数字货币的互联网架构 1/3（从零开始学区块链 88）

2017-01-10Meher Roy

发一篇译文，把数字货币的体系结构讲得比较清楚，由于原译文比较长，为了方便阅读，决定分成三部分分别转发出来，本文是第一篇（共三篇）

1 介绍

中本聪最伟大的发明比特币，可以因为以下两处不同的特征广受赞誉：

1. 比特币是公开的，去中心化的，加密总账（cryptographic ledger），同时拥有基本总账能力。
2. 加密总账能追踪新的比特币的余额。

以比特币为基础的平行金融体系正在被着力打造当中。加密总账在灵活性上的便利开发诸多。例如多重签名账户，去中心化兑汇，机器间交易的新应用，而这些成为了开发的驱动力。这一论文分析加密总账在目前金融体系中的应用，同时促进对一下内容的讨论：如果金融机构利用公共加密去中心化总账，同时有基本总账能力，当他们检测资产负债余额情况时，哪些速度、成本、灵活性上面的优势可以达成？

这些总账给实时全额结算系统（Real Time Gross Settlement）例如 CHAPS 和 FedWire 的构建带来了新的方式，同时还有延迟净额清算系统（Deferred Net Settlement）例如 ACH，Bacs 和对应银行，外汇交易市场，股票交易市

场和其他金融体系的支柱。这篇文章把这些去中心化的元素压缩进一个基于层级的连续框架，同时称它为：货币的一种互联网体系架构

货币的一种互联网体系架构带来的可感知好处将会随着对系统的介绍一同枚举。这些好处是邀约的动机。

2 缩写和定义

ACH：自动清算系统，确保美国基于延迟净额清算基础的零售支付过程可行的系统。

Bacs：确保英国基于延迟净额清算基础的零售支付过程可行的系统

CHAPS：英国用来实施高价值交易的基础全额结算基金交易系统

Consensus Pool：一组服务器，拥有给定的主人，使用容错算法来持续达到共识状态的总账。健康的共识池（consensus pool）一般由不同对手方控制若果服务器。

DApp：去中心化应用

DE：去中心化交易

DEP：去中心化交易协议(protocol)，在 7a 部分有描述

DNS：延迟净额清算

DNSP：延迟净额清算协议，在 7d 部分有描述

FedWire：美国用来实施高价值交易的基础全额结算基金交易系统

Issuer：在加密总账上发放财产的对手方。这一对手方可以是一家银行，公司，去中心化的匿名机构，政府或者私人个体。财产可以是商品保障代币，货币，情报类货物，公司内部股权，代表航空里程的代币。

Ledger contracting：请在 3,4 小节找到释义

ODFI：初始存储金融机构，一家创立自动清算贷款的银行。

OFI：初始金融机构，一家创立 FedWire 贷款的银行。

RDFI：存储接受金融机构，一个结束 ACH 贷款的银行。

RFI：接受金融机构，一家结束 FedWire 贷款的银行。

RTGS：实时全额结算系统。

GTGSP：实时全额结算系统协议，在 7c 中有描述。

SIPS：重要支付系统。

SL3P：静态流动性支付过程协议，在 7b 中有描述

Tx：交易

3 框架

由 OSI 层模型得到启发货币互联网构架按图一(Figure 1)进行：

接下来的部分详述每一层的需求和能力，论文和划分为以下分段：

4,5 节描述了总账协议，由比特币和以太坊项目概念升级引领的创新。总账协议给此文多重组成建造了基础。在 4 小节对比特币的描述中，尽管在抽象有利情况下来看是正确的，但又与目前的实现有所偏离。

6,12,13 小节讨论总账层，6 小节做了整体假设，省略了理由。理由和详述在 12 小节。13 小节的目的写在 5 小节。

7a，7b，7c 和 7d 描述了 DEP，SL3P，RTGSP 和 DNSP。这一段阐述了货币互联网的潜在核心创新。

8 小节展示了 7 小节中的协议可以统一成两个基本的总账运行。这一联合使得实现易于处理。

9,10 和 11 小节分别介绍了寻找的目标，协议一节程序层。

14 小节展示了重要的观察和开发问题。

4 比特币的总账合约

总账协议是追踪价值余额账户的协议。它们允许客户在自己账户里减去 X 单元，同时在另一个账户里计入 X 单元。为了达成一个重要的运作，客户的账户必须有超过 X 的余额。图一形象化了两个花旗银行客户，Alice 和 Bob。Alice 创立了这个支付。

在上图的运行中，比特币通过总账协议增加了财富。总账协议是保持余额的账户在预定规则下运作。比特币外部的实体，像 Alice 和 Bob，在完成规则集(rule sets)前不能用总账协议来缔约。这一实施因为违背协议规则拒绝比特币节点来进行。

例如，Alice 想要把比特币转给 Bob，同时 Bob 只能在 15 年 12 月 31 日后使用比特币。创立一个保持比特币暂时余额的总账协议(ledger contract)就能进行。对 Bob 的转账，在总账协议中设置给定日期后才能获得比特币。图三展示了这个流程：

总账协议可以被认为是中立的，自动的第三方，调停 Alice 和 Bob 之间的转账关系。读者需要知道上面的图是一个抽象（abstract）概念，比特币可以不同方式地来实施交易。

图四提供了第二个注释。Alice 是一个买家，Bob 是一个卖家。货物交易有个很长的运输时间。Trent 是同时被 Alice 和 Bob 信任的第三方。在这一买卖中，Alice 把买物价值存在总账协议，按以下条约：

三方中任意两个必须签约保证协议资金不能动。

如果货品错误接受，Alice 和 Trent 能把资金给回 Alice。

销售顺利结束，Bob 和 Trent 把支付款项给到 Bob。

图四展示了成功销售交货时候的交易流程。总账协议就像一个中立的自动第三方调停 Alice，Bob 和 Trent 直接的交易关系。

比特币总账协议由堆栈为基础的（stack-based）字节代码(bytecode)语言编程，我们叫它为“Bitcoin script”。每个总账协议都有代码和缓存数据结构。

比特币协议系统有两个重要的限制：

价值盲区(value-blindness)：协议不能执行比总共存储在内的资金金额低的交易。也就是说检索时间内应用人要一次提出所有资金。

缺少持久储存/状态：协议不能存储数据，这限制应用人不能做去中心化交易。

图五展示了强调限制的假设情况。Alice 想用总账协议把比特币换成狗狗币。她建立了一个总账协议，并规定用比特币来交易。条约为：当对方给 Alice 的地址提供了狗狗币支付证明(payment proof)，协议会把比特币给到对方指定的地址。

价值盲区限制指 Bob 作为另一方，必须交易 Alice 在协议里实际指定的数额。对方可能希望一个较小的交易量，然后得到总账协议里相应部分的资金。这一操作在单比特币总账协议中无法进行。

假设部分交易可行，比特币总账协议必须存储能使用的支付凭证。当这一存储流失，对方能重复提供同样的凭证，不公平地提尽资金。无法存储和价值盲区限制了去中心化交易等程序。

目前的例子仅为了强调限制。它有其他未被提及的瑕疵。去中心化交易比特币在另一个结构——原子交叉链交易(Atomic Cross Chain Trrade)中，可以更好地实施。尽管它也有价值盲区限制。

5 含有以太坊的总账合约

以太坊项目含有许多创新，其中以下几个对本文很重要：

1. 总账协议是有价值意识(value-aware)，拥有持久存储能力。
2. 总账协议在需要的时候能存入/提取(loaded/unloaded)资金。存入/提取条件由协议代码(contract code)执行。
3. 有数据的消息可以传送到总账协议。协议能用数据回复，把价值传到输入处。

7 小节对以上的使用进行了演示。因此此处举例省略。其他以太坊创新对我们的讨论是次要的，将在 12 小节提到

1. 总账协议能进入一些随机数据。目的是为投机应用提供熵源(entropy source)
2. 用来创立总账协议的改编语言是图灵机完成的。
3. 总账协议能创立另一个总账协议。因此，与外部人控制账户有同样的权限。这是指“联系第一阶级市民的财富”(contract first class citizen property)

b，c 两点的连结意味着在升级以太坊总账时可能会产生无限循环情况(loops)。在估计任意脚本在有限时间内终止或者阻止网络节点拒绝交易导致无

限循环时，Halting 问题提供了一个限制。当一个程序为了防止节点拒接交易而陷入死循环时，Halting 问题对此进行判断之后创新引发的风险有两个：

1. 阻止无限循环的交易费用法在某些未知情况下是有缺陷的。
2. 明确设计的恶意协议代码能从以太坊虚拟机中逃逸并引发网络节点损坏。

12 小节讨论了防范风险的方式，同时还能得到以太坊的若干好处。驱动力是在邀约实施孵化期避免风险和复杂性。

6-10 小节假设以太坊总账协议能力的完整集是有效的。

【未完待续】