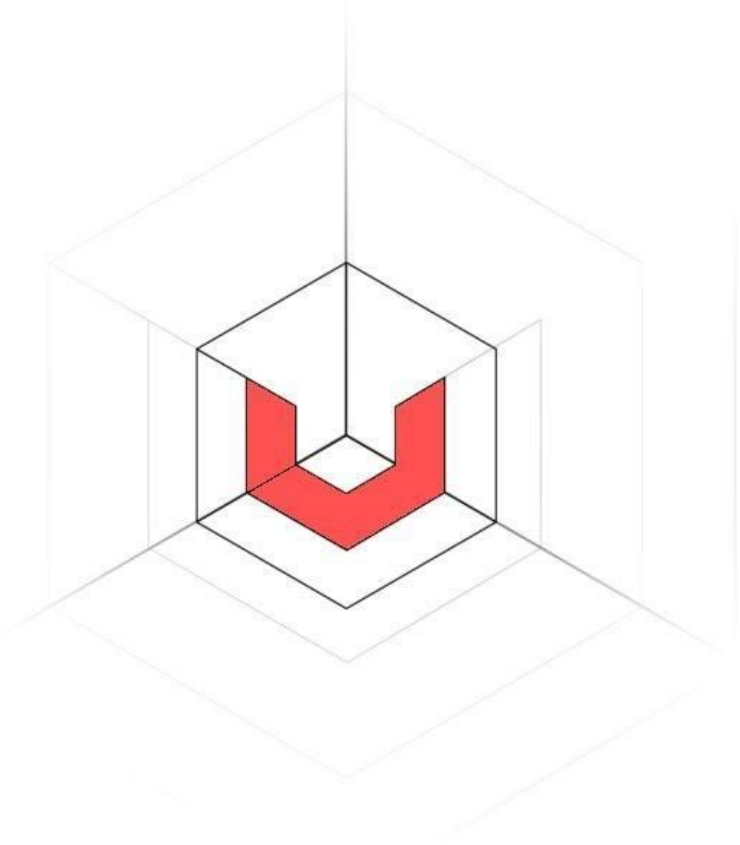
_universa.io

_区块链

_平台

_白皮书



_v1.0a

_准备_

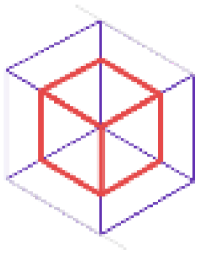
_universa_公司_ltd

_08_sep_2017

http://universa.io

_目录

_提要



摘要

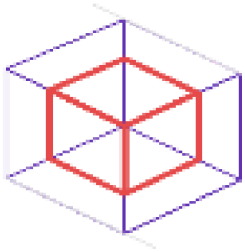
“未来已经到来,只不过还没有分布均匀。”

—威廉吉布森1993，赛博朋克科幻作家

在写作的时候，分布式分类账的数字资产价值累计超过了1400亿美元。根据Mozilla Foundation 在2017年第一季度的报告，现代的密码技术最终保护了有超过一半的http+ssl(1995年发明)形式的网络流量。 靠数学支持的非对称的加密是安全的、且可免费使用的，而且最终被绝大多数服务广泛采用，这项服务对当今地球上大多数人的日常生活产生了影响。

超过40年的计算机发展历史，证明了最早的技术采用者是个业余爱好者。可是他们引起消费者，然后企业，最后政府的注意。在这方面，比特币和以太坊这样的数字资产首先引起的是业余爱好者的注意，现在他们正渗透进消费者的钱包，而企业和政府的适应和采用都要慢得多。虽然一些勇敢的投资者已经用这种数字资产来存储他们的毕生挣的钱，但许多企业仍不愿将其作为支付手段，而大多数政府甚至都不承认数字资产的“货币”地位。

在这些方面,加密分类帐”区块链”技术仍然可以被认为是处于初级阶段, 现代著名的中本聪的2009年白皮书仅描述了假设用例的第一次迭代，将钱数字化为无信任和分散化的协议。第二次主要迭代产生了以太坊概念,一个平台和虚拟机不仅仅是一个货币,因为它支持复杂的智能合约逻辑和去中心化应用程序的新领域或“dApps”。在需要一定程度的监管和责任的企业用例中，这两种方法都不完全适用。

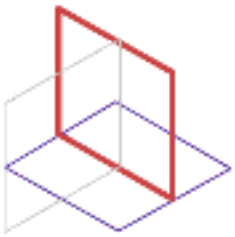


概述

Universa平台是新一代的区块链技术。这个项目使用合约 执行机器和去中心化状态分类账，重点在于令牌化和合约协议，通过改进必要条件来改善比特币和以太坊技术。传统区块链主要在于货币交易,而Universa的支持令牌可表示护照、登机牌、公交票或出租车费; 它们可以当成礼品卡、优惠券或健身房会员卡。您可以做一个表示产权的令牌，或者仅仅是房子的钥匙。

传统区块链在完全不可靠的分类帐上记录所有交易和它们对网络的影响(“大协议，小逻辑”), Universa通过维护所有行为的输出(“小协议，大逻辑”)的可验证的图表，提高了速度和加强了可用性。换句话说，代替区块成为一个完整的分类帐，客户的每一组变更从以前的阶段在一个单独的合约链(“c-链”)上被申请。结果是矢量化的和散列的,只有签名的每侧链的状态去更新的新的区块链,才会丢弃旧的状态用来存储新的。不过每个链都保留自己的历史记录，任何带有交易副本的节点都可以尝试重放它们，并验证结果是否相同，从而确保可信环境中的有效性和公平性。

与传统商业区块链技术不同,Universa并不依赖于不受信任的公众作用物。Universa系统节点由我们的合作伙伴拥有和运营，他们必须由Universa公司授权。他们是受信任的，经过培训的，经过审计的，他们提供了可用性、快速性和安全性的保证。这和为了收入，每小时都不必要地消耗掉全球的千兆瓦电力浪费的挖矿不同, Universa所有的节点都通过交易费用来获得，他们还参与了合约的验证和执行。Universa云计算机器上唯一的“工作”是关键任务数据处理和合约执行。这并不需要昂贵的GPU硬件。敏感的业务数据不知不觉快速的存储、它严格接受的认证组织(ISO 27001、27001)安全地加密与监管。这个技术使得商业中可以相信较为敏感的或私人业务流程的区块链。



Universa是什么

Universa平台通过Universa的网络运转。Universa网络是使用节点并且Universa支持安全签署文档和支持的服务(代号为“公证云”)的Universa Core客户。它们在一起组合成了Universa区块链。区块链只是负责执行交易状态的有效性,而公证云作为一个可核查仓库签名的合约正本。

例如,如果合约规定了“令牌”的资产和对10000方中的每个方分配一个令牌,则只会将最终余额的哈希状态存储并保存到完整的块 (约90字节), 而不是像比特币或以太坊这样的情况，全部计算所有的万笔交易和所有用户账户的余额。因此，连接到网络的任何未来节点都将从与块链同步该特定执行的超过99.99%的大小中获益，并且仅需要在该块高度保留当前状态的短散列以验证它。此外，由于每个合同的哈希值通过有向非循环图（DAG）被归纳到主Universa链，而不是一个简单的同步排序的块链，可能来自不同合同和重播的异步操作发生无序，仍然产生与全局状态相同的最终散列。

网络以这种方式设计，围绕合同及其执行 - “交易” - 每次执行动作时，所有节点都将传送合同的当前状态和要执行的操作的来源。

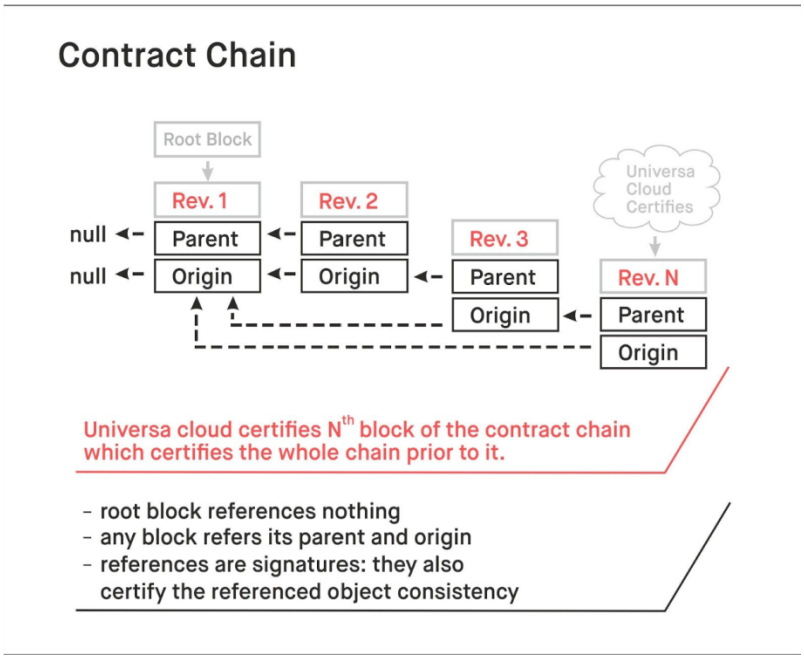
状态和来源被相同合约的存储，当前状态侧链(“C-Chains”)的散列函数验证, 操作应用，然后这个新状态被散列和共识达成90%。在短时间内(目前10天)的节点放弃合约和状态。它们的哈希函数和签名在公证云存储,所以原来的合约可以提供节点以及证明真实。只有散列需要在群落节点保留。通过这种方式，交易速度得到极大改善和区块链的大小减少到为验证完整历史分类帐检查仅仅需要的信息。验证一个特定的

C-Chain，如在三元分类帐中对货币类合约余额的有效性进行核算，任何行为人均可保留合同来源和交易历史（如有必要，请求公证云进行验证）并重复行为将哈希值与分类帐中当前状态下的当前值进行比较。

实现

区块链

Universa的区块链是一个靠授权和信任的节点，每秒可以处理上千万的交易状态改变的合作分类帐。通过客户的执行合约与被每个新区块90%一致算法的创建过程验证输出进行。区块链不需要存储所有交易的历史,这些东西可以通过每个作用物在侧链中负责执行。在区块链或别的平台通常存储的交易记录、数字签名等东西稍后可以在公证云服务核实真实性。公证云负责处理资产和数字签名,但又从区块链中独立(这增加了交易速度和同步时间)。

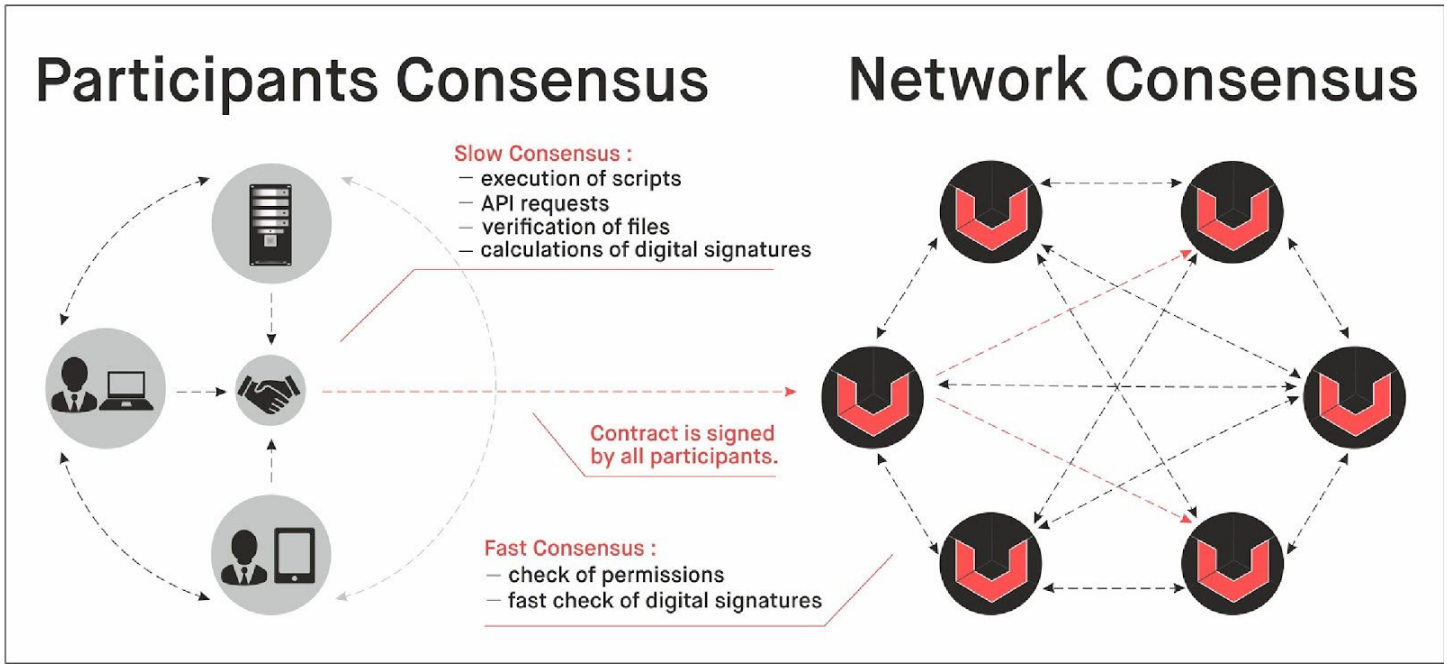


持有量证明

Universa节点主要的功能是完成合约并验证其状态。在宇宙中，不是依赖古老的技术来刻录时钟周期，在Universa中，创建新区块的许可来自于作为一个许可节点的参与。因此与其等待一个新区块被挖矿创造不同，不如在随意时间可以发生状态变化，由可信的参与者验证，并且在不到10毫秒的时间内，也常常得到一致的认可。每个独立的合约维护自己的状态链,所以合约可以没有阻碍或影响其他合约异步执行操作。结合状态共同的变化形成一个定向非周期性图表(DAG),这就是区块链。

作用物

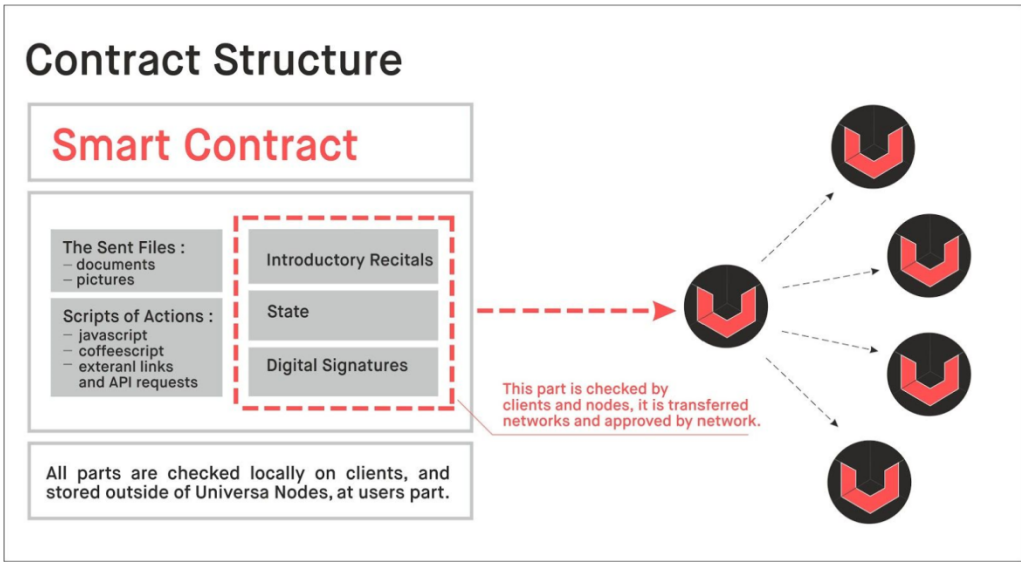
1. 共同产生了通用的公证云和通用C-链分类账的节点.
2. PC, Mac, Android and iOS 的客户
3. 通过Universa服务提供额外的服务，比Universa加密云。



智能合约

一般来说，Universa智能合约是存储在树结构中的可执行脚本数据。它存储“键值”格式的任何信息;每个键都表示为一个全局惟一的地址，一个值可以是固定值、二进制可执行逻辑、动态执行脚本，甚至是对其他树、地址的引用等，允许任何复杂嵌套表示的结构。

在Universa智能合同中的脚本是图灵机完成的;简单地说，这意味着脚本可以执行其他脚本，包含可编程逻辑的显著复杂性。在某些情况下，以执行某些操作和管理表示为适当逻辑有可能很复杂。比如，您可以把共享与外部数据(美元汇率或在特定情况下出售一套股票指数)关联起来。虽然在合约规范中几乎不包含这种类型的所有可能的条款，但这很容易通过在合约中存储的可执行脚本实现。该脚本是一个签名的、不可更改的部分。为了检查复杂的条件、启用某些触发器并根据需要进一步执行相应的操作，它可以执行任何复杂、智能逻辑。



因此，从整体上看，一个智能合约树创造了一个智能合约链。它代表引用与确认彼此的智能合约组。C-链表示一组实际的相关文档。每个新C-链的特点是由它第一份全新的智能合约规定的。但是再次强调,区块链不存储合约本身,只是保持现状。合约主体是存储在其他实体,例如您闪卡或加密云。这也意味着通过Amazon服务器或内部硬件，您可以促进智能合约会计的基础设施。由于合约执行被您签署与接受节点交易状态的验证,其结果可以被所有Universa平台的作用物证明。

附加文件

智能合约可以包括对现实对象的所有产权，比如以附件形式包括的知识产权(IP)或对购买财产合约(通常是另一份智能合约)。

任何文件都可以添加进合约内部或可以作为防止更改文件签名认证的链接更改文件。

Universa客户端在智能合约执行时检查链接的对应。智能合约和公证云将证明合约并为其提供时间戳。合约的最大尺寸为1gb。

时间戳

Universa智能合约的一个更重要的特征是时间戳。用户客户端给Universa节点发送合约的状态，最后的客户检查和验证状态存储发生的时间。由于公证云在一秒钟内执行，可以理解为合约被Universa验证或拒绝的确切时，支持了Universa 智能合约的合法使用。

标记

有时您需要证明一份智能合约的旧状态的能力。在这个情况下您需要在引用定时间点合约的状态创建一个“标记”。这是一份特殊的小型智能合约，它能证明存储一份需要两年的旧合约。

节点

每个Universa节点都是一个存储了Universa网络结构的相同主机。每个节点都是受信任的，因为它属于已知的负责任所有者，并且是承担了运行公证服务的责任的法律实体。节点运行在常规的Unix服务器上，并包含了一个动态副本。当客户端向Universa发送一个智能合约时，合约首先被传播到已知节点的Universa客户端检查。如果智能合月仅由几个部分签名组成，那么Universa节点将其状态存储10天。

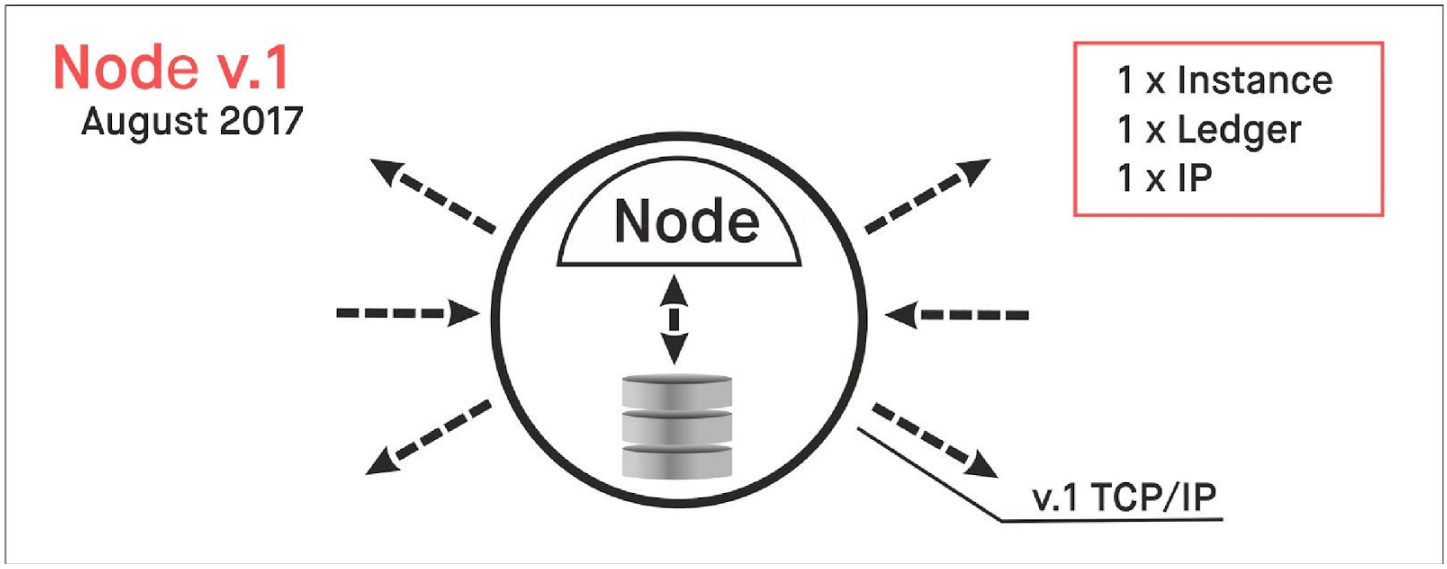
如果该节点拒绝了智能合约的注册，为了防止欺诈，则合约保留30天的状态。

客户端

- 随着时间的推移，Universa将提供参考设计和MVPs:
- 在桌面环境和安卓平台操作的开源Java数据库
- 为了Windows,MacOS，Linux的客户机应用程序，这是Universa基本的功能设置
- 安卓移动应用程序
- 一个图形用户界面(GUI)合约构造器，包含合约模板和典型动作。该GUI将提供在没有特殊技术技能的情况下创建智能合约的能力

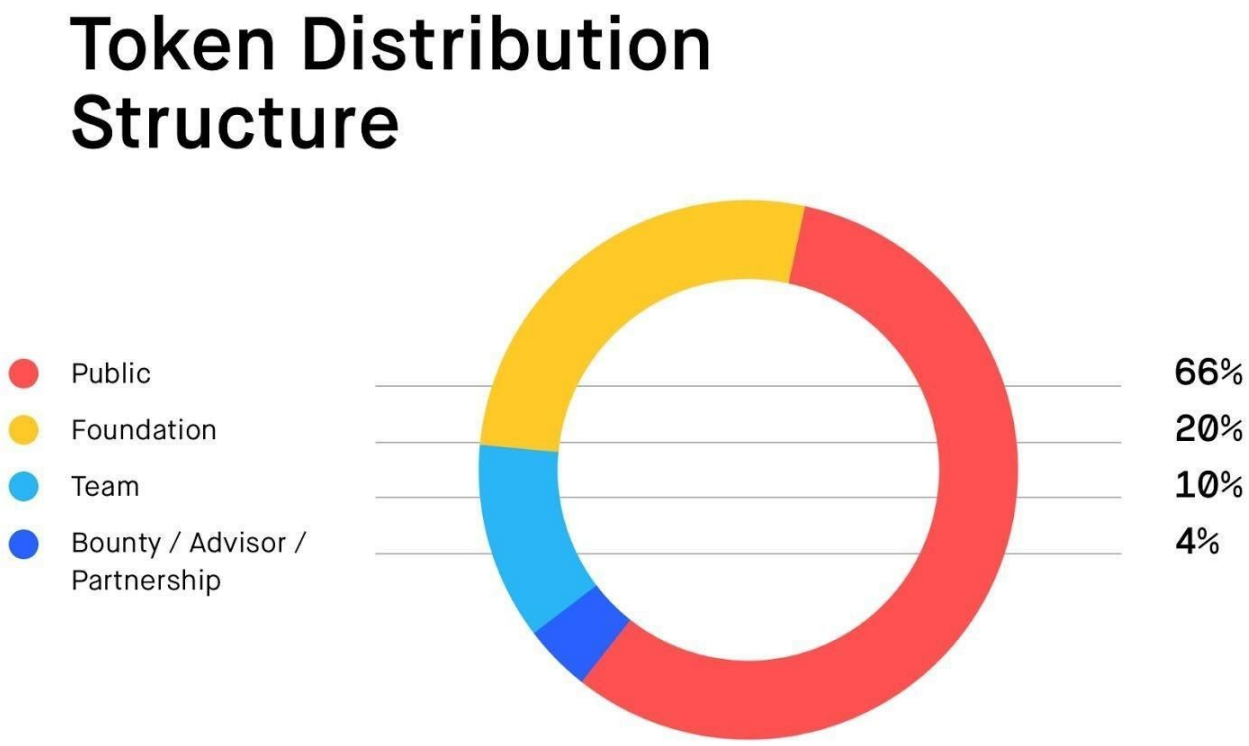
每种类型前端都连接上已知的节点，这些节点发送给

其他活动节点列表和法定人数的大小。Universa客户总是检查申请人的文件是否适合该合约，例如如果您通过电子邮件接收到文件和合约，GUI或Universa客户端将检查该智能合约的签名是否与您所收到的文件的准确版本相对应。



_令牌_经济

Universa的生态系统是由“UTN”令牌所形成的，这是一种数字资产，它本身就代表着Universa 智能合约。每个UTN都能被18个十进制数整除，允许进行交易。为了方便和日常使用，UTN令牌部分的别名如下——



Unit名称	UTN 价格	贸易比率	TGE USD 价格
kUTN	1000	1 : 1,000	$10
UTN	1	1 : 1	$0.01
mUTN	0.001	1,000 : 1	0.001 US cents
uUTN	0.0000001	1,000,000: 1	0.000001 US cents

nUTN	0.0000000001	1,000,000,000: 1	0.000000001 US cents

预售和令牌事件

令牌在两个阶段开始分发，下面是日程安排。在TGE期间以太坊“ERC20”令牌生成一个占位符和分发给参与者,所以在Universa区块链启动以前，令牌占位符可以在公开执行交易。参与者可以选择立即要去中心化，以太坊钱包声称他们的占位符令牌或等到Universa平台启动。令牌在Universa平台主区块链基础上声明与分布。没有声称ERC20 “UTN-P‘占位符令牌TGE和预售的参与者中直接他们“UTN-p”令牌。这些令牌将被分配到一个“占位符偿还”账户中，而持有者将能够兑换他们以换取UTN。

	9月2017年 - 预售	10月 2017 年- 令牌现代时间
类型	公开发行	公开发行
了解客户的“KYC”	要求	要求
令牌出售	10,000,000	到99百万USD
提高量	$3-10 百万 USD	-
每UTN令牌价格	$0.01 + 20% 奖金	$ 0.01$(最小购买$10 ）

循环和需求

为了奖励参与者把网络提供的处理能力的节点，并维持正在进行的开发，Universa平台智能合约行为的执行需要UTN支付的交易费用。节点将保留80%的交易费用，20%将归到Universa公司。每天Universa保留的1%的费用将永久地销毁，或者“燃烧”，将其从循环中移除，并经常对货币产生通货紧缩的影响。

Universa的“代币”事件是从公开的众筹中获得资金支持。

Universa的代币活动旨在从一个开放的众多合作伙伴那里获得资金支持，这些人希望支持我们的未来发展。我们的计划是动态的，能够适应各种各样的情况。我们为一次筹款活动做好准备。只用预售中筹集的资金，我们继续推进我们的计划。然而乐观地说，我们的最终目标和愿景是先进的，我们已经准备好了一个计划，将公司规模扩大到9900万美元或更高。我们的ICO是无上限的，因为我们的目标是在全球范围内建立的许多法律和政治框架，并建立Universa的基础。完整的预算和支出计划，包括发展目标、法律结构和研究目标，都可以在http://bit.ly/2jSOSIql网址上浏览

	当前	$5m	$10m	$25m	$50m	$75m	$99m+
员工人数	17	17	25	30	35	40	45
发展	$2,167,500	$2,167,500	$3,187,500	$3,825,000	$4,462,500	$5,100,000	$5,737,500
研究	$0	$0	$400,000	$900,000	$2,000,000	$5,000,000	$7,000,000
营销	$0	$400,000	$800,000	$1,200,000	$2,000,000	$5,000,000	$7,500,000
法律	$250,000	$400,000	$400,000	$800,000	$800,000	$2,000,000	$2,000,000
商业发展	$0	$250,000	$600,000	$1,200,000	$2,400,000	$3,000,000	$4,000,000
教育	$0	$200,000	$400,000	$1,000,000	$1,500,000	$2,500,000	$3,000,000
年度预算	$2,417,500	$3,417,500	$5,787,500	$8,925,000	$13,162,500	$22,600,000	$29,237,500

_发展_能力

附加服务

服务提供者可以使用Universa活动合约的服务器注册。从“Universa”的角度来看有没什么特别,节点像区块链参与者一样,但为了交互扩展的功能网络和提供高级功能，他们可以提供自己的规定。
例如一个合约云可以包含允许执行操作，调用外部服务，产生结果一组的API。共享服务合同有一个通过指定GET或向给定URL POST HTTP请求执行所有者“投票”操作的端点。这个端点还可以作为发出的电子货币的电子银行服务。

_用例中

在启动时或者之后不久，Universa提供参考实现的几种常见Universa智能合约平台用例。这些参考实现是开放源代码的和可适应的，允许任何人直接复制或者对未来开发使用。将提供“令牌”、“发票”、“Escrows”和“组织”的引用。

合约令牌

普遍

令牌 最基本使用合约的例子是通用令牌而生成的资产。这些资产可以被分割、交易、替代。为了检查一个钱包的平衡与把令牌转移到另一个钱包，该合约按规定行动。这样对驱动其他平台和交易所，Universa平台可以举办各种各样的可交易资产活动。更高级的令牌合约可能包含了出售新令牌的功能，解决现有的供应，冻结或锁定一个帐户或所有帐户的交易活动，被中介方的颁发费用的授权。

银行的支持令牌

Bank-Backed令牌 由于智能合约完全是图灵完成的，还可以与外部API互相作用，有可能规定共享令牌合约。这种合约中包括处理内外资产类(包括但不限于比特币、以太坊，甚至是法定货币)转移的附加规定。例如一个合约可以规定名为“usd - tether”的令牌和支持一个美国银行帐户的互相作用，还可以定义“sellTokensToFiat”函数，该函数接受使用usd - tether令牌作为输入，并将SWIFT地址作为输入，并将一个传出的连接到相应的银行帐户上。在收到交易时，可以定义一个相应的“buyTokensWithFiat”动作，即铸造出新的usd - tether令牌。这样一个合约可能同样用其他数字资产还Universa资产, 同时通过Universa平台允许与外部资金完全互操作性的方法。

发票合约

例如您任何一家线下服务公司的老板。交付后您立即想要得到服务付款与小额交易费用。您创建了包含附录和条件所有文档相关的智能合约。在这个合约指出规客户应该用USD-TETHER令牌发送给您费用。能够给经理账户或者您应收账款部门直接转发，合约被定义。当您的员工提供交付时，他们请客户提供给终端上的数字签名，然后交易被立即执行。交易可以离线进行，然后在网络上注册。如果有必要，为了谈判你们合约签署以前可以发送本体给彼此,但是如果一方用官方数字签名签署合约，它将变成一个不可更改的文档。另一方将只能够选择签署合约或不签署合约。

托管合约

数字交易所或“股票市场”

类似于银行支持令牌可以利用外部API来允许其他的交易数字资产或法定资产，为了双方都公布了他们的付款时实行释放一笔交易，智能合约提供两把交易托管锁。通过这种方式，对在其他类型的证券交易中用UTN，fiat或其他数字资产支付交易，可以使数字资产更便利，甚至可以与股票经纪人服务整合。

卖公寓

首先，卖方应该准备包括确认同财产公文的智能合约。这可以包括财产图像的文件。这些文件是在他的法律数字签名上签署的，在一些国家也有公证。这应该允许更改所有者以交换一个已定义银行令牌。在本例中为超过定义的USD系绳令牌的250000。

现在双方可以协商和修改合约。双方签约后他们互相发送到Universa的任何节点。Universa检查所有签名还确保25万个USD-令牌的足够存在。如果合同通过了所执行的90%的节点的验证，买方就获得了该公寓的所有权，而卖方则成为银行票据令牌的所有者。现在买家可以与当地政府或注册部门联系，向他们的新公寓所有者发送文件。

数字自治组织“DAO”合约

您是一家公司的首席执行官，正在组织新的首席财务官投票。首先，你要创造有新首席财务官的提议的智能合约。在合约中，按照标准法律文件的所有常见的细节，描述新首席财务官权利和义务。在此之后您按下“开始投票”的按钮。接下来您可以通过任何渠道，不论是用闪存卡还是您的腿，把合约发送给同事。参与者发动合约，使用数字签名和投票表决，证明他们的身份和权利。每一次投票都创造了包括一个人投票另一个新独立智能合约，就像之前在主要智能合约中所定义的那样。之后这些人发送给您“投票”的合约。之后您收到足够这种合约，您参加一个新的首席财务官可以更新主要企业职能。智能合约是数字工作流基础设施的元素,因为它包含文件作为附件,它在同一时间代表了一个完整法律文件。这种智能合约允许新首席财务官支付账单，支付工资，适用于法庭和政府的税务服务等。

_结论

Universa平台迭代密码分类技术基于八年的经验，证明比特币分配和调整成功，解决基本业务问题和政府遵从性所需的工具相适应。由于事务吞吐量提高了几个数量级，内置的支持验证文档的真实性以及一个可信的节点网络，为了开辟企业采用的新途径，Universa能够提供必要的可用性。随着消费者越来越多地需求，比特币和以太坊技术快速的进步, 为了服务可靠性和安全企业的要求，Universa将继续倾向于区块链采用和去中心化创新技术的利用。