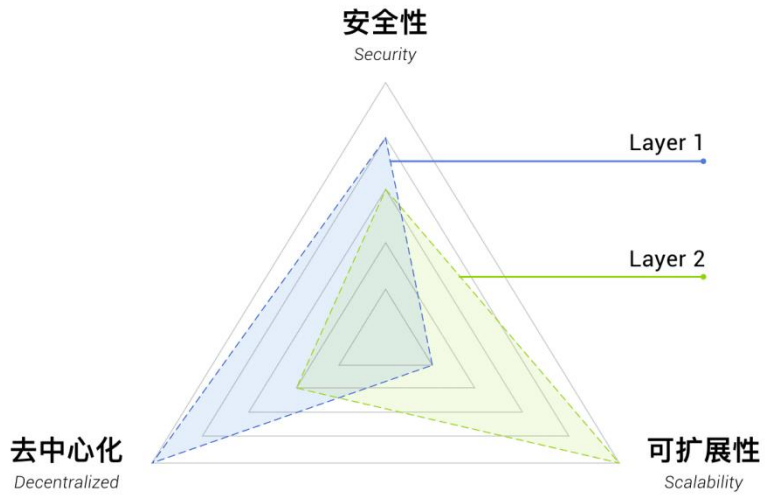

图 1

业内有将区块链系统分为清算层和计算层，代币运行在清算层，是整个系统的基础。计算层提供智能合约、身份认证、消息通信等功能，方便开发者开发应用。但是上述方案并不能很好的支持不同业务场景，比如同样是做资产上链，股权和商业积分对区块链功能的需求是不一样的，商业积分并不需要建立用户真实身份，股权则需要对应用户真实身份，且交易对象受限于“股东人数不能超过 200 人”等《公司法》的规定。单一 Layer2 不能像 Layer1 一样通用于所有业务场景。为此，比原链团队创新地提出一主多侧链架构的 BaaS 架构——Bystack，以 Bytom 公链作为统一 Layer1，可根据不同业务场景需要，接入不同 Layer2 侧链。

2 主侧链协同工作模型

Bystack 解决方案是主侧链（一主多侧）协同工作模型，主链采用 PoW 共识保证多样资产的安全和去中心化，侧链通过可插拔技术实现不同的解决方案，从而满足不同的业务场景和对更高性能的要求，加速区块链商业应用的落地。

主侧链协议本质上是一种跨区块链解决方案。这种解决方案，可以实现数字资产从一条链到另一条链的转移，当然也可以从另一条链安全返回到第一条链。在 Bystack 中，创建、存储资产的区块链网络通常被称主链，而作为业务辅助的链则被称为侧链。侧链协议被设想为一种允许数字资产在主链与侧链之间进行转移的方式。

Bystack 的主链需要保证安全和稳定，所以性能、可扩展性以及更多的创新的尝试会在侧链上落实。

2.1 主侧链架构

下面是主侧链协同的架构图：

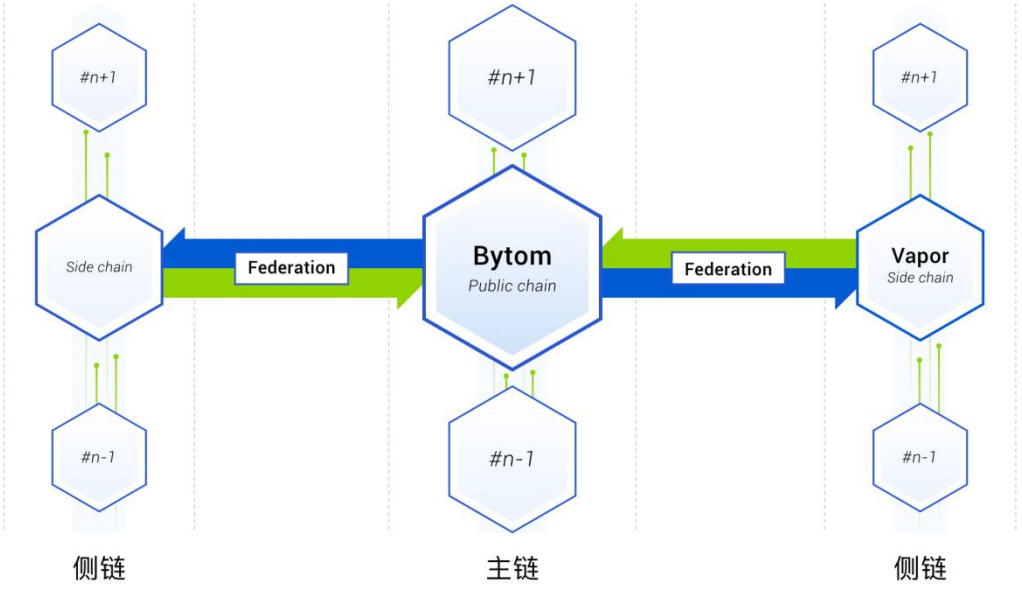

图 2

2.1.1 主链的角色

Bystack 的主链采用基于对 AI 计算友好型 PoW（工作量证明）算法 Tensority 的 Bytom 公链[i]。主链主要担任价值锚定，价值传输和可信存证的角色。任何的资产创建，传输和销

毁都由主链发起，再通过 Federation 楔入到侧链上，从而保证资产的安全性。同时所有的业务或者资产的数字指纹信息都在主链上做可信存证，因为只有算力保证的主链才能做可信存证。

2.1.2 侧链的角色

Bystack 的侧链主要是服务于垂直领域的业务，满足那些对 TPS 要求较高，且数据量比较大的业务。同时侧链支持更加灵活的搭建方式，企业或个人可以使用已运行的侧链，也可以生成属于自己的侧链，并在侧链上搭建自己的生态应用。主链资产通过 Federation 楔入到侧链，然后在侧链的内部流通和使用。侧链支持可插拔的共识，数据库插件，可以更好的搭配以满足实际的业务需求。

2.1.3 Federation

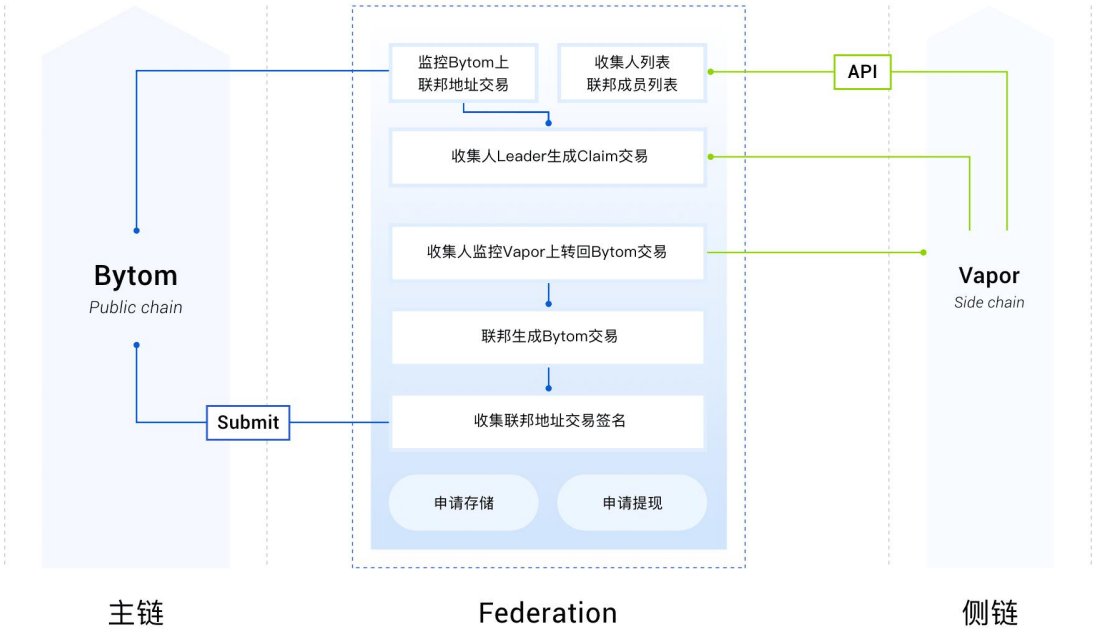

图 3

Federation 当中分为三种角色：

验证人：侧链的出块人，任何人都可以成为验证人。

收集人：监控主链锁定在联邦合约地址的交易，收集交易并生成 Claim 交易，发送到节点验证人进行验证后进入交易池。

联邦地址： 侧链充值是指资产从主链楔入到侧链的转移过程，是需要资产先锁定到联邦合约地址。

联邦合约地址生成：

（1）联邦合约地址需要多名联邦成员公钥生成，系统开始启动由初始出块人担任。

（2）运行一段时间后 Vapor 侧链上用户可以注册为联邦成员候选人，由 Vapor 侧链用户投票，从注册候选人中选出联邦成员，每次联邦成员变动不能超过联盟总成员的 1/3。

（3）选出联邦成员后，由新的联邦成员生成新的合约地址，以前的联邦合约地址转账到新的联邦合约地址。

（4）转账完成后，主链锁定资产到新的联邦地址，以后可以再竞选联邦成员。

收集人：

（1）系统启动之时，由初始出块人担任。

（2）运行一段时间后，Vapor 侧链上用户可以注册成为候选收集人，由 Vapor 侧链用户投票，从注册的候选人中选出收集人(DPoS 出块一轮筛选一次)。

（3）下发新的监控主链的联邦合约地址的收集人，收集交易，并附带收集人列表、收集人签名、原始交易、收集人公钥的 Claim 交易到节点。

侧链提现流程：

（1）Vapor 侧链用户发起提现请求，销毁 Vapor 侧链的资产。

（2）联邦合约地址针对请求向 Vapor 侧链用户的主链地址发送对应对应数量的资产(前提交易已经在侧链上达到不会回滚的确认数).

（3）联邦在侧链上生成一笔完成提现的操作的交易。

2.1.4 创新性

（1）共识层创新

侧链共识以投票人(Voter），共识节点（Delegate）和领导节点（Leader）来组织网络。首先以 DPoS 的模式进行投票来选出共识节点，然后共识节点以高效独创 BFT 的模式来达成共识。

（2）网络层创新

传统联盟链是主从节点架构，甚至是 C/S 模型， 服务端会实现完整协议而客户端尽量架构简洁，着重产品功能和交互， 相对于从节点不参加共识甚至不验证来说，侧链可以完

整保留对等节点的可用功能，这样就需要更快的网络，而且更复杂的环境中可靠传输交易和区块信息。

Vapor 神经元中继（Vapor Neuron Relay）(VNR)。基于 UDP 和向前纠错（FEC）协议，传输区块头和缩短的交易 ID 和部分对等节点不具备的交易信息，接收方节点将尝试使用接收到的信息，以及在本地内存池（Memory Pool）当中的交易，来重新构建整个区块。只有仍然缺失某些交易时，才会请求广播对端节点交易。

（3）协议层创新

以太坊账户模型受限于串行验证效率瓶颈， 难以提高吞吐。 Vapor 基于 BUTXO 可并行验证区块，且可多线程并行验证交易 BUTXO， 设计并行滑动窗口验证算法 PSWV（Parallel Sliding Windows Validation)， 该算法一次同步上百个区块，并获取它的所有输入，批量区块形成校验窗口，算法验证器滑动验证窗口内区块交易的合法性。

（4）存储层创新

去掉了公链普遍使用的本地 KV 数据库 LevelDB， RocksDB 等，替换为更通用和强大的数据库层接口，满足使用高性能 MySQL，PostgreSQL， MongoDB 等企业级数据库的业务需求，另外对于数据分析的需求， 也同时兼容 HDFS, HIVE，融入 Hadoop 或 Spark 生态系统。

2.2 资产和操作类型

2.2.1 资产类型

多类型的资产发布是 Bystack 的一大特点，我们按照资产的可分割性（Severability）和可互换性[②]（Fungibility）将资产定义为四种类型（如图 4）：

1、比特资产（BAP-01），可分割，可互换。对应 Token 等虚拟资产以及货币、积分、股票（同股同权）等现实资产，相当于以太坊 ERC-20 协议。

2、原子资产（BAP-02），可分割，不可互换。如 Bytom 原生资产 BTM 或其它通过 BAP-02 发行的股票（同股不同权）等现实资产，相当于比特币等非同质加密货币协议。

3、夸克资产（BAP-03），不可分割，不可互换。适合应用于游戏道具、游戏宠物等虚

② 可互换性：拥有某个属性的某个事物（例如资产或商品），在支付或结算时，某个部分或数量可以被另一个同等部分或数量所替代

拟资产和房产、收藏品、商品、防伪码等所有权类现实资产，相当于以太坊 ERC-721 协议。

4、量子资产（BAP-04），不可分割，可互换。可应用于红包等虚拟资产以及优惠券、门票、二维码等凭证类现实资产。③

图 4

事实上，我们并没有发明新的资产，而是试图在区块链的世界真实的映射现实世界的各种资产，并从物理属性的角度给予资产更基础的分类，方便人们在金融、政务、游戏、积分等场景中对资产进行更方便的归类、组合及划分。

2.2.1 操作类型

Bystack 将资产间的互操作定义为四种类型：

映射：资产数字化，现实经济中的真实资产上链。如股权，债权，收益权等资产

存证：数字资产化，信用、身份、品牌、行为数据等数字资源上链，通过链上可以转移所有权和使用权。

跃迁：资产从侧链迁入主链。

楔入：资产从主链迁入侧链。

以上所有操作都是原子操作，即，要么完全完成，要么根本不发生。不存在会导致资产损失或欺诈发生的可能。

③ BAP 协议 Bytom Asset Protocol

2.3 部署和使用

本地部署： 面向个人开发者，用户可以在服务器中部署属于自己的侧链，然后测试自己的侧链上的商业应用。

跨云部署： 面向企业用户，企业的侧链可以支持多种不同的云服务，包括阿里云，腾讯云，华为云等等。区块链的节点可以分散部署到不同的公有云平台上。

混合部署：为了满足不同的业务需求，可以根据联盟参与方需求部署区块链节点，即部分侧链的节点运行在云平台上，部分侧链的节点运行在客户的私有 IT 环境或者私有云内。

3 共识网络

比原链的主侧链模型中，主链主要采用 Tensority PoW 共识算法④，侧链提供可插拔的共识，可以满足不同的业务需求，但 Bystack 本身还独创了一种 DPoS+BBFT 的共识算法，所以本章主要详细阐述侧链的 DPoS+BBFT 的创新共识算法。

3.1 网络层面

3.1.1 DPoS

DPoS 的原理是让每一个持币者进行投票，选出一定数量的持币者代表,或理解为一定数量的代表节点，并由这些代表节点来完成交易验证和区块生产的工作。持币者可以随时通过投票更换这些代表，以维系链上系统的“长久纯洁性”，保证该协议有充分的去中心化程度。

在目前区块链的实现中 DPoS 共识只用于账户模型， UTXO 模型与 DPoS 的结合也会有许多额外的优势，UTXO 模型是存放记录的一种方式，用于交易存储、组织及验证；DPoS 是一种共识算法，用于保证在分布式网络中参与者也可以对交易数据取得一致认识。

UTXO 和 DPoS 结合的一大难点在于时间戳，DPoS 共识基于时间，会严格检查区块时间。全节点系统时间必须设置为和标准时间一样，否则共识一致性会出现问题。而 UTXO 本身也记录了时间戳的功能，但时间戳并不基于标准时间。在 LBTC 里将时间戳统一成标准时间协议，以保证区块的正常运行。当存在作恶节点或者时间不同步的区块时，出块被作为异常块处理，出块节点被作为异常节点处理。

④ 《比原链：一个多元比特资产交互协议》

在 UTXO 模型中，并不支持查询地址余额的功能，是通过全局遍历 UTXO 数据，实时计算地址余额。实时计算的工作量相当巨大，现实中不具备可行性。为了 DPoS 算法的需要，Vapor 中新增地址余额计算、节点注册、节点投票新功能。考虑到共识算法的高性能要求、注册节点数目的有限性，把地址余额、节点注册及投票信息保存在内存中，并把数据回写到数据库。通过数据库和地址余额、投票信息来链接 UTXO 记账信息和 DPoS 共识机制。

注册、投票的信息由 Vapor 底层协议负责传输。把注册、投票信息保存在内存以及数据库中。DPoS 共识模块查看注册、投票信息，完成共识。

3.1.2 BBFT(Bystack Byzantine Fault Tolerance)

共识(Consensus)是分布式系统中节点对数据或者网络的最终状态达成的某种协议。由于网络环境和节点状态的不可控性，共识机制需要同时考虑性能，可靠性，以及安全性的问题。尽管 PoW 共识在非许可（Permissionless)链上应用广泛，但是它的概率模型在提供较高可靠性的同时牺牲了效率同时浪费了大量的计算资源。在具体的商业应用环境中，许可（Permissioned)机制的采纳保证了一定程度上的节点可信度 (Semi-Trust)，而用户更关心执行效率（TPS）- 交易确认所需时间，和最终性（Finality）- 交易结果能否最终被确认。ByStack 侧链采用了 BBFT 共识来解决用户的痛点。

BBFT 是一种基于实用拜占庭容错 PBFT[⑤]的衍生共识。在保证拜占庭容错，即允许少量节点（$f \leq N/3$）作恶的情况下，具有以下 ”C.A.S.H.“ 特性：

（1）配置性（Configurable）：

采用模块化，可插拔设计，按需配置，并在一定程度上保证对新技术的兼容（Future-Proof)。

（2）适应性（Adaptive）：

针对不同的网络环境，提供稳定的执行效率。BFT 需要节点之间互相交换验证结果来取得多数共识。一般来说，每个节点需要得到足够多（>= (2/3) * N）的来自其他节点的回复才能做出有效的判断。网络延时是信息交互效率的重要因素。特别在跨地域以及跨境应用中，延时将成为网络的瓶颈。在 BBFT 中，共识节点维护当前网络拓扑，按最短路径原理相近的节点采取优先通信，对通信的聚合可以进一步降低延时。同时领导节点（Leader）的角色被

⑤ Practical Byzantine Fault Tolerance http://pmg.csail.mit.edu/papers/osdi99.pdf

弱化，类似 PBFT，当共识节点拿到超过 2/3 票数的情况下就可以做出判定，从而在领导节点的通信受到阻塞的情况下也不会对整个网络的决策产生巨大影响。

（3）扩展性（Scalable）：

保证共识复杂度随网络容量线性（Linear）或低于线性（Sub-Linear）增加。一方面共识节点越多网络的可靠性相对越高，但另一方面传统 PBFT 中节点通信的复杂度 O(N^2)随网络容量指数级增长，极大的限制了节点的数目。BBFT 中对消息的有效聚合可以有效的减少消息发送的次数，从而保证 O(N)的复杂度要求。与网络拓扑相结合，可以把网络分割为多层结构，消息数据可以在同层内有效共享，以多签聚合的形式跨层传播。对多签信息的验证可以使用现有的成熟的方案，比如像基于 Shnorr 签名的 MuSig 算法可以保证多签验证的效率同时抵御 Rogue Key Attack 攻击。

（4）异构性（Heterogeneous）：

分离共识的验证和通信。共识的达成需要验证和通信，但两者并没有很强的关联。采取低耦合的共识框架可以进一步提高网络的可靠性和效率。验证模块往往取决于具体用户逻辑，对算力和安全性都有一定要求。通信模块和用户逻辑相对独立，主要处理网络连接和请求。网络拓扑和最短路径的计算和选择可以在这里完成。由于和用户逻辑无关，通信模块可以以抽象层（Abstraction Layer）或者中间件（Middleware）的形式和验证对接。异构带来的优势还体现在用最优的工具做最适合的事。验证和通信允许运行在不同的系统上，不同的操作环境中，针对不同硬件的算力优势和安全保证（Trust Zone)来发挥最大的效能。

共识过程示意（假设一个由 7 个节点组成的单层拓扑共识网络）：

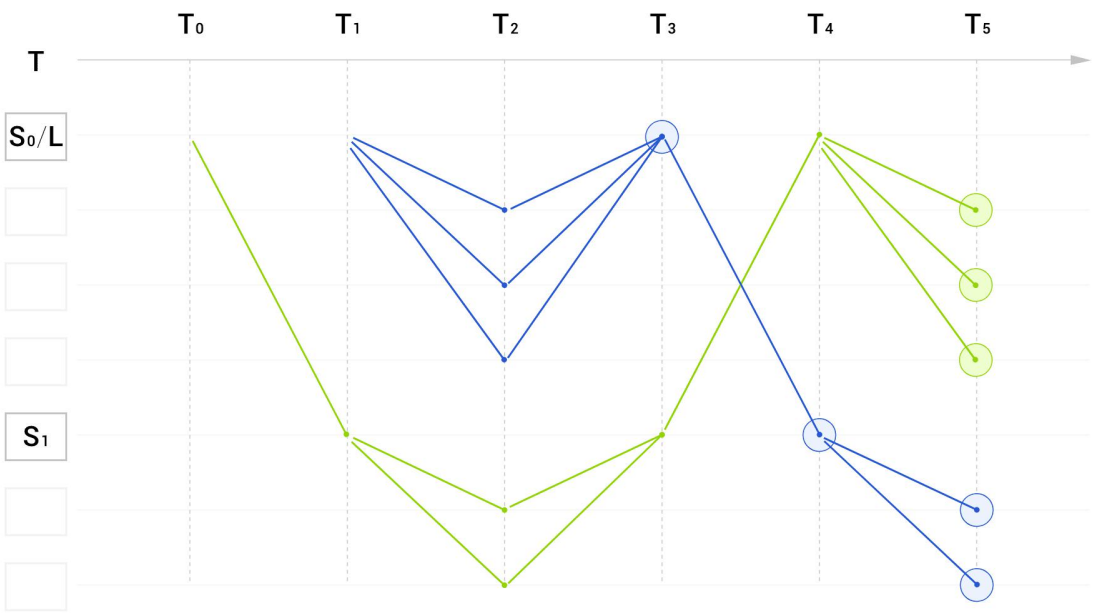

图 5

S0, S1：超级共识节点。选举可以采用网络拓扑延迟和资产抵押结合的方式，目的是在减少节点作恶的可能性的同时尽量减少网络的整体延时。作为普通节点和领导节点之间的中继，对信息做整合和转发。

L：领导节点。选举可以采用普通的轮询方式在超级节点中选出。

T0：L 发送交易和提案（签名）到 S0 和 S1

T1：S0 和 S1 转发交易和提案给同属共识节点

T2：共识节点验证交易并发送提案（签名）给 S0 和 S1

T3：S0 和 S1 对提案进行多签整合并相互发送多签提案

T4：S0 和 S1 发送多签提案给同属共识节点

在 T3，S0 已经获取超过 2/3 的节点提案，同样在 T4，S1 获取超过 2/3 的节点提案，其他节点在 T5 获取所有节点提案。

投票结果的真实性有签名保证，作恶节点只能更改自己的投票结果或者增加投票延时。

领导节点作恶：

领导节点只负责初始的提案发送，领导节点作恶会破坏共识的达成，但不会减缓共识的达成。

超级共识节点作恶：

超级共识节点由于承担了其所属的网络分片的出入口的角色，其作恶对分片的影响较大。以上例子中由于 S0 和 S1 分片划分不均匀，如果 S1 作恶，并不会影响共识的达成，而 S0 作恶则影响共识的达成。应该根据应用的具体场景，选择合理的网络分片划分。

普通共识节点作恶：

由于节点共识的达成只需要超过 2/3 节点的提案，某些节点作恶并不会对网络整体性能产生很大影响。

复杂度分析：

假设网络中总节点数为 N，超级共识节点的个数为 M，则信息传输总量为

$$S = M^2 + 3N - 2M$$

当 $M \le \sqrt{N}$ 且 $M \ge 1$ 时，$S \le 4N - 2\sqrt{N}$，通信复杂度为 O(N)。

特例：

1. 当 M = 1 时，BBFT = FBFT[⑥]
2. 当 M = N 时，BBFT = PBFT

扩展：

BBFT 对网络的有效划分和分层是解决可扩展性的关键。当网络中存在大量节点的情况下，可采用横向（节点和超级共识节点）及纵向（多层网络）的划分：

节点数和超级共识节点数：总节点数 N 和超级节点数 M 的关系决定了网络通信的整体复杂程度。对于任意 N，当 $1 \le M \le \sqrt{N}$，通信复杂度为 O(N)。当 M 过小时，超级节点作恶的影响会越来越大，而当 M 过大时，通信复杂度会上升。

网络层级：以上示例采用了 1 级分层（Single Hierarchy），在具体应用中也可以采用多级分层的方案（Multi Hierarchy）。

以上两种类型的划分可以相互组合。特别是当节点数多，网络环境复杂的情况下，网络可以被划分成由节点构成的森林（Forest），由超级共识节点和其他共识节点构成树的结构。共识网络是一个动态的系统，新节点可以加入，老节点可以退出，错误节点会下线。网络划分参数的自动调整对保持整个网络健康至关重要。BBFT 的网络模块会对网络状态定时监控，

⑥ Fast Byzantine Fault Tolerance https://harmony.one/whitepaper.pdf

对网络结构进行自适应来保证其高速运转。

3.2 经济层面

3.2.1 核心角色

侧链发起方：主导形成侧链的个人或组织。

中继节点：承担链接主链和侧链的角色，负责主链资产的锁定和释放，侧链资产的验证。

共识节点：共识节点是侧链上的全节点，主要承担侧链出块任务。

委托人：将持有的 Token 委托给共识节点的人。

3.2.2 规则

中继节点主要规则：

（1）竞选机制

由侧链发起方直接指定中继节点，中继节点可以是一个也可以是多个。

（2）奖励机制

中继节点收取主链和侧链间的转账费用，中继节点可自行设定收取转账费用的比率。

（3）退出机制

由侧链发起方更换中继节点，指定更换中继节点的替代者。

共识节点主要规则：

（1）竞选机制

竞选共识节点需抵押一定量 BTM⑦，才有资格参与共识节点竞选；

获得投票排名靠前的参选者才能成为创造区块的共识节点和备选的共识节点。

（2）奖励机制

总共识节点奖励，来源于每个出块中 Token 奖励，出块中的 Token 奖励部分奖励给出块节点，剩余部分根据节点所接收的委托投票来进行分配。

（3）惩罚机制

一旦中继节点出现下面几种异常行为将受到惩罚：

- 打包不合法的资产进入侧链；

⑦ Bytom 的原生 Token

- 长期不在线；
- 或其他恶意行为等。

共识节点出现异常行为将解除其共识节点身份。

（4）退出机制

共识节点提出退出申请或被解除共识身份，20 天后，共识节点抵押的 Token 返还。

委托人主要规则：

（1）投票方式

侧链提供委托人投票的操作功能，委托 Token 也称为绑定 Token 给共识节点。绑定后的 Token 不能交易。

（2）收益

作为委托人，收益来源于出块奖励，向共识节点委托 Token 的份额越多，获得的收益就越多。共识节点可设定出块奖励分配给委托人的比例。

（3）解绑和解绑期

委托人可以通过发送解绑交易来降低他们自己绑定的 Token。这些被解绑的 Token 不会立即成为流通的 Token。

执行解绑交易之后，在解绑期结束之前，相应的委托人不能再次在相同的验证人节点上发起解绑交易。解绑期为 20 天。一旦解绑期结束，被解绑的 Token 将自动成为流通的 Token。

（4）转让委托

委托人可以将其委托的 Token 从一个验证人转移到另一个验证人。分为两个步骤：从第一个共识节点上解绑和把解绑的 Token 绑定到另一个共识节点上。在解绑期结束之前，解绑操作不能立即完成。

3.2.3 节点收益来源

侧链发起方可以向侧链提供 BTM 激励共识节点，也可以提供基于比原链发行的其他资产作为激励。侧链发起方每年定期对外公布向侧链提供奖励的数量。每年具体激励的 Token 数量根据侧链生态的发展规模由侧链发起方确定。

4 Bystack 介绍

4.1 Bystack 概述

Bystack 是一个通用区块链应用堆栈平台，继承并实现了区块链三层架构， 分别由 Bytom 主链，Vapor 侧链， Blockcenter 中台，及 Bycoin，Byone，Bystore 等接入组件组成。下图是 Bystack 的基本架构图：

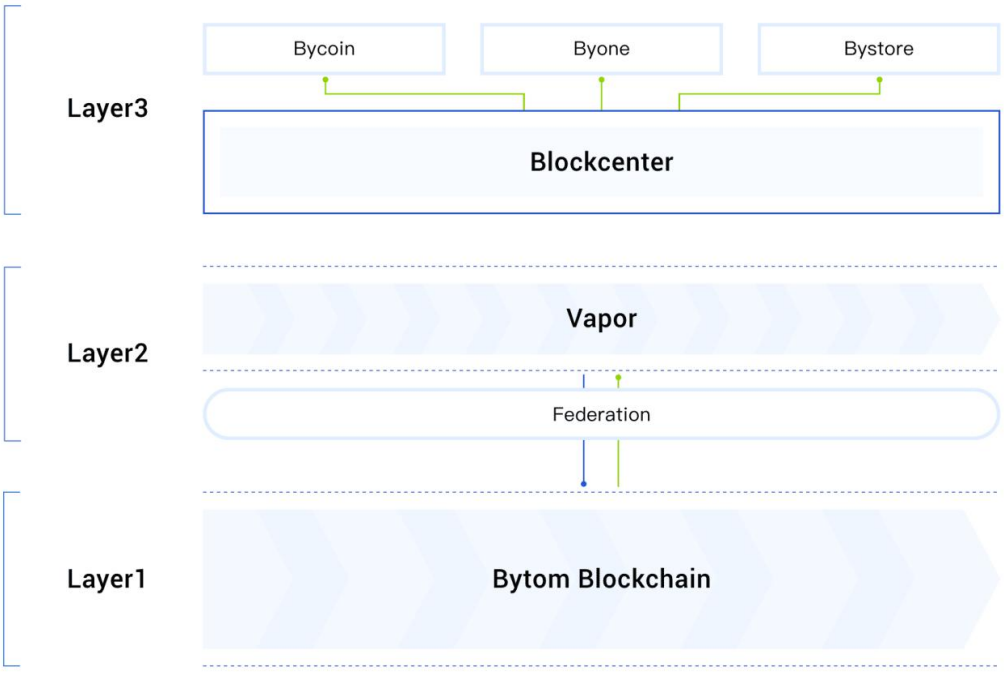

图 6

Bystack 依靠 Bytom 公有区块链技术平台和 Vapor 侧链技术，通过 Federation 作为主链与侧链之间的交互协议，为价值传输提供了通道，给上层应用奠定了坚实的基础。Blockcenter 作为业务中台，也是整个系统核心。他和上层服务如 Bycoin,Byone, Bystore 实现了区块链应用的第三层。

Blockcenter:在分层的基础上，Blockcenter 结合分层设计和模块化,把通用的业务拆分成不同的模块， 抽象了各类典型的区块链应用，提供了典型应用的基本能力和实现框架，用户可以根据自己的需求，像“搭积木”一样叠加自己的业务，轻松完成业务逻辑的区块链实现。对于底层，它提供了高度的业务抽象，让用户不必要了解底层的区块链技术原理，更加专注自己的业务开发。Blockcenter 是连接区块链技术和商业应用的桥梁，也是驱动的引擎。

Bycoin：移动客户端的生态入口和解决方案。它支持储蓄多种资产，资产与资产之间可以轻松兑换，并可以在集成了 Bycoin SDK 的其他系统中使用。Bycoin 不仅仅支持多种资产

存储，流通和互换功能，它也类似我们的微信，支付宝一样，还提供给我们很多日常需要的应用。比如：娱乐，日常消费等。

Byone:桌面客户端解决方案，我们只需要在电脑的浏览器端安装 Byone，注册登陆后，可以用它在桌面端管理我们的多种资产，同时在浏览器中打开支持 Byone 的应用，就可以连接到 Byone 的账户和资产，使用基于 Bystack 开发的 Dapp 和商业应用。

Bystore：它是支持比原链合约开发部署一整套完备且强大的开发框架，该框架支持多种语言编写智能合约，合约编写完成以后对合约进行预编译并调用合约交易接口直接发布合约。对开发者非常友好。Bystore 提供非常丰富的合约模板，只需要要在合约模板上修改合约参数，输入自己的账户参数就可以发布自己的合约应用。

4.2 Bystack 创新点

4.2.1 开放共识

Bystack 的侧链的共识是 DPoS+BBFT，但也可以使用其他的共识算法，Bystack 提供了非常丰富的可插拔共识机制，比如 DPoS，PoS 等等。同时侧链可以让任何人都可以加入成为共识节点，这和联盟链的准入机制有很大区别。

4.2.2 主侧链架构

独创的主侧链架构，主链负责发行和销毁资产，主链保证去中心化和安全性，侧链负责运行大规模商业应用，侧链牺牲部分去中心化来大幅度提升性能，同时可以存在无限多的侧链以满足不同的领域和性能需求。

4.2.3 BUTXO

基于比特币 UTXO 模型的创新，从底层模型上支持多资产的交易。BUTXO 保证了资产交互操作的原子性，异步交易的时候可以进行验证，支持多资产上链，智能合约结果布尔化。由于 BUTXO 的无状态，所以在一定程度上增强了用户的匿名性。

4.2.4 最短路径交易

签名不在交易而在每一个输入上，可以在不同时间，不同人之间自主的构建交易，从而

构造出不同模式的交易类型，比如磁力交易。

4.2.5 定制化可插拔服务

比原链的 Blockcenter 可以提供非常丰富的可插拔服务，商家可以根据不同的业务场景，来集成不同的服务，比如身份服务，多重签名，隐私交易。

4.2.6 国密标准

Bystack 可采用国密标准 SM2，SM3，SM4 密码学算法，满足金融行业，公共事业等行业在用户地址的生成，交易签署以及交易验证等过程中对国家标准的合规和安全性要求。

4.2.7 多语言合约虚拟机

支持 Equity，Javascript，Python，Go 等多种语言的合约虚拟机，可以满足熟悉不同语言的开发者开发商业 Dapp 的需求。

4.3 优势

4.3.1 领域支持

区块链可以服务于金融行业以及供应链，还有垂直领域的行业生态。但是一般的公链或者联盟链无法服务于每个行业，但是 Bystack 通过多条侧链能做到更全面的技术支持。每个侧链根据不同行业的特性进行定制化的组装和开发，满足不同行业和领域的业务需求。

4.3.2 扩容

目前主要有两种扩容方案，分别式 Layer1 扩容和 Layer2 扩容，Layer1 扩容主要改进区块链自身，把区块链自身变的更快、容量变的更大，Bystack 通过压缩交易和增加出块速度，从而在 Layer1 层得到扩展。Layer2 扩容是把很多的复杂业务过程迁移到链下，而 Bystack 构建在侧链基础上的 Blockcenter 正是在 Layer2 的扩展。

4.3.3 性能

性能方面主要从下个角度分析：

出块时间：Bystack 的主网是依托的比原链（Bytom),平均每 2.5 分钟产生一个区块。侧链采用 DPoS+BBFT，出块速度大概在 0.5 秒。

区块大小：侧链压缩交易来压缩区块大小，从而减少带宽开支，让全节点可以更快的同步区块。

TPS：侧链的 TPS 能达到数万，且通过横向扩展吞吐可达百万以上。完全可以满足目前企业级服务平台的基本应用。

容错率：主链的 PoW 基于概率的系列算法理论上允许少于一半的不合作节点，而侧链的 BBFT 共识算法确定性算法理论上则允许不超过 1/3 的不合作节点。

4.3.4 安全

主链共识算法：单一 DPoS 或 PBFT 都不是真正意义上的非准许（Permissionless）共识，需要许可则意味着该网络是被一小部分人控制，数据不可篡改、交易不可逆转等区块链根本属性不复存在，基于区块链的资产确权、数据存证等业务的安全性亦将无可保障。Bystack Layer1 采用创新 PoW 算法 Tensority，在挖矿激励机制作用下，全网算力不断增长， 发起 51%攻击成本不断提升，尤其是 Tensority 采用对人工智能芯片友好型算法，使得挖矿芯片可能采用人工智能通用芯片挖矿，从而降低了硬件成本，并为人工智能芯片产业赋能。

侧链共识算法：Bystack Layer 2 采用 DPoS+BBFT 共识算法，提供高可用的拜占庭容错能力，支持共识状态自动恢复，区块数据互备恢复，数据存储自动均衡，节点服务自动路由。从而保证系统的自身的安全和稳定。

基于 BUTXO 模型的合约安全性：主链采用 BUTXO 模型，每一个 BUTXO 都由单独的合约程序锁定，破解合约只能获取该合约锁定的资产，其他资产不受影响，从而很好的保护主链资产的安全性。

主侧隔离：支持简单支付验证 SPV（Simple Payment Verificaiton），侧链能够验证主链块上 Header、Merkle Tree 的信息。主链负责账本的更新维护和数据安全，资产发行、数据存证、数字身份等关键业务在主链上完成，不同侧链针对股权、版权、积分等不同资产交易场景，负责交易效率。主链不需要关心侧链的运行状态。当侧链被攻击，主链的安全性不受影响。

侧侧隔离：不同的业务隔离，每个行业领域分属于不同的侧链，如果一条侧链受到攻击或者影响不影响其他侧链业务的安全稳定运行。

Federation 安全性：通过侧链跃迁到主链（Pegout），收集人，验证人等角色确保资产转移过程切分成多个流程，防止单一验证人的作恶。

4.3.5 隐私保护

Bystack 采用多种加密算法组合的方案来提供全方位的隐私保护。高可配置性保证了方案的灵活度并能适应不同的用户场景。

隐私交易：对于多签交易，使用 Schnorr 签名和 MuSig 算法来对多个签名进行集中验证。对交易金额的加密可以采用零知识证明（Zero Knowledge Proof, ZKP）的方案，比如 zk-SNAKRS 和 Bulletproofs。在私密要求较高的场景，可以使用 MimbleWimble 模式对交易双方地址和交易金额同时进行加密。目前主流的加密算法都基于 Pedersen 承诺系统（Commitment Scheme）。它虽然能绝对隐藏交易内容（Perfect Hiding）但只在计算力有限的情况下提供绑（Computational Binding），这意味着交易金额有可能被改动。为了应对未来算力的突破，绝对绑定（Perfect Binding）的系统，例如 ElGamal 加密，可以以开关激活的模式被采用。

隐私合约：以上的隐私交易方案也可以应用于隐私合约中。除此之外，使用默克尔语法抽象树（Merkelized Abstract Syntax Tree，MAST）对合约本身进行优化，在减少体积的情况下提供一定程度的隐私保护。

4.3.6 支持 Bancor 协议

Bancor 是一个去中心化的流动性网络，为用户提供简单、低成本的买卖 Token 的方式。Bancor 的开源协议通过智能合约直接授权具有内置可转换性的 token，允许集成的 token 立即相互转换，无需在交易中匹配买卖双方。Bancor 钱包可以直接在钱包内实现 token 的自动转换，价格比交易所更容易预测，并且不会受到操纵。Bystack 的 bancor 协议可以让多种资产(比如商业积分，多种数字资产)可以快速，低成本，高效的转换。

5 Blockcenter 介绍

5.1 Blockcenter 整体架构

Blockcenter 作为整个区块链企业级服务平台核心系统，一方面扩展底层的主侧链的能力，另一方面抽象底层的区块链技术，提供典型的应用开发框架，同时也提供维护，监控和

升级的必要能力。

整个 Blockcenter 的主要功能结构图如下：

图 7

从上面的中台(Blockcenter)我们可以看出整个中台分为核心业务层，适配层和业务监控。这些都属于系统层面的业务模块，这些业务模块的详细介绍如下：

身份认证：负责业务上层的用户身份鉴别和认证，提供用户的身份注册和登陆服务，如果需要更加严格的身份认证服务，可以使用第三方集成连接到权威认证机构。

账户管理：管理用户身份信息，维护用户身份和区块链身份的对应关系。

权限管理：设置用户身份的权限，扩大或缩小该用户的操作权限。

信用评价：传统互联网的信用评价是基于信用累加模型，而不记录交易的时间戳，这带来恶意刷好评或差评的风险。Bystack 利用每一笔链上交易都销毁币天（Coindays）这一特性，将币天销毁引入信用评价，以币天和交易金额作为评价因子，使得刷信用机制不再成立。

$$\mathrm{R_n} = \sum_{i=1}^{i=n} R_i * W_i$$
$$\mathrm{W_i} = C_i * D_i$$
$$R_i \in \{-1,0,1\}, i, W_i, C_i, D \in (0,+\infty)$$

R_n 代表用户的信用值得分，R_i 为第 i 次交易时间用户所得的信用值，W_i 为第 i 次交易

时间的币天销毁，C_i 为第 i 次交易时的金额，D_i 为第 i 次交易距离上一次交易所积累的时间。

支付管理：提供用户的支付信息，并根据这些信息做进一步的统计和风控预警动作。

充值提现：提供数字货币充值和提现服务，商家可以非常简单的接入，无需开发。

交易计费：提供预支付功能，根据商家的扣费逻辑自动进行计费。

资产管理：提供主侧链不同资产的后台管理功能。

订单管理：管理用户发起的订单，并可跟踪不同的订单。

活动运营：自定义应用内活动，设置交易手续费减免或其他优惠活动。

业务监控：负责商家应用运行过程中整个业务监控，包括对用户，资金，行为等等监控并进行预警和风险控制。

适配层：适配层完成区块链底层的抽象工作，底层的技术都在这里面封装成业务接口，隐藏底层技术复杂性，同时通过配置平台进行相关参数配置，通过统计监控对链上数据进行监控。

基于 Blockcenter 的模块化设计目标是实现“可插拔”模块应用， 核心业务模块，适配模块和业务监控模块都最大限度对外开放 API 服务， 用户可自由搭配选择符合自身业务需求的最佳可行方案， 例如在去中心化交易场景下，仅仅选择资产管理，交易计费和交易管理，侧链管理这些模块就可满足需求， 实现真正系统级的商业解决方案。

5.2 区块链适配器——打通应用和区块链技术

在适配层中的区块链适配器是抽象底层技术，隐藏底层技术复杂性的核心模块，通过适配器接口，上层的应用可以方便地使用底层区块链的技术功能，同时我们也提供更加复杂的配置接口，满足用户个性化定制化的需求。

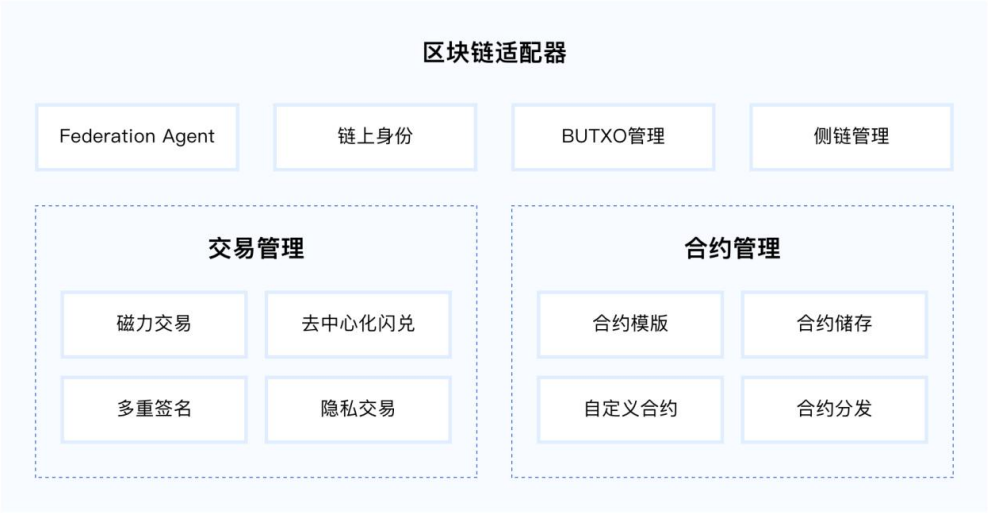

图 8

Federation Agent：主侧链通信的业务中介， 掌握侧链跃迁主链（Pegout）， 主链楔入侧链（Pegin）业务层面的管理能力，将跨链交易从区块链层转换为上层业务交易。

链上身份：主要服务于去中心化身份系统， 解析区块链中的身份存储信息，将内容传递到核心业务层鉴权。

BUTXO 管理：每个用户的 BUTXO 存储和识别， 并选择合适算法在创建交易和使用 DAPP 时确定正确的 BUTXO。

侧链管理：管理使用的或者创建的侧链。

交易管理：主侧链资产与资产交易模式的管理，支持多种类型的交易。

合约管理： 有 Equity 或 WASM 等语言实现的模块选择使用，并提供链上或链外存储，还可以自定义合约内容，可分发到侧链或主链上。

5.3 开发工具

Blockcenter 提供了完整的开发工具和规范,结合 Bycoin SDK 可以提供移动端解决方案，结合 Byone 接口可以提供桌面端的解决方案，以及 Dapp 开放平台 Bystore，同时我们支持多语言的 SDK,可以非常方便的进行使用 Blockcenter 的各项功能。

6 应用领域

6.1 积分兑换

消费者在消费过程中会遇到各个银行、商家、机构等不同的积分系统。这些积分系统由于在各个组织内封闭，不能通用，造成了积分消费困难、利用率低。此外，积分数据有被篡改风险，无法保证信息安全。各机构积分系统复杂，无法准确制定平衡的兑换比例。

基于区块链技术可以在各个企业之间建立一种不可篡改的信任登记机制，为不同积分的打通互换提供了可能，从而能够盘活积分，促使各家消费服务手段的升级，共同打造互信共赢的协同商圈。通过区块链搭建各个商家参与的积分联盟链，用户将联盟中不同商户内的自有积分，在区块链通用积分交易平台兑换成通用积分，即可用通用积分在联盟内任意商户进行消费结算。用户在系统内以账户地址形式存在，不同商户间无法获取用户信息。数据存于区块链中不可篡改，积分操作记录存于本地可被溯源，避免用户积分数据造假。商户自有体系内的积分可以通过兑换成通用积分流通起来，提升用户获取积分积极性。

基于 Bystack 的主侧链架构，可以很方便的主链上发行商家自己的积分，再定义一个和通兑积分的通兑比例，打通和用户之间的积分系统， 让商家之间的积分能够真正的流通。

6.2 版权确权

版权的保护不仅是对原创作者的尊重和权利的保护，更是社会进步的一种象征。在政府部门积极推动版权保护、诸多企业对区块链+版权应用项目进行落地尝试、人们版权意识不断提高。

目前技术可实现记录版权，可作为被侵权后维权的取证渠道，但是技术上与完全保护版权尚有距离，目前并未观察到完善的解决方案。认证平台互通：在单一系统中，可方便地进行版权维护和追溯。但是如果 A 用户把 B 用户的内容放在其他平台，则容易造成纠纷。因此需加强各个区块链版权平台间统一认证、标记、识别的方式，或提供唯一的认证平台，以提高维权效率。非标化的版权认证还待发展：对于一些非标化的物品，比如算法、数据等的版权的认证，目前也许可以通过零知识证明等加密方法来保证其可以很好的被交易，但是其前提条件是保证规则的标准化，这还需要一段时间去实现。区块链可以促进优质内容产出：通过区块链去中心化的思想，取消第三方平台的版权垄断，让版权真正属于内容生产者，从而内容生产者会有更多的收益和实现价值的可能，可以促进内容生产者生产内容的动力。方

便司法举证，减少版权纠纷：基于区块链上的版权平台，无论是作者作品的提交，还是后续的交易，以及用户的购买，均有相应的时间戳证明，并在链上开放透明。对于出现版权纠纷的情况，司法部门只需要根据版权的数字身份 ID 进行追溯，轻松调取作品版权的历史交易信息，举证变得简单。

使用 Bystack 作为版权的确权平台，作者的版权可以轻松上链，同时使用去中心化和防篡改的特性，真正让版权保护没有争议。

6.3 产品溯源

假冒伪劣问题一直以来都是各行业亟待解决的痛点，高频率、大范围的商品造假使得公众对于商品溯源的诉求日益提高。如何能对商品的生产与运输信息实现有效追溯成为了行业研究重点。

利用Bystack 技术，通过其独特的不可篡改的主侧链特性与物联网等技术相结合，对商品实现从源头的信息采集记录、原料来源追溯、生产过程、加工环节、仓储信息、检验批次、物流周转，到第三方质检、海关出入境、防伪鉴证的全程可追溯。

6.4 供应链金融

中小微企业的资金不断受到上下游企业的挤压。虽然它们是国家重点扶持的对象，但是传统金融融资方式不适合它们的发展路线。为了跟上它们的发展，供应链金融将为中小微企业的发展注入新的活力。

基于 Bystack 技术保证让借贷的交易信息和相关文件具有公开、透明、可查询、不可篡改的特点。实现跨供应链层级的金融合作。所有的参与方都可以通过分布式账本对整个供应链的流程有清晰的认识，供应链金融的每一个参与方都是点对点网络中的一员。网络不存在单点故障，整个网络高可用。Bystack 上的交易速度和成本都远远优于传统银行。各方可以减少人力成本和操作风险。依托项目的现金流，降低系统性风险。

6.5 数字政务

从市场规模来看，2017 年我国数字政务市场规模达 2722 亿元，2018 年有望突破 3000 亿元。但处于转型期的数字政务面临着数据孤岛、成本高昂、网络安全、效率低下、监管缺失等痛点。

区块链可为数字政务提供新的解决方案。目前我国共有 17 项区块链数字政务应用，分别涉及七大细分场景：政府审计、数字身份、数据共享、涉公监管、电子票据、电子存证、出口监管等。

通过 Bystack 的技术，将政府机构、金融机构、监管机构、其他中介机构放置到区块链生态中，通过智能合约和接口的多级权限管理，实现一定范围内的政务处理与数据共享。

Bystack 可以帮助建立一个牢靠、透明的平台，允许政府部门对访问方、访问数据通过智能合约授权，安全地处理敏感信息。保障数据安全，可溯源性保障溯源

6.6 去中心化交易

中心化交易存在着一些缺陷。最令人担忧的就是安全问题了，为了满足性能要求，当前的平台一般将交易放在链下，交易撮合的数据都存储在中心化的数据库中，意味着他们是作为第三方中介来为客户操作，而交易也并不记录在区块链里，易于被黑客攻击，导致大规模的安全漏洞，以及信息、资金和私钥的不安全。对于硬分叉这样的特殊区块链变化事件应乏力，而在运营的同时还伴随有高政策性风险。

从业务视角来看，去中心化交易模式简单，它只需要承担主要的资产托管、撮合交易及资产清算。而不需要承担像中心化交易所需要承担的非交易的功能像账户体系、KYC（Know Your Customer）、法币兑换等。用户在区块链上的账户公钥就是身份，无需注册个人信息，因此就不存在个人信息安全问题也不需要 KYC。

基于 Bystack 的主侧链模式，主链进行资产登记，利用侧链来满足高 TPS 的去中心和交易撮合需求，是非常好的一种应用场景。

6.7 分布式身份系统

从历史上看，我们在日常交往中需要的身份证件——护照、驾照、社保卡等，都是由民族国家和私营机构等中央机构颁发的。使用这种标识带来许多问题:（1）如果国家吊销个人凭证，个人可能会失去身份；（2）身份受到国家或地域的限制，某一民族国家颁发的身份，通常不被其他国家接受；（3）集中控制仅在一个司法管辖区或一个在线服务中。即使是上文所介绍的 PKI 体系，用户的身份也是掌握在中心化机构手中，用户对于个人的身份数据并没有控制权。我们也常常可以看到用户身份数据被泄露的事件发生，例如，2018 年 Facebook 爆发数据泄露丑闻，掌控在 Facebook 手中的将近五千万的用户数据隐私被泄露；

同样是在 2018 年，华住集团爆发了国内迄今为止规模最大的酒店信息泄露事件，约 5 亿条公民个人信息在暗网上被拍卖。这些大规模的数据泄露事件，对用户的隐私安全造成极大的威胁。

随着区块链技术的出现，新的身份管理模式也随之出现。基于区块链技术的去中心化的身份管理方法具有分布式数据存储、点对点传输、加密安全、共识确认等特征，可以有效解决身份验证和操作授权问题。区块链身份管理为数字身份提供安全且去中心化的解决方案，从而实现分布式信任模型。区块链技术通过在去中心化网络上提供自我主权身份来改变现有身份管理系统，因为共享多个 ID 可能导致安全问题和数据泄露。由于区块链实现了去中心化，因此它消除了任何交互和沟通之间的中介。区块链技术通过解决身份盗窃，重复 KYC（Know Your Customer）和缺乏对个人数据的控制等问题，有助于改善现有的身份管理。

6.8 物联网+5G

5G 将服务万物互联并改变我们对家庭，企业和交通工具连接的看法。在 5G 世界中有许多场景即将成为现实，如增强现实，虚拟现实，人工智能等基础技术构建的应用程序将受益于海量数据管道和超低延迟。智能汽车和无人机将通过低延迟网络相互通信并协调周围的事物，从而作为连接工业和消费者的新通道。 5G 将使我们更接近实现数百万接入网络的传感器设备的真实物联网世界。当然可以预知，传统中心化服务架构难以承载设备指数级增长后管理压力，而区块链会是一个解决方案。

Bystack 主链采用的 Tensority 共识算法天然适合部署于含有 AI 组件的物联网设备中，将机器通过区块链连接起来，形成去中心化的物联网系统。 通过区块链的智能合约可使机器和机器之间直接通信，极大提升了管理效率。同时，5G 技术落地后带来数据传输能力的提升，使得区块链通信延迟大大降低，通信吞吐大大提高，从根本上创造了区块链工业化运行的理想环境。

6.9 公司股权管理及交易

尽管中国股权投资行业正处于蓬勃发展期，每年投资规模已经超过 1.5 万亿人民币，但缺乏流动性、退出困难已经成为股权持有者最大的痛点。由于上市概率低、时间长，传统 IPO、并购的退出方式已经完全无法满足股权持有者对于流动性的需求。无论是公司创始人，还是投资人，或是员工期权持有者，都十分渴望在公司上市之前有机会能将所持股份变现流

通。

导致这一难题出现的主要原因是缺乏交易机制与手段，以及信息的不透明而带来的交易不可信。

区块链技术将这些难题迎刃而解。区块链去中心化、不可篡改的特性，将解决股权权属的登记及管理中因中心化和可篡改特性所导致的不透明、不可信问题；智能合约是解决传统股权发放、授予、登记过程中低效、高成本问题的不二法宝；而基于 Bystack 的合约转让应用，则将为这些登记在区块链上的股权提供快捷、高效、透明的流通交易方式。

6.10 区块链游戏

游戏是区块链上最早的应用类型，早在 2012 年就有一些基于比特币区块链的游戏，借助比特币和区块链的内在特性完成简单的对赌功能，实际上已经蕴含着非常深刻的去中心化理念。近些年来，许多结合区块链的游戏雨后春笋般出现，前有纯基于区块链以太坊的加密猫（CryptoKitties），后有基于腾讯区块链的《一起来捉妖》，都引起了较大的反响。Bystack 在游戏领域有着体系化的考量，主要从游戏的高并发低成本支撑、资产类型（如夸克资产）的交互、分布式与中心化的融合三个方面为区块链+游戏做系统准备。

（1）高并发低成本支撑。Bystack 侧链单并发超过 1 万（TPS），横向拓展后可达百万，为高并发的区块链游戏实现提供了充分准备，并且基于 Bystack 侧链的交易成本较低，便于开发者进行开发。

（2）多资产类型交互。除了满足基于区块链上发行游戏资产的基本需求，Bystack 根据资产的物理及权益属性，将资产分为比特、原子、夸克、量子四大类，这些资产可以非常贴切的适应游戏中种类繁多的道具及积分，各类资产可积木式组合满足游戏需要。比如游戏中的关键性稀缺性道具可以用夸克类资产承载，这一类资产在链上即是不可分割、唯一且不可替代；游戏中的通用金币等可以用比特类资产承载，这一类资产具备良好的分割和互换属性。

（3）分布式与中心化的融合。区块链游戏天然具备较高的信任度，Bystack 通过开源的合约建立游戏过程的透明度和信息的对称，同时 Bystack 主侧链之间有着中继的“网关”角色，游戏的开发者和监管者可以起到一定的审核作用，保障区块链游戏可以在内部小闭环和外部大生态之间自如切换，做到分布式与中心化的有机融合。

7 实际案例

7.1 积分宝

积分宝是以 Bystack 作为底层架构，针对企业积分打造的集营销、宣发、通兑、社交、用户运营为一体的区块链综合服务平台。

7.1.1 背景

积分作为企业为维系客户，通过设置合理的条件给予达成的用户一定的奖励，积分累积到一定额度时，可以换取一些奖品或者抵扣商户的消费金额。积分消费已成为各大银行、电商、商超、购物商城留住客户、激发客户的通用商业模式。但封闭的消费形式导致积分成为用户和平台的双重鸡肋，现实中大多数用户的积分，不是过期作废，就是沉淀在用户平台上永久搁置。

在积分概念比较深化的行业，如航空、酒店等，商业巨头之间通过达成产业联盟为用户实现积分互通，权益流转的一系列服务。但对于一些体量不大的企业，以及积分运营能力较弱的企业，即使自身拥有足够基数的用户量，却也难以针对积分做细化的运营与商业扩展。一方面自身没有足够的资本和明确的盈利模式来吸引外部合作方加入积分生态，另一方面没有多余的人力和财力针对积分进行精准运营。而考虑由第三方建立平台托管的方式，第三方的主体归属、行业资质、服务费用、企业隐私安全等一系列问题，又很难以独立的企业主体去承载。

7.1.2 功能概述

基于此，形成了以 Bytom 主链+Vapor 侧链为底层架构的技术方案来建立一个区块链积分综合平台。该平台主要定位包括以下几点：

（1）为用户创建 Bystack 上身份体系，积分作为比原资产其所属权在于用户，颠覆传统互联网模式下中心化登记用户积分的管理模式；

（2）针对积分通兑实现 C2C 市场兑换以及算法兑换，针对比原 BUTXO 模型技术特点实现多笔通兑请求合并为一的磁力交易；

（3）针对不同企业发行的积分资产，有相应的 DAPP 配置页，企业自身或社区开发者可以根据资产特征结合业务内容开发独立的 DAPP 以供用户使用，用户可以根据积分类型

和应用类型快速定位到自己想用的 DAPP；

（4）建立用户社交系统，拓展积分覆盖面积，深化积分社交属性；

（5）打造企业后台管理面板，企业可以通过后台面板对发行的积分资产进行增发、销毁、监控等操作，并可以收集用户积分的消费情况、流转情况、兑换情况，根据用户行为建立用户画像，并通过糖果分发等功能进行精细化运营，从而增强用户黏性、发展外部用户转化。

（6） 向用户提供侧链资产与主链资产互转的功能模块。

7.1.3 技术实现

积分宝作为一个平台级应用，考虑其业务内容涉及高频交易以及资产增发的场景，将 Bystack 侧链 Vapor 作为后端底层。

积分资产将由发行方通过在 BYTOM 主网以企业认证的账户发行比原资产，并锁定至积分宝所在的侧链上，在根据用户属性向用户地址进行量化分发。

注册用户将在 Vapor 上建立自己的账户体系，并通过积分宝执行积分的转移、消费等操作。

通兑平台将通过构建智能合约的方式去中心化执行。

企业方通过后台管理系统便捷部署和运营自己的积分，根据要求从原本维护积分体系的服务器接入 API 即可使用，无需对原有积分体系进行彻底改造。

企业开发团队或个人开发者可以根据需求通过比原 SDK 自主开发响应积分资产的 DAPP，并上传到积分宝 DAPP 市场。

7.2 区块链合同

7.2.1 项目简介

区块链合同是一款以区块链为底层技术支撑的企业级合同、票据综合管理平台。我们试图改变传统互联网模式下服务商主导用户的现状，通过区块链技术来实现信用的传递、保障业务的安全。依靠区块链的技术特性，通过智能合约赋能，实现合同制定、执行、管理的智能化。同时基于区块链安全、透明、不可篡改的特征，为用户的资产安全以及相应的合法权力提供强有力的保护。

7.2.2 项目架构

区块链合同采用三层结构：

图 9

服务层：高性能云主机支持文件的存储与交互；

上链层：基于完备的 SDK 与区块链相交互，将用户操作和文件加密信息同步上链;

应用层：区块链合同在应用层实现了 PC、WEB、移动设备全平台支持，用户可以在应用　　内实现用户信息管理、合同签署、文件管理、链上信息查看等操作。此外对于企业级用户同样提供 API 方式接入提供完整服务，功能部署快捷高效。

7.2.3 项目的创新和优势

（1）公私钥体系的私有化部署

不同于传统互联网服务由运营商完全掌握用户的信息，区块链合同在用户注册阶段将会根据用户信息与随机数匹配，在离线状态下生成符合区块链账户体系的公私钥，用户通过密码来管理和使用自己的公私钥对。

图 10

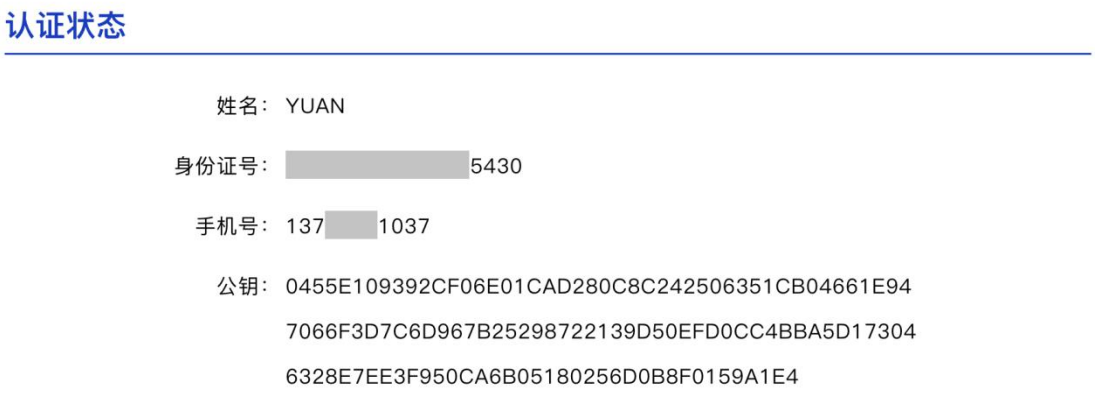

图 11

（2）CA 认证化的区块链身份

传统金融服务通常是为了生成 CA 证书而实时部署一个公私钥对来请求认证，而区块链合同是先为用户创建一个区块链账户，然后通过集成 API 对用户的区块链上的公钥进行认证，从而使用户在区块链上的行为同样具备 CA 认证过后的法律效力。

（3）基于私钥离线签署合同

我们在传统电子签章的流程之上，自主研发出一种基于区块链私钥通过区块链脚本语言特性与智能合约相结合的签名方式，用户签署过程中只需要输入一次私钥管理密码，就可以实现本地私钥签名，并实时在区块链上形成记录。

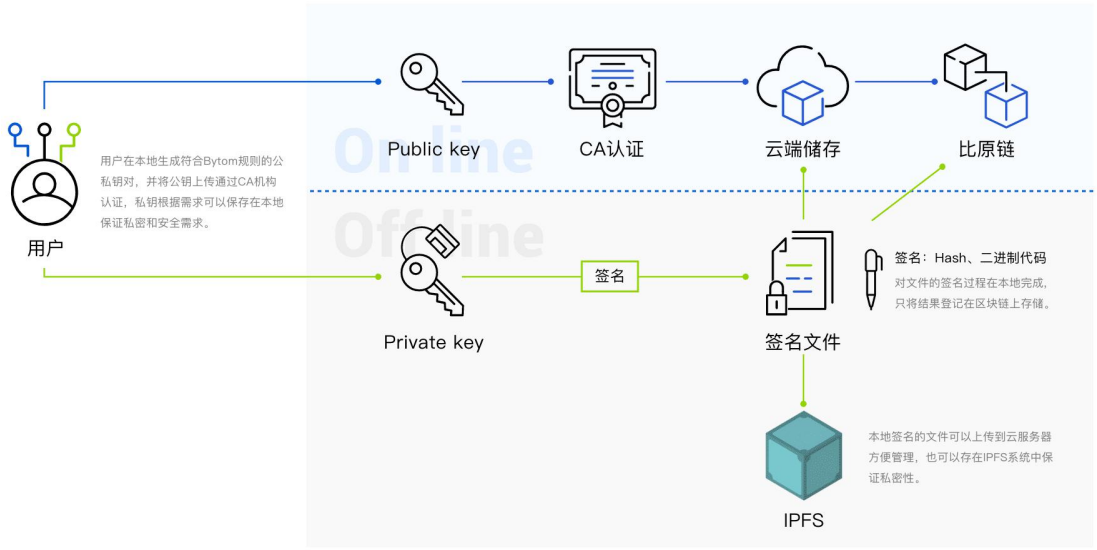

图 12

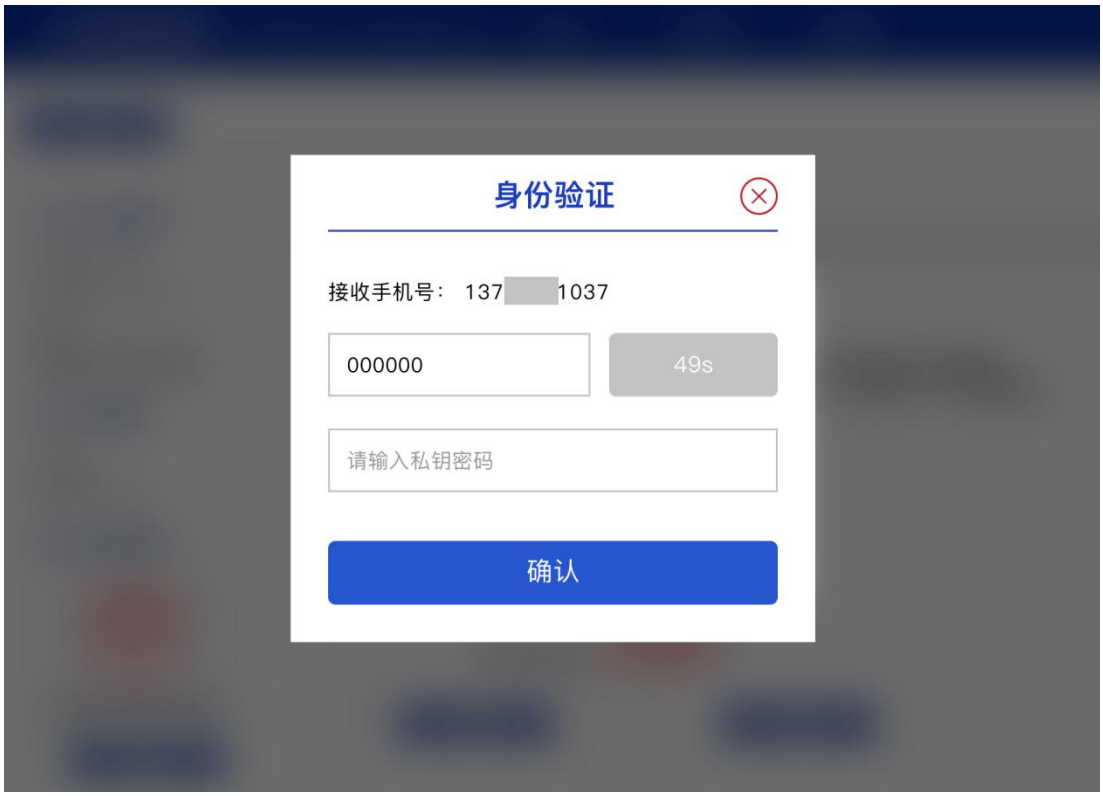

图 13

（4）绝密文件存储

传统互联网服务用户签署合同的信息是存储在运营商的服务器上的，因此我们为用户提供一个文件存储的可选项，对于一些涉及到款项、核心条例、机密信息的文件，可以通过重加密的模式加密上传到 IPFS 网络上。既能为用户提供随时浏览、管理、编辑文件的便利，

同时又保证了文件内容只对用户和授权方可见。

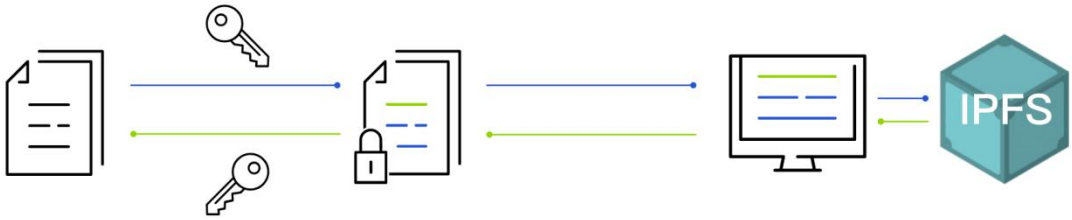

图 14

（5）合同的智能合约化

基于 Bystack 专注于资产的技术特征，区块链合同为用户提供了部分智能合约的在线模板，对于涉及金融类的合同，可以以智能合约的方式承载合同本身，从而实现合同的可编程化。进而实现合同的智能化编写、智能执行、智能取证等一系列服务。

图 15

7.3 数字政务云链

7.3.1 项目背景

Bystack 用于市民身份验证系统的区块链改造工程。主要负责全市政务数据和公共数据平台建设和管理，其中包括组织实施城市“数据大脑”政务系统建设等重大项目。数据资源管理局方面决定从“市民身份验证系统”作为区块链技术方案试点。比原团队将作为指定技术提供方，为该政务模块的制定区块链技术方案并实现完整开发。

7.3.2 项目概述

“市民身份验证系统”的功能主要是通过线上终端以及线上服务平台，将采集的市民信息与公安部留存档案进行比对，并根据返回的结果出具验证证书。

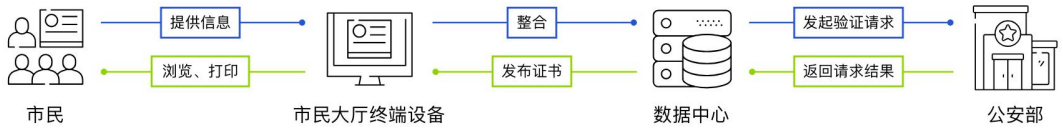

图 16

在该系统的基本架构下，下一步将以比原链侧链搭建底层服务，公安部反馈的结果将通过接口实时地形成链上数据记录，并配有相应地查询界面，可以根据流水号定位到链上信息的存储状态。

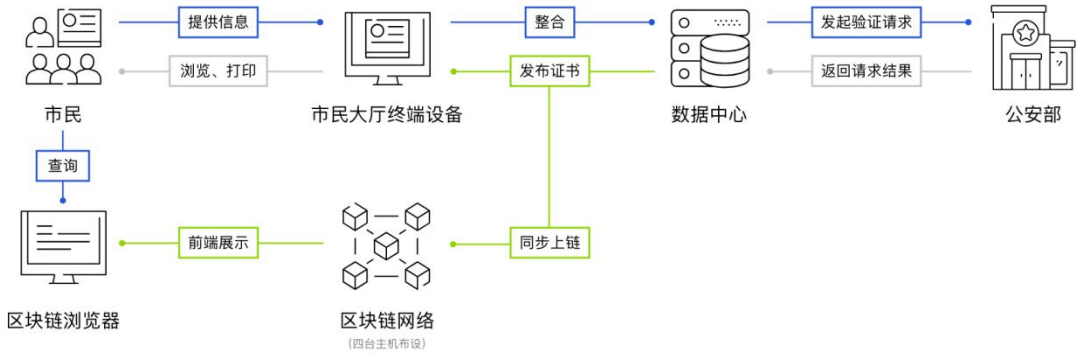

图 17

7.3.3 技术实现

该项目将以 Vapor 侧链为技术底层，第一阶段核心业务实现主要是信息上链。目前数据资源管理局数据中心和公安部数据库将作为该区块链网络的节点维护出块和执行数据上链。数据上链之前将根据业务需求进行格式化和加密处理。整体区块链服务的参数是可配置化的，共识机制初步将使用 DPoS，出块时间将根据实际业务吞吐量做调整。

在未来该系统将会根据不同政务部门之间工作的协同要求，对节点配置、共识机制等进行迭代维护，从而使市民身份信息数据能跨部门、跨市属的形成共识，降低公共服务的维护成本，提高效率。

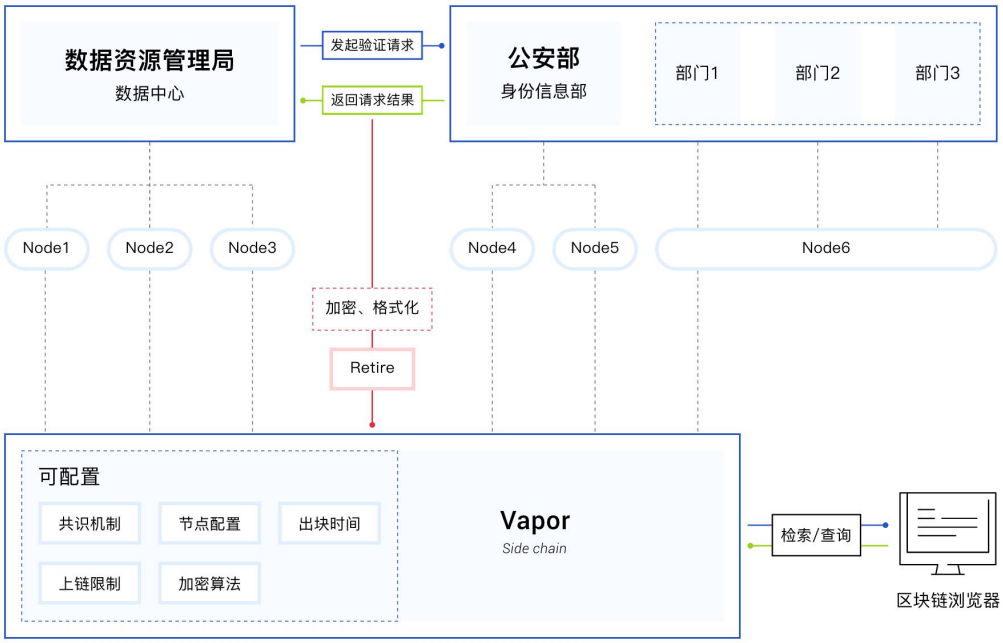

图 18

7.3.4 项目意义

（1）市民在申请身份证明证书之后在链上同步生成查询记录，可以通过流水号来实时查询自己的身份信息状态；

（2）不同政务部门之间依靠节点设置共同维护政务系统数据协同的监控，并以链上数据作为工作流程的证明和记录；

（3）本身系统具有高度可扩展性，针对公民身份信息系统以及其他设计多部门协同的政务系统，可以做到便捷扩展。这也为跨部门、跨市属、跨省属协同政务办公提供了一种可行的解决方案；

比原链及侧链应用在某省会城市政府政务系统当中，也说明比原链本身从底层协议和数据安全性方面，已经达到了市政府政务系统的要求，未来将会依托比原链及其侧链的技术底层，开展政务领域专项的区块链服务。