universablockchain.com

Universa 区块链平台

版本1.0h
为universa公司编制
2017年9月8日

白皮书

目录

简介

摘要

> “未来已经存在，只是没有被非常均衡地分配。”
>
> William Gibson 1993年，赛博朋克科学小说作者

在编写本文件时，分布式加密分类账返回数字货币数值的累计价值已经超过1400亿美元。根据Mozilla基金会出具的2017年第一季度报告，现代密码学最终，已经通过HTP+SSL （于1995年发明）保护一半以上的网站流量。经证实，数学支持的非对称加密是安全、可自由使用、持久、并且被广泛应用于绝大多数数字化服务，影响和授权地球上大多数人的日常生活。

超过40年的计算机发展历史表明，最早采用该技术的人往往是业余爱好者，其后依次是消费者、企业和政府。在这点上，和数字资产，例如比特币和以太坊，迅速让业余爱好者们惊心动魄一样，其正在渗透消费者钱包。而相似地，企业和政府就很难适应和采纳。虽然一些勇敢的投机者已经把毕生积蓄押在这些货币上，许多企业仍然不会将其用作支付方式，而大多数政府甚至不承认它们是“金钱”。

在这一点上，仍然可以在初始阶段，考虑加密分类账“区块链”技术；当前，在由采用假名中本聪（Satoshi Nakamoto）的人员编写的著名的2009年白皮书中，仅仅描述了假设用例的第一次迭代和金钱数字化为无信任的去中心化协议。对于这一新概念，在第二次主要迭代过程中，产生了以太坊，一种涉及多种货币、支持复杂智能合约逻辑和分布式应用的新边界的平台和虚拟机，或者“去中心化应用程序”。但是，目前均不完全适用于企业用例，还需要一定程度的监管和问责机制。

因此，这两种应用程序仅仅是人类交流和合作的新时代的开端。区块链已经开始破坏货币传输和软件逻辑的执行。但是，目前几乎完全没有探索其改变商业逻辑和政府过程的方式。它是一个完全开放、等待创新和开拓新系统的领域，将成为世界商业、企业以及政府，在未来岁月里，几十年甚至更远时间内，塑造社会和人类文化的基础。它是一个领域开放的、成熟的创新和新系统的开拓，它将形成商业、商业和治理在全球范围内形成的基础，塑造社会。而人类文化在未来的岁月里，几十年又远，远不止。未来确实在这里。未来确实已经存在。

概述

Universa平台是新一代区块链技术。其采用合约执行机和设计，用于改善比特币和以太坊技术的分布式状态分类账，提供企业采用所需的改进措施，重点强调标记化和合约协议。在主要采用货币进行交易的传统区块链区域，Universa被设计用于支持从护照到登机牌、公共汽车票或者出租车费在内的所有代币表示；它们可以是礼券、抵用券或者健身会员卡。你可以做一个代表你所有权证书或者仅仅是房屋钥匙的代币。

虽然传统区块链记录了所有行动、交易及其对网络影响的完全不可信的分类账（“fat协议，tiny逻辑”），Universa改善了其速度和可用性，保证提供所证实的所有行动输出的散列的有向图（“tiny协议，fat逻辑”）。换言之，不再采用数据库堆积，构成单一的完整分类账，客户在各合约（“C-链”）中对先前状态进行系列变化，并且将结果矢量化和散列-只将各边链状态的签名更新为区块链的新状态，丢弃旧状态并存储新状态。尽管如此，仍然保持各链自己的历史，并且可以尝试重新进行各交易副本节点，并且证实结果相同，从而确保可信环境中的有效性和公平性。

在传统区块链技术演生的关键业务中，Universa不依赖于不受公众信赖的参与者。我们的合作伙伴拥有和操作Universa系统节点；必须获得Universa公司的批准和授权。其必须是可信的、经过培训的以及经过审计的；并且，保证其可用性、速度以及安全。除激励性矿挖（一种每小时不必要地消耗全球千兆瓦发电量，并且没有产量的浪费性活动）之外，通过交易费用就其参与合同确认和执行，而奖励所有节点。Universa云机器的唯一“工作”就是处理关键任务数据和执行合同，并且不需要昂贵的GPU硬件。在全球未知领域内，不会轻率无意识地存储敏感商业数据，需要通过最佳实践组织安全实践（ISO27001，27002）进行数据加密和管理，从而使得企业最终可以信任敏感或者私人业务过程的区块链。

用途

Universa平台受Universa网络支持–包括Universa区块链且支持Universa安全签名文档服务的大量Universa核心节点（代号为“公证云”）。区块链仅需要确保交易状态的有效性，而公证云充当原始合约签名的可验证仓库。

例如，如果执行合约，定义“代币”资产且向10000方中的各方分配1代币，那么仅需要在全部区块链（大约90字节）中存储和保存最终余额的状态散列，而不是完全记录全部10000项交易和所有用户账户余额，比特币或者以太坊就是这种情况；因此，在该区块链详细执行信息同步过程中，连接到网络的未来节点均会受益于超过99.99%的尺寸缩减。并且，仅需要在该区块高度处保持当前状态的简短散列，以便用于验证。此外，由于需要通过无回路有向图（DAG），而不是单纯的同步有序区块链，将各合约散列汇总为Universa主链，可能进行不同合约的异步行动，重新实现无序，并将仍然产生相同的最终全局散列状态。

网络设计方式如下，合约和其执行–“一项交易”–并且每次仅执行一项行动，通过当前合约状态和要执行的操作源来传输全部节点。通过散列和验证状态和源，并且与合约侧链（“C链”）的当前存储状态一样，采用该操作。然后，由90%一致性散列和约定新状态；短期（目前为10天）之后，节点可以自由丢弃合约和状态–随后在公证云中存储器散列和签名。可以向节点提供原始合约并且证实其真正性–仅需要在各节点大量留存散列。如此，可以大幅度提高交易速度，减小区块链尺寸，从而使其信息刚好足够验证完整的历史分类账。为了验证特定的C链，例如货币类似合约余额有效性的三倍分类账记录，参与者可以保留合约来源和交易历史（在要求时，如果需要，需要由公证云验证），重新进行交易，并且在分类账的当前状态中，将散列与当前价值进行对比。

实施

区块链

Universa区块链是由各许可和信任节点执行的状态变化的合作分类账，每秒能够处理数以千计或者数以万计的交易（±20,000TPS，access.mainnetwork.io/benchmarks）。其可以在客户端执行合约并且在创建各新区块时采用90%一致性算法验证其输出内容，从而达到前述状态。不需要在区块链存储全部交易的完整历史，因为由负责该事物的各参与者负责在侧链中予以存储。对于通常需要在另一平台区块链上存储的任何事项，例如交易记录、合约来源以及数字签名，可以随后通过相关公证云服务验证其真实性。其中，相关公证云服务负责处理资产和其数字签名，但是与区块链分开且有区别（提高交易速度和同步时间）。

状态证明

Universa节点的主要功能是执行合约和验证状态。不依赖于无故消耗时钟周期的古老矿挖技术，在Universa中，允许创建新区块，作为批准节点参与其中。因此，不再等待待矿挖的新区块，随时可能发生状态变化，由可信任的参与者予以验证，并且经常在小于十毫秒规模的情况下予以一致批准。各单独合约均保持其各自的状态链，因此合约可以在不阻塞或者影响其他合约的情况下，异步地执行各行动，并且各组合状态变化共同构成无回路有向图（“DAG”），从而构成区块链本身。

合约链

Universa云证明合约的第N个区块，并且在此之前证明全部链。

— 根区块无引用依据。
— 任何区块均由父区块和起始区块。
— 引用是签名：它们也证明了引用对象的一致性。

参与者

01

节点，共同产生Universa 公证云和Universa C链分类账。

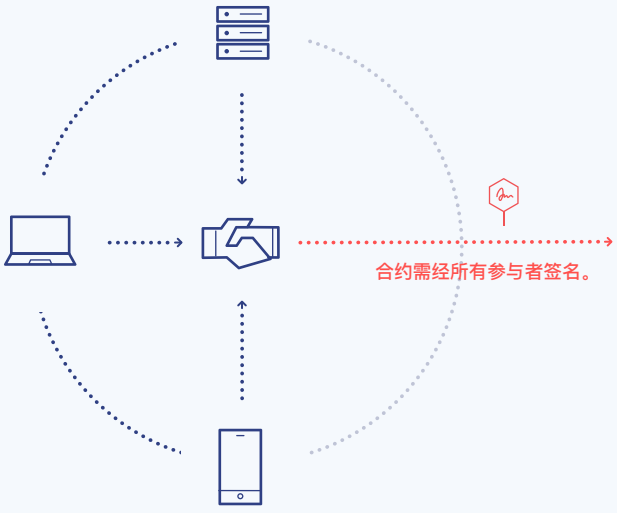
02

客户–对于PC、Mac、Android以及iOS来说。

03

附加服务，类似Universa 隐云，和侧实体，可以通过Universa提供服务。

参与者共识



缓慢达成共识：

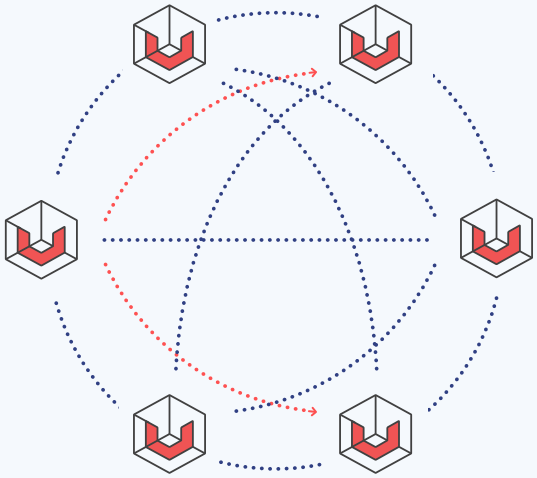
— 执行脚本

— 请求API

— 验证文件

— 计算数字签名

网络共识



快速达成共识：

— 检查许可

— 快速检查数字签名

智能合约

通常，Universa智能合约仅仅是指树状结构中存储的可执行脚本数据。其信息存储格式为“键–值”；各键均拥有全球唯一的地址，数值可以是固定数值、二进制可执行逻辑、动态执行脚本，或者甚至为对其他树形或者地址的引用等等，同时几乎允许任何复杂嵌套表示结构。

Universa智能合约脚本为图灵完备的；简单来说，就是指脚本可以执行其他脚本，并且包括显著复杂性的可编程逻辑。在某些情况下，履行特定行动和/或管理的恰当逻辑可能过于复杂，从而不能被表述为一套配置属性。例如，可能想要将股票与外部数据联系起来，例如美元汇率或者一套股票指数，允许仅在某些情况下出售股票。虽然，几乎不可能在合约规范中包括所有这类可能情节规定，可以在合约中存储的可执行脚本轻松达到这一目的。签名脚本在合约中不可更改，并且可以执行任何复杂的智能逻辑，检查复杂条件，启动特定触发器以及根据需要执行进一步相关行动。

合约结构

因此，总体来说，智能合约树可以创建智能合约。其代表一组智能合约，并且可以互相引用和确认。C链代表现实世界中的一组相关文件。各新型C链的特征是基于其第一个全新智能合约确定。但是，再一次，区块链不能存储合约本身，而仅仅存储其当前状态。而且，合约本身是由其他实体存储。例如，闪卡或者隐云。这也意味着，可以通过亚马逊服务器或者室内硬件通过任何基础设施促进智能合约会计。并且，由于仍然需要签字执行和接受交易状态的节点予以验证，Universa平台的所有参与者仍然可以信任该结果。

附加文件

智能合约可以包括真实世界中对象的所有权，例如作为附件的知识产权（IP）项目，或者某些财产的购买合约（通常为另一个智能合约）。

可以在合约自身内部添加任何文件，或者将其用作大型文件的签名验证链接（防止更改文件）。在执行职能合约时，Universa客户检查链接的对应内容。在公证云之后，验证合约并且提供时间戳。

合约最大容量为1GB。

时间戳

Universa职能合约的另一个重要特征是时间戳。当从客户端向Universa节点发送合约状态时，最后一个需要检查和证明其存储状态和发生时间。由于公证云可以在一秒以内予以执行，当Universa验证或者拒绝合约，并且支持合法使用Universa智能合约时，可以知道准确的验证或者拒绝时间。

标记

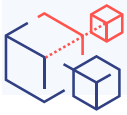
有时，需要有能力证明智能合约的过去状态；如果你需要参考某一特定时间点的合约状态，可以创建“标记”。这是特殊的小范围智能合约，可以证明和存储所需合约的过去状态，持续2年时间。

节点

各Universa节点是存储Universa网络结果的对等主机。各节点均可信，因为其均由负责运行公证服务的著名的合格所有人、法律实体所拥有。其在常规Unix服务器上运行，并且包括分类账的动态副本。当客户向Universa发送智能合约时，沿已知节点传送的Universa客户端首先进行检查。如果仅少数方在智能合约上签字，Universa节点仅将其状态存储10天。如果节点拒绝登记该智能合约，其状态将被保持30天，防止欺诈。

客户

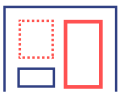
Universa适时提供参考设计和MVPs：



开放源码Java库，将在桌面和Android平台中起作用。

Windows、MacOS以及Linux客户应用端，作为基本Universa特征集的命令行。

Android移动应用程序。

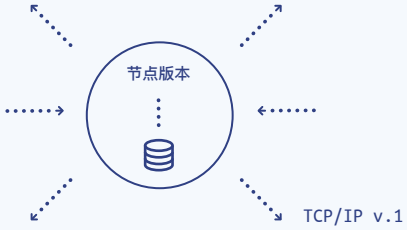


图形用户界面（GUI）合约构造器，其中包含合约模板和典型操作。图形用户界面可以用于创建智能合约，并且无需特殊技能。

各类前端客户需要与最后一个已知节点相连，并且这些节点需要发生其自己的其他活动节点清单和容量。如果申请人文件适用于合约，Universa客户需要始终予以检查；例如，如果通过电子邮件接收文件和合约，图形用户界面或者Universa客户需要检查确认，该智能合约的签名是否与所接收文件的确切版本相符。

节点版本1

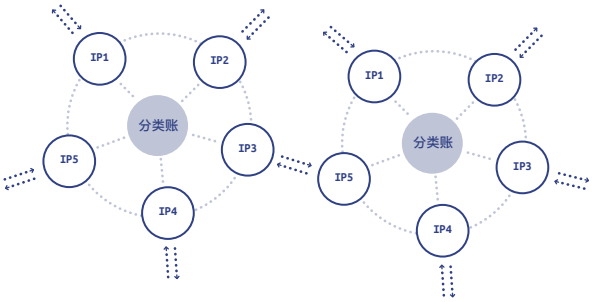
2017年8月



1 x 实例
1 x 分类账
1 x IP

v.2节点

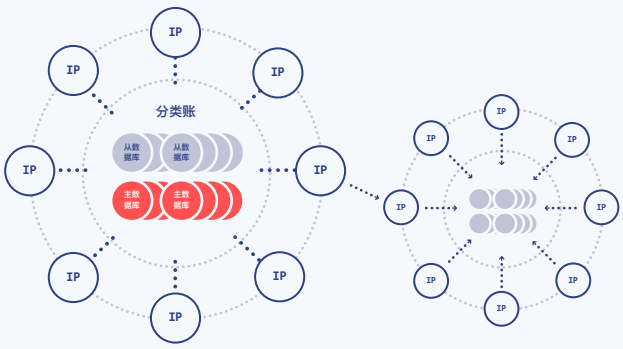
2018年，或者当日流量达到1000万笔交易时。



3+ x实例
1 x 分类账
3 x IP

v.3节点

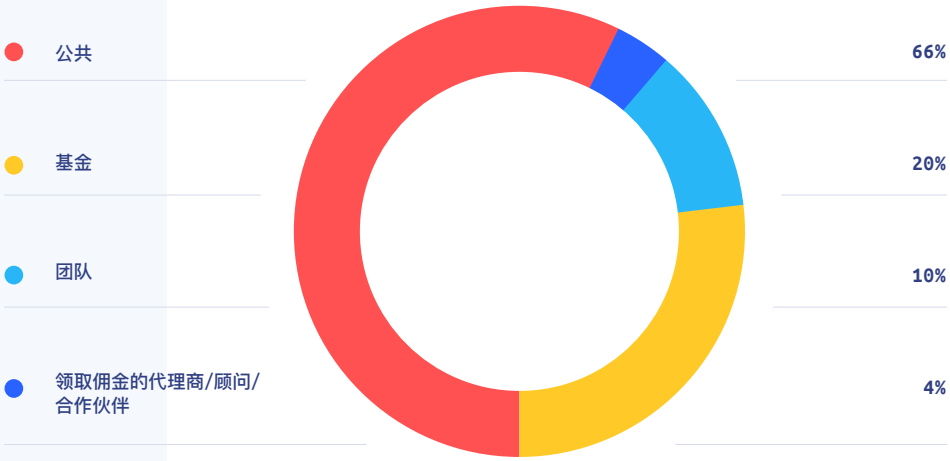
2018年后半年或者当日流量大于1000万笔交易时。



50+ x实例
1+ 主分类账
1+ 从分类账
>60 IPs
v.2 UDP

代币法

代币分销结构



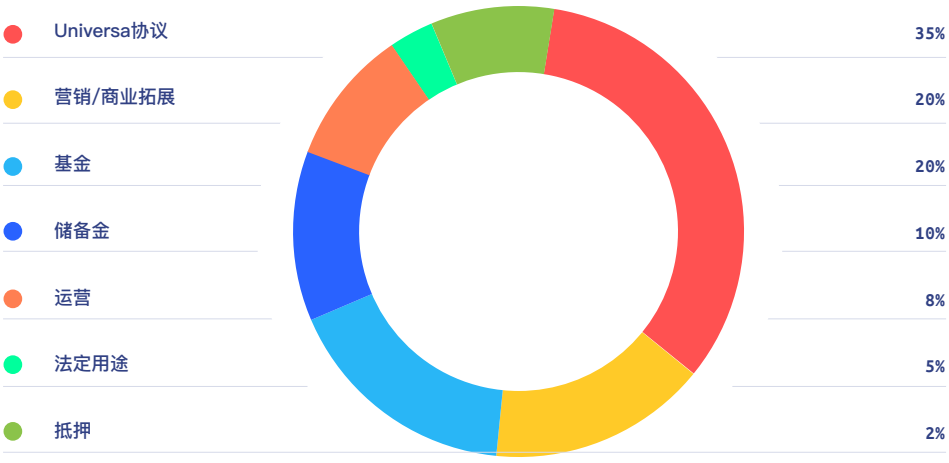
Universa生态系统由“UTN”代币资助，数字资产本身代表Universa智能合约。各UTN可被细分至18个小数位，允许进行散列交易。为便于日常使用，小数的UTN代币均具有代号，如下所示：

单位名称	UTN数值	交易比率	代币生成事件美元值
kUTN	1000	1 : 1,000	$10
UTN	1	1 : 1	$0.01
mUTN	0.001	1,000 : 1	0.001 美分
uUTN	0.0000001	1,000,000: 1	0.000001 美分
nUTN	0.0000000001	1,000,000,000: 1	0.000000001 美分

预售和代币生成事件

最初，可以将代币分为下列两个阶段。在代币生成事件期间，作为占位符产生以太坊“ERC20”代币，并且将其分配给参与者，从而可以在Universa区块链启动之前通过开放交易所进行占位符代币交易。参与者可以通过分配给以太坊钱包，立即要求得到占位符代币，或者等待，知道Universa平台运作之后要求得到报酬。在推出Universa平台时，在主区块链上产生和分配代币。对于没有要求得到占位符ERC20“UTN–P”代币的代币生成事件和预售参与者，将直接分配同时隙网报酬；代币处于“占位符赎回”账户，并且其持有者UTN–P可以用UTN作为交换，将其赎回。

	预售 2017年9月	代币生成事件 2017年10月28日
类型	公开发行	公开发行
了解客户“KYC”	需要	需要
待售代币	1,000,000,000	–
待接收金额	300万–1000万美元	高达9900万美元
UTN代币价格	0.01美元 + 20%红利	0.01美元（最低购价为10美元）



流通与需求

执行智能合约行动，需要以UTN方式支付交易费用，以便奖励其提供给网络的处理能力的参与节点，并且维持Universa平台的持续发展。该节点需要保留80%的交易费，剩余20%由Universa公司所有。Universa有权每天消耗平台所持有费用的1%。

平台结算仅采用代币进行，
不接受其他方法。

在每次交易期间，使用实际代币汇率确定各服务所需支付的代币金额。

今天，请购买（和持有！）更多代币。
明天，对于Universa服务，你将需要最终支付更少金额。

所有价格单位为美元（节点价格除外，因为节点结算可以采用代币进行）。

所有用户均需要购买代币，以使用平台。自助服务门户中的加密交换模块，可以用于管理外币（和数字资产）与UTN代币之间的相互自动转换。

预算+支出计划

Universa代币生成事件被设计用于，从希望支持未来发展的合作伙伴的开放人群销售，获得金融支持。我们的计划是动态的，并且能够调整，适应各种情况；我们保守地筹划了一项适度筹款活动，并且仅适用预售所筹款项继续推进我们的计划，即使首次代币发售没有募集到又一美元。然而，乐观地说，我们对于该项目的最终目标和愿景均是先进的，并且我们已经做好充分准备，计划将公司规模扩大至9900万美元，并且实现最终增长。我们的首次代币发售上限为9900万美元，因为我们的目标是破坏许多遍布全球的法律和政治框架，建立Universa基金会。

关于完整的预算和支出计划，包括发展目标、法律结构以及研究目标，请浏览 http://bit.lv/2fkELHm。

出资额	目前	$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
业务开发	$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

发展潜力

附加服务

服务提供商可以注册为常规服务器，并且签订有效的Universa智能合约。从Universa的观点来看，没有什么特别之处，因为节点将作为典型区块链参与者。但是，其可以提供自定义交互作用，扩展网络功能并且提供高级功能。

例如，合约可以将一组API调用合并到外部服务之中，从而允许和/或执行行动，并且生成结果。公共股票合约拥有终点，规定特定URL的GET或者请求POST HTTP，对其所有者“投票”；或者，作为电子银行服务发出的电子货币产生股息的终点。

用例实例

在推出时或者随后时间内，Universa需要在Universa平台中，提供一些智能合约通用用例的参考实施方法。同时，这些参考实施方法是开源和可适用的，允许任何人直接复制，或者用作未来发展基础。并且，提供“代币”、“发票”、“信托”以及“组织”参考。

代币合约

常见代币

智能合约的最基本案例是生成通用代币资产。此类资产是可分割、可交易以及可替代的；合约中定义行动，检查钱包余额和将代币转移到另一钱包中；这样，Universa平台可以提供各种可交易资产，以便支持其他平台和交易。更先进的代币合约可能包括下列功能，铸造新代币、消耗现有物资、冻结或者锁定一个账户或者所有账户的交易活动以及通过中介方给与支出授权。

银行支持的代币

由于智能合约是完全图灵完备并且可以与外部API交互，所以可以定义通用代币合约，其中包括用于处理与外部定义资产类周转用额外用品，包括但不限于比特币、以太坊或者甚至为法定货币。例如，合约可能规定代币为“美元–TETHER”并且支持与美元银行账户整合，并且定义“使用法定货币销售代币（sellTokensToFiat）”功能，同时接受使用美元–TETHER代币和所输入的环球银行金融电信协会地址，触发向相关银行账户汇出。相反地，可以定义相应的“使用法定货币购买代币（buyTokensWithFiat）”行动，可以在收到入境线交易时铸造新的美元–TETHER代币。类似地，可以使用此类合约退回Universa资产和其他数字资产，同时也允许通过Universa平台，与外部融资方法实现充分互操作性。

发票合约

例如，你是离线服务公司的老板，并且想在提供服务之后立即收到付款并且支出较少的交易费用。你可以创建一份智能合约，其所包含的所有文件均在附件和条件中列出，并且规定客户可以使用美元–TETHER代币予以支付；定义合约，将资产直接转给经理人账户，或者您的应收账款部门。当您的雇员交付相关服务之后，员工可以要求客户提供数字签名，确认服务结束，就可以立即进行交易。甚至可以离线然后在网络上注册进行该活动。如果需要，在签署合约之前，可以互相发送合约以供协商。但是，如果一方在合约上签订官方数字签名，那么该合约将变为不可变文件，并且另一方只能完全签订该相同合约，或者完全不签署该合约。

托管合约

数字交易所或“股票市场”

与银行支持的代币使用外部API交易其他数字或者法定资产类似，可以定义智能合约，提供双方交易的无信任托管锁，以便在双方通知付款时发布该交易。这样，交易所可以进行密码对密码交易，或者甚至与证券经纪业务整合，以便允许使用UTN、法定货币或者另一种数字资产作为支付方式，而交易其他类型证券。

公寓出售

首先，卖方应当准备一份智能合约和一套确认其财产的文件。可以是有关其财产的纸质文件图像，并且带有其合法数字签名，并且在一些国家内，可能还需要公证人签字。同时，允许使用规定银行代币来改变其所有者，在这种情况下，例如使用上述规定250,000美元–TETHER代币。

现在，双方可以协商和修改合约。在双方签订合约之后，其中一方将其发送至任意Universa节点。Universa检查双方签名并且保证存在足够金额，即250,000美元–TETHER代币。如果该节点证明合约通过率为90%，买方获得公寓所有权，卖方成为银行券代币的所有者。现在，买方可以联系地方当局或者登记部门，向他们提交有关该公寓新业主的相关文件。

数字自治组织“DAO”合约

你是一家公司的首席执行官，并且正在组织有关新任首席财务官的投票。首先，你可以创建一份智能合约，描述有关新任首席财务官的提议、以及在所有法律标准文件中的所有细微差别权利和义务。随后，在你的图形用户界面点击“开始投票”按钮。然后，通过任何渠道–甚至通过闪卡和亲自送达，将合约发送给相关同事。参与者使用该合约，通过数字签名证明其身份和投票权，并且开始投票。每一票均将构成与投票人之间的另一个新的单独智能合约，与主智能合约在前面定义的一样。之后，这些人将他们各自的“投票”合约发送给你。在收到足够多的此类合约之后，你可以更新与新任首席财务官有关的主要企业智能合约；智能合约是数字工作流基础设施的一部分，因为其包括附件文件，同时也代表完全合法的文件。智能合约允许新任首席财务官向实体开票据并且支付薪金，并且适用于法院和政府税务服务。

结论

Universa平台可用于迭代加密分类账技术，并且经证实，在货币分配方面已经拥有八年的比特币交易成功经验，并且适用于所需工具，以解决基本业务问题和政府遵从性。通过若干个数级提高实物吞吐量，内置支持验证文件真实性以及可信任的认证节点网络，Universa能够提供必要的可用性，为企业提供可采用的新途径。随着比特币和以太坊技术快速发展，满足越来越多的消费者需求，Universa将继续探索更精细的区块链采用方法，使用分布式创新满足企业的可靠性和安全性需求。

universablockchain.com