在分布式应用帐本上的

去中心化的应用程序，智能合约，价值转移，

和自治协议

摘要：权益证明（Proof of Stake，简写 PoS）算法与工作量证明（Proof of Work，简写 PoW）相比，在实现分布式共识上具有明显的优势 。结合权益证明与其他重要需求, 例如，支持简单的支付验证（SPV）技术的移动钱包，这样的跨组织协作的自动化将允许更广泛的行业采用。此外，现成的用户友好的基础构架已经拥有可以数字化和自我管理的代币化生态系统，这对于实现全球采用至关重要。现今领先的智能合约平台以太坊（Ethereum）正面临可扩展性问题，因为其计算成本高昂的工作量证明（PoW）算法以及节点下载整个区块链的必要性限制了以太坊区块链的实用性。这本白皮书介绍了尤里卡（Eureka）旨在实现社会技术应用适用性的智能合同框架，确保长期可扩展性和可靠性。尤里卡区块链是由零通胀的原生电子币供应。这种电子币会使用开发公司 Polaris Universal 所有净利润来不断回购和焚烧，以及 10%的交易费也被不断烧毁。开源去中心化平台将准备好使用 SPV 解决方案，此外这还可以允许侧链的多样化实行。这个区块链将附带一个基于权益证明（PoS）的代币，成为可以建立，存储和交易自我管理的完整基础构架。尤里卡是为广泛用于行业用途应用而打造的最先进的区块链。

1.简介

智能合约是在同意方之间促进，验证和制定协商协议的计算机协议。这些合约允许在没有中间人的情况下履行可信交易。这项技术突破可以很大的推进不同的领域，例如，数字签名解决方案[1]，物联网（IoT）[2]，金融科技[6]，价值转移，储值等。智能合约建立在去中心化账本之上，它需要通过诸如工作量证明（PoW）[7]和权益证明（PoS）[3]方式的去中心化验证系统。实现智能合同的核心技术被称为区块链，它是一个去中心化账本，它的连续块通过验证并把去中心化的节点添加到链中。因此区块链不需要任何第三方就可以可靠和安全地运行。该技术最初是通过比特币[8]的发明而引入和推广的，比特币是一种点对点加密货币和支付系统。比特币使用工作量证明（PoW）进行区块验证，意味着节点使用运算昂贵的设备进行验证。

比特币允许在其协议之上完成一组有限的操作。另一方面，许多去中心化账本使用图灵完整语言Solidity（类似于 JavaScript 语法），后者允许制定智能合约，例如，以太坊虚拟机（EVM）[9]。在撰写本文时，以太坊已被证实成为全球领先的 DAPPs 和智能合约平台，尽管它还是有多个问题。以太坊工作量证明（PoW）机制限制网络的可扩展性选项，使其实际上无法应付行业案例应用。以太坊始终面临着不同的安全问题；例如，基于以太坊的去中心化应用程序最近因缺乏正式验证所需的最新工具[11]而被黑客攻击[10]。这次黑客攻击导致了 5000 万美元的损失，以太坊在事件发生后进行了硬分叉，导致两个独立的链条。后来，由于阻断服务攻击 [12] ，以太坊又进行了另一次硬分叉。预计以太坊区块链 [5] 未来将有更多的硬分叉。

限制以太坊大规模采用的原因有很多：当前工作量证明（PoW）验证系统的低效率，需要更安全稳定的区块链虚拟机和更好的执行权益证明（PoW）交易验证[3]，以及缺乏外部与相关内部私人合同之间差异的隐私保护，这使得在以太坊区块链上，跨组织的信息物流无法实现。此外，以太坊缺乏正式可验证的智能合约语言，不需要下载整个区块链的精简钱包，以及具有简单支付验证（SPV）的智能合约的移动设备解决方案，这意味着客户只需要在连接到完整节点时下载区块头[4]。

要实现行业可扩展性，智能合约平台需要利用侧链和未花费的交易输出（UTXO）[13]的力量 ，以及能够实现与其他的区块链系统的兼容性，例如比特币。此外，采用比特币闪电网络[14] 的功能，通过双向微支付渠道达到高效的可扩展性。由于上述原因，以太坊一直在挣扎，难以实现全

球大规模采用，而尤里卡旨在引入去中心化区块链，它可提供所有去中心化帐本最先进的选项，包括解决上述问题并实现利用跨组织信息物流来优化成本和时间。尤里卡是为大规模采用而建造的区块链。

2. 尤里卡的优势

尤里卡是一个基于 UTXO 的去中心化区块链，它使用权益证明（PoS）共识模式，其中下一个块的创建者是根据区块链原生币（尤里卡币）的持有量选择而不是像使用比特币的工作量证明（PoW）一样的哈希率的度量标准。在权益证明（PoS）中，区块由权益拥有者铸造而不是由矿工开采。结果是，权益拥有者获利网络的交易和部署费用（Tx 费用）。值得注意的是，尤里卡币的通货膨胀率为零，这意味着每个区块的创建没有产生任何新币，同时每个区块的 10%交易费（Tx 费用）会被烧毁，剩余的 90%将被分配给权益拥有者。当一个币被烧毁时，这意味着它完全被排斥在流通之外，没有人可以使用它。

尤里卡与比特币和以太坊生态系统兼容，以及尤里卡虚拟机可以不断向后兼容。尤里卡区块链采用行业用例，同时也针对移动设备用户。这允许将区块链技术推广到广泛的互联网用户阵列，从而开阔了在尤里卡生态系统中的交易验证过程的去中心化。

o 共识机制

尤里卡使用权益证明（PoS）机制达成共识管理。在比特币网络中，矿工通过散列工作量证明（PoW）来参与验证过程。当矿工的哈希值（散列值）能够计算并满足特定条件，矿工可以向网络要求开采新区块。区块头随每个不同的随机数而变化。挖矿的困难调整取决于区块链网络的总哈希算力。当两个或两个以上的矿工同时解决一个区块时，会产生一个小分叉，链分成两部分。这是节点需要决定他们应该接受哪个区块的地方。在比特币网络中，最有成效工作量的成为合法链。

值得注意的是，有不同的工作量证明（PoW）算法，比如 CryptoNightV8，Scrypt11，Equihash 等。推出新算法的背后的原因是为了防止一个实体的算力的积累并确保专用应用集成电路（ASIC）不能引入生态系统，这是加密货币社区中许多人更青睐的。尤里卡选择权益证明（PoS）以达成共识。

开启权益证明（PoS）整体理念的概念是“币龄”，早在比特币存在的第一天，Satoshi Nakamoto 就知道了，并被用于优先比特币网络上的交易。币龄只是简单的电子币金额乘以持有期。举一个简单的例子，如果您从朋友那里收到 100 个电子币并持有 10 天，这意味着你累积了 1000 个电子币日的币龄。此外，在你花掉那 100 个电子币以后，我们说你积累的这 100 个电子币的币龄被摧毁或消耗。

在传统的权益证明（PoS）中，权益拥有者付钱给自己来消费他的币龄，同时获得为网络创建区块的特权和参与权益证明制度。新区块的创建必须满足以下条件：

ProofHash (证明哈希值)<电子币×币龄×目标值

这种方法的重大问题是恶意实体可以通过积累大量的币龄来发动双重支付攻击。由币龄引起的另一个问题是节点不鼓励在获得奖励后继续保持在线状态。因此，在尤里卡使用的改进的权益证明（PoS）版本中，删除币龄鼓励节点一直在线，使生态系统更加安全可靠。

由于潜在的币龄攻击和其他类型的攻击，原版的权益证明（PoS）的实现受到多种安全问题的影响。尤里卡权益证明（PoS）的版本奖励投注电子币时间更长的权益拥有者，同时又没有给予钱包保持离线的电子币持有者任何激励。

o 智能合约

在以太坊中，智能合约使用以太坊虚拟机执行。以太坊中的虚拟机假定用来转移价值的系统是帐户系统，而不是 UTXO 系统。尤里卡有一个类似的虚拟机来运行智能合约，但是区别在于尤里卡是基于 UTXO 模式，这与以太坊的账户模式不同。尤里卡虚拟机的功能与以太坊虚拟机类似。尤里卡有一个抽象层，可以将 UTXO 模式转换为尤里卡虚拟机基于帐户的界面。这个抽象层对于促进互操作性和平台独立性是必不可少的。

尤里卡的交易使用的脚本语言和比特币一样，除此之外，除了以下三个操作码外：

- ❖OP_EXEC：触发交易的特殊处理并执行特定的输入虚拟机字节码
- ❖OP_EXEC_ASSIGN：触发 OP_EXEC 等特殊处理并输入合同地址和合同数据。
- ❖OP_TXHASH：推送当前执行的交易的交易 ID 哈希

当交易输入引用输出时，执行和验证会发生。当输入脚本向返回非零的输出脚本提供有效数据时，交易有效。

尤里卡允许在合并区块链时，立即执行智能合约。这是通过包含 OP_EXEC 或 OP_EXEC_ASSIGN 的交易输出脚本的特殊处理来实现的。当检测到其中一个操作码时，在交易放入一个区块后，所有节点会执行该操作码。尤里卡的脚本语言将数据传送到尤里卡虚拟机。

为了使尤里卡区块链的 UTXO 组不会变得太大，OP_EXEC 和 OP_EXEC_ASSIGN 交易输出也是可花费的。OP_EXEC_ASSIGN 输出发送电子币或代币到另一个合同，或者到公共密钥哈希（keyhash）地址时，它会被合约花费掉。只要合同使用自杀操作将其从尤里卡区块链中移除，就会花费 OP_EXEC 输出。

尤里卡虚拟机的设计可以用于运行基于帐户的区块链，这个概念是从以太坊借来的。但尤里卡是基于比特币并使用 UTXO 区块链，它还包含一个抽象层，这个抽象层允许在无需对以太坊虚拟机和现有的以太坊合同进行重大修改情况下，使尤里卡虚拟机在尤里卡区块链上运作。

虚拟机帐户模式易于编写智能合约的程序员。检查当前合同和区块链上的其他合同的余额的操作是存在的，还有发送资金和/或信息到其他合同的操作。

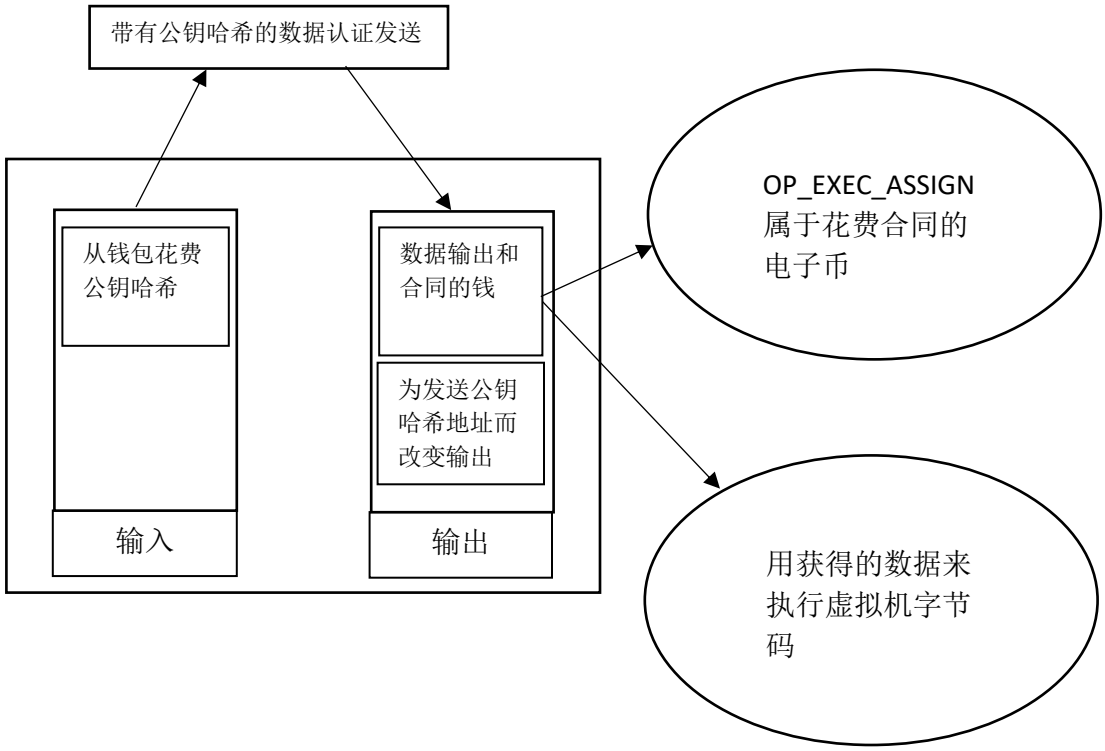


图 1. 用于分配资金和消息的合同交易

上图显示了从一份合同中发送资金到另一个合同的方法 。当合同将资金发送到另一个合同或公钥哈希地址时，发送合同方花费其拥有的一个输出，它涉及到发送的预期合同交易。这些交易必须在对尤里卡网络有效的区块里。预期合同交易是由权益拥有者在验证和执行交易时生成，而不是由消费者生成，并且这些交易没有在尤里卡网络广播。

操作码 OP_TXHASH 是允许履行尤里卡的预期合同交易的机制。OP_EXEC 和 OP_EXEC_ASSIGN 有两种不同的模式。原先的操作码作为输出脚本处理的一部分在执行时，尤里卡虚拟机会运行。另一方面，当操作码作为输入脚本处理的一部分在执行时，虚拟机不会运行从而避免双重执行。相反 OP_EXEC 和 OP_EXEC_ASSIGN 操作码的行为类似于无操作和返回 1 或 0，这就分别转化成了 “可花费” 或 “不可花费” 。OP_TXHASH 推动当前花费交易的 SHA256 哈希到脚本堆栈上。操作码 OP_EXEC 和 OP_EXEC_ASSIGN 在花费尝试期间，检查预期合同交易列表。

如果交易传递给预期合同交易清单中存在的操作码，结果是 1 表示可花费。如果不是，则返回 0，表示不可花费。因此，只有在合同和抽象层需要输出向量是可花费的时，OP_EXEC 和 OP_EXEC_ASSIGN 使用的输出向量才是可花费的。值得注意的是，在尤里卡和以太坊之间的合同兼容性是很强的，将以太坊合约移至尤里卡区块链所需的修改很少。

管理周期对于确保智能合约是至关重要，并且必须在制定之前对潜在的合作方进行适当的审查。当合同中出现业务交易冲突时，智能合约能够解决现有跨组织模式中可能出现的许多问题。尤里卡框架的价值主张是跨组织的信息和价值传递的物流自动化。尤里卡框架是可用，可扩展，适用，易于采用，经济可行，高度自动化，灵活且安全。智能合约管理周期如下：设置，部署，制定，回滚，终止。实现行业采用的工具概念之一是建立和维护社会技术尤里卡系统[16] 的信任，从长远来看是可靠的。在这种情况下，信任涉及到了使用技术实现人之间的依赖关系的目标。尤里卡在经济上是可行的，易于采用。前者意味着使用尤里卡系统可以带来经济的投资回报，而后者则意味着与尤里卡合作的进入壁垒极低。

o UTXO 模式

在 UTXO 模式中，每当交易发生时，它都使用被销毁的未使用的电子币作为输入，并创建新的 UTXO 以更改并返回给发送者作为输出[15]。 因此，每当在不同的私钥之间转移一定数量的电子币时，在交易链中花费并创建新的 UTXOs。 交易的 UTXO 被用于签署修改版本的交易的私钥解锁。 在比特币中，脚本系统通过堆栈处理数据，开发人员使用 isStandard（ ）函数[15]来总结脚本类型。 比特币客户支持：P2PKH（支付到公钥哈希），P2PK（支付到公钥），MultiSignature（少于 15 个私钥签名），OP_RETURN 和 P2SH（支付到脚本哈希）。

例如，使用 P2PKH 创建和执行脚本，假设我们向某人支付 0.01 BTC，此交易的输出为：

OP_DUP OP_HASH160 <Public Key Hash> OP_EQUAL OP_CHECKSIG

OP_DUP 复制堆栈中的顶部项目。

OP_HASH160 返回比特币地址作为首要项目。

要建立比特币的所有权，需要比特币地址以及数字密钥和数字签名。 如果前两项完全相等，OP_EQUAL 给出 TRUE（1），如果不是，则给出 FALSE（0）。 然后，OP_CHECKSIG 生成公钥，签名和与交易的哈希数据相关的签名的验证，如果匹配发生则返回 TRUE。

根据锁定脚本的解锁脚本是：

<签名> <公钥>

与上述两项的组合脚本：

<签名> <公钥> OP_DUP OP_HASH160

<公钥哈希> OP_EQUAL OP_CHECKSIG

仅当解锁脚本和锁定脚本具有匹配的预定义条件时，脚本组合的执行才为真。 这意味着签名必须通过匹配有效地址签名的私钥签名，然后结果才为 true。 这样说的话，值得注意的是比特币的脚本语言不是图灵完全，意味着没有像尤里卡那样的循环函数。

UTXO 模式允许大量隐私，因为用户可以使用更改地址作为 UTXO 的输出。 此外，在此模型中，可以通过公共帐本透明地追踪每笔交易的历史记录。 由于前面提到的原因，尤里卡基于 UTXO，其区块链允许实现基于创新设计的 UTXO 模式的智能合约，而不是以太坊的账户模型。

在以太坊中，余额管理类似于现实世界中银行账户的样子。 每个帐户都有自己的余额，存储和用于调用其他帐户或地址的代码空间基础，，并存储相应的执行结果。 内部交易仅在每个账户的余额中可见，并且在以太坊的公共账本跟踪它们是一项挑战。 尤里卡基于 UTXO 模式，我们认为它比帐户模型好得多。

o 气体（gas）模式

气体模式在以太坊中用作交易费用协议。 为了将比特币区块链转换为图灵完备协议，必须有一种机制来确定支付给权益拥有者的费用，而不仅仅依赖于交易的规模。 原因是交易可能无限循环并削弱整个区块链。

尤里卡采用了以太坊的气体概念，其中每个气体执行的虚拟机操作码都有自己的价格，每笔交易都有一定数量的气体消耗。 交易一发送，任何剩余的气体将退还给发件人。

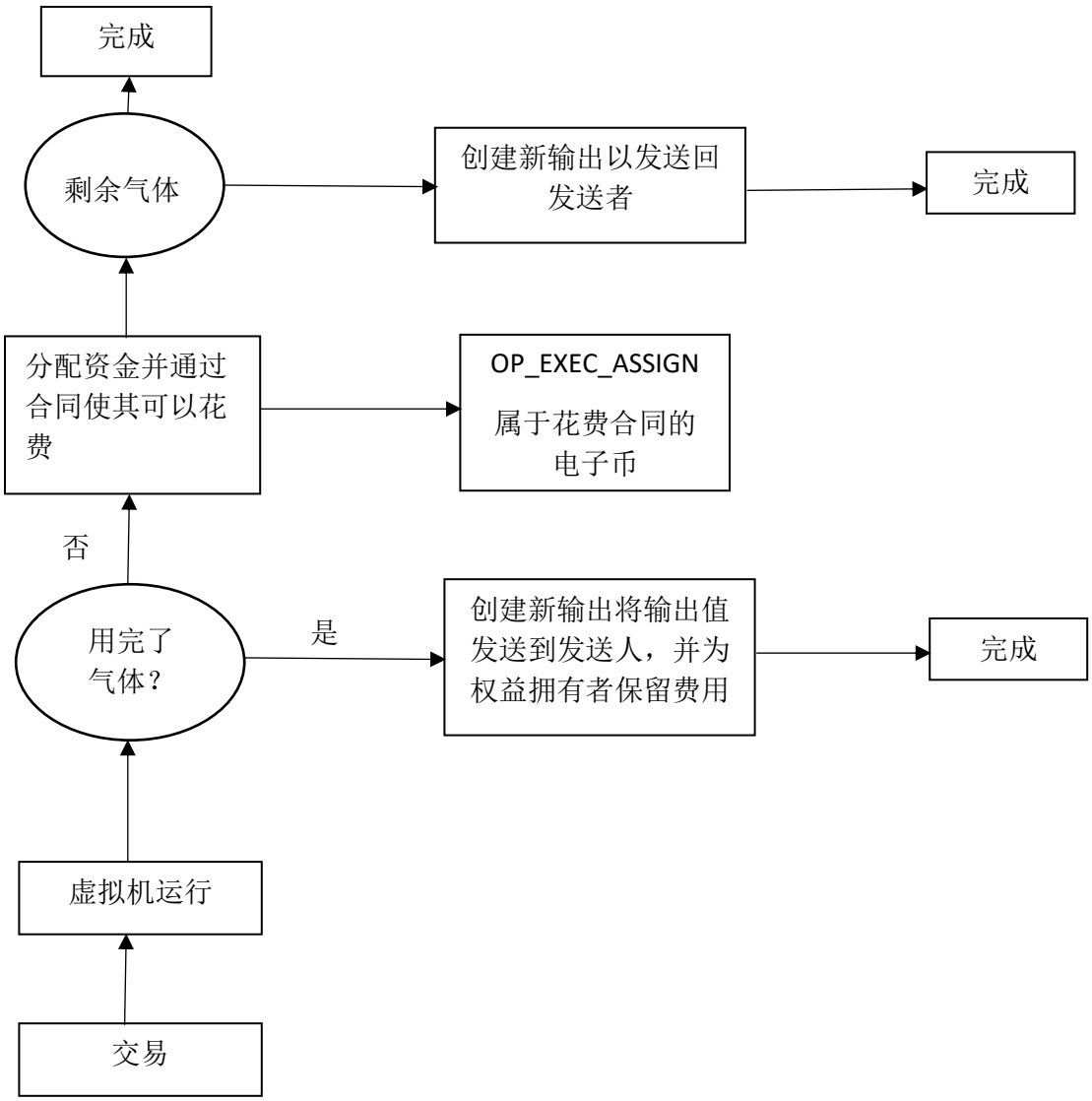


图 2. 气体退款模式

当合同执行所需的气体超过交易中可用的气体量时，交易引起的变更将被恢复。 因此，任何修改的永久存储器都将被还原，并且不会花费资金。 但是，由于已经花费了投注资源，所以交易的所有气体都被消耗并提供给处理器。 由于尤里卡网络的规格与以太坊相反，我们预计每个虚拟机操作码的气体价格（GasPrice）与以太坊明显不同。

在创建交易或部署合同时，用户为气体指定两件事。 首先是气体上限（GasLimit），它确定合同执行的可消耗气体量。 第二个方面是气体价格（GasPrice），它设定了用户准备支付的每个气体单位的确切价格，并且它在 Yuris 中给出，它们等同比特币中的 Satoshis，这意味着它们是尤里卡区块链最小的记录单位。 合同执行的最高尤里卡支出等于气体价格和气体上限的乘积。 如果该最大支出超过交易提供的交易费，则后者无效且无法处理。 扣除此最大支出后的剩余交易费用是交易规模费用（Transaction Size Fee），类似于标准比特币费用模型。

为了确定交易的适当优先级，权益拥有者考虑两个指标。 首先，交易规模费用必须与交易的总规模相匹配。 第二个指标是合同执行的气体价格。 通过将这两者结合起来，权益拥有者选择最有利润的交易来处理并包含在一个区块中。 因此，这有一个自由市场费用模式，权益拥有者和用户优化最适合他们的交易速度和他们愿意支付的价格的费用。 值得一提的是，尤里卡区块链非常快速，便宜而且可靠。 这是因为结合了链上和链外缩放解决方案的理念，并没有为生态系统提供可能成为可扩展性瓶颈的任何不必要的限制。

3.侧链

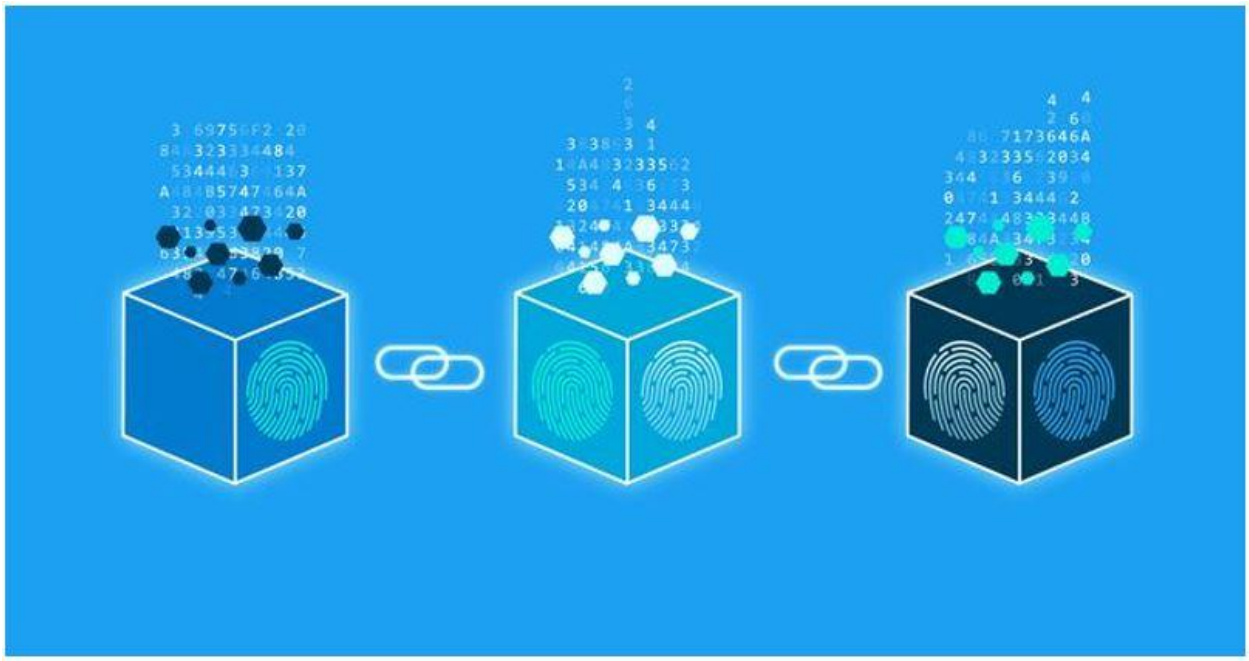
尽管尤里卡的构建是为了能够在链上进行大规模扩展，但在协议之上构建侧链将确保高效率，这将有助于每时每刻保持网络的平稳运行。侧链是与尤里卡区块链并行运行的次级账本。尤里卡区块链的进入可以与侧链相连; 这允许侧链独立于尤里卡区块链运行。 Polaris Universal 正在开发的侧链的两个主要功能是支付渠道和权益证明代币。侧链的可能性是无穷无尽的，来自世界各地的人们可以在尤里卡上建立侧链。开发公司正在开发用户友好的界面，开发人员可以使用这些界面快速在尤里卡上构建安全可靠的侧链。比特币的闪电网络是在全球范围内廉价而快速地进行交易的最有效方式之一。 尤里卡拥有举办类似闪电支付渠道所需的所有规格。另一方面，构建权益证明代币的能力将允许开发人员构建自治代币，并且代币的持有者将获得当代币转手时产生的交易费用，此外还能够通过管理节点来管理侧链。 尤里卡是一个开源区块链，我们期望在未来几年及更长时间内在侧链领域看到更多创新，而尤里卡是一种先进的开源区块链，具有全球采用所需的所有特征。

4.尤里卡生态系统的基础构架

尤里卡的技术允许在协议之上构建侧链。 尤里卡区块链配备了一个基础构架，可确保从一开始就支持采用。 用户友好的界面将允许任何人启动代币，类似于以太坊的 ERC20 标准，该标准通过单独的权益证明机制进行管理。 这意味着代币的持有者将能够堆栈他们的代币以保护和管理代币的侧链并收集代币生成的交易费用。 值得注意的是，交易费用将使用尤里卡币支付，因为它是主要区块链的原生币或燃料。 用户可以简单地转到界面并输入新权益证明代币的名称，符号，小数和总供应量，以便创建它。 拥有此类界面的目标是使代币化和数字化更加用户友好，同时还响应对自治代币化生态系统日益增长的需求。

尤里卡还配备了一个用户友好的钱包，用于存放尤里卡币和基于协议构建的代币。 相同的钱包界面将允许电子币持有者和权益证明代币持有者参与权益证明。 此外，任何创建的代币都可以立即开始在点对点去中心化兑换中进行交易，该兑换建立在尤里卡之上，尤里卡也是尤里卡区块链附带的基础构架的一部分。 Polaris Universal 开发公司支持这一基础构架，可以确保尤里卡成立的早期阶段的采用和实用性。

5.尤里卡区块链经济



o 尤里卡的概念

在 20 世纪，由于在全球传播信息方面取得了突破，人类在提高地球上每个人的生活质量上，迈出了重要的一步。随着计算机的兴起，互联网的出现解决了许多问题，并通过 TCP / IP 协议使传输信息极其快速和可靠。互联技术的发展引入了互联网，物联网和虚拟现实等多种可以在人，信息和物体之间进行交互的方式，并允许更多的东西变得数字化和代币化。人类现在需要的下一次进化是通过优化安全性和信任来解决全球信息共享带来的许多问题。启动新一代技术所需的关键创新是使用点对点方法共享信息和价值的某种方式。比特币是由 Satoshi Nakamoto 在 2008 年末推出的，这个理念永远的改变了人类。 Satoshi 发明了一种点对点电子现金系统，这意味着他终于找到一种完全安全和去中心化的数字化传输价值和信息的方法。尤里卡是这个故事的延伸。

❖尤里卡区块链的背景和意义

尤里卡使用了比特币在 2008 年引入的区块链技术。区块链是去中心化的账本，这表示没有任何的服务器位于系统之上，又意味着没有单点故障。这创建了极其安全的系统，全世界都可以构建其基础架构，而不是依赖于可能出现单点故障的集中式服务器，并且当这些服务器遭到黑客攻击时，损害可能是灾难性的。区块链分布在全世界的节点之间，每个节点充当帐本的审阅者。去中心化对安全的影响确实是突破性的。另一方面，去中心化本身对人类来说是一件好事，因为它赋予人们在不需要第三方时免除它的权力。无论何时，当中间人不被需要时，强行拥有中间人实际上对国家财富都是有害的。历史告诉我们，在许多情况下，中间人可以发展出一种权力，他们不该拥有指挥人们该怎么用钱，支配资产，有时甚至是主宰他人的生命。这没有办法确保那些强大的中间人与好人共享相同的道德价值，这就是为什么集权在宏观层面上可能是非常有害的，唯一的解决方案就是去中介化。换句话说，每当不需要第三方时，就不应该有任何第三方。

❖尤里卡区块链的愿景

今天的区块链行业仍面临许多技术和实施挑战。 主要问题是缺乏新的和更强大的智能合约平台以及缺乏与现实世界数据的交互等。 我们正在引入一个全新的区块链生态系统，尤里卡作为世界价值转移协议的替代选择。 尤里卡基于 UTXO 模式并使用类似于以太坊的虚拟机来实现比特币和以太坊之间的公共区块链兼容性

尤里卡的目标是通过与其他区块链社区，第三方开发商和技术创新合作，创建一个具有全球影响力的开源社区。 尤里卡旨在将区块链技术引入金融，游戏，物联网，社交媒体和其他行业。 尤里卡是一个兼容的生态系统，它利用 Oracle 和数据馈送并与监管逻辑相结合，将现实世界与区块链世界联系起来。

我们有足够的理由相信，当集权化带来的财务损失达到顶峰时，人们自然会转而使用开源数字货币进行商品，服务和生产资本的交易。 尤里卡币是去中心化货币的一个完美例子，该货币的构建是为了能够长期存储价值，因为它背后的经济模式。

o 尤里卡的技术模式

❖ 与 UTXO 和以太坊虚拟机的兼容性

我们认为，确保交易一致性和代币可追踪性的最佳区块链技术是比特币的 UTXO 模式。另一方面，所有以太坊的智能合约都可以在尤里卡区块链上运行，如果有需要修改的话，都只需要最小的变化。尤里卡区块链结合了比特币和以太坊网络的优势，同时解决了所有固有问题。

❖ 达成共识

尤里卡采用了一种权益证明共识机制，这意味着价值不会浪费在外部实体上，而是保留在生态系统中。 比特币矿工花费数十亿美元给外部 ASIC 制造公司，这是浪费价值，应该用于购买比特币本身。 在尤里卡案例中，权益拥有者需要购买尤里卡币并将其放入钱包中以参与权益证明（PoS）流程。

❖账本

账本存储所有智能合约，并允许尤里卡用户根据自己的兴趣在点对点网络中下载代码和合同。 账本提供透明度，可读性和可听性。 数据馈送是从链外获得的数据资源。 Oracle 选择最合适的数据来触发智能合约的执行，智能合约以可读格式存储在尤里卡区块链中。

• 数据馈送：

代表从链外资源（如货币汇率，股票市场，航班时刻表等）获得的数据的馈送，这些数据被放入区块链中以执行智能合约或去中心化的应用。

• Oracle：

在尤里卡，oracle 可以表示节点，特定的受信任组织，实体或公钥地址。 当存在用于查询的数据输入的多个数据资源时，oracle 基于预定义的规则集选择最合适的数据资源。

• 链上和链外触发器：

在尤里卡，链上和链外因素都可以用作执行智能合约的触发器。

o 尤里卡币

尤里卡币是尤里卡区块链的原生电子币，它是该协议的燃料。 购买该币需要能够发送交易或在去中心化的账本上部署智能合约，DAPP 或侧链。 尤里卡币是一种实用电子币，有足够的理由吸引持续的需求，开发公司正在使用其所有净利润添加回购和燃烧策略，预计可以确保对尤里卡币的价格有强烈的购买支持。 Polaris Universal 拥有多项业务，包括加密货币采矿场，并参与加密货币金融市场的活跃交易。 公司在支付所有管理费用后实现的所有净利润不断回购并燃烧尤里卡币，这减少了供应量，同时确保了对该电子币的不断需求。

尤里卡币的初始供应恰好是将要存在的电子币总量。尤里卡币的通货膨胀率为 0%意味着不会再创造任何电子币。 事实上，由于 Polaris Universal 的回购和燃烧过程，流通中的电子币数量只会不断减少，而且 10%的交易费用也会持续燃烧。 尤里卡币的总供应量为 1.5 亿枚电子币。 尤里卡币是为尤里卡区块链提供动力的燃料，此外还具有实体价值的所有特征。

2019 年尤里卡币销售

出售的硬币数量	1.25 亿枚尤里卡币
电子币的分配	每次销售都会向推荐人提供 10%的联盟佣金。 如果电子币买家没有被任何人推荐，10%的佣金将立即被烧毁。 1500 万枚电子币将用于开发团队和早期支持者。 1000 万枚电子币将用于尤里卡基金会。 所有未售出的电子币将在电子币销售结束时被烧毁。
在电子币销售期间 1 枚尤里卡币的价格	￥0.06 美元
电子币销售期间，接受的货币	比特币 Bitcoin (BTC), 比特币现金 Bitcoin Cash (BCH) 和 以太坊 Ethereum (ETH)

免责声明

电子币销售的参与者可以使用尤里卡币。 购买者需理解，在法律允许的范围内，尤里卡既没有明示或暗示的保证，并且尤里卡币是按“原样”购买的。 购买者也需明白，尤里卡不会在任何情况下提供任何退款。

6.结论

本白皮书介绍了最先进的区块链技术解决方案的尤里卡框架。尤里卡使用权益证明（PoS）验证和类似于以太坊的虚拟机。后者始终保持向后兼容。尤里卡借鉴了比特币的 UTXO 概念。

将权益证明（PoS）集成到尤里卡，与使用了工作证明（PoW）的以太坊先比，大大节省了运算工作量。虽然以太坊也计划采用权益证明（PoS），但目前还不清楚何时会实施这个计划。与以太坊的帐户管理相比，使用 UTXO 可以实现更大的可扩展性。 结合简单的支付验证（SPV），开发公司已经开始为尤里卡构建智能合约移动设备解决方案，以实现大规模采用。尤里卡框架具有完整的用户友好基础构架，允许创建，存储和交易权益证明代币。尤里卡是一款可扩展且可靠的去中心化区块链，专为商业用途而设计。 有关最新更新和发展的更多信息，请访问尤里卡网站。

参考

1. N. Emmadi and H. Narumanchi. 加强许可的不变性
具有无密钥签名基础构架的区块链。 在十八世纪的会议录中
分布式计算与网络国际会议, ICDCN '17，页码 46:1–46:6, New York, NY, USA, 2017. ACM.

2. Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman. 在物联网中，走向一个
基于区块链技术的隐私保护访问控制模式，页码 523–533. Springer International Publishing, Cham, 2017.

3. I. Bentov, A. Gabizon, and A. Mizrahi. 没有工作量证明的加密货币，页码 142–157. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

4. D. Frey, MX Makkes, PL Roman, F. Ta¨iani, and S. Voulgaris. 将安全的比特币交易带到你的智能手机上。 在第 15 届国际会议，适应和反射中间件研讨会论文集中, ARM 2016，页码 3:1–3:6, New York, NY, USA, 2016. ACM.

5. https://bravenewcoin.com/insights/casper-plasma-and-sharding-a-light-on-ethereums-scaling-spectrum

6. O. Bussmann. 金融的未来：金融科技，技术中断和精心策划
革新，页码 473–486. Springer International Publishing, Cham, 2017.

7. M. Vukoli´c. 可扩展区块链结构的探索：工作量证明与 BFT 复制，pages 112–125. Springer International Publishing, Cham, 2016.

8. S. Nakamoto. 比特币：点对点电子现金系统，2008.

9. G. Wood. 以太坊：一种安全的去中心化式广义交易账本。以太坊项目黄皮书，2014.

10. https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

11. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N.

Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Zanella-

Beguelin. 智能合约的正式验证：简短的论文。在 2016 年 ACM 编程语言和安全分析研讨会论文集中，PLAS '16, 页码 91–96, New York, NY, USA, 2016. ACM.

12. https://cointelegraph.com/news/ethereum-hard-fork-no-4-has-arrived-as-dos-attacks-intensify

13. K. Croman, C. Decker, I. Eyal, AE Gencer, A. Juels, A. Kosba, A. Miller, P.

Sax- ena, E. Shi, E. Gu¨n Sirer, D. Song, and R. Wattenhofer. 关于扩展去中心化区块链，页码 106–125. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.

14. J. Poon and T. Dryja. 比特币闪电网络：可扩展的脱链即时支付，2015.

15. AM Antonopoulos. 掌握比特币，2014.

16. E. Paja, AK Chopra, and P. Giorgini. 基于信任的社会技术系统规范。 数据与知识工程，87:339 – 353, 2013.