说 明 书

一种基于分布式账本技术的去中心化自治银行构建方法

技术领域

本发明涉及分布式账本技术、数字金钱领域，具体地应用于实现基于分布式账本技术的去中心化自治银行的构建。

背景技术

分布式账本技术（Distributed Ledger Technology）是在一个对等网络上能够同步、验证、存储记录的账本技术。历经数年的发展，分布式账本技术从第一代仅能够自定义简单脚本发展到第二代能够运行图灵完备的智能合约程序。因其与互联网金融领域联系密切，一直是技术研究的热点。

数字金钱（Digital Money）是指依托分布式账本技术，由分布式账本软件定义和发行的数字货币（Digital Currency）或者数字资产（Digital Asset）。第一代分布式账本技术最早且最成功的实现是比特币（Bitcoin，BTC），基于其发行的数字货币是比特币。第二代分布式账本技术最为成功的例子是以太坊（Etheruem，ETH），基于其发行的数字货币是以太坊。此外，商业团体能够应用第二代分布式账本技术发行数字资产或代币。然而，值得注意的是，数字金钱目前没有法定的地位，其相关的法律条文尚不明确。

智能合约（Smart Contract）是指为了方便、验证或强制执行而将合同变成代码的形式并在约定的条件下自动执行的计算机协议。第二代分布式账本技术的出现为智能合约提供了运行的基础。通过智能合约，用户可以创建自己的账本，降低了用户使用分布式账本技术的门槛。通过这个账本，用户可以用于去中心化自治组织的管理，或发行其数字资产，将现实中的资产代币化，例如黄金代币。

但是，目前分布式账本技术仍未完善。一方面其没有解决数字货币发行的问题，数字货币的发行量不应该由个人或团体决定，而应由总的市场和经济决定。然而大多数数字货币总量是固定的，且集中在少数早期参与者手中，这将导致数字货币面临严重通货紧缩的问题，并且数字货币早期的参与者获得暴利，这些对货币价格的稳定是极大的威胁。另一方面大多分布式账本技术是用户和地址解绑的，难以评价用户的信用，使得各种金融业务难以开展。

因此，需要一个能够吻合市场需求，能够自适应的发行数字货币以及对用户信用进行评价，同时对用户的贷款和存款的需求予以满足的系统。传统银行需要大量的风险评估和审计，增加了人力物力及时间上的成本，可仍然具有放贷坏账的可能。若是存在一种具备无需繁复操作的信用审批流程、保证信用安全、低风险等特性的的银行体系，必然将受大众追捧。这也是本专利——去中心化自治银行（Decentralized Autonomous Bank, DAB）提出的主要动力。

发明内容

鉴于上述内容，我们设计和发明了一种基于分布式账本技术的去中心化自治银行的构建方法。

在去中心化自治银行的系统中，存款用户通过存入储备金货币，获得存款代币（Deposit Token，DPT）和信用代币（Credit Token，CDT）。储备金货币被分到两个储备金池，一个是存款代币的储备金池，一个是信用代币的储备金池，分别保证存款代币和信用代币的价值，同时分别开展存款和贷款的业务。

本发明提供了一种基于分布式账本技术的吻合市场和经济的货币发行方法。

在该系统中，引入了动态调整存款代币储备金率（Cash Reserve Ratio，CRR）的机制，通过这个机制动态调整存款代币的价格以及存款代币的发行量和信用代币的授予量。同时，储备金率将会把用户存入的储备金货币划分到两个储备金池里。在货币的发行过程中通过收取一定比例的铸币税，集中一定比例的存款代币和信用代币，进而利用这些代币进行宏观调控，维系系统的稳定运行。并且，采用动态调整储备金率

和征收铸币税的方法后，系统能够将铸币的利益分散到早期和后期参与者，避免了早期投资者的暴利，保障了存款代币汇率的稳定。

本发明还提供了一种基于分布式账本技术的用户信用评价方法。

在系统中，引入了一个储备金率大于 1 的信用代币储备金池，通过这个储备金池对信用代币价值的保证，开展贷款的业务。保证信用代币价值的方法有：将信用代币按照其汇率换取储备金货币，或者使用信用代币获得贷款。由于储备金率大于 1，直接按照汇率换取储备金货币是一种不明智的选择，系统鼓励用户正常进行贷款。用户遵守信用，支付利息并偿还本金，将获得原本的信用代币和新发行的信用代币。新发行的信用代币按照其支付的利息计算。另外，拥有信用代币的用户可以进一步授信。但信用代币的总量不变，这样让人与人之间形成信用的授权网络。这个过程实现了信用在社会网络中流通，而传统意义上的信用是某个人或组织的固定属性，不具有流通性。当信用成为像货币一样具有流通的性质后，就会形成信用的市场，进而保证信用的价值。信用的价值还在于信用贷币的在传统金融行业中的作用。在与传统金融行业实现有效对接之后，信用代币将是获得基于分布式账本技术的金融业务的必要条件，这些行业会根据用户信用代币的多少作为其风险和信用评估的参考，以提高行业运行效率。

本发明还提供了一种基于分布式账本技术的去中心化自治组织的管理方法。

在系统中，引入了一个没有具体实体的去中心化自治组织（Decentralized Autonomous Organization）的智能合约。这个组织是本发明中设计的去中心化自治银行的所有者。用户通过持有存款代币参与组织的管理和决策，其权利由其持有的存款代币的数量决定。用户可以花费一定数量的存款代币向去中心化自治组织注册一项提议，号召其他用户支持该项提议，如果这项提议获得了一定比例要求的存款代币的支持，那么就可以执行这项提议。用户不能够重复参与投票，其所投的票会被临时冻结，直至提议结束。

本发明，可以在分布式账本技术上实现自适应的发行数字货币和对用户信用进行考评，同时对用户的贷款和存款的需求予以满足，还实现了其去中心化自治的管理。

本发明的具体内容将在随后的说明书中阐述。本发明的目的和其优点可通过在所写的说明书、权利要求书、以及附图中所指出的来实现和获得。

附图说明

附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

图 1 是根据本发明采用的基于分布式账本技术的自适应的货币发行方法；以及

图 2 是根据本发明得到的基于分布式账本技术的货币发展的两个阶段；以及

图 3 是根据本发明得到的基于分布式账本技术的具体系统实现的架构图。

具体实施方式

以下结合附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

在本发明实施例中提供了一种基于分布式账本技术的去中心化自治银行的构建方法。其利用动态变化的存款储备金率自适应地控制存款代币的发行和信用代币的授予，调节存款代币储备金池和信用代币储备金池的大小。在本发明中，存款储备金池和信用储备金池，共同保障存款代币和信用代币的价值。接下来，将分别通过实施例来对此加以描述。

本发明中所涉及的分布式账本技术是第二代分布式账本技术的最成功的实现——以太坊，本发明在以太坊的智能合约的基础上实现了本发明所描述的功能，作为实施例。

在本发明的实施例中提供了一种基于分布式账本技术的去中心化自治银行的构建方法。详细说明如下：

去中心化自治银行主要通过存款代币（DPT, Deposit Token）、信用代币（CDT, Credit Token）、次信代币（SCT, Sub-Credit Token）和失信代币（DCT, Discredit

Token）四种代币和一个主要的智能合约来实现。其中信用代币、次信代币和失信代币统称为广义的信用代币（Generalized Credit Token）。其中主合约也相应包含了存款和信用两个分合约的功能。下面详细介绍四种代币。

存款代币（DPT）：是符合 ERC20 标准的代币，是存款的单位，可以流通。

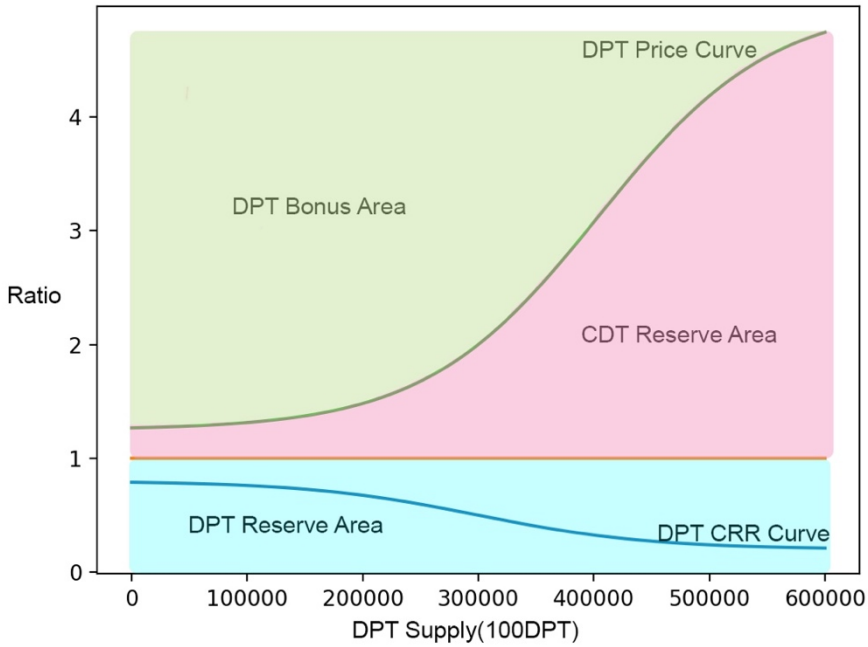
信用代币（CDT）：是符合 ERC20 标准的代币，是衡量用户贷款额度和信用度的单位，能从信用合约里面换取储备金货币，可以流通，且没有手续费。

次信代币（SCT）：是符合 ERC20 标准的代币，是在使用信用代币贷款后，信用合约将信用代币转为了次信代币。不可以流通，但是需要在一段的时间期限内通过还款将次信代币转变为信用代币，如不能还款，则需要在这个期限内通过合约将其转变为失信代币，进入可流通状态，否则将在此期限后被销毁。

失信代币（DCT）：是符合 ERC20 标准的代币，是在用户不足以或不愿意还款的情况下将次信代币转化为的失信代币。不能提现，但可以流通，流通具有一定的手续费，这部分手续费直接销毁。

存款合约：存放存款用户存款储备金的合约。能够根据合约外的存款代币流通量自动调节存款合约的储备金率，并计算相应存款代币的价格。

信用合约：是存放信用代币储备金的合约。能够保证信用代币的价值。信用代币的价格根据储备金量，储备金率和当前流通的信用代币数量（包括信用代币，次信代币和失信代币），计算信用代币的价格。并能够开放对信用代币的提现。



图一 基于分布式账本技术的自适应的货币发行方法

$$CRR(DPT,\ x)=a*1/(1+e^{((x-1)/d)})+b \quad (0<b<a<1) \tag{1}$$

$$IP=1/100 \tag{2}$$

$$IP(DPT)=1/CRR(DPT,\ x)*\ IP \tag{3}$$

$$Issue(DPT)=\ 1/IP(DPT) \tag{4}$$

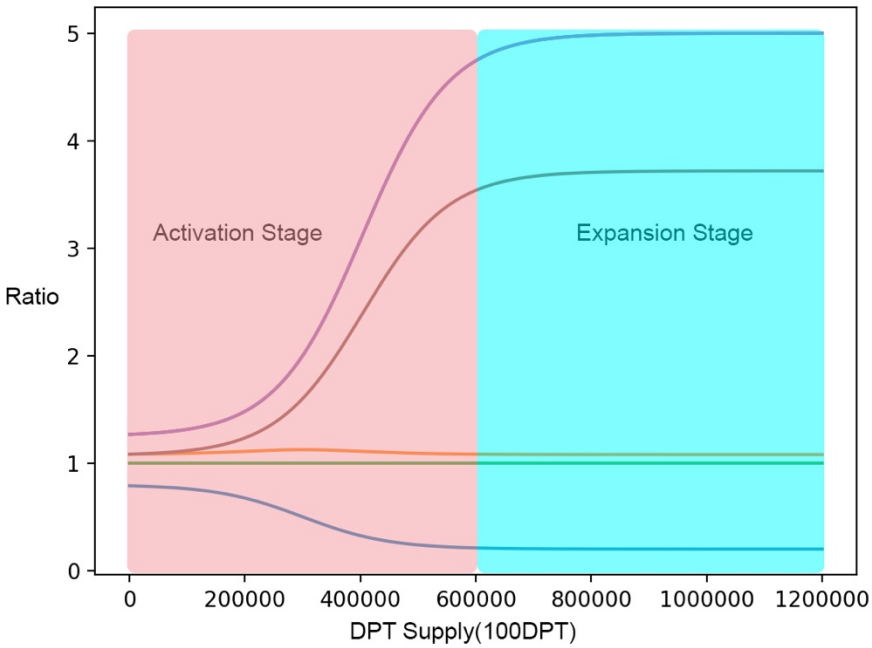
$$WP(DPT)=Reserve(DPT)/(Supply(DPT)*\ CRR(DPT,\ x))\ *IP(DPT) \tag{5}$$

$$CRR(CDT)=3 \tag{6}$$

$$IP(CDT)=2*IP(DPT) \tag{7}$$

$$Issue(CDT)=(1-CRR(DPT,\ x))/\ IP(CDT) \tag{8}$$

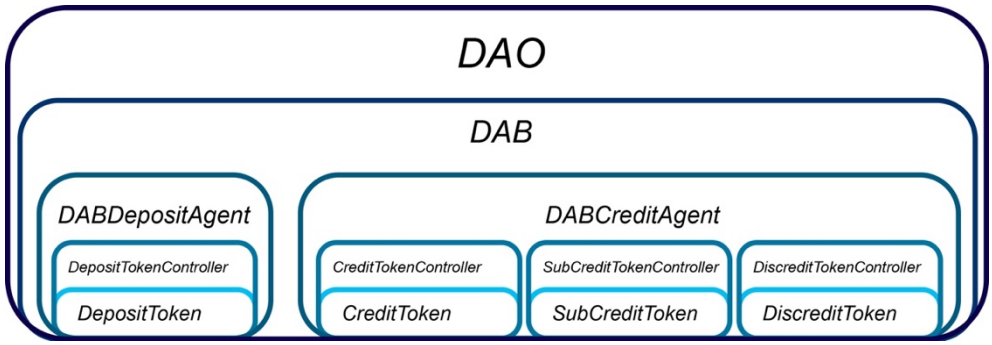
如图一所示，蓝色曲线为存款合约储备金率和存款代币流通量的函数关系，其中 a, b, l, d 是调节储备金率的曲线位置和形状的参数（公式 1）；绿色曲线为存款代币的发行价格 （Issue Price of DPT，IP）和存款代币发行量的函数关系（公式 3），发行相应数量的存款代币（公式 4）；蓝色区域是存款代币储备金池；红色区域是信用代币储备金池；绿色部分是存款代币的早期参与者获得奖励的区域；存款代币汇率价格（Withdraw Price of DPT，WP）和存款代币发行量的函数关系（公式 5）；。CRR(DPT, x)为存款代币的的储备金率，表示当前存款划入存款合约的储备金的比例，剩下的 1-CRR(DPT, x) 比例的储备金存款将作为信用合约的储备金，并发行相应数量的信用代币(公式 8)。图中的参数设置 a=0.6,b=0.2,l=30000000,d=7500000。



图二 基于分布式账本技术的货币发展的两个阶段

在图二中，添加了两条曲线，并且去中心化自治银行划分成两个阶段。褐色曲线表示的是存入的第一份储备金货币扣除 35%的铸币税后获得的存款代币和信用代币的价值与存款代币发行量的关系。橙色曲线表示的是在当前存款代币发行量下存入一份储备金货币扣除 35%的铸币税后获得的存款代币和信用代币的价值与存款代币发行量的关系。 在银行的激活阶段，存款代币和储备金货币之间的汇率和储备金率浮动变化，进入扩展阶段后，存款代币和储备金货币之间的汇率和储备金率趋于恒定。整个曲线呈 S 型，类似生态系统中种群的发展。从橙色曲线可知，通过激活的阶段，可以避免早期参与者获得过多的利益，同时确保之后加入的参与者获得利益。铸币税的存在又为对货币进行宏观调控提供了条件。进入扩展阶段后，用户只要参与铸币就能够获得利益，那么此时所有持有存款代币的用户之间会进行一个群体博弈。用户会选择持有储备金货币或者持有存款代币。通过利息鼓励用户持有存款代币，同时通过低利率的贷款权力鼓励用户持有信用代币。存款合约和信用合约相互依存，互相促进。存款合约为信用合约募集早期的储备金池，而信用合约通过贷款业务获得的利益反馈存款合约，贷款业务获得的利息中的 90%将从存款合约中回购合约中剩余的存款代币，如果合约中没有剩余的存款代币，那么将引起新的存款代币发行和信用代币的授予，这部分代币资产属于所有信用代币的持有者，而剩余的 10%用于信用合约自身的增长，这 10%的利息中的一半以信用代币的初始价格发行信用代币并授予给支付利息的用户。由于在这个去中心化自治银行中，没有传统银行作为中介，直接连接了存款用户和贷款用户，同时满足了两种金融需求。另外，区别于目前的 P2P 贷款业务，去中心化自治银行是一

种无中心化自治管理的组织，其鲁棒性随着其业务的扩展而增强，系统会趋于稳定和自适应的运行。也就意味着银行这种中心化的组织和机构走向去中心化自治的道路，变成自组织的、自治的扁平结构。这种扁平结构实际上不是单纯的离散的点，而是点与点之间直接相连的网络，因此是一种扁平的网络。人们之间的距离更近，经济活动的效益更高，网络的价值也是和节点数量的二次方成正比。随着更多的人进入到这个人与人直接进行价值交换的网络中时，类似传统银行的中心化组织就被淘汰了，或者说完成了进化。



图三 基于分布式账本技术的具体系统实现的架构图

本专利提出的一种基于分布式账本技术的去中心化自治银行的构建方法能够有很多具体的实现方式，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。上图展示的是优选实施例中基于分布式账本技术的具体系统实现的架构图。在存款合约激活之后，用户可以自由的存取存款代币。用户将存款代币换取储备金货币后，存款代币将保留在存款合约中，其他用户存储备金货币时优先兑换合约中剩余的存款代币给他，这种机制抑制了过度铸币和授信。存款代币存取款价格计算采用的机制如下：

当存款合约中有足够的存款代币

原则和规律：存款代币价格尽量按高的价格计算，从而用户获得的存款代币比实际少。用户存款之后的存款代币的市场价格应当稍微低于存款时计算的存款代币的价格。用户存款之后，存款代币价格上涨，因此 Price(low)=Price(before)，Price(before)<Price(after)；储备金增加；储备金率下降。用户获得的比实际少的存款代币作为手续费支付给所有存款代币的持有者。

步骤：

1. 计算最多要给存款用户多少 DPT，假设用户存入 d 个储备金货币：deposit(max)=d/Price(low)。
2. 计算存款之后的储备金量：b+d。
3. 计算最小储备金率：f(s+ deposit(max))，s 为合约外流通的存款代币。
4. 计算存款代币的最高价格：Price(high)=(b+d)/(s*f(s+ deposit(max)))。
5. 实际价格：Price(actual)= Price(high)。
6. 实际给存款用户 DPT：deposit(actual)=d/((b+d)/(s*f(s+ deposit(max))))。

当存款合约中存款代币不够存款

原则和规律：当存款合约中存款代币不够时。不仅会涉及到存款的问题，还会涉及到合约中剩余的存款代币用完之后合约进入铸币和授信的状态的问题。所以整个存款的储备金货币分为两个部分分别考虑。对于兑换合约中剩余的存款代币的这部分，原则是存款代币价格尽量按高的价格计算，用户用于存款的这部分资金兑换的存款代币就会比实际少。这部分的计算和合约中存款代币足够时一致。因此，用户存款之后的存款代币的价格应当稍微低于存款时计算的存款代币的价格。用户存款之后，存款代币价格上涨，因此 Price(low)=Price(before) ，Price(before)<Price(after)，储备金增加，储备金率下降。但是用户还有一部分资金会用于铸币和授信。用户获得的比实际少的存款代币作为手续费和铸币税支付给所有存款代币的持有者和货币管理者。因此原问题的相反的问题是，合约中剩余的存款代币最多能抵用户多少存入的储备金

货币。进而，用户实际存款减去抵掉存款代币的部分就是用户应该用于铸币和授信的储备金货币。铸币一方面增加了储备金，另一方面降低了储备金率，还增加了存款代币的流通量。因此，中间的影响很复杂，当存款代币流通量很大的时候，储备金率下降不明显，存款代币与储备金货币之间的汇率趋于稳定。这个变化的位置大概在（l+4d）的地方。这种机制迅速补充信用代币储备金的总量。铸币的存款代币的发行价会要高出兑换存款合约中剩余的存款代币的价格很多，因为铸币的同时伴随着授信，但是铸币的用户可能面临着很高的铸币税（存款代币和信用代币各付 35%的铸币税）。

步骤：

1. 起初合约不知道存款代币是否足够，因此先假设是足够的。通过前面讲述的方法计算出 deposit(actual)如果大于存款合约中剩余的存款代币 sin，那么进入当前的计算方式。
2. 通过起初的计算知道最多能增加多少 DPT 的流通量。deposit(max)=deposit(actual)，因为实际上铸币费用更高，所以实际上存款代币流通量增加的比 deposit(max)小。
3. 计算最大的存款储备金：b+d。
4. 计算最小的存款代币储备金率：f(s+ deposit(max))。
5. 计算存款代币的最高价格：Price(high)=(b+d)/(s*f(s+deposit(max)))。
6. 计算最多抵用用户存入的储备金货币：Price(high)*si。
7. 计算剩余应该用于铸币的储备金货币：d-Price(high)*si。
8. 如果用于铸币的储备金货币小于 0，则合约没有达到铸币的条件，刚好将合约中剩余的存款代币给用户。如果大于 0，则使用铸币的计算方式发行新的存款代币和信用代币给用户。用户获得的就是 si+issue(DPT, d-Price(high)*si)的存款代币和 issue(CDT, d-Price(high)*si)的信用代币。

取款

原则和规律：取款价格尽量按低的价格计算。因此，用户取款之后的存款代币的价格应当稍微高于取款时的计算的存款代币的价格。用户取款后，存款代币价格下降，因此 Price(high)=Price(now)，Price(before)>Price(after);储备金下降；储备金率增大。用户获得的比实际少的储备金货币作为手续费支付给所有存款代币的持有者。

步骤：

1. 计算最多要给取款用户多少储备金货币，假设用户取出 x 个 DPT：withdraw(max)=x*Price(high)。
2. 计算取款之后最小的储备金量：b-withdraw(max)；
3. 计算取款之后的储备金率：f(s-x)，s 为合约外流通的存款代币。
4. 计算存款代币的最低价格：Price(low)=(b-withdraw(max))/(s* f(s-x))。
5. 实际价格：Price(actual)= Price(low)。
6. 实际给存款用户 DPT：withdraw(actual)=x* (b-withdraw(max))/(s* f(s-x))。

基于分布式账本技术的去中心化组织与传统中心化的组织产生了激烈的竞争。在传统金融体系中，银行通过集中社会财富，为一部分勇于创业的人提供必要的初始资金，同时通过从贷款中获取利息，为其他存款用户创造经济效益。传统银行的收益非常高，除去员工的工资仍然能够实现高额的收入，而这一部分收入理应属于存款用户和贷款用户。银行成为了最大的“代理商”，每年赚取了原应属于存款人的巨额利益。我们将传统的银行搬到分布式账本上，但是保留银行的职能，在去中心化自治的运行模式下，银行的收益完全归属于存款用户，减去了传统银行必要的支出。这样在实现原有银行职能的同时，存款用户可以获得更高的利率，而贷款用户同时承担更低的利率。

如上所述，本发明提供了一种基于分布式账本技术的去中心化自治银行的构建方法，为存款用户和贷款用户提供存款和贷款的金融服务，实现银行自适应的货币发行和信用的授予，同时为其他基于分布式账本技术的金融业务提供用户的信用评价。

以上所述仅为本发明的优选实施例，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、优化、等同替换等，均应包含在本发明的保护范围之内。

说 明 书 附 图