技术白皮书 V1.0

2018年12月6日

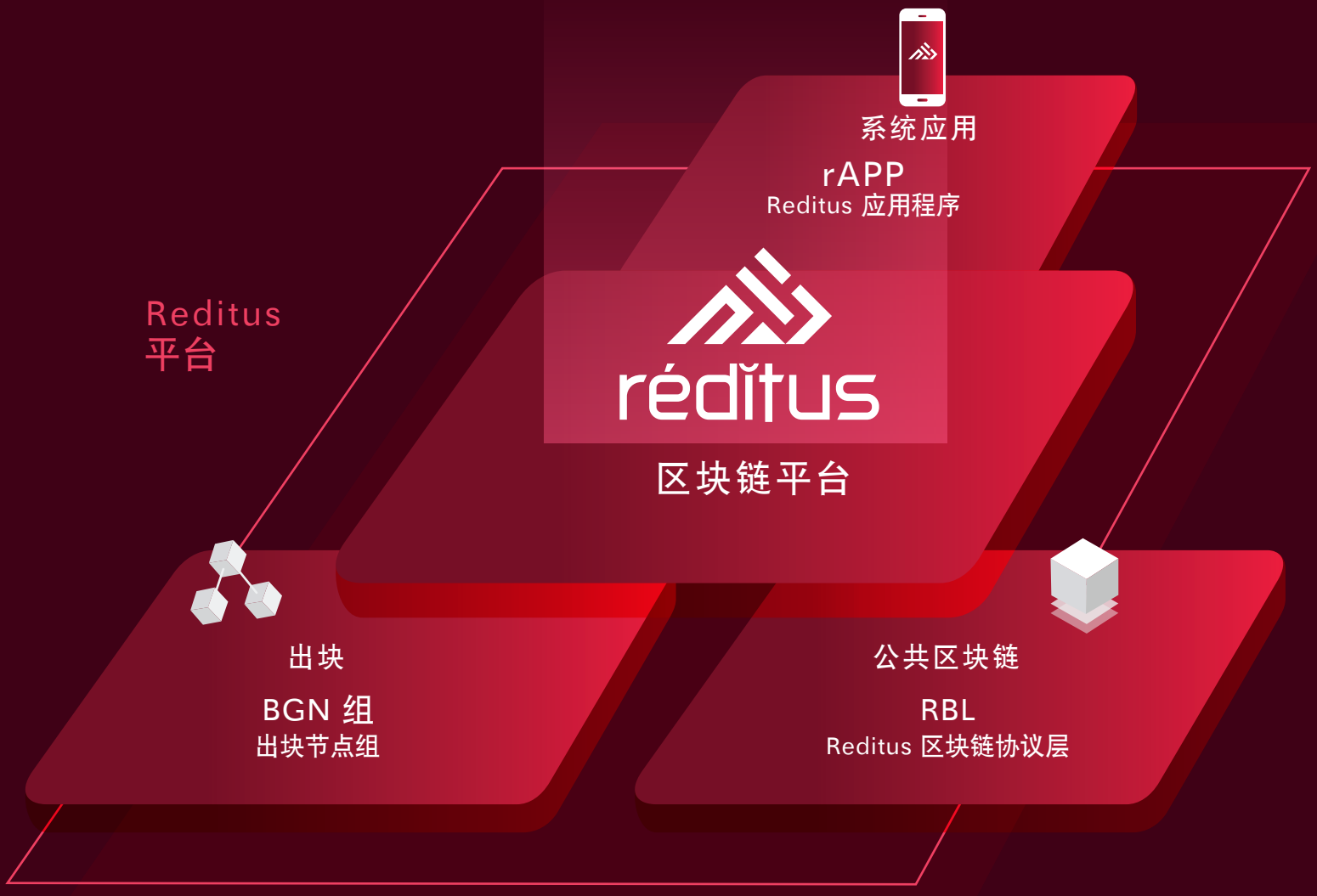
内容

1. 技术

1.1. 平台介绍

Reditus®平台结合了“区块链、区块链网络中使用的协议及通过其运行的应用程序平台”，以下是RMS处理的任务，首个Reditus应用程序(rAPP)与Reditus®平台:

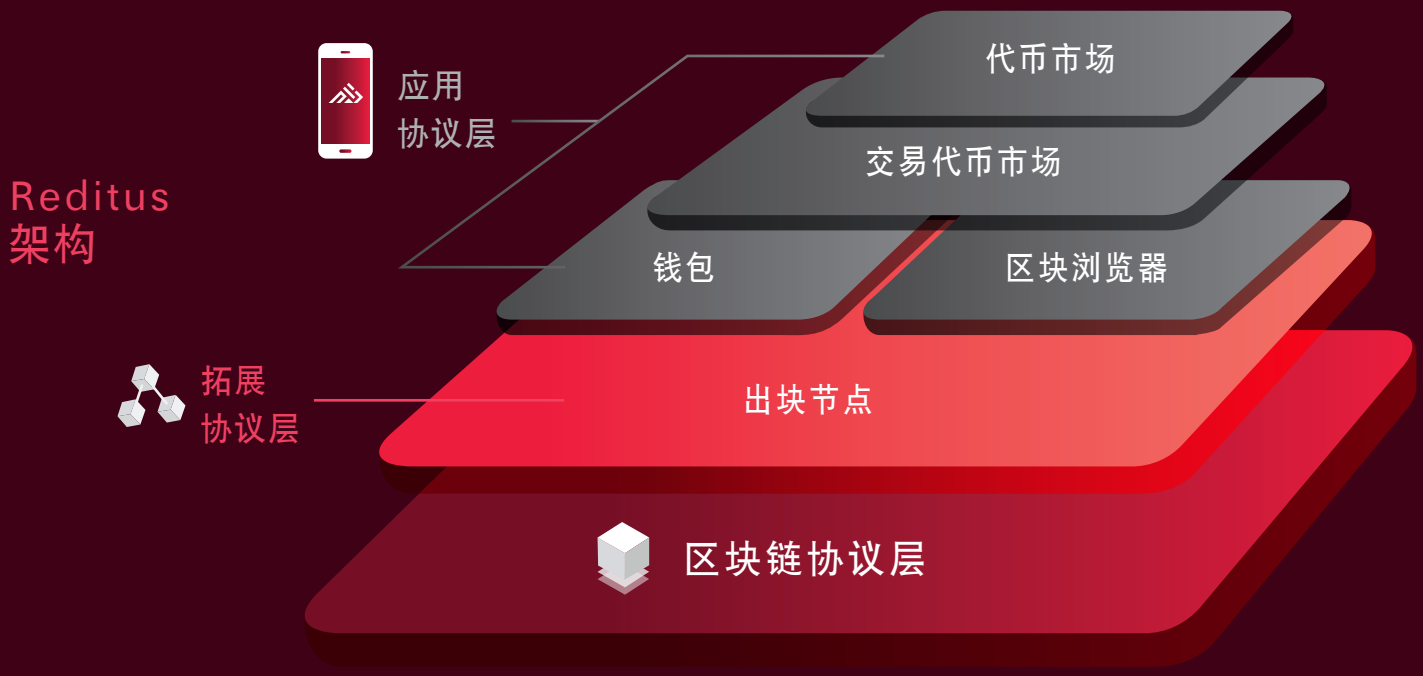
- 应收账款代币化及已代币化的应收账款的交易(Reditus®RED代币)
- 追收状态管理及登记应收账款信息
- Reditus®RED代币与Reditus®IT代币的交易，以及交易费用的征收和结算



1. 技术

1.2. 平台架构

具有分层Reditus®架构层，如下所示:



区块链协议层

区块链协议层是个数据层，Reditus®下的所有数据都记录在分布式分类账中。 所有区块都通过哈希算法连接。区块链协议层确保数据的完整性。

拓展层

拓展层具有区块创建权限的出块节点，可用于区块链的一般可用性及应用程序的有效操作。协议层就有关区块的创建验证整个节点，代币合同的验证与分发，以及代币的发布和销毁，并确保交易的一致性。

应用层

Reditus®应用程序在区块链协议层与拓展层之上运行，主要应用如下:

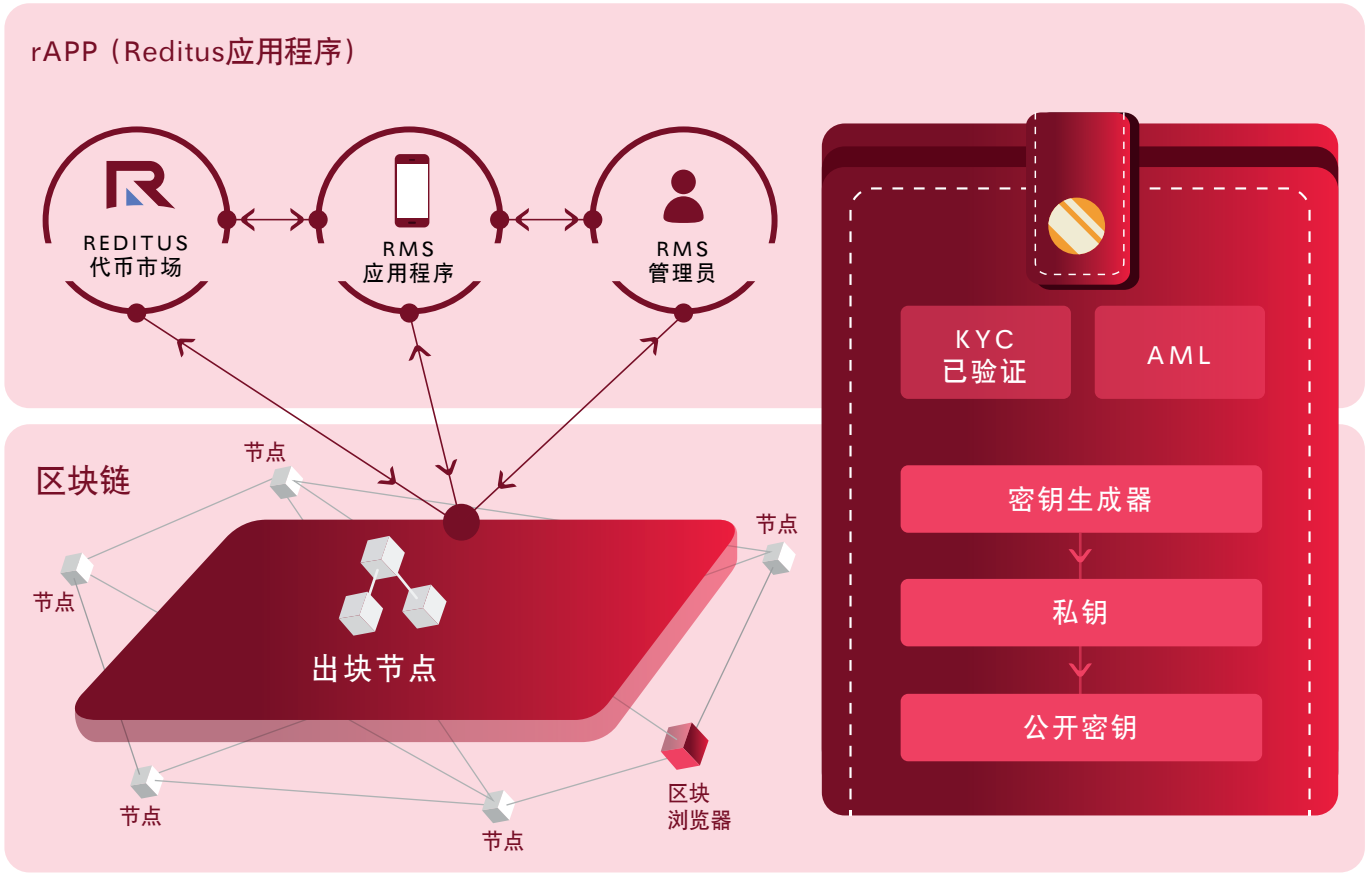
- 钱包 – 存储和传送加密货币的电子钱包
- 区块浏览器 – 是一个浏览器，使阁下可以搜索及检查区块链的历史记录
- RMS – 用于对应收账款进行代币化、管理和运营的系统
- 代币市场 – 由RMS产生的交易代币市场

REDITUS平台结构

在Reditus®架构层中，平台架构负责每个应用程序的操作，以及BGN(出块节点)的数据验证。

1. 技术

Reditus 平台结构



钱包是区块链和应用程序交互操作的中介

BGN可以验证，并同意从应用程序收集的KYC和AML数据

Reditus区块链共识架构可以通过BG节点验证创建区块、发放代币和代币，其中PoV(证明值)用作验证算法。PoV识别并验证网络的功绩(价值)或资产价值，以便创建全新区块或发行代币。

在RMS中，Reditus应用程序，资产的PoV用于BG节点在存入时（即是信托账户）验证已收回的应收账款。

1. 技术

1.3. 平台范围（技术规格）

区块链

区域链协议层内(顶部)的BG节点(出块节点)运行并控制网络上方的Reditus应用程序。

验证算法

Reditus使用PoV(价值证明)作为验证算法，BG节点证明了网络贡献和实际(经济)价值。

代币合约

Reditus代币合同是Reditus应用程序的合同记录，用于通过BG节点验证向区块链添加新块，并通过此问题分发代币。

代币化

Reditus代币是一种交易手段，当代币合约发行的各种权利和利益被标准化时产生。通过RMS发行，代币Reditus应用程序是应收账款的抵押，其最高价值是分开的。

哈希算法

Reditus区块链使用<SHA-256>哈希算法来加密数据与区块之间的连接。

电子钱包地址结构

REDITUS平台采用的签名与签名验证算法是ECDSA（椭圆曲线数字签名算法）。
以下描述如何生成电子钱包地址(公开密钥):

- 公开密钥是使用256位私钥与ECC(椭圆曲线密码)算法函数生成的。
- 使用SHA256与RIPEMD160将公开密钥转换为160位(20字节)的哈希值。
- 已转换的20字节公开密钥与4字节校验和被组合在一起创建出字符串(24字节)。
  然后将此字符串转换为十六进制数字，并在48位数字符串之前添加“0r”。
  50字节的地址值用作最终的电子钱包地址。
- * 函数示例 – concat(“0r”, hex(concat (哈希值20 bytes, 校验和4 bytes)))
  Ex) 0r3ae893ae4b22d70432899a3471230face41fe912

1. 技术

节点

监控节点

监控节点用于认证及管理BG 节点，并验证参与者的节点。它是已安装的节点，可执行所有功能，例如区块的创建和传送，以及代币合同的注册和分配。

BG节点

BG节点可分发与执行Reditus应用程序界面和代币联系人以发行代币。这是执行PoV(价值证明)的核心节点。

普通特权节点

普通特权节点可以查询区块链事务的详细信息，传送代币及传播区块。它是一般参与者和合作伙伴的节点，其应用程序包括区块浏览器。

认证机构

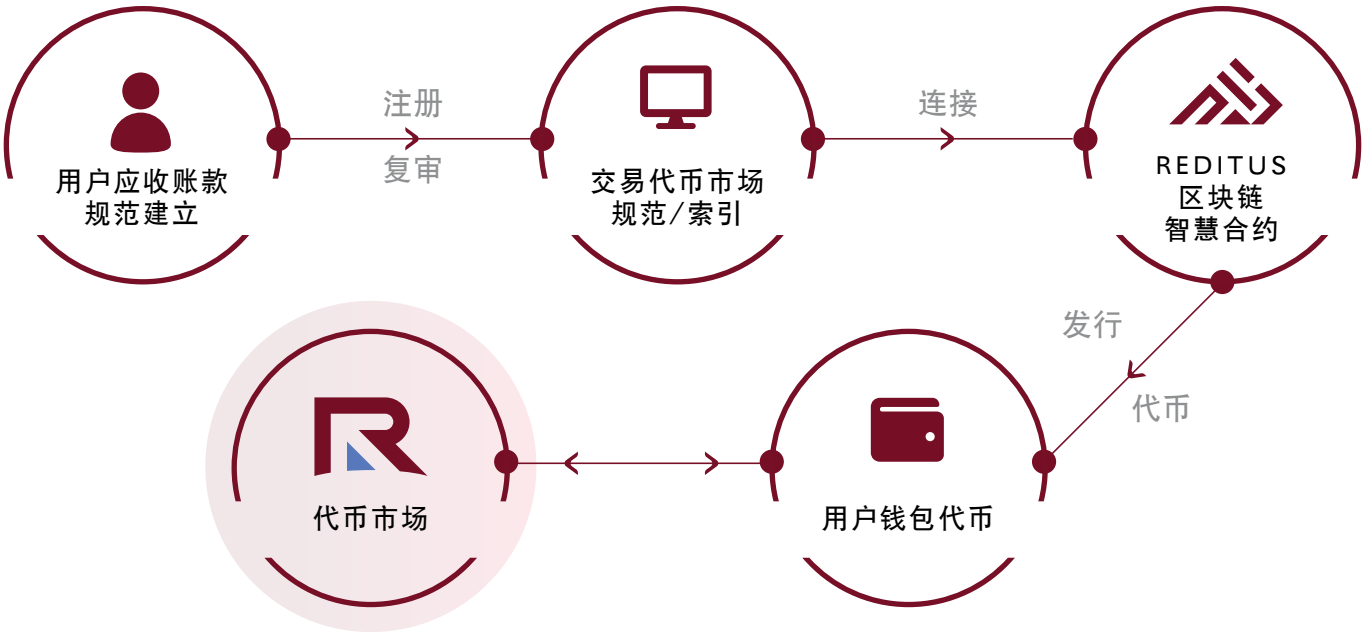
对于节点间验证，密钥交换和验证系统使用<RSA2048>方法操作。对于电子签名，无需单独的证书颁发机构。

签署交易

所有交易的电子签名都采用ECDSA(椭圆曲线数字签名算法，这是一种公共密码技术)。

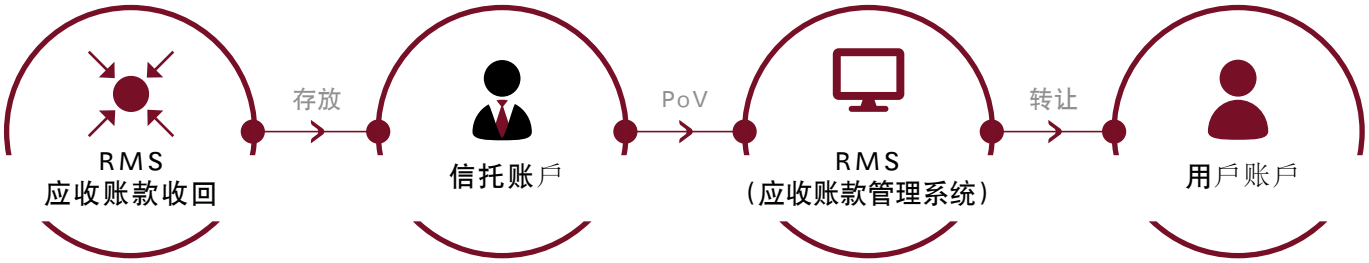
2. REDITUS® RMS
（应收账款管理系统）

Reditus®RMS是个管理应收账款的系统，具有各种形式及权利结构，代币基于应收账款的权利，以及权利的利害关系。包括用于注册债权人的债权人应用程序，以及用于管理应收账款的创建、传送、追收和代币化的一系列流程的RMS管理工具。



这允许通过行使应收账款权利而进入的实际资产纳入代币经济。

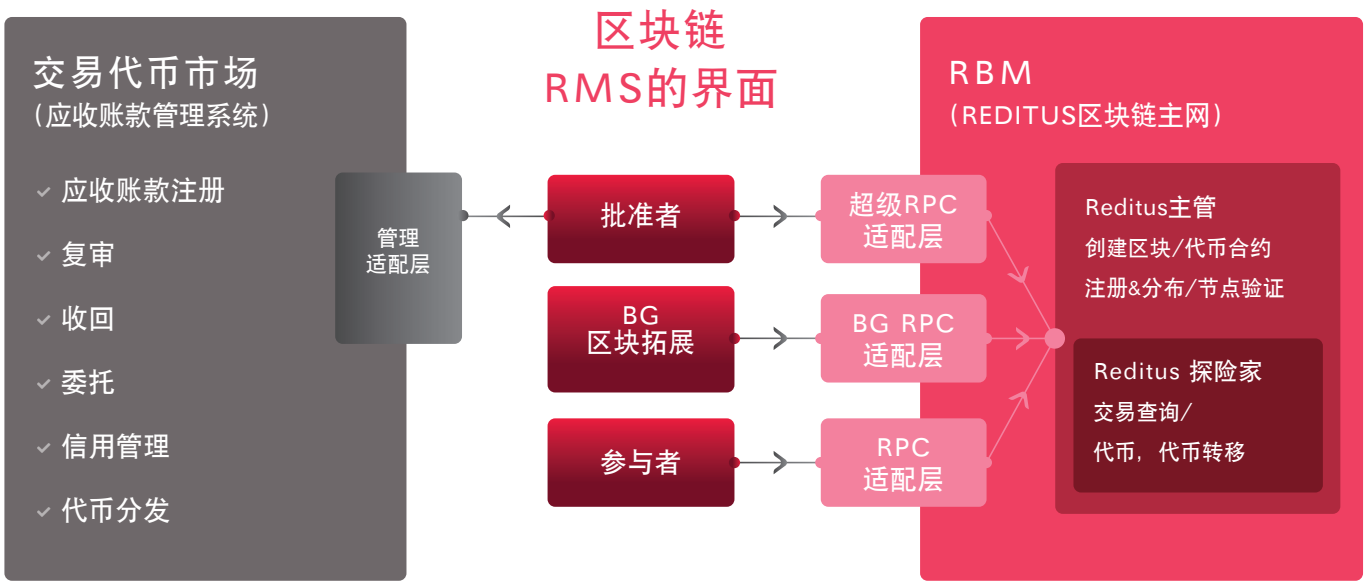
运营RMS的实体(公司)在委托及转让应收账款时收到代币，作为应收账款追收活动的奖励。



2. REDITUS® RMS
（应收账款管理系统）

在RMS中恢复的价值（金融资产）应根据RED代币的数量分配给RED代币持有者。

RMS（Reditus®应用程序）的区块链接口与影响接口的节点如下:



批准者

批准者在每个应收账款创建时验证应收账款以验证代币生成。

出块（节点）

出块（节点）每分钟创建一块区块，区块内容达到共识，并进行验证。

参与者

参与者可以查看Reditus®区块链。