DOI:10.19729/j.cnki.1009-6868.2018.06.004
网络出版地址:http://kns.cnki.net/kcms/detail/34.1228.TN.20181114.1306.002.html

区块链概念剖析及其在物联网中的部分应用

Concept and Partial Applications of Blockchain in Internet of Things

田海博/TIAN Haibo
(中山大学,广东 广州 510275)
(Sun Yat-Sen University, Guangzhou 510275, China)

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868 (2018) 06-0019-004

摘要: 把去中心化、不可篡改和激励机制定义为区块链技术的典型特点,而把可追踪、匿名和可编程定义为区块链技术的功能特性,同时分析了每一个特点和特性的底层支撑技术,以更好地判断区块链项目的真伪及可实现性。在该定义的基础上,分析了物联网(IoT)场景下几个典型的区块链项目,并对其中的一些主要问题和主要方法进行了详细阐述,认为IoT的数据体量和数据安全问题依旧是需要重点考虑的问题。

关键词: 区块链;支撑技术;IoT应用

Abstract: The decentralization, non-tampering and incentive mechanism are defined as the typical features of blockchain technology, and the traceability, anonymity and programmability are defined as its functional characteristics. Then the underlying supporting technologies of each feature are analyzed to better judge the authenticity and realization of blockchain projects. Further, several typical blockchain projects in the Internet of things (IoT) scenario are analyzed, and main problems and technical methods are described. It is pointed out that the data volume and data security of the IoT are still the key issues to be considered.

Key words: blockchain; supporting technologies; IoT applications

中本聪提出一种点到点的现金系统[1],并在2009年公开了源代码。通过社区的推进,人们开始尝试使用比特币进行支付,第一个例子就是使用一万个比特币购买一个披萨。比特币源于社区,并自带粉丝,社区内成员自我铸币、自我消费。继比特币之后,出现了如莱特币[2]、点点币[3]、名字币[4]等以各种名目发行的密码货币,因其总量固定,所以粉丝越多其汇率越高。

GAVIN W[5]在2014年对比特币做了2个改进:第1个是提供以太坊虚拟机(EVM),用于执行任意用户自定义的代码,实现智能合约;第2个就是把比特币中存放在未花费输出交易(UTXO)中的货币和状态、代码存放在一个账户下面,即所谓的账户模型。以太坊的出现,极大地简化了人们发行新币的过程,于是区块链领域上演了一场初始代币发行(ICO)的大剧,各类项目良莠不齐。

IBM开发的Fabric[6]看到了另外一个生存空间,那就是避开以太坊,构造联盟链,在企业中运行。得益于IBM的代码质量和一贯良好的形象,Fabric很快在联盟链中占据了主导地位。Fabric的特点是不用密码货币,转而用节点背书,其中每个节点的身份可以识别,不诚实的节点需要付出代价。目前在大部分所谓落地的应用中,例如:银行、供应链、积分、税务等场景,无一例外地采用了联盟链的模式。

区块链是内生在比特币中,用于记录比特币交易,所以有时称之为账本。ARUIND N等人[7]从数据结构上看,认为区块链就是一个用哈希指针取代了内存指针的一个链表。PASS R等人[8]从协议上看,认为区块链就是一个协议,协议参与者各自本地维护的一个数据列表称为链,参与者把收到的消息包含在自己的和其他所有参与者的链中。这些定义各有其优缺点,例如:ARUIND N的定义没有考虑共识,PASS R等人的定义专门用于比特币。

本质上,区块链由一组基于点到点(P2P)网络的节点形成,各节点通过执行共识算法,维护其各自数据的一致性。去中心化、不可篡改和激励机制通过该定义可以体现。其中,P2P网络和共识算法是去中心化的具体体现,也是不可篡改的前提和必要条件,激励机制则是各节点维护其数

收稿日期:2018-10-22
网络出版日期:2018-11-14
基金项目:国家重点研发计划(2017YFB0802500)

据一致性的动力所在。可追踪、匿名、可编程这些特点则是对区块链的一致数据赋予语义之后得到的功能特性。我们下面对区块链技术进行分析，指出其典型特点和功能特性的技术支撑，然后再探讨区块链技术在物联网（IoT）场景的几个应用。

1 区块链典型特点

区块链技术的典型特点包括去中心化、不可篡改和激励机制。

1.1 去中心化

去中心化属于区块链技术的基本属性，是区块链技术和其他技术得以区分的基本特点。去中心化既有物理基础又有组织形式，具体如下：

（1）物理基础

比特币、众多山寨币和一些无币区块链项目大都会坚持使用P2P网络，这其实是去中心化的物理基础。我们知道纯粹的P2P网络是没有服务器角色的，每个节点既是服务器又是客户端，彼此地位均等。这种地位均等与设备的计算能力、网络带宽等无关。

（2）组织形式

在P2P网络之上，基于比特币的工作量证明（PoW）算法，比特币中每个节点潜在地具有记账的权力，这是一种表面的去中心化，因为这种权力与节点的算力等资源密切相关。事实上，比特币网络中记账的权力集中在几个大矿池手中，是一种联盟记账的模式。成为这个特定联盟的节点并不需要其他节点的允许，而是单纯地依靠算力比拼，可以称之为无组织算力联盟。我们使用无组织这个词汇，是因为在这个联盟中，各个成员节点是纯粹的竞争性关系，不存在哪一个矿池服从其他矿池的情况，这与一般的由某个企业或者单位主导形成的联盟有所不同；在基于其他共识算法的区块链中，具有记账权力的节点首先是独立的，然后节点之间依靠某种规则确定记账节点的集合，形成一个动态的记账联盟，与比特币的最终形态是类似的，不同之处在于不依赖PoW的记账联盟往往则需要某种集体许可的机制，这是一种有组织的联盟。

1.2 不可篡改

数据不可篡改是区块链中数据的基本属性，我们分基于PoW、基于数字签名和基于数据冗余3部分来阐述。

（1）基于PoW的不可篡改

对于采用PoW的区块链技术，每一个区块的生成背后都有算力的竞争，进而有区块难度的概念。区块难度基本表明了一个区块生成时生成该区块的节点所需要付出的计算代价。因此，给定一个比特币区块链，任何设备想要重新生成一条具有同等难度的区块链都必须付出同等的累积计算力量。鉴于比特币区块链消耗的巨大计算资源，在计算能力没有本质突破的前提下，任何设备都难以承受重新生成一条区块链的代价。因此，比特币区块链的数据拥有者们只能删除自己存储的数据，而无法对其进行任何修改；而单个节点对数据的删除，并不会改变其他节点拥有的数据副本，因而比特币网络中的数据具有非常强的不可篡改性。

（2）基于数字签名的不可篡改

权益证明（PoS）是根据节点权益决定区块的生成节点的一种共识算法。当PoS共识指定某个节点充当区块的生成节点时，该节点通过数字签名表明该区块是其生成的。因此基于PoS的区块链是一种由数字签名保护的区块链。给定任意一个PoS区块链，一个节点可以删除数据，也可以自己生成很多的公私钥对，进而形成一个具有不同数字签名的伪区块链。与基于计算难度的区块链不同，这个伪区块链只能通过验证数字签名来区分，进而需要PoS区块链明确哪些公钥是属于这个区块链的，哪些是合法的。只有这些明确了，才能明确哪一个PoS区块链是真的，哪一个是假的。在一个PoS区块链有明确的参与节点边界之后，单个节点的数据删除并不会影响其他节点的数据副本，因而数据具有不可篡改性。如果这个节点边界的范围非常小，并且所有节点的数据都被删除了，数据就真的从这个区块链删除了，这就是明确的边界带来的代价。

（3）基于数据冗余的不可篡改

采用拜占庭容错类算法的区块链或直接采用修改的分布式数据库技术保持数据一致性的区块链，如果不采用数字签名，其数据的不可篡改性只能来自数据冗余。任意节点可以修改自己的本地数据，但是节点是独立的。一个节点删除或修改自己的数据并不影响其他节点，因而当查询一份数据时，多数节点给出的结果就是该数据的真实情况。此时数据的不可篡改依赖维护一个区块链的诚实节点的数量。我们再次强调节点独立的重要性：对于一些直接采用了分布式数据库技术的区块链项目，经过测试，维护分布式数据库的节点并不是独立的，因而任意有权限的节点删除数据会使得其他节点“同步”地删除数据，这样的区块链项目是没有不可篡改性的。类似地，由单个企业或者单位维护的区块链项目，其不可篡改性是需要质疑的。

1.3 激励机制

激励机制在区块链中有重要的作用，它使得人们对联盟节点的行为可以预期，进而产生信任。以无组织算力联盟为例，联盟成员一般不会特意地阻断某一个交易，联盟成员会努力计算，期望自己获得区块的奖励。这种可预期的行为是信任产生的基础。所以区块链的可信与区块链节点行为的可预期相关，而行为的可预期则与激励机制相关。比特币长期的实践经验告诉我们：激励良好且相互制衡的联盟成员行为可以预期、可以信任。在有组织的联盟中，激励机

制同样是不可或缺的，在其治理下，可以使用奖惩的方法，并且形式也可以多样化，可以不使用货币，形成所谓的无币区块链项目。

在有币的区块链项目中，激励机制是否有效取决于项目的代币是否可支付，例如：比特币的可支付来自社区内的认同。众所周知，有一万个比特币换取披萨的事情，那么为什么是一万个不是五千个呢？我们可以推测持有比特币的一方用电费来衡量自己获取的比特币在当时的价值，披萨的销售者一方面必然是比特币社区的成员，一方面还可以用电费衡量披萨的价值，于是你情我愿之下，才会有这样的一笔交易。我们特别推测了披萨店主应该是比特币社区的成员，或可以说是比特币的粉丝；否则，这笔交易是不会发生的。所以我们认为认同是支付的前提。如果项目的参与者对项目不认同，可支付性降低，激励机制失效，那么这个项目就很难有效地运行。

1.4 功能特性

区块链技术的基本特点是区块链得以成为区块链的关键，而功能特性则是对数据进行不同的语义赋值之后得到的特性，例如：可追踪、匿名和可编程。

（1）可追踪

当区块链中的数据彼此具有链接关系时，就有了某种可追踪性。以比特币为例，一个新生成的比特币交易中包含输入交易的哈希值，输入交易也是交易，也包含其输入交易，以此类推，可以直接推到多个铸币交易。那么，从铸币交易集合到新生成的这个比特币交易就形成了一棵树，树根是新生成交易，树上的任意一笔交易都与新生成的交易相关。然而，在不使用区块链技术的情况下，一个中心化的服务器也可以使用这种链式关系来形成其存储数据的可追踪性。因此，可追踪性只与具体的数据结构以及应用的语义有关系。

（2）匿名

区块链中的数据都是有来源的，在大多数项目中，这个来源只能使用一串公钥标识出来。公钥是可以任意生成的，因而与人或物的一些真实身份信息没有直接的对应关系，因而具有了某种匿名性。比特币提供的这种匿名准确一些叫做假名。一个实体可以随便生成公钥，但公钥与资产绑定后，通过交易的可追踪性可以大概率地通过一些简单的聚合算法找出一个实体的不同公钥。这些公钥尽管还不能直接对应到人，但再加上一些交易时间分析、IP地址分析和社会工程学方法，终究还是可以把人找出来，因此比特币的这种假名技术并没有提供太多的保护。有许多的项目致力于提高匿名性，提供真实匿名的系统，例如：零币，可以隐藏交易金额、实体等信息，具有更好的匿名性。匿名性是对数据的语义分析之后得到的某个项目是否保护参与实体身份等信息的安全属性。

（3）可编程

比特币提供的脚本语言可以让交易方明确比特币转移的条件；而脚本语言本质上是一种编程语言，因而人们一般认为区块链资产具有可编程的特点。以太坊的出现强化了人们的这种观念。以太坊提供了一个准图灵机，让人们可以自定义智能合约，以完成资产的管理。智能合约是一种技术手段，随着合约内容涉及的应用领域不同，出现了对保险、供应链、公证等诸多社会生活领域的智能合约，因而出现了所谓可编程社会的观点。事实上，可编程也可以看成对数据的语义赋值之后的功能特性，只不过现在维持一致的数据包括了“代码数据”而已。

以上我们把区块链的技术特点分为去中心化、不可篡改、激励机制3个，并把可追踪、匿名、可编程看成区块链数据的语义赋值。通过这些分析，我们自然地可以把单个企业提供的“区块链”服务、“云区块链”等项目与真正的区块链项目区分开。

2 区块链技术在IoT中的部分应用

IoT场景有2个典型特点：数据量大，设备无时无刻不在产生数据；数据安全很重要，因为IoT数据可以与工控安全、居家环境等现实社会的生产生活建立直接的关联，因而其数据的机密性、完整性和可用性是必须要考虑的。区块链技术所保障的仅仅是数据的完整性，为数据的可用性提供了便利，但是并没有对数据机密性进行任何的考虑。下面我们选择几个典型的IoT场景区块链项目来分析区块链技术在IoT中的应用。

2.1 IOTA技术

IOTA[9]是区块链技术在IoT中应用的一个主要代表，主要考虑了IoT数据体量的问题。IOTA技术的白皮书主要披露了一个纠缠（Tangle）账本。纠缠账本是一种基于有向无环图（DAG）的分布式账本底层技术，其基本安全假设为：攻击者生成交易的速度需要小于诚实网络节点生成交易速度的和。在这一假设下，为了鼓励诚实节点生成交易，不收交易费。考虑到IoT设备生成的数据体量较大，不收交易费也就成了该技术适用于IoT的一个主要原因。

纠缠账本的问题集中在账本安全性和激励机制2个方面：在账本安全性上，交易速度的假设还需要实践检验；在激励机制上，在没有交易费的情况下如何激励节点存储大量的IoT交易也是需要经过实践检验的。

2.2 沃尔顿链

沃尔顿链[10]是一个结合硬件的IoT应用项目，考虑了IoT数据的产生和管理问题。该团队开发出了区块链读写器，可以把标签数据的哈希值通过读写器直接写入区块链中。同时读写器与标签具有双向认证的功能，可以确保数据的来源是经过认证

的。对于数据量较大的问题，该团队构思了跨链架构，希望该架构能承载众多不同形态、不同应用场景的子链。该项目的跨链思路还需要实践检验。

2.3 智能混杂网络（SMT）项目

SMT项目[11]，致力于为移动设备提供一个有激励措施的通信平台，其考虑更多的是IoT的数据通信方式的问题。从愿景上看，该项目希望提供一个平行于互联网的全球移动设备通信平台。从技术组成上看，该项目基于以太坊，准备采用雷电网络的技术支持移动设备之间的“链下”支付。该技术特点与愿景是有矛盾的，因为雷电网络终究是不能离开以太坊的在线支持。该项目的激励措施在于转发数据可以获得奖励，但白皮书中并没有披露具体的奖励算法，毕竟数据的来源往往是一个用户，而参与转发的则涉及多个用户。另外，IoT场景中的通信问题是否是一个关键性的问题还需要实践检验。

2.4 Streamr项目

Streamr项目[12]，意在基于以太坊智能合约建立一个适用于IoT的数据产生和消费平台。IoT设备作为数据产生的源头，把经过接收方公钥加密的数据发送给该网络的中介节点。不同的中介节点群处理不同的IoT数据，形成可扩展的架构。中介节点群之间的管理通过以太坊智能合约实现。数据接收方通过中介节点获得加密的数据，并通过自定义的该项目的合约平台完成数据处理。然而，以太坊作为一个一般性平台，最近一直受到交易速度的困扰。该项目底层完全依赖以太坊，其基本的交易处理速度受限于以太坊，因此在IoT中的实用性还需要进一步的检验。

2.5 Ruff项目

Ruff项目[13]，把边缘计算的概念和区块链结合在一起，提供了统一的IoT应用接口，并提供IoT主控设备和受控设备的全局管理，它属于IoT数据应用层面的项目。该项目中轻节点代表具体的IoT受控设备，该设备通过存储主控设备的公钥来识别主控设备的命令。通过智能合约，主控设备可以把受控设备的部分功能以租赁或转移的形式提供服务。该项目搭建自己的公链，采用了股份授权证明（DPoS）共识算法，每轮选择105个节点参与区块生成。该公链能否承载其设备租赁的服务模式，还需要在实践中检验。

以上我们对几个典型的以IoT为应用场景的区块链项目进行了分析，可以看到目前人们对于IoT场景下数据量较大、数据较为敏感的问题已经有了初步的建议方案，另外对IoT的通信方式、数据使用方式、数据生成方式进行了积极的探索。

3 结束语

本文中，我们提出去中心化、不可篡改和激励机制属于区块链技术的本质特点，而可追踪、匿名、可编程属于区块链数据之上的功能特性，以此可以区分一些区块链项目和借区块链概念的项目。进一步地，我们分析了区块链技术在IoT场景的几个应用，对其中的主要问题和主要方法进行了阐述，指出IoT的数据体量和数据安全问题依旧是区块链技术在IoT场景应用需要重点考虑的问题。

参考文献

[1] SATOSHI N. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. [2018-10-22]. https://bitcoin.org/bitcoin.pdf
[2] QIWEI L. Litecoin – Open Source P2P Digital Currency [EB/OL]. [2018-10-22]. https://litecoin.org
[3] KING S, NADAL S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [EB/OL]. [2018-10-22].https://peercoin.net
[4] Namecoin [EB/OL]. [2018-10-22].https://github.com/namecoin
[5] GAVIN W. Ethereum: A Secure Decentralised Generalised Transaction Ledger [EB/OL]. (2018-11-08)[2018-10-22]. https://ethereum.github.io/yellowpaper/paper.pdf
[6] Hyperledger Fabric [EB/OL].[2018-10-22]. http://hyperledger-fabric.readthedocs.io/en/release-1.1
[7] ARVIND N, JOSEPH B, EDWARD F, et al. Bitcoin and Cryptocurrency Technologies A Comprehensive Introduction [M]. Princeton: Princeton University Press, 2016
[8] PASS R, SEEMAN L, SHELAT A. Analysis of the Blockchain Protocol in Asynchronous Networks [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. France: Springer International Publishing, 2017, (10211):643-673
[9] SERGUER P. The Tangle [EB/OL]. (2017-10-01)[2018-10-22].http://www.docin.com/p-2088809407.html
[10] Waltonchain. Waltonchain White Paper [EB/OL] [2018-10-22]. https://www.waltonchain.org/templets/default/doc/Waltonchain White Paper 2.0_CN.pdf
[11] SMARTMESH. The Smartmesh whitepaper [EB/OL].[2018-10-22]. https://smartmesh.io
[12] STREAMR. Unstoppable Data for Unstoppable Apps: DATAcoin by Streamr [EB/OL]. [2018-10-22]. https://www.streamr.com
[13] ROY L. Ruff IoT Blockchain Whitepaper [EB/OL]. (2017-10-01)[2018-10-22].https://github.com/RuffNotes/RuffChain/blob/master/WhitePaper.md

作者简介

田海博，中山大学数据科学与计算机学院副教授、网络空间安全系副主任；主持国家自然科学基金项目、教育部基金项目、广东省自然科学基金项目等，作为骨干人员参与了国家重大研发计划网络空间安全专项2项；目前已发表论文60余篇，公开专利30件，参与起草已发布的行业标准1部。