NetCloth白皮书1.0

独特的你与你的网络

每一个人都是独特的存在，我们想要定制一种"互联网3.0"来保护我们小小的个性。

1. 它要有一种特别的账户，由我们自己产生与控制。我们能用它进入所有应用场景。在我们不同意的情况下谁也不能向我们发垃圾短信；
2. 它的数据一定是在我们终端上加密的，而不是服务器加密后传给我们；
3. 它在传递信息时一定得是加密的，钥匙只在我们自己手里；
4. 它上面运行的应用要公开代码，同时我们还要保证运行环境的安全一致；
5. 它需要让我有主动选择的权利，类似的服务我们可以更灵活地选择服务商；
6. 它还需要向我们提供一套安全的数据存储方式，我们上网产生的数据最好由自己控制；
7. 最后，这个网络的所有权要是我们自己的，如果我们的上网行为繁荣了整个网络，我们需要获得相应的回报。

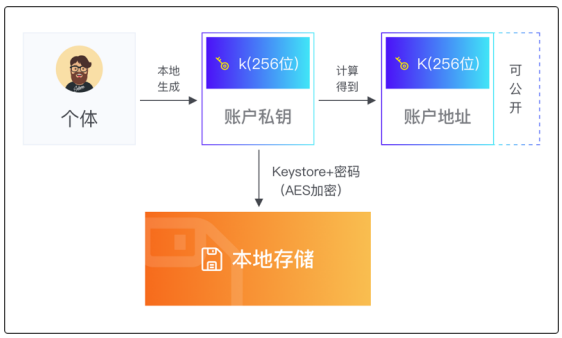
本项目正是为了实现以上目标而创建。我们从已知的计算机技术中找到了可以实现以上内容的技术工具。非对称加密是一套很好的安全机制，它可以用于产生我们的账户。现有的非对称加密算法很多，如RSA、Elgamal、背包算法、Rabin、D-H、ECC等，考虑到安全性与成本的兼顾，同时兼容现存区块链项目的账户，我们使用了ECC作为生成账户的算法。我们无法信任第三方替我们加密数据，所有加密的行为必须由我们自己——也就是我们的终端来完成，同时ECDH能符合第三点——传输中的安全问题。至于第四点，应用开源问题我们可以借助已有的代码开源平台（如github），运行环境则需要使用到虚拟机及智能合约。理想状态下，应用的前端应当由设备终端本地展示，并直接与区块链交互，而非服务器；同时后端的执行环境应部署在全局维护统一的虚拟机中。应用开源后，服务商没法通过后台作弊引导用户习惯，我们只需要搭建一个开放的对等网络就能实现第五点。第六点有点复杂，我们不仅需要用到智能合约，还需要用到可信计算，最后再基于分布式网络进行数据加密存储。第七点我们可以通过数字资产来确保我的所有权与利益，当然它本身还是对等网络中节点间的激励，用于解决对等网络因激励缺失而无法长期稳定运行的问题，这一方面与比特币类似。

1 NetCloth版本1.0——镖局

互联网完成的第一个功能是通信，我们将NetCloth网络中去中心化的通信功能命名为“镖局”，这也是NetCloth网络的第一个版本名。下面我们将以去中心化的即时通信场景为案例，开始解释NetCloth网络。

1.1 账户

在互联网中，我们通过第三方的协助来管理和使用网络身份。这种方式给使用者带来了方便的同时，也导致了信息泄露和流量竞争。现在，我们引入一种新的身份体系，定义非对称加密ECC的公钥为账户地址，由用户终端离线产生的账户私钥生成。



由于离线生成和本地参数选择，该账户私钥不仅独一无二（碰撞概率极低），也不被除了使用者以外的第二人知晓。

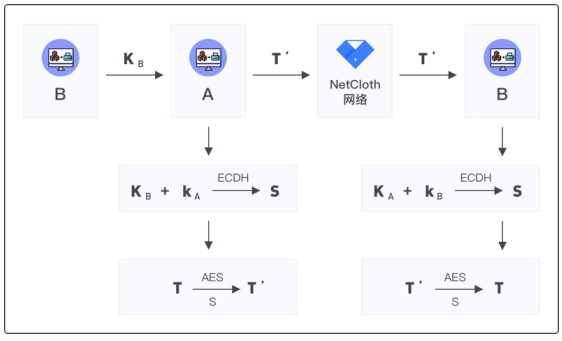
1.2 建立连接

将区块链技术的公开账本作为“号码本”，用户通过查阅公开账本获得对方通信地址。用户A将自己的公钥 K_A与选择的通信地址 IP_A告诉给验证人（Validator），验证人将该信息记录到最新的区块当中。当用户B需要与A建立连接时，B通过检索用户A最后一次申明的通信地址 IP_A，再通过ECDH进行加密通信。

1.3 加密传输

我们利用ECDH来确保网络中任意两人之间的信息交互都是独立加密。假设用户A希望将消息T发送给用户B，A的公、私钥分别为 K_A、 k_A，B的公、私钥分别是 K_B、 k_B，那么他们之间的信息交流步骤如下：

1. B告知A自己的账户地址（公钥） K_B；
2. A将自己的私钥 k_A和B的公钥 K_B通过ECDH计算出共享秘钥S
3. A将 T用 S通过AES将T加密生成 T'；
4. 用户A通过NetCloth网络将密文 T'发送给B；
5. 用户B使用自己的私钥 k_B和A的公钥K_A，获取共享秘钥S
6. 用户B将密文 T'通过AES解密获得信息 T。



1.4 信息转发

信息转发由NetCloth中的海星节点（NetCloth的服务节点称为海星节点）来负责。任何一个网络使用者都能成为海星节点，建立自己的通信服务器。首先，使用者要拥有自己的账户和一个具备公网IP的服务器，下载通信服务开源代码并执行。最后完成IPAL申明，即可为所有使用者提供信息转发服务。由于转发内容是由用户本地独立加密后发出，其破解难度及成本使得海星节点不会有窃取用户数据的动机。

1.5 总结

按照以上方式，我们实现了使用者之间去中心化的即时通信问题。该应用已经开源至github上，并上架了应用市场(App Store及Google Play)。这是我们基于中去中心化的安全通信问题开发的第一个使用场景。我们把这一版本的NetCloth网络叫做“镖局”，今年还将开发基于安全通信功能的第二个、甚至第三个开源应用（详见NetCloth生态建设2020年）。

2 网络角色

2.1 客户端-账户与钱包

NetCloth网络的账户与区块链钱包是统一的，使用者不仅可以通过一对ECC公私钥对进入未来各种去中心化的应用场景，也可以通过这对公私钥控制全部数字资产（即进入NetCloth网络的使用者能自动产生BTC、ETH等绝大部分区块链网络的钱包），当下就能使用区块链已有的去中心化应用场景。

2.2 服务端-海星节点

在NetCloth网络中，使用者通过成为海星节点能非常容易的为其他人提供服务。基于开源程序，节点只需要提供后台程序运营的基础硬件并于网络中注册，就可为其他使用者提供服务，省去了程序开发的成本。节点之间的关系是并行的海星组织关系，使用者能随意切换提供服务的节点，唯一能衡量节点服务质量优劣的是使用者。

2.3 共识端-验证人

NetCloth网络的共识端，用于维护网络的稳定性。主要包括网络使用凭证NCH的获得与交换、网络服务关系的记录、生态系统的建立与维护三个方面。NCH的获得是基于BPoS（BFT+PoS）算法，即持有者共同制定和维护网络规则。网络中使用者和服务者的账户（公钥）都会由验证人记录于公开账本，以保证网络关系的确定性和不可篡改。生态场景通过侧链实现，每个场景都需要在NetCloth主链上申明建立人并定期同步区块内容，以保证侧链稳定运行。

共识端的维护者统称为验证人，任意海星节点都可注册成为验证人，得票数前100名的验证人称为活跃验证人，参与网络记账。活跃验证人每年总量恒定增加10名，上限不超过300名。

3 网络治理

3.1网络使用凭证-NCH

对等网络中的激励问题是区块链网络凭证产生的原因。由于对等网络的节点是匿名的、完全自治、理性自私的，使得系统存在稳定性差和节点作弊的问题。区块链中使用凭证的出现，就是用于解决以上问题。因为使用凭证是基于一般等价物的激励模式，因此又被称为数字资产，如BTC、ETH等。

NetCloth网络中的使用凭证是NCH，用于公开信息记录、所有权证明和共识维护。

3.2 共识机制（BPoS）

我们认为越是利益相关者越不会对网络稳定进行攻击，因此NetCloth网络的共识算法是基于拜占庭容错和权益证明的，简称BPoS。BPoS是确定型证明，能够容忍网络中1/3的验证人离线或故障，同等安全性下能容纳更高的交易吞吐量，使得交易确认速度更快且减少了节点恶意分叉的风险。

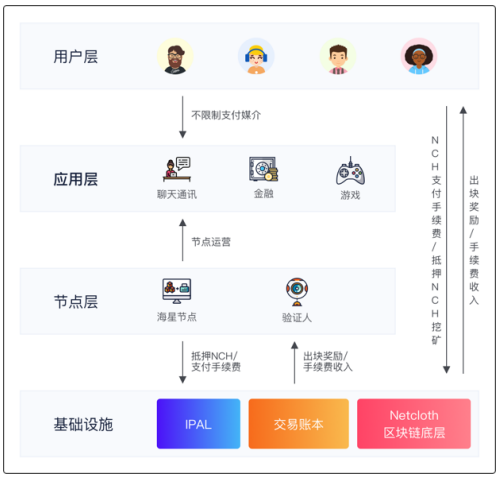
3.3 治理与投票

NetCloth网络的治理主要用于避免网络作弊和生态自治。对于权力较大的使用者，通过NCH抵押和公共监督的形式来防止其作弊；对于灵活性较高的生态，提供弱共识的自治方式，生态建设者可以约定自己的共识机制，主要用于侧链生态建设的高性能与安全稳定。

我们认为链下治理是链上治理的过渡阶段。在弱共识的侧链上，允许生态建设者进行链下治理，作为链上治理的补充。

我们认为，主网相关的基本参数验证人节点数量、网络最低使用费用、侧链映射标准等参数，需要通过链上提案与投票进行治理。所有NCH的持有者有权参与提案及投票。而例如具体业务服务质量等评价，将主要由链下治理的方式完成。

3.4 生态架构



上图为NetCloth网络的架构图，其中IPAL是主链上的一种特殊寻址申明，可以视为寻址协议。节点层与账本层之间通过NCH作为使用媒介，完成海星节点的公开信息披露和不可篡改；应用层与用户之间不限制使用媒介，方便不同国家和地区的海星节点。NetCloth是无门槛的公开区块链网络，使用者能够以最低的成本成为海星节点，服务不同国家和地区的其他使用者。根据NetCloth网络的开发路线图，将支持不同功能的去中心化应用场景。

4 重点技术

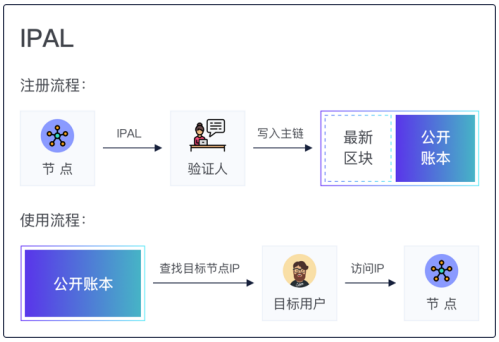
NetCloth网络的每一个版本都将只侧重简介一到两个关键技术，其余内容均可从github上的文档和开源代码中了解。开源地址：https://github.com/netcloth

4.1 虚拟机

为了降低开发者学习和编写智能合约的成本，NetCloth网络已经集成EVM，后期将逐步升级为eWASM。

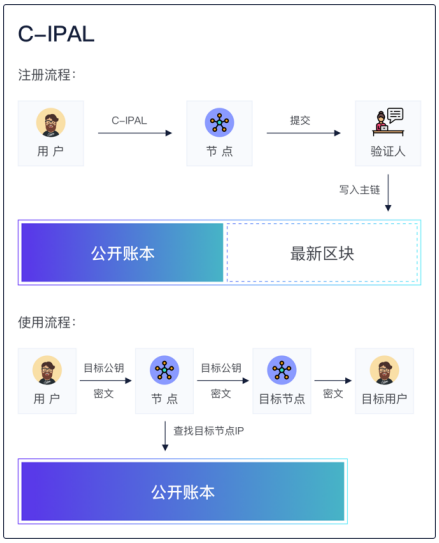
4.2 IPAL寻址协议

IP Address List 是NetCloth网络特有的寻址模块，IPAL记录的是海星节点的信息，包括接入点IP、节点名、联系方式等信息。用户可以通过链上查找IPAL列表，筛选自己喜欢的海星节点并使用服务。



4.3 C-IPAL申明

C-IPAL（Client IP Address List）协议是IPAL的一种扩展，面向客户端用户。用户使用各类服务均需要通过C-IPAL申明地址。C-IPAL具体的实现方式已在1.2章中阐述。



4.4 侧链

NetCloth的侧链和主链的完全去中心化不同。侧链允许部分去中心化，可大幅提升交易处理速度，适合运行大规模、高并发的应用场景，作为主链性能的扩展。侧链允许使用者发行侧链凭证，其发行方式与主链凭证发行不同，侧链验证人首先必须是主链验证人，其次需要使用智能合约设定主链凭证与侧链凭证之间的固定兑换比率，最后通过运行合约兑换侧链凭证。

5 路线图

NetCloth网络将通过主网升级的方式，陆续实现去中心化的各个功能，升级路径分为4个阶段，分别是镖局、集装箱、集市、工厂。

5.1 信息交互-镖局

我们将第一个版本命名为镖局，为使用者提供解决去中心化的安全通信的开源代码。使用者可以直接实现即时通信服务，也可以基于开源代码进行二次开发，实现如社交、信息交互类游戏等其他场景的应用。

5.2 数据存储-集装箱

第二个版本称为集装箱，为使用者提供安全可靠的去中心化数据存储功能，将主要分为本地存储、集群存储和去中心化存储。其中去中心化存储，将使用读取付费的方式，实现对有价值数据的筛选，筛选出被反复“回忆”的数据，以实现网络的群体记忆。

5.3 数据交换-集市

该版本是基于使用者已经拥有自身数据的情况下而开发的功能，主要为使用者提供各类数据交互、交换的智能合约以完成数据的合理使用和存证，保证使用者的数据安全和利益不被侵占。

5.4 可信计算-人工智能工厂

NetCloth的最后一个功能版本将针对数据极易复制的特性，提供第三方可信计算空间，通过时间、动机和成本来阻止海星节点对使用者数据的窃取。结合集市的数据交互与交换功能，我们认为这个版本将训练出大量的人工智能模型，所以我们将它称之为人工智能工厂。

6 社区门户

- 官网：https://www.netcloth.org
- 开源地址：https://github.com/netcloth
- Blog：https://blog.netcloth.org
- Twitter：https://twitter.com/NetCloth
- Medium：https://medium.com/@NetCloth