NewCloud 白皮书

目录

1. 背景
2. 为什么选择Variant
3. 项目介绍
4. 技术方案
    4.1.账户系统
    4.2.双向锲入的侧链方案
    4 .3 共识机制
        4.3.1 DPOS
        4.3.2 委托人选举
        4.3.3 拜占庭容错
        4.3.4 委托人选举
    4 .4 隔离桥接设计
    4 .5 协同分级签名(Collaborative Hierarchical Signature)
    4 .6 分布式存储方案
    4 .7 New Cloud App Engine 动态建站
        4.7.1 动态代码解析
        4.7.2 NewSQL 区块链数据库
        4.7.3 NAE 优势
    4 .8 智能合约
    4 .9 New OS
        4.9.1 什么是 New OS
        4.9.2 New OS 架构图
        4.9.3 去中心化数据存储&动态建站&手机挖矿
        4.9.4 硬件隔离私钥管理理(HD PKM)

目录

5. 代币介绍
5.1.什么是区块链资产
5.2.NEWC
5.3 分配方案
6. 风险提示
7. 免责声明

1.背景

区块链概念来源于比特币，中本聪详细描述了如何创建一套去中心化的电子交易体系。这种体系不需要创建在交易双方相互信任的基础之上，首次通过技术手段实现了交易主体间共识机制的建立，而“区块链”技术正是构成这种电子交易体系的基础技术。为了实现比特币协议，中本聪使用非对称密码解决电子货币所有权问题，用区块时间戳解决了交易的存在性问题，用分布式账本解决了交易的验证问题，最后统一的区块链解决双重支付问题。

以太坊（Ethereum）是继比特币之后的又一个开创性的区块链项目。以太坊开创性地将智能合约（Smart Contracts）和区块链结合起来，在交易主体间共识机制建立的基础上，通过自动触发可执行的电子合约，解决了交易主体间承诺履行的问题，有效推动了区块链产业化应用的进一步发展。

近年来，区块链技术的不断发展和随之而来的数字货币热潮，它所带来的多主体共识协同机制的思想，将对社会治理和商业运作产生深刻的影响。目前人们已经广泛认识到区块链巨大的应用价值，但是区块链的技术发展却还没有到达成熟阶段，尤其在企业级应用方面，区块链的交易并发能力、数据存储能力、通用性、功能完备性、易用性都还存在明显不足。

2.为什么选择Variant

Variant全称为Variant Network，是全球首个基于UTXO模型的分片(sharding)算法的公有链项目，是融合IPFS和AI的新一代智能合约区块链3.0平台。 基于UTXO模型的分片(sharding)算法显著提高了交易吞吐量，Proof of AI 共识算法赋予了区块链机器学习的能力，智能合约虚拟机融合IPFS解决了大数据存储的痛点。Variant 致力于让算力为社会产生真正的价值，不断突破区块链的能力边界让去中心化应用的落地成 为可能。

不同于其他智能合约平台。目前现有的智能合约平台主要是基于工作量证明 (POW)，而工作量证明(POW)的共识机制由于资源和硬件限制很难被部署到大规模的应用场景中。同时共识机制本身缺乏

灵活性，因为参与者的不同，在公有链中和联盟链中，对共识机制的要求是不一样的。Variant 系统包括 Variant 公链和 Variant 侧链，因为网络环境和参与者的不同，考虑到公链的去中心化程度、参与门槛、安全性和可靠性，在公链网络中使用基于 POS 机制的 IPOS 。因为侧链对共识机制的考量不同于公链网络，所以Vriant 侧链提供的智能合约虚拟机和分片算法，可以满足可信网络中，对区块链速度和容量的要求。

同时现有区块链系统具备很大的封闭性，目前大多数智能合约的触发条件来自于 区块链系统本身，很少有外界的触发条件，缺乏与现实世界的交互。而通过Variant 系统中的 Oracle 和 Data Feed 可以把现实世界的数据作为合约触发条件，打破智能合约本身的封闭性。

NewChain是一个由未来众多分布式储能设备为全节点的共有链，基于Variant来构建 NewChain，能更好的保证整个NewCloud云生态的安全稳定、去中心化，并且拥有极高的性能来处理能源信息流与价值流间的沟通。

3.项目介绍

NEW Cloud是一个去中心化存储网络，它让云存储变成一个算法市场。这个市场运行在有着本地协议令牌的区块链。区块链中的旷工可以通过为客户提供存储来获取NEWC,相反的，客户可以通过花费NEWC来雇佣旷工来存储或分发数据。和比特币一样，NEW Cloud的旷工们为了巨大的奖励而竞争式挖区块，但NEW Cloud的挖矿效率是与存储活跃度成比例的，这直接为客户提供了有用的服务（不像比特币的挖矿仅是为了维护区块链的共识）。

这种方式给旷工们创造了强大的激励，激励他们尽可能多的聚集存储器并且把它们出租给客户们。NEW Cloud 协议将这些聚集的资源编织成世界上任何人都能依赖的自我修复的存储网络。该网络通过复制和分散内容实现鲁棒性，同时自动检测和修复副本失败。客户可以选择复制参数来防范不同的威胁模型。该协议的云存储网络还提供了安全性，因为内容是在客户端端对端加密的，而存储提供者不能访问到解密秘钥。它对去中心化数据，构建和运行分布式应用程序，以及实现智能合同都非常有用。

NEW Cloud 在设计之初，秉承的理念就是通过开放、创新、合作，让区块链能够更好的服务于当前和未来的企业，通过区块链的分布式节点、安全、无法篡改等特性可以解决企业用户在大数据存储、建站、资产数字化等等方面所面临的痛点，使得企业以极低的成本在一个安全、高效、大数据量、大吞吐量、高 TPS 的区块链分布式应用平台上构建自己的系统。

NEW Cloud 协议由四个新型组件组成

① 去中心化存储网络(Decentralized Storage Network)(DSN)：我们提供一个由提供存储和检索服务的独立服务商网络的抽象（在第二节）。接着我们提出了NEW Cloud协议作为激励，可审计和可验证的DSN构建（在第4节）。

② 新型的存储证明：我们提出了两种新型存储证明方案（在第三节）：（1）“复制证明”（Proof-of-Replication）允许存储提供商证明数据已经被复制到了他自己唯一专用的物理存储设备上了。执行唯一的物理副本使验证者能够检查证明者是否不存在将多个数据副本重复拷贝到同一存储空间。（2）“时空证明”（Proof-of-Spacetime）允许存储提供商证明在指定的时间内存储了某些数据。

③ 可验证市场：我们将存储请求和检索需求作为两个由NEW Cloud网络操作的去中心化可验证市场的订单进行建模（在第五节）。验证市场确保了当一个服务被正确提供的时候能执行付款。我们介绍了客户和矿工可以分别提交存储和检索订单的存储市场和检索市场。

④ 有效的工作量证明（Proof-of-Work）：我们展示了如何基于“时空证明”来构建有效的工作量证明来应用于共识协议。旷工们不需要花费不必要的计算来挖矿，但相反的必须存储数据于网络中。

4.技术方案

4 .1 账户系统

NEW Cloud 的每个账户由一个口令、一对公私钥、一个地址组成。用户还可以额外设置一个二级密码。注意这里与比特币有所不同的是，每个账户仅对应一个地址，而比特币中每个钱包对用多个地址和私钥。

口令(passphrase)是符合 BIP39 标准的用于产生确定性钱包的助记符。这种助记符与二进制或十六进制字符相比对人类记忆更友好。口令的生成方式是将一个 32bit 倍数长度的熵转换成若干个单词，NEW Chain 系统选择的熵长度为 128bit，将转换成 12 个单词。口令作为一级密码，由用户保管，不对外公开，一旦丢失用户将失去对应账户的所有权。口令 形式如下:

```
barely decline dust stamp protect color certain cup arena busy
latin shell
```

密钥对包括公钥和私钥，是以口令的 sha256 哈希做种子，再通过 ed25519 爱德华兹 曲线签名算法生成的。形式如下:

```
公钥:
9989388b220a13465e49f52df5ba28ba08eb1e7a973320347f9687a107dc2f 9a
私钥:
91e891f653e3ed0232d8c7de2e72b625d50d48593fc0fb570c0db25c5e4456
9a9989388b220a13465e49f52df5ba28ba08eb1e7a973320347f9687a107dc 2f9a
```

账户地址是取公钥的 sha256 哈希的前 8 位，逆序后转换成 bignumber，其形式如下

```
5034187504202890358
```

4 .2 双向锲入的侧链方案

为了将Variant父链币转移为NEW Chain侧链币，VAR被发送到Variant上的一个特殊输出中，该输出只能由NEW Chain上拥有的一个SPV证明来解锁。为了在两条链上进行同步，我们需要定义两个等待周期：

1．侧链间转移的确认期，是指币在转移至侧链之前，在Variant上必须被锁定的期间。此确认期目的是生成足够多的工作量，让下一个等待期内的拒绝服务攻击变得更困难。

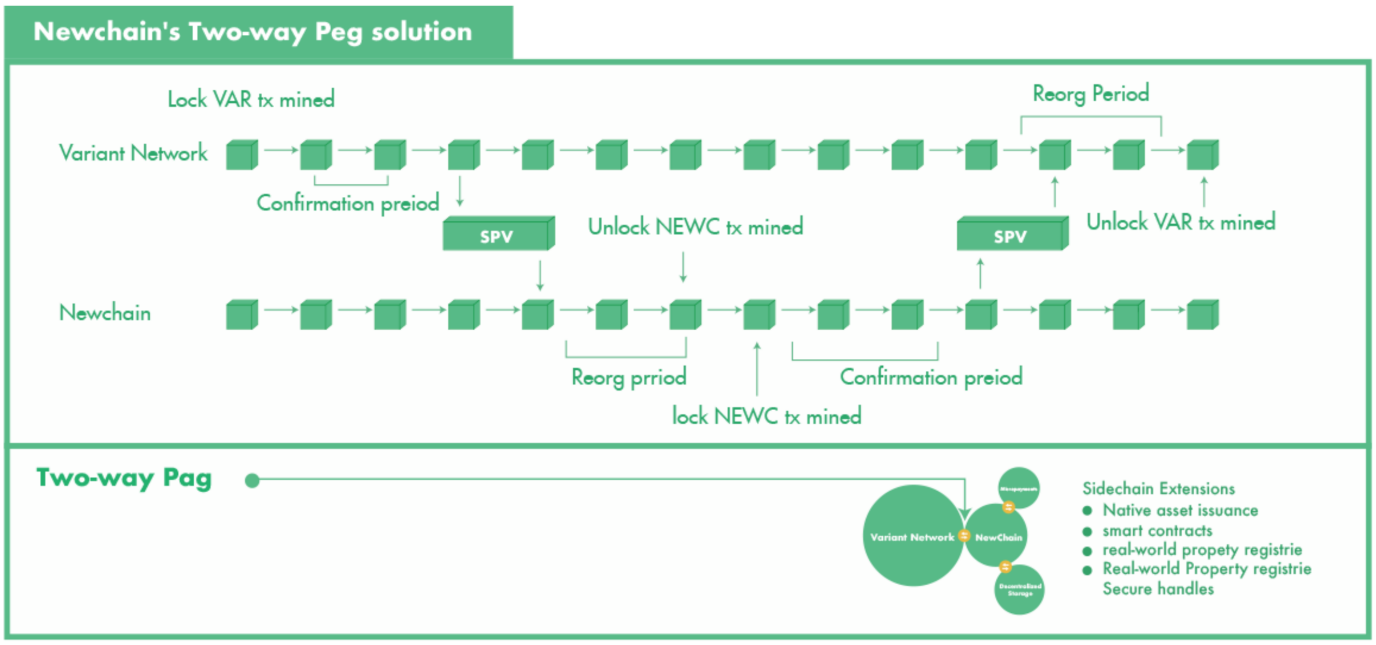
当Variant上生成了特殊输出后，用户等待确认期结束，然后在NEW Chain上生成一个引用该输出的交易，提供出一个它已被创建并在Variant上被足够工作量覆盖的SPV证明，

2．接下来，用户必须等待一个竞赛期。这个期间，新转移过来的币不能在NEW Chain上花费。竞赛期的目的是防止重组时出现双花，在重组期间转走先前锁定的币。在这个延迟期内的任何时刻，如果有一个新的工作证明发布出来，对应的有着更多累计工作量的链中没有包含那个生成锁定输出的区块，那么该转换将被追溯为失效。我们称此为重组证明。

只要有可能，所有NEW Chain上的用户都会有动力来制发重组证明，因为对不良证明的承认会稀释所有币的价值。

当币在父链Variant上被锁定时，该币可以在NEW Chain内自由转移，不需要与Variant进一步交互。不过，它仍保留着父链币的身份，仅能转回到它所来的那一条链上。

当用户想把币从NEW Chain上转回Variant时，与原先转移所用的方法相同：在侧链上将币发送至一个SPV锁定的输出，产生一个充分的SPV证明来表明该输出已完成，使用这个证明来解锁父链上先前被锁定的那个等面值的输出。整个转移过程如下图所示。



我们假设 A 用户要将手中的 1 个VAR换成 B 用户手中的 10000 个NEWC，那么可以写一个智能合约运行在侧链上，合约相当于一个账本，记录和 A 和 B 用户可从合约提出 的NEWC，合约约定:

1. 创建智能合约，初始时A和B在合约里面的账目都是0。

2. B用户在合约创建后向合约转入10000个NEWC，记在B用户账上。

3. 账目发生变化后，双方都不能将NEWC从合约马上转走(提现)，必须在状态变化后经 过 N 个块的锁定时间才能转走。N 个块的时间必须大于其他链上交易的确认时间和侧链同步块数据时间之和。如果在这期间账目又发生变化了，那么能够转走的时间也将按照这个规则往后延。

4. A向B发起比特币交易时，会设置一个锁定时间，这个时间要大于上面的锁定时间。

5. 合约监听Variant上的交易信息，当收到 A 向 B 转对应比特币的交易事件后，在合约里面记录交易相关信息，并且在后续收到块信息时验证这笔Variant交易有没有双花。如果经过 7 个块确认并且没有双花后，合约将 B 用户账上减 10000 个NEWC，在 A 用户账 上加 10000 个NEWC。这时候 A 账上有 10000 个NEWC，B 账上有 0 个NEWC。

6. A用户在N个块后从合约将10000个NEWC转到自己的账户里。

7. 如果出现侧链数据同步延迟或者出现争议，一方可以将双方从合约提现的时间延后。如果一方需要马上取现，只要双方签名同意，也可以不用等 N 个块的锁定结束，马上就可以取现。

8. 由于合约是其他链上的交易驱动的，所以只要其他链上交易发生了，合约就会自动将相应的NEWC转到另外一方，所以不会出现抵赖的问题。在上面的步骤中，任意一方终止，双方都不会有损失。

4 .3 共识机制

NEW Cloud 使 DPoS和Proof Of Storage来实现区块链记账和数据存储的共识机制。

4 .31 DPOS

现有区块链项目的主要共识机制为PoW和PoS，少部分项目采用修改后的BFT(拜占庭容错)的共识机制，BTC就是PoW机制下最成功的加密货币。PoW机制虽然已经成功证明其长期稳定和相对公平，但在现有框架下，采用PoW的“挖矿”形式，将消耗大量的能源。其消耗的能源只是不停的去做SHA256的运算来保证工作量公平，并没有其他的存在意义。目前BTC所能达到的交易效率为约5TPS(5笔/秒)，以太坊目前受到单区块GAS总额的上限，所能达到的交易频率大约是25TPS，与平均千次每秒、峰值能达到万次每秒处 效率的VISA和MASTERCARD相差甚远。

为了让处理效率能有质的突破，DPoS机制应声而出。DPoS(Delegated Proof of Stake)机制，源于Graphene，中文名叫做股份授权证明机制（也称受托人机制），DPoS机制要求在产生下一个区块之前，必须验证上一个区块已经被受信任节点所签署。相比较于PoS的“全民挖矿”，DPoS则是利用类似“代表大会”的制度来直接选取可信任节点，由这些可信任节点(即见证人)来代替其他持币行使权力，见证人节点要求长期在线，从而解决了因为PoS签署区块人不是经常在线 可能导致的产块延误等一系列问题。它的原理是让每一个持有代币的人进行投票，由此产生29位代表，我们可以将其理解为29个(可无限扩展)超级节点或者矿池， 这29个超级节点彼此的权利是完全相等的。DPoS机制通常能达到万次每秒的交易速度，在网络延迟低的情况下可以达到十万秒级别，非常适合企业级的应用。

NEW Cloud 系统的一大亮点是使用了一个增强 DPOS 的共识算法，在 DPOS 的基础上加入了一

个高效的实用拜占庭容错算法，极大地降低了网络分叉的可能性，只要不超过 1/3 节点联合做恶，系统就不会分叉，也就没有双重支付的风险。

4 .32 委托人选举

NEW Cloud 系统的委托人选举制度与 DPOS 是类似的，核心系统是由 29个委托人节点组成，委托人是被社区选举的可信账户，得票最高的 29个委托人负责生产区块。得票排名 未进入前 29名的账户被称为候选人，当他们将来获得足够多的选票并进入前 29名后， 将成为正式的委托人。
每个 NEW Cloud 用户都有权利投票给最多 29位委托人，选票的权重是由用户持有的 NEWC 数量决定。

每一个选举周期产生 29个区块，每一次投票和委托人排名的变化将体现在下一个周期。每个区块产生的间隔时间是 5 秒，新创建的区块会被广播到网络中并添加到区块链 中。每当新的区块被添加到区块链中，该区块之前的所有交易的确认次数加一，得到 6 个 确认后，可以认为交易是安全的，如果数额较小的交易，可以允许更小的确认次数，相反，数额较大的交易可以通过增加确认数来保证安全性。

如果有少数委托人发生故障，比如被攻击或者宕机，就会错失区块，这会被记录在案，这将影响该节点的在线率，进而影响社区的投票。因此委托人的竞选是需要严肃对待的，委托人应当由有一定网站运营经验的人来做，委托人要保障自己节点的稳定性，并以此促进整个系统的安全和稳定。

4 .33 拜占庭容错

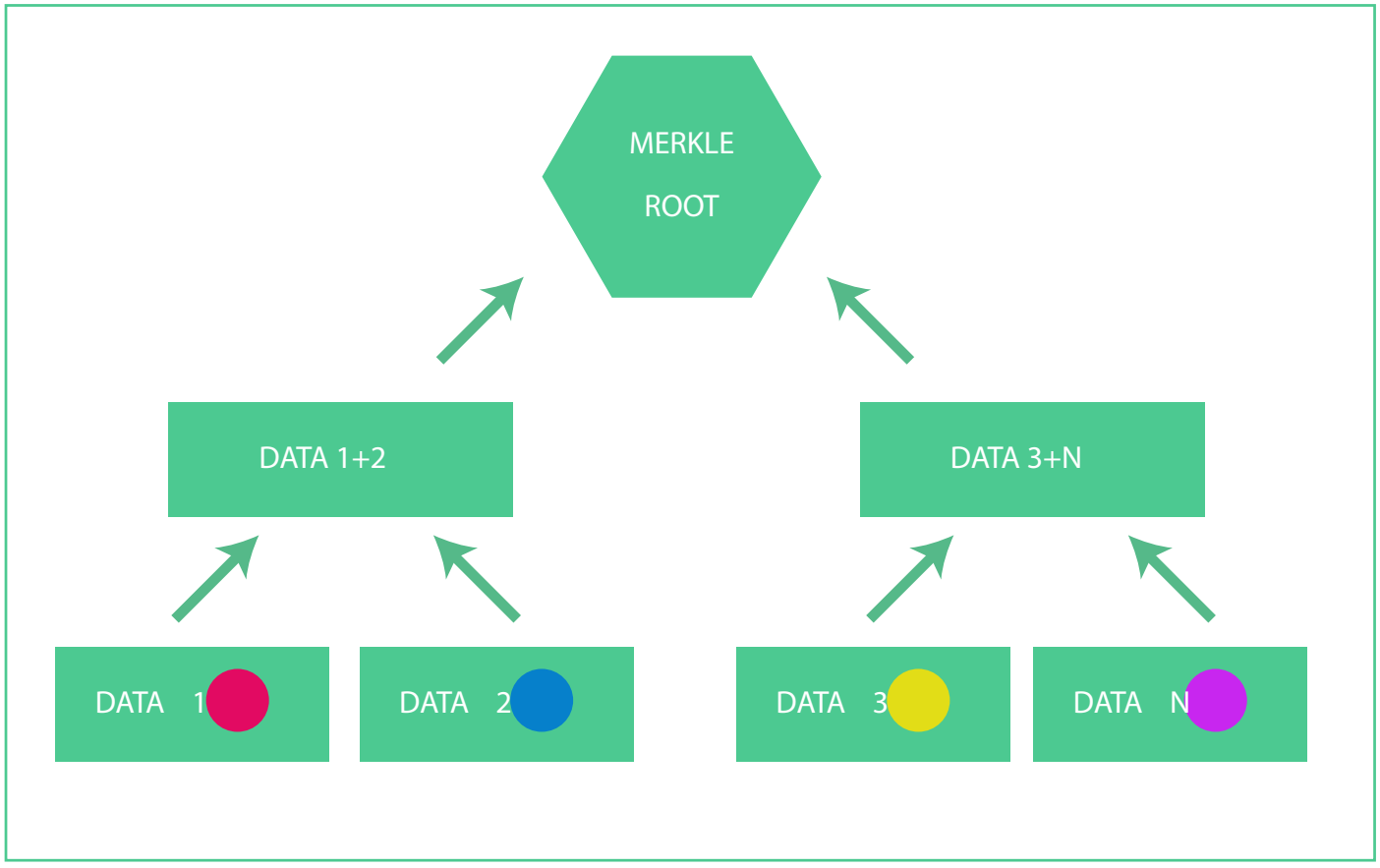
NEW Cloud系统与 DPOS 的不同主要体现在算法的后半部分。

DPOS 采用的方法是，首先对当前 round 的委托人列表进行随机的排序(保证每一轮 的委托人顺序不同，也无法预测下一轮委托人顺序)，然后通过 round-robin 的方式依次 让每个委托人创建区块。这个算法的主要缺点是，如果某个委托人节点叛变了，他可能会 广播多个不一致的区块，这些区块间可能包括双重支付交易，导致整个网络被分叉了。当 然，如果只有一个委托人叛变的话，这个分叉很快就可以通过下一次最长链同步的方法来 消除，但是随着叛变节点的增加，消除分叉的时间将越来越长，少量节点的联合叛变将严 重影响系统的安全性，即使一个交易达到 6 次确认，也很可能是不安全的。

为了解决这个问题，我们引入了 PBFT(Pratical Byzantine Fault Tolerance)算法。PBFT 算法也是使用 round-robin 的方式选择委托人，但是选出委托人后并不立即创建区块，而是首先发起一个提议(propose)，这个提议的目的是确定下一次区块的 hash。 当超过 2/3 的节点都赞成该提议时，才接受由提议人创建的的下一个区块，下一个区块的hash 必须与当前 round 达成共识的区块 hash 一致。从本质上来说，PBFT 算法的加入解 决了委托人权利滥用的问题，使得委托人的记账能力更为可控。

4 .34 Proof Of Storage

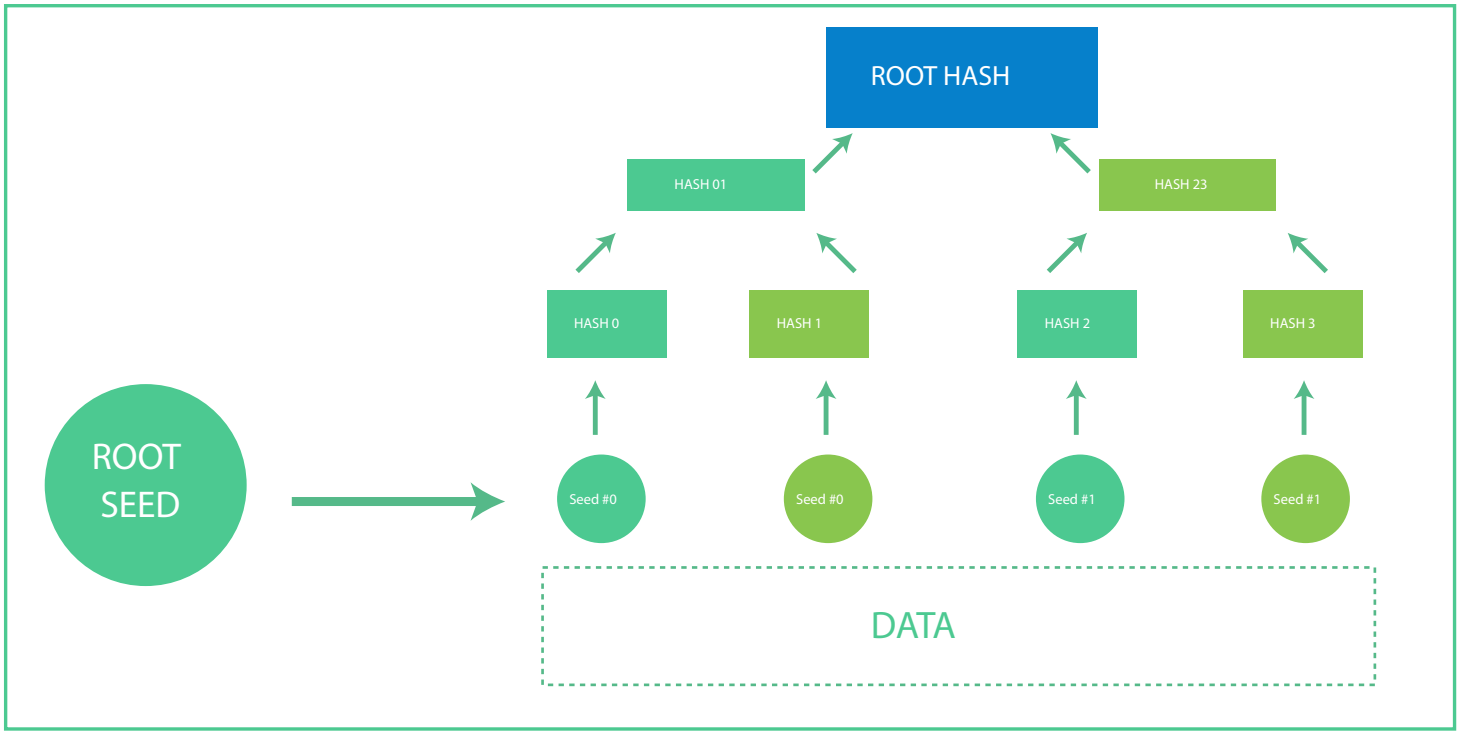
Proof Of Storage机制，是NewChain自主设计开发的共识机制，中文名叫做存储证明机制。为了实现一个去信任的数据存储网络，我们必须给客户提供一个审计方法，证明他或她存储在网络上的数据可用并且没有被修改。我们通过使用Merkle树[2]和Merkle证明来做到这一点。 我们采集数据的集合并生成Merkle树，如下图所示：



树的叶子应该是256字节碎片或更小。理想情况下，树应该比数据大，因此树应该在生成而不是存储。对远程位置上的数据的审计仅由特定索引和由位于该索引处的子分片加上Merkle树SPV证明的响应组成。

我们通过哈希挑战（质询算法）来实现审计，在客户端产生一系列种子（由根种子确定），可以添加到文件并且进行哈希，产生唯一的哈希值。我们把这个过程称为心跳。客户端产生这些哈希挑战（质询算法），建立一颗merkle树[2]并且把merkle根加入到中本聪类型的区块链中。然后把除去叶子节点的merkle树发送给农户。客户端可以定期的发送种子给它托管数据的农户，检查农户的返回结果是否能和它产生的哈希值匹配，通过验证农户返回的值与merkle树中的值。（客户端自己有完整的merkle树，所有节点都在，农户只存储了某一个碎片，给它发送种子，它会返回一个哈希值，我检查这个哈希值是否在我的merkle树中就可以了）

农户不能修改或者删除文件，因为他或她进行哈希挑战（质询算法）时会失败，这会在第8节深一步描述。通过加密和哈希的前提，这些心跳不能蛮力强迫。客户端不能欺骗农户，因为哈希返回值能够通过merkle根验证，它是加入到区块链中的。这样，我们用区块链给存在证明背书，以使各个部分都是诚实的。

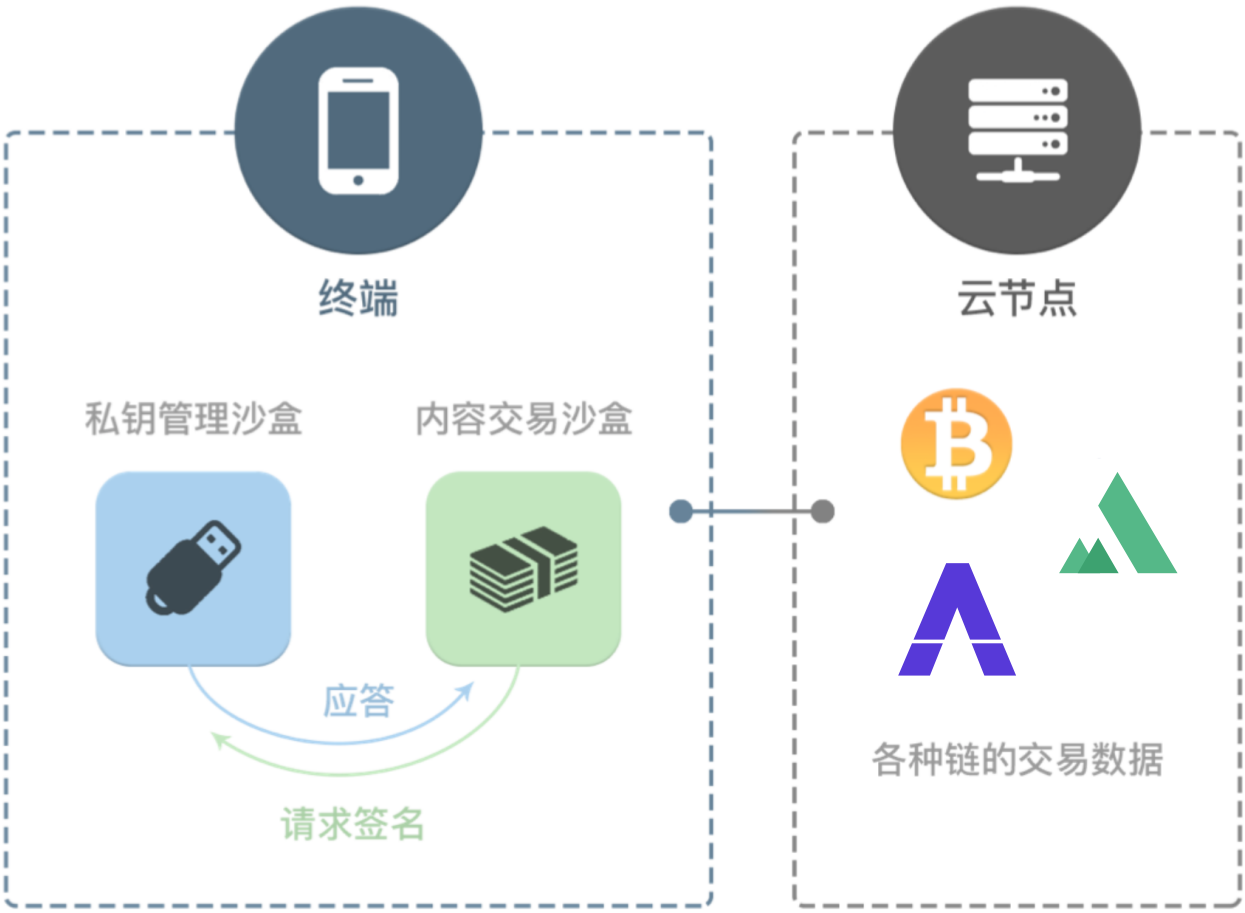


4 .4 隔离桥接设计

NEW Chain 钱包被特意设计成两个独立沙盒(Sandbox)来实现高安全性:私钥管理沙盒 (Private Keys Management，以下简称 PKM)和内容交易沙盒(Exchange Client，以 下简称 EXC)。其中 PKM 仅包含两个功能:一是管理种子和私钥，二是为交易提供签名。

EXC 负责从服务器加载数据，如发起交易、检查交易等。双沙盒的分离设计，可以杜绝因内存共享而泄露私钥的可能性。

由于 PKM 功能的独立性，它并不需要使用网络:所以从安全性考虑，设计它为离线 沙盒。首先，种子和私钥完全没必要也不应该与服务器共享，仅仅存储在本地即可。其次， PKM 的签名服务也是在本地进行的，它接受 EXC 的调用请求并给出应答。下图是 NEW Chain 钱包的结构示意图。



4 .5 协同分级签名(Collaborative Hierarchical Signature)

协同分级签名允许多人共同管理该钱包。它既可以防止单点故障，又可以增强账户的 安全级别。协同分级签名设置了这样一个条件，假如记录脚本中的公钥分为 W 级，则至少 需要提供 V 级满足 M-N 组合的公钥才能解锁。通用的 W-V 协同分级签名锁定脚本形式为:

```
W <PK1j Multi Sign> <PK2j Multi Sign> .. <PK1w Multi Sign > V CHECKMULTISIG
```

其中 PKij Multi Sign 的脚本可扩展如下:

```
PKij Nij <PK(i+1)1 Multi Sign><PK(i+1)2 Multi Sign>...<PK(i+1) Nij Multi Sign> Mij
```

它表示，第 i 级的第 j 个公钥，包含的子公钥有 Nij 个。每一层的子公钥需满足 M-N 组合 多重签名。最终综合形成 W-V 协同分级签名。3-2 协同分级签名条件，其中一种状态如下 图所示:

上述脚本可以由含有签名和公钥的脚本予以解锁:

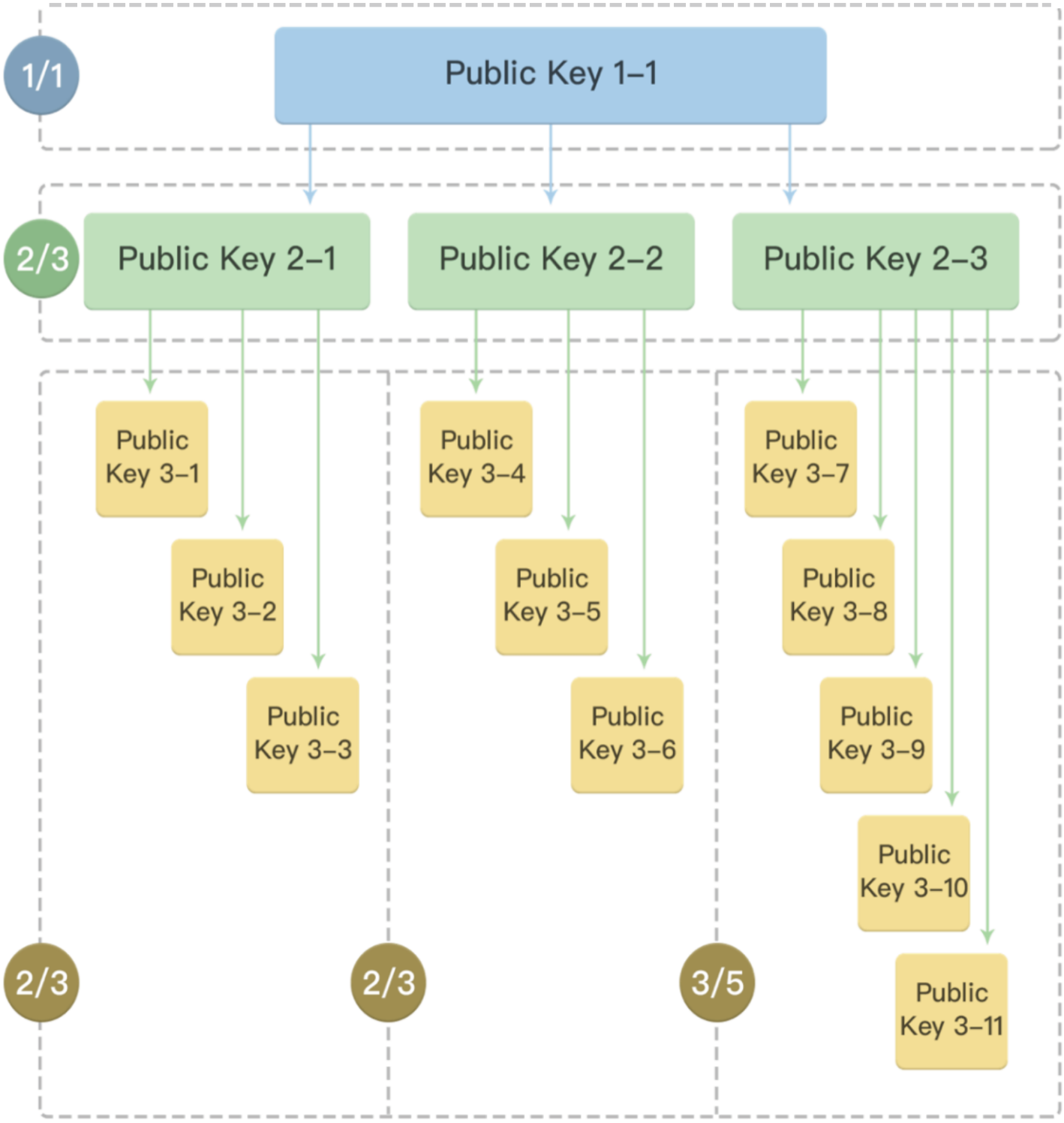
```
<Sign 3-4> <Sign 3-5> <Sign 2-1> <Sign 2-3>
```

或者 3 级存档公钥中任意 2 级相一致的私钥签名组合予以解锁。 两个脚本组合将形成一个验证脚本:

```
<Sign 3-4> <Sign 3-5> <Sign 2-2> <Sign 2-3> 3 <3 <PK3-1><PK3-2><PK3-3> 2 PK2-1> <3 <PK3-4><PK3-5><PK3-6> 2 PK2-2> <5 <PK3-7><PK3-8><PK3- 9><P-K3-10><PK3-11> 3 PK2-3> <PK1-1> 2 CHECKMULTISIG
```

执行时，只有当锁定脚本与解锁脚本设置条件相匹配时，组合脚本才显示得到结果为 True。上述例子中相应的设置条件即为解锁脚本是否含有与 3 级公钥中任意 2 级私钥(每级符合 M-N 组合多重签名)的有效签名。

Collaborative Hierarchical Signature



4 .6 分布式存储方案

在NewChain生态中，数据被存在多个存储供应者的主机里，通过Reed-Solomn（代码算法）使文件分成多个部分，存储在各个托管主机里。

假设把一个文件分成3个碎片，在无数个托管主机中随机选出30个用来重复存储，每个机器存储一个碎片，这个“3对30”的方案意味着文件会有十个备份，只要能够提取出3个各不相同的碎片，这个文件就能被完整下载。按照数学的算法，存储文件的30个托管主机中只要有12个托管主机正常在线，就能够正常提取出完整的文件。有的人会疑问如果文件容量太大怎么办？托管主机能够容纳的下吗？如果遇到这种情况，只要把文件分割更多份就可以了，每个碎片就会很小。

每个托管主机接收到的加密文件，都会受到合约的约束。

所有存储数据进入NewChain客户端的时候都被分割成很多小块，只留下用于恢复数据的少数片段；敏感的用户信息块被压缩到4MB，用于保护用户隐私；最后，每个压缩块又使用客户端的秘钥进行加密。托管主机只会接收到一个加密的二进制块，并且没有存储文件其他部分的任何信息。当一个文件上传时，智能合约将确保：托管主机只有在完成约定的保管条款后，才能拿到支付款。托管主机也要缴纳一定的押金，如果没有完成合约，它不仅得不到支付款，还会失去部分押金。
即使文件受到黑客攻击，他们也需要破解每个文件碎片的秘钥，用以恢复文件。当黑客试图篡改数据时，客户存有加密校验将提醒用户注意，用户可以随时取回文件并销毁云存储数据。

对于Sybil冗余攻击，我们的机制也能有效防御。因为每个碎片都是唯一加密的，因此，攻击者不能通过审核，除非他们有每个唯一冗余副本。客户端节点应按照步骤将其冗余副本分发给地理上分布且独立的节点。如果随机分散，相同的冗余片被托管在同一个控制节点的概率在统计学上概率相当小。采用随机分布和我们独特加密冗余副本的标准方法，攻击者是不能进行Sybil冗余攻击的。

这种实现点对点加密技术的对等云存储网络，它允许用户能够不依赖第三方数据供应商而传输和共享数据。验证机制预防了女巫攻击和节点连接失败，通过使用独特地加密冗余副本，和定期检查文件可用性和完整性的审核算法。通过使用加密货币，我们提供适当的激励促使网络壮大，并且能够在客户和农户之间进行数据交易。我们给予客户足够的权力，超过了处理文件验证和支付的算法。使用这些方法，我们把云上数据的控制权交还给用户。

系统特点

- 随处等同：全网无中央数据中心，任何人都可以随处获得其存储的数据，快速有效，动态的数据分布系统可以实现自动，智能的动态数据跟随。
- 永久记录：分布存储，冗余备份，互不影响，永久存储，直至主动消除或者人类社会尽头。
- 无人管控：所有参与者责任平等，能力相同，所有人都可以参与，遵守去中心化的特性，因此无人管控。
- 多协议支持：兼容支持多样P2P协议（如IPFS,MAGNET,BITP2P,PPK），保证网络文件传输的高效和稳定。
- IPFS技术支持：IPFS点对点对等分布式超文本协议，让网络更快，更安全，更开放。基于全球统一的可寻址空间，使用唯一的哈希值，对文件进行验证。
- 激励机制：存储空间的终端将由文件存储方支付相应的奖励，性能越强存储量越大获得奖励越多

4 .7 NewChain App Engine 动态建站

在NewChain生态中，用户除了可以存储文件以外，还可以上传网站代码，通过29个高性能受托人节点进行代码动态解析。

NewChain App Engine(NAE)是全球首家公有链云服务商，应用托管平台，分布式Web应用/业务开发托管、运行平台。

NAE是真正意义上具有高可靠、高扩展、免运维的区块链计算服务,致力于成为全球最大的BaaS(-Blockchain as a Service)服务厂商。

4 .71 动态代码解析

NAE支持PHP、Java、Python三种语言环境，适用于多种业务场景。NAE基于先进的容器资源隔离技术，并采用多层沙箱保护提供安全运行环境，同时针对运行环境提供了多种扩展服务，并提供了可视化的控制面板。既拥有了传统虚拟主机的易用性，同时具备攻击隔离、弹性扩展等云产品特性，使得中小型网站用户的网站运行更加稳定和安全。

4 .72 NewSQL 区块链数据库

NewSQL 通过 SQL和 API 的接口为上层应用场景提供区块链基础服务的功能。核心定位于打造领先的企业级区块链基础平台。中间是平台产品服务层为 New Platform，在底层（New SQL）之上构建高可用性、可扩展性的区块链应用基础平台产品，其中包括共享账本、鉴证服务、共享经济、数字资产等多个方向，集成相关领域的基础产品功能，帮助企业快速搭建上层区块链应用场景。应用服务层（Trust Application）向最终用户的提供可信、安全、快捷的区块链应用，腾讯未来将携手行业合作伙伴及其技术供应商，共同探索行业区块链发展方向，共同推动区块链应
用场景落地。

4 .73 NAE 优势

1)直接将你的服务连接到区块链上，永不宕机，免除监管；

2)通过外包托管服务降低开销；

3)免除昂贵的租用高带宽线路费用；

4)集中精力在核心商业目标上，而不是将时间和金钱消耗在复杂的主机和连接问题上；

5)您的WEB、和电子商务应用受益于快速可靠的因特网访问；

6)享受安全，高速的因特网访问；

7)弹性扩容。

4 .8 智能合约

在 NewChain 区块链系统中，将智能合约设计为一个包含代码和数据存储的链上对象。合约的拟定者可以用支持的计算机语言描述合约条款，设定执行条件，以及达到执行条件后执行的 操作，参与接口等。在合约拟定者将合约注册到区块链上后，其他用户可以通过调用接口来参与合约。在合约语言正确表述合约内容的前提下，在达到执行条件时，系统会按照合约代码的描述执行相应的操作。并不会有现实中参与方拒绝履行条款的现象。

NewChain默认使用Variant的智能合约虚拟机，Variant VM 拥有优秀的性能和AI学习能力，NewChain也因此获益。

除此之外，NewChain也可以支持拓展其他类型的合约虚拟机，智能合约的升级本身是极具争议性的题目，但现实商业环境中即使软件经过了最严苛的测 试依然可能存在需要升级智能合约的情况，这份权利应该被如何控制和监控，从而避免区 块链不可篡改的特性。NewChain 从博弈论的角度通过升级协议最终实现智能合约的升级，保障各方利益。根据与智能合约产生交易及充值金额赋予相关账户不同的投票权重，由区块 链的出块账户冻结该智能合约的交易，如果对新智能合约代码(新的合约字节码链上 HASH 值)按投票达到了 81%的比例支持，智能合约将按照预定的协议升级，而之前智能 合约的状态与存贮都将被保留下来。

4 .9 New OS

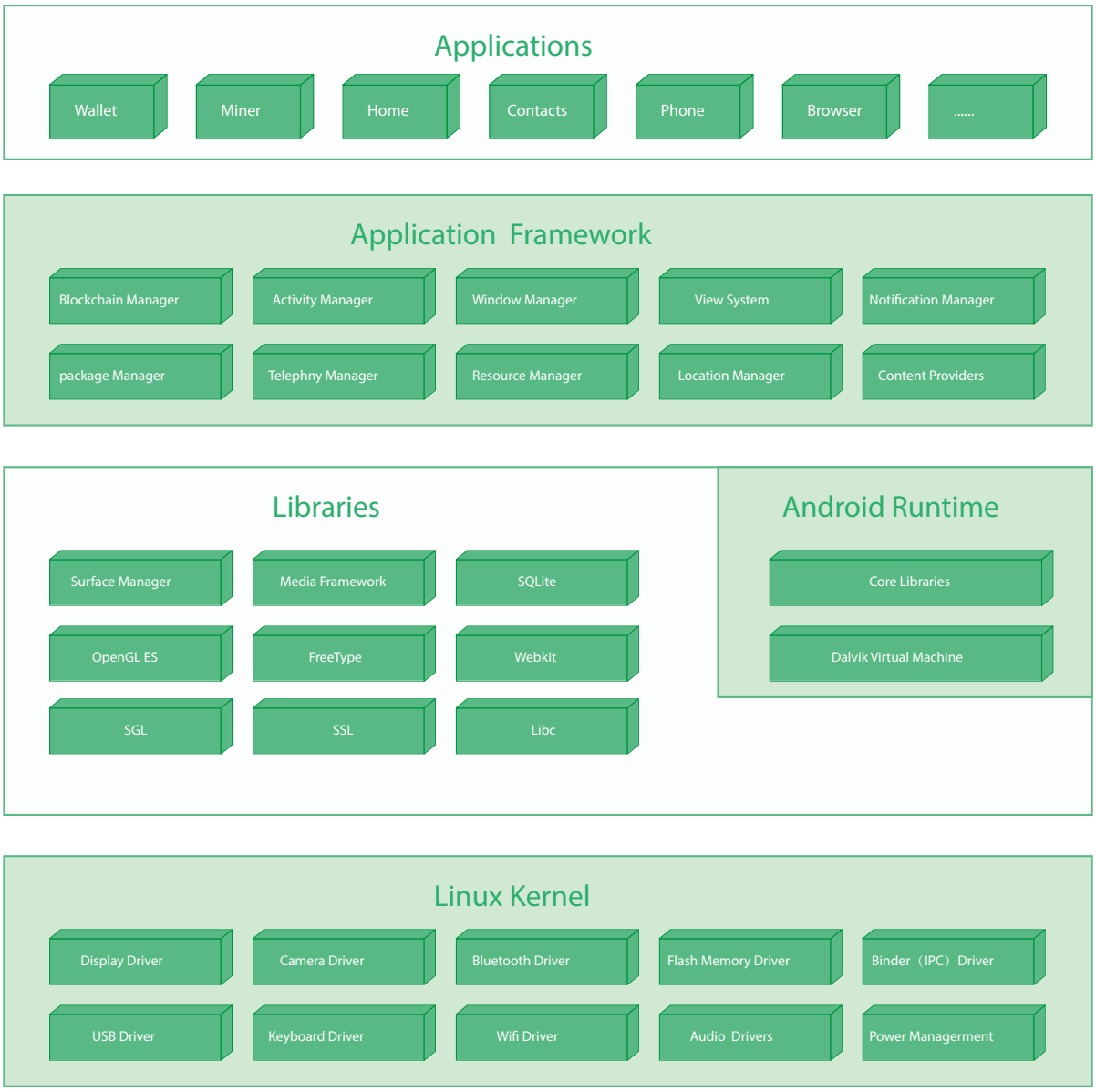
4 .91 什么是 New OS

New OS 是基于Android操作系统进行深度定制的区块链手机操作系统，将区块链核心代码整合到操作系统层面，手机启动同时启动区块链的网络通信。这样使区块链更好地适配手机硬件和网络性能，提高区块链运行的稳定性、可靠性，也带来更大的安全性。

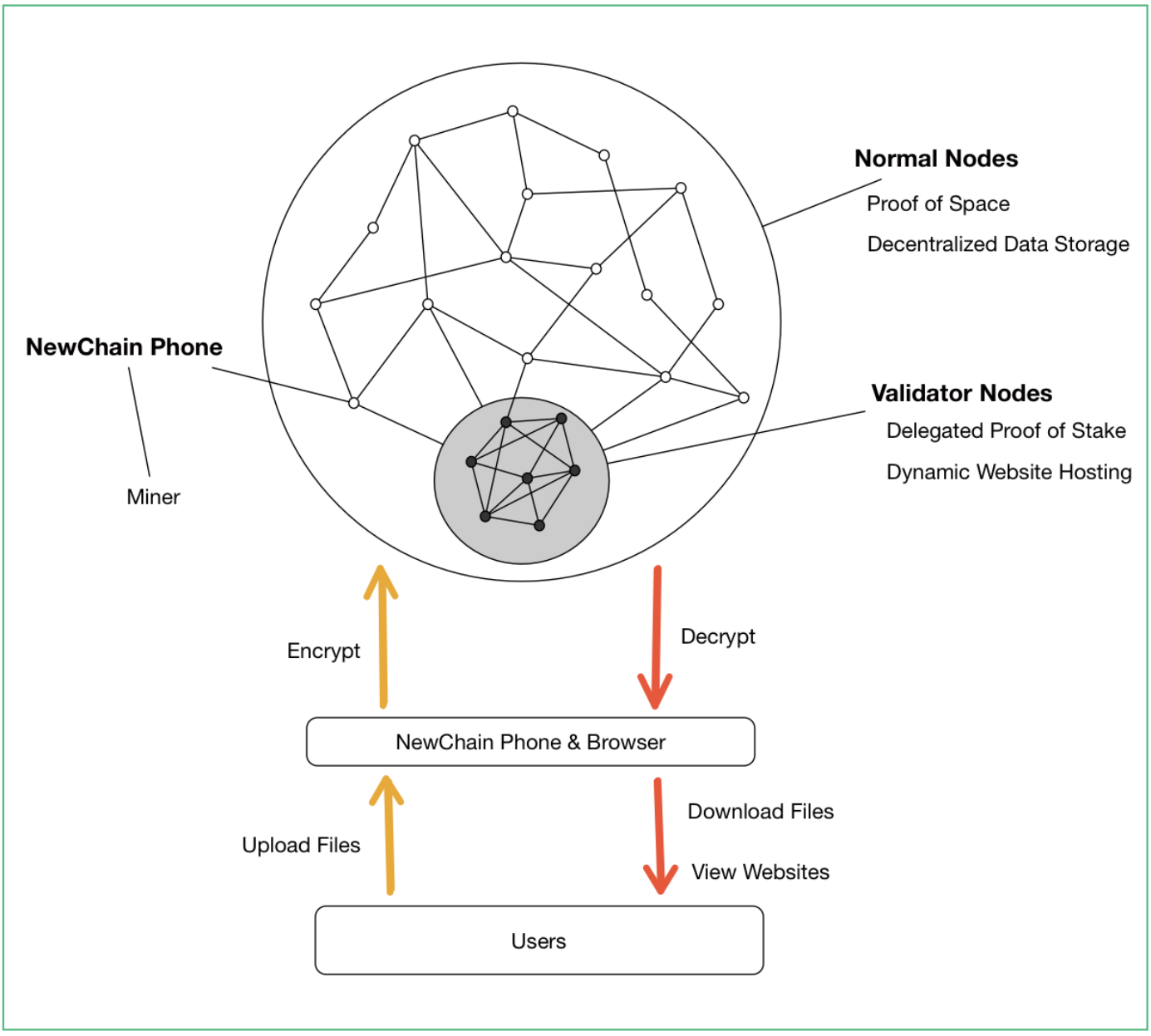
New OS极大增强了数字资产的安全性，支持的特性包括 加密钱包、安全访问、加密通信、可信显示、IP地址隐藏、MAC地址随机化及物理安全开关等，并采用了硬件隔离私钥管理方案确保数字资产安全。

同时 New OS 融合了区块链资产钱包、New Cloud云存储、智能挖矿等功能，搭载New OS的智能设备将成为一款会自动赚钱的手机。

4 .92 New OS 架构图



4 .93 去中心化数据存储&动态建站&手机挖矿



4 .94 硬件隔离私钥管理理(HD PKM)

硬件钱包的控制芯片被设计为只能写入，不能读取，种子及私钥被存储在芯片中。即使硬件钱包丢失，种子及私钥也不会泄露。硬件钱包提供存储种子/私钥，以及隔离签名的 功能;从最终结果看，硬件钱包替代了 PKM 的功能。

5. 代币介绍

5 .1 什么是区块链资产

区块链资产我们将存储并流通于区块链上的数字资产统称为区块链资产，借助区块链的独特特征，区块链资产具备众多传统资产所不具备的优势，因此很多人认为区块链资产很有可能引领新一轮互联网科技金融变革，NEW Cloud的诞生正是基于此。我们称NEW Cloud上主要流通的区块链资产为NEWC。

5.2 NEWC

NEWC是NEW Cloud上的一种权益凭证，也是一种与NEW Cloud 系统共生的特殊资产，同时也是NEW Cloud 协议的一部分。

NEW在网络里的主要用途为：

1.作为矿工激励，驱动矿工参与提供储存节点、挖矿，以实现区块链的正常运转，并保证安全。

2.用户动态建站，转账时，将消耗一定量的NEWC。

3.用户使用NEW Cloud 过程中，需要依靠NEWC作为流通媒介才能在区块链上流通，并消耗一定量的NEWC作为流通成本。

4.使用NEW Cloud 提供的其他服务时，将消耗一定量的NEWC。

5.3 分配方案

EW chain是基于NEW OS操作系统开发的智能硬件产出，根据硬件贡献值、运行时长、有效节点数等决定贡献值进行激励奖励。

NEWC代币总数约等于4.2个亿:

节点机制为百分百节点产出

单日总数:

节点有效运行数+运行时常*上行传输值（算力）

每年浮动产出比为:

初始节点数+新增算力产出除以2+激励值

第一年产出总数:

等于3600万+浮动产出值

算力奖励:

每台矿机算力奖励为推荐激活奖励，激活一台矿机增加被激活矿机每日产出值6%算力奖励

算法:

首年发布量：3600万+节点增加数+激励值

初始节点数为1万=（A），节点增加数以1万的倍数除以2=（B），,激励值=(C)

第一年总发币量=(A+B（B=A/2))=D+D*C=当年总产出币数

NEWChain算法列举：

如3万台节点贡献算力挖矿（首批硬件算力为100G无差异），那么预期每天总产量为：（3600万+1800万+900万)=6300万+(6000万*0.06)=6660万/365天=6.08（每个节点每天贡献值奖励）

8. 风险提示

您清楚地理解区块链和虚拟货币NEWC是超出对发行人的控制权， 平台和项目受以下风险的限制，您明确承认并承诺：

1.安全及价值

您承若虚拟货币NEWC或许并无价值，黑客或其他恶意组织或组织可能会尝试以各种方式干扰NEW Cloud平台，超出NEW Cloud团队的控制范围。

2.监管不明

NEW Cloud团队无法预测监管机构何时或是否应用现有法规或制定有关此类技术及其应用的新规定。 监管行为可能以不同方式对NEW Cloud平台或者NEWC产生负面影响。

3.使用局限性

NEW Cloud平台可能不会被大量的个人，公司和其他实体所使用，或者在分布式生态系统的创建中受到限制，这种缺乏使用或兴趣可能会对NEW Cloud平台的发展产负面影响。

4.团队

基金会和NEW Cloud团队有可能无法执行或执行此处列出的项目。

5.其他

除了本白皮书中已经描述的风险之外，NEW Cloud团队还有其他风险尚未提及或未预料到。

9. 免责声明

本白皮书仅用于提供一般信息为目的，不构成招股说明书，要约文件，证券要约，投资招标或任何产品出售，物品或资产（无论是数字资产还是其他形式的资产）的要约。本白皮书的信息可能不是详尽的，也不说明任何合同关系的要素。 本白皮书和基金会对于这些信息的准确性或完整性无法保证，也不保证或承诺提供这些信息的准确性或完整性。

本白皮书包含部分从第三方获得的信息，NEW Cloud团队尚未独立验证此类信息的准确性或完整性。对于这些信息的准确性或完整性无法保证，也不保证或承诺提供这些信息的准确性或完整性。

本白皮书不构成NEW Cloud团队出售任何NEWC（如本协议所定义）的任何要约，亦不构成其任何部分或其任何部分呈现的事实形成基于或依赖于与NEWC相关的任何合同或投资决定。 本白皮书中所包含的任何内容都不是或可能被视为对NEW Cloud未来表现的承诺，陈述或保证。

发布日期起，对于这些前瞻性陈述进行的任何修改的事件NEW Cloud团队明确表示不承担任何责任（无论明示或暗示）。

未经NEW Cloud团队书面同意，本白皮书的任何部分均不得以任何方式进行复制、转载、分发或传播。