白皮书

具有一致性算法的加密货币
股权证明

版本2020年3月

目录

1. 摘要

PZM Cash 是一种为快速增长的生态系统的支付工具而创立的加密货币。在这种生态系统中每个参与者的经济动机都将保障整体财富的增长。PZM Cash 战略成功的主要因素是对货币量供求规模的扩大和平衡的预期。

PZM Cash 的结构优势：

- 保证分布式总账安全的侧链协议；
- Proof-of-Stake 的共识算法；
- 为去中心化应用程序的开发者（DApps）提供最多功能。

PZM Cash 团队对先前使用的 POS 共识算法进行了重大升级。PZM Cash 网络中的交易费是固定的，从而保证锻工之间报酬的公平分配。

PZM Cash 和 PoS “传统” 概念的关键区别在于货币供应量网络的填充机制。PZM Cash 团队放弃了在第一区块生成时的全部发行——使用预挖矿进行网络发布时，只有货币总数的 1%会被分配。其他货币在 Pos 挖矿中发行——以奖励 PZM Cash 的忠实持有对网络的支持。

锻工将获取在链上添加区块的交易费。同时，添加区块的机会线性地取决于钱包资金量，即当前的 PZM Cash 堆栈。除了交易费之外没有锻造的任何额外费用——网络启动后所有发行将通过 PoS 挖矿进行。

PoS 挖矿机制由两个主要成分组成：

- “主导的”激活钱包；
- 支持钱包——由主钱包的交易而激活的钱包。

酬金支付到主钱包，其数额取决于主钱包和所有支持钱包的余额。并且，余额中的货币量是影响酬金的唯一因素。酬金数额不会随时间的变化而改变。

如果钱包堆栈达到总发行量 （1000000 PZM Cash）的 0.011%，PoS 挖矿停止。这样该网络可以避免资产过度集中的风险。

通过 PoS 挖矿向忠实用户提供报酬为网络提供了有支付能力的用户基础，并在 PZM Cash 生态系统中产生对服务的需求。此外，侧重开发具有最大功能的 DApp 的便利性的体系架构将通过创建大量独立的应用程序来提供广泛的服务和定制案例。

在 JavaScript 上实施的 PZM Cash 可以额外地扩展第三方应用程序的范围——语言的相对简单性允许多数开发者参与扩展 PZM Cash 生态系统功能的工作。这样也可以大大扩展与 PZM Cash 相关的浏览器方案的功能。

通过使用 JavaScript 提供的 PZM Cash 的最终优势是能够将解决方案应用于 Web3 js 钱包。因此，广大的合作伙伴将可以访问余额并统一 PZM Cash 作为付款工具。

2. 产品和用例

用例

PZM Cash 首先是与其相关业务的独立透明的国际付款方式。

任何用户在不受地理位置的约束下可以进行交易并自愿参加网络管理，为此需要部署节点并安装需要的软件。

任何一个 PZM Cash 用户有加密货币的两个用例：消极的和积极的。他们的区别在于参与的网络开发程度的不同。在消极的用例中网络参与者是普通用户，在积极的参与中用户也充当网络管理员（锻工）并积极地参与网络的发展和扩大。

因此，网络中有两种参与者：

- 使用热钱包（在 web 环境内）的普通用户。他们不会在计算机上为网络需求分配空间，不部署节点，仅通过在钱包中持有 PZM Cash 来获得收入；
- 锻工——通过锻造获得收入，即在链上添加新的区块。

消极用例

在这种用例中客户使用钱包的浏览器（web）版本（热钱包），该版本允许进行网络上的交易（包括智能合约的执行）等主要功能。

已注册并激活的钱包可让客户通过双因素 PoS 挖矿算法获得额外货币的收入。用户钱包中的货币愈多，他的奖励愈高。详细的计算因素可以参见相关部分。

浏览器方案允许用户不需为区块链的需求在硬盘上分配空间，也不要部署节点。

为实施消极用例参与者需要：

1. 在 PZM Cash 网站上创建并激活热钱包。激活需通过输入交易来完成。
2. PoS 挖矿程序在当钱包余额达到最小值——1PZM Cash 时开始。
3. PZM Cash 的额外收入取决于 PoS 挖矿因素——主钱包余额和支持钱包的总余额。
4. 用户可以将多余的货币（流动性过剩）在加密货币交易所兑换另一种必要的货币，并使他们的数字资产多样化； 或用于支付 DApps 服务和交易。

积极用例

在该用例中用户积极地参与网络构建——在分类账中添加新的区块和记录并确认，即区块链的同步和管理。

参与者因其他用户交易的确定和新的区块的添加而获得以锻工佣金形式的收入——收入百分比取决于区块交易量。

为实施积极用例参与者需要：

1. 部署完整节点：为区块链的需求在计算机硬盘上分配空间并安装特殊的 PZM Cash 程序。
2. 随时保持尽可能多的 PZM Cash 货币余额。货币余额的增加会提高添加区块的机会。
3. 保持节点在线，形成新的区块并建立包含哈希交易记录的区块链分支。
4. 以手续费的形式来获得确认交易的报酬——其百分比取决于交易金额（锻造）。

部署节点后帐号将有权在 PZM Cash 区块链上（锻造）添加新区块。如果在形成区块期间，在世界上的任何一个地方进行交易，并从未分配的交易池中进入该区块，则生成该区块的帐户会收到一笔因交易而产生的固定佣金。该区块中所有交易的佣金金额是构成该区块的帐户应计的锻工报酬

使用特定帐户将新区块添加到区块链的机会越高，钱包中的静态 PZM Cash 货币的余额就越高，并且新区块未添加到区块链的时间越长。

PZM Cash Wallet

PZM Cash 钱包是用于管理账号余额中货币的唯一工具。它可以通过用户的私钥来执行输出交易，并生成详细信息（公钥）以接收来自其他用户的交易。

钱包功能：

- 进行 p2p 交易；
- 执行智能合约时进行交易；
- 用样板创作智能合约；
- 提供 PZM Cash 生态系统去中化应用程序的访问；
- 显示钱包的余额及其变化的动态。

区块链密码学基于非对称的加密。这意味着每个钱包都有公钥和私钥。数字钥匙是存储在钱包中货币访问控制的记录（字符集）。

数字密钥始终成对：每个钱包都有一个私钥和公钥。公钥是识别网络上的钱包所必需的，并用作接收收入交易的详细信息。私钥用于签署输出交易并把货币转移到区块链上的其他钱包。私钥负责控制钱包中的货币，因此应始终在帐户持有人的控制下。

此外，数字密钥由用户创建并保存，或者可以由用户钱包的软件生成并管理，因此完全独立于区块链协议。

首次访问 PZM Cash 时，每个参与者都必须使用 Web 客户端（浏览器访问）并创建帐号——通过简单的操作即可生成私钥。

私钥是按照用户在网站上首次进入个人中心时输入数据生成的。必须确认字段的标准填写格式，将私钥以符号记录的形式在其中表示，或者可以自己输入字符集。确认输入后私（非公开的）钥将生成。

私钥必须记录下来，因为这是独一无二的并且无法重新生成。如果私钥丢失，将无法登陆帐号，并且钱包资金将不可访问。只有正确的私钥才允许访问钱包。私钥类似于数字签名，建议保存在便携式存储器或本地磁盘中。

之后需要在 PZM Cash 网站上激活钱包。这样可以充分地利用钱包功能进行交易并参与 PoS 挖矿。

为此需生成公钥——指导其他用户将货币转账到您的钱包时的账户信息。当进入钱包后的第一个交易被确认后（交易信息在区块链中记录），您的钱包变成完全可用的。公钥与其数据一起存储在验证数据分支中。

为了接收及发送 PZM Cash，还需要使用通过这两个密钥生成的另外两个元素。其中一个是地址。地址是由公钥和私钥创建的一行数字和字母，这些密钥的“指纹”。因为私钥和公钥有复杂的格式，为方便起见，根据数学算法被转换为更方便的格式。这类公钥和私钥的版本分别称为公开地址和私人地址。

私人地址提供对帐户的访问权限，并因此提供对货币的访问权限，公开地址是钱包号码，其他用户可使用该钱包号码将货币转移到该钱包。

要创建输出交易，您必须确认其中的货币的所有权为此，有必要表明用户知道密钥。因此需使用数字签名。数字签名是根据私钥和交易中包含的其他信息组合（由创建交易的用户输入）被计算出来的加密元素。因此数字签名是同意进行输出交易的确认，并且是独一无二的。由于数字签名是使用私钥和其他交易信息的组合来计算的，因此它们还展示了有关密钥的信息以及确认交易中数据的权利。因此每个签名只对一个特定交易有效。

Web3js

在 JavaScript 中实施 PZM Cash 可以使用到 Web3js 技术，它能通过规范化而大大地扩展 PZM Cash Wallet 的功能。该钱包可用在合作平台上（例如，在交易所和赌场中），而无需要为每个项目创建单独的钱包。此外，浏览器版本无需访问区块链内核以集成新资源。

Web3js 是 JavaScript 库的集合，允许使用 HTTP 或 IPC 连接与以太节点进行远程交互，从而通过专用 API 简化 PZM Cash Wallet 的集成。因此合作伙伴无需部署完整的节点即可以进行集成。

智能合约

我们的钱包不仅允许把交易发送到网络其他参与者的地址，还可以发送到智能合约的地址，从而基于数字算法发起各种交易。

智能合约是使用数学算法在满足既定条件后自动执行交易的数字协议。该程序完全由算法逻辑被控制，因此智能合约的执行不需要第三方的参与——代码的不变性是其保障。通过在创建智能合约时将其代码写入区块链，可以保证代码本身的不变性。智能合约经输入交易激活，并以此从区块链中“提取”并接收数据。

为了访问智能合约，用户需要创建输出到具体合约地址的交易。交易一旦确认，合约就开始执行。

参与者的义务以“如果....就.....”的形式，即交易的形式被确定。例如：“如果甲汇款数字货币，乙就转让任意资产（数字化）权”。在区块链中会产生一个无法更改的相关记录。同过对该记录的查询，可以随时确权数字资产并确定其交易事实。

智能合约从外源接收有关资产数字化确权的信息，并且每个区块链的节点独立地执行智能合约。这意味着每个节点都独立地收到来自外源的数据。但是为了在区块链中没有冲突并达成共识，每个节点必须从外源收到相同的响应（在一段时间内保持不变）。 为此，“甲骨文”就是外源和直接位于区块链中的智能合约之间的软件层。

智能合约并不直接访问外源，而是访问相应“甲骨文”，该“甲骨文”创建在一个将必要数据写入分类账的输入交易中。因此每个节点接收相同的数据副本，使智能合约的执行成为可能。

3. 技术的实施（core）

讨论加密货币的技术实施或“内核”时，需要指出的是共识算法和区块链协议，并且还远远不止这些。协议是区块链的体系结构和主要规则，而算法是借此执行的机制。协议确定规则，而算法告诉系统遵守这些规则的所有条件并为了获得所需的结果应该采取哪些措施。换句话说，协议是一个“静态”网络，共识算法负责其动态性：对协议进行更改并由网络根据协议获取新状态。

协议：分布式帐本（分布式总账技术）和网络节点（节点）

区块链是通过链表概念实施的数据库（分布式总账技术），其中每个新记录都以加密（散列）形式包含上一个记录的信息。分布式总账技术保障交易记录的永久保存，并查明交易按顺序关联。区块链主要优势是其稳定性。如果某个区块被更改（例如，受到恶意攻击），则所有后续区块将自动更改，这将可以立即检测到任何伪造企图。

PZM Cash 加密货币在专注于去中心化应用程序的开发、发展及功能扩展的区块链上实施。与以太坊以及其他为了创建去中心化应用程序并启动智能合约（例如，Solidity）而使用专门编程语言的区块链不同，PZM Cash 使用更流行也更简单的 JavaScript。这一特性使该平台对许多开发者开放，并保证规模的扩大和定制案例的开发。换句话说，为开发 PZM Cash 的去中心化应用程序（Dapps）不需要学习特殊的语言。

JavaScript 为开发者提供大量的特殊程序库，有助于在密码学、交易、P2P 等领域进行开发。每一个程序库符合 ZPM Cash 协议。因此，PZM Cash 方案是为尽可能广泛的受众而设计的。

区块链的主要特征是在同一平台上为启动经过完全调试好的应用程序和独立的区块链而使用侧链技术。侧链是在主帐本上实施的独立分类帐。创建的侧链不会影响主网的大小。

这样就可以达到：

1. 无限的可扩展性：使用侧链技术允许无限地扩展网络。
2. 提高网络安全性：由于侧链位于主网之上，因此不可能通过在“子”网络中制造故障或破坏其运行的稳定性来破坏主网的运行。例如，在以太坊中如果发生错误，则需要使用硬分叉进行修复。
3. 开发功能的扩展：开发者可以在侧链中试验应用程序，而不必担心产生的错误会破坏主网的运行。每个项目（dApp）都是在单独的侧链中创建的，因此开发者较大权限来调整应用程序。
4. 侧链技术可以不需要部署虚拟机来消除故障。例如，在 EVM（以太坊虚拟机）中为了消除故障则需要。

此外该平台为执行智能合约提供了去中心化的文件存储和监管服务。甲骨文服务可以确认已发生或正在发生的事件的信息。

为用户提供去中心化应用程序的目录（包括为便携式设备：智能手机、平板电脑等等提供）。每个实用程序都在主链中注册，客户可以在每个侧链中看到所有可用的应用程序和服务。用户可以在同一地点访问所有去中心化的应用程序，像 GooglePlay 或 Apple Store 一样。

PZM Cash 的重要特征是 PoS 挖矿——一种除了最初的货币产生外，还为网络填充额外的流动性的算法。

开发者意识到这是扩展货币供应量的较激进模型，因此选择了最初设计的用于创建补充用例的内核。这样可以达到 PZM Cash 货币的供求平衡，从而避免发生生态系统中通货膨胀机制以及汇率贬值。

主链包含侧链的哈希数据——一种经过特殊方式加密的记录，通过它们可以检查原始记录的完整性和真实性，但不允许解密。这是做都是为了提高所需的网络运行速度。

每个 PZM Cash 区块包含以下信息：

1. 关于区块的信息：

- 区块版本和唯一的区块标识符；
- 按秒计的区块暂时标记；
- 上一个区块的标识符和加密哈希值； 从侧链收到的信息；
- 网络状态指标（印痕）；
- 区块创建的 ID 账号，以及为了识别该区块的帐号公钥。

2. 关于交易的信息：

- 存储在区块中的交易数量；
- 交易数据：含在区块中所有交易的数据，包括其标识符；
- 包含在区块中交易的 PZM Cash 总额，包括佣金金额；
- 智能合约的数据。智能合约的状态信息；
- 区块有效载荷长度和区块有效载荷的哈希函数值；
- 锻造阈值和区块的累积复杂度。

PZM Cash 节点

区块链节点或网络节点是另外一个不可分割的体系结构元素。许多独立节点的存在可以创建分布式（去中心化）结构的网络。这个想法是，每个独立设备在专用硬盘上存储分类帐的当前有效版本，即任何具有 PZM Cash 软件的设备都算为一个单独的节点。

同时，节点是同步的，因此，即使大量节点发生故障，其余节点也将指出错误。这导致了一个事实，即，为了对区块链进行攻击，攻击者需要同步更改大量节点中的数据，随着网络的发展，这一点变得越来越困难。

PZM Cash 网络中的每个节点都具有按块处理和转移交易和信息的能力。此外，节点彼此同步（它们包含区块链当前状态的相同记录）。这样就消除了货币双重支出（double spending）错误的可能性，意思是：同一枚货币同时参与不同的交易。

PZM Cash 使用两级节点的结构：

1、全节点。

全节点是有安装有 PZM Cash 软件并存储区块链的完整当前有效版本的设备。全节点可以作为共识节点（参与创建新的区块——锻造）。全节点的持有者可以积极地参与区块链的形成，将输入的交易不断地分组到区块，并通过网络进行分配。

全节点还可作为审核节点。在这种情况下节点定期检查（并确认）其他节点的锻造结果，并在网络上分配负载，从而作为区块链数据的一种内容分发网络（CDN）。

2、轻客户端

第二种节点是轻客户端。它们之所以被称为“轻“，是因为没有完整版本的区块链，仅包含对节点重要的数据，这样可以限制硬盘上所需的分配内存量和计算能力。因此这是创建专用加密货币钱包很好的方案。

轻客户端只存储实施自定义用例所需的数据。例如，这种轻客户端可以生成交易并跟踪钱包的余额。如果用户不需要其他的，那么他的设备不会加载任何多余的东西。

于是，我们获得可以在移动设备上或在 PZM Cash Wallet 网站上的个人中心里工作的客户。同时，用户不必存储区块链的本地副本，因为存储私钥足够用于发送交易，借助私钥记录交易数据。

但是，与其他加密货币不同，PZM Cash 轻客户端的用户可以因支持生态系统而获得奖励。的确，轻客户端无法参与锻造并添加新的区块，但是 PoS 挖矿算法可以为轻钱包中的余额提供稳定的新货币流量。

共识算法

网络的主要程序是交易程序，从技术上讲，这与往分类帐中添加新块有关。新区块的添加根据一定的
一致的算法（共识算法）进行。

共识算法可以查明并确认每个交易的真实性，以及同步所有节点上的区块链版本。此外，需要在某些节点可能挂起或掉线的条件下提供每个节点对区块链相同的“观点”。同时，它还旨在保护系统免遭未经授权的访问，更改过去的交易列表和黑客攻击。这必须按照仅在网络上处理消息的通则进行操作。

共识算法可确保系统的动态性（即系统的发展和增长），同时保留区块链的独特属性：节点的平等性（每个人都可以参与添加区块）和客观性（无需要信任某些第三方来源即可确定交易日志的当前版本——信任的根源在区块链自身中并在算法中已设计）。

并且，共识是被不断保障的：处理每个交易和每个区块后网络的每个节点都达到相同的状态。也就是说，共识算法保证网络上的所有节点始终有区块链相同的版本，并消除节点之间的冲突。

共识算法确定条件：如果有权向网络中添加区块的网络参与者满足该条件，则他将获得优先机会把自己形成的区块放入分类账中。网络将识别出该区块，并在网络上就其新状态达成共识，并且该区块的“作者”将获得奖励。

有许多不同的共识算法，它们在此条件以及满足该条件的情况下彼此不同。其中最受欢迎的是两种：工作量证明（Proof of work）和股权证明（Proof of stake）。

工作量证明（Proof of work）算法要求创建新区块的作者来解决特定数学问题，而该问题只能通过数值的暴力破解来解决。典型的方案是查找包含前个比特币区块链接的区块名称的特殊哈希值

所有挑战者都可以通过添加区块来解决该问题，率先解决该问题而获得奖励的机会取决于可用的计算能力。节点的计算能力越大，机会就越多。根据网络节点的总功率，必要的工作速度由所选问题的复杂度保障

工作量证明的缺点很明显：进行着无用的计算浪费大量的计算能力。该算法的正确性也很有争议。简而言之，可以归结为一个简单的规则：“谁拥有更强大的设备谁就有优势”。换句话说，成功完全取决于设备投资的金额。先不说电力成本，为此引起的环保问题以及创立 ASIC 专用设备生产的整个行业的兴起，除了计算特定加密货币区块链中的问题外，对于其他都毫无用处。此外大型玩家实际上可以通过获得总计算能力的 51％夺取网络的控制。

与算法相关的另一个基本缺陷是在体系结构设计时的网络集中化的前提。达成共识这个问题的复杂性的日益提高导致计算能力的成本增加。目前网络比较小，家用计算机的资源就足够。但是随着网络的发展，必要的设备成本也会不断增加。这就导致了为增加了添加区块以获得不间断奖励和稳定的投资回报和收益（增加矿池）的机会为目的的玩家团结。但是，这可能会使网络受到大型玩家的控制。

从原则上需要注意的是，网络的每个参与者都将为其工作获得奖励。酬金是为成功添加的区块支付的，通常由两个部分组成：区块中所含的交易总额的佣金（这里有些人意识到可以在交易中设置更高的佣金，以便矿工有动机将交易添加到他形成的区块中） ，以及固定的区块奖励（用于挖矿）。固定的区块奖励可能会随着时间的流逝而减少，例如，比特币减半的原理。

在 PZM Cash 中我们放弃了委托的股权证明，并应用了经过显著改进的“典型” PoS 算法。因此大多数用户都获得了参加网络并获得报酬的机会-这没有任何重大限制或任何重大障碍。

PZM Cash 的 POS 共识

PoS 共识算法意味着，参与者添加新区块的概率取决于其堆栈的大小-网络上其钱包余额上的货币数量。余额中货币越多，机会就越高。

要添加一个区块，还必须解决目标问题（类似于 PoW），但是，此问题的复杂性是针对每个用户单独计算的。钱包中货币越多，计算就越简单。

典型 POS 涉及所有货币在网络开放时（创世块的形成）在用户之间进行立即分配，以及使用交易费用作为对网络维护的奖励。在某些模型中添加区块的酬金额取决于货币的使用期限指标——货币的总数乘某一用户其存放时间的结果。因而可以激励把货币保存在钱包中，并保证其减少流通。

POS 也受制于中心化，但是购买货币比购买设备并安排挖矿（像在 POW 中一样）要容易得多，因此大量购买和拥有货币的人保证了限制垄断的内部机制。

股权证明算法的主要优势以及其创立的主要原因是防止“ 51％攻击”。要进行攻击，需要购买货币当前量的 51％。实际上，一个用户必须买下“股票控制额”，但这概率很低。此外，因为在“51％攻击”的情况下，大部分货币将位于攻击发起者的余额中，主要受害者必定是他本人。因此攻击不仅极其困难，而且完全没有意义。

POS PZM Cash 主要的公设：

1. 添加新区块的机会取决于账户中的货币数量（锻造余额）。
2. 货币的年龄完全不影响添加区块的奖励金额。
3. 锻造余额是用户拥有的货币：在一定时间段内在钱包中保持静态（货币未参与交易，包括未确认的交易）。
4. 佣金为交易金额的 0.5％，并且是固定的。添加区块的参与者将得到区块中所有交易总额的 0.5％。
5. 不提供其他锻造酬金。

添加区块的程序

添加区块的程序与网络主要程序（实行交易）相关联，并且始于客户端。为了描述 PZM Cash 的操作，我们必须明确地限制用户部分和内核的程序。交易与内核完全无关——它们是在客户端发起的。

用户使用私钥进入自己的钱包，并决定进行交易后再创建交易。为此：

1. 他要指出其参数：金额、收款人的公钥（地址）等。必须在钱包中正确填写所有参数后才能创建交易。PZM Cash 收款人或者合同的公钥（地址）是必填的。
2. 交易的申请则形成。连接加密货币网络的软件会通知网络上有进行交易的意图。最容易的方案是使用 PZM Cash Wallet 的轻型加密货币钱包。
3. 加密货币网络中的活跃节点（网络节点）会仔细检查区块链的记录，并确保用户的余额中确实有他打算发送的货币。
4. 在确认交易的可能性之后，该交易由私钥签名并发送到等待分配给区块链的未分配交易池中。锻工就是从该池中将交易收集到他们试图添加的区块中。
5. 然后交易进入区块。随后，也将再次检查网络上的节点。确认后，交易无法取消或更改，只能发起新的交易。

此外，该交易应记录在区块链的内核上，其中还包括共识算法。内核不对单个交易进行操作，而是对交易仅作为记录之一的区块进行操作，因此这些区块是共识算法的产物。区块确定列入交易日志的交易顺序以及“过账”的顺序。

下一步是确定谁将构成分布式总账中的下一个区块。

谁有添加区块的权力？

如前所述，区块链的本地副本存储在 PZM Cash 网络的每个节点中。在账号中至少有一次输入交易被确认了 1440 次的条件下，每个没有因公开私钥而被冻结的帐户都能生成区块。符合这些条件的任何帐号都有锻造的权利。

区块生成器如何选择？

为了参与锻造区块，准许的帐号使用其公钥对之前生成的区块进行签名。然后使用 SHA256 哈希函数对签名进行哈希处理。

PZM Cash 共识算法的唯一性与计算机制有关，与工作量证明算法也有一点相似之处。

在工作量证明中（POW）所有矿工都参与一种竞争，以查找所需类型的哈希（哈希记录开头带有一定数量的零）。只能通过暴力破解来获得所需值。同时，随着所需记录的开头的零的数目逐渐增加，需要破解方案的数量以及在所需时间添加区块的所需功率也增加。

在 PZM Cash 中搜索所需的哈希有类似的方式，但是随着符合条件的值的数量逐渐增加，计算不会变得更加复杂，而是会随着时间的推移而简化。正是计算下一个区块哈希值的复杂程度确定区块生成的概率：计算越复杂，概率就越低。而且，对每个特定锻工的复杂程度是不同的。

基本规则是第一个得到指定阈以下的哈希值的生成器获得形成区块的权力。随着阈值的提高，从而保证添加区块所需的速度（以确保网络的操作速度），因为未知哈希值的“允许误差”更高，正确结果的数量也更大。

在股权证明中拥有更大钱包堆栈（货币余额）的参与者形成区块的机会更多。钱包中的货币越多，“个人阈”和添加区块的机会就越高。在 PZM Cash 中核算该 1440 区块的账户中保持静态的减去未确认交易中涉及的货币的钱包余额（货币）。每个节点访问钱包以查询余额并计算阈值的提高程度。

最终，比别人能早获得所需的哈希值（在对他指定的阈以下）的锻工有权形成区块并将其添加到区块链中。交易从未分配交易池中收集到区块中（一个区块的交易最大数量为 255）。在区块中记录从交易池中到达的交易，并输入其他数据（例如，哈希），等等。交易总数受区块大小的限制。形成的区块发送到节点以进行确认其正确性的验证。区块经过十次确认后，交易才被认定是安全的。正确添加该区块后，其中包含的所有交易被认定是已确认（即完成），货币即被重新分配（包括支付佣金）。已确认的交易将永久记录在区块链中，因此无法更正或更改。

锻造

“锻造”术语与工作量证明所特有的“挖矿”术语相对立使用。这意味着要使用最小的计算能力来达成共识（与工作量证明相反）。

PZM Cash 锻造的独特之处在于，不会向网络中添加任何新货币，因为对锻造没有任何奖励会导致网络中额外的流动性。唯一可以预见的对锻造的支付是，落入区块中的交易的费用为 PZM Cash 货币总量的 0.5%。

区块创建成功后，交易费用将奖励给该帐号。随着网络的扩展，其内部的交易数量相应增加，以锻造形式获得的收入也将增加。

网络参数

为了对 PZM Cash 网络的状态进行交互式显示和可合理的监控，该网站上实施了一个 PZM Cash Explorer 交互式分析表，每个参与者都可以在其中查看当前的网络性能、货币流通和交易费用金额。

新区块产生的平均时间为 60 秒。此逻辑与交易数量无关，但是一个区块内可包含最大交易数量的限制为 255。在最大网络性能的条件下（每区块中有最大交易数量），PZM Cash 可以每天确认的交易达到 367200 个（1440 区块/天）。

安全

- 基于 Merkle-Damagard 构造建立久经考验的 SHA256 加密哈希算法 。
- 要进行“ 51％攻击”（消除交易或更改交易顺序的动机），攻击者需要控制所有 PZM Cash 货币的 51％，即对锻工进行控制或贿赂、唆使，但是随着网络的发展，这种概率越来越低。
- 攻击者可以通过重新分配，即大量货币转移到一个帐户中，来试图增高锻造的可能性。为了避免此类行为，引入了在一天之内 1440 区块的账户中的 PZM Cash 保持静态的规则。正是余额中的这些货币决定了锻造的可能性。如果发动此类攻击，攻击者将一天之内完全无法锻造，这预示他将蒙受巨大的损失。

4. 发展模式

我们的战略目标是生态系统的快速增长。这是很重要的，因为：

1. 新项目的出现通过添加新的产品和服务为消费者创造额外的价值。
2. 需求的增加导致供应的平衡，而流通量的增加则有助于 PZM Cash 相对于外部环境的稳定性（稳定性和汇率升值）。

为了成功发展，有必要提供一种合理的流动性网络汇兑算法（发行 PZM Cash 硬币），以及网络的扩展渠道。

PZM Cash 公共生态系统的参与者可以是：

- 私人项目；
- 个人用户；
- 项目和应用程序的开发者和创建者；
- 资金和投资提供者（风险投资、天使投资人、加速器、孵化器）；
- 公共和政府的机构；
- 协会、联盟和联合会；
- 其他参与者。

参与生态系统具有一系列竞争优势：

- 访问不断增长的有支付能力的客户群，因此可以扩大业务规模并增加利润；
- 获得许多技术解决方案并实现业务流程自动化：相互结算系统、智能合约系统、形成公司的经营历程、跟踪交易对手的声誉、打击伪造等等。
- 可以建立合作伙伴关系和价值链；
- 随着周围环境的发展，提高企业声誉和地位；
- 可以得到融资以及受到风险基金和其他融资来源的关注；
- 加入网络后可以进入国际市场。

网络的金融流通性

显然，供求关系影响商品和服务的价格。而正是货币的供求影响了其汇率。任何加密货币的关键问题是其相对法定货币和其他加密货币的汇率稳定性问题。为了稳定的汇率，必须保证根据流动性兑换算法在生态系统中形成的 PZM Cash 货币的足够供应量。以及因参与者可用服务和用例数量的增加而保证充足的需求。

对 PZM Cash 的需求将增长的原因如下：

- 整合将使用 PZM Cash 作为支付单位的合作伙伴；
- 开发 Dapps 和 Apps 应用程序（网络扩展服务）。

另一方面，我们必须提供正确的流动性网络汇兑机制（发行 PZM Cash 货币）。生态系统流动性（PZMCash 货币）的保障将分两个阶段：

- PZM Cash 初始供应（在预挖矿阶段）；
- PZM Cash 流动性扩展 （在 PoS 挖矿阶段）。

初始供应是指在第一区块生成时在预销售（预挖矿）期间分配的 PZM Cash 货币。初始供应是网络上线之始所需的 PZM Cash 的量，即启动系统的初始流动性。在此阶段任何加入网络的参与者都因早期进入而具有优势，可比别人早得到通过 PoS 挖矿提供额外流动性的权利。

网络开始运行（主网上线）后，将启动扩大流动性的过程——PoS 挖矿。PZM Cash 生态系统中的流动性将由于网络参与者获取其参与的收入而增加。

PoS 挖矿是 PZM Cash 额外发行的唯一机制，且并未提供其他机制。锻造作为通过提供网络维护服务来获取货币的一种方式，不会产生额外的流动性，表现为将货币从交易参与者重新分配给其注册的参与者的流程。重新分配流程不会导致系统中 PZM Cash 总数的增加和网络中流动性的增长。与其相关的有：

- 交易手续费（fee）；
- 与智能合约有关的款项；
- 其他业务的费用；
- 兑换业务（PZM Cash ——加密货币，PZM Cash ——法定货币）。

预挖矿

- 初始发行量为 9000 万 PZM Cash （或 90 亿 PZM Cash 最终流动资金总额的 1%）。
- 货币分配将实施如下方式：
  - 0.7%（6300 万 PZMC）公开销售分配；
  - 0.1%（900 万 PZMC）分配给 PZM Cash 项目团队，提现冻结期限为 1 年；
  - 0.2%（1800 万 PZMC）在区块链发布后三年内用于营销活动。
- 货币在网络启动时（在网络中第一原始区块生成时）将发行并分配（发送到地址）。
- 最初发行的货币将分散在大量参与者之中，他们将构成最初的用户群。
- 根据 PoS 逻辑，最初用户将获得早期进入优势，因此他们能够比其他用户提早开始锻造。

PoS 挖矿

Pos 挖矿是网络流动性增长的唯一机制，也是 PZM Cash 忠实用户货币余额增加的机制。它按参与者任意一个激活的钱包中的资金余额的累积率来加算 PZM Cash。其中，仅考虑有效的钱包余额，不包括未确认交易中包含的货币。

复利率以每月百分比表示，取决于两个参数：

1. 主活跃钱包的当前余额。
2. 支持钱包的当前总余额——该钱包是主钱包的所有者作为支持而添加的。

累积率不会随时间的变化而改变。为了避免危险的网络中心化，一个钱包的最大余额可以为 1000000 PZM Cash（或 90 亿 PZM Cash 最终流动资金额的 0.011%）。达到该余额值后，该钱包无法进行 PoS 挖矿。

如何添加支持钱包

如前所述，钱包通过使用公钥对该钱包进行输入交易来激活。重要的是该交易来自哪里——发款人应为主钱包，因为它把新用户引入网络中。因此，通过他交易激活的钱包成为他的支持钱包。此外，新激活的钱包有主钱包的权限； 因此，每个主钱包都有一个支持钱包独特的结构。

钱包激活后，就可以进行 PoS 挖矿。为此，主钱包在输入交易中必须传入至少 1 PZM Cash。

如何计算钱包货币余额的增长率

钱包中的余额增长率是通常的累积率，以简单的百分比表示，是基于两因素计算的。累积率是货币余额增加的基本利率，并取决于钱包的当前余额。倍增器取决于每个具体主钱包的支持钱包中的货币量。两个值越高，货币总数越大。支持钱包关联在深度最多为 2 级的结构中。

加算是根据通过累积率乘以倍增器得出的利率进行的。参与者的货币余额的最大增长率为每月 21%，最小的为每月 1.2%或每年 14.4%。

表 1

“计算货币增长率的指标”

主钱包的余额	月利率	支持钱包的余额	倍增器	范围（最小和最大值）%/月
最高持有人		成熟的网络		
700000 至 1000000	6.89%	超过 100000000	3.14	21%
500000 至 699999	5.35%	30000000 至 99999999	3.0	
300000 至 499999	4.14%	10000000 至 29999999	2.9	
普通持有人		发达的网络		
200000 至 299999	3.69%	5000000 至 9999999	2.7	
100000 至 199999	3.15%	1000000 至 4999999	2.5	
50000 至 99999	2.63%	500000 至 999999	2.3	
20000 至 49999	2.11%	200000 至 499999	2.1	
少数股东		初始网络		
10000 至 19999	1.70%	100000 至 199999	1.7	
5000 至 9999	1.61%	50000 至 99999	1.6	
2000 至 4999	1.52%	20000 至 49999	1.5	
1000 至 1999	1.43%	10000 至 19999	1.4	
500 至 999	1.37%	5000 至 9999	1.3	
100 至 499	1.28%	1000 至 4999	1.7	
1 至 100	1.20%	少于 1000	1.16	
		0	0	1.20%

什么时候加算额外的货币

确认钱包任意的输出交易（当前余额的变化）后，就加算累积的货币。此时，将对支持钱包的余额进行“印痕”。（未分配交易池中的货币除外，也就是说，它们正在等待发送）。因此，来自帐户的输出交易越多，支付的次数就越多。另一方面，将货币保留在钱包中并根据复利计划收取附加费用也是有经济意义的。

5. 网络的扩展

如前所述，PZM Cash 的主要特性是其对开发人员和合作伙伴的货币供应和服务产品的快速可扩展性的定位。PZM Cash 的基础设施可以朝几个方向发展和扩大。

1. 创建 Dapps

这样任何开发者可以扩编自己的去中心化应用程序。这样就可以给开发者分配在分布式总账上记录的自己的侧链。并且，该应用程序的每个用户将拥有自己的钱包。

2. 协议导出

PZM Cash 源代码是公开的。任何开发者都可以在自己的项目把 PZM Cash 协议作为核心。为此需要部署并启动完整的节点（网络节点），安装并同步特殊的 API 模块。

3. 合伙人持有货币

PZM Cash 货币可以用作合作项目和平台上的支付工具。PZM Cash Wallet 所使用的 Web 3js 技术允许在合作平台上（兑换处、交易所、等等）用钱包进行结算。

6. 路线图

2020年第二季度

- PZM Cash 公开销售
- PZM Cash 主网和在线钱包发布
- 在CoinMarketCap上市

2020年第三季度

- 安卓/iOS钱包发布
- Web3js 发布
- 创建连锁兑换点
- 进入亚洲市场
- 积极吸引应用程序和服务的开发者

2020年第四季度

- 创造智能合约
- 进入拉美市场

2021年第一季度

- 创建自动柜员机连锁点并发行借记卡
- 开设PZM Cash Foundation技术枢纽

2021年第二季度

- 举行第一届PZM Cash Summit国际会议

2021 年第三季度

- 为了扩展支付方式引入新的合作伙伴和服务

7. 注意！关于声明

本文档所包含的所有在通讯稿中或在任何公众可以访问到的地方作出申明，以及 PZM CASH 或代表 PZM CASH 的董事，高级管理人员或雇员（视情况而定）所作出的无关历史事实的口头申明，均属于“愿景声明”。 其中一些声明可以使用预测性术语来定义，例如“目的”、“预期”、“相信”、“评估”、“期望”、“如果”、“打算”、“可能”、“计划”、“可能”、“有可能性”、“项目”、“应该”、“将要” 或其他类似术语。但是，这些并不是确定预测声明的唯一方式。关于 PZM CASH 的财务状况、业务战略、计划和前途、以及 PZM CASH 所处行业的未来前景等所有的声明都是预测声明。这些预测声明包括但不限于关于 PZM CASH 的收入和盈利能力、前景、未来计划、其他预期的行业趋势以及其他在本文档中讨论到的跟 PZM CASH 相关的问题的声明不属于历史事实，而仅是预测。

这些预测声明包括已知和未知的风险、不确定性和其他可能导致 PZM CASH 的实际未来结果或成就与预期，明示或暗示的任何未来结果或成就存在重大差异的因素。

这些因素包括但不限于：

a）证券市场或加密货币市场的政治、社会、经济和市场状况以及 PZM CASH 运营所在国家的监管环境的变化；

b）PZM CASH 可能无法进行或实施其相关未来业务战略和计划的风险；

c）法定货币和加密货币的利率和汇率变化；

d）PZM CASH 预期增长和预期内部增长战略的变化；

e）存在和支付给 PZM CASH 的与其运营有关的费用变化；

f）PZM CASH 为企业的相关管理和运营所必须的职员的数量和其工资的变化；

g）PZM CASH 客户偏好的改变；

h）PZM CASH 运营的竞争条件的变化，以及 PZM CASH 在这种条件下的竞争力；

i）PZM CASH 未来资本需求以及为满足这样需求而提供资本的可能性的变化；

j）战争或国际或国内恐怖主义行为；

k）影响 PZM CASH 业务和/或运营的灾难性事故和自然灾害；

l）其他与 PZM CASH 无关的因素；

m）与 PZM CASH 及其企业和运营，XXX 代币，PZM CASH 代币和 PZM CASH 钱包的初始销售（均在白皮书中列出）相关的任何风险和不确定性。

所有 PZM CASH 或与代表 PZM CASH 的人员所作出的或与之相关的预测声明由这些因素直接确定。鉴于风险和不确定性可能导致 PZM CASH 的实际未来结果或成就与在本白皮书预测声明中预期、明示或暗示的未来结果或成就发生重大差异，不应过分依赖这些声明。这些预测声明仅自本白皮书发布之日起适用。

PZM CASH 或任何其他人不声明，不能保障和/或保证 PZM CASH 的未来实际结果或成就将与这些预测声明中所讨论的一样。PZM CASH 的实际结果或成就可能与这些预测声明中预期有重大差异。