VAO 白皮书

目录

1、区块链的兴起和未来之路

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新。联合国、国际货币基金组织，以及美国、英国、日本等国家对区块链的发展给予高度关注，积极探索推动区块链的应用。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

随着区块链的产业价值逐渐确定，区块链迅速地成为一场全球参与竞逐的“军备”大赛，中国也开始从国家层面设计区块链的发展道路（发改委委托信通院组织国内主要区块链公司进行区块链的顶层设计的研讨，工信部的信软司也在积极确定区块链的顶层设计机构）。2018 年，区块链及相关行业加速发展，中国将领跑全球进入“区块链可信数字经济社会”，我们正面临区块链重大的产业机遇。

1.1 区块链的兴起

1.1.1 从摆脱第三方制约起步

区块链技术起源于化名为“中本聪”（Satoshi Nakamoto）的学者在 2008 年发表的奠基性论文《比特币：一种点对点电子现金系统》。文章提出，希望可以创建一套新型的电子支付系统，这套系统“基于密码学原理而不是基于信用，使得任何达成一致的双方能够直接进行支付，从而不需要第三方中介参与”。

该论文催生了比特币，标志着人类社会的货币体系向前迈出了一大步。比特币采用了公开的分布式账本的设计思路，真正摆脱了第三方机构的制约。随后比特币进入快速发展期。

2009 年 1 月 3 日，区块链的第一个区块诞生，该区块又名“创世区块”。

2009 年 1 月 12 日，中本聪发送了 10 个比特币给密码学专家哈尔芬尼。

2010 年 7 月，比特币交易所 Mt.Gox 的成立，比特币的价值被世界认可。

此后几年里，由于比特币的挖矿机制造成巨大的资源消耗，比特币的匿名性对传统金融监管提出了挑战，使得比特币价格随之出现了大起大落。

1.1.2 从比特币跃迁到区块链+

由于比特币系统设计的非图灵完备性，其系统无法处理更为复杂的业务逻辑。受比特币启发，于 2015 年左右开发上线的公共区块链平台以太坊则将区块链的应用更进一步，允许开发者在平台上部署智能合约，以处理更为复杂的业务逻辑。智能合约使得通过代码设定好的业务逻辑能够自动按照触发条件执行而无需人为干预，并且合约部署在区块链上公开透明。因此区块链技术可以被广泛的运用在涉及合同处理、数据交换、所有权转移的金融、物联网、物流和共享经济等场景中。

如果从比特币诞生开始计算，区块链技术已有近 10 年的发展历史。目前区块链的发展方向主要可以分为公有链和联盟链：前者以比特币和以太坊为代表，任何人都可以随时加入其中，链上记录对所有人公开；后者则由指定区块链的参与成员组成联盟，成员之间的业务往来信息被记录在区块链中，限定了使用规模和权限，典型代表如 Linux 基金会旗下的开源区块链项目 Hyperledger 等。

区块链的诞生，标志着人类开始构建真正的信任互联网。

有一种新的观点认为，区块链技术可以构建一个高效可靠的价值传输系统，推动互联网成为构建社会信任的网络基础设施，实现价值的有效传递，并将此称为价值互联网。我们注意到，区块链提供了一种新型的社会信任机制，为数字经济的发展奠定了新基石，“区块链+”应用创新，昭示着产业创新和公共服务的新方向。

区块链可为经济社会转型升级提供系统化的支撑。区块链+的显著优势在于优化业务流程、降低运营成本、提升协同效率，这个优势已经在金融服务、供应链管理、知识产权、智能制造、社会公益以及教育就业等社会各领域初步体现出来。

1.2 区块链的设计思想

1.2.1 经济层面的设计思想

在区块链体系中，参与者可以不需要了解对方基本信息的情况进行交易，实现了“无需信任的信任”，改变了传统模式中以第三方为中心的信任模式。

第一，交易信任由机器和算法确定。区块链通过构建一个依赖于机器和算法信任的交易体系，解决在匿名交易过程中的相互信任问题。所有参与者将在无须建立信任关系的环境中，通过密码学原理确定身份，依靠共识机制实现相互间的信任。

第二，交易过程可以由程序自动执行。区块链通过可编程的智能合约，自动执行双方所达成的契约，排除了人为的干扰因素，从制度上防止任何一方的抵赖。从而推动经济社会进入一种智能的状态，实现当前经济交易系统的质的飞跃。

基于区块链技术的“弱中心化”特性，现有的经济体系可以脱离当前通过制度约束或第三方机构背书，双方直接实现价值交付。这种“弱中心化”特性可以有效降低交易成本，提高交易效率，减少因交易一致性所引发的摩擦。

1.2.2 技术层面的设计思想

通俗的说，区块链可以看成是一套由多方参与的、可靠的分布式数据存储系统，其独特之处在于：一是记录行为的多方参与，即各方可参与记录；二是数据存储的多方参与、共同维护，即各方均参与数据的存储和维护；三是通过链式存储数据与合约，并且只能读取和写入，不可篡改。

1.3 区块链的核心技术

区块链技术不是一个单项的技术，而是一个集成了多方面研究成果基础之上的综合性技术系统。区块链核心关键技术有：分布式账本、共识机制、智能合约和密码学。

1.3.1 分布式账本

分布式账本技术 DLT (Distributed Ledger Technology)本质上是一种可以在多个网络节点、多个物理地址或者多个组织构成的网络中进行数据分享、同步和复制的去中心化数据存储技术。相较于传统的分布式存储系统，分布式账本技术主要具备两种不同的特征：

①传统分布式存储系统执行受某一中心节点或权威机构控制的数据管理机制，分布式账本往往基于一定的共识规则，采用多方决策、共同维护的方式进行数据的存储、复制等操作。面对互联网数据的爆炸性增长，当前由单一中心组织构建数据管理系统的方式正受到更多的挑战，服务方不得不持续追加投资构建大型数据中心，不仅带来了计算、网络、存储等各种庞大资源池效率的问题，不断推升的系统规模和复杂度也带来了愈加严峻的可靠性问题。然而，分布式账本技术去中心化的数据维护策略恰恰可以有效减少系统臃肿的负担。在某些应用场景，甚至可以有效利用互联网中大量零散节点所沉淀的庞大资源池。

②传统分布式存储系统将系统内的数据分解成若干片段，然后在分布

式系统中进行存储，而分布式账本中任何一方的节点都各自拥有独立的、完整的一份数据存储，各节点之间彼此互不干涉、权限等同，通过相互之间的周期性或事件驱动的共识达成数据存储的最终一致性。经过几十年的发展，传统业务体系中的高度中心化数据管理系统在数据可信、网络安全方面的短板已经日益受到人们的关注。普通用户无法确定自己的数据是否被服务商窃取或篡改，在受到黑客攻击或产生安全泄露时更加显得无能为力，为了应对这些问题，人们不断增加额外的管理机制或技术，这种情况进一步推高了传统业务系统的维护成本、降低了商业行为的运行效率。分布式账本技术可以在根本上大幅改善这一现象，由于各个节点均各自维护了一套完整的数据副本，任意单一节点或少数集群对数据的修改，均无法对全局大多数副本造成影响。换句话说，无论是服务提供商在无授权情况下的蓄意修改，还是网络黑客的恶意攻击，均需要同时影响到分布式账本集群中的大部分节点，才能实现对已有数据的篡改，否则系统中的剩余节点将很快发现并追溯到系统中的恶意行为，这显然大大提升了业务系统中数据的可信度和安全保证。

这两种特有的系统特征，使得分布式账本技术成为一种非常底层的、对现有业务系统具有强大颠覆性的革命性创新。

1.3.2 共识机制

区块链是一个历史可追溯、不可篡改，解决多方互信问题的分布式（去中心化）系统。分布式系统必然面临着一致性问题，而解决一致性问题的过程我们称之为共识。

分布式系统的共识达成需要依赖可靠的共识算法，共识算法通常解决的是分布式系统中由哪个节点发起提案，以及其他节点如何就这个提案达成一致的问题。我们根据传统分布式系统与区块链系统间的区别，将共识算法分为可信节点间的共识算法与不可信节点间的共识算法。前者已经被深入研究，并且在现在流行的分布式系统中广泛应用，其中 Paxos 和 Raft 及其相应变种算法最为著名。对于后者，虽然也早被研究，但直到近年区块链技术发展如火如荼，相关共识算法才得到大量应用。而根据应用场景的不同，后者又分为以 PoW（Proof of Work）和 PoS（Proof of Stake）等算法为代表的适用于公链的共识算法和以 PBFT(Practical Byzantine Fault Tolerance)及其变种算法为代表的适用于联盟链或私有链的共识算法。

工作量证明 POW 算法是比特币系统采用算法，该算法于 1998 年由 W. Dai 在 B-money 的设计中提出。以太坊系统当前同样采用 PoW 算法进行共识，但由于以太坊系统出块更快（约 15 秒），更容易产生区块，为

了避免大量节点白白陪跑，以太坊提出了叔（Uncle）块奖励机制。PoS（Proof of Stake）算法最早由 Sunny King 在 2012 年 8 月发布的 PPC（PeerToPeerCoin 点点币）系统中首先实现，而以太坊系统也一直对 PoS 抱有好感，计划后续以 PoS 代替 PoW 作为其共识机制。PoS 及其变种算法可以解决 PoW 算法一直被诟病的浪费算力问题，但其本身尚未经过足够验证。PBFT 算法最早由 Miguel Castro（卡斯特罗）和 Barbara Liskov（利斯科夫）在 1999 年的 OSDI99 会议上提出，该算法相较原始拜占庭容错算法具有更高的运行效率。假设系统中共有 N 个节点，那么 PBFT 算法可以容忍系统中存在 F 个恶意节点，并且 3F+1 不大于 N。PBFT 共识算法虽然随着系统中节点数增多而可以容忍更多的拜占庭节点，但其共识效率却是以极快的速率下降，这也是我们能看到的应用 PBFT 做共识算法的系统中很少有超过 100 个节点的原因。

无论是 PoW 算法还是 PoS 算法，其核心思想都是通过经济激励来鼓励节点对系统的贡献和付出，通过经济惩罚来阻止节点作恶。公链系统为了鼓励更多节点参与共识，通常会发放代币（token）给对系统运行有贡献的节点。而联盟链或者私链与公链的不同之处在于，联盟链或者私链的参与节点通常希望从链上获得可信数据，这相对于通过记账来获取激励而言有意义得多，所以他们更有义务和责任去维护系统的稳定运行，并且通常参与节点数较少，PBFT 及其变种算法恰好适用于联盟链或者私链的应用场景。

1.3.3 智能合约

什么是智能合约？

智能合约（Smart contract ）是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易。这些交易可追踪且不可逆转。其目的是提供优于传统合同方法的安全，并减少与合同相关的其他交易成本。

智能合约概念可追溯到 20 世纪 90 年代，由计算机科学家、法学家及密码学家尼克·萨博（Nick Szabo）首次提出。他对智能合约的定义如下：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。” 尼克·萨博等研究学者，希望能够借助密码学及其他数字安全机制，将传统的合约条款的制定与履行方式，置于计算机技术之下，降低相关成本。然而，由于当时许多技术尚未成熟，缺乏能够支持可编程合约的数字化系统和技术，尼克·萨博关于智能合约的工作理论迟迟没有实现。

随着区块链技术的出现与成熟，智能合约作为区块链及未来互联网合约的重要研究方向，得以快速发展。基于区块链的智能合约包括事件处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约，数据的状态处理在合约中完成。事件信息传入智能合约后，触发智能合约进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足，则由状态机根据预设信息选择合约动作的自动执行。因此，智能合约作为一种计算机技术，不仅能够有效地对信息进行处理，而且能够保证合约双方在不必引入第三方权威机构的条件下，强制履行合约，避免了违约行为的出现。

1.3.4 密码学

信息安全及密码学技术，是整个信息技术的基石。在区块链中，也大量使用了现代信息安全和密码学的技术成果，主要包括：哈希算法、对称加密、非对称加密、数字签名、数字证书、同态加密、零知识证明等。以下从完整性、机密性、身份认证等维度，简要介绍区块链中安全及密码学技术的应用。

①完整性（防篡改）

区块链采用密码学哈希算法技术，保证区块链账本的完整性不被破坏。哈希（散列）算法能将二进制数据映射为一串较短的字符串，并具有输入敏感特性，一旦输入的二进制数据，发生微小的篡改，经过哈希运算得到的字符串，将发生非常大的变化。此外，优秀哈希算法还具有冲突避免特性，输入不同的二进制数据，得到的哈希结果字符串是不同的。

区块链利用哈希算法的输入敏感和冲突避免特性，在每个区块内，生成包含上一个区块的哈希值，并在区块内生成验证过的交易的 Merkle 根哈希值。一旦整个区块链某些区块被篡改，都无法得到与篡改前相同的哈希值，从而保证区块链被篡改时，能够被迅速识别，最终保证区块链的完整性（防篡改）。

②机密性

加解密技术从技术构成上，分为两大类：一类是对称加密，一类是非对称加密。对称加密的加解密密钥相同；而非对称加密的加解密密钥不同，一个被称为公钥，一个被称为私钥。公钥加密的数据，只有对应的私钥可以解开，反之亦然。

区块链尤其是联盟链，在全网传输过程中，都需要 TLS(Transport Layer Security)加密通信技术，来保证传输数据的安全性。而 TLS 加密通信，正是非对称加密技术和对称加密技术的完美组合：通信双方利用非对称加密

技术，协商生成对称密钥，再由生成的对称密钥作为工作密钥，完成数据的加解密，从而同时利用了非对称加密不需要双方共享密钥、对称加密运算速度快的优点。

③身份认证

单纯的 TLS 加密通信，仅能保证数据传输过程的机密性和完整性，但无法保障通信对端可信（中间人攻击）。因此，需要引入数字证书机制，验证通信对端身份，进而保证对端公钥的正确性。数字证书一般由权威机构进行签发。通信的一侧持有权威机构根 CA(Certification Authority)的公钥，用来验证通信对端证书是否被自己信任（即证书是否由自己颁发），并根据证书内容确认对端身份。在确认对端身份的情况下，取出对端证书中的公钥，完成非对称加密过程。

此外，区块链中还应用了现代密码学最新的研究成果，包括同态加密、零知识证明等，在区块链分布式账本公开的情况下，最大限度地提供隐私保护能力。

1.4 未来发展趋势

①应用模式升级。鉴于公有链的安全性及交易量与日俱增对现网容量之间的平衡问题，未来区块链的应用领域将以联盟链、私有链或混合链为主。比特币模式增加了区块链网络的维护成本，对于低价值、低风险的交易来说并非完全适用。考虑到效率及安全的提升，未来将是以联盟链、私有链、或由联盟链和私有链组成的混合链组成。

②多中心化。未来区块链系统架构将是构建可信任的多中心体系，将分散独立的各自单中心，提升为多方参与的统一多中心，从而提高信任传递效率，降低交易成本。即在信息不对称、不确定的环境下，建立满足各种活动赖以发生、发展的“信任”生态体系。

③从金融创新带动其他行业应用突破。区块链的应用领域将先从对交易各方有相互建立信任的需求，但又不容易建立信任关系的领域切入，如金融、证券、保险等领域。随着应用普及和社会认知度的提高，区块链将逐渐向社会各领域渗透。比如区块链已经初步的应用于政治选举、企业股东投票、博彩、预测市场等领域。

④智能合约的社会化。未来，所有的契约型的约定都实现智能化，利用智能合约可以保障所有约定的可靠执行，避免篡改、抵赖和违约。除了将社会中的有形资产转变为数字智能资产进行确权、授权和实时监控外，区块链还可应用于社会中的无形资产管理，如知识产权保护、域名管理、积分管理等领域。

1.5 区块链应用的要求

一个成功的区块链应用平台，应该需要满足以下要求：

①支持百万级别用户

如 Ebay，Uber，AirBnB 和 Facebook 这样的应用，需要能够处理数千万日活跃用户，在某些情况下，应用程序可能无法正常工作，因此可以处理大量用户数量的平台至关重要。

②免费使用

有时候应用开发人员需要灵活的为用户提供免费服务，用户不必为了使用平台而付出费用。可以免费使用的区块链平台自然会得到更多的关注。有了足够的用户规模，开发者和企业可以创建对应的盈利模式。

③轻松升级和 Bug 恢复

基于区块链的应用程序在进行功能迭代的时候自然需要能够支持软件升级。所有软件都有可能受到 bug 的影响。一个区块链底层平台在遭遇 bug 的时候，需要能够从 bug 中修复错误。

④低延迟

及时的反馈是良好用户体验的基础。延迟时间如果超过了几秒钟，会大大影响用户体验，严重降低程序的竞争力。

⑤串行性能

有些应用程序由于命令执行必须是顺序的，从而无法用并行算法进行实现。诸如交易所之类的应用经常需要处理大量的串行操作，因此一个成功的区块链架构需要具有强大的串行性能。

⑥并行性能

大规模应用程序需要在多个 CPU 和计算机之间划分工作负载。

2、游戏产业

2.1 游戏产业的发展

2017 年，中国游戏行业整体保持稳健发展。移动游戏进入存量市场阶段，增幅有所回落，对行业整体增长仍有较大带动作用。社会对游戏娱乐消费支出不断增加，有效带动了游戏游艺及家用游戏机行业高速发展，整体来看，2017 年游戏行业营业收入平稳提升。

随着硬件技术的提升，以及用户游戏习惯的转变，网络游戏内部结构有较大分化：移动游戏以全年约 1122.1 亿元的营业收入领先，同比增长

38.5%，占网络游戏市场份额的 55.8%；客户端游戏营业收入约为 696.6 亿元，同比上升 18.2%，占网络游戏市场比重为 34.6%；网页游戏营业收入约为 192.3 亿元，同比下降 14.7%，占网络游戏市场总份额的 9.6%。

从用户规模上来看，2017 年，中国网络游戏用户存量市场特征明显，增幅继续放缓。其中，客户端游戏用户数量约 1.5 亿，与 2016 年基本持平；移动游戏用户数量约 4.6 亿，同比增长 9.0%；网页游戏用户数量约 2.4 亿，同比下降 2.0%。

由此看来，我国游戏市场规模将继续增长，随着移动游戏市场的成熟和游戏用户消费观念的升级，网络游戏市场仍有较大增长潜力。

2.2 游戏产业的痛点

①道具不能跨游戏、跨服交易

不同游戏厂商甚至同一游戏不同区服之间的道具无法互通交易，游戏间对接成本高；

②缺乏信誉体系，交易成本高

缺乏信誉体系，用户间道具交易往往需要线下进行或者有第三方担保，费时费力。

③苹果手机游戏充值成本高

苹果公司要从游戏玩家充值的金额中抽成 30%。苹果手机对有内购的手游进行了严格的规定：玩家只能够通过苹果官方 AppStore 进行充值购买操作，不能使用第三方渠道。

④游戏经济体系不合理，可能加速游戏死亡

游戏内道具交易需要稳定的经济体系支撑，如果设计不合理，会导致游戏快速死亡。

2.3 VAO 的前景

目前大多数网络游戏基本都是基于 HTTP 协议下的，这使得去中心化从技术上不可能实现。而区块链技术的出现和不断成熟，将使得虚拟资产去中心化储存、游戏规则去中心化制定从技术层面变得可行。相比现有的网络游戏，区块链游戏在去中心化技术的支持下，玩家将拥有虚拟资产的完全产权，开发者也无法随意更改游戏的规则。游戏开发者和玩家的关系会发生根本的改变。

另外，对于苹果手机游戏充值成本高这一产业痛点，在 VAO 系统下，如果用通用的 token 来充值的话，可以节省苹果公司 30%的抽成，因此 VAO 大有商业利益空间。

目前“区块链+游戏”已经有了一些案例，仅枚举一些。

①Crypto Kitties 是第一款风靡全球的区块链游戏。它只是一款电子宠物养成游戏，玩家需要用以太币交易购买虚拟猫，这些猫其实是由不同的“代码”写成的，猫咪也因此被赋予了不同的 DNA，价值也就各不相同。这款游戏最大的特色有以下几点：游戏最开始有 100 只初代猫，之后每隔 15 分钟系统会产生一只新的初代猫；两只猫可以交配产生后代，后代的 DNA 越稀有，价值就越高；虚拟猫可以兑换成现实货币。

截至目前，虚拟猫已经卖出超过 18 万只，总价值超过人民币 1.1 亿元。而最贵的一只是 2017 年 12 月 3 日完成交易的，当时卖出 114,481.59 美元，也就是人民币 70 多万元，而现在已经升值超过 125 万元。

②Gameflip 是一个数字游戏商品平台，目前累计超过 200 万用户，不少玩家在 Gameflip 上使用比特币交易。

③Firstblood 是一个电子竞技平台，Firstblood 采用以太坊为基础的区块链，玩家可以自由交易。

④Eloplay 是一个电子竞技平台，玩家可以自由组织和参加电竞锦标赛，Eloplay 利用智能合约让玩家和知名企业组织任何规模的电竞锦标赛，奖金为数字加密货币。

3、设计理念

3.1 应用场景

区块链有着去中心化、点对点传输、透明、可追踪、不可篡改、数据安全等特点，可以用来解决现有业务的一些痛点，实现业务模式的创新。VAO 的应用场景如下：

①数字资产化

游戏内玩家账号的金币、点券和游戏装备等各类资产均可被整合进区块链中，成为链上数字资产，使得资产所有者无需通过各种中介机构就能直接发起交易。

②清算和结算

区块链技术的核心特质是能以准实时的方式，在无需可信的第三方参与的情况下实现价值转移。通过基于区块链技术的法定数字货币或者是某种“结算工具”的创设，与前文所述的链上数字资产对接，即可完成点对点的实时清算与结算，从而显著降低价值转移的成本，缩短清算、结算时

间。在此过程中，交易各方均可获得良好的隐私保护。

VAO 系统架构如图 3-1 所示：

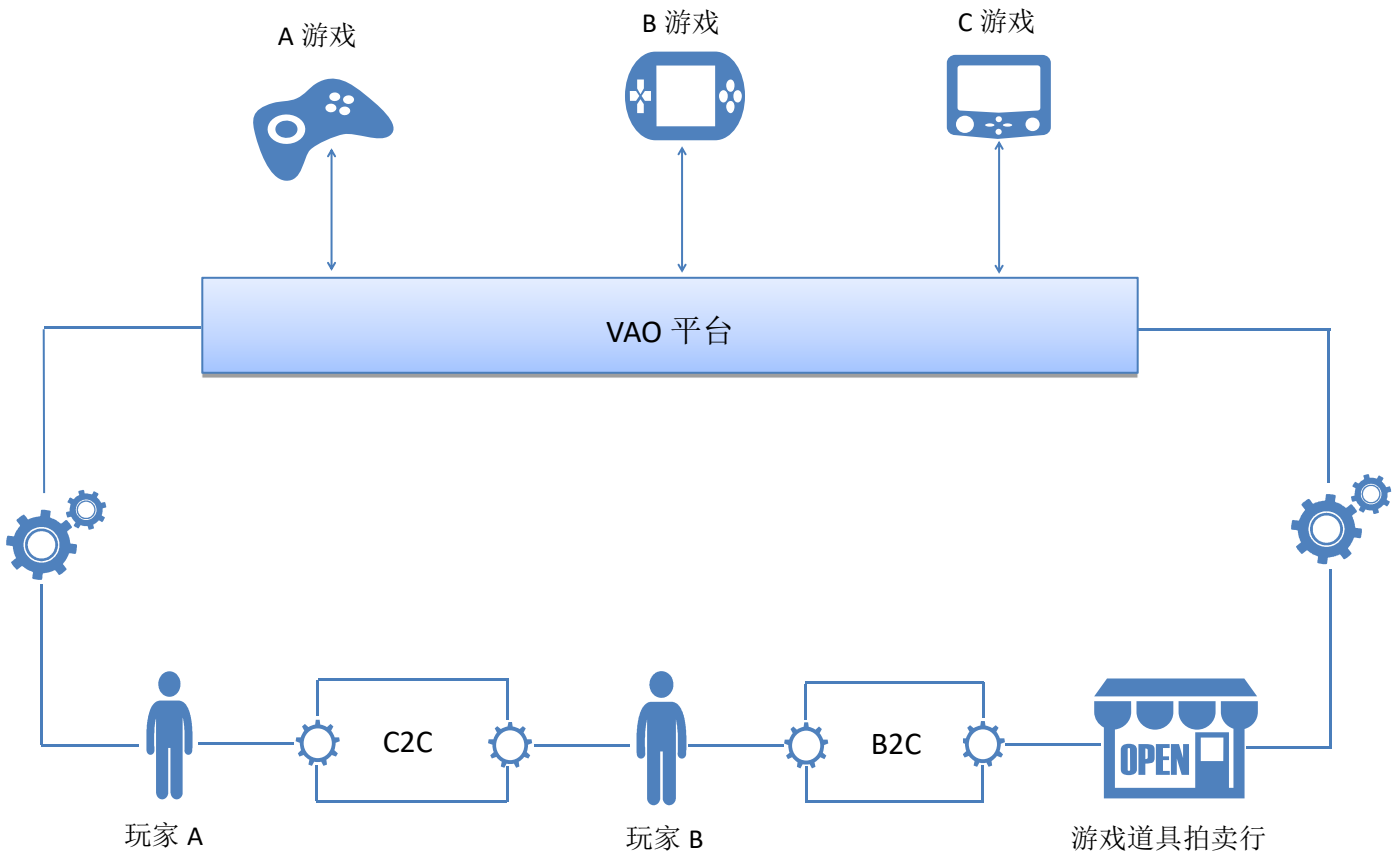

图 3-1 系统框架

3.2 VAO 的优势

①保障游戏的虚拟价值

游戏的虚拟财产无法“持有”。例如，某一款游戏的运营商发布公告称“由于运营不善，即将停服”，那么玩家自然跟着蒙受损失。归根结底的原因在于：游戏公司管理数字虚拟财产的载体是自家服务器，服务器的存在对玩家产生了制约：玩家所拥有的只是虚拟财产的使用权，而非所有权。区块链协议的不可破坏性使得链上的财产权明确，不会因为游戏服务器的停止运营而凭空消失。

②实现游戏虚拟财产的自由转移

游戏玩家的虚拟财产无法“转移”。游戏玩家在某一款游戏上花费了大量的金钱或精力，当玩家决定不玩这款游戏时，却不能将本应属于自己

的虚拟财产兑换从而用于另一款游戏。VAO 可以解决不同服务器、不同游戏间道具实现自由转移与交易，大幅提升用户活跃度和充值率，有效促进游戏品牌传播。但是“转移”的自由度取决于区块链适用游戏规模的大小，也就是说是否存在足够多的游戏同时遵循某一区块链。

③重塑游戏世界的信用体系：由信任人到信任机器

结合智能合约，可以利用区块链创建和交易独特的数字资产。信任不再是问题，因为区块链系统是去中心化的，数字商品不存储在私人服务器上，而是直接存储在区块链上，任何人都可以看到。智能合约就是区块链运行的一个协议，该协议事先由程序设定并且公开透明，譬如一个算法。此协议一旦确立，任何人为的干预都属无效。协议就像人类世界的法律，制约着社会的运行，而且协议的约束效力远远超过法律，从这个层面上讲，区块链的存在使得人们将对人的信任转为了对机器、协议的信任。

由于区块链可以用来编程记录链上任何有价值的东西，游戏世界内的所有充值、兑换交易、被奖赏、时长、余额等有价值的信息都会永久存留于链上，对于玩家而言，数据就是他们绑定的财富。玩家在进行交易行为时，也用不着去调查交易对象是否足够有信用，因为此时他们信任的不是人，不是机构，而是机器，是协议。

3.3 设计原则

在架构和实现上遵循以下的几个设计原则。

①面向业务

企业场景的特点是需求非常多样，性能要求高。在设计上首先从分析企业应用的典型用例出发，设计协议和系统功能特性，确保系统的实现能够最终适应广泛的企业需求。

②标准化

由于区块链应用场景是一种跨主体的有多方参与和协作的场景，VAO 从顶层开始设计了标准化的协议和数据结构，解决企业间数据的交互问题，避免多链并存的区块链技术演进过程中形成数据孤岛，使区块链真正地成为一种标准化的互联网价值交换和信任传递的基础协议。

③松耦合与模块化

采用模块化设计，通过定义模块间清晰的接口实现模块之间的松耦合，以此获得整个系统的良好扩展性，系统可以根据不同用户和场景的需要，采用不同的可插拔的模块组件。

3.4 VAO 的性质及主要功能

VAO 使用区块链技术完成游戏内虚拟资产的数字化。

主要功能如下：

①道具自由转移与交易

不同服务器、不同游戏间道具可以实现自由转移与交易，大幅提升用户活跃度和充值率，有效促进游戏品牌传播。

②建立游戏内信誉体系

长期的交易过程中，建立起可靠的信誉体系，维持游戏内社会稳定。

3.5 底层平台的选型

目前，Bitcoin 和 Ethereum 以及 Fabric 是区块链技术平台的三大原型。

Bitcoin 即比特币，是第一个加密数字货币，区块链技术也正是由 Bitcoin 系统引申而出。Bitcoin 是健壮稳定的加密数字货币系统。Bitcoin 系统具备以上描述的区块链技术的各种特征，分布式、去中心、去信任、数据不可篡改等。

Ethereum（中文译：以太坊） 概念在 2013 至 2014 年间由程序员 Vitalik Buterin 提出，当时的概念大意为“下一代加密货币与去中心化应用平台”。Ethereum 是一个具备智能合约功能的公共区块链平台。Ethereum 能够通过其自带的专用加密数字货币 ETH 作为手续费用支付用户在 Ethereum 的虚拟机（EVM）中部署、调用智能合约所需要的算力占用的节点。而 Ethereum 官方主推的智能合约编写语言为 Solidity，它是一种图灵完备的编程语言，能够完美运行于 EVM（以太坊虚拟机）中，这就意味着通过智能合约，用户可以实现任何业务逻辑。

Fabric 是由 IBM 和 DAH 主导开发的一个区块链框架，是超级帐本的项目成员之一。它的功能与以太坊类似，也是一个分布式的智能合约平台。但与以太坊和比特币不同的是，它从一开始就是一个框架，而不是一个公有链，也没有内置的代币（Token）。作为一个区块链框架，Fabric 采用了松耦合的设计，将共识机制、身份验证等组件模块化，使之在应用过程中可以方便地根据应用场景来选择相应的模块。

根据 VAO 的特点，区块链平台的选型主要考虑以下几个方面：

①所有人和组织都可以加入系统，即系统完全开放；

②是否能够部署智能合约；

根据①确定选择公有链为底层开发平台，Fabric 属于联盟链，因此被

排除。又由于 Bitcoin 系统不支持智能合约，是纯粹的加密数字货币系统，所以不适合在 Bitcoin 系统上做深度开发。根据②可以排除 Bitcoin 平台。最终选则 Ethereum 作为底层开发平台。

Ethereum 平台在目前主流的区块链技术平台的综合属性相对而言更加优秀，尤其在于提供的 SDK 十分丰富，能够让开发者实现各类需求。

3.6 Token 流转

利用区块链 token 的价值转换能力，游戏中将不再存在可交易和不可交易之分。除了习以为常的装备、道具之外，游戏人物的服饰、等级、宠物等都可以通过 token 进行量化交易。通过区块链技术发行 token，能够实现不同游戏间的资产交互，相比于传统的游戏交易平台，区块链技术不仅解决了中介的信任问题，还大大降低了中间成本。

当区块链中的两个用户发起一笔交易时，比如说用户 A 想要通过将游戏 a 中的某些道具（如游戏币）转换为 token 后去购买用户 B 的游戏 b 中的某些道具。那么具体的流程如下：

①用户 A 通过接口函数调用 exchange(参数 1,参数 2,…)，将 a 游戏中的道具兑换为 token。其中需要提供的参数有一个随机字符串，用户 A 的签名，用户 A 的私钥，用户 A 的账号密码，资产 ID，资产兑换数量，交易类型等。

②用户 A 发起一笔交易，通过函数调用 transferasset(参数 1,参数 2,…)，将用户 A 账户中的 token 转移到用户 B 账户。其中需要的提供的参数有一个随机字符串，用户 A 的交易签名，资产转出方（用户 A）的账户地址和账户密码，资产转移的数量，资产转入方（用户 B）的账户地址，交易类型，资产锁定脚本等。

③用户 B 在收到用户 A 转入的 token 后，在游戏 b 内，若用户 B 拥有用户 A 所期望的道具，那么就在游戏内直接将道具转至用户 A 的账户内，若没有，则可以利用 token 购买相应的道具再进行相同处理。当用户 A 确认收到期望的道具后，向用户 B 发送资产解锁脚本，如此一来，用户 B 就能够自由使用这笔 token 了。

利用同态加密、椭圆曲线等密码学技术来对用户的账户地址、交易金额、身份信息等提供密码学级别的保护，能够有效的防止第三方的信息窃取以及自身的账户风险等。

3.7 法律与合规

VAO 是一种区块链协议，没有货币方面的法律争议，不是五部委《关

于防范比特币风险的通知》所指虚拟货币。

3.8 愿景

任何可数字化的资产都可以在平台上实现登记、发行，各种主体（个人、机构）均可以在平台上登记、发行自己的数字资产。实现资产登记即公示，利于数字资产追踪查询，可以有效减少资产纠纷问题。

围绕金融、文化等行业的典型应用需求，研究提出区块链行业应用解决方案。面向基础条件好、示范效应强的行业领域，探索组织开展区块链应用试点示范工作，推动区块链技术和行业应用的融合发展。

4、用户系统

4.1 私钥、公钥、地址、账户、账户地址

①私钥：由用户自己保管且对外保密的一个 32 字节的随机数。私钥可被用来进行数字签名，是用户用来证明自己账户身份和账户资产的工具。

②公钥：公钥与私钥相对应，每个私钥都有一个与之相配的私钥。由私钥和椭圆曲线加密算法可以生成私钥对应的非压缩公钥。

③地址：地址就是由摘要算法和公钥生成的一串 26 位到 34 位的字母或数字字符组成的字符串。

④账户和账户地址：账户由不同数量的公钥组成，其账户地址就是通过公钥和摘要算法生成的签名地址。为了安全起见，账户可以由两个不同的公钥组成，一个公钥可以用作日常登录、查询等普通权限操作。另一个公钥可以用作账户转账等高级权限操作。结合隐私方案，用户可以通过公开账户地址来进行一系列的交易，同时避免了自己的信息泄露。

4.2 身份认证

用户通过 CA 认证授权实现准入机制。当一个新成员被准许加入时，他需要将自己的公钥和一些必要的经私钥加密后的身份标识信息发送给证书签证机构 CA。然后 CA 会根据用户所提交的这些信息，在核实无误后为其颁发数字证书，作为其加入联盟的许可证。数字证书包含了公钥、用户身份信息、CA 签名等一系列信息。该证书其实就是 CA 签发的对用户公钥的认证。这样就建立了用户和公钥之间的唯一对应关系。

用户在使用本系统时，需要用公钥对应的私钥对交易进行数字签名，

以此来标识交易的发起者。包含用户身份信息数字证书可以由用户存储在本地。这样一来，第三方无法获知用户的身份信息。

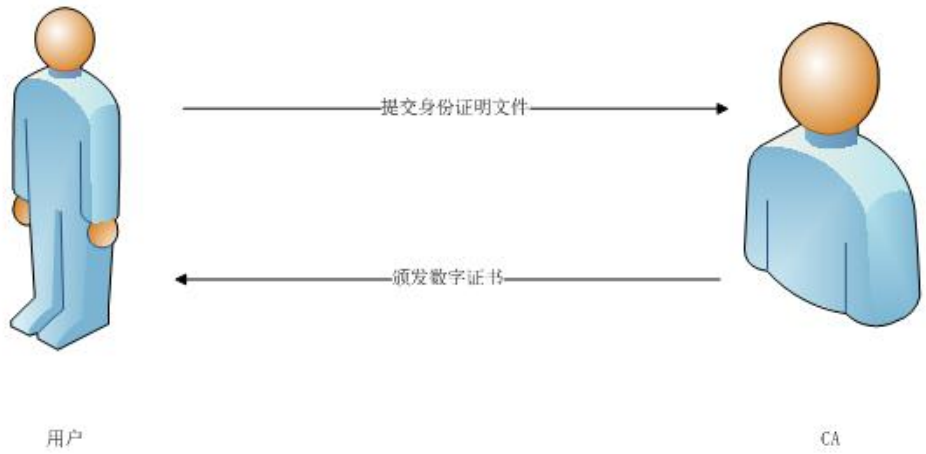

图 4-1 进行身份认证

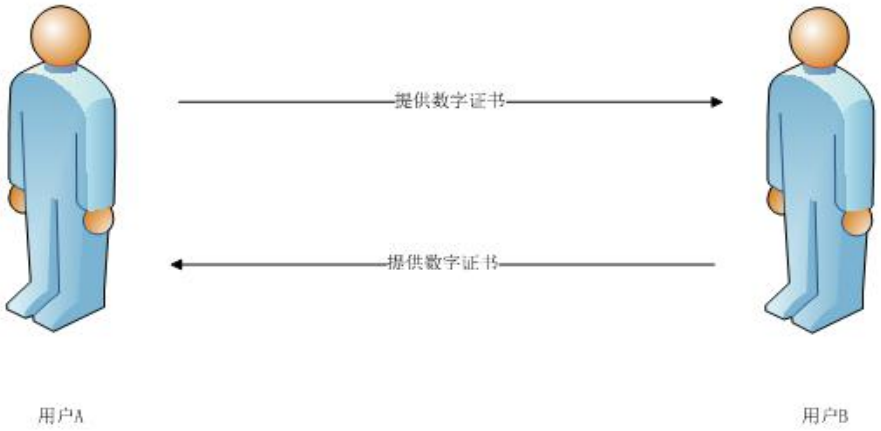

图 4-2 交易时提供数字证书

4.3 隐私保护

采用同态加密来实现账户余和交易金额的加密。同态加密是基于数学难题的计算复杂性理论的密码学技术。同态加密简而言之，就是对明文进行处理之后的结果与先对明文进行加密再对密文进行处理得到的结果是完全相同的。同态加密的这个特性，可以使得在不知道用户的账户余额和交易金额的前提下，能够对交易的合法性进行验证，并将通过验证的交易记录到区块链上。

采用群签名将区块链上的交易用户的身份隐匿起来。群签名是指一个

群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名。与其他数字签名一样，群签名是可以公开验证的，而且可以只用单个群公钥来验证。

5、交易

交易是指 VAO 系统中引起资产的权益发生变化的事务。VAO 系统内设计了多种交易类型，每一笔交易都包含输入列表、输出列表、签名列表以及与交易类型相关的特定数据。

5.1 资产相关交易

5.1.1 资产创设

根据用户游戏账号内的各类资产发行数字资产。创设资产需要消耗一定数量的“结算代币”作为附加服务费。

5.1.2 资产分配

在资产创设所设定的总量上限范围内，在游戏玩家指定的地址中生成该玩家等价的数字资产。资产分配可以一次性完成，也可以在任意时间内分批完成。

5.1.3 资产变更、注销、冻结

多款游戏之间支持资产变更的功能，即游戏玩家可以从某款游戏将资产转移到另一款不同的游戏内。同时支持资产的注销和冻结功能。有时，智能合约的行为会发生异常或不可预知，无法按照预期执行：有时应用程序或账户可能发现一个漏洞，使其消耗不合理的资源。当此类问题不可避免地发生时，区块生成者应当有能力纠正这种情况。

所有区块链的区块生成者有权选择哪些交易被包含在区块中，从而使他们有冻结账户的能力。如果区块生成者滥用权利，他们就被淘汰，账户将被冻结。

5.2 转移、交换资产相关交易

5.2.1 合同交易

合同交易可以指定所有参与方的交易，并可以根据参与交易的资产类

型判断是否要求对方确认接受，例如同一款游戏内不同游戏玩家之间进行交易时，对方可以选择接受或拒绝。

5.2.2 委托交易

不指定对手方，由代理人负责完成交易。例如某游戏玩家在不同游戏之间进行资产转移时，代理人根据玩家的委托单来完成交易。委托单信息包括：代理人，交易物，交易总量，交易价格，委托人，签名列表等。

5.3 记账相关交易

5.3.1 登记、撤回候选记账人

用户应在登记成为候选记账人之前就做好记账的技术准备。希望登记为候选记账人的用户，需要支付一笔附加服务费。

5.3.2 选举记账人

详见记账机制。

5.4 交易费用

交易费用分为基本字节费和附加服务费。其中，附加服务费会被销毁，成为未分配的部分，参与未来分配；基本字节费支付给记账人作为记账奖励。

5.4.1 基本字节费

基本字节费是因交易占用传输带宽和区块链字节所产生的费用。

基本字节费和交易的字节数正相关，由记账人收取。记账人可自行决定是否收取以及费率标准。

5.4.2 附加服务费

需要支付附加服务费的交易类型为：资产创设、资产变更、资产注销、资产冻结、候选记账人登记。

5.5 交易确认

一笔交易平均 2 秒后，会被写入区块链中，同时被所有出块节点知晓这笔交易。这就意味着只需要 2 秒，一笔交易可以认定为 99.9%被区块链接收了。

有一些非常情况下，例如，软件 bug，Internet 拥塞或恶意出块者出

现，区块链可能出现分叉。在分叉产生的 9 秒钟内，出块节点就可能发现这个分叉并警告用户。一个节点观察网络的时候如果发现连续 2 次的丢块事件，这意味着该节点有 95%的可能性在区块链的分叉分支上。出现 3 个连续的丢块以后，该节点有 99%的可能性在一条分叉出来的区块链上。解决办法是生成一个预测模型，利用节点丢失的信息，最近参与率以及其他因素来快捷地警告用户出现的问题。

5.6 交易证明

要求每笔交易都包括最近的区块头的哈希，这个哈希有两个目的：

①防止分叉区块链上出现大量交易记录；

②使得系统能够感知到用户是否在分叉出来区块链上。

6、记账机制

6.1 区块链记账原理

区块链就是一个不断增长的全网总账本，是由一个个区块构成的有序列表，每一个区块中记录了一系列交易，并且每一个区块都指向了前一区块从而形成了一个链条。这样的区块链就构成了一个便于验证的（只需要验证最后一个区块的 Hash 值就相当于验证了整个账本），不可更改的（任何一个交易的更改都会让之后的所有区块的 Hash 值发生变化，这样就无法通过验证）账本。

一个完整的区块链包含了自创世区块以来所有的交易信息，依次执行这些交易就可以得到当前所有资产的归属和状态。

区块链的分布式账本技术缩减了信息传递的环节与层级，提高了效率。这种分布式账本，避免了中心化的第三方，保证了交流的直接快捷。链上交易数据的公开保证了系统的公正性和透明性。密码学的应用提升了安全性，为敏感隐私信息的安全提供了保障。共识机制使得所有的记账节点间达成共识，从根本上杜绝了造假的可能。

6.2 共识机制

共识机制使得所有的诚实节点能够保存一致的区块链视图，同时满足：

①一致性。所有诚实节点保存的区块链的前缀部分完全相同。

②有效性。由某诚实节点发布的信息最终能够被其他的诚实节点记录

在自己的区块链中。

本系统通过投票选举记账人机制，来决定记账人及其数量；被选举的记账人通过简化的拜占庭算法对区块的内容进行共识，来验证其中的交易。

6.2.1 记账的特点

本系统主要通过各节点持有的代币数量的多少来决定是否拥有记账权。记账节点没有更改交易数据的权利，只能验证交易的合法性。一旦节点造假，它将损失一定数量的代币作为惩罚，以此来规范节点的行为。

本系统的记账区块链的特点：

①20 秒左右的出块速度。

②区块的共识需要全体拥有记账权的节点参与，只有确认后才能提交到区块链上。

③记账人可以放弃参与记账的权利，此时由候选记账人补上。

④记账人不能人为地拒绝某笔交易进入区块中。

6.2.2 选举记账人

本系统会根据节点的数量来动态调整记账节点的数量。当系统中节点的数量不超过 200 时，将节点数量的一半选举为记账节点。当系统中节点的数量大于 200 时，固定选择 100 个节点作为记账节点。这样一来，通过缩减参与记账的节点的数量，能够加快共识的达成速率，提高系统的效率。

本系统会在每一个周期（100 个区块）的开始时选举记账人。系统根据每个节点拥有的选票数和节点拥有的代币数量按照某些规则来对节点进行排序，具体如下：

①一个代币一票，节点可以给某个节点投多票，但是一个代币不能给多个节点投票。

②节点的得票数=选票数*80% + 自身代币数*20%。

③按照得票数进行排序后，根据节点的数量选出记账节点，记账节点之外的排好序的节点均为候选记账节点。

当记账节点放弃记账权（突然掉线等），就由候选记账节点中排第一的节点转为记账节点。

6.2.3 对区块所包含的交易达成共识

选举出的记账节点中排第一位的就自动成为主节点，由该节点来收集系统中发生的所有交易，同时由主节点打包交易区块。

当交易区块生成后，就将交易区块广播发送给记账节点。在记账节点间通过运用简化的拜占庭共识算法来对交易区块达成共识。具体如下：

①当每个记账节点收到区块后，对区块中每一笔交易的合法性和正确性进行验证，全部通过之后对该区块进行签名，然后广播 commit 消息给所有的记账节点。

②其余记账节点在收到 commit 消息后，对签名进行验证，当有超过 2/3 多数正确的 commit 消息后，广播发送 commit-ensure 消息。

③其余节点在收到 commit-ensure 消息后，验证该消息，当收到 2/3 多数的 commit-ensure 消息后，就将区块添加到本地区块链中。此时，共识达成。

6.2.4 对代币分配达成共识

每个区块中都包含了一笔特殊的交易，用于将一定数量的代币分配给参与记账的节点。其中记账节点数量为 N，代币数量为 M，那么主节点就分得其中的（M/N）*1.2，其余记账节点均分剩余的代币。

7、总结

VAO 使用了区块链技术来完成了游戏资产的注册登记、转让交易、清算结算。通过将游戏资产数字化，实现游戏道具自由转移与交易，建立游戏内信誉体系等，使得游戏玩家的虚拟资产的财产权益得到保障。