


***（蔡维德）熊猫CBDC央行数字货币模型

 大圣2017 (/u/a78a1a2a847e) [+ 关注](#)

2017.03.03 19:44* 字数 12320 阅读 1155 评论 0 喜欢 3

/u/a78a1a2a847e)

2016-11-05 天德科技 熊猫-CBDC央行数字货币模型 (https://link.jianshu.com?t=http://mp.weixin.qq.com/s?__biz=MzI3MjQ5NTI0NA==&mid=2247483726&idx=1&sn=4b95100c143d2c169c799f936b429ba1&chksm=eb30e6addc476fbb6efa70a226512eee59310ba64054e60dcd3ff7581e11d57dccc96cd81fcf&mpshare=1&scene=1&srcid=02108HEUMMAhSNUBEFQK0m52##)

作者：蔡维德1,赵梓皓1,张弛1, 郁莲2, 邓恩艳3

1-(数字社会与区块链实验室,软件开发环境国家重点实验室, 北京航空航天大学,北京100191)

2-(软件与微电子学院, 北京大学,北京102600)

3-(北京天德科技有限公司, 北京100089)

1.简介

RSCoin是世界上第一个的央行数字货币（Central Bankissued Digital Currency,简称CBDC）模型[15][1], 是英国央行赞助而由伦敦大学学院发展的。目前针对CBDC模型的研究还比较少，之前数字货币模型诸如比特币、以太坊等都属于“私人发行”的数字货币，这些数字货币在中国没有受到法律的承认和保护。**不同于“私人发行”的数字货币，RSCoin模型是第一个CBDC模型，英国央行认为CBDC会对于英国经济以及金融市场有重大影响，是几百年才遇到的一次金融变革。**

前文已经提到RSCoin是基于第一代区块链比特币而发展的，有很大的成长空间[15]。本文提出一种新的CBDC模型——**熊猫央行数字货币模型（Panda-CBDC）** [1]，本模型是基于第三代区块链北航链上，相比于前两代区块链，第三代区块链在很多方面都有所优势，例如处理速度、可扩展性。

本文将分析CBDC的优势。其次，本文将对区块链进行简单的介绍，详细分析迄今为止三代区块链的发展和优势，然后介绍熊猫-CBDC，对其进行相关分析。

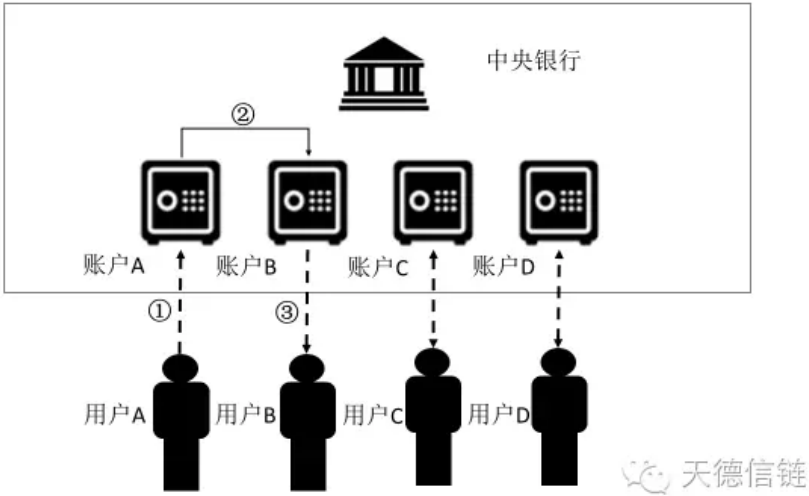
2.CBDC简介

英国央行在2015年率先提出CBDC的理念、构想和模型，明确表示要发行CBDC。2016年9月8日在英国伦敦举行了2016P2PFSY（2nd International Workshop on P2P Financial Systems 2016）大会[7]，英国央行出纳总管（Chief Cashier）Victoria Cleland会议上所做主题演讲，她谈到目前新金融科技现在正在大力度的改变英国的金融市场，第三方支付的崛起、P2P交易的增长、众筹模式的兴起等经济活动给英国经济带来了巨大的变化，迫使英国央行改变其货币政策和运行流程[15]，大力推进CBDC的发行。根据英国央行的一系列报告，英国央行发行CBDC的原因如下：

- 1.CBDC能使得交易活动更加高效地进行，而且成本更低，能见度则更高。
- 2.由央行来发行CBDC可以给市场灌注信心，并对其进行有效监管。
- 3.在英国第三方支付越来越重要，英国的金融市场在朝着P2P和众筹的新方向发展，这些新金融业务都不在传统银行的监管之下，所以英国央行发行CBDC来监管这些业务。
- 4.传统上英国银行与银行之间的交易都有英国央行来作保证，英国央行决定对于第三方支付等其他类似的金融机构给予同样的保证。以CBDC为基础，英国央行可以和新的金融机构直接来往监管以及保护交易双方。

对于CBDC的发行模式，根据Ben Dyson和Graham Hodgson文章”**Digital Cash: Why Central Bank Should Start Issuing Electronic Money**”，CBDC存在三种模型[6]：

- **直接模型（大央行模型）：**任何一个商业机构和个人都可以在央行开通账户，而钱存在央行中，钱可以用来进行支付和转账，模型如图3所示。这种模型的一个重要缺点是央行的工作量大大增加，因为央行需要处理大量非银行机构、公司和个人的账户。



- **间接模型（央行和商业机构合作）：**在这个模型中，所有账户仍然存在央行，但是有中间商业机构来处理个人账户，这个模型比较类似于现有的央行-商业银行的模型，即商业银行处理个人账户，央行只需要处理商业银行的账户，模型如图4所示。

1. 央行的工作量大大减少；
2. 鼓励商业银行市场运作；
3. 可以借鉴现行的监管机制；
4. 增加现有银行账户和支付系统的竞争，因为央行可以成为第三方支付系统，从而与其他第三方支付互相竞争。

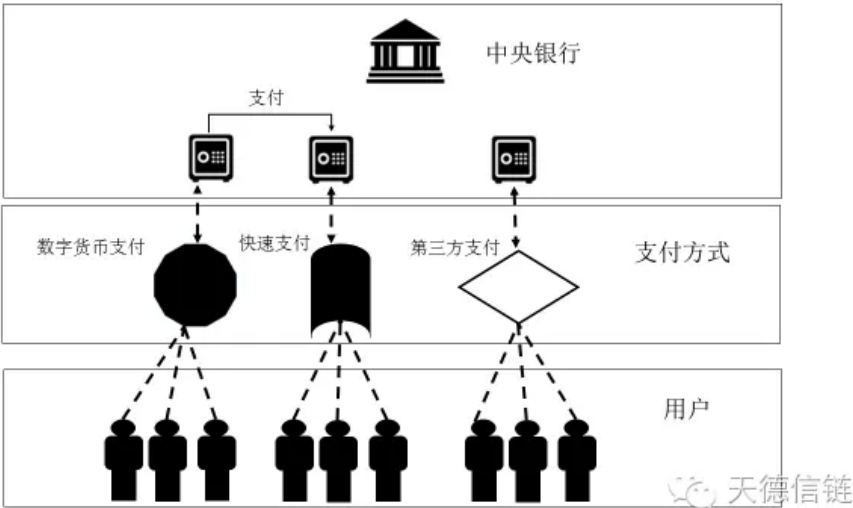


图2 间接模型

- **混合模型：**央行直接对商业机构开放，而通过间接方式对个人开放。因为CBDC的钱都在央行中，这两个机制是可以同时存在的。对于个人客户而言，不同的商业银行可以提供个性服务，满足人们不同形式的需求，而对于商业机构，其经济活动应该受到央行的监管，因此央行可以直接对其提供服务。这是一个新的模型。

CBDC的发行必将带来市场的巨大改变：

- **CBDC的发行尽量保持现有的银行架构，即央行-商业银行，中央银行管控货币的发行，商业银行则提供多元化的服务，与央行共同维护CBDC的流通。**这种模式更易在现有货币框架下逐步推进CBDC的广泛应用，而颠覆现有货币流通和发行体系，更容易被市场接受。
- **银行需要开放其核心系统，使更多非银行支付服务供应商（第三方支付系统）接入央行货币，扩大央行的服务范围。**随着第三方支付、P2P交易的流行，给央行对与金融市场的监管产生了难题，如果央行能够开放自己的核心系统，给这些新经济活动提供服务，就能很好的对这些活动进行有效的监管，维护市场的稳定。
- **央行可以借由CBDC快速实施货币政策和经济政策。**例如，CBDC的利率就是央行调控的一种工具，CBDC的利率与现有货币的利率可以不同，英国央行曾在2016 P2PFSY表示，在CBDC上，为了促进经济的发展，鼓励贷款，英国央行可能会对CBDC上所有钱收取利息，即采取负利率的措施，此外可以通过及时调整利率来调控经济的发展。但是英国央行对现有货币不采取同样政策，表示两套不同的货币政策同时进行。
- **CBDC可以使用一种全新的监管框架，**CBDC是基于数字货币，所有的钱本质上是存在于央行之中，因此所有资金的流动都会记录在区块链中，从而产生大量数据，这样央行CBDC可以与大数据相结合，分析市场的运行情况，及时调整政策，更加有效的监管和保护经济发展。

3.区块链技术简介

区块链是一种难以篡改、可追溯的分布式账本式数据库[10]。目前，区块链技术已经受到了广泛的关注，而且区块链的影响已经不仅仅局限于金融领域，知识产权保护、社会监管等等领域都开始关注区块链技术。

区块链也被称为**分布式共享总账（Distributedledger Technology, DLT）**，将相关数据存储在块中，这些块在逻辑上串联成链条，同时应用数字签名与完整性校验保证块数据的真实性、时序性、完整性。区块链采用分布式平等部署系统、分布式共享相同数据，全网参与的节点协作完成交易验证和存储。区块链技术具有不可伪造、不可抵赖、不可篡改、不可撤销等属性，在应用层面具有公开透明、交易可跟踪等特征，适合构建大规模、长历史复杂数据的分布式存储与管理系统。在安全层面上可以同时防御外部以及系统内部的安全威胁。综合区块链的特性来看，区块链技术非常适合于构建CBDC的系统，但要把区块链应用于CBDC中，区块链也需要能够满足CBDC的需求，主要有以下几个方面：

1. 高吞吐量：高吞吐量包括高速接受和处理外来信息、迅速对交易进行验证和建块、高速查询、后端即时监控。

- 2. 低延迟：延迟是指交易从发出到收到确认信息的时间差。对于央行数字货币系统需要提供良好的用户体验，及时处理交易请求并给予用户反馈。
- 3. 低能源：维护该系统所需要消耗的资源应该较小。
- 4. 安全性：主要包括外部安全和内部安全。对于一个金融系统，安全是最核心的需求，倘若系统的安全性受损则会导致整个市场的混乱。
- 5. 隐私性：主要是指需要保障客户的数据不被非法窃取。
- 6. 合规性以及监管：指金融活动的合法性，包括开户、存储、支付、汇款、交易都符合法律法规，例如简化KYC（了解客户，Know Your Customer）与AML（反洗钱，Anti-moneyLaundering）是央行的重要需求。
- 7. 可靠性和持续性：银行系统的任何微小的故障都可能带来巨大的金融风险，银行系统宕机会给银行的安全性、可用性等方面产生严重影响，适用于央行的数字货币需要保证很高的可靠性和持续性。
- 8. 即时性：许多金融活动都需要即时的反馈，例如交易完成时，需要立即告知交易客户。
- 9. 可扩展性：系统运行过程中，随着应用需求的逐步扩大，良好的扩展性能保证系统能处理更多的交易，保证系统的可用性。

(/apps/redi
utm_sourc
banner-clic

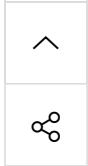
从以上需求来看，并不是所有的区块链产品都适合来构建CBDC系统，我们将以目前已经出现的三代区块链来进行分析：

比特币是第一代区块链，其账本中只记录了交易的历史信息，对于账户余额等账户信息则没有记录，而且在比特币中，每个账户只能使用一次，这就会导致系统在查询效率和便捷性方面有所不足。另一方面，比特币的一致性算法使用“工作量证明机制”（Proof of Work or PoW，俗称“挖矿”），这导致维护比特币的系统的资源消耗非常大，系统的处理速度较慢，延迟较大。RSCoin是基于第一代区块链发展而来，因此也只保存了交易的历史，没有账户信息，因此有改进空间。

随着区块链的发展，出现了以**以太坊（Ethereum）[14]**为代表的第二代区块链，第二代区块链解决了比特币没有账户历史的缺点，**在以太坊中，使用状态树来维护所有的账户信息**。因此以太坊区块链既维护交易历史，也维护账户信息，是一个完整的账本。以太坊也设计了一套“链上代码”，以太坊在区块链中引入的“链上代码”，能够快速有效的管理账户，简化交易的流程，降低交易成本。以太坊的另外一大优势是**提供了区块链平台，开发人员可以使用以太坊来进行二次开发，基于以太坊来构建自己的应用**。

如今，新的第三代的区块链技术已经产生，例如**基于新的区块链架构的北航链（BeihangChain）**。第三代区块链在全账本和链上代码的基础上，采用私有链（或者称为许可链，Permissioned-Blockchain）的设计，而前两代区块链的设计都是基于公有链。根据Z/Yen Group的调查，**目前没有一家大型银行机构计划使用公有链来运行自己的业务**。私有链相对于公有区块链来说，节点具有一定的可控性，具有更高的安全性。

同时，第三代区块链设计的是一个底层系统而非应用，**以太坊和比特币都是一种应用，包括了区块链系统和构建在其上的货币应用系统**，如果使用以太坊来构建新的应用则会带来一些冗余代码。第三代区块链作为一个底层系统，除了更好的支持二次开发，也采



用了很多工程化的方法，例如**考虑了可扩展性在系统中的重要性**，北航链设计了独有的**ABC（Account Blockchain，账户区块链）和TBC（Trading Blockchain，交易区块链）** [8]。

- 当有新的银行成立或者原有银行需要进行扩展时，可以设立ABC来解决；
- 当交易量较大时，系统可以增加TBC来增加处理速度，通过这两种途径来解决可扩展性方面的需求。

下表是第一代、第二代和第三代区块链在多个角度的比较[10]。

第一代	第二代	第三代	
分布式账簿	部分功能，只处理数字货币	完全功能,可处理数字货币和法币	完全功能,可处理数字货币和法币
交易速度	极其慢	略好	更好
交易处理	开放	开放	私有，内部
结算	较快	快	非常快
实例	比特币	以太坊	北航链
网络	P2P网络	P2P网络	高速网络

表1：第一、二、三代区块链比较

4.熊猫-CBDC模型

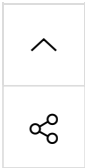
4.1 ABC与TBC

ABC与TBC 的设计思想是将执行交易和维护账本账本分析，ABC负责维护账户信息，TBC负责执行交易和维护交易历史。

ABC存储帐户信息。例如，某个小银行可以维护一个ABC，而一个较大的银行可以维护两个或者多个ABC来防止某个ABC负载过大。ABC采用多节点的设计，节点之间采用拜占庭容错协议（PBFT）来维护一致性，通过这种方式，内部员工将很难篡改账户信息。

ABC主要有以下操作：

- 创建账户：创建账户的过程包括信息录入、产生公私钥、将信息加入区块链等过程，账户的关键信息需要存储在区块链上，以防止非法篡改
- 上传账户：在上传账户时，需要对账户使用的金额进行锁定，同时，需要在ABC节点使用拜占庭算法来保证一致性，防止产生双花问题。同时，还能避免账户不一致的问题。但为了避免锁导致同一时间一个账户只能使用一次的问题，可以在每次上传时，对账户产生一个子账户，子账户包含需要的金额，只对子账户进行加锁，保证账户可以继续使用。



- 更新账户：当TBC执行完成交易后，会给ABC返回信息。若交易执行成功，则ABC需要修改账户余额，同时解锁。这些修改必须保存在区块链上，同时使用拜占庭算法来保证一致性，来防止篡改。若交易执行失败，则需要对子账户进行解锁，返还未使用的金额。

TBC则是用来交易和结算的通道（或场所），由多个节点共同组成一个TBC。TBC不保存交易双方账户信息，只是在需要的时候从ABC获取账户信息。当交易完成后，TBC删除账户信息，同时，将交易打包成区块链加入分布式账本中。

TBC可以分为两类TBC，内部TBC和跨ABC的TBC。

- 内部TBC由内部维护，可以较快与ABC通信，这样ABC内部的交易就可以快速完成。
- 当需要进行跨ABC交易时，则使用外部的TBC，由于通信等因素的限制，跨ABC的交易在执行速度上会慢于内部交易。

为了保护用户和银行的隐私，存储在TBC的数据必须加密，使得只有参与银行或是央行可以看到数据。这样的设计需要配置会员网络权限，限制访问区块链数据库。这种定制的访问意味着在交易后，银行可以给予访问区块链权限；而底层的客户端的数据只能由相关银行和监管机构可以看到。

4.2模型简介

基于ABC和TBC，提出一种央行的架构，主要分为三个部分：

1. 第一部分为账户信息，账户信息由ABC来维护，账户信息主要维护自己所负责的账户的信息，包括户主信息以及余额等，所有对账户的修改都会被区块链记录，防止篡改。
2. 第二部分为交易区块链，该区块连是由许多TBC区块链构成，这一部分负责处理所有交易。用户需要进行交易时，会把交易发送给交易区块链，TBC根据交易的输入和输出方分别向涉及到的ABC发送账户上传请求，收到账户信息后进行交易，并把账户信息返回给两个ABC，完成清算。TBC主要可以分为两种：一种TBC是处理某一个ABC内部的所有交易；一种TBC处理跨ABC的交易。
3. 第三部分为央行，央行有两个功能。第一，发行货币。所有货币的最根本来源都是央行，央行通过控制货币的发行来调控整个国家的经济，维护货币的稳定。第二，监控所有区块链的行为。央行需要审计所有ABC和TBC的行为，这些ABC和TBC处理完交易以后，都需要向央行发送日志，央行对这些数据进行保存和审计。通过这种方式，央行对整个网络的所有货币的流通进行追踪，从而评估社会的发展状况，也能发现交易中的违法行为，从而能够追踪违法者的账户信息来。

央行的主要构成包括节点、监管科技（RegTech）和大数据分析。

- 节点是构成区块链的部分，所有账户和交易信息都会保存在央行节点之上，节点之间运行拜占庭协议来保持数据的一致性。节点也为监管和大数据分析提供数据，这些数据来自于区块链上，因此数据具有可靠性，大数据和监管科技的基础更为扎实。



- 监管科技能够及时发现和阻止非法交易的执行，保证交易的合规性，简化KYC与AML的复杂性，能够降低KYC与AML的成本，提高监管效率。
- 大数据分析除了作为监管科技的一部分外，还能够获取经济运行的数据，帮助央行了解经济发展的态势，从而能够更科学的调整经济政策，促进社会和经济的发展。

(/apps/redi
utm_sourc
banner-clic

整体架构如下图所示：

图4 整体架构

在上图中，ABC-1负责维护银行1的所有客户的账本，TBC-1负责处理ABC-1内部的交易。ABC-1和TBC-1共同构成银行1的内部系统。同样，ABC-2和TBC-2构成银行2的内部系统。

若发生跨ABC交易，例如ABC-1中的账户需要与ABC-2中的账户交易，则交给TBC-A来处理，TBC-A分别从ABC-1和ABC-2中收集与本次交易相关的账户，交易结束后再将帐号更新信息发送给ABC-1和ABC-2，ABC则根据这些信息更新账户，完成交易。

央行对ABC和TBC的所有行为进行登记和监管。

4.3交易流程

对于整个交易流程，以A和B两个账户参与交易，且A和B分别来自于不同的ABC-1和ABC-2为例，交易（A->B,N）表示A账户给B账户 n单位数字货币。整个交易流程如下图：



图5交易流程

1. 发起交易：A先用自己的数字签名对该信息（A->B,N）进行签名,然后将该信息发送给TBC，由该TBC负责处理这个交易。
2. 上传账户：TBC收到交易后，分别向ABC-1和ABC-2发送请求，ABC-1收到该请求后，对交易进行验证（数字签名，A账户是否属于自己管理，A账户余额是否大于N等等），如果验证成功，则锁定A的账户，然后把A的相关账户信息上传到TBC上，ABC-2进行类似操作，将B账户上传。
3. 执行交易：TBC中的节点对交易进行验证、投票、建块。当建块成功后，TBC把交易成功的信息返回给ABC-1和ABC-2，ABC-1和ABC-2更新自己的账户。
4. 登记：ABC和TBC处理完该交易后，把交易信息发送给央行，央行记录该条交易。

至此，整个交易结束。对于内部TBC，交易的流程与上述流程类似，只是在上传和更新账户的时候会向同一个ABC发送请求和指令，其余过程与跨ABC的交易操作一致。

4.4模块算法

4.4.1 TBC交易区块链

TBC采用以下方法来进行交易的。不失一般性，假设只有两个ABC A和B参与了本次交易：

- 银行A将发送到TBC的资产冻结，使用区块链加密的方法将需要交易的资产帐户数据从一个银行帐户（ABC）复制到TBC，TBC对A发送到TBC所有节点的数据进行投票、建块，保证资产来到TBC；
- 同时，银行B也一样，TBC对B发送到TBC所有节点的数据进行投票、建块，保证资产来到TBC；

- 银行A和银行B在TBC中进行交易，并直接结算，交易结果存储在TBC中，TBC投票建块，保证TBC交易和结算完成；
- 在TBC中交易完成后，TBC使用区块链加密的方法把交易数据备份复制到A银行的ABC分类账，这将保证复制的数据是正确的。同样，TBC将交易数据复制到B银行的ABC分类帐。
- B在各自ABC分类帐都正确完成后。在TBC的数据将被标记为“过期”表示该数据是不再可用于交易。

算法伪代码如下：

```
Algorithm TBC
Input: a transaction Tx1 (A->B,N)
1 CheckTx(Tx1)
2 forall Account in Tx1
3 Request(Account.owner, Account)
5 ACCReceive from Account.owner
4 Byzantine(ACC) // obtain Account
5 CheckBalance(ACC)
6 update(ACC) // transAction
7 Byzantine(ACC)
8 forall Account in ACC
9 send(Account.owner, Account)
10 receive(Account.owner ,success) //download to ABC
11 delete (Account)
12 send(CentralBank,Tx1) //send message toCB
```

4.4.2 ABC账户区块链

ABC的主要算法是上传和更新账户信息，其算法如下：

上传账户：

- 检查请求是否合法，（数字签名、账户是否属于本ABC负责、账户是否被锁、A账户余额是否大于N），如果不合法则返回出错信息。
- 对账户的现在状态进行一次投票，保证账户的状态一致，防止出错。
- 对账户进行锁定，同时，将账户信息加密后上传到TBC。

上传账户的伪代码如下：

```
Algorithm ABC.Send
Input: Tx1 (A->B,N) , Request(Account)
1if CheckTx(Tx1) = 0 and CheckReq(Request(Account)) = 0
2 Byzantine(Account)
3Lock(Account)
4return (Account)
5else return(false)
```

更新账户：

- 检查更新指令是否合法，检查该账户是否正在被使用（锁）
- 预更新账户信息

- 对账户目前状态进行一次投票，保证整个网络中该账户的信息一致
- 更新账户信息，对账户解锁
- 向中央银行发送信息

更新账户的伪代码如下：

```
Algorithm ABC.Update
Input: Tx1 (A->B,N) , Request(NewAcc)
1  if  CheckTx(Tx1)  = 0 and CheckReq(Request(NewAcc)) =0
2  if  Lock(Account)
3  PreUpdate(NewAcc)
4  Byzantine(NewAcc)
5  Update(NewAcc)
6  UnLock(Account)
7  return (success)           //Return to TBC
8  send(CentralBank,Tx1, NewAcc)  //Send message to CB
9  Else  return(false)
10 else  return(false)
```

4.5交易

在处理交易方面，主要分析熊猫-CBDC模型对第3节中需求的满足情况：

- (1) 高吞吐量和低延迟：地方交易地方处理，跨地域交易需要高速网络，这样方式下，地方交易的处理速度能够加快，而且延迟较小。跨地域交易则需要高速网络来降低网络延迟的影响。
- (2) 低能源：使用私有区块链，使用PBFT协议，而不是用POW的挖矿机制。参与投票的节点都是被授权的节点，这样整个区块链的维护不需要庞大的算力来支持，减少电力等能源的消耗。
- (3) 安全性：区块链上所有数据都是用加密算法，发起交易时需要验证客户的数字签签名。通过密码学手段来保护系统的安全。使用分布式账本技术，既可以防范来自于外部的攻击，也能有效防止内部攻击，防止内部职员篡改数据。
- (4) 隐私性：1.商业银行可以保护自己客户的隐私2只有当需要交易的时候才上传客户必须的信息（只上传和交易有关的信息），3交易结束后会把客户信息封闭。以上任何环节出现问题，所泄漏的信息少。
- (5) 合规性：1.央行会在ABC和TBC设立自己的节点来监控区块链运行2.每生成一个区块，都会给央行发送信息，央行可以对比1中节点信息来监管运行
- (6) 可靠性和持续性：使用拜占庭将军问题的算法，不超过三分之一的节点出错都不会影响系统的正常运行。这种机制大大增强了系统的可靠性和持续性。
- (7) 即时性：交易处理过后，都会即时的给用户返回成功或者出错的信息，对于即时清算结算，可以根据需求进行相关的设计，无论是即时或是非即时，该模型都能够支持。

4.6货币管理

本节主要讨论以下四种情况：货币的发行、“直升机撒钱”（helicopter money）、利率调整、补贴救济。



在货币发行方面，遵从现有的银行体系，即央行-商业银行模式。央行有权创建一种特殊的交易，“凭空”产生一笔货币，并将其转移给商业银行。商业银行收到该货币后可以放贷，这样央行和商业银行共同合作来完成货币的投放。而央行可以控制货币发行的速度，从而调控经济。

“直升机撒钱”，即给每个公民一笔钱，这样的政策可以用CBDC来轻易执行。传统货币的发行是从商业银行购买公债，从而把钱从央行转到商业银行，这种方式相对来说是比较费时的，而且公民比较难拿到钱。在熊猫-CBDC中，央行可以以给每一个用户发放货币的方式来完成“直升机撒钱”，这种方式不需要第三方和个人的参与就可以进行，是一种能够快速、简单地将货币直接发放给公民的方式。

在CBDC中，央行可以快速的修改货币的利率。例如英国央行提到，为了防止CBDC与商业银行竞争客户的存款，促进货币的流通，可能会采取负利率的措施，即商业银行存在央行的CBDC必须支付央行利息，而央行可以通过调整利率来执行货币政策。负利率的实施可以通过链上代码或者TBC交易来完成，在链上代码上修改利率，所有账户会在无人参与的情况下上自动执行这些代码，完成对利率的调整。

在社会补贴和救济方面，则可以由央行统一进行管理和发放。央行产生另外一种特殊交易，不需要经过商业银行就将这些款项直接发放给特定的人员，快速、定向地发放货币，同时这些款项的流向将会被严格监控，从而使社会救济和补贴更加高效合理。

4.7监管

在央行对商业银行的监管方面，央行可以采取如下两个措施：
ABC和TBC在处理完交易后都需要将交易详情发送给央行，央行对这些信息进行分析、建块，并将块加入自己的区块链中，形成高级区块链。

央行可以在ABC和TBC中设立自己的节点，这样央行就能够获取每一个区块链上的所有数据。一个简化的熊猫-CBDC模型的节点构成如下图所示：

图6节点构成

说明：

央行需要在所有的ABC和TBC中设立节点，以便监管银行的运行来判断用户或是银行是否存作弊行为，也能及时发现央行在每个区块链上至少设置两个节点，这样当一个节点宕机时，另一个节点也能继续进行监管。

TBC中的节点应该由央行以及参与银行共同构成。

(/apps/redi
utm_sourc
banner-clic

对于CBDC的监管模型，我们提出了以下的架构：

图7监管架构

在这个模型中，需要将数据同时发送给监管机构和区块链系统来处理。监管机构可以使用多种技术对数据进行分析：其一是即时分析：若在交易执行结束之前发现非法或者出错的行为，监管机构可以给区块链发送信息，停止该交易的执行。为此，必须保证监管机构能够快速响应，即时发现出错湖综合非法的交易。在这一模型中，监管和交易都必须是即时系统。其二是对历史数据的分析，能够从历史数据来检测整个系统的运行。

针对监管科技，熊猫-CBDC有以下的设计：

1. 央行保存了所有商业银行的一切数据。这样央行就可以综合分析每个用户的行为，从而及时发现错误信息，阻止违法行为的发生。
2. 使用KYC和AML，央行和商业银行都可以验证交易双方的身份，从而对其进行分析，判断交易是否合法。
3. 所有违法或者出错的交易应该被即时发现和阻止，因为在CBDC中，所有的交易都会即时处理。如果违法或者错误交易没有被及时阻止，可能导致这些非法所得被转移。因此，CBDC必须有即时的监管和阻值非法交易的机制。区块链和监管科技都必须是一个即时系统来防止欺诈行为的发生。当用户登录时，系统会验证其身份，如果怀疑该用户可能存在作弊行为，必须即刻在全球范围内禁止其进行交易，当这个用户创建交易时，系统将会搜索和分析与其相关的所有信息，并在其完成之前阻止交易的发生。

在监管可以方面，央行还可以进行大数据分析。央行将系统所有的数据都格式化存储，这样就可以使用很多计算机的技术来对数据进行有效的分析，例如使用大数据分析技术来获取经济运行中的很多信息，能够使用机器学习的算法来识别偷税、漏税、洗钱等行

^

为。随着计算机技术的发展，数据的价值越来越高，将这些数据进行格式化存储是非常有价值的。

4.8扩展性

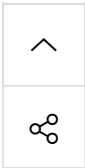
ABC自身扩展性：ABC提供一个对账户进行分割的方法，当账户数量过多导致ABC不能及时维护这些账户时，ABC可以分割为两个ABC，两个ABC都保存旧账本，以保持历史账户的完整性，同时两个ABC之间使用负载均衡的策略，共同维护账本，来满足可扩展性的需求。ABC账户分割如下图：

图8 ABC自身扩展

TBC扩展性：如果银行之间的交易量增多，则可以通过增加TBC来解决TBC性能不足的问题，因为所有的TBC都可以并行运行，因此，系统的处理速度随着TBC的增多而变快。

系统扩展性：对于整个系统，如果新开设了一家银行，则该银行需要建立一个ABC和内部TBC，同时可以选择加入到已有的跨行TBC中。此外，如果某些银行之间存在大量的交易，为了提高整个系统的效率可以设置一个专用TBC来处理交易。例如，在4.2系统架构图中，增加银行-3，同时，银行-2与银行-3之间存在大量的业务来往，则整个系统的可以扩展为：

(/apps/redi
utm_sourc
banner-clic



(/apps/redi
utm_sourc
banner-clic

图9系统扩展性

如上图所示，银行-3开设自己的ABC-3和银行内部TBC-3，同时银行-3加入原有的TBC-A以便能够与银行-1和银行-2进行交易。因为银行-2与银行-3有大量业务往来，为了提高系统运行的效率，可以设置TBC-B来专门处理银行-2与银行-3之间的业务。

4.9安全性和通信量

这一部分，我们主要来计算在一定节点数量的情况下的安全性和通信量，首先假设条件如下：

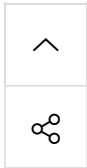
- 1. 一个交易涉及2个ABC和一个TBC
- 2. 每个ABC（TBC）由n各节点组成
- 3. 每个节点在一次交易中出错的概率为P

则安全性计算如下：
根据拜占庭协议，只有在超过1/3各节点出错的情况下系统才会出错，对于一个ABC（TBC），一次运行出错的概率为：

Paste_Image.png

每次交易，只要有任意一个ABC或者TBC出错，整个系统就会出错，因此，一次交易中，整个系统出错的概率为：

则连续处理t个交易不出错的概率为：



假设每次运行出错概率 $P=0.01$ ，连续正常运行1, 000,000次概率和节点的关系如下：

图10安全性分析

由图可知，随着 n 的增大，正常运行概率越高。但是当 $N>18$ 后，连续正常运行1, 000,000次概率基本不变
通信量计算如下（按照交易流程来计算）：

第一阶段通信量：
因为第一阶段user需要给所有TBC节点发送交易，通信量为 n

- 第二阶段通信量：
- 1. 请求阶段，TBC中每个节点给对应的ABC中节点发送请求，通信量约为 $2n$
 - 2. 收到请求后两个ABC都需要运行一次拜占庭算法（一次拜占庭协议的通信量约为 $2n^2$ ），通信量约为 $4n^2$
 - 3. 发送账户信息通信量约为 $2n$
 - 4. TBC收到账户信息后，为了保证信息一致性再一次运行拜占庭协议通信量为 $2n^2$

因此，第二阶段通信量约为 $6n^2+4n$

- 第三阶段通信量：
- 1. 交易执行后，TBC为了保证交易执行的正确性要运行一次拜占庭协议，通信量为 $2n^2$
 - 2. 发送账户信息通信量约为 $2n$

- 3. 两个ABC收到账户更新后，为了保证账户一致性需要运行一次拜占庭算法，通信量约为 $4n^2$
- 4. 两个ABC需要给TBC返回更新成功信息，通信量约为 $2n$

因此，第三阶段通信量约为 $6n^2+4n$

第四阶段：
所有ABC节点和TBC节点都需要给央行中的节点发送交易信息，通信量约为： $3n$
因此，一次交易需要的通信量为 $12n^2+12n$

一次运行通信量和节点关系如下：

图11通信量分析

4.10容错性

由于熊猫-CBDC系统有多备份的设计，因此，系统具有较强的容错性。系统可以从两个方面来对错误的节点进行恢复：

- 1. 同一区块链中的其他节点。由于每一个TBC和ABC的每一个节点都保存了该区块连所有的数据，因此任何一个节点数据的损坏都可以从其他节点来拷贝。
- 2. 通过央行的数据。央行保存了所有的历史数据，因此任何节点都可以从央行来获取自己的历史数据，进行错误恢复。

节点也可以将两种方式进行结合，来进一步保证数据的正确性和安全性

4.11对比

RSCoin是伦敦大学学院所设计的CBDC模型，其主要思想有以下几点：

- 1. 将比特币的节点分成组，每一组来处理不同的交易，这样随着组数越多交易处理越快。
- 2. 组间通过用户来进行传递，这样的设计避免了广播系统大量通信的缺点。

使用两段提交协议，而不是比特币的工作量证明机制。在节点的正确性方面采取少数服

从多数的策略。

3.每个节点都是被授权的，与比特币不同，RSCoin的每一个节点都被央行授权来处理数据。

下表是RSCoin与熊猫-CBDC的比较：

RSCoin	熊猫-CBDC
交易和分布式账簿	支持交易，每个mintettes保存一部分账本，这些账本不是链结构。央行保存所有账本，是链结构
支持交易，每个ABC保存账户，TBC执行交易，都是完整的区块链	
吞吐量	随着mintettes增多吞吐量线性增加，原始系统吞吐量约2000交易每秒
地方交易地方处理，跨地域交易需要高速网络上传到TBC，这样可以增加吞吐量	
低延迟	延迟较高，因为每次交易需要4个阶段，每个阶段都需要通信，延迟较大
地方交易地方处理，延迟较小。跨地区交易上传账户的通信消耗较大，延迟较大	
低能源	不使用挖矿技术，能源消耗较少
不使用挖矿技术，能源消耗较少	
安全	安全性与参与验证的mintettes数量有关，使用少数服从多数原则
安全性与ABC和TBC节点数量有关，使用拜占庭将军问题算法	
隐私性	mintettes处理的交易是动态分配的，这样交易可能会被不同mintettes收到，有一定不确定性，但是mintettes不会保存所有交易
因为ABC包含自己机构的消息，不与别人分享，而ABC只分享必要的消息给TBC，TBC做完交易后，消息也被贴上标签“过时”，让留在TBC的消息失去时效性。所以隐私性强	
合规性	央行可以审计所有交易，但是所有信息都是完全来自于mintettes
A.央行可以审计所有交易；B.央行在ABC和TBC中设有节点，可以参与投票	
即时性	较高，处理交易后会即时收到处理结果
较高，处理交易后会即时收到处理结果	
可扩展性	使用授权的mintettes，增加mintettes就增加交易速度
使用系统工程以及云计算技术来扩展：1，分ABC和TBC（每一个区块链只做一件事情），2，负载均衡；	

而在商业模式方面，相比于RSCoin，熊猫-CBDC更适合现有的央行-商业银行模式。

- 交易发起授权方式——在RSCoin中，交易发起是需要获得不同mintette组的授权。而**熊猫-CBDC则只需要管理其账户的ABC的确认**，熊猫-CBDC更符合现有模式。
- 交易的分配策略——RSCoin对交易的分配采取动态分配的策略，即一个用户的信息会被保存在不同的mintette中，这会造成两方面的影响。其一，用户的隐私权难以保障，用户无法选择将信息保存在哪一个机构中。其二，银行难以给用户提供个性化的服务，因为用户的信息被碎片化的保存在不同的mintette中，银行难以针对每个用户的特征来提供服务。**而在熊猫-CBDC中，用户可以选择某一个ABC来负责管理其账户，因为该用户的所有信息都保存在这个ABC上，因此，商业银行可以为该用户提供个性化服务，也能更有效的对用户行为进行分析。**
- 熊猫-CBDC综合考虑了隐私性、监管以及交易执行速度等问题，RSCoin则重点在于**交易执行速度方面，在监管方面的设计还有所欠缺。**同时，上文也提到RSCoin在隐私保护方面有所不足。在速度方面，熊猫-CBDC以北航链为基础，同等节点情况下交易处理速度较快。

5.总结

随着CBDC受到广泛的关注，越来越多的央行已经宣布将要发行数字货币。然而，有关CBDC的模型讨论较少，RSCoin是世界上第一个CBDC模型，受到了广泛的关注。但是RSCoin的设计是基于第一代区块链（比特币）而构建的，随着区块链的发展和第三代区块链技术的产生，我们提出了基于第三代区块链北航链的一种新型CBDC系统。

熊猫-CBDC使用北航链独有的ABC（账户区块链）和TBC（交易区块链）以及中央银行的架构，ABC和TBC保证了银行账户的有限隐私性，同时ABC和TBC技术能够对区块链提供一种可扩展的机制。另一方面，央行的设计能够保障对于整个系统的有效监控，保证金融活动的合法性。在此基础上，针对本系统设计了央行相关的执行交易、货币发行、监管等方法。另外，本文将RSCoin与熊猫-CBDC模型进行了一系列的对比。熊猫-CBDC综合考虑CBDC在交易执行即时性、监管、隐私等方面的需求，契合现有的商业体系，更易得到市场的认可。

英国央行于2014年提出CBDC的构想，RSCoin于2015年提出，并在2016年对原型进行了测试。从RSCoin的发展轨迹来看，熊猫-CBDC还有很大的进步空间，随着**金融科技**的不断发展，央行的系统需要不断的为新经济活动提供服务、监管和保护；随着**监管科技**的发展，越来越多的监管技术可以应用到CBDC模型当中，使央行和金融机构能够更好地分析和监管经济的发展，也能更加及时准确地惩处不法经济行为。

文献引用

[1]G. Danezis and S Meiklejohn, “CentrallyBanked Cryptocurrencies,” Proc. of NDSS, 2015.
http://arxiv.org/abs/1505.06895 (https://link.jianshu.com?t=http://arxiv.org/abs/1505.06895)

[2] “One bank research agenda,” 2015,
www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf
(https://link.jianshu.com?t=http://www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf).

[3]”The economics of digital currencies”,2014,
http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q302.pdf (https://link.jianshu.com?t=http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q302.pdf)

[4] ——, ”Innovations in payment technologies and the emergence ofdigital currencies”,2014,
http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q301.pdf (https://link.jianshu.com?t=http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q301.pdf)

[5] Harjeet Baura, ”Peer pressure: How Peer-to-Peer Lending Platforms are Transforming theConsumer Lending Industry”, Feb 2015,
http://www.pwccn.com/home/eng/peer_to_peer_feb2015.html (https://link.jianshu.com?

- t=http://www.pwccn.com/home/eng/peer_to_peer_feb2015.html)
- [6] Ben Dyson and Graham Hodgson, "Digital Cash: Why Central Bank Should Start Issuing Electronic Money," Positive Money 2016, www.positivemoney.org (<https://link.jianshu.com?t=http://www.positivemoney.org>)
- [7] Victoria Cleland, "Fintech: Opportunities for all?" 2nd International Workshop on P2P Financial Systems 2016, 8 September 2016. <http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech919.pdf> (<https://link.jianshu.com?t=http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech919.pdf>)
- [8] W.T. Tsai, R. Blower, Y. Zhu and L. Yu, "A System View of Financial Blockchains," IEEE Computer Society, 2016.
- [9] 王永红, "数字货币技术实现框架", 中国金融 2016 年第 17 期[M], <http://www.cnfinance.cn/magzi/2016-09/01-24312.html> (<https://link.jianshu.com?t=http://www.cnfinance.cn/magzi/2016-09/01-24312.html>)
- [10] 蔡维德, 罗佳, "浅析私有区块链技术", <http://sanwen8.cn/p/1efjDL3.html> (<https://link.jianshu.com?t=http://sanwen8.cn/p/1efjDL3.html>)
- [11] Andrea Pinna and Wiebe Ruttenberg, "Distributed Ledger Technologies in Securities Post-Trading - Revolution or Evolution?" 22 Apr 2016, <http://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf> (<https://link.jianshu.com?t=http://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf>)
- [12] "【FX168 专访】北航国家'千人计划'特聘教授蔡维德谈数字货币技术在英国央行的应用及展望", <http://finance.sina.com.cn/money/forex/datafx/2016-09-28/doc-ifxwkvys2228025.shtml> (<https://link.jianshu.com?t=http://finance.sina.com.cn/money/forex/datafx/2016-09-28/doc-ifxwkvys2228025.shtml>)
- [13] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2009.
- [14] "Ethereum: A Next-Generation Generalized Smart Contract and Decentralized Application Platform" <http://ethereum.org/ethereum.html> (<https://link.jianshu.com?t=http://ethereum.org/ethereum.html>)
- [15] 蔡维德, 赵梓皓, 张弛, 郁莲, "英国央行数字货币 RSCoin 探讨", 金融电子化 2016 年第 9 期, 78-81.
- [16] 蔡维德, 赵精武, "两种选择, 两种结果——the DAO 事件的反思", <http://ethfans.org/posts/141> (<https://link.jianshu.com?t=http://ethfans.org/posts/141>)
- [17] 蔡维德, 罗佳, "区块链所带来的公信力革命——以区块链对保险行业的影响为例", <http://www.sosobtc.com/article/14755.html> (<https://link.jianshu.com?t=http://www.sosobtc.com/article/14755.html>)

(/apps/redirect?utm_source=click_banner)

小礼物走一走，来简书关注我

赞赏支持





大圣2017 (/u/a78a1a2a847e)

写了 1951493 字, 被 2462 人关注, 获得了 1962 个喜欢 (/u/a78a1a2a847e)


+ 关注

(/apps/redi
utm_sourc
banner-clic

喜欢 | 3



下载简书 App ▶
随时随地发现和创作内容



(/apps/redirect?utm_source=note-bottom-click)





登录 (/sign_in?utm_source=desktop&utm_medium=not-signed-in-comr


评论

智慧如你, 不想发表一点想法 (/sign_in?utm_source=desktop&utm_medium=not-signed-in-nocomments-text)咩~

被以下专题收入, 发现更多相似内容

- 

区块链技术研究 (/c/65eb459d50cc?
utm_source=desktop&utm_medium=notes-included-collection)
- 


区块链技术 (/c/1ce1650dde5f?utm_source=desktop&utm_medium=notes-
included-collection)
- 

区块链 (/c/11bad11114dd?utm_source=desktop&utm_medium=notes-
included-collection)

^

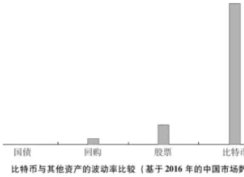
区块链丛书笔记一：区块链—从数字货币到信用社会 (/p/67fd83e3a35b?utm...

区块链丛书笔记一：区块链—从数字货币到信用社会 按：达鸿飞的几章写得不错；有几章晦涩难懂；也是因为几个作者各写一到几章；都是忙人，内容组织、统筹欠缺些。“区块链是一种思想，是许多个开源项...

 物流人杨浩峰yhf (/u/34e6d5ece5a3?)

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio (/apps/redi
banner-clic


(/p/9694eaac54b1?



utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendatio

（姚前）法定数字货币的理论与技术逻辑：货币演化与央行货币发行创新 (/...

2017-09-27 姚前 《比较》关于数字货币，你不可不读的文章中国人民银行数字货币研究所所长姚前在《比较》发表最新文章 9月4日，中国人民银行等六部委联合发布公告：停止各类代币发行融资活动。仅仅十...

 大圣2017 (/u/a78a1a2a847e?)

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio


(/p/c49ed7a9c532?



utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendatio

***（蔡维德）区块链互联网•正式演讲稿 (/p/c49ed7a9c532?utm_campaig...

2017-05-27 直播 贵阳数博会5.27@国际生态会议中心二楼会议室42017-05-27 简书 贵阳数博会（蔡维德）
区块链互联网2017-06-03 天德信链 链网实验室 区块链互联网（演讲稿）蔡维德@贵州数博会（2017年5...

 大圣2017 (/u/a78a1a2a847e?)

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio


(/p/acdff92bd16c?



utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendatio

深度观察 | 区块链与数字货币：原理、特征和构想 (/p/acdff92bd16c?utm_...

区块链和比特币是什么关系？电子货币、虚拟货币、数字货币有什么区别？央行在研究的数字货币是什么样的？和区块链有关系吗？区块链和数字货币，这两个对大部分人还挺陌生的概念，其实近期已经引起了监...

 烛微虑远 (/u/ab237ec6f0a8?)

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio

(/p/e84cb55bc2cc?

utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendatio

稳定数字货币手册Beta版 (/p/e84cb55bc2cc?utm_ca...

Beta版当中我增补了更多货币学范畴以外的内容，以解答如下问题：去中心化（Decentralization）与去中介化（Disintermediation）究竟是一种终极目标，...


 shenciyou (/u/be1ed69aa45c?

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio (/apps/redi
utm_sourc
banner-clic

Illustrative Summary of the LCR	
(percentages are factors to be multiplied by the total amount of each item)	
Item	Factor
Stack of HQLA	
A. Level 1 assets	
Cash and bank notes	100%
Qualifying negotiable securities from sovereigns, central banks, PSEs, and multilateral development banks	
Qualifying central bank reserves	
Domestic sovereign or central bank debt for non-0% risk-weighted	
Qualifying sovereign or central bank debt for non-0% risk-weighted	
B. Level 2 assets (maximum of 80% of HQLA)	
Level 2B assets (maximum of 20% of HQLA)	
Sovereign, central bank, multilateral development banks, and PSE assets qualifying for 20% risk weighting	80%
Qualifying corporate debt securities rated AA+ or higher	
Qualifying covered bonds rated AA+ or higher	
Qualifying sovereign or central bank debt for non-0% risk-weighted	
Level 2A assets (maximum of 60% of HQLA)	
Qualifying RMBS	75%
Qualifying corporate debt securities rated below AA+ and BB+	70%
Qualifying common equity exposures	50%

《聚会散记》 (/p/f07b5ff48427?utm_campaign=maleskine&utm_conten...


今天，晴，周二。2018年9月4日。好几天未写日记，心里还有些失落感。也读同修们的日记，愧疚自己怎么就写不出那么深刻的感悟?原来是自己没有用心去链接生活中的人或事，只是一略而过，冷漠不关心周遭的...

 雾里看花_c7e4 (/u/53ba65797855?

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio

我的美乐家故事 (/p/2f9d3739c957?utm_campaign=maleskine&utm_con...

2014年五一家里发生一些变故，需要我辞职在家带孩子。一种全职家庭妇女的不安全感油然而生。爱人为了安慰我，怕我多想，提出要把房本上加上我的名字。其实，我的不安全感，不是经济。说白了一对刚结婚...

 北京时间管理学院 (/u/df9dfd7474e6?

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio


(/p/a4d4fdbefcfb?



utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendatio

安意如：有一种本事把残缺活成了美 (/p/a4d4fdbefcfb?utm_campaign=m...

五年前端午节的午后，在北京西单图书大厦，邂逅了一系列古文诗词解析，邂逅了美文同时邂逅了安意如。从此，便爱上了这么一个女子。她柔美中带着灵性，恬静带着优雅，她安静的样子如同一幅美人胚子的画...

 女公子99 (/u/d1970c9f1f66?

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio


(/p/0885a457c31d?



utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendatio

她们都是怎么做的：减龄显瘦的秘诀=换发型？ (/p/0885a457c31d?utm_ca...


今日入伏，预示着炎热的夏天正式向我们敞开了怀抱！夏天是个很适合剪短发的季节，今天小编就给大家整理了一些迷人的短发造型，给广大小仙女们做一下梳理。短发会令你变得优雅、青春、有活力。合适的短...

 美黛定制补发 (/u/8b7b99ec222d?

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio

《师兄请喝茶》第5章 真相 (/p/34f032d1a3aa?utm_campaign=maleskine...

赵菲家庭条件不是很好，性格有点沉默寡言，可能上大学最勇敢的事，就是找陈温帮忙介绍兼职。陈温把她推荐给了学校里的一位老教授，帮忙整理一些资料，批改一些作业。工资是老教授支付，每月三百块，据...

 李方知 (/u/b601b4e1084f?

utm_campaign=maleskine&utm_content=user&utm_medium=seo_notes&utm_source=recommendatio
banner-click

(/apps/redi

utm_sourc

banner-click

