VTChain 技术白皮书
V3.0

商业级区块链应用底层操作系统

VTChain 项目组

目 录

版 本 声 明

VTChain 项目文档提供给所有关注 VTChain 的用户、机构阅读，在项目发展过程中，我们可能会不定时更新文档版本。请关注 VTChain 官网(http://www.vtchain.org)及微信公众号，以最新版为准。

本技术白皮书明确 VTChain 研发方向和技术方案，将用于指导 VTChain 的技术研发。

VTChain 团队感谢您的关注和支持！

一　区块链现状的理解

1.1 区块链行业分析

2017 年是区块链行业爆发的元年，各种区块链项目层出不穷，区块链逐渐走向实体生产生活的方方面面。从行业分析看，每一个区块链项目都有其独特性和创造性的一面，尽管场面泥沙俱下，终归有难掩珠光宝气的优质项目。

区块链技术日益发展、繁荣，使其进入了全球开发者和机构的视野，越来越多的人们开始关注区块链如何应用于商业企业产品、帮助人们实际解决现有中心化系统所面临的日益增长的成本和日渐明显的安全性问题。从最初的比特币、以太坊等公有链项目开源社区，到各种类型的区块链创业公司、风险投资基金、金融机构、IT 企业及监管机构，区块链的发展生态也在逐渐得到发展与丰富。

我们相信，区块链技术的繁荣发展必将带来各行各业的颠覆性变革， 在不久的未来，区块链技术就会落地到实体经济应用层面。

1.2 区块链应用内涵

中心化应用自诞生以来，越来越成熟，在交易规模、交易速度、易维护性等多方面获得好评，但日益突出的一些问题依然困扰着用户，如软硬件研发投入、系统安全性、运维成本、系统升级等。

从现有区块链的技术应用看，区块链基础架构一般由数据层、网络层、共识层、激励层、合约层和应用层组合。其中，数据层封装了底层数据区块以及相关数据加密和时间戳等技术；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；激励层将经济因素集成到区块链技术体系中，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类脚本、算法和智能合约，是区块链可编程特征的基础；应用层则封装了区块链的各种应用。在这一模型中，基于时间戳的链式区块结构、分布式节点的共识机制、灵活可编程的智能合约是区块链技术最具创新性的技术环节。

全球区块链应用探索非常活跃，总体而言还处于小规模的概念验证阶段。当前的区块链技术应用主要集中在两个方面：

一是在不同机构或个人之间缺乏互信并缺少中介的情况下，实现数据的直接交换。区块链技术源于比特币，是比特币的底层数据存储技术，因此金融是区块链应用最热门的领域。美国 Ripple 公司早在 2012 年就已经引入区块链技术为多家银行提供跨境转账、清算和支付服务，与 SWIFT（环球同业银行金融电讯协会）等传统渠道相比，能够节约 1/3 手续费，把跨行对账等操作时间从数天压缩到几秒。区块链在数字货币、支付结算、证券交易、互助保险等金融场景中的应用也受到高度重视。

二是用于重要数据的保全与可靠存储。利用区块链不可篡改的特点，重要数据（如权属、协议、票据等法律文书）的保全成为应用探索的热点。目前，爱沙尼亚、格鲁吉亚等国家政府正尝试采用区块链技术对重要资产进行登记，开展了土地注册、商业登记、电子征税等重要信息的登记工作。

1.3 区块链应用落地困难分析

区块链应用截至目前，尚没有大面积普及的可信区块链应用落地。究其原因，很多区块链应用都无法解决区块链自身特性与商业应用固有的矛盾之处，或是认知和技术能力不足。

1、区块链自身不可篡改的特性，在商业应用某些环节中不是必须的。日益增大的账本数据使得区块链网络节点臃肿、笨重，极其消耗资源。

2、节点类型同质化严重，执行速度慢，交易规模和交易速度远远达不到商业应用高并发、高响应速度的需求。

3、现有智能合约编程要求高，业务表达能力不够，对于大中型商业应用没有合适的解决方案。

4、区块链所有交易（注册、转账、应用等）的高昂手续费，限制了商业应用的发展期望，因为这在高频次、大规模的商业应用中，手续费是非常惊人的，不符合商业应用成本规划。

综上所述，VTChain 认为，以区块链的思路去研发商业应用，必须跳出区块链现有的框架设定，从底层架构入手，以商业应用需求为导向，不用过于关注现

有的公有链、联盟链等基础概念的界限划分，大胆突破创新改革，将区块链技术优质特性与商业应用结合，方能从根本上解决问题。

二　VTChain 如何去做区块链 3.0

2.1 VTChain 是什么

VTChain 是一种构建商业级区块链应用的分布式、生产级开放生态，致力于推动将区块链技术与商业级产品应用紧密关联起来，充分利用区块链技术的优势，解决应用系统实践中心化系统日益明显的成本与安全保障问题。

VTChain 项目的性质：项目为公益项目，旨在推动区块链 3.0 应用技术在国内外的发展和提高。VTChain 基金会为公益组织，负责推进、管理 VTChain 项目发展和运营。

VTChain 将选择成熟时机对项目进行全部开源。

VTChain 基于比特币、以太坊、Neo、Hyperledger 等区块链开源技术框架基础，创新提出软件即服务(Software as a Service,简称 SAAS)的区块链应用技术，推动区块链技术快速构建商业级应用产品，充分吸收和借鉴比特币、以太坊、Neo、Hyperledger 区块链技术的基础构件，使其更加适合企业和开发者、终端用户，尤其是中国区域的应用级产品的开发与实践。

同时，借鉴比特币、Neo、以太坊和 Hyperledger 的技术框架设计思想，VTChain 采用插拔式、松散耦合的模块化设计，适用于普初中高级不同水平的开发者构建商业级大规模应用产品。用于构建支撑业务的行业应用和平台，以便支持各种各样的商业应用场景。

2.2 设计目标

自区块链诞生开始，“让人人都参与使用区块链、享受区块链的发展成果”成为 VTChain 社区共同愿景，因此 VTChain 项目的设计目标是重构区块链底层架构，以商业级应用需求为驱动，面向所有 B2B 和 B2C 应用设计，并提供国产化、界面友好、多语言的 IDE 开发环境。

2.3 创新点与特性

VTChain 主要具有技术特点：

2.3.1 生产级公有链和私有链结合

VTChain 是真正实现区块链技术所见即所得的生产型技术平台，基于 VTChain 系列模块和工具，可以快速结合商业应用业务实际，生产出分布式账本应用。

2.3.2 图灵完备的多语言共存生态

VTChain 采用图灵完备的计算机语言和虚拟机，支持多种开发语言 C#、JAVA、Node.JS、JavaScript、Python 等，开发者可自由选择适合的语言开发跨平台的区块链应用，或通过智能合约在 VTChain 虚拟机实时解释运行。

2.3.3 多态节点和参与者身份共识机制

为避免参与者和 Peer 节点增多造成的网络拥堵，VTChain 将区块链节点分为多种：共识节点、普通节点、数据节点。经过申请授权的节点，可以作为共识节点或数据节点存储参与者身份数据，共识节点之间采用多种共识机制使所有主机之间保持一致性状态。

VTChain 具有 CA 证书中心，所有接入的商业级应用和参与者都必须签发 CA 证书才能使用本系统。通过严格的 CA 证书认证，可有效控制客户端（Peer 节点）的权限和内容。

2.3.4 数据隔离和保密

在共识服务上采用“发布-订阅”机制，支持多通道消息传递，使得 Peer 节点可以基于应用访问控制策略来订阅任意数量的通道；也就是说，应用程序指定 Peer 节点的子集中架设通道。 这些 Peer 组成提交到该通道交易的相关者集合，而且只有这些 Peer 可以接收包含相关交易的区块，与其他交易完全隔离。

此外，Peers 的子集将这些私有块提交到不同的账本上，允许它们保护这些私有交易，与其他 peers 子集的账本隔离开来。应用程序根据业务逻辑决定将交易发送到 1 个或多个通道。 这不是内置的限制，区块链网络不知道并假设不同通道上的交易之间没有关系。

2.3.5 数字资产无缝流动

为了解决不同参与者所持有的数字资产流动问题，VTChain 提供了一种结算中心的机制，使得持有比特币、以太坊币、莱特币等数字资产的参与者（包括机构），可以进行实时动态结算，参与者无需关心数字资产之间的转换关系，只使用自身持有的资产交易，由结算中心按照实时动态“换算率”进行结算。

2.3.6 跨平台、国产化 IDE 开发环境

VTChain 使用 C#语言开发，努力建设跨平台、适合国内开发者和企业的 IDE 开发环境，提供 Web 版 IDE 和桌面版 IDE。国产化并非抄袭和模仿，而是从系统架构、业务逻辑、使用习惯、开发目标等综合考量，建立真正国产化的区块链商业应用方案和开发套件。

2.4 法律属性

VTChain 基于区块链的去中心化思想开发,但一切设计目标以遵循全球法律、维护现有经济秩序为基础，以实现区块链企业应用落地研发为前提，在现有中心化 IT 系统繁荣的行业大环境下，可以作为一种扩展或升级，逐步拓展去中心化应用生态，降低企业成本。

我们的法律定位是与现有经济秩序、中心化应用相互兼容并蓄，和谐发展，通过 API 协议和中间件系统实现互容互通，在不久的未来，作为实体经济的新型补充和扩展，以解决在垂直细分领域需要区块链技术适配的问题。

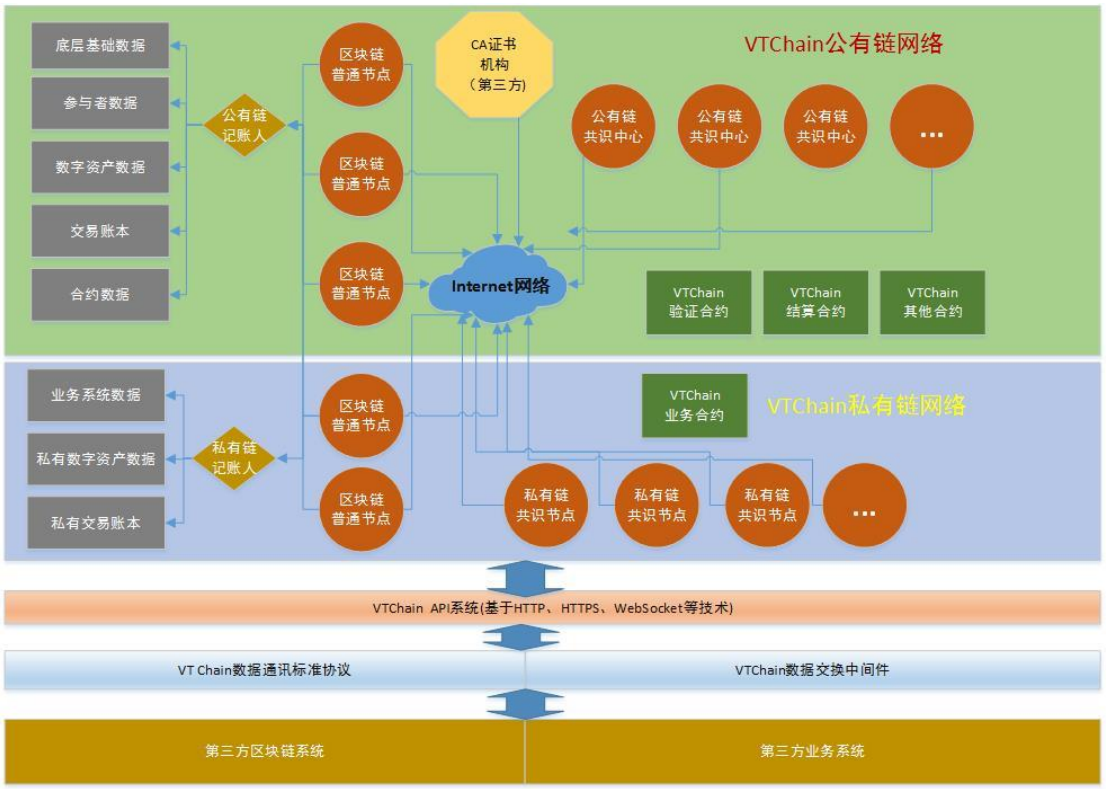
三　技术架构

3.1 总体架构

VTChain 的重要特征是在自身公有链的基础上支持多 Chain 和多通道技术。

所谓的多链实际上是包含 Peer 节点、账本、订阅通道的逻辑结构，它将参与者与数据（包含链码）进行隔离，满足了不同业务场景下的“不同的人访问不同数据”的基本要求。

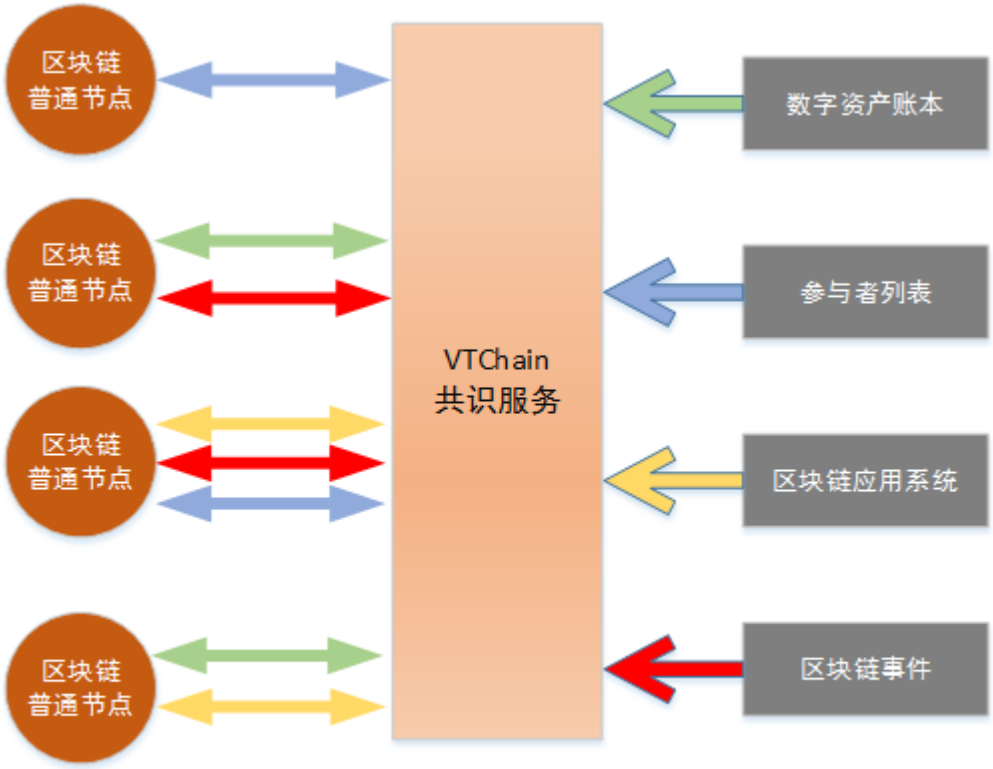
一个节点既存在于公有链，也可以参与到多个私有链中（通过接入多个通道）；如下图所示：



VTChain区块链应用系统 技术原理图

通道：通道是由共识服务提供的一种通讯机制，是发布-订阅设计模式产生的信息管道，任何消息和业务的网络传输都基于通道机制完成。在 VTChain 区块链网络中，数字资产、交易账本、业务合约等都可以通过“发布-订阅”模式通讯。它定义了一种多对多的依赖关系，每个节点都可以订阅监听某一主题对象，当主题对象在自身状态变化时，会通知所有订阅节点，使他们能自动更新自己的状态。

基于这种发布-订阅关系，将区块链节点和共识服务连接在一起，形成一个个具有保密性的通讯链路（虚拟），实现了业务隔离的要求。如下图所示：



VTChain发布-订阅的通道机制

由上图可以看出,VTChain 的发布-订阅模式，其实是一种解耦合的通道机制，它使得通道所传输的对象都是独立、标准化的抽象模型，这些抽象的模型包括：数字资产账本、参与者列表、区块链应用系统、区块链事件等。各个对象之间可以互相依赖，也可以互相独立。对象与节点之间的通讯管道，即为通道。换句话说，通道存在于抽象的理论模型中，实际上并不是物理存在。

节点与对象之间的验证、交易、应用等服务，由共识节点提供。

发布-订阅的通道机制可以将公有链、不同的业务系统私有链明确的区分开，保持了 VTChain 公链和各个应用系统之间的逻辑独立，通过通道机制，VTChain 区块链应用系统的参与者可以有效的关注其关联的参与者对象、数据和业务系统。

3.2 1+N 多链结构(Multi BlockChain)

VTChain 是一种运行于互联网、由广大社区参与者共同维护管理的去中心化公链与私链混合型的系统，区块链上的所有参与者既属于公链，又可以自由选择

进入私链。

公链账本包括参与节点（共识节点、数据节点）的全部数据、参与用户的数字资产数据和交易数据等全部内容，由共识服务自动维持全网一致性，无需人工干预。公链账本一旦达成共识，任何人无权篡改和删除。

VTChain 基于区块链应用的特点，允许任何参与者建立自有的私有链应用系统，私有链中可以自定义数字资产、参与者列表、智能合约、应用 UI 模板等内容。

3.3 CSL 账本与动态存储技术

区块链技术不可篡改的分布式账本技术一度成为最具竞争力的核心技术，但分布式账本技术仍然存在以下问题：

1、不可篡改的特性在赢得呼声的同时也给区块链带来了巨大的麻烦，大量垃圾账本和应用数据充斥链上区块中，使区块账本变得臃肿、笨重，钱包等相关应用变得越来越消耗系统资源(CPU、内存、硬盘等)，难以使用（应用简单、速度慢）。

2、大一统的总账本结构使得普通用户被迫下载和存储大量垃圾账本和无关数据，增加不必要的使用成本，也使得钱包和应用软件同步成为问题。这显然不符合商业应用的开发需求。

VTChain 针对这种根本性问题，采用分类静态账本+动态存储技术解决，这样既保留了区块链不可篡改的初衷，又能保证账本数据均为有效区块，同时避免了终端应用软件笨重、难使用的问题。

分类静态账本（Classified Static Ledger）：VTChain 基于 Multi Block Chain 多链技术，将链上账本分为资产账本、合约账本、应用账本、日志账本等不同类型。其中，资产账本指包含用户地址信息、交易信息、数字资产信息等基本元素，合约账本包含智能合约注册发布信息、交易信息、注销等，应用账本包括应用程序源码、发布程序、应用数据、应用日志等，日志账本指系统交易确认日志、应用发布日志等信息。

动态存储技术（Dynamic Storage）：对于合约账本、应用账本采用分布式动态存储技术，合约拥有者和应用拥有者可动态更新、升级相关应用。

3.4 多态节点设计

区块链商业应用的用户终端软件应是轻客户端软件，基于 Web 或桌面客户端程序，无需同步或下载大量账本数据，随时使用。基于这一理念，VTChain 将链上节点分为普通节点、共识节点、数据节点等类型。

其中普通节点即为用户节点，此节点采用 VTChain 统一 HTTP 协议或 TCP/IP 协议连接 VTChain 多链网络，普通节点提供为 DAPP 应用用户使用。

共识节点为多链网络中的共识机制，提供交易验证、签名认证等作用。

数据节点提供数据存储、共享、应用服务器等服务。

3.5 Universal 共识与多共识机制

VTChain 区块链的共识服务同时存在于公有链和私有链中，由各自的共识节点使用有效的哈希算法维护分布式账本的一致性和合法性。

VTChain 主链采用独立自主创新、独一无二的 Universal 共识（宇宙共识）算法完成数据一致性验证，该算法是在 DPos、Paxos、IOTA 等优势特征基础上创新发展而来的、自主产权的商业级共识机制。

Universal 共识是一种真正能实现高并发、大规模集群应用的共识机制，面向大中型商业应用开发，依赖于多链结构和共识分片算法，节点功能分为 Verifier、Block Collector、Acceptor。Verifier 用于验证账本交易，每 N 个节点组成一个共识分片，采用多级见证人机制对交易进行签名，Block Collector 对 Verifier 的签名进行验证，负责收集区块、异步写入区块链。Acceptor 负责接收区块数据。

Universal 共识机制可在同一时刻完成 N 多个区块交易的验证和生产，相比于 POW、POS、DPOS、IOTA 等现有的共识机制而言，速度更快，去中心化程度更高，安全性更可靠，高并发性能更快。

VTChain 子链提供多种共识算法动态切换，由区块链共识节点和 DAPP 开发组织根据具体业务应用的需求设置共识协议，如 PBFT，Raft，POW，POS，DPOS 等等。

多种共识机制如何并存，会在随后的研发和白皮书中逐渐说明。

3.6 VTChain 加密算法

与大多数的加密货币相同，VTChain 的账户采用基于 ECC 椭圆曲线密码机制的公私钥生成算法。

椭圆曲线密码机制(Elliptic Curve CryptoSystem,ECC)是 1985 年由 Koblitz N 和 Miller V 提出的，其安全性是建立在求解椭圆曲线离散对数问题困难性基础上的，在同等密钥长度的情况下，ECC 的安全强度远高于 RSA 体制等密码机制，因为 ECC 在网络信息安全领域有着非常重要的理论研究价值和广阔的实际应用前景。另一方面，在安全性相当的情况下，ECC 所使用的密钥长度更多，这意味着对于带宽和存储空间的需求相对最小，并且到目前为止，尚未出现针对椭圆曲线的亚指数时间算法。因此，ECC 将会是今后最重要的主流公私钥加密技术。

椭圆曲线密码机制的安全性，依赖于椭圆曲线上离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）的难解性。而对椭圆曲线密码机制的攻击，也可归结为对 ECDLP 的攻击。对 ECDLP 的攻击类似于对有限域的乘法群上离散对数问题的攻击，但是攻击方法并不能有效地移植 ECDLP。对 ECDLP 的攻击主要分为两类：一类是对所有曲线的离散对数问题的攻击；另一类是对特殊曲线的离散对数的攻击。

在 VTChain 公私钥体系中，私钥是钱包账户持有的唯一凭证，私钥可以生成公钥，公钥可以产生钱包地址。此过程为单向、不可逆的过程。因此外部无法暴力破解账户信息。

3.7 安全沙箱机制

区块链是去中心化的系统平台，因为源代码开源，因此系统的安全性和健壮性非常重要和必须可靠，VTChain 完整地推出一种基于区块链网络实时运行的安全沙箱模型。

VTChain 安全沙箱模型，包括三个层次：VTChain 虚拟机、动态智能合约、VTChain 状态机。

VTChain 虚拟机是一种轻量级的运行时环境，其实质作用是 CLR((Common Language Runtime,通用语言运行时)，负责链上代码（不同语言）的解释和运行，

支持的语言包括 C#、JAVA、JavaScript、GO、Node.JS 的语言。

动态智能合约指运行于 VTChain 虚拟机上的一组或多组经过的签名验证的动态执行代码，参与者可以使用自身偏好的语言，自定义自己的应用逻辑和数字资产结算方式。动态智能合约分为两种运行模式：预编译执行和动态执行。常规固化的应用逻辑可以在预编译后发布至区块链系统，以节省系统开销、提高执行效率。而动态变化的参数内容、实时变动的应用预制逻辑，则可以实时动态编译执行的方法，例如未来可能运行在 VTChain 区块链上的人工智能、云计算、大数据算法等内容。

VTChain 状态机是 VTChain 团队创新提出的一种实时安全监测机制，它将对 VTChain 区块链链上数据和节点进行实时安全扫描和监测。状态机负责的内容包括：智能合约的类型安全(Type Checker)、代码安全、垃圾回收（Garbage Collector）、异常处理(Exception Manager)和向下兼容(COM Marshaler)等。

3.8 数字签名算法

数字签名是指在区块链交易、区块验证、区块上链等过程中，对关键信息进行签名的过程。数字签名是确保使用者身份、防伪的重要手段之一。

VTChain 的数字签名采用 Schnorr 数字签名算法。

1989 年，Schnorr 提出了一种随机化的签名方案，成为 Schnorr 数字签名方案，用于解决 ElGamal 签名与离散对数问题。

Schnorr 数字签名算法基于离散对数困难性问题，可扩展至椭圆曲线上的 Schnorr 签名算法，主要优势为：可实现多重数字签名与批验证，即多个用户对同一消息的签名可聚合成单个，且仅需要单次验证过程。

因此，相对于 ECSDA 数字签名方法，Schnorr 具有更短的签名、更强的安全性、更快的签名/验证时间，因此网络传输流量和存储空间需求将大大缩减。

3.9 X509 数字证书体系

在区块链网络中，由于用户身份采用匿名制，一旦非对称加密算法和数字签名中的公钥被替换和篡改，后果将不可设想。因此对于保证交易和数字签名

的原始性，必须有足够的保护。VTChain 的 PKI 数字证书可以很大地解决用户数字身份认证和公私钥保护等问题。

PKI 数字证书是 VTChain 网络证明用户数字身份的重要权证，由 VTChain 基金会实现颁发、验证、撤销、作废等，未来可实现去中心化的数字证书颁发。

VTChain 主要采用业内成熟、可靠的 X.509 数字证书 V3 版的证书体系。

在 VTChain 网络中，X.509 证书提供基于匿名机制的可信数字身份机制。每一个拥有 X.509 证书的用户都认为是相对可信的节点，轻节点暂不需要证书。

数字证书可确保签名的公钥来自原始的用户，而非伪造的公钥。

初期使用数字证书的用户主要包括：共识节点、数据节点、协调器节点（索引服务节点）等，以后可能扩展在 DAPP 节点、IPFS 节点等。

节点登录 VTChain 网络后，首先验证数字证书，数字证书缺失、作废或过期的节点，将被不允许接入 VTChain 网络。

VTChain 的 PKI 证书治理体系包括：CA(Certification Authority)、RA(Registration Authority)、证书数据库等组件组成。

3.10 应用系统

VTChain 终端应用系统是提供给终端用户（数字资产持有者、应用系统用户等）的工具软件和应用入口。

终端应用系统包括：VTChain 终端应用客户端软件、VTChain 钱包软件、VTChain 区块链浏览器、数字交易网关系统等内容。

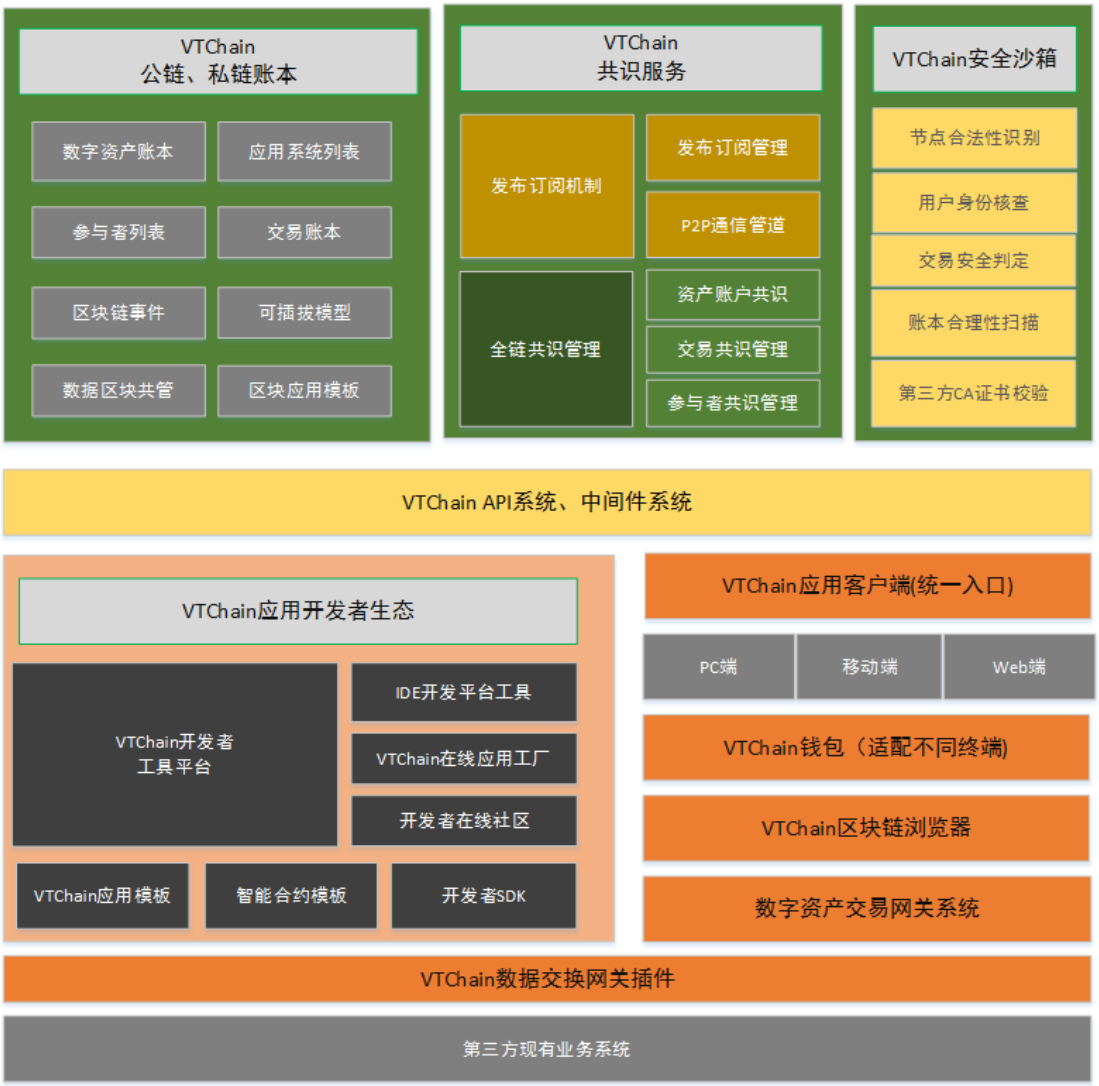
VTChain 终端应用客户端软件为区块链应用的统一入口，终端用户通过它接入 VTChain 区块链网络，在其之上运行各种智能合约、区块链应用，类似于微信-小程序之间的主副依赖关系。

VTChain 钱包软件用于创建、管理、交易用户的数字资产。终端应用客户端软件与钱包软件单独设置的设计模式，有利于保护链上用户数字资产的安全，同时减少那些只希望使用钱包、对应用不感兴趣的用户的体验负担。

3.11 DAPP 生态

VTChain 应用开发者生态是将区块链技术应用落地的生态环境，由广大社区

爱好者和开发者共同维护。其基本内容为：VTChain IDE 开发工具、Web 在线应用工厂、开发者社区、VTChain 智能合约模板、VTChain 应用模板、开发者 SDK、VTChain API、VTChain 数据交换插件等内容。



VTChain区块链3.0应用系统生态框架图

四 经济模型

4.1 经济模型综述

VTChain 经济模型围绕系统内业务模型设计，既要满足系统业务需求，又能对共识节点和数据节点进行有效激励。

4.2 数字资产机制

VTChain 区块链系统的基础数字资产包括 BVC 和 BVG 两种类型。

其中，BVC 为 VTChain 系统创世的令牌，一开始便已经产生，发行总量不再增加，并随着系统的使用和交易过程逐渐消耗、减少。为减少 VTChain 系统中的无效交易，每一次转账操作，将自动扣除交易金额的 0.001%（未来可能是动态费率）的交易费用，自动打入黑洞地址，永远消除，单次交易最多扣除 100BVC。

BVG 为 VTChain 的燃料令牌，它不需要发行，由系统自动随着区块的创建而产生，用于奖励系统共识节点和社区贡献者。

令牌使用范围：BVC 主要用于系统应用交易结算和系统投票，而 BVG 将用于区块链网络的创建、记账等。BVG 随着区块的不断增加自动产生，奖励给区块制造者，并在 25 年内全部产生完毕，总计 10 亿。

BVC 发行计划请关注 VTChain 官网，我们将适时推出。

BVC 和 BVG 将在 VTChain 平台上线稳定后，在 VTChain 去中心化交易所实现交易。

VTChain 平台上线前，系统使用基于以太坊的代币 BVT，使用属性等同于 BVC。

4.3 费用设计

本系统中，数字资产作为价值持有凭证，同时也用于支付用户交易和使用应用所支付的报酬。

具体费用提现在：

1、数字资产转账费用。

2、数字资产注册发行费用。

3、智能合约发行费用。

4、应用程序发布费用、租用费用等。

5、其他服务所必须的费用。

费用主要奖励给共识节点、数据节点等。

4.4 节点激励计划

VTChain 为促进网络发展，初期对共识节点、数据节点实施奖励计划，具体计划如下：

1、矿工创建区块、完成共识机制的服务，可额外获得若干个 BVT 作为奖励。

2、数据节点提供数据服务，每天可获得若干个 BVT 奖励。

3、其他不定期奖励。

具体实施内容将在系统开发和内测期间确定。

4.5 DAPP 经济模型

DAPP 是 VTChain 企业应用区块链系统上的重要核心内容，针对 DAPP 的干系人（开发者、数据节点提供者、用户），均设计一定的经济模型。

开发者发行 DAPP 应用需要支付一定的旷工费。

数据节点提供者提供应用数据服务，可收取用户的使用费，具体费用由开发者配置，二者共享收益。

五　用户模型

5.1 使用者

指 VTChain 企业应用的使用者，包括政府、企事业单位和个人用户。

5.2 开发者

指基于 VTChain 区块链网络，使用 VTChain API 协议和中间件产品，开发企业应用的开发者，包括商业组织或个人开发者。

5.3 服务商

指为 VTChain 提供基础网络和数据服务的个人或单位。

5.4 商业单位

指在VTChain系统里的商业组织，以商业应用为核心提供咨询等上下游服务。

5.5 第三方机构

指在 VTChain 系统里相关的第三方机构，比如 CA 证书颁发机构、版权认定机构等等。

六　应用场景

6.1 基于 VTChain 技术的 P2P 网贷聚合平台

从目前的技术应用和行业现状来看，区块链技术在金融领域的商业价值最为清晰可见，我们将首先谈谈如何基于 VTChain 应用平台,实现 P2P 网贷聚合平台 BCLP 系统（Block Chain Lending Platform，以下简称 BCLP 系统）。

BCLP 系统是一种使用区块链技术、大数据技术实现的 P2P 网贷、信用共享、信息聚合、智能评估等数字资产管理系统。

使用区块链技术的网贷聚合平台具有如下特性：

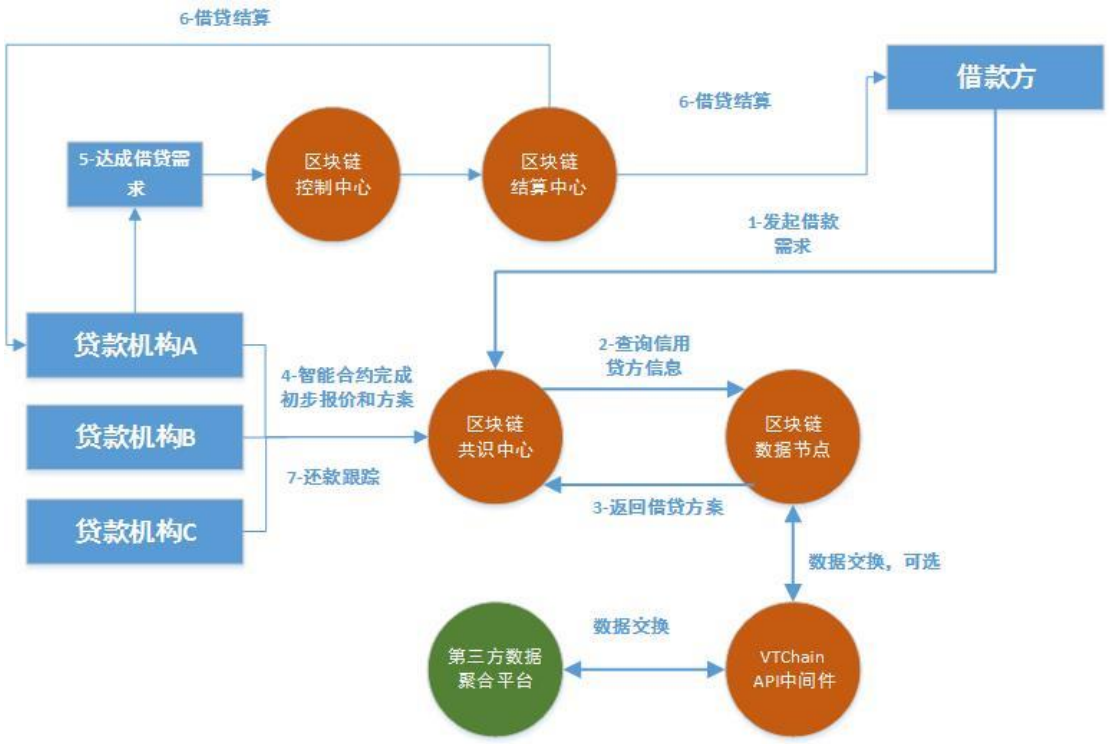
1、身份共识机制：BCLP 系统要求参与者具有明确、可靠的身份数据，参与者包括借方用户、贷方用户，此方面的数据可以在 BCLP 数据区块中从新建立，也可以从现有的应用系统中拉取(Pull),BCLP 系统提供统一的 API 接口和工具对接现有的应用系统。

2、信息聚合机制：借贷系统要求对借方的信用、贷方的可贷款额度等内容有足够可靠的信息，并且具备不可操作和篡改的特性，BCLP 系统将个人信用、贷方的贷款机制（包括额度、利率等）信息保存在分布式数据节点，在 BCLP 控制列表（由共识机制自动控制）未经授权的情况下，不允许修改。因此 BCLP 系统的相关资讯均可认为是合理有效的。同时 BCLP 通过可插拔的智能合约逻辑提供借贷双方必要的服务。

3、大数据分析策略：BCLP 系统将对接第三方合作的信用平台采集大量的原来数据，采用大数据分析策略和分布式计算方法智能评估借方贷款额度，通过比价机制提供最佳的借贷方案。

下面我们来谈谈具体如何使用 VTChain 实现这一目标。

BCLP 系统技术原理框架如下：



基于区块链技术和VTChain的BCLP业务系统 技术原理图

BCLP 系统所有借贷业务均通过智能合约和共识机制完成，全程无需第三方干预。

全部智能合约，只需要若干行代码。我们需要首先判断这个发起人的身份和可靠，确保实名、信用良好，系统自动对接相关金融机构。如果有多个金融机构参与，则需要金融机构竞争性报价接单。智能合约以接单指令的时间戳为排序标准，优先分配给时间戳靠前的贷款机构，如果交易达成，则结算中心将自动结算借贷双方的数字资产（可以是有价数字货币或法币），任何一方都无法篡改和抵赖。

6.2 基于 VTChain 区块链技术的汽车拍卖平台

在 Hyperlydger 官方资料中，基于区块链技术的汽车拍卖平台是其经典的一

个应用解决方案，因为 VTChain 也将其作为一种案例，以便大家更好的理解 VTChain 的企业级应用特点。

在汽车拍卖平台中，构成交易的三大要素：参与者、资产与事务。参与者包括拍卖业务所有的利益相关者，包括汽车持有人、买家、平台管理方等。资产在此主要指汽车转换而成的数字化等价标的物，事务指双方由此产生的查询、拍卖、管理等交易事件。

平台管理方首先在注册机构(区块链共识节点提供注册服务)中登记参与者、资产等数据，并存储于数据节点，通过共识机制在所有系统客户端达成一致状态，此状态包括各方数据、资产数据、拍卖状态（拍卖中、已完成、作废等）。

拍卖开始后，由参与者开始向共识节点发起身份验证，获得其被授予的权限（由控制中心管理），并取得授权的 CA 证书。智能合约采集其出价数据，并随时判定拍卖是否结束，拍卖结束条件为拍卖时间结束或第一价高者产生，系统将自动结束。

此系统中，所有参与者、机动车采用各自统一的编码方式获得唯一标识，作为拍卖系统中的令牌，由注册机构和共识机制完成采集和验证。

总　结

VTChain 区块链自开创以来，得到了行业同仁及相关区块链爱好者的广泛关注和好评，很多社区用户对 VTChain 项目发展提出了良好的建议和思路。在此，VTChain 团队表示衷心的感谢，并希望在未来的日子里一路有广大朋友们陪伴。

VTChain 社区是一个开放、开源的区块链项目社区，任何关注和区块链人才都随时欢迎加入我们团队，与我们共同助力，精心研发，脚踏实地地做好区块链技术研发，推动新一代 IT 系统革命性发展，带着 VTChain 独有的情怀去实现我们对区块链的理解和梦想。

时间终将证明，只有专注研发、认真落地的区块链项目才会得到长足的发展和认可。

参 考 文 献

[1] A Brief History of Blockchain, Vinary Cupta.

[2] Singapore experimenting with Blockchain technology ． 新华网.

[3] 2017 年国内外区块链发展现状、发展类型、发展特性及发展生态分析

[4] http://www.8btc.com/blockchain-poc-hyperledger

[5] https://bitcoin.org/bitcoin.pdf

[6] http://www.8btc.com/hyperledger-fabric1-0

[7] http://blog.csdn.net/bluecloudmatrix/article/details/51859333

[8] https://www.hyperledger.org/community

[9] https://www.hyperledger.org/blog

[10] http://blog.csdn.net/BlueCloudMatrix/article/details/51898105