WISEDOM BLOCKCHAIN WHITEPAPER

智慧链技术白皮书

目录

Wisedom 智慧链

智能数据资产互联协议

摘要

Wisedom Blockchain（简称“智慧链”或“WDC”）致力于实现智能数据资产互联基础区块链生态系统，是一个实现生活设备物联，生活信息互联的一种全新的基于区块链技术的智能合约通信平台。旨在为人们众多的智能物品提供分布式的数据连接以及身份验证、数据资产交换等服务。智慧链作为底层的支撑系统，以社区自治的公链形式部署，最终支持多链并行的运行结构，支持多层通信协议，包含设备互联协议、终端数据共享协议以及身份验证协议和即时通信协议等。

智慧链的设计在于将区块链技术真正应用到人们的日常生活中，在技术组成的设计中，侧重安全可靠的算法和数据结构，采用底层 PoW 与上层 PoS 的混合共识机制，充分保证网络自治的公正性，对于密码算法的应用也会经过一个从 ECC 到后量子密码算法的迭代过渡，提供网络的抗破解能力，对于脚本指令层，设计为特定功能指令集，从执行系统底层防止可能的缺陷漏洞的发生。

智慧链，一个智能数据资产互联协议。

1 智慧链的设计理念

1.1 设计目标

信息化的发展，将人类对于数据的处理能力带入到了一个全盛的时代，数据共享以及网络服务极大的提升了人们的生活水平，促进了社会生产力的发展。多年来产生了无数的信息化管理系统以及互联网应用，所提供的服务已经渗透到了人们生活的方方面面。然而，互联网本身依然在进化，数据共享和网络服务并不是互联网的终点，当经济社会由数字构成的时候，互联网的内在价值就开始进一步的发生迭代了，通过网络不仅仅是共享数据，而会使得数据带有一种依附于网络的价值，并且这个价值可以流通，通过这种价值数据的传递，构建新型的数字经济形态，这种下一代的网络，我们称之为价值网络，在价值网络中可以承载数字资产的运行。

区块链技术是实现价值网络的支撑技术。

价值网络不再满足于数据的传播，而更加关注数据资产的部署以及传递。而当价值网络技术与实际的生活应用结合，将会产生更大空间的新型应用，这种应用是附带价值和所有权的数据应用，而非传统的数据共享式应用。人们在生活中会产生各种各样的个人数据，如个人物联设备信息、个人作品、个人资产所有权以及个人医疗和个人生活习惯数据等，这些数据都是属于个人的数据资产，而这些数据又会

与其他人进行交互，产生社交、设备数据共享、身份信息验证以及数据资产交换的需求，这些需求在现有的互联网模式下，不能很好的解决信任、存证、隐私以及价值公证的问题。

智慧链，就是为了解决这个问题而设计。

智慧链的设计目标包含两个主要的方面，如下所示：

1）、构建智能生活时代的个人数据登记以及交换的基础链系统

2）、构建基于链的个人数据应用，促进人们的生活质量与效率

1.2 使命愿景

“我们的愿景是促进人们的生活数据资产化，通过实现个人生活数据资产化的交换流通，打造深度挖掘个人数据价值的区块链服务网络”。

智慧链将创建面向个人生活数据的特定区块链系统，一切围绕着为人们的智能生活服务，通过去中心化的网络形式，基于社区共识的应用协议，通过内建的资产交换机制激励体系的运行，为本地和全球的人们提供一种生活应用服务。我们相信，任何一个系统的最终价值都需要体现到人们的生活中来，都需要体现到生产力的促进中，当人工智能、物联设备、个人数据、数据系统通过智慧链衔接起来的时候，我们可以创造真正的价值。

提高人们的生活质量，推进价值网络的发展。

1.3 创新要点

1.3.1、安全脚本系统

脚本系统是是区块链系统中的驱动器，正是通过脚本指令，才可以进行各种数据资产的生成与转发，各项交换规则以及验证规则也都是通过脚本来实现的，因此脚本系统的安全性至关重要。理论上对于运行资产数据的区块链系统，其安全性需要达到银行级的要求，这个安全性必须在架构设计一级上保证。智慧链的脚本系统在设计上会遵循如下准则：

1）、数据资产的转换传递需要外部触发，不能通过脚本内部触发，防止程序内部问题导致用户的数据资产损失；

2）、限制近似数值的定义，防止计算过程导致的误差

3）、设计功能约束的指令，避免脚本程序自定义开发带来的扩展性问题

对于底层调用以及数据资产相关的操作，智慧链提供一组调用库以供外部程序实现，在整个脚本指令的设计中，保持受限的编程能力，对于智慧链来说，功能场景是特定的，因此脚本指令的功能也是特定的。

安全性是智慧链首要的保证。

1.3.2、支持动态共识

在智慧链的第一阶段，采取的是 PoW（Proof of Work，工作量证明）+PoS（Proof of Stake，权益证明）的混合共识。这是在综合目前的共识模型发展的基础上，确定的相对公正而安全的机制。随着智慧链的发展，共识机制必然会有相应的变动以适应未来的变化。为了适应这种变化，需要引入动态共识机制，共识模型的选定和激活，不是由开发团队单方决定，而是通过设计社区投票决定的机制，将这个决定权交给社区，开发团队仅负责提供功能模块。

动态共识的设立，是智慧链维护社区公正性的一项机制，对于一个面向公众的数据资产服务系统，系统核心机制的设置将充分交付给社区。

1.3.3、应用模板

智慧链支持通过脚本程序开发业务应用，并部署在链上，基于链的开发与传统面向服务器的开发有很大的不同，同时开发过程会调用到开放的 API，为了方便技术人员开发应用，降低部署门槛，同时也为了能够让更多社区成员参与智慧链的应用开发，在主链的应用支持模块中，将提供标准的应用模板支持，开发人员可以在模板的基础上进行扩展开发，提高开发效率。

应用模板是智慧链开发生态的重要组成部分，也是对开发友好的一个方面。

1.3.4、后量子密码技术

在第一阶段，智慧链会使用椭圆曲线加密算法作为密码体系，在以下章节中会介绍智慧链具体采用的 ECC 算法。这里要阐述的是，在智慧链的技术迭代过程，会提前设计对于抗量子计算的支持。目前区块链系统中所使用的密码技术包括 ECC，是互联网中广为使用的核心安全协议，这些密码技术的理论成熟，已经运用了数十年，然而这几年量子计算的发展迅速，随着量子计算的高速发展，传统密码体系越来越面临着被全面破解的威胁。时至今日，IBM 和 Google 已经研制发布了 50 和 72 量子比特的原型机，也宣告了量子计算从理论到应用实质性的进展。

区块链系统中的账户地址、智能合约签发、交易事务签发等，都依赖于密码技术的安全性，因此智慧链在技术迭代中会从椭圆线算法升级到抗量子密码算法。抗量子密码算法目前有多种体系，如基于 HASH 函数的数字签名、基于纠错码的密码、基于格的密码以及多变量公钥密码学。如下所示：

图 1 抗量子技术体系

如图1所示，这是目前的抗量子技术体系，从公钥的规模以及计算性能角度，在智慧链的迭代技术进程中，将考虑使用基于Hash函数的公钥签名体系以及基于格的密码。一个格定义为n个线性无关向量b1,…,bn∈Rn的一个整线性组合。基于格的困难问题有：最短向量问题、最近向量问题以及最短独立向量问题。基于格的密码体系可以有效的抵抗量子计算。

1.3.5、内置多链

智慧链在生态的设计中，将会支持从资产通证定义到资产数据的应用等多层次的业务功能体系，整个网络系统将会按照业务功能的划分而以多链的形态来支持，提供状态通道隔离不同的业务链，每一条业务链运行特定的应用，业务链与主链之间保持锚定，并且与主链运行在同一个节点上。

在智慧链的设计中，对多链的支持是构建在内置的基础上的，主链与分隔的其他业务链共享区块数据，因此不存在数据中继的问题。

1.4 设计哲学

智慧链的设计，是建立在特定的应用场景上的，因此从技术到经济模型的设计都有自己的规则，会遵循既定的设计哲学。

1）、使用 UTXO 账户模式[1]，充分保持网络中账本数据的一致性

2）、不支持脚本程序关于数据资产的内部事件触发

3）、共识机制充分保持网络的社区自治

4）、稳定性与安全性优先

在智慧链的设计中，时刻保持与社区的沟通交流，本设计哲学在迭代中会发生变更，在非必要的情形下，会保持既定原则。

2 系统架构

2.1 架构组成

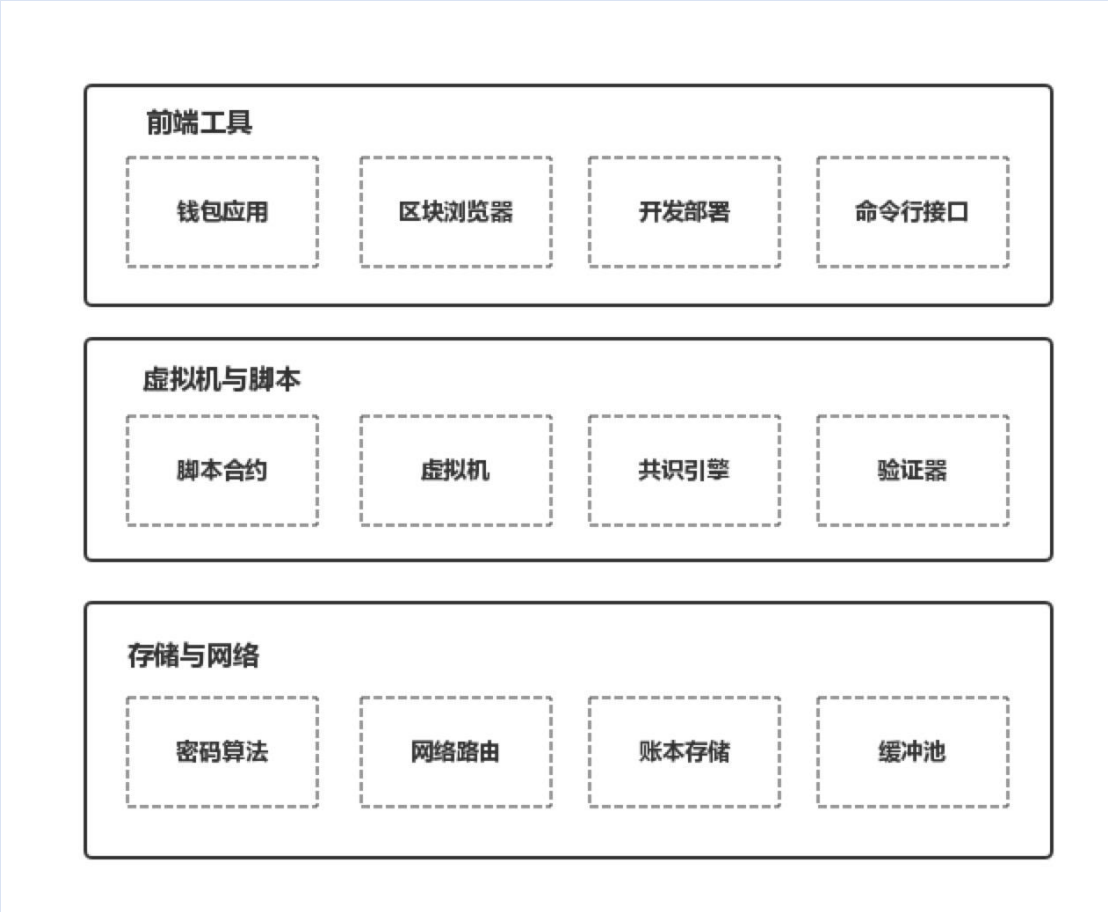

图 2 智慧链架构组成

如上图所示，这是智慧链的基本架构组成，主要分为存储与网络层、虚拟机与脚本执行层以及前端工具 3 个部分。其中第 2 和第 3 部分是主链节点的主要组成，实现所有的核心技术栈部分。前端工具是与主节点进行通信而完成功能的。

2.2 虚拟机

智慧链虚拟机实现为栈式结构，所有的程序编译指令都在操作数栈中执行。每一个完全节点都运行同样的虚拟机实例。对于智慧链中的密码计算、账户地址构造、区块数据读写等提供直接的支持。智慧链虚拟机支持准图灵完备的程序执行，不支持死循环，并且通过设置运行消耗限制指令的执行步数。在虚拟机执行过程中，会分配临时的内存存储空间，临时存储空间存在于虚拟机的运行实例中，每个运行实例都有自己的临时存储并且互相隔离。操作数栈的大小没有限制。智慧链虚拟机只能执行定义在智慧链规范中的字节码。

在虚拟机执行的过程中，如果由于某些原因导致异常中止，调用者支付的运行消耗将会被退回。并且，当脚本程序的所有者只有一个账户角色且未发生过数据状态变更时，所有者会有机会删除部署的脚本合约。

在智慧链的设计中，合约之间可以进行功能调用，但是对于数据资产不能进行内部的触发调用。数据资产在智慧链的定义中是通过特殊的标记定义的。

2.3 经济模型

在智慧链中具备基础的价值通证，用以实现对数据资产的价值标定，以便于进行交换和流通，同时也用于激励网络节点的良好运行。它的作用如下：

1)、作为智慧链价值网络的基本通证；

2)、标定数据资产的价值，并可用于流通交换；

3)、激励网络节点；

4)、激励社区的应用建设；

5)、支持持续的技术投入；

6)、作为链上应用的价值基础

经济模型的设置还可以通过智慧链脚本程序开发设定，开发者可以按照自己的业务需求，实现自定义的应用内经济模型。

3 核心算法与数据结构

3.1 共识算法

在第一阶段，智慧链采取 PoW+PoS 的混合共识，其中 PoW 作为底层协议，保证共识节点需要参与竞争才能获得区块生产的资格，并确保一定的公证性，同时在发生恶意网络分区的时候，PoW 机制可以让分叉链最终找回主链。通过 PoW 的计算消耗，发生的实际硬件运算成本也可以作为智慧链网络的基本价值保证。PoS 作为上层的共识协议，也是智慧链共识的表现层，通过权益的权重分配，融入智慧链的经济模型，促进社区合作与社区治理。

对于共识机制中设定的难度系数，会在每个区块间隔进行调整，区块生产的平均周期大约为 12 秒。共识节点会获得区块的奖励，同时有效地址账户将会周期性的获得系统的派息奖励。有效地址账户的含义是，至少发生过一次事务操作。

3.2 不对称密钥算法

在智慧链完全实施后量子密码技术之前，将会采用椭圆线密码算法，实现具体的 ECDSA 以及 ECDH。

Curve25519/Ed25519/X25519[2][3]是著名密码学家 Daniel J. Bernstein 在 2006 年独立设计的椭圆曲线加密 /签名 /密钥交换算法。Ed25519 使用一个性能极高的数字签名算法，并且签名过程不依赖随机数生成器，不依赖哈希函数的防碰撞能力。签名与公钥的长度都比较紧凑。25519 系列曲线可以说是目前性能最高的椭圆曲线加密算法。

3.3 区块存储结构

在智慧链主链的实现过程中，区块由区块头和区块体组成一条单向的主链，区块体中存储交易事务以及合约代码。区块的存储大小没有限制，但是对区块中所能消耗的 Gas 会有限制，区块大小是动态调整的。区块中不允许存储空块，在存储结构中，必须至少存在一条事务。

区块结构实现隔离见证，区块体中的每一条事务数据必须以上一个区块的哈希值作为前缀。严格的说，是必须包含最近的区块哈希值。这将防止发生分叉时，在分叉链上存储大量的事务。

3.4 梅克尔证明

区块体中的每一条事务数据都会被计算出一个哈希值，相邻的事务哈希两两成对计算，得出一棵事务哈希树，树结构的根也就是梅克尔根存储在区块头中。梅克尔树结构用来证明事务数据的完整性，使用在节点数据同步以及客户端验证事务存在性和完整性的时候。

在支持内置多链时，会分别计算多链的梅克尔树结构，以便于实现跨多链之间的价值数据交换。

4 实施及发展规划

4.1 智慧链实施步骤

智慧链的发布包含主链以及测试链。

测试链包含智慧链第一阶段的技术实现，并可提供给社区进行体验试用。为方便社区试用，测试链将支持 PoA（Proof of Authority，权威证明）机制。除了共识机制具备可选性，测试链与主链在所有协议的实现中都将保持一致。

测试链启动后，经过一段时间的观察期，将决定启动主链。随后将展开一系列应用的部署。

4.2 未来演进规划

在技术层面，智慧链将持续迭代升级密码算法并最终支持完善的后量子密码算法；同时共识机制也切换到由社区投票决定；对于主链的支持也将由单一主链升级到支持内置多链。

应用层面，智慧链将持续发展并部署面向智能生活的应用，以解决现实问题为己任，通过系统内在应用的增值而保持智慧链的价值基础。对于社区的应用协作开发，智慧链官方将提供全面的技术和激励支持。

4.3 社区治理规划

智慧链社区划分为如下类型：

1）、技术社区

促进主链的开发推进，提出有效的建议，积极参与系统开发的结构设计与算法设计，协助编写技术开发文档。积极参与智慧链的建设。

2）、应用社区

开发部署面向智能生活的应用，促进传统实体业务场景与智慧链的结合，协助应用场景的设计，并推动应用的发展。

3）、拓展社区

拓展智慧链的发展生态，协助标准的制定，安全性解决方案，不同国家社区的监管以及法律协调，推动智慧链生态的健康发展。

5 应用场景

5.1 设备身份认证

物联网的快速发展，将会带来数以亿计的智能设备，从小型的个人生活设备到大型的家用设备。这些设备都具备使用身份认证，当运行设备的数据通信、维修检验、智能充电等各项业务时，这些各种各样的设备需要能够被识别，并能与某种确定的身份衔接，以便于有效的结算。众多的设备很难通过一个单一的服务方来提供设备认证服务。智慧链可以为设备身份提供集合存储并关联账户地址。

任何需要进行设备认证的场合，只需要与智慧链连接，并调用认证接口，即可实现全球范围内的设备认证服务。

5.2 数字资产

智慧链最基础的服务就是支持价值数字资产，数字资产的范围很广泛，人们的各种所有权都可以上链并进行数字化，实现现实所有权的链上映射。进入到链内的数字资产，可以通过脚本合约进行自定义规则的流通与管理，使其产生新的应用价值。

除了通常的所有权外，对于个人设备所产生的数据，同样也是属于个人所有权数据，通过设备私钥签名上链，并通过全网见证成为链内资产数据。

5.3 医疗数据共享

医疗数据也是属于个人数据的范畴，为促进公共卫生事业发展，并使个人医疗数据发挥更大的作用，通过部署链上的医疗数据共享应用，在保证个人身份隐私的前提下，连接各个医疗机构的数据，减少医疗机构间系统集成的昂贵成本，并使数据可以在全球范围内具备快速的传播能力。

同时通过创建合适的经济模型，可以使数据分享的多方获得激励，链内的数据可以免费无缝的提供给其他分析系统调用，为疾病分析与防治提供有效的数据支持。

5.4 生活习惯数据

个人产生的生活习惯数据，将通过各种智能设备产生，比如健身数据、作息数据、订餐习惯数据等，这些数据通过个人或设备的私钥签发，发布到链内，确保个人隐私，同时使生活习惯数据具备资产化特征，个人通过分享数据获得激励，同时对于整个系统来说获得有效的分析数据。对于社会管理和商业管理提供更针对性的数据分析支持。

附件

术语表

编号	术语	解释
1	通证	数据所有权的表征定义
2	后量子密码技术	抗量子计算的密码体系
3	UTXO	未花费交易事务输出，比特币中的交易模型
4	共识	保持区块链网络中节点数据一致的算法机制
5	分叉	区块链网络由于协议的变更产生新的分叉链

参考文献

[1] https://bitcoin.org/bitcoin.pdf
[2] https://en.wikipedia.org/wiki/Curve25519
[3] https://ed25519.cr.yp.to

版本变更记录

版次	变更记录	备注
1.0	创建	