方舟块，一种借助主区块链交易签名验证构建可信任区块链的方法

Paul Baoyong Liu
paul@bindpay.com
www.ArkBlockchain.org

1．前言

2009 年 1 月 3 日，一个化名中本聪的人挖崛了比特币系统的初始区块，称为创世区块，他在创世块中刻下这样一句永不磨灭的话语："The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"，这正是泰晤士报当天的头版文章标题，意思是央行面临第二次救助银行的边缘。

分布式去中心化的比特币已经获得成功，作为比特币技术基础的区块链技术因其创造性及技术特质而被称为上帝链，目前炙手可热。相比中心化系统，它的数据完整性及准确性更值得信赖，它的交易处理更加安全、高效。区块链技术已经被广泛接受为下一代互联网价值互联网的基础，它将重构现代社会和商业文明体系，在包括金融、物联网、医疗、教育、贸易、社会管理等广泛领域获得应用。

比特币系统可靠性虽然已经获得广泛信任，但其区块及交易的数据结构相对简单，它仅包含实施其加密货币比特币交易的必须信息，无法满足其它广泛的业务需求。

目前，试图建立各种功能更完善区块链的项目开发如雨后春笋，不断涌现，比较著名的有以太坊、超级账本、R3 联盟区块链等，其它藉藉无名的更是数不胜数。成功的区块链系统不仅安全、稳定、可靠、功能完善，还要有足够多的互不信任的节点加入，这是一个非常艰难的挑战。

如果能将已经广受信任的比特币区块链功能扩展以满足其它各种业务需求将事半功倍，因而也有众多的开发者在比特币系统上绞尽脑汁。

一个公认的对比特币系统创造性拓展是侧链(Sidechain)技术，由 Adam Back 等人于 2014 年提出的侧链，是采用一种类似联系汇率机制，用多方签名(联名)账户的方式，将一定数量的比特币从主链转出锁定，使之以代币形式在侧链流通，并扩充侧链的数据结构，以便提供复杂的业务支持，其核心是维护新生区块链与比特币之间的双向价格锚定。

其实早在侧链之前的 2012 年，J. R. Willett 就发布了后来称万能层(Omni Layer)的 Mastercoin 白皮书，方法就是从上帝链引出比特币，并将引出地址称为出埃及(Exodus)，如同摩西遵从上帝旨意出埃及，白皮书强调这并不是背叛比特币，而是对比特币的发扬光大，其特色是比特币协议依旧是万能层的底层协议，万能层节点具备比特币全节点的所有功能，其实万能层就是侧链的特例。

侧链及万能层的思想值得肯定，但其核心思想依然是从金融服务角度维护一个货币体系，对服务于诸如供应链、医疗、物联网等领域应用仍然存在障碍。

有没有一种更简单实用的办法，扩充作为上帝链的比特币区块链功能以满足任意复杂的业务需求？

本质意义上，区块链应当只有一条，作为上帝链的比特币区块链应当是唯一。

本文将介绍一种全新的地址化原始数据密钥(Addressed Raw-data Key)概念，简称方舟(ARK)，一种借助比特币交易签名验证外部数据块并以 ARK 构建方舟块及方舟链的方法，不同于侧链及万能层主要着眼于价值的链外转移及协议层维持，方舟块则着眼于链外数据的完整性确认及工作流控制，价值管理仍然采用主链货币体系，仅以松散而可信任的方式建立起任何形式的资产与比特币之间的关系，这将对上帝链绝对忠诚，却可以简化业务处理，也将大力推动主链比特币的广泛应用。

方舟，它是一把小巧的钥匙，却开启了区块链应用的宽广大门。

2．定义

主链 – 本文指比特币区块链，也称上帝链；

交易 – 主链中的交易记录；

外部块 – 外部与主链无关的数据块；

方舟(ARK) – 地址化原始数据密钥(Addressed Raw-data Key)的简称；

方舟块(Ark Block) – 通过地址化原始数据密钥建立主链交易签名验证关系的外部块；

方舟链(Ark Chain) – 由方舟块参与组成的区块链，也称方舟区块链(Ark Blockchain)；

全方舟链 – 所有块均为方舟块的区块链。

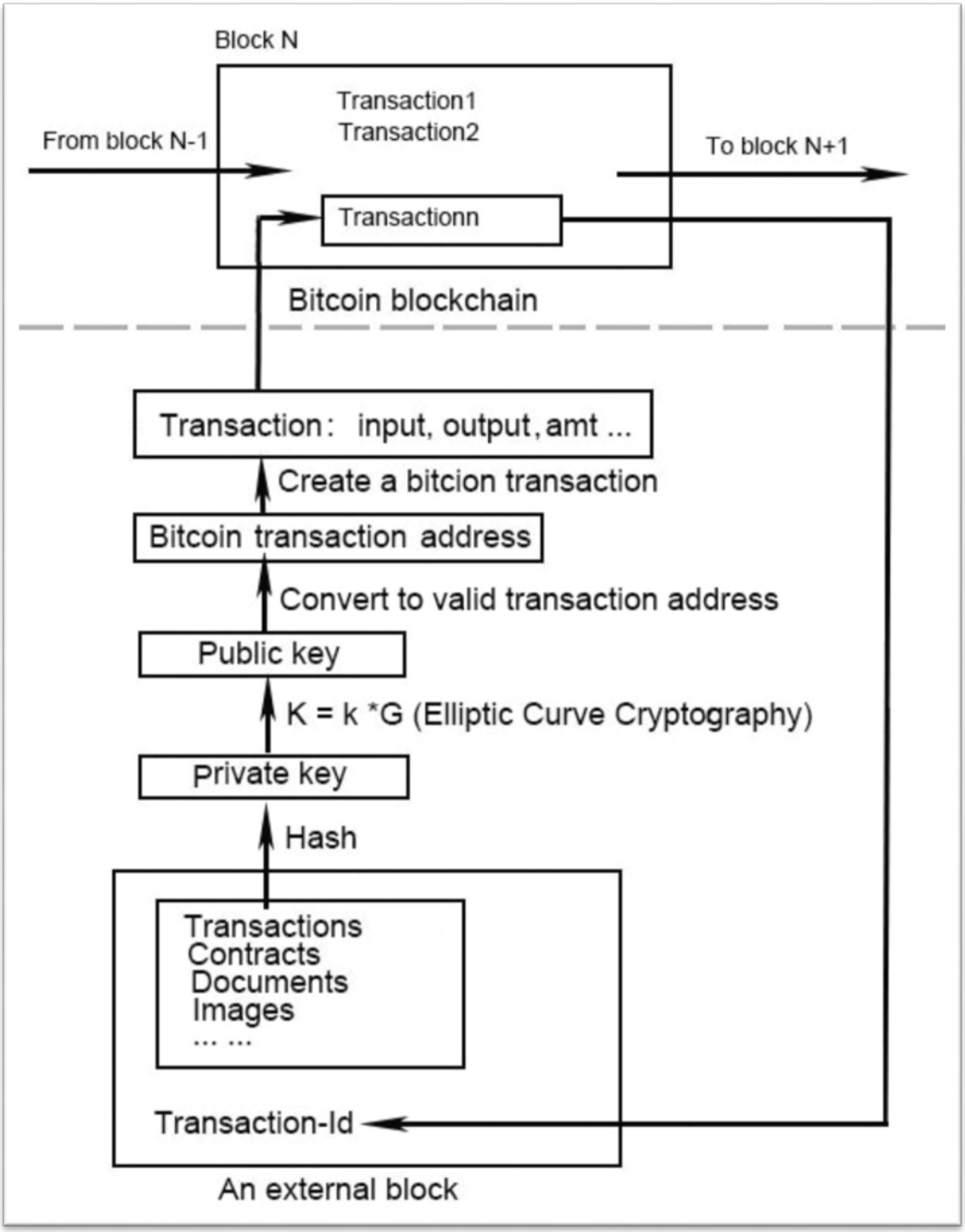
3．方舟块构建方法

对一个与主区块链无关的外部数据块作如下步骤的操作：

（1） 对该外部数据块的数据进行哈希(Hash)运算生成一个数字作为私钥 k；
（2） 将该私钥按主链的椭圆加密算法(K=G*k)运算生成公钥 K;
（3） 将公钥进行格式/制式转换、变换，生成符合主链要求的地址；
（4） 用这个生成的地址创建主区块链的交易(唯一地址或联签地址之一)；
（5） 将这个交易提交到主区块链，作为存档；
（6） 将主链交易号(ID)存入这个外部块。

方舟块中可以包含任意复杂的数据，包括交易、合同、文档、图像、视频、音频等，也可以是外部数据的 Hash，当然更有意义的是智能合约；而由数据产生的地址即可以是普通的交易地址也可以是数据输出地址。

方舟块的构造方法见下图示意：



方舟块构造方法示意图

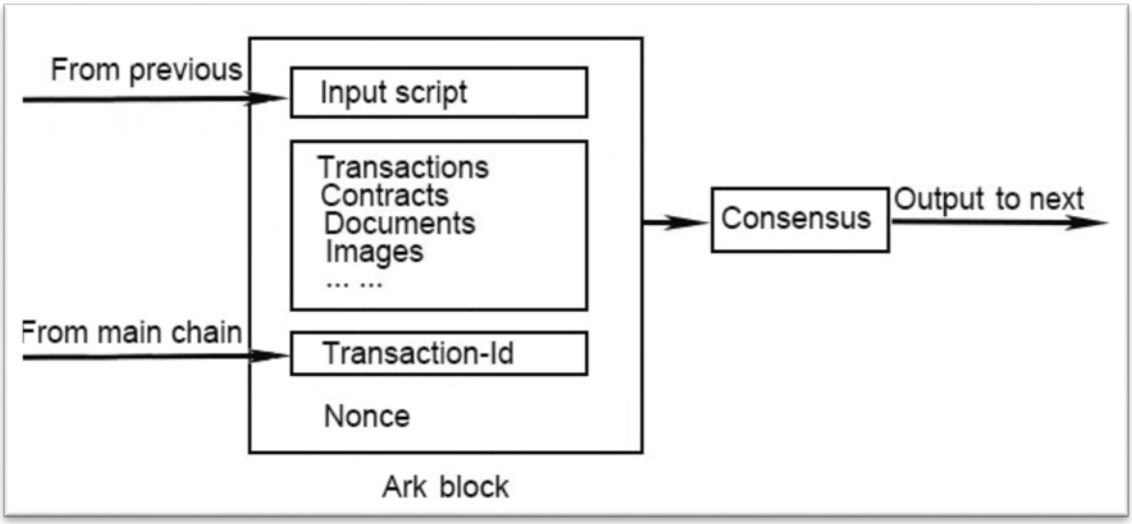
这样这个独立的方舟块就构造成功了，它的完整性由主链的交易地址签名保证，可以通过重复相同的过程进行验证，而交易是永久存放在主链上的。

方舟块数据可以存放在任何地方，电脑、手机、云服务器、智能卡均可，只要相关需要的人能取得即可，这使得精细化的数据可以信任且松散存储，并可以独立通过比特币系统进行验证。

4．继承性输出方舟块构造方法

很多情况下，我们需要将方舟块加入一条区块链以构造方舟链，为了强化主链签名验证的继承性，可以将主链的签名验证加入输出运算，使方舟块成为继承性输出方舟块，一般是将交易号(ID)作为参数之一，与前一个块的输出、当前块的数据一起按照共识机制参与运算，以生成该方舟块的输出。

见下图所示：



方舟链中的方舟块构造方法示意图

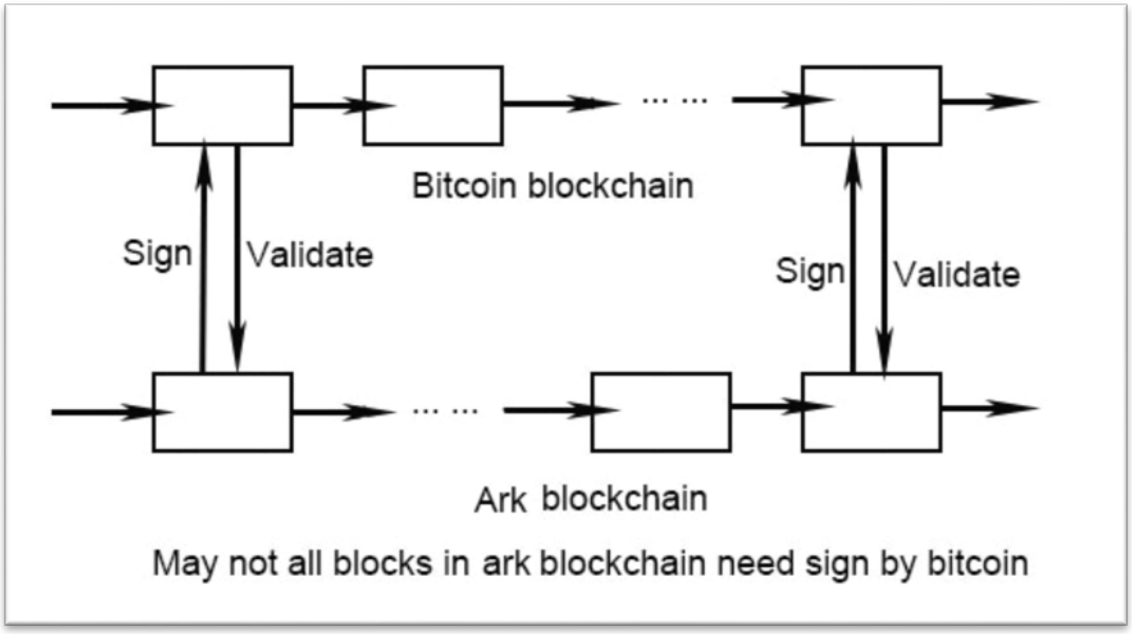
方舟链是一条服务于工作流的功能完善的区块链，由于借助主链交易签名对方舟块进行验证，且将交易号通过输出运算向下传导，因而，即使没有很多节点（服务器）参与，数据的完整性及可信任性也与主链相当。

5．方舟区块链构造方法

如果一条区块链中的所有块均是通过主链验证的方舟块，则这条链称为全方舟链。

实际应用中可能只有部份区块需要经过主链验证。

如下图所示：



由部份块经主链验证成为方舟块组成的方舟链

6．方舟块及方舟区块链应用前景

方舟块及方舟区块链的构建，使得数据完整性及可信任机制变得多样化，某种情况下可能仅需一个方舟块，比如颁发证书之类的单纯一次性交易过程；有时可能需要为一个有限的处理流程构造一个很短的依附于主链的局部区块链；当然更为常见且复杂的场景是，伴随着主链无限延伸的方舟链，甚至从方舟链上再衍生出另外的区块链，这样，仅从比特币这条主链，就可以缔造出一个无限延伸无所不能的节点可信网络，甚至通过节点中智能合约实现跨链节点间的通讯，则可能构成一个复杂拓扑结构的图，这样就已经突破了链的概念，构成为一个庞大复杂的生态体系，而其价值体系依然是比特币。

要人为构建这样的应用网络并不容易，但如果仅将协议限制于方舟块内部的智能合约，将方舟块及方舟链应用作为客户端设计成操作系统及浏览器组件，这样就可以使广域泛 IT 环境上架构了一个松散但可信任的层，而其核心就是作为主链的比特币，如果再配以若干骨干云平台分别作为独立海量存储器，这大概就是下一代互联网 – 价值互联网应有的样子吧？无处不在的节点数据，其完整可信任性可以即时通过主链进行验证。

设计这样一个体系的关键就在于基于方舟块的标准及智能合约。

当然首先要做的，是开发作为操作系统组件及浏览器插件的方舟块客户端，包括文件格式及数据库，以及作为其灵魂的智能合约规范。

方舟块的最大好处就在于，即使没有庞大的用户规模也是可信的，因为主链可信，而数据可以松散存贮，这也是形成规模化的前提。

7．结束语

方舟块及方舟链为比特币系统服务于广泛的实际业务需求开辟了道路，为数据松散式分布存贮以及为服务于形式多样的业务需求而并无众多节点参与的可信任区块链的建立，提供了有效手段，区块链的施展空间变得极其广阔，各种外延区块链及方舟块中的智能合约是应用技术关键。

本质上，应该只有一条真正意义上的区块链（Only one blockchain matters !），作为上帝链的比特币区块链就是唯一，其它区块链应该只是其拓展或侧链。如同诺亚遵从上帝旨意所造方舟一样，方舟块凭藉对主链的忠诚和借助于主链的承托而成为连接链内价值与链外数据完整性关系的载渡之舟，驶向未来社会及商业文明的海洋。

注：本文仅介绍基本概念，具体应用方法将在基础及应用开发白皮书公布，欲了解基础方舟区块链的详情，请关注: www.arkblockchain.org，项目开源（MIT 协议）托管于 github。

关于各型类型方舟链的共识机制，请关注共识联盟网站: www.ConsensusAlliance.org。

方舟区块链技术将率先应用于如下商业系统：

物联网支付平台：www.BindPay.com

定制电商平台：www.diyPlant.com

电子医疗门户：www.eMedHub.com

问题咨询: paul@bindpay.com

参考文献：

1. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
2. Omni Layer Specification, https://github.com/OmniLayer/spec
3. Enabling Blockchain Innovations with Pegged Sidechains, Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille∗† 2014-10-22 (commit 5620e43)
4. Blockchain – Blueprint for a new economy, Melanie Swan
5. Mastering Bitcoin, Andreas M. Antonopoulos, O'REILLAY, First Edition, December 2014.
6. The Business Blochchain – promise, practice and application of the next internet technology, William Mougayar