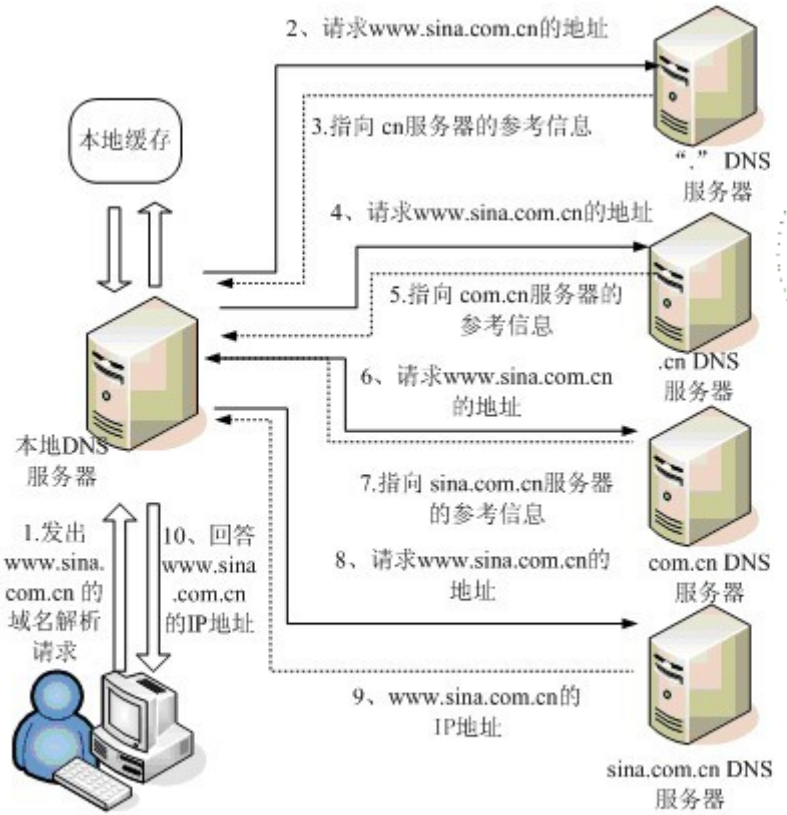
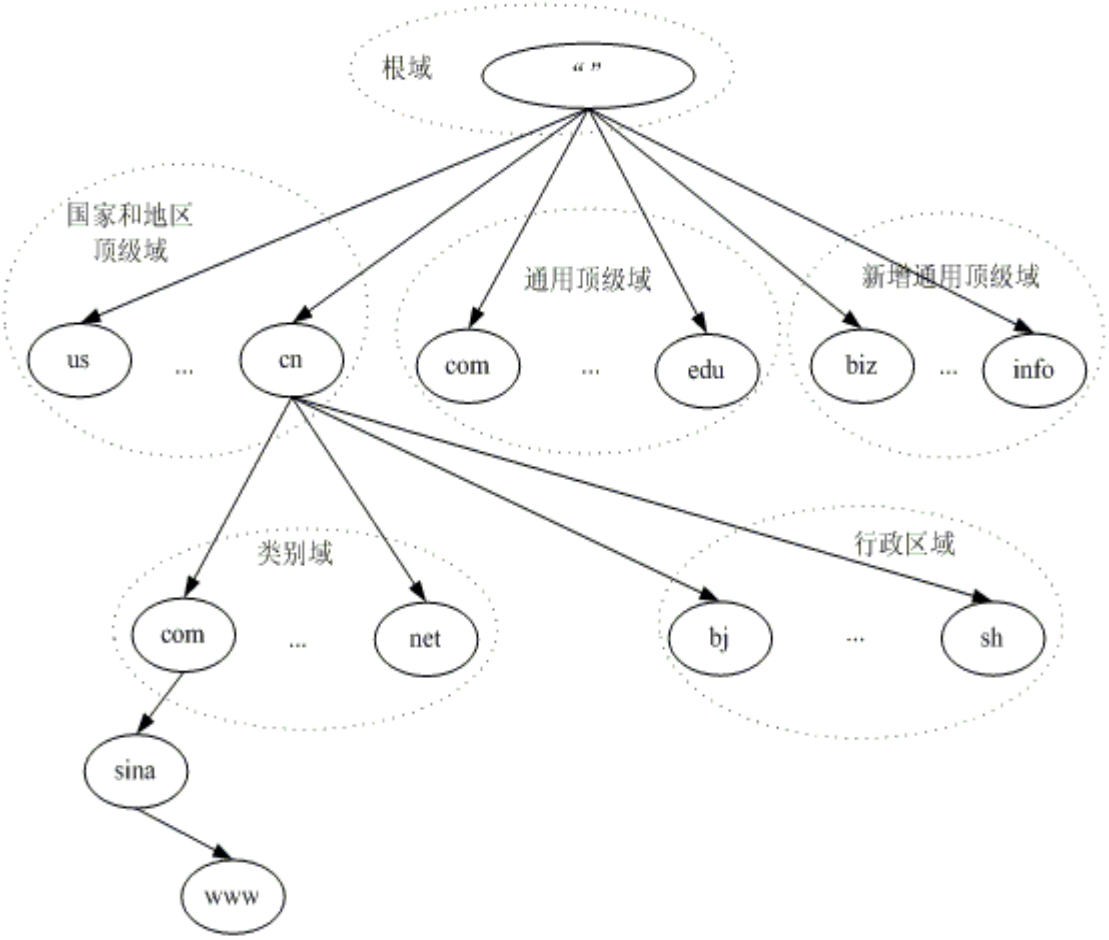
ODIN : Open Data Index Name

融合多区块链的自主、可信的新型 DNS

从域名和 DNS 说起





域名系统将主机名解析成 IP 地址使用到一个全局的、层次性的分布式数据库系统。

虽然互联网本源是分布式、自治性的系统，而 DNS 却不是自治性的系统， Why?

13 台根服务器：没有美国，没有互联网

根服务器主要用来管理互联网的核心主目录。
DNS 体系诞生 30 年来，作为互联网的基础设施，运行的稳健性超出预期。
由于历史的原因，根域、重要的顶级域和根证书此前多由美国政府
或由美国政府授权的非营利性机构 ICANN 掌控，
这对各地区互联网络自主能力的威胁始终存在。

ICANN 的独立将淡化美国对互联网的控制，但 DNS 体系的一些固有缺陷仍在那里

等待改变： DNS 体系的缺陷和不足

- DNS 信息易被篡改

由于 DNS 报文协议天生不足，其域名信息容易被篡改，包括报文欺骗、缓存中毒等，通过实施 DNSSEC 可以解决此问题。但实施 DNSSEC 需要完善的电子证书体系，以美国为核心的电子证书体系从国家层面来说存在更大的危险性。

- DDoS 集中攻击

由于 DNS 是一个拥有中心的树状结构，很容易遭受 DDoS 攻击，且无有效手段防范，攻击越靠近中心效果越显著。

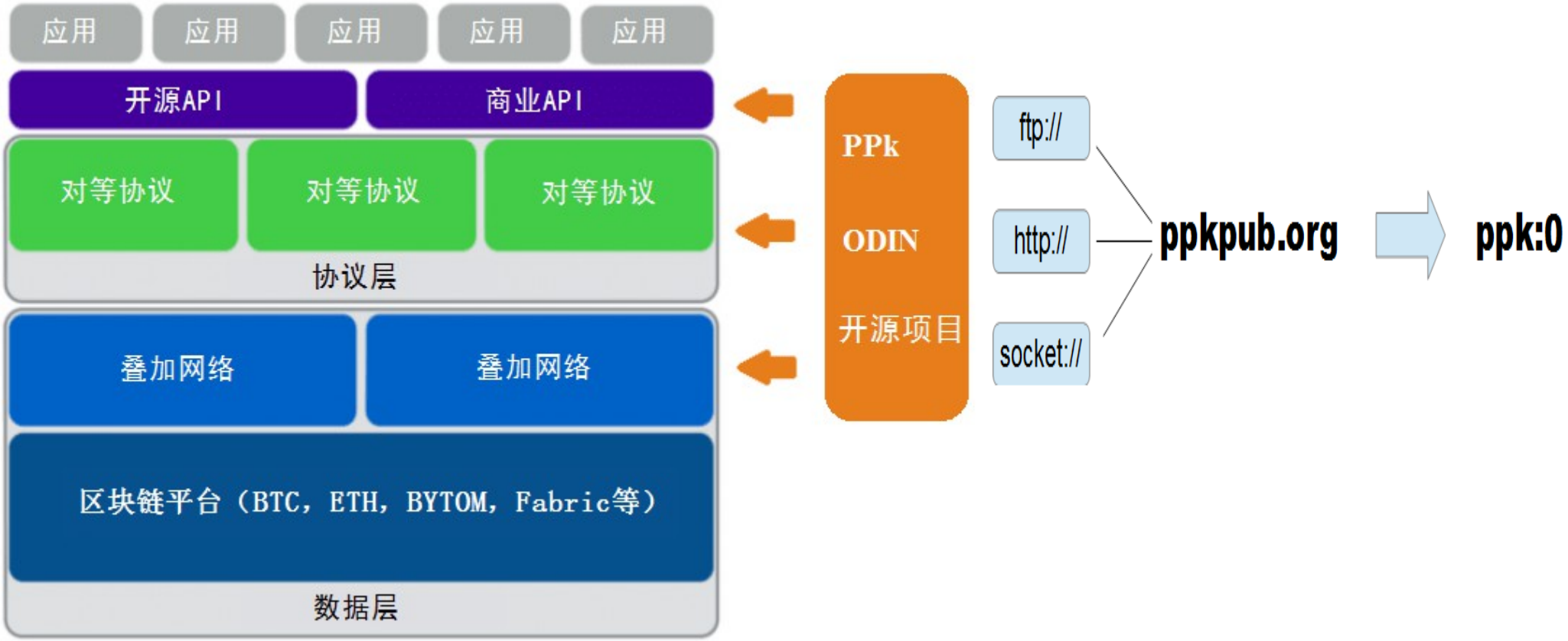
- 商业收费模式不尽合理

只能通过 ICANN 或多家顶级域名机构授权商家进行注册，不仅注册费用偏高，每年都要交，而且还有一些不尽合理的限制性条款（比如故意设置很繁琐的转出政策）。

面对 DNS 的这些不足之处，已经有了一些方案试着来弥补。
但为了保证 DNS 体系的稳定性，这些“小修小补”方案无法从根本上解决问题。

在未来 DT 时代能否跳出既有 DNS 体系，从根基上去中心化，走向完全自主？

ODIN 开放项目：融合多区块链的 DNS



ODIN(Open Data Index Name) 是基于区块链（ BlockChain ）定义的“数据时代的去中心化 DNS”，是在网络环境下自主命名标识和交换数据内容索引的一种开放性系统，遵从 URI(统一资源标识符) 规范。

ODIN 相比传统 DNS 的特点

- 自主性

ODIN 标识符基于去中心化的区块链技术由申请者自主生成并管理，其生成和管理规则是完全开放的，没有中心化的控制机构。除了拥有管理密钥的申请者之外，其他组织和个人都无权控制和篡改。

- 安全性

每一个 ODIN 标识符的拥有者都对应拥有一对非对称加密技术的公私钥，可以通过私钥对自主发布的数据内容进行签名，接受数据内容的个体可以通过公钥进行验证，以确保收到的数据是来源可信和不被篡改的。

- 唯一性

结合比特币区块链， ODIN 标识符能对任何数据内容对象（如文本、图片、声音、数据、影像、软件等）的开放访问索引进行唯一标识，使数据内容对象能被人们准确地识别和提取。

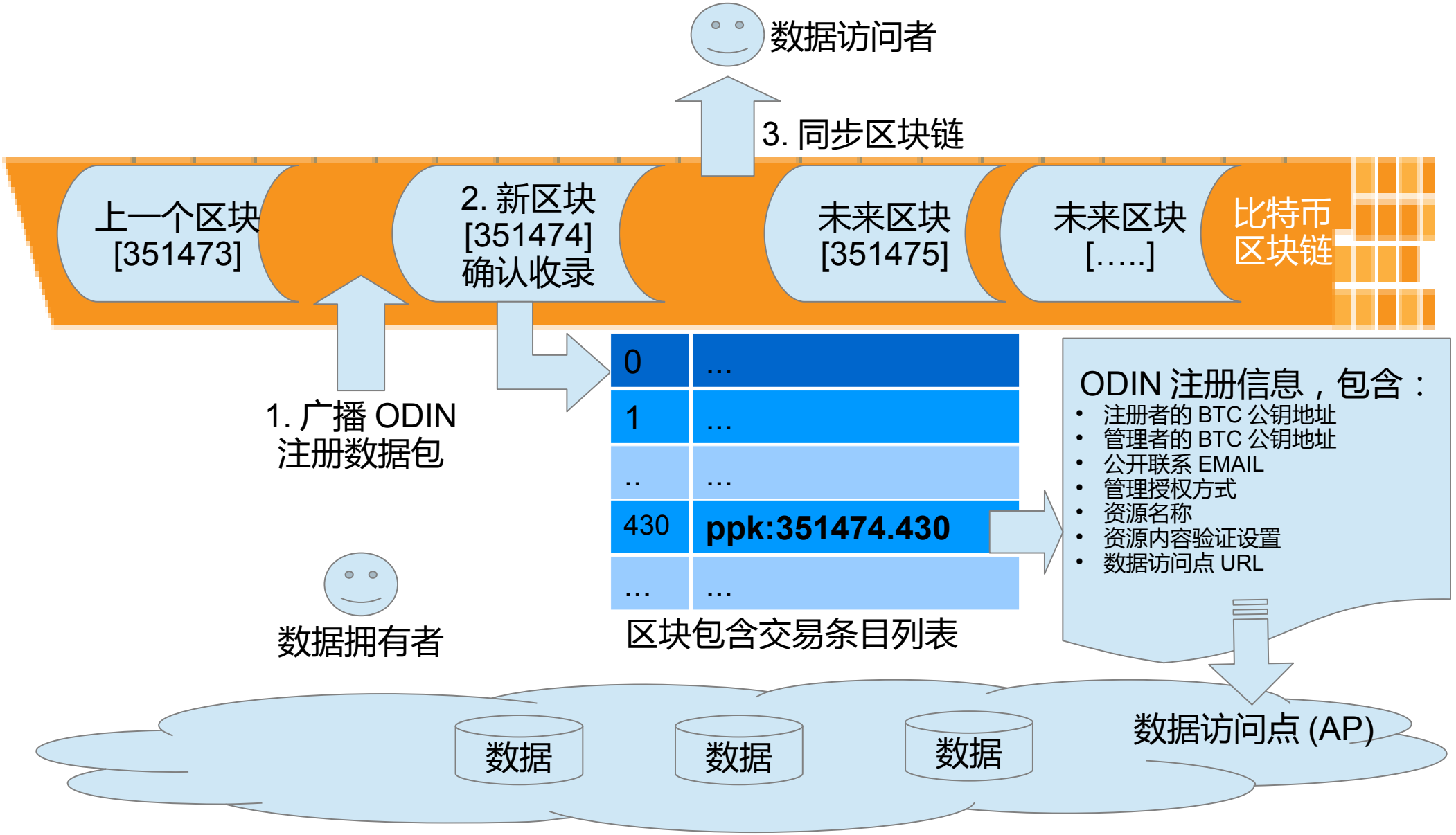
- 持久性

ODIN 标识符一旦生成就不可篡改，不随其所标识的数据内容对象的持有者或存储地址等属性的变更而改变。

ODIN 与其它基于区块链的标识类解决方案的差异

	ODIN	Namecoin	Onename
基础区块链	Bitcoin	Namecoin	Namecoin → Blockstack based Bitcoin
多级扩展	灵活扩展多级标识引入其他区块链（公有链、联盟链、私链等）	--	--
命名方式	用区块记录位置作为名称标识，确保唯一性	抢注字符串	抢注字符串

运行机制



完全开放、自主的 ODIN 运行机制

ODIN 根标识注册和解析过程

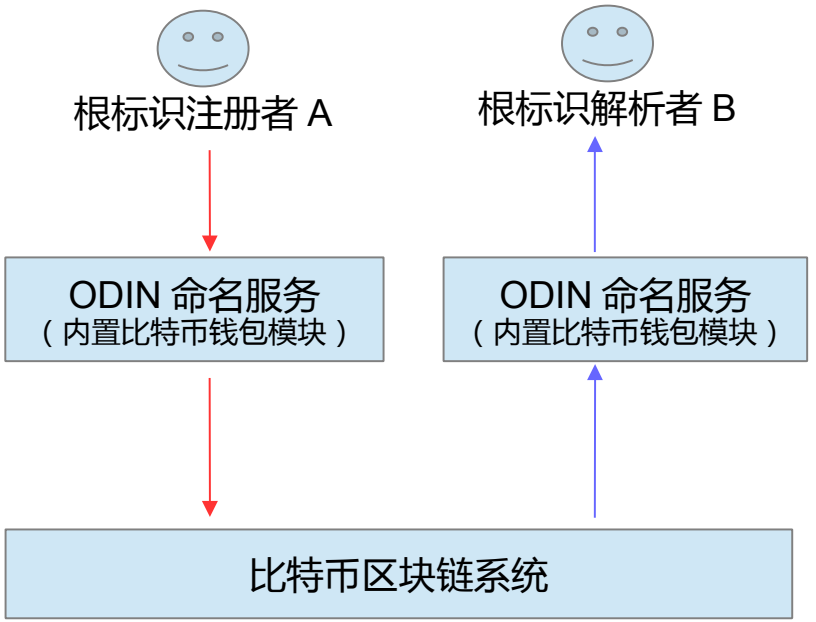
ODIN 根标识注册过程：
1. 根标识注册者 A 运行 ODIN 命名服务

2. A 输入根标识相关注册信息

3.ODIN 命名服务将注册信息块按二进制分 n 段，并对应转换为 n 个比特币收款地址

4.ODIN 命名服务通过内置的比特币钱包模块向（ n+1 ）个收款地址合并发送一笔比特币多重转账交易。（这里多加的 1 个收款地址是 B 自己的比特币钱包地址。 ）

5. 这笔交易被比特币区块链的新出区块收录，其收录位置（区块号和区块内部索引号）即新注册生成的 ODIN 根标识。



ODIN 根标识解析过程：
1. 根标识解析者 B 运行 ODIN 命名服务

2. ODIN 命名服务通过内置的比特币钱包模块同步比特币区块链数据直到最新区块。在此同步过程中，遇到带有 ODIN 根标识特征的交易时，从中提取出相关根标识注册信息并存入本地数据库

3. B 向 ODIN 命名服务提交一个 ODIN 根标识请求解析

4.ODIN 命名服务从本地数据库中查询出对应根标识的注册信息并返回给 B

数据示例：ppk:351474.430

- **Title**: PPk public group
- **Email**: ppkpub@gmail.com
- **Authorize: 2**
- **Access Points**:
  - http://ppkpub.org/AP/

编码方式：一级基础 ODIN

- 一级 ODIN 的标准结构式为：
  ppk:[BTC_BLOCK_SN].[BTC_TRANS_INDEX]/[DSS]

举例：
ppk:351474.430/
ppk:351474.430/#
ppk:351474.430/#1.0
ppk:305678.568/ISBN2890321345#1.0
ppk:305678.1000/ISBN2890321345-P235#2

- 一级骨干 ODIN 可以采用短编码方式，结构式为：
  ppk:**[REG_ORDER_INDEX]/[DSS]**

举例：
ppk:1/
ppk:356/#1.0
ppk:356/ISBN2890321345#1.0

编码方式：一级基础 ODIN 的特例

ppk:351474.430
ppk:351474.430#
ppk:1
ppk:1#

这四种特殊编码都表示对应一级 ODIN 标识的解析记录配置数据。

编码方式：多级扩展 ODIN

- **多级 ODIN 的标准结构式为：**
  ppk:[PARENT_ODIN_PREFIX]/[SUB_BLOCK_SN].[SUB_TRANS_INDEX]/[DSS]

举例：
ppk:351474.430/21.35/
ppk:351474.430/21.35/ISBN2890321345#
ppk:351474.430/21.35/ISBN2890321345#1.0
ppk:305678.1000/23.678/235.32/ISBN2890321345-P218#

- **多级 ODIN 自定义结构式为：**
  ppk:[PARENT_ODIN_PREFIX]/[SUB_TRANS_ID]/[DSS]

举例：
ppk:351474.430/22/
ppk:1/22/ISBN2890321345
ppk:1/22/ISBN2890321345#2.1
ppk:1/china/books/
ppk:1/china/books/#
ppk:1/china/books/ISBN2890321345-P218#

ODIN 与超级账本 Fabric 结合应用示例

超级账本 Fabric1.0 调用接口的 URI 形式定义：

fabric:[server_ip1:port1,ip2:port2,....]/channel_id/contract_id/function_name(argv1,argv2,....,argn)

合约里针对注册管理标识、更新数据块等具体功能可以定义若干 function

在此基础上，在 ODIN 标识协议框架下定义
ppk:odin_id1/odin_id2/.../function_name(arg1,arg2,...,argn)

这样的 URI 形式来映射支持通用的、分布式的方法调用，
其中的 arg 参数可以递归采用符合 ODIN 定义的 URI 资源标识，
与函数式编程方法结合可以很好地满足应用开发需求。

FAQ: 采用比特币区块链作为一级骨干是否能确保安全？

比特币作为第一个提出和实现区块链的加密货币，经过多年的运行已形成一个具有超强算力的分布式网络，其算力已经远超传统超级计算服务集群的合计算力且还在持续增加，从而充分保证了其区块链的安全性和稳定性。

理论上，如果比特币网络的超大算力有超过一半被一个个体所控制，该个体就可以篡改近期的若干区块数据（即著名的 51% 攻击），但其攻击难度随区块增长呈现指数级提高，超过 6 个区块确认后基本就不可能了，而且攻击者也只能篡改自己相关的交易信息（比如重复消费自己的比特币）或者不记录别人发出的交易，但不能凭空伪造别人比特币地址相关的交易，所以 ODIN 申请者在向比特币网络广播 ODIN 注册消息后，只需要等待 6 个区块就可以规避以上攻击风险以确认注册是否成功，即使在极小概率的情况下比特币网络被攻击成功导致注册不成功，也只需重新发起注册即可，对于注册者来说除耽误了一些操作时间外没有损失。

所以采用比特币区块链作为 ODIN 的一级骨干区块链是安全可信的。

FAQ: 比特币价格的大幅调整是否会对 ODIN 标识体系的稳定运行产生很大影响？

每条 ODIN 消息存储到比特币区块链的成本主要是支付给收录该交易的比特币“矿工”的费用，当比特币价格有大幅调整时该项费用也可以适当调整达到相对合理的费用（调整客户端的参数配置即可）。另外，通过使用二级扩展标识还可以大幅降低标识的注册和维护成本（可以接近 0 成本）。

如果未来比特币价格存在大幅走低的可能性，导致矿工关闭矿机使得算力减少，在一定程度上会降低比特币网络的健壮性，但对于 ODIN 标识来说，只要等待 6 个区块的确认仍能保证相当高的可信和稳定性。

所以比特币价格的大幅调整会对 ODIN 标识体系整体的稳定运行影响有限且通过适当的规则可有效规避相关风险。

FAQ: 与现有 DNS 域名体系的差异？

现有 DNS 域名体系是组织形式和逻辑上都中心化，与承载 OODI 的区块链相比无法提供自主性，且 DNS 协议因为出现历史早，在安全性等多方面上也存在不足，但因为其作为现有互联网的基础协议以稳定为重，很难做出大的改变。

ODIN 形式上和 DNS 域名有点像，但借助区块链的独特性使得运行机制上有本质的差别，强调自主和安全，是“数据时代的自主域名” 。

FAQ: 与 EMULE 、 BT/MAGNET 等 P2P 网络的差异？

EMULE 、 BT/MAGNET 等 P2P 网络是形式上的去中心化，但却没有进一步达成逻辑上的中心化，因此无法提供一个集中的目录索引服务。比特币区块链是借鉴了 EMULE 、 BT 等 P2P 网络的经验，并将非对称加密等技术集大成组合到一起形成的创新技术体系，逻辑上能提供一个唯一性数据索引目录，同时能提供更好的安全性。

另外，以“ magnet:?” 开头的磁力链接为例，这种链接的“数字指纹”是通过文件内容的 Hash 结果来生成的，并以此来定位和识别文件的，当文件内容发生变动，其磁力链接的“数字指纹”地址也会发生变化，导致无法通过原有磁力链接来定位到新版本的文件内容。

ODIN 可以兼容磁力链接地址并将其作为 AP 设置选项，这样当文件内容发生改变时，只需更改 AP 设置即可，不影响 ODIN 标识，通过既有 ODIN 地址仍能访问到新修改的文件。

FAQ: ODIN 与 URI/URL 的差异性在哪？

ODIN 不同于 URL （ Uniform Resource Locator ，统一资源定位符），它是数据资源的索引名称，而与实际地址无关，与 URL 的最大区别就是实现了对资源实体的永久性标识。

ODIN 实际上是一种 URI （ Universal Resource Identifier ，统一资源标识符）或 URN （ Universal Resource Name ，统一资源名称），是信息索引的数字标签和身份证。有了它，就使数据资源具有了自主、安全的唯一性和可追踪性。