Wisdom Chain Technology WhitePaper2.0

Wisdom Chain 技术白皮书 2.0

目录

背景

Wisdom Chain（简称“WDC”，中文名称“智慧链”）是一个面向商业应用的基础公链，其功能设计围绕着资产定义、多重签名、条件支付和存证来进行，稳定安全与多方自治为设计原则，在性能、安全性以及系统的开放性设计上引入了独特的验证引擎实现方式。

区块链技术的发展从 2008 年比特币诞生开始，各类技术的迭代探索层出不穷。从共识机制到指令系统，从隐私保护到跨链交互等。除了具体的技术组件外，区块链系统的应用侧重点也是百花齐放，智能合约平台、去中心化交易、存证溯源等。

对于一个基础公链来说，密码技术、共识机制、P2P 网络层、账本存储层以及脚本系统是最核心的五大基础模块，Wisdom Chain 在这五大模块的设计上吸收了前人的优点也借鉴了很多的缺陷教训，并且在基础上进行深度的研究创新。

Wisdom Chain 关注的是资产的安全管理，包括资产定义、转发、多签、条件支付、隐私签名、离线签名以及原子交换等。专注才能做到性能与安全性达到最好的平衡。Wisdom Chain 是一个功能专注的公链，追求的是安全可靠以及降低用户使用门槛。

Wisdom Chain，为改变而来，为通证经济而来

● Wisdom Chain 的特点

○ 安全可靠

公链网络部署在互联网之上，节点遍布世界各地，成千上万的用户在链上定义以及管理自己的数据资产。对于一个点对点的网络系统，技术设计的安全性至关重要。Wisdom Chain 从密码算法的选型，共识机制的设计，尤其是脚本指令系统的设计，着重于网络的公正性设计以及在应对可能出现各种攻击时的抵御能力。安全可靠是 Wisdom Chain 网络的基石。

在核心的指令系统部分，Wisdom Chain 采用了外部触发机制，使用规则模板提供灵活性，防止指令编程过程中的漏洞攻击。

○ 低延时

公链系统的数据吞吐能力以及出块速率是一个需要综合考虑的指标。Wisdom Chain 的区块大小限制为 4M，出块周期为 10 秒，可以提供全网满负荷 1400 的 TPS 处理能力。均衡考虑了区块数据在异步网络环境中广播的性能要求，同时也尽可能降低了孤块率和临时分叉的概率。

- **分叉抵抗**

分叉是公链系统的一个典型问题，对于纯竞争模式的共识网络，分叉是比较容易触发的。分叉发生对于用户来说意味着链上的资产可能会有潜在的损失风险，网络的稳定性也会受到挑战。Wisdom Chain 混合了 DPoS 和 PoW 机制，矿工节点出块需要付出基本的算力成本，同时需要进入到前 15 的投票排名中，除非超过 2/3 以上的节点同时进行分叉行为，个别节点是难以发起网络分叉的。如果是 2/3 以上的节点发起分叉，则网络仍然是稳定的，因为网络的稳定性由多数节点来决定。

- **低门槛**

公链面向大众使用，一般不设专门的身份鉴权机制，其使用门槛主要体现在两个方面：

I、矿工手续费

II、功能使用的难度

Wisdom Chain 签发事务的最低手续费仅为 0.002 WDC，几乎可以忽略。对于链上的各项功能，用户也可以通过很直接的接口进行调用，在有界面工具的支持下，无论是资产定义还是多签等操作，甚至是不需要有编程能力的要求，从而大大的降低了普通用户的使用门槛。

- **低成本**

Wisdom Chain 使用的低成本不仅仅是在入门级的手续费上，还体现在节点部署成本上，部署一个 Wisdom Chain 全节点的建议硬件要求为：

1）、8 核 CPU、16G 内存

2）、网络带宽 100M 及以上

无论是普通全节点还是矿工节点，都不需要很特殊的硬件配置。特有的共识机制也能避免高性能矿机带来算力垄断而导致的挖矿中心化的问题，从而使普通用户都有参与成为网络节点和矿工节点的机会。

- **账本存储**

对于账本存储层的处理，结合了区块存储的 KV 结构以及关系数据存储的优势，节点间同步数据时可以快速发送二进制序列化的事务和区块，而在进行检索查询时则通过关系查询提高处理性能。在进行连续快速的数据读写时，进行读写锁以及索引的优化处理，确保同步的稳定性和性能达到一个平衡点。

- **脚本系统**

脚本系统的设计是 Wisdom Chain 的一大特点，既不是纯粹的固定逆波兰表达式指令结构，也不是简单的迁移图灵完备的编程环境。前者功能过于固定死板，后者缺乏安全性。Wisdom Chain 采用的是特别设

计可验证规则编程引擎，对于内置的 WDC 转发以及投票、抵押和存证采用的是固定指令结构；对于资产定义、多重签名以及条件支付采用的是规则编程。

● 共识机制（DPoS+PoW)

○ 基本特点

Wisdom Chain 的共识算法在设计时主要考虑了如下的要求：

1）、具备抗分叉的能力

2）、保持较低的孤块率

3）、具备可用的出块效率

4）、抵抗挖矿中心化

5）、促进矿工维护社区

6）、挖矿具有基本难度

在综合考虑了各种共识的优劣后，Wisdom Chain 设计了 DPoS+PoW 的混合机制，在网络的处理效率与公正性以及安全性之间取得一个平衡。Wisdom Chain 每个区块的大小限制为不超过 4M，平均每 10 秒/块。

○ 矿工轮选

区块通过 15 名生产者轮流产生，每一个出块纪元（120 个区块为一个纪元）开始时，网络选出 15 个区块生产者。区块生产者需要抵押至少 10 万 WDC，并且在当前纪元开始时确保所获得的投票排名在前

15 名。

投票排名并不是固定的，除了受到投票以及撤销投票的影响外，在实际的排名计算中，依据的是实际投票权益的数据，在投票初始纪元，投票权益等于投票数，然后每过 2160 个纪元就会衰减，按照 2160 个纪元 10%的衰减比例逐渐累次衰减。

根据投票权益衰减规则可以得出衰减公式：**V * 0.9^(n-1)**，其中 V 的投票的数量，n 是当前投票生效后衰减周期数（一个衰减周期等于 2160 个纪元）。

假设 V 的票数为 10,000 WDC：
第一衰减周期的投票权益为 10,000 * 0.9^(1-1) = 10,000
第二衰减周期的投票权益为 10,000 * 0.9^(2-1) = 9,000
第三衰减周期的投票权益为 10,000 * 0.9^(3-1) = 8,100 …… 以此类推

由于投票权益的衰减，因此矿工需要维护好与社区的关系，以确保自己能获得足够的投票，并且愿意为自己进行持续的投票。

矿工在下一轮的筛选过程中，若抵押金额不足或者累计投票权益没有达到前 15 名则落选。若某节点在轮到出块时，由于某种原因没有出块，则其他节点将其踢出本轮列表。

○ 出块流程

当矿工列表依据抵押以及投票权益产生后，出块时还需要完成一定的工作量证明，矿工需要在最多 30 秒内解决一个哈希计算难题，找到一个随机数，使得能够满足区块头计算的哈希值小于当前纪元的难度值。难度值每过一个纪元调整一次。

难度值的计算过程，会使用如下的六种哈希算法进行连续计算：

WhirlpoolDigest（0，1）

RIPEMD-256（4，5）

BLAKE2b-256（6，7）

SHA3-256（8，9）

KECCAK-256（A，B）

Skein256（C，D）

其中括号里面的十六进制数字是表示哈希函数的计算顺序，计算顺序并不是固定的，而是根据前一个区块头的哈希值的最后 4 个字节，再根据上述 8 个哈希算法的数字标号，进行相应顺序的调用。

计算参数为：

1）、区块版本

2）、上一个区块的哈希值

3）、梅克尔根

4）、时间戳

5）、难度目标值

6）、随机数

每个矿工出块间隔最多 30 秒，若在时间周期内没有成功出块，会直接跳过该矿工，按照顺序安排下一个矿工出块。出块后广播到其它节点进行验证。若某矿工节点在 1 个纪元内没有出块，则会被网络拉入黑名单。

- **主链规范化**

矿工在出块时，广播出的区块并不会立即进入主账本，而是首先进入到 ForkDB 账本临时保存，当区块得到 2/3 矿工出块确认后，本区块就永久确认，进入到主账本。出块时若矿工产生多个区块，将会根据难度值取得难度最大的保留，实际上由于有难度计算以及时间周期的约束，矿工在出块时要想产出多个版本的区块是有难度的。

若节点偶尔发生了硬分叉，在同一个高度存在不同的被确认的块，则通过节点的运维服务可以检测出分叉点，并自动修复保留高度最高的那条分支作为主链。

● 规则验证引擎

○ 验证机制

指令系统是区块链的核心模块，也是一切资产功能的驱动器，不同于完全固化的指令功能，也不同于图灵完备的虚拟机系统，Wisdom Chain 使用了特有的规则验证机制。在保留指令功能灵活性的同时，确保安全性。

传统的指令系统，一般存在着如下的问题：

1、缺乏对资产定义的专门描述

2、不能保证程序脚本的健壮性

3、语法元素太丰富，不易使用

4、支持内部触发，容易被攻击

5、“执行”而非“验证”

Wisdom Chain 的设计规范中，侧重认为指令系统应该被更好的实现为一个事务验证机制，而不是一种用户自定义程序的虚拟机执行系统。系统应该为用户资产的安全性负责，从机制上保证效率和可靠性，而不是依靠用户自己的自觉性。用户自定义程序的行为以及潜在的漏洞很难被全部检测出来。

在验证机制的设计中，Wisdom Chain 的指令功能通过验证模版实现，例如资产定义、多签、条件支付等，节点接收到指令事务后可以进行完整的合法性校验。用户在模板的基础之上，同时也可以实现一定的自定义，但却约束在验证模板允许的范围中。由于是完全验证的机制，避免了行为多样的代码在虚拟机中可能导致的各种安全问题。

所有的规则定义，语法结构都是如下：

<规则类型>

{

//属性值

//规则

}

属性值相当于状态量，是需要被存储到账本，规则是一组验证条件，决定事务的有效性。属性可以是规则级别，也可以是账户级别，比如资产定义规则，初始的发行总额就是属于规则级别，资产名称也是规则级别，当验证语句发现某个属性的值可以合法的更新到另外一个账户时，就是账户的属性，比如资产金额。

规则也是有地址的，区别于普通地址，规则地址具备 WR 字符前缀。规则定义在事务结构的 payload 字段。使用规则时，首先要进行部署，签发部署事务，然后发起规则的调用事务。

以下将分别介绍验证模板对资产定义、多签以及条件支付的实现。

- **资产定义规则**

Wisdom Chain 中的资产规则语法如下所示：

```
{
    "ASSET_RULE":{
    "code":"",
    "offering":,
    "totalamount":,
    "create":"",
    "owner":"",
    "allowincrease":,
    "info":{}
  }
}
```

其中的属性分别为资产代码、初期发行额度、发行总量、规则创建者公钥、规则所有者公钥哈希、是否允许增发以及资产备注。

资产定义的规则函数：

规则函数	**备注**

"changeowner": {
"newowner": ""
}
	更换所有者公钥

"transfer": {
"from": "",
"to": "",
"value":
}
	转发资产
	from 为签发者公钥
	to 为接收者公钥哈希
	value 为数额

"increased": {
"amount":
}
	是否增发

- **多签规则**

Wisdom Chain 中的多签规则具备如下特点：

本规则支持的多重签名逻辑如下：

1）、签名没有顺序要求；

2）、支持 WDC，也支持其它链上资产；

3）、两个多签地址之间以及多签地址与普通地址之间均可以任意

转发。

多签的规则语法如下所示：

```
{
    " MULTISIGN _RULE": {
        "asset160hash":
        "m":
        "n":
        "pubkeys":[],
        "signatures":[],
        "pubkeyHashs":[]
    }
}
```

其中的属性分别为资产的 HASH160 值，总计可具备的签名数、最小需要达到的签名数、公钥数组、签名数组、公钥哈希数组。

多签的规则函数：

编号	**规则函数**	**备注**
1	"transfer": { "origin":"", "dest":"",	origin 表示账户类型，多签或者普通地址

	"from": [], "signatures":[], "to": "", "value": , "pubkeyHashs":[] }	dest 的定义同 origin from 表示多签规则或者普通账户的公钥数组 signatures 表示签名数组 to 表示目标地址对应的公钥哈希 value 表示数额 pubkeyHashs 表示多签规则或者普通账户的公钥哈希数组

其中为了保持账户模型的统一性，遵循如下规范：

I、公钥：使用部署事务的哈希值替代，长度都是 32 字节；

II、公钥哈希：使用部署事务的哈希值的 160 哈希值替代，长度为 20 字节。

多签规则不仅适用于 WDC, 同时也适用于构建在 Wisdom Chain 的自定义资产。

○ 条件支付规则

当一笔支付需要满足到某个条件时才能被触发，称之为条件支付。“哈希时间锁定”就是一种条件，“哈希高度锁定”也是一种条件。支付对于区块链来说，就是一种事务结构，验证通过并且入块后即表示资产发生了转移，然而资产发生了转移不代表目的方就可以立即使用，因为在计算自己的余额时，它会判断是否符合了条件。

Wisdom Chain 支持两种条件，“哈希时间锁定”以及“哈希区块高度锁定”。“哈希时间锁定”的规则语法如下：

```
{
    " HASHTIMELOCK _RULE": {
        "asset160hash":,
        "pubkeyhash":
    }
}
```

支持规则函数

编号	规则函数	备注

	"transfer": { "value": 50, "hashresult": “”, "timestamp": “” },	转发资产

	"get":{
	"transferhash":
	"origintext":
	}
		获得锁定资产

“哈希区块高度锁定”的规则语法如下：

{

" HASHHEIGHTLOCK _RULE": {

"asset160hash":,

"pubkeyhash":,

}

}

支持规则函数

编号	**规则函数**	**备注**
	"transfer": { "value": 50, "hashresult": “”, "blockheight": },	转发资产

	"get":{
	"transferhash":
	"origintext":
	}
		获得锁定资产

- **扩展规则**

Wisdom Chain 将会根据发展的需要以及社区的共识，定期扩展新的规则模板，新的规则模版仍然是围绕着资产管理为中心。

● 隐私保护

Wisdom Chain 对隐私保护的定义都是针对资产管理的，主要涉及到聚合签名、零知识证明以及隐私群。隐私保护在 Wisdom Chain 中作为一个备选策略来设计，而不是一个必选项。

- **聚合签名**

在多签场合会需要使用到签名数组，数组格式需要对签名的顺序进行处理，Wisdom Chain 不关心签名的顺序，在需要高效处理多个签名时，聚合签名是一个合适的方案。

- **多项式隐藏**

这是 Wisdom Chain 对零知识证明的实现，是构建在多项式计算的隐藏基础上的。在 Wisdom Chain 中始终可以查询每一笔事务之间的溯

源关系，然后在需要隐藏比如金额或者某些表达式结果时，可以通过椭圆线加法同态隐藏的方式来高效的实现。

○ 隐私群

隐私群是 Wisdom Chain 对集体事务参与的一种公正性保护，例如投票活动，投票者可能不愿意让其他人知道自己投给了谁，或者说不愿意其他人知道还投给了其他哪些人。则可以通过创建隐私群，在群中置入若干个账户地址，并且定义群的行为范围。只要是群中的地址发起的事务动作，都会模糊为“群”的身份，“群”内部的动作对于验证者来说仅仅只需要知道对于“群”这个集体概念是否合法，而并不需要去验证具体某个成员，从而可以杜绝群成员的行为暴露。

● Token 经济模型

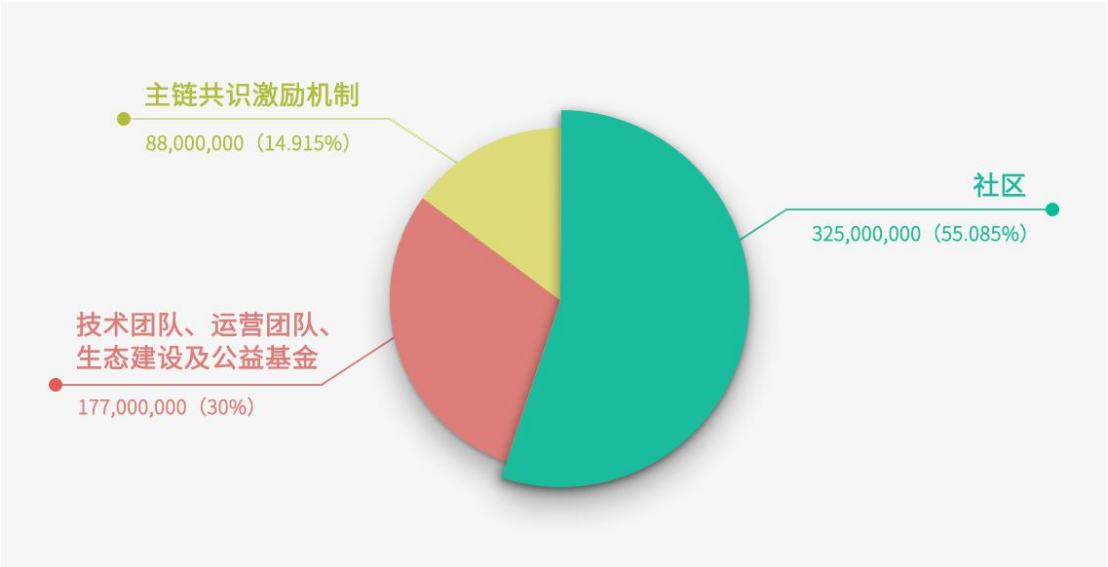
WDC 是 Wisdom Chain 的底层唯一通证。

WDC 恒定总量：590,000,000；

WDC 经济模型：社区 325,000,000（55.085%）；

技术团队、运营团队、生态建设及公益基金：177,000,000（30%）；

主链共识激励机制：88,000,000（14.915%）。



○ **区块奖励**

Wisdom Chain 总量为 590,000,000，其中矿工奖励总额为 88,000,000，主网在 285,600 区块高度时（新加坡时间 2019 年 10 月 23 日 18 点 10 分 47 秒），对主网出块速度与共识奖励作出了调整（285,600 区块高度前的出块平均速度为 30 秒/块，每个块的奖励为 20 WDC；285,600 区块高度后的出块平均速度为 10 秒/块，每个块的奖励为 6.66666666 WDC）。首次减少出块奖励的区块高度为 5,736,000，以后固定每隔 6,307,200 个区块（时间约为两年）调整一次，调整比例为较上次减少 47.781818%。

- **手续费**

最低为 0.002 WDC，矿工可以自行进行调整。

- **投票权益**

见本文【矿工轮选】中的解释。

● 离线现金

Wisdom Chain 将会提供对离线支付的支持，离线支付是对链上在线支付的补充形式，意在为用户提供更快捷方便的小额支付。用户离线支付的对象称之为离线现金，离线现金可以合并也可以拆分，却无法双花，但具备实物现金的原子传递特征。离线现金与主链账本资产是一体的，可以进行任意的互相转换。

● 跨链交换

- **原子交换**

Wisdom Chain 主要针对两种场景支持原子交换：

1）、用户地址之间的 WDC 资产与自定义资产；

2）、用户地址之间的自定义资产与自定义资产。

通过原子交换，用户之间可以不通过第三方平台以可信的方式完成资产的交换。

○ 跨链资产交换

跨链交换是对原子交换功能的通用扩展，可以支持对其它链上资产或者强力背书的中心化资产的直接交换。

● 治理

○ 矿工协作

Wisdom Chain 采取社区自治的方式进行日常的主网治理，矿工之间更多的是互相协作而非互相竞争，共同维持网络的稳定，并提供对链上各种事务的处理支持。

○ 升级协议

在 Wisdom Chain 网络中，只要 2/3 及以上矿工同意升级，则主网节点即可完成大版本的更新迭代。

● 总结

让信用前所未有地流动

让无限的想象可能发挥，让无穷的价值可以体现

直到星球的每个角落.....

让价值互联网，通过 Wisdom Chain，实现更安全的保证

Wisdom Chain 主网已于 2019 年 7 月 8 日启动，可通过如下链接查看主网数据：

官网地址： www.wisdchain.com

区块浏览器地址： https://scan.wisdchain.com/index.html

开源代码库: https://github.com/WisedomChainGroup