# V SYSTEMS：区块链数据库及应用平台

英文原文由 Sunny King、Kate Shan、Rob Zhang、Scott Nadal 撰写
2018 年年 9 月 16 日

本中文版由 V SYSTEMS 社区爱好者翻译，请在 http://www.v.systems 阅读英文原版

## 背景

我们会时常记起，互联网的诞生 —— 可以说跟工业革命或信息时代到来同等重要的一个科技事件 —— 发生在仅仅不到 30 年前。走在中国城市的大街小巷中，似乎每个人都要时不时地翻看一下他们手机。这就是互联网无孔不入的普及带给我们生活的改变。近年来，人工智能已在我们社会中有了无数的实际应用，而它在围棋领域已经远胜于人类冠军 [Silver 2016]。还有人提到，作为量子时代即将到来的信使，"量子霸权"（Quantum Supremacy）即将出现在不远的未来。 似乎互联网的创造，就像电脑一样，已经属于了一个古老的过去。 作为一名技术人员，有时候不得不赞叹人类文明的巧思以及它所能够取得的惊人的进步速度。

相对而言，中本聪所宣布的比特币 [Nakamoto 2008] 所带来的影响并不如之前提到的那些技术突破来得大。相反，它一直受到很多的质疑。而这也表明了中本聪的思想远超过了他所在的时代。然而，他的杰作所带来的影响已然日益增加。到 2017 年，随着比特币价格突破 1 万美元大关，区块链技术也被广泛接受为一个主要的技术创新及颠覆者。即便如此，区块链技术所带来的影响可能仍然被低估了。事实上，我们可以认为，区块链为我们带来了一个具有强私有财产的世界，其对人类未来可能有着极为深远的影响。简要回顾人类文明史就不难发现私有财产是其基础支柱之一。因此，可以认为区块链技术将会给世界带来的影响会比工业革命还要深远。基于这样的理念，我们将这一新经济时代称为虚拟经济时代（Virtual Economy Era），并将我们平台的基础代币记为 VSYS 为向中本聪的比特币致意，我们内部将 2009 年记为虚拟经济元年（V.E.1）。

但人们应该对比特币和区块链技术加以区分。 拜占庭将军问题 [Lamport 1982] 是以前计算机科学中的一个困难的分布式共识问题，而比特币是其第一个实际可行的解决办法。区块链技术派生于中本聪发明的支撑比特币网络运行的底层算法。如今，被广泛接受的看法

是区块链技术包含了所有相似的网络，不论公有的还是私有的，只要在其共识模型中有一定程度的去中心化现象。
比特币被设计成虚拟货币。 比特币区块链存储的是它的账本，用以确定每个比特币的所有权。 2011 年，Namecoin 的出现标志着在区块链中存储其他类型信息的第一次尝试。 其后有很多将比特币区块链作为数据存储用于各种应用目的的尝试。 但是，比特币通常不鼓励这种用于存储的做法，因为比特币不是为此而设计的，它会使得这种做法困难且昂贵。

不过，区块链技术一般来说应该被看作是一个分布式的数据库系统。这意味着，世界上很大一部分数据可能存储在这样的系统中，就像传统的关系数据库和最近的云数据库一样。 在本文中，我们将探索区块链技术的这一方面，并证明区块链可以成为未来数据库非常有竞争力的选择。

## 引言

由于比特币不是为一般的数据使用而设计的，所以试图将比特币区块链作为一个数据存储仓库已被证明是困难和昂贵的。 为了让其区块链不被用作数据存储，比特币协议将合法的数据使用限制在每笔交易 100 字节的范围内（这个限制改变了几次，但数量级本质上是相同的）。虽然也存在通过将数据拆分成较小片段来存储数据的方式，但是其不可避免地引入了过多复杂性与开销，从而非常困难和昂贵。 比特币有意引入这个限制是因为适应数据使用是与系统性能相冲突的。提高比特币区块的最大容量限制是一场漫长的斗争与戏剧性博弈，也反映了该技术固有的可扩展性限制。 为了促进数据的使用，它会导致有限的存储资源被更多地消耗，同时还将降低系统的最大吞吐量。

可扩展性问题源于以下事实：与以前的分布式数据库不同，比特币是一个极其冗余的系统。 比特币网络的每个完整节点都有比特币区块链的一个完整的数据集，也必须完全地验证整个区块链。 这样的极端冗余带来的成本是我们可以看到的其对可扩展性的影响。 比特币最初通过一个称为轻量级验证的系统来处理冗余，通过巧妙地将交易组织到 Merkle 树数据结构中，使用户仍然可以按去中心化的方式仅使用轻节点来达到区块链共识。 这个技术显著降低了比特币网络的冗余度。 目前，比特币网络中轻节点数量远远超过全节点的数量。

后来，Blockstream 建议可以将应用程序移动到侧链上[Back 2014]。 为了维持一个以比特币为中心的世界，他们在这一方案中提出了一个比特币的锚定系统。

以太坊则建议通过分片处理冗余。 分片是分布式的数据库技术将大型数据库分成更小的

“碎片”，这些碎片存储在不同的节点。 这个系统引入了分片可用性降低的风险。 为了应对这种风险，以太坊可能需要多个存储了整个区块链的高度可用的全节点。

Plasma [Poon 2017] 最近的一篇论文提出了另一种可扩展性的解决方案。

## V SYSTEMS 平台：重构区块链技术

据估计，现在已出现了数以万计的区块链项目，甚至还会更多。 对于许多想要进入区块链行业的个人和团队来说，开发和维护区块链系统的成本已经成为一个巨大的挑战。 现在是时候将区块链技术作为一个整体来重新加以审视了。 如果我们能够在提高可扩展性的同时大幅降低区块链技术的成本，这将会为区块链技术带来更多创新用途并加速其被广泛地接受。

### 区块链作为数据库

区块链技术所带来的主要模式转变是去中心化。 我们应该从这个新视角来看一下区块链数据库。

一般来说，传统的用户账户在区块链中可以用公钥和私钥地址代替。 通常，传统数据库有很严格的访问控制， 几乎所有的数据都只限于经过认证的帐户。 在传统的数据库中，帐户创建是中心化的。 也就是说，数据库管理员授予用户一个访问帐户。通过区块链，任何人都可以自由生成密钥对，而无需中心化管理。除了以加密形式存储的数据之外，区块链中的大部分数据都是公开的。 即使是在组织内部局域网搭建的私有区块链，其未加密的数据仍然应该被视为公开的，因为非法入侵局域网总是不可避免的。 所以隐私的保护依赖于虚拟身份的匿名性。有趣的是，与中心化模式相比，这可能实际上是一个更强的隐私保护策略。在中心化模式下，我们经常会听到有关因黑客攻击而丢失客户数据的情况。

如果一个应用程序需要某种形式的集中管理呢？ 这可以通过客户端/节点软件内的业务逻辑来加以实现。 被称为管理员的特权密钥对可以被内置到客户端软件中。 然后，管理员可以选择标记那些违反服务协议的密钥对为违规者。 管理员也可以标记特定的数据以作审查。 违规者的数据或不适当的或非法的数据将被节点软件视为无效。

值得注意的是，由于违规者数据仍然允许进入区块链，只是不被官方节点软件所承认而已，所以这类中央审查是一种弱形式的审查。

如果有应用程序需要客户身份识别功能呢？ 通常这种应用程序在账户激活使用前需要用户按开户条件通过身份认证。也可以通过引入通过身份认证的公钥的白名单在客户端/节点软件内实现这一功能。 只有来自该公钥列表的数据才能被该软件识别。

考虑到上述概念，现存的一大部分数据库都可能适合于迁移到区块链数据库中。

V SYSTEMS 平台将数据库中的元素视为对象（objects）。

如下是一些基本对象的例子：

- 公钥：用户所产生密钥对的公开部分
- 地址：公钥的一种缩简形式
- 虚拟身份/化身：与供临时使用的公钥相比，为长期使用身份
- 组织：每个身份与多个虚拟身份/化身相关联，并由多个虚拟身份/化身所管理
- 可替代物：可替代属性的虚拟资产/代币，如货币、股份等
- 账号：身份所拥有可替代物的容器，类似于银行账户。注意其与传统数据库用户账户的区别。

如下是一些基本关系的例子：

- 所有权：身份与对象之间的关系
- 创建关系：对象与创建对象的身份之间的关系
- 发行关系：代币发行者与可替代物之间的关系

如下是一些基本的用户数据库操作：

- 创建数据库
- 插入对象
- 更新对象
- 删除对象
- 创建索引
- 按索引键值查询

JSON 格式的对象是非常强大的表现结构化数据的数据结构。键值对（key-value pair）可以认为是对象的一个简单例子。需要注意的是，键值对中的键（key）与虚拟身份的公

钥（public key）不是同一事物。因而，有时为了避免混淆会将"键值对"称作"名值对"（namevalue pair）。数据库的键空间或名字空间既可以是用户本地的，也可以是全局的。

在所有权类型的数据模型中，数据对象可以认为是由插入该对象的身份所"拥有"，即对象仅可以被其所有者修改或删除。对于全局命名空间而言，存在着命名空间解析问题。它也可以理解成全局惟一性约束问题。当一个用户试图插入一个键值对时，另一用户可以在广播中看到相应的键（或名），因而可以插入使用相同键（或名）的一个竞争键（名）值对。该竞争键值对有可能抢在原键值对之前被区块链确认。Namecoin 引入了一个解决该问题的协议，其基本思路如下：

- 用户发送一个预插入（pre-insertion）预订交易，该交易中键（或名）通过哈希隐藏。协议规定预订交易将为插入给定的键保留一定操作时间。
- 等待预订交易确认。
- 预订交易确认后，将实际插入交易广播到网络中去。插入交易应当包括有一个指向预订交易的链接/引用以便协议验证其与预订交易相互吻合。

由于别的用户在预订交易被广播时无法得知相应的键（或名），他也就不能抢在该键实际所有者之前完成该键的插入，除非在插入交易被广播后发生了区块链重整（reorganization）现象。

然而，这仍然不能阻止恶意用户猜测其他用户所要插入的键并抢先插入，如同域名系统所遭遇的一样。

所有权可以进行转让。对象的所有者随着转让交易而发生改变。

在默认情况下，只有对象所有者可以对其进行修改或删除。但也要考虑其他一些允许更多灵活性的模型。例如，一份文件或 Wiki 应用或许并不需要为每一个数据记录标明所有权。

一旦对象被插入，所有人都可以自由地对其进行修改或删除。另一个可能模型为使用身份白名单，只有对象的白名单成员可以对其进行修改。

**高级数据库功能**

V SYSTEMS 平台还计划引入高级数据库查询功能。类似于 MongoDB 的对象-关系型查询语言比传统关系型查询模型（即 SQL）更加灵活。谷歌 MapReduce 也给出了一种新的数据处理形式。

**数据库迁移**

作为一个数据库，迁移功能通常被认为是重要的。随着数据库的扩展，应用数据可以迁移到应用自有的独立区块链上去，区块链手续费可以针对性降低，这将使应用更加节省费用。V SYSTEMS 平台将会提供迁移工具供数据库在区块链间迁移使用。

**模块化目标**

模块化是降低系统复杂性及减少未来开发维护费用的一个重要的设计目标。这一设计不仅仅是为了 V SYSTEMS 平台本身，也是为了在 V SYSTEMS 生态中运行应用的其他区块链。

协议分层：

- 共识管理层
- 区块树（Block tree）管理层
- 链间（Interchain）处理层
- 交易处理层
- 数据格式层
- 对等网络层
- 互联网协议层

系统组件：

- 可插拔式共识模型
- 可插拔式业务逻辑容器
- 数据库管理组件
- 数据库操作组件
- 数据库查询组件
- 共享对等网络服务
- 进行区块链处理的全节点

- 智能手机端轻节点冷钱包
- 智能手机端轻节点热钱包
- 浏览器端钱包

**共识系统**

最初的比特币工作量证明共识机制现在被称为中本聪共识。中本聪共识是一个标志性突破，是一切的开始。 8 年多的运行，比特币系统无疑证明了它的可靠性。

协议分层
共识管理层
区块树管理层
链间处理层
交易处理层
数据格式层
对等网络层
互联网协议层

质数币 [King 2013] 介绍了基于质数的工作量证明共识机制，我们称之为质数币共识。质数币共识是第一个也是唯一一个能在挖矿同时得到有趣副产品的共识系统，达成网络共识的同时具有可预测的安全级别。 质数币已经可靠地运行了 4 年多时间。

股权共识（Proof-of-Stake）首先由点点币引入[King 2012]。 与中本聪共识或质数币共识中基于消耗的计算资源来分配权重相比，股权共识的主要区别是通过参与共识的代币持有量来分配权重，因此也被称为区块铸币（block minting）。 这种算法将共识安全级别与能源消耗级别从系统中分离出来，消除了达到共识所需要的能源消耗，从而解决中本聪共识中的能源消耗问题，同时降低整个系统的运营成本。

股权共识是一个重大突破，因为它显着降低了区块链技术成本和进入壁垒，从而让大量的多元化区块链生态系统得以实现。 我们相信在未来的某个时候，世界上运行的区块链的数量可能超过世界人口的总数。 股权共识正是区块链技术能达到如此巨大规模应用的使能技术。

有几个主要的区块链网络已经运行了数年的股权共识系统，相互之间有一些区别。 股权证明共识已经很好地证明了自己。V SYSTEMS 平台计划至少实现以上三种已被证明过的创新性共识机制。

当然还有其他共识机制。随着项目推进，V SYSTEMS 平台也将评估其他共识机制的可靠性。

具有创新性与可靠性的共识算法都将是 V SYSTEMS 平台可能实现的候选者。

**主链-侧链模型**

V SYSTEMS 平台引入了独特的主链与侧链模型。

区块链 S 被称为另一区块链 M 的一条侧链，如果 S 满足:
• 感知性（Awareness）：S 的全节点同时也是 M 的全节点，并对 M 的所有交易进行处理
• 同步性（Synchronization）：S 遵守与 M 的抽象时钟同步
相应地，M 被称为 S 的主链。

抽象时钟同步处理两个区块链之间的区块排序问题。设想区块链为一个抽象的时钟，其每一个区块为一个时钟滴答。称其为抽象时钟，是因为它与写进区块的本地时间戳并无关系。时间戳是局域数值，不能全局地决定事件的正确顺序。而区块链中的区块高度可以决定一个全局时间序列。观测者可以放心地认为前一个区块中的事件总是在后一个区块事件之前发生，不论两个区块的时间戳如何。

当一个侧链区块产生时，它将链接到主链上最新的区块，以其作为主链父区块（mainchain parent）。允许多个相继产生的侧链区块共享同一主链父区块。这种主链-侧链间的父子关系必须也是保序的（oder-preserving）。

主链-侧链模型使得我们可以在两个区块链之间开发一种专用通信方式。与 Blockstream 的方案不同，我们的模型不需要侧链锚定，从而给侧链项目更多可以创新的自由空间。

**云特征**

V SYSTEMS 平台计划提供为应用建立区块链所需的工具包。区块链模板制备（template preparation）允许用户从不同协议参数及可插拔组件（如共识模型）中进行选择。

一旦定下模板及选项，V SYSTEMS 平台提供的工具包甚至可能在应用所需具体业务逻辑尚未完全开发之前即为应用部署好一个全新的区块链。

**智能合约**

智能合约 [Szabo 1996] 允许各方在没有可信第三方的情况下创建具有约束力的协议。比特币在验证交易时使用了简单的脚本系统。 但是由于担心潜在的问题，这个脚本系统有很强的限制性，只能进行标准化交易。 后来，以太坊 [Buterin 2014] 重新设计了一个智能合约系统，拥有称为 Solidity 的图灵完备的编程语言。 这是区块链技术的一个重大进步，使得在许多应用场景中可实现可自动执行与去中心化的智能合约。

EOS 最近提出使用 WebAssembly 来实现另一个被称为 Wasm 的智能合约系统。

Wasm 是浏览器内部客户端低级脚本语言的新兴 Web 标准。 Wasm 通常通过 C 或 C++ 开发后编译得到。

V SYSTEMS 平台计划以兼容方式同时支持以太坊和 EOS 类型的智能合约。 虚拟机将以模块化方式实现，以便应用程序可以选择启用其偏好的智能合约类型。 V SYSTEMS 平台也将评估和考虑越来越多被开发出来的竞争智能合约系统。

**可扩展性**

许多团队针对单个区块链上的可扩展性限制花费了大量的精力。 虽然其中一些可能是值得注意的，但我们相信可扩展性的最终解决在于无限数量的区块链生态系统。 如前所述，我们的愿景是一个可能同时运行着数十亿块区块链的世界。V SYSTEMS 平台允许不同的应用程序必要时可以在不同的区块链中运行，从而实现与同一生态系统中其他应用系统的完全可扩展性隔离（scalability isolation）。

**可用性**

可用性一直是限制加密货币被广泛接受的一个瓶颈。V SYSTEMS 平台计划开发基于浏览器的钱包以及智能手机上具有现代用户体验和高安全性的移动轻节点钱包。 冷钱包会做到

让每个人都可以轻松使用，让用户安心无忧地管理自己的虚拟资产，免除来自网络黑暗角落的威胁。

## 结论

V SYSTEMS 平台旨在大幅度降低区块链技术的成本，增加区块链作为数据库平台相对传统数据库系统的竞争力。 我们的愿景是，区块链的未来不仅在于某些数十亿美元区块链，更应在于数十亿块区块链之中，而这将为全球带来一个新的经济时代。

## 参考文献


[Back 2014] Enabling Blockchain Innovations with Pegged Sidechains, https://blockstream.com/sidechains.pdf

[Buterin 2014] Ethereum: A Next-Generation Smart Contract and Decentralized application
Platform,
http://www.the-blockchain.com/docs/Ethereumwhitepapera_Nextgenerationsmartcontractanddecentralizedapplication_platform-vitalik-buterin.pdf

[King 2012] PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, https://peercoin.net/assets/paper/peercoin-paper.pdf

[King 2013] Primecoin: Cryptocurrency with Prime Number Proof-of-Work, http://primecoin.io/bin/primecoin-paper.pdf

[Lamport 1982] The Byzantine Generals Problem, http://lamport.azurewebsites.net/pubs/byz.pdf

[Nakamoto 2008] Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

[Poon 2017] Plasma: Scalable Autonomous Smart Contracts, https://plasma.io/plasma.pdf

[Silver 2016] Mastering the game of Go with deep neural networks and tree search,
https://storage.googleapis.com/deepmind-media/alphago/AlphaGoNaturePaper.pdf

[Szabo 1996] Smart Contracts: Building Blocks for Digital Markets,
http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwint
ersc hool2006/szabo.best.vwh.net/smartcontracts2.html