清 华 大 学

综 合 论 文 训 练

题目：基于区块链和手机传感器的车辆位置验证

系　　别：计算机科学与技术系

专　　业：计算机科学与技术

姓　　名：李玮祺

指导教师：向　勇　副教授

2020 年 6 月 11 日

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：学校有权保留学位论文的复印件，允许该论文被查阅和借阅；学校可以公布该论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存该论文。

(涉密的学位论文在解密后应遵守此规定)

签　名：_____ 导师签名：_____ 日　期：_____

中文摘要

车载自组网是在交通环境参与者间构建的开放式网络，可以为用户提供去中心化的数据传输能力。基于车载自组网，可以实现事故预警、辅助驾驶、道路交通信息查询、车间通信和网络接入服务等应用。这些应用对于数据和地理特征的联系较为紧密，但也存在着一定的安全隐患。针对这一问题，本文利用部署在车载自组网上的区块链网络，开发了一套车辆位置验证及信誉评估系统以完成车辆的位置验证。

首先，本文选用 GeoHash 作为系统中统一的位置信息表示方法，分析了引入 GeoHash 所带来的系统误差，并开发了基于 GeoHash 的几何计算函数。在系统实现上采用浏览器与智能合约相结合的方式，在浏览器端实现计算量较大的数据采集和基于 GeoHash 的位置修正和道路匹配工作，车辆的信誉评估工作则实现在智能合约端，充分利用了区块链的性质保证车辆信誉数据的安全性、可溯性和在网络内的同步性，并可以为其他使用用户位置信息和信用情况的应用提供数据支持。最后通过使用真实的 GPS 数据对系统进行测试，验证了该车辆位置验证和信誉评估系统的可行性。

关键词：车载自组网；区块链；道路匹配；智能交通系统；GeoHash

ABSTRACT

VANET is an Ad-hoc networks between participants in trafic and providing decentralized data transmission service. VANET can be uesd in application like accident warning, drive assist system, trafic information service and Inter-Vehicle Communication. These applications are closely relevant to geographic information and have potential safety problem. To solve this problem, this thesis uses blockchain deployed in VANET and develops a vehicle position verification and reputation evaluation system.

First, this thesis use GeoHash for storage and calculation of position. Then analyzes the error of GeoHash and develope geometric calculation functions base on GeoHash. The system in this thesis is made up of browser-side programs and smart contract. The browser-side programs gather position data, find the actual road vehicle on and correct the location data, then the smart contract calculates the reputation of this user. Blockchain makes this step safe, traceable and synchronized. This system can also provide reputation data for other applications. Finally, the thesis uses real GPS data for test and analyzes feasibility of the system.

Keywords: VANET; Blockchain; Map-matching; ITS; GeoHash

目 录

第 1 章　引言

1.1　课题背景

随着城市交通的发展和汽车保有量的增加，为了更好地利用蕴含在大量运行车辆中的信息并提供更加安全高效的交通环境，智能交通系统的概念应运而生。在智能交通系统中，车载自组网（VANET，Vehicular Ad-Hoc Network）占有了重要地位。车载自组网是指在交通环境参与者（车辆与车辆、车辆与道路设备、车辆与行人等）之间相互通信组成的开方式移动 Ad-Hoc 网络，并能提供去中心化的、自组织的数据传输服务。基于车载自组网，可以实现事故预警、辅助驾驶、道路交通信息查询、车间通信和网络接入服务等应用。

区块链技术最早由中本聪与 2009 年首次提出，是一种随着比特币等数字加密货币的日益普及而兴起的一种全新的去中心化架构和分布式计算范式，随着区块链技术的发展，其从金融市场出发，逐渐引起了政府部门，科技企业的重视和关注，区块链技术具有去中心化、时序数据、集体维护、可编程和安全可信等特点，特别适合构建可编程的货币系统、金融系统乃至宏观社会系统[1]。最近，由于对区块链兴趣的爆发式增长，区块链与物联网领域相结合的研究也逐渐增加。有了区块链，以前只能通过可信中介运行的应用现在也能运行在非集中系统上，不需要一个权威中心，并能够以相同的确定性实现相同的功能。这与车载自组网的一大特性——去中心的分布式结构不谋而合[2]。将区块链技术运用到车载自组网中，能够利用其不可篡改性、可追溯性等安全特性，为车载自组网中的陌生节点信任问题提出一种解决方案。

然而，车载自组网中车辆对数据的需求具有较高的地理特征，同时，基于车间信息交流的路况查询、事故预警等应用也与自组网参与者所提供的位置信息息息相关。因此，考虑在提供区块链服务的车载自组网络上研究实现一套车载自组网中的位置验证系统，增强其安全性和扩展应用场景。

1.2 相关调研

1.2.1 车辆位置验证

目前主流的车辆位置系统是传统的集中式验证，需要中心服务器统计网络中的车辆行驶数据，对车辆提供的位置信息进行确认[3-4]。这种系统的优点是中心服务器具有绝对的权威，车辆终端仅需要提供自己的行驶数据，即可从服务器获得所需数据。但集中式验证在面对日益增加的车辆数量时承受着巨大压力，同时该方法通常由一定程度的延迟（包括数据传递的延迟和服务器计算的延迟），而在自组网的应用中，数据的实时性十分重要，尤其是预警和路况查询等应用。一种解决方法是利用路侧单元（RSU，Road Side Unit）进行位置验证，车辆通过与路侧单元进行通信留下自己的位置信息，同时路侧单元之间通过互联网交换车辆信息。这一系统一定程度上解决了集中式验证带来的服务器压力，同时路侧单元的地理信息固定且准确，路侧单元之间的网络也可以通过有线网络实现，极大程度地提高了系统效率[5]。但基于路侧单元的车辆位置验证需要极大的前期基础设施投入，在短时间内建立大规模的车辆验证服务系统存在一定难度。另外存在一种通过邻居车辆进行验证的位置确认系统，近邻节点通过私钥加密的短距通信确认双方关系，并将该关系广播到互联网中[6]。该系统虽然不需要额外基础设施的参与，但要求参与车辆拥有一定的短距通信设备[7]。此外还可以根据车辆自身位置信息进行验证，主要通过分析车辆历史轨迹、速度，分析数据的合法性，检测车辆的可信程度，这种方式的好处是系统结构简单，对环境依赖小[8]。

1.2.2 道路匹配

现有的道路匹配算法一般可以分为如下四类：几何算法、网络拓扑算法、概率统计算法以及高级算法[9]。几何算法主要考虑道路的距离、角度等信息，如点到点、点到线的位置关系等，实现简单，匹配速度快，但无法处理复杂的路口和多条道路并行时的数据，精度较低。网络拓扑算法在进行道路匹配时利用车辆的行驶方向和道路拓扑信息进行匹配，利用道路间的连接关系、行驶方向等信息，比纯几何算法一定程度上提高了精度。概率统计算法利用不同的评价指标对一定范围内候选道路进行概率分析，以此进行道路匹配，评价指标可以包括车辆位置和轨迹、周围路网等，算法的效果受到参考信息的选择和相关参数调节的影响较大。总体上来说这些算法较为简单，对于密集道路情况的处理能力较差，而高级算法引入了一些成熟的模型进行道路匹配，或者使用机器学习算法等，这些算法精确度较高，但实时性较差[10-11]。

1.2.3 地理位置表示

在传统的地理位置表示中，普遍使用了经纬度坐标系统，它是一种球面坐标系统，某地经度是其所在南北方向大圆与 0° 经线所在大圆的夹角，纬度是其所在位置与地心连线和赤道平面的夹角。因为这是一种球面坐标系统，需要计算两点间距离时要利用到球面距离公式，涉及了较为复杂的三角函数计算。

GeoHash 是一种比较新的地址编码方式，它将传统的二维经纬度编码转换成一维的字符串，同时给地理位置进行了分区。在位数较少时，它可以用来表示某一区域在地球上的坐标，在位数足够时，它也可以用来表示某个具体点在地球上的坐标。GeoHash 在编码的过程中保留了一定的相对地理位置信息，在大部分情况下，GeoHash 编码共同前缀越长的区块物理距离越近。

1.2.4 区块链和智能合约

区块链是一种新兴的互联网应用模式，利用其分布式、去中心化、点对点、集体维护、共识机制等特点被使用到不同领域中。比特币在区块链网络上实现了一种去中心化的货币，而其它领域也有区块链的应用，如医疗、公共事业、房地产、政府等[12-14]。

智能合约是部署在区块链上自动运行的程序，它能接受信息并按全网统一的规则执行相应的计算。其具有去中心化和自动执行的特点，因为不易被篡改且能持久地保存数据，在很多领域进行了应用。有很多区块链平台上实现了智能合约功能，目前比较多使用的是以太坊上的智能合约。

1.3 论文的研究内容及贡献

本文实现了一套车载自组网中的位置验证系统，通过对用户节点进行信誉评价进行节点的认证工作，同时系统得到的信誉值在需要时也可以可信比例来参与其他应用计算。

（1）针对以太坊区块链上智能合约对小数计算和复杂数学函数支持较弱的情况，系统中采用 GeoHash 作为位置表达方式，为了在程序实现时选择合适的 GeoHash 位数，论文对引入 GeoHash 所带来的误差进行了分析，并开发了基于 GeoHash 的几何计算函数以充分利用 GeoHash 所带来的计算简化。

（2）针对 GPS 传感器所获取位置信息存在一定误差的情况，实现了在线利用历史位置及周边道路情况进行位置修正程序。系统依据 [15] 中提及的概率统计道

路匹配算法，实现了实时的道路匹配和位置修正系统。

（3）编写区块链上的智能合约，通过接收用户上传的实时位置等信息，根据数据的合法性、有效性、持续性等因素，评估并更新用户信誉值，以此完成用户位置验证。

第 2 章　基于 GeoHash 的位置表示

为了简化合约中的距离相关计算，加速基于邻近路网的位置修正，在本文实现的车辆位置验证系统中采用 GeoHash 代替传统的经纬度坐标作为地理位置的表示方法。本章主要对 GeoHash 进行介绍，同时说明在修正车辆位置坐标时利用 GeoHash 加速道路匹配过程的方法。另外本文对采用 GeoHash 进行表示坐标时引入的误差进行分析，并实现了基于 GeoHash 的几何计算用于车辆位置修正和合约中的用户信誉值更新评估。

2.1　GeoHash 简介

Geohash 是由 Gustavo Niemeyer 和 G.M. Morton 发明的一种地理编码系统，它将地理位置编码为一个固定长度的字符串，被广泛应用于基于地理位置的应用中。GeoHash 使用了 Peano 曲线来填充空间（图 2.1），在编码时首先将经纬度坐标分别转换成二进制串，二进制串的每一位取决于坐标点在根据经纬度二分后的位置所属。之后将得到的经纬度二进制串交替组码，最后利用 Base32 编码将组码后的二进制串转换为字符串进行存储。一个 GeoHash 值对应一个近似矩形的覆盖区域，编码长度越长，区域范围越小，同时编码相近的两个区块在地理位置上通常也距离较近。因此 GeoHash 在一定程度上保留了原有的地理位置信息，

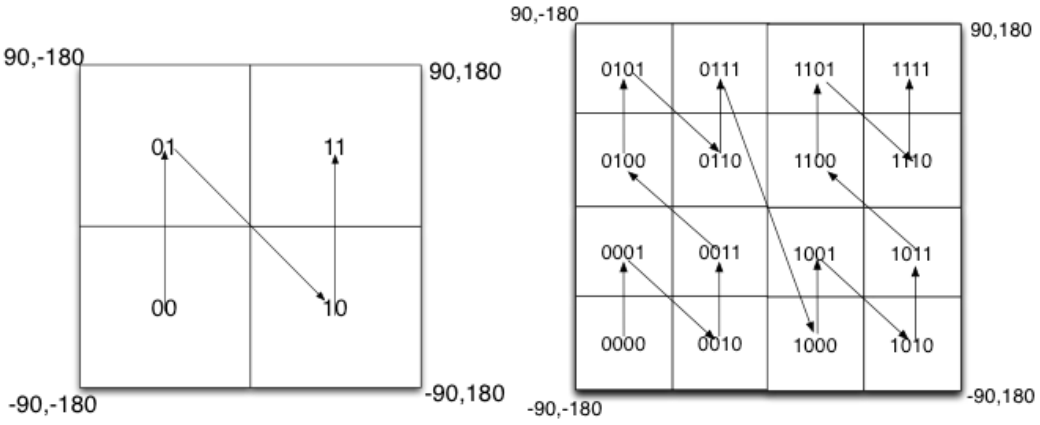

图 2.1　GeoHash 利用的 Peano 曲线编码，编码长度分别为 2 和 4。

2.2 基于 GeoHash 的地图存储

一方面由于智能合约语言 Solidity 的限制，在智能合约中不方便定义树状结构，另一方面在寻找坐标点附近的所有道路时，若采用传统经纬度坐标存储道路，需要对大量道路进行距离计算和筛选，对计算终端的性能需求较大。以上两个问题，若在存储道路信息时将道路位置设计的坐标点（包括起始点、结束点、中间节点）统一采用 GeoHash 存储，能得到较好解决。利用 GeoHash 字符串存储道路可以将道路信息平面化，避免了树状结构的应用。同时，根据 GeoHash 编码的定义，一个 GeoHash 值所表示的区域一定包含在该 GeoHash 值前缀所表示的区域内。

在存储地图时，我们将地图划分成精度较低、范围较广的 GeoHash 块，并储存对应 GeoHash 块中所包含的所有路径。因此寻找某一具体 GeoHash 表示的坐标附近的道路信息只需要取其坐标前缀至数据库中查询。但是值得注意的一点是 GeoHash 编码的边界问题。如图 2.2中，与红色点最近的点是位于相邻块的绿色点而不是位于同一块的蓝色点。因此除了使用定位点的 GeoHash 编码进行匹配外，还使用周围 8 个区域的 GeoHash 编码进行查询。使用这种道路查询方式可以很大程度上缩减寻找坐标点附近道路数据的所需时间，为在算力有限的移动终端上部署该系统创造了可能。

2.3 GeoHash 误差分析

由于 GeoHash 值所对应的是地理位置上的一块区域，在用 GeoHash 表示精确坐标时，会引入一定的误差。本节估算了这一误差的大小，并据此选择了在程序实现中所使用的合适的 GeoHash 位数。

在 GeoHash 位数较多的情况下，所得对应的区域较小，可以忽略由地球表面带来的弯曲，并将 GeoHash 单元格近似视作矩形。由于 GeoHash 的编码方式为将地球上的经度/纬度进行等分，所以一个 GeoHash 单元格的南北边长固定（式 (2-1)），东西方向随纬度增加而减小且与纬度成余弦关系 (式 (2-2)) 其中 R_{Earth} 为地球半径，取 6371km，$Latitude$ 为当地纬度，n 即为经度/纬度对应的二进制串长度。

$$length = R_{Earth} \cdot \frac{\pi}{2^n} \tag{2-1}$$

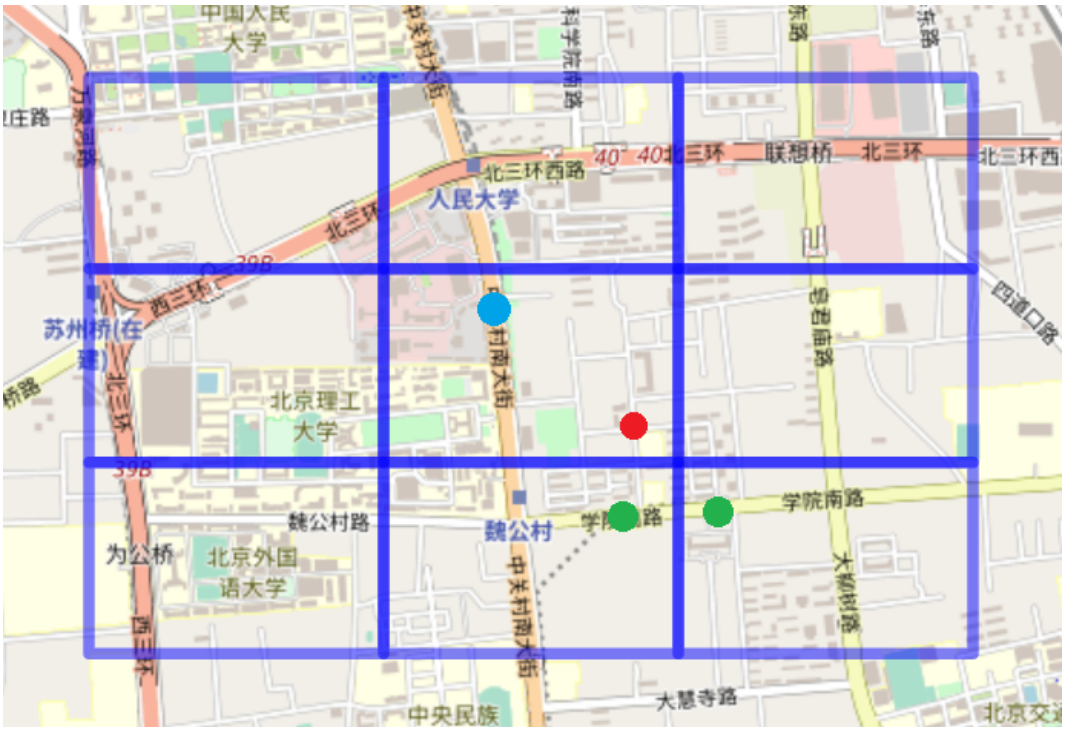

图 2.2　GeoHash 的边缘问题

$$length = R_{Local} \cdot \frac{2\pi}{2^n} = \cos\frac{2\pi \cdot Latitude}{360°} \cdot R_{Earth} \cdot \frac{2\pi}{2^n} \tag{2-2}$$

表2.1简要列出了在 GeoHash 取不同位数的情况下，一个单元格边长的情况，由于单元格东西方向边长与纬度有关，表中给出了该边长的最大值，该最大值位于地球赤道处。

表 2.1　不同 GeoHash 位数下单元格边长

GeoHash 位数	纬度位数	经度位数	南北方向（m）	东西方向（m）
2	5	5	625471.5	1250942.9
3	7	8	156367.9	156367.9
4	10	10	19546.0	39092.0
5	12	13	4886.5	4886.5
6	15	15	610.8	1221.6
7	17	18	152.7	152.7
8	20	20	19.0	38.2
9	22	23	4.8	4.8
10	25	25	0.6	1.2

在考虑 GeoHash 取 8 位情况下，一个单元格南北方向固定且约 19m，东西方向边长在 38 米至 16 米范围（考虑地球上纬度小于等于 65° 的区域）。利用单元格中点作为精确坐标的估计位置时，各方向距离误差不超过单元格对应边长的一半，平均误差为单元格对应边长的 $\frac{1}{4}$。因为相邻区域的 GeoHash 单元格边长幅度变化范围较小，可以在引入较小误差的情况下按纬度划分进行估计。

若将 90° 纬度范围平均划分成 8 份，既考虑每份跨越 11.25° 的范围。根据单元格边长计算公式，该区域下单元格东西方向平均边长处于该纬度范围中位线向高纬度偏移处，但经过计算，以处在纬度范围中位线的 GeoHash 单元格边长作为该纬度划分区域单元格东西方向边长的情况下，带来的误差不会超过 0.17%（在纬度 65° 情况下，误差随纬度减小而减小），因此以纬度范围中位线处单元格边长作为该划分中所有单元格边长的估计值，避免了计算球面距离时所需的三角函数计算。

在上述情况下，笔者统计了该估计方法带来的绝对误差和相对误差（见图 2.3）。由估计单元格边长的方式可知，在某一单元格离其所在纬度划分中位线越近时，其单元格边长越接近位于中位线上作为标准的单元格边长，反之，在某一单元格离其所在纬度划分中位线越远时，其单元格边长与近位于中位线上作为标准的单元格边长相差越大。因此在误差图上出现了误差周期性分布的情况：谷底意味着该纬度与其所在纬度划分中位线较近，误差较小，而峰值意味着其处于两个相邻纬度划分的边界附近，误差较大。对比图中的相对误差和绝对误差曲线，二者的变化规律基本相吻合，但由于随着纬度增加，单元格边长呈下凸函数下降，因此相对误差快速增长的同时，绝对误差的增长幅度相对较小。

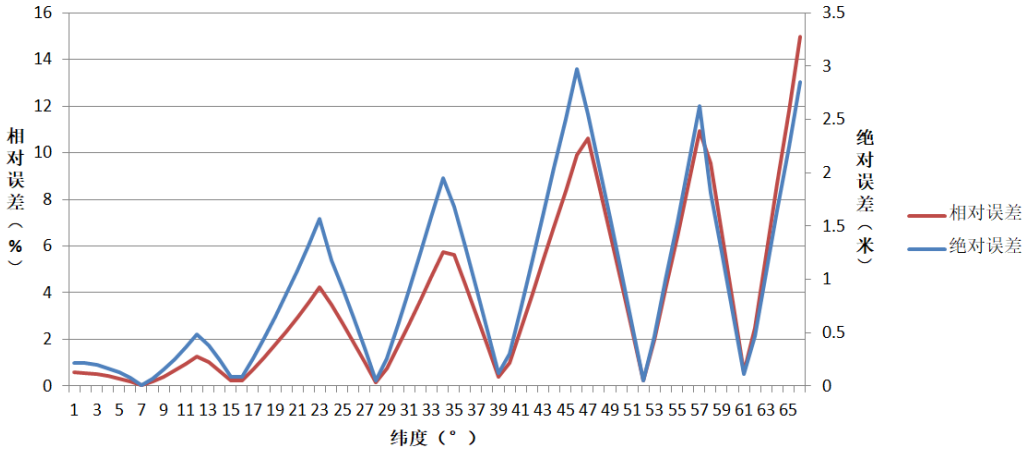

图 2.3　8 位 GeoHash 在纬度均分 8 份时误差

经过上述分析，在 GeoHash 精度取 8 位的情况下已经可以基本满足代替传统经纬度坐标作为车辆位置精确表示的需求，且若只考虑中国所处纬度（3°51′N 至 53°33′N），精度将会提高。但考虑到城市道路中可能存在的主路辅路情况，以及在后续依据周边路网和历史轨迹的位置修正过程中需要更高精度的位置表示，笔者在之后系统实现中采用了 10 位长度的 GeoHash 编码。同时为了减小 GeoHash 单元格边长估计误差，笔者采取将 90° 纬度范围平均划分成 16 份，既考虑每份跨越 5.625° 的范围。在上述情况下，笔者同样统计了该估计方法带来的绝对误差和相对误差（见图 2.4）。可见此时引入 GeoHash 作为精确位置描述的误差范围已经在可以接受的范围之内。

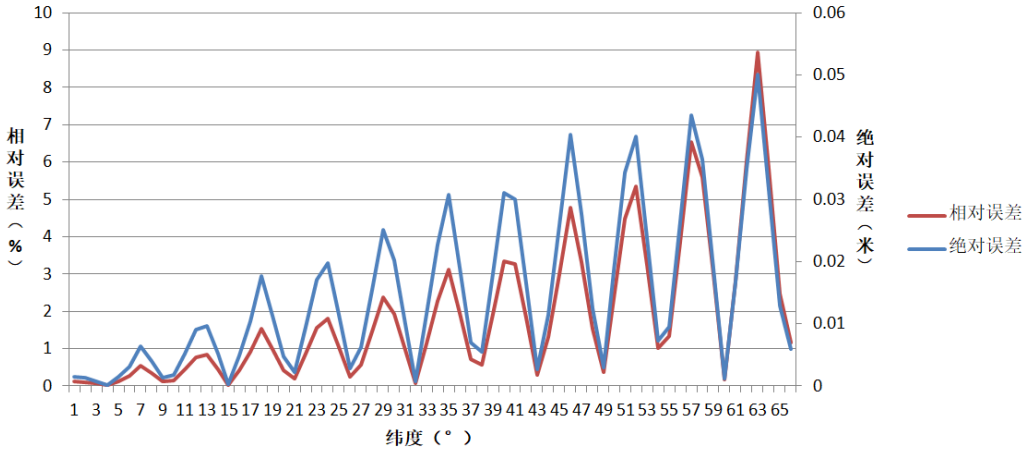

图 2.4　10 位 GeoHash 在纬度均分 16 份时误差

2.4　基于 GeoHash 值的几何计算

由于传统计算两个经纬度所表示坐标点距离时需要使用球面距离公式，若在以 GeoHash 为坐标表示的系统中沿用这套算法，则丧失了 GeoHash 带来的计算简便性。因此笔者利用 GeoHash 的编码性质及前节所述的 GeoHash 单元格边长估算方法，开发了直接利用 GeoHash 编码计算距离的方法，并基于此完成了以 GeoHash 为距离表示的点点向量、点线距离、点线投影、点到线段投影等常用几何计算函数，并将其应用于位置修正和验证系统中，避免了三角函数等复杂函数的使用，也为开发其他基于 GeoHash 的计算程序提供便利。

虽然根据 Peano 编码曲线的性质，两个编码之间的物理距离可以近似表示为编码之间的距离，但由于编码曲线突变的存在，在特定情况下可能存在较大误差，

因此程序采用了另一种距离计算实现。首先，将 Base32 编码的 GeoHash 值转换为二进制表示，然后将表示经度和表示纬度的二进制位分离。至此我们可以获得该位置在经过 GeoHash 编码分割后的地球表面所处东西方向和南北方向坐标 (x, y)。这时获得的坐标可以理解为将地球的经度和纬度等分之后，当前位置位于划分中心 $(0, 0)$（包含纬度 0°，经度 0° 点的单元格）向东偏移 x 个单元格，再向北偏移 y 个单元格后的位置。这种定义方式类似于平面直角坐标系中的位置表示，因此可以仿照平面直角坐标系中点与点距离计算方法，将经度和纬度的 GeoHash 编码作为平面直角坐标系中的横纵坐标进行计算。但值得注意的是横纵坐标的距离单位分别为上节中求出的 GeoHash 最小单元格对应边边长，在计算实际距离的时候需要乘上单元格对应边边长作为系数。

在基于 GeoHash 的几何计算实现过程中，使用了向量计算作为主要计算方式，计算中间过程均使用上文提到的单元格坐标进行，只有到最后一步才将单元格边长带入计算实际空间中的真实距离，这样简化了计算过程，也减少了计算过程中频繁使用估计值增加的误差。几种主要的几何计算过程如下：

（1）点点距离：在实现点与点距离时，先将两点的经度、纬度的 GeoHash 坐标分别相减得到两点间向量，再利用勾股定理求除向量长度。

（2）点线投影：在计算点线投影时，首先求出待求点和线上两个参考点之间的向量，之后利用向量点积，求出待求点在线上的投影点到参考点之间的绝对距离，作为系数乘上直线的单位向量可以得出投影点与直线上参考点之间的向量差，进而求出点在直线上的投影点。

（3）点线距离：先根据（2）中的步骤求出点在线上的投影点，再根据（1）中点点距离的求法得到点到线距离。

（4）点到线段投影：首先利用待求点到线段端点的向量与线段向量点积，判断点到线段所在直线的投影点是否位于线段内，若位于线段内部，则直接进行投影，若位于线段外，则取近端的线段端点作为投影点。这一函数主要运用在位置修正算法中，提供的点到直线投影与线段的关系也被利用在了道路匹配算法中。

2.5 本章小结

本章介绍了在位置修正和验证系统中所以使用的 GeoHash 地理编码，并对采用此编码所引入的误差进行分析，以此选择实际实现时所采用的精度范围。同时简要介绍了笔者实现的基于 GeoHash 的几何计算。该计算方法利用了 GeoHash

编码的特点，避免了复杂的三角函数和球面计算，并且适用于对小数支持较弱、不提供复杂数学函数计算支持的区块链智能合约编写语言 Solidity。

第 3 章　车辆位置验证及信誉评估系统

本章对车辆位置验证及信誉评估系统进行了详细介绍。本系统主要分为车辆位置采集修正系统和信誉评估系统两个部分。车辆位置采集修正系统运行在网页端，获取用户的 GPS 信息，并根据附近道路实时对其进行修正，并将得到的数据上传至区块链中的智能合约。信誉评估系统由智能合约实现并部署在区块链上，负责接受位置采集修正系统上传的数据，结合已保存数据进行用户信誉的更新，同时提供信誉查询接口供其他应用使用。

3.1　总体框架和运行环境

随着终端处理能力的增强，同时在区块链智能合约上进行大量计算时会消耗数量可观的 gas（执行费用，用于补偿矿工为智能合约提供算力所需的计算资源），本文实现的车辆位置验证及信誉评估系统将车辆位置修正部分放置在浏览器端，提前修正数据，方便之后区块链上进行的信誉评估计算。车辆位置验证及信誉评估系统的主要处理流程如下：

（1）系统初始化。在浏览器端，程序需要通过 web3.js 接口初始化所使用的信誉评估合约和地图存储合约。初始化本地存储为获得和处理位置数据做好准备。在合约端，合约对用户和初始信誉进行相应初始化。另外在浏览器端配合本地缓存生成用户的通用唯一识别码（UUID，Universally Unique Identifier）[16]，使用该识别码可以避免绝大情况下用户名冲突，并作为识别某一用户身份的唯一依据。

（2）获取位置。浏览器在获取用户位置信息时，采用 HTML5 Web APIs 的 `Geolocation.getCurrentPosition()` 方法获取当前 GPS，同时利用 `Date.getTime()` 方法获取本地时间。浏览器会将这些信息储存在本地缓存中，并运用于之后的位置修正计算。

（3）位置修正。位置修正模块是浏览器端的重要部分，其提供的结果是后续信誉评估系统运行的重要依据。位置修正主要依据终端当前获得的 GPS 坐标，此前的运动轨迹和周边路网来决定，具体情况见 3.2 节。

（4）上传信息。浏览器端通过 web3.js 接口将获取的实时 GPS 数据、修正后的 GPS 数据，时间戳打包上传至区块链网络。部署在区块链上的智能合约接收到数据之后，一方面将该数据保存至合约中，另一方面启动信誉评估更新程序。同

时为了方便观察效果，本文在网页端利用了 LeafLet（一个对移动设备友好的开源地图 JavaScript 库，支持在地图上动态增添和消除坐标点线）在线地图数据进行展示。

（5）信誉评估。信誉评估模块是车辆位置验证及信誉评估系统的重要组成部分，它主要依靠已保存的用户轨迹数据和新获得的位置数据更新用户的信誉评级。因为智能合约需要避免因为计算机之间对当前时间的分歧而存在分歧，因为智能合约无法依靠自己获得当前时间，因此信誉评估系统的更新计算仅当用户提交或请求新信息时发生。信誉评估系统的具体情况见 3.3 节。

关于本系统的运行环境，智能合约采用了较新的 Solidity v0.4.21，浏览器端则使用了较新的 Web3.js v1.2.6 与之配套。在开发和测试时，采用 Ganache v2.1.2 提供本地和局域网内的区块链私有链服务，并采用基于 Web3 Provider 的 Remix IDE 辅助进行合约开发，极大的方便了开发和测试流程。因为本文所使用的开发运行环境较新，作者在工作之初遇到了不少环境上的问题，因此完成了一份在 Windows 10 操作系统下安装配置该套环境并运行简单示例文件的帮助手册，为后人提供便利。

3.2 实时位置修正

本文中位置修正的思路是，先进行道路匹配，再将坐标点修正至匹配出的最佳道路上。因为系统对实时性的要求较高，因此选用基于概率的道路匹配算法，使用的实时位置修正算法使用了 GPS 直接获取的车辆当前位置，车辆历史位置，周边道路网络信息及简单的拓扑结构作为依据，将车辆坐标修正至合适道路上，算法的具体流程如下：

（1）获取周边道路。用待修正的坐标点 GeoHash 值前缀在地图数据库中找出所属大块和周围八个大块中的所有道路，道路信息中包含了由特征点连接而成的路段信息。

（2）初步筛选道路。对上步获得的道路进行去重操作，再对剩余道路的所有路段进行遍历，筛选出在当前坐标点一定范围内的候选道路。

（3）道路评分。参与道路评分的因素有：待修正点距离该道路所有路段的最短距离，以及取该最短距离时修正点的投影在路段线段内或延长线上，待修正点距离道路始末两端的距离。具体公式见式 (3-1)，其中 c 为依据修正点投影与路段线段的关系决定的参数，点投影在路段线段内时取 1，点投影在路段线段外时取

0.5。该公式的意义是，当一个点接近道路起点或终点时，转到相邻道路的可能性较大，因此相应地减少这条道路被选为匹配结果的可能性，当一个点位于道路中段时，其在这条道路上稳定行驶的可能性较大，相应地提升这条道路的匹配可能性。

$$v=\begin{cases}\dfrac{Const}{0.5\times c\times Distance+0.1}, & \text{所处道路不变，接近道路起点或终点}\\ \dfrac{Const}{1.5\times c\times Distance+0.1}, & \text{所处道路不变，处于当前道路中段}\\ \dfrac{Const}{c\times Distance+0.1}, & \text{所处道路改变}\end{cases} \tag{3-1}$$

（4）选择道路并进行修正。将上步所得的道路依据评分进行排序，并对排序结果从评分高的候选道路开始遍历，根据历史位置和当前位置，考虑是否满足所在道路的单行道情况，或满足当前所考虑道路与之前所在道路满足相邻的拓扑条件，选择出满足单行道和道路拓扑的评分最高道路作为当前道路。再将坐标点垂直投影至该道路的某一路段上，使得修正前后坐标点的几何距离最短。返回修正值并更新当前道路位置情况缓存。

通过以上流程，能实时高效完成车辆坐标修正，并将修正后的结果缓存以备后续位置修正和信誉评估系统使用。

3.3 基于合约的信誉评估

信誉评估系统采用智能合约实现并部署于区块链上，为数据的安全性提供保障，同时评估系统得到的用户信誉值也能为奖惩机制、节点授权等其他与信用和安全有关的应用提供支持。一般车辆位置验证和信誉评估系统可以采取多种验证方法如：自我验证，利用节点的位置、历史轨迹信息、速度和方向，进行信誉评估；友邻验证，利用同一局域网或其他近距离通信方式内的其他节点为节点提供证明以进行信誉评估。本文中采用的是自身数据验证的方法，通过分析网页端提供的修正前后位置信息等数据，进行节点的信誉评估。

由于智能合约的限制，信誉评估系统的实现也是本文的难点之一。由于智能合约在早期并不打算支撑复杂的业务逻辑，它限制了内存访问，对栈的限制使得递归结构在智能合约上较难实现，对小数的支持较差，同时不提供三角函数、开平方根等复杂数学函数库，另外每一步操作都会消耗一定量的 gas，限制了合约的实现复杂度。为了应对这些限制，如前文所述系统采用了 GeoHash 作为位置信

息表示。另外，针对智能合约调试复杂的情况，在进行信誉评估合约开发之前，笔者编写了能将数据输出至区块链交易记录的调试类，利用在正式合约中继承该类的方式，减小了调试难度。

在信誉评估合约中，采用 `mapping(string => user)` 的方式建立起从用户通用唯一识别码 UUID 至用户信息之间的映射。每个普通节点在刚加入区块链时的初始信誉值为 0，管理员节点等可信节点初始信誉值为 100，信誉值的范围为 [0,100] 之间的整数，100 为完全可信，0 为完全不可信。这样的信誉值划分方法也为以信誉值作为可行比例参与计算的应用提供了便利。

智能合约在收到浏览器端上传的用户识别码、修正前的当前位置、修正后的当前位置和时间戳之后，首先判断用户是否注册过，未注册用户将先完成初始化过程并将信誉值记为 0。接着合约将保存收到的用户相关信息并调用再估值函数。在再估值函数中，首先通过计算当前坐标与合约内保存的上一时间戳坐标的距离进而求出平均速度。若平均速度显著超出正常范围，则将该用户信誉值清零。同时，若本次用户提交数据时间距离用户上次提交数据的时间过长，则依据 10 分钟、30 分钟、60 分钟三个档位分别对用户信誉值进行减 1、20、100 的操作。与此相反，当用户连续 20 次在正常时间范围内提交有效数据时，用户的信誉值将会增加，使得用户在组网内连续正常工作的时间越久，其信誉度越高。另外，再估值函数还会对当前位置的修正前后距离进行计算，在修正前后距离不超过 20m 的情况下对用户信誉值进行额外加分，意味着能提供更准确和更高精度坐标数据的用户能更快提升自己的信誉值并完成验证。

3.4 本章小结

本章主要介绍了车辆位置验证及信誉评估系统进行的具体实现。在浏览器端，系统完成了车辆位置信息获取和修正，在合约端，系统对用户的信誉值进行评估，以此为标准完成车辆位置信息验证。二者相结合，能在不给区块链带来较大计算量的情况下，实现对用户的信誉评估和验证，并利用区块链的天然性质解决了数据间的交互和同步问题。

第 4 章　系统测试

本章使用了一段真实的 GPS 位置序列，对于实现的车辆位置验证及信誉评估系统进行测试，并对系统的运行效果进行分析。

4.1　实验数据

对于在位置修正中所使用的道路数据，笔者使用了从 `OpenStreetMap` 上获取的开源地图数据利用 `osm2pgrouting` 转换后得到的道路信息。道路信息中存储了该道路的编号、级别、名称、起始点坐标、终止点坐标、是否为单行道、前序道路和后继道路编号、组成道路的路段关键节点等信息。为了更细致地判断用户的具体位置，数据中将部分道路的主路辅路等信息拆解成不同的道路。得到了北京地区约八万七千条道路，在此基础上进行位置修正计算。

对于所使用的 GPS 位置数据，为一段跨度 18 分钟，包含 1127 个数据点的实际车辆行驶数据，原始数据构成的路径见图 4.1。

图 4.1　测试路径

4.2　位置修正结果

位置修正后的行驶路径见图 4.2，红点为原始位置，绿点为修正后位置。其中图 4.3和图 4.4为路径中的局部放大图，对比了修正前后的路径状态，可以体现出车辆位置修正程序的效果。

图 4.2　整体结果

图 4.3　局部放大结果 1

4.3　信誉评估结果

与此同时，笔者输出了该用户在信誉评估系统中的信誉值变化曲线（图 4.5），可以看出该用户在第 5 分钟左右时信誉值到达了可信状态。最初一组坐标值由于用户定位离道路较远，对其信誉值贡献不大，从 45 秒左右开始用户驶上中关村南大街主路，130 秒左右用户转入北三环，由于立交桥的影响，用户定位与实际行驶的立交桥下道路不时出现一定误差，用户信誉值增长较慢，之后用户转入中

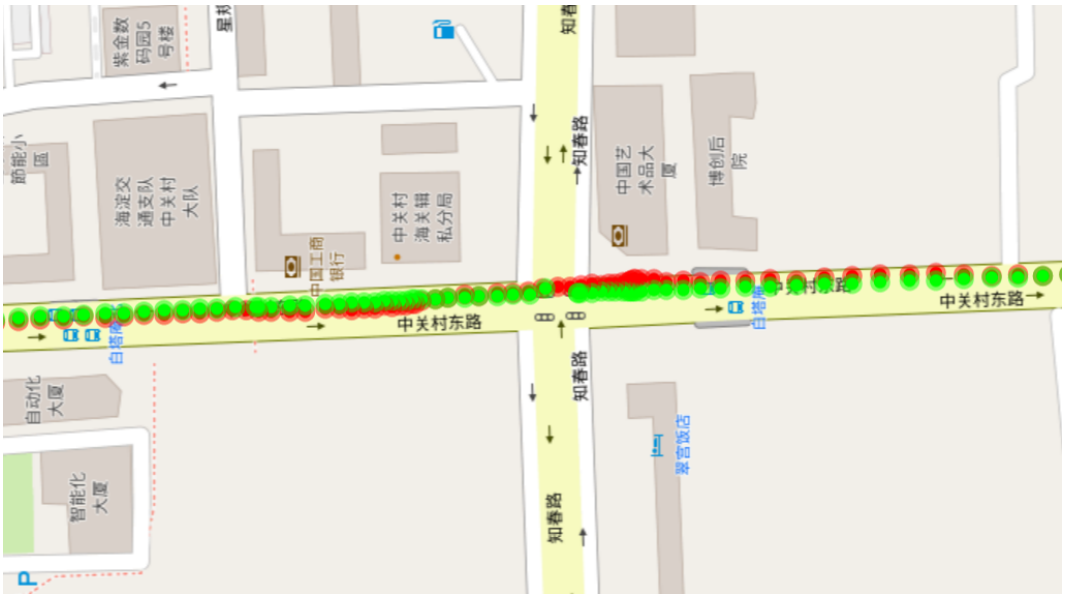

图 4.4　局部放大结果 2

关村东路，定位精度提高使得信誉值增长速度增加。

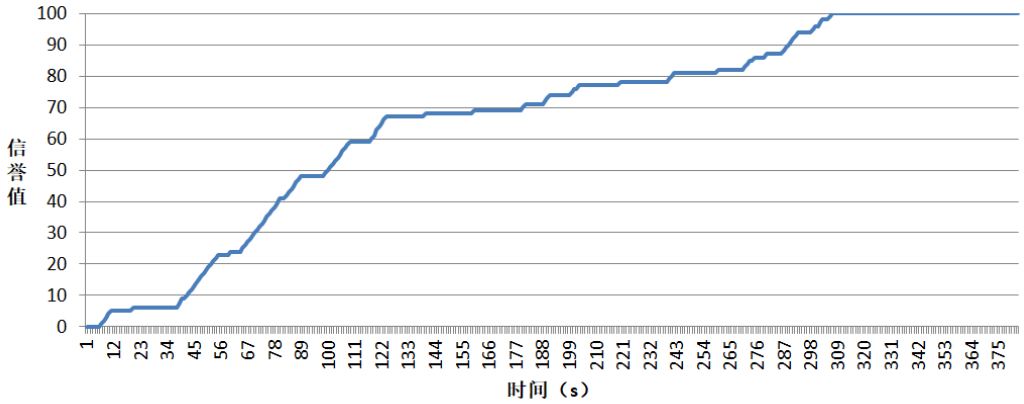

图 4.5　信誉曲线

4.4　分析与改进方向

从上述位置修正和信誉评估结果可以看出，该系统能较好地完成预期设想中的功能。在路口和高架处也能较好地分辨出车辆所处的具体道路。但由于条件限制，笔者没能对更多不同状态下的车辆运行数据进行测试，同时对于位置修正算法在复杂路况下的修正情况以及所涉及的评估参数，可能还需要更多的实地测试和调整。

4.5 本章小结

本章主要叙述了对笔者实现的车辆位置验证及信誉评估系统进行测试。经过测试，该系统能较好地完成预定功能。笔者对测试结果进行简要分析，并提出了今后的改进方向。

第 5 章　结论

城市中大量的运行车辆蕴含了海量的信息，建立在车辆之间的车载自组网能将这些车辆组织起来，分享和传递数据。而车载自组网的自组织、去中心化、结构开放的特点使得我们可以将运行在无需信任的去中心化网络上的区块链系统部署在其上，为其提供安全可溯服务。针对车载自组网中对数据与地理特征有较为紧密的联系这一特点，笔者开发了一套基于区块链服务的车载自组网中的位置验证系统，在完成用户验证的基础上还可以为其他基于使用者位置信息和信用情况的应用提供数据支持，增强了车载自组网的安全性的同时扩展了应用场景。

考虑到区块链计算所消耗的计算资源以及区块链智能合约编写语言的限制，本文采用了浏览器端和区块链端相结合的系统结构，使用 GeoHash 作为系统中统一位置表示的同时，在浏览器端完成了车辆数据收集校准，在智能合约上完成了用户信誉值评估，并利用实际数据对系统进行了测试。但由于条件限制，笔者的测试还不能说尽善尽美，在未来的工作中，一方面需要收集更多不同状态下的车辆运行数据进行测试，另一方面对于位置修正算法的细节参数需要进行更多的测试和调优。

插图索引

表格索引

参考文献

[1] DORRI A, STEGER M, KANHERE S S, et al. Blockchain: A distributed solution to automotive security and privacy[J/OL]. IEEE Communications Magazine, 2017, 55(12):119-125. https://doi.org/10.1109/MCOM.2017.1700879.

[2] LEIDING B, MEMARMOSHREFI P, HOGREFE D. Self-managed and blockchain-based vehicular ad-hoc networks[C/OL]//LUKOWICZ P, KRÜGER A, BULLING A, et al. Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp Adjunct 2016, Heidelberg, Germany, September 12-16, 2016. ACM, 2016: 137-140. https://doi.org/10.1145/2968219.2971409.

[3] SONG J H, WONG V W, LEUNG V C. Secure location verification for vehicular ad-hoc networks[C]//IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference. IEEE, 2008: 1-5.

[4] 彭鑫, 李仁发, 王东, 等. 车载自组网协作定位算法研究[J]. 计算机研究与发展, 2013, 50(6):1210-1216.

[5] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks[J/OL]. IEEE Internet of Things Journal, 2019, 6(2):1495-1505. https://doi.org/10.1109/JIOT.2018.2836144.

[6] BRAMBILLA G, AMORETTI M, ZANICHELLI F. Using block chain for peer-to-peer proof-of-location[J/OL]. CoRR, 2016, abs/1607.00174. http://arxiv.org/abs/1607.00174.

[7] 黄金国, 周先春. 多传感器融合与邻居协作的车辆精确定位方法[J]. 电子技术应用, 2017, 43(6):138-142.

[8] 徐会彬, 施星君, 任斌, 等. 基于车辆运动轨迹的 VANETs 位置验证[J]. 电子科技大学学报, 2013, 42(4):586-591.

[9] QUDDUS M A, OCHIENG W Y, NOLAND R B. Current map-matching algorithms for transport applications: State-of-the art and future research directions[J]. Transportation research part c: Emerging technologies, 2007, 15(5):312-328.

[10] KIM W, JEE G I, LEE J. Efficient use of digital road map in various positioning for its[C]//IEEE 2000. Position Location and Navigation Symposium (Cat. No. 00CH37062). IEEE, 2000: 170-176.

[11] SYED S, CANNON M E. Fuzzy logic-based map matching algorithm for vehicle navigation system in urban canyons[C]//ION National Technical Meeting, San Diego, CA: volume 1. 2004: 26-28.

[12] KAR I. Estonian citizens will soon have the world’s most hack-proof health-care records. [EB/OL]. 2016[2016-03-04]. http://qz.com/628889/this-eastern-european-country-is-moving-its-health-records-to-the-blockchain/.

[13] LACEY S. The energy blockchain: How bitcoin could be a catalyst for the distributed grid [EB/OL]. 2016[2016-02-26]. http://www.greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-for-the-distributed-grid.

[14] OPARAH D. 3 ways that the blockchain will change the real estate market[EB/OL]. 2016 [2016-02-06]. http://techcrunch.com/2016/02/06/3ways-that-blockchain-will-change-the-real-estate-market/.

[15] 张禹. 基于车辆轨迹的动态路况挖掘[D]. 北京: 北京理工大学, 2018.

[16] LEACH P J, MEALLING M, SALZ R. A universally unique identifier (UUID) URN namespace [J/OL]. RFC, 2005, 4122:1-32. https://doi.org/10.17487/RFC4122.

致　谢

衷心感谢清华大学计算机系的向勇副教授对本人的悉心指导。在老师的指导下，我能够学习新的知识并运用到实践中，一步步完成了这篇论文。我也学会了如何安排自己的工作计划，提升自己的学习效率。另外，感谢实验室全体老师和同学们的帮助和支持，为我提供了很多帮助，也对我的论文提出了宝贵的意见。

感谢母校四年来为我提供的优秀的课程资源，良好的学习氛围，便利的生活环境，也让我收获了同学间宝贵的友谊。在清华大学度过的这段时光使我终身受益。

声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：_____ 日　期：_____

附录 A　外文资料的书面翻译

物联网中的区块链和智能合约

中文摘要

最近，由于人们对区块链的兴趣爆发式增长，我们开始研究区块链是否可以很好应用于物联网领域。区块链允许我们建立一个分布式点对点网络，在这个网络中，非信任成员能在没有可信中介的环境中以可验证的方式互相交互。这篇文章回顾了这一机制的工作原理并研究了智能合约——区块链上的允许多步自动处理的脚本。然后我们转向物联网领域，并描述如何讲区块链和物联网结合：1）促进服务和资源的共享、从而在设备之间建立服务市场；2）允许我们以密码学可验证的方式自动化几个现有的耗时的工作流。同时我们指出一些将区块链技术应用于物联网之前应该考虑的问题：从交易隐私到数字化商品的预期价值。在适用的情况下，我们确定了解决方法。我们的结论是，区块链-物联网的结合很强大的，并可以引起多个行业的重大变革，为新的商业模式和分布式应用铺平道路。

关键词：区块链；分布式系统；物联网

ABSTRACT

Motivated by the recent explosion of interest around blockchains, we examine whether they make a good fit for the Internet ofThings (IoT) sector. Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a verifiable manner. We review how this mechanism works and also look into smart contracts—scripts that reside on the blockchain that allow for the automation of multi-step processes. We then move into the IoT domain, and describe how a blockchain-IoT combination: 1) facilitates the sharing of services and resources leading to the creation of a marketplace of services between devices and 2) allows us to automate in a cryptographically verifiable manner several existing, time-consuming workflows. We also point out certain issues that should be considered before the deployment of a blockchain network in an IoT setting: from transactional privacy to the expected value of the digitized assets traded on the network. Wherever applicable, we identify solutions and workarounds. Our conclusion is that the blockchain-IoT combination is powerful and can cause significant transformations across several industries, paving the way for new business models and novel, distributed applications.

Keywords: Blockchain; distributed systems; internet of things

A.1 引言

区块链最近吸引了多个领域的关注：从金融、医疗到公共事业、房地产和政府部门。出现这种关注增加的原因是：有了区块链，以前只能通过可信中介运行的应用现在也能运行在非集中系统上，并不需要一个权威中心，并能够以相同的确定性实现相同的功能。这在以前是无法实现的。

我们认为区块链技术让不可信网络成为可能，因为网络各方可以在彼此不信任的情况下进行交易。无需可信中介意味着交易双方可以更快达成共识。区块链的一大特征，密码学的大量运用，使网络中的交易具有权威性。智能合约—— 区块链上的自动执行脚本—— 集成了这些概念并支持了适当的分布式的高自动化

的工作。这使得区块链吸引了区块链领域的研究和开发人员。

当然，网络去中心化并不是总能实现。更重要的是，即使有去中心化的需求，基于区块链的网络不一定能满足其应用的需求。区块链和智能合约有一系列的优点，但同时也有很多不足。

这篇文章的目标是对区块链和智能合约的工作原理进行详细描述，指出它们的优缺点，并指出区块链和物联网结合的方式。便于读者发现潜在的物联网应用，并帮助读者决定是否将区块链引入项目。

本论文由以下部分构成。在第二章中，我们将解释什么是区块链，区块链如何工作，以及智能合约如何满足我们从根本上重定义网络交易各方的交互。然后我们以区块链的分类结束本节。在第三章中，我们将探讨如何将区块链和物联网结合使用，同时重点介绍现有的基于区块链的物联网应用。在第四章中，我们指出了物联网开发者和研究者在部署基于区块链的系统时应该注意的问题。我们将在第五章中展示我们的结论。

A.2 前期调研

A.2.1 区块链的工作原理

区块链是一种分布式数据结构。它被与比特币一起引入以解决双重支付问题。作为比特币网络上节点（矿工）互相验证的结果，达成共识后，比特币区块链存储了权威的账簿以记录财产所有者。

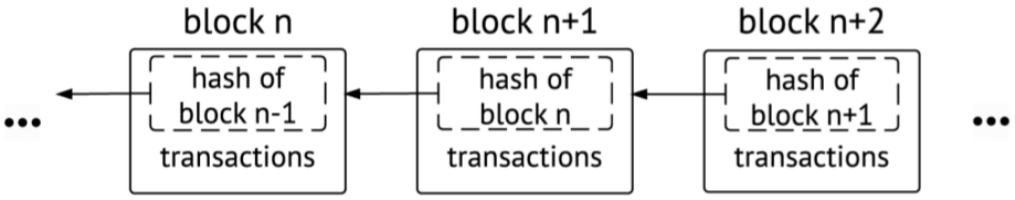

图 1 区块链上的每一块记录了交易列表和前一个区块的哈希值，除了链上的第一块。它被成为创世区块，它被区块链网络所共有且没有祖先。

然而区块链可以独立存在—— 不一定需要加密货币。我们可以将区块链看作是一个日志，用于存储带时间戳的块。每个块由密码哈希标识[①]。每个块记录了它前一个块的哈希值。这样就在块间建立了联系，从而创建了这个区块链——见图 1。任何有权限的节点都可以访问这个顺序反向链接的区块列表并计算出当

① 哈希是在块的内容上生成还是在块的头上生成 (比如在比特币中)，是一个设计上的选择。

前交换数据时区块链的状态。

我们可以通过研究区块链网络的运行方式更好理解区块链的机制。这是一组节点（客户端），它们通过各自持有的副本对相同的区块链进行操作。一个节点通常可以作为几个不同的区块链用户进入网络的入口点，但是为了简单起见，我们假设每个用户都通过独享节点在网络上进行交易。这些节点形成一个点对点网络，其中：

（1）用户通过一对公私钥与区块链交互。用户通过私钥签署交易，而这些交易可以通过公钥在网络上被定位[①]。非对称密码体系的使用为网络带来了可认证性、完整性和不可抵赖性。每一笔被签署的交易都被用户广播给它的一跳邻居。

（2）邻居在进一步转发前要验证这笔交易的有效性；无效交易将被丢弃。最终这笔交易会被广播到整个网络中。

（3）在一个确定间隔中，由上述流程收集和验证的交易会被排序打包进入一个有时间戳的候选块中。这个过程被称作挖矿。矿工节点将候选块广播回网络。（矿工节点的选择和块内容的选择取决于网络所使用的共识。参考第二章第二部分）

（4）节点验证候选块通过（a）包含有效交易和（b）正确引用链上前一个块的哈希值。在这种情况下，就将这个候选块加入链尾，并通过其记录的交易更新世界状态。否则，这个候选块将被遗弃。这步是一轮流程的结尾。

注意这是一个不断循环的过程。

当我们讨论第二步的交易验证时，通常存在这样一个问题：什么是有效交易？我们需要记住，在区块链网络中，本质上我们拥有的是一组不可信的写入者，他们共享一个没有可信中间人的数据库。为了防止在这个分布式环境中发生混乱，为了帮助网络达到一个共同的全局状态 (即达成共识)，每个区块链网络需要建立每个数据库交易应当符合的特定规则。这些依赖于应用程序的规则被写入每个区块链客户端中，然后使用它们来决定交易是否有效，从而决定是否应该将其转发到网络。在我们这里提出的简化的 “共享数据库” 模型中，让我们假设数据库的每一行都映射到一个公钥 (或地址)，该公钥 (或地址) 控制谁可以编辑它。然后，一个有效的交易是尝试修改具有相应签名的行。

当网络中的每个节点都按照上面列出的步骤进行操作时，它所操作的共享区块链将成为带身份验证和时间戳的网络活动记录。请注意，节点不必信任任何其他实体，从而产生了所谓的 “无信任环境”; 另一方面，正如在中所指出的，系统

① 根据实现的不同，地址可以是公钥本身，也可以 (通常) 是公钥的散列。

中的信任是通过不同参与者之间的交互来实现的。

以上是宏观层面和一般情况下的介绍。当我们研究区块链如何用于资产的转移和跟踪 (第二节第三部分) 或运行代码 (第二节第四部分) 时，事情变得更加有趣。

A.2.2 在网络上达成共识

节点需要在交易和交易顺序上达成一致。否则，将存在不同的区块链分支。这样节点对于整个网络状态会有不同的理解，除非解决了这个分支问题，网络无法维护一个权威的历史记录（即区块链）。

因此，在每个区块链网络中都需要一个分布式共识机制来实现这一点。正如我们在上节中所述，所使用的共识协议类型取决于区块链网络的类型和网络管理者采用的攻击向量。（不幸的是，“视情况而定” 的将在这篇文章中反复出现。它可能会让事情变得不那么容易解释，但它也说明了区块链的多功能性以适应多种情况。）

在一个理想的场景中，所有验证节点将对下一个块的交易顺序进行投票，以少数服从多数进行决定。但是，在任何人都可以加入的开放网络中，这将是灾难性的，因为女巫攻击：同个用户可以使用多个身份加入，进行多次投票，从而影响网络，使之有利于该用户的利益。换句话说，少数人可以控制网络。

比特币通过让挖矿变得 “昂贵” 来解决这个问题; 因为任何单个用户的计算资源都是有限的，所以网络上的多个虚拟实体不会产生影响。具体来说，只要它们能在块的头中找到正确的随机数使得头拥有期望的 SHA-256^2, 哈希值的前导 0 数量[①]。任何可以解决这个难题的节点，都已经生成了所谓的工作证明 (PoW)，并形成该链的下一个区块。由于涉及到单向密码散列哈希，所以任何其他节点都可以轻松地验证给定的答案是否满足要求 (如果满足要求，则为其区块链采用此块)，但这个步骤无法逆过来进行; 即根据结果进行推算输入。

请注意，当两个竞争节点几乎同时找到答案时，网络上仍然可能发生分叉。这样的分叉通常在下一块自动解决；工作证明机制规定节点应该采用最大工作量的分支，一般来说两个竞争分支不太可能同时生成下一个块。无论哪个分支先变长，节点都将采用其作为正确的分支。这使得网络再次就事件的正确顺序达成共识。除了 SHA-256 外，其他哈希算法也可用于 PoW，如 Blake-256 和 scrypt(在 Litecoin 中被使用)。还有一些机制融合了这些算法，比如 Myriad。

① 注意到，需要的前导零越多，解决这个问题就越困难。我们称之为目标增长。网络每 2,016 个块会调整难度级别，以适应网络 CPU 能力的变化，并确保生成块的速度恒定。

权益证明（PoS）是 PoW 的一种替代，降低了挖矿所需的 CPU 计算能力。在 PoS 中，矿工找出下一个区块的几率和节点的平衡成正比[①]。PoS 方案有自己的优缺点，并被证明实现起来是相当复杂的。

在中可以找到更详尽的对 Proff-of-X 机制的描述和分析。

然而，在私人网络中，当参与者处于白名单时，不需要开销巨大的共识机制 (如 PoW); 因为女巫攻击的风险并不存在。这实际上消除了对挖矿的经济刺激的需要，并使我们有更广泛的协议可供选择。

实用拜占庭容错 (PBFT) 就是这样一个算法。它为拜占庭将军问题提供了一个解决方案，这个解决方案可以在互联网这样的异步环境中工作。（比特币，通过上述机制，也为解决同样的问题提供了方法）它涉及一个三阶段协议和充当块矿工的主节点/领导节点的概念; 如果系统崩溃或表现出专制行为 (拜占庭故障)，网络的其他部分可以通过所谓的 “视图更改” 投票机制来更改领导节点。PBFT 的工作原理是假设不到三分之一的节点是错误的 (f)，这就是为什么说它至少需要[②]3f + 1 个节点。

Tangaroa，一个流行的 Raft 算法的拜占庭容错变体，在 Juno 中用作协商机制。Tendermint 提供 BFT 容忍度，与 PBFT 算法相似; 但是，当超过三分之一的节点出错时，它为返回给客户机的结果提供了更严格的保证，并允许一组动态更改的验证服务器和轮询的领导节点，以及其他优化。

Ripple 的一致性算法使用了叫做 “唯一节点列表”(UNL) 的 “集体可信子网” 来处理在 BFT 容错系统中常见的高延迟。一个节点只需要查询它自己的 UNL，而不是整个网络，就可以达成共识。它可以容忍不多于五分之一的节点出错 (5f + 1 复原力)。

在挖矿多样性策略 (在多链中使用) 中，白名单的采矿者以轮询的方式向链中添加块，并在一定程度上对故障节点进行宽大处理。一个名为 “挖掘多样性” 的网络参数用于计算采矿者在尝试再次挖矿之前应该等待的块数量 (否则其提出的块将被拒绝)。挖掘多样性参数的值越小，意味着需要越少的矿工勾结控制网络; 如果串通矿工的数量等于或大于每个矿工在尝试再次采矿之前应该等待的块的数量，那么就有可能发生这种情况。相反，挖掘多样性参数的值越高，就越能确

① 注意，PoW 和 PoS 实际上都需要一个支持加密货币的区块链; 前者是为了激励矿工进行挖掘一个区块所需要的大量哈希计算，这样做的代价很高，而后者是为了让矿工在采矿时将他们的 (加密) 货币置于危险之中。

② 如果使用了超过 3f + 1 个节点，那么中列出的仲裁阈值可能会导致分叉。相反，应该使用中指定的界限。例如，这是在 HyperLedger Fabric 项目中采用的。

保轮询中包括更多的被允许的矿工，从而使由少数人控制网络更加困难。

Sieve 是 HyperLedger Fabric 项目中使用的一种机制，它受中提供的执行-验证体系的启发，通过添加推测性执行和验证阶段来增强 PBFT 算法。这允许网络检测并过滤掉可能的不确定请求，并且还可以对交易的输出状态达成共识（还能对输入顺序达成共识）。

参考对比了 PoW 和 BFT 共识协议，并提供了一个关于可扩展性的优秀总结。

请注意，无论使用何种协商机制，区块链网络中的矿工 “比传统集中式数据库的所有者拥有的权力要小得多，因为他们不能伪造交易”。

A.2.3 在区块链上转移数字资产

为了说明资产转移是如何工作的，我们考虑一个来自银行业的简化示例。设想一个银行的 (集中式) 数据库，它跟踪每个客户的总余额。我们基本上是在查看一个包含三列的表:“资产类型”、“所有者”(“交易对象”) 和 “数量”(“金额”)。例如，表中带有 “USD”、“Alice”、“10” 的一行表示 Alice 在该银行有 10 美元存款。鲍勃在同一家银行有一个账户，里面有 0 美元。当 Alice 将 $2 转到 Bob 的账户时，USD/Alice(资产类型/所有者) 行的 “quantity” 被更新为 $8，而 USD/Bob 的 “quantity” 现在是 $2。一份资产 (2 美元)，或者更确切地说是这个资产的数字表示，通过转换数据库中相应的行，在两个实体之间转移。

这种数字标记资产的转移可以通过使用使用比特币交易模型的区块链网络以密码验证的方式轻松实现。再次考虑数据库的模型[①]，该数据库由不信任的作者在不信任的环境中使用，如第 II-A 节所示。每一行都带有与上面银行示例相同的字段，不同之处在于 “持有者” 字段现在持有允许编辑该行的用户的公钥。假设数据库显示 Alice 拥有 10 单位资产 X(我们将了解这个事实是如何建立的，即这些资产是如何在短期内生成的)。也就是说，数据库中的一行在 “持有者” 列中包含 Alice 的公钥，在 “资产类型” 和 “数量” 列中分别包含 “X” 和 “10”。假设 Alice 知道 Bob 的公钥。Alice 是如何将 2 单位 X 传递给 Bob 的? 她签署一笔交易，修改她的行，将 X 的值减少 2，并创建一个新行，其 “owner” 设置为 Bob 的公钥，其 “asset type” 和 “value” 字段分别设置为 “X” 和 “2”。

Alice 向 Bob 传输了 2 个单位的 X，用这个信息创建了一个新行，并把它签署给 Bob; 见图 2。(事实上，Alice 的交易也删除了她自己的行，创建了一个分配给她的一个公钥的新行，并移动了她持有的其余 8 个 X 单位。这样做是为了控制

① 正如我们稍后将看到的，它也可以通过智能契约来实现，但是有一些关键的区别，特别是在性能方面; 见二章第五节。

并发性 (参见第二章第五节) 并防止系统中并发写操作之间的冲突; 不修改行，而是删除它们，并使用更新后的值创建新行。

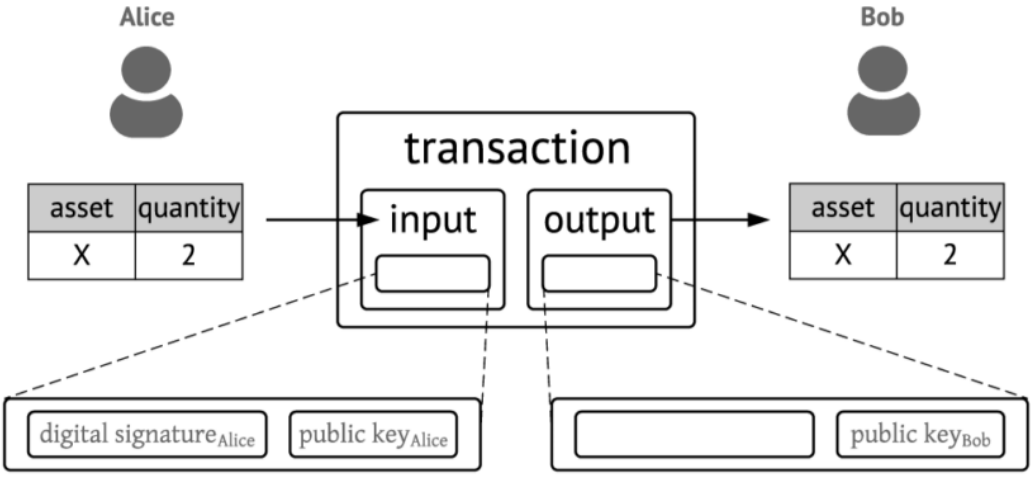

图 2 一笔交易将（X）从 Alice 的账户转移到 Bob 的账户。Alice 签署了这笔交易，并将输出锁定在 Bob 的公钥上，使得只有 Bob 可以使用这笔财产。

Bob 的资产 “X” 的新余额可以通过聚合数据库中与他的公钥对应的所有行来计算，这些行的 “资产类型” 被设置为 “X”。爱丽丝也一样。

我们将编码一些验证检查到一个区块链网络的所有节点，来确认资产转移: 提供的地址是否存在？它的签名是否正确，以便删除该行 (或多行)? 这一行是否已被先前的已验证交易寻址 (使用)? 一项资产不能重复使用。它是否将正确的数量转移到新行? 例如，如果事务的行读取 “10 个单位的 X”，那么尝试传输 “2 个单位的 X”(给 Bob) 和 “9 个单位的 X”(给 Alice) 应该失败。同样的道理也适用于试图转移的，比如说 “10 个单位的 Y”。投入的总和应等于产出的总和，即转移不应增加某一资产类型的总数量。

请注意，一个交易可以涉及多个现有行，而不是一个行，即传输分散在数据库中的资产，只要对它们进行了正确的签名以访问它们。这些现有的、尚未删除的行在比特币中称为未使用交易输出 (unspent transaction output, UTXO); 它们是由系统中较早的交易创建的。交易消耗的 UTXO 称为交易输入；交易创建的 UTXO 称为交易输出。

然后，交易基本上删除一组行 (UTXO) 并在数据库中创建一组新行 (UTXO)(参见图 3 中的示例)。

上面描述的一个突出问题是: 我们如何生成资产并在链中引入它们? 在我们

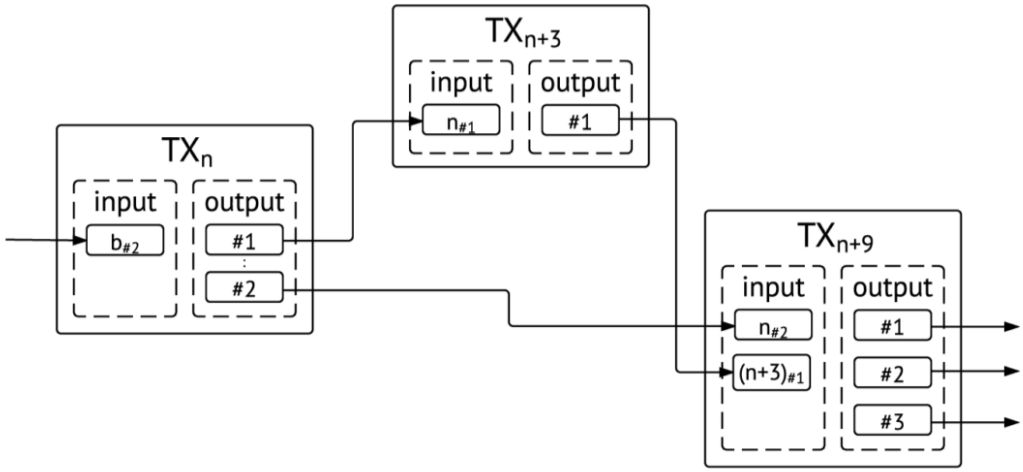

图 3 交易 n 使用了交易 b（未在图中显示）的输出（b#2），并产生了两个输出 n#1 和 n#2，分别被交易 n+3 和 n+9 使用。类似过程发生在网络中每笔交易中，使得交易间互相联系并可以被追踪。

达到 Alice 有 10 个 X 单位的状态之前，这 10 个 X 单位必须来自某个地方。答案是，这取决于网络和它的用途。通常，经过适当授权的节点使用一种特殊类型的交易将资产 (或资产的新单元) 引入到网络中。

例如，假设 Alice、Bob 和 Carol 之间有一个私有区块链网络。Carol 使用多链，这是一个区块链平台，它将权限 (可以连接到网络，可以在网络上进行交易，可以在网络上发布) 分配给公钥。Carol 负责配置网络，以便她的公钥可以在网络上发布资产。她邀请爱丽丝和鲍勃加入; 他们都对卡罗尔发行资产的能力感到满意。它们都有一对私有和公共密钥。Carol 提交一个生成 10 个单位 x 的签名交易，网络上的节点认为这个事务是有效的，因为她的公钥得到了适当的许可。然后卡罗尔把这些新生成的 X 单位转移给爱丽丝，爱丽丝就有了 10 个单位 X。

以比特币为例，每挖掘一个比特币块，新的比特币就会被引入到网络中: 挖掘节点在它向网络广播的交易块中包含一个所谓的 coinbase 交易。这个 coinbase 交易没有输入，它向挖掘节点提供预先确定的比特币数量 (由网络决定)

关键的是: 如果你有一组用户 (a) 想要交易数字令牌, 和 (b) 已经同意这些令牌是如何生成的, 然后一个区块链网络交换是一种理想的工具，它能同时使用这些令牌并跟踪谁有什么。由于网络上的每个节点都进行必要的检查，并对接受的结果达成一致，所以不需要任何中间人来促进交换。资产跟踪是开箱即用的，因为每个节点都可以访问区块链上商定的一组加密可验证的交易。

A.2.4 智能合约是如何工作的

Nick Szabo 在 1994 年引入了这一概念，并将智能合约定义为 “执行合同条款的计算机化交易协议”。Szabo 建议将合同条款 (担保等) 转换成代码，并将其嵌入到能够自我执行的硬件或软件中，最小化交易各方之间对可信中介的需求，以及恶意或意外的发生。

在区块链中，智能合约是存储在区块链上的脚本。(可以将它们大致看作类似于关系数据库管理系统中存储的程序。) 因为它们位于链上，所以它们有唯一的地址。我们通过处理一笔交易来触发智能契约。然后，根据触发交易中包含的数据，它以规定的方式在网络中的每个节点上独立自动执行。(这意味着智能契约区块链中的每个节点都运行一个虚拟机 (VM)，而区块链网络充当一个分布式 VM。)

智能合约允许我们在链上进行通用计算。然而，他们擅长的是管理网络实体之间的数据驱动交互。让我们用一个例子来解释一下。考虑一个区块链网络有参与者 Alice、Bob 和 Carol，类型 X 和 Y 的数字资产在其中进行交易。Bob 部署智能网络上的智能合约规定:(a)“存款”：允许他存入 X 至合同；(b)“交易”：每接收 5 单位 Y, 发送回 1 单位 X(从合同存款中)；(c)“取款”：允许 Bob 撤回合同的所有资产。

请注意，“存款” 和 “取款” 函数只有 Bob(通过他的密钥) 可以调用它们，这对于我们的示例也是有意义的; 它也可以被设定成网络上的任何用户都可以调用它们。

Bob 将一个交易发送到该智能合约的地址，调用它的 “存款” 功能并将 3 个单位的 X 移动到该合约。该交易将记录在区块链上。Alice 拥有 12 个单位的 Y，然后发送一个交易，将 10 个单位的 Y 移动到合约的 “交易” 函数，并返回 2 个单位的 x。这笔交易也记录在区块链上。然后 Bob 向契约的 “取款” 函数发送一个已签名的交易。合约检查签字以确保提款是由合约所有者发起的，并将所有的存款 (1 单位 X, 10 单位 Y) 转回给 Bob。

让我们注意以下几点:

1）该合同有自己的规定，可以管理区块链上的资产。我们说用户在区块链上有自己的帐户，而区块链支持也基于帐户的模式。在上面的例子中，它可以包括资产 X 和 Y (如果我们回到共享数据库模型，合约是一个单独的 “用户”/实体，它可以拥有、删除和创建行)。

2）合同允许我们用代码表达业务逻辑;” 用 1 单位 X 换取 5 单位 Y ”

3）一份适当的智能合约应该描述合约的所有可能结果。例如，上面的“交易”函数可能会被写成拒绝那些带来的不是 5 的倍数的 y 的请求; 也就是说，12 单位的 y 将被拒绝。或者可以这样编写该函数，将转账分解为 5 的最大倍数 (该倍数将在没有问题的情况下进行交易) 和余数 (该余数将被返还)。如果对方出价 12 单位的 Y，就会向发送方返回 2 单位的 X 和 2 单位的 Y。

4）Bob 希望与他的交易对方建立数据驱动的的关系。毕竟，交易是一个带符号的数据结构，它表示了数值的传输。Bob 部署了一个智能合约有效地实行 “如果发送给合约这个数据 (5 个单位的 Y)，它将如何响应 (1 个单位的 X)”。

5）智能合约由发送到其地址的消息/交易触发。

6）智能合约有确定性：相同的输入总会产生相同的输出。如果写入一个非确定性合约，当它被触发并在网络上的每个节点上执行，可能返回不同的随机结果，网络无法对其执行结果达成一致。在一个正确建立的区块链平台上，非确定合约是无法存在（通过强制合同开发人员使用一种编程语言, 没有任何不确定性结构）或存在但不被允许的。

7）智能合约处于区块链上，因此每个网络参与者都可以检查它的代码。

8）由于与合约的所有交互都是通过区块链上的签名消息进行的，所以所有网络参与者都可以获得合约操作的加密可验证历史。

支持比特币式交易的区块链允许在互不信任的交易方之间进行资产转移。然而，支持智能合约的区块链更进一步，允许在相互不信任的交易方之间进行多步处理 (交互)。交易实体 (a) 在参与合约之前检查代码并确定其结果 (b) 获得确定性结果，因为代码已经部署在网络上, 并由他们两人完全控制 (c) 过程可验证因为所有交互都进行数字签名。争端不可能存在 (当所有可能的结果都被考虑在内时)，因为参与者不能对他们参与的这个可验证过程的最终结果产生分歧。

智能契约自主运行，其行为是完全可预测的。它们可以被可信地用于处理区块链上自己权限范围内的数据（在上面的示例中, 合约不能使用不属于它的资产）。

在本节最后，智能合约还催生了 “分散自治组织”(DAOs) 的概念，即如果遵循合约中编写的某个过程，区块链上的实体的行为可能会得到到改善。正如在中所描述的，最简单的示例是通过地址调用另一个合约的主程序。此地址位于合约的内部数据库的可变部分。该契约还包含一个可以对其行为进行投票的成员、地址 (公钥) 列表。可以在合约中写入一个规则，如果这些投票者中的大多数人以某种方式投票，则合约将通过调用获得多数选票的地址来修改其行为，执行其主过

程。

A.2.5 区块链的分类

有几种方法可以对区块链网络进行分类。我们根据中提供的优化/权限方法，重点关注:

（1）谁可以访问网络: 如果任何人可以加入，我们处理的是一个公共的或者说无许可的网络，而如果我们有一个白名单，我们处理的是一个私有的或者说许可的网络。这个问题的答案决定了采用的共识机制。由于 Sybil 攻击，公共网络中的共识代价高昂，通常需要对矿工 (以加密货币的形式) 提供经济激励。私有网络对于希望在受控、规范的环境中运行的受众来说更有意义，或者对于希望比公共网络提供更高的吞吐量的受众来说更有意义。

（2）谁可以交易或挖矿: 可能不允许所有参与者都可以交易、部署智能合约或参与挖矿。这个条件通常只适用于所有的参与者都是可识别的私有网络。

（3）Bitcoin-style 交易 (UTXO 模型) 或智能合约 (基于帐户的模型): 正如第二章第三节中解释, 支持 UTXO 模型的区块链适合转让和跟踪数字标化的资产，而支持帐户模型的区块链 (第二章第四节) 给使我们可以运行任意逻辑并建立可验证的多步骤过程。然而，当涉及到并发执行和交易吞吐量时，这种对任意逻辑的支持带来了严重的代价。在节点的 VM 处理传入消息到智能合约之前，它无法判断它将如何影响契约的内部状态，或者它是否会触发系统中的另一个合约，因此它不能支持并行运行一个块的所有交易。但在 UTXO 模型中，每个事务都显式地标识其输入和输出; 如果交易的输出和输入之间没有依赖关系 (即只要交易并不试图花另一个交易在同一个块上的输出), 执行的顺序就并不重要, 所有的这些交易就可以被并行处理。

对于区块链和分布式账本的其他分类尝试，请参见和。无论如何，重要的是，无论具体设置如何，区块链都能给我们带来以下好处:

（1）一个健壮的、真正分布式的能够容忍节点故障的对等系统。

（2）一个可以识别冲突和分支并自动解决它们的网络，最终聚合到一个单一的、被全体接受的状态。

（3）网络活动的透明性、可验证性和可审核性。不管这些过程涉及数字资产的交换还是各方之间的数据驱动交互，我们得到了可验证的过程。每一笔交易都提供了一个可公开验证的证明，证明它被授权与系统进行交互。避免了纠纷的可能形，也不再需要调节过程。

（4）正如中所指出的:“一种将不同的信息片段标记给不同的参与者，并在没有中央权威的情况下使用这种形式的数据结构的系统。”

（5）允许不信任的参与者以可预测的、特定的方式相互交流的系统。

A.3 区块链与物联网

在中，为了使不断扩张的物联网设备生态系统可持续发展，作者提出了分散架构。从制造商的角度来看，当前的集中模式有很高的维护成本，考虑在数百万台设备上的软件更新，而这些设备已经停产多年。从消费者的角度来看，对需要在后台与服务器进行交互的软件缺乏信任是情有可原的，而且消费者也需要透明安全的操作方法。这些问题可以通过一个可扩展的、无需认证的、可以透明操作和安全分发数据的点对点模型来解决; 作者指出，区块链为这个问题提供了一个优雅的解决方案。

请考虑以下情况，以了解它是如何工作的。制造商的所有物联网设备都在同一个区块链网络上运行。制造商部署了一个智能合约，允许他们在网络上存储最新固件更新的哈希。设备要么在区块链端附带智能合约的地址, 或者通过已发现设备发现智能合约 (见第四节)。他们可以通过像 IPFS, 的分布式点对点文件系统查询合约并了解新固件。对该文件的第一个请求将由制造商自己的节点 (也参与到网络中) 提供服务，但是在二进制文件传播到足够的节点之后，制造商的节点可以停止提供服务。假设这些设备被配置成可以共享它们获得的二进制文件，那么一个设备在制造商停止参与网络很久之后仍然可以得到热门的固件更新，并确保它是正确的文件[①]。这一切都是自动发生的，没有任何用户交互。在集中式模式中，设备只会向制造商服务器寻求更新，并收到 404 错误。

此外，交换加密货币的区块链网络提供了一个方便的计费层，并为设备之间的服务市场铺平了道路。在上面的例子中，存储二进制文件副本的设备可能会对服务收取费用，以维持它们的基础设施成本 (或者只是为了盈利)。其他的例子包括:Filecoin 允许设备 “租用他们的磁盘空间”，21 和 EtherAPIs，这使 API 调用货币化成为可能—— 调用者需要在请求它们之前提供必要的微支付 (分别以比特币或以太坊)。有了加密货币，每台设备都可以在互联网上拥有自己的银行账户; 然后，它可以将其资源公开给其他设备 (或用户)，并通过微交易获得对其使用的代价。

① 例如，通过协议，如 ipfs-cluster。

这也促进了服务和财产的共享。Slock.it 工作在智能电子锁 (“Slocks”) 上，可以通过携带适当令牌的设备解锁。这些令牌是在 Ethereum 区块链上购买的，这是一个公共的区块链网络，为使用加密货币 Ether 的智能合约进行了优化。想要租房子或车的车主会对电子门锁的使用时间设定一个价格。相关方可以使用移动应用程序识别锁，以第三方支付请求的金额，然后通过正确签名的消息与锁通信 (使用 Whisper 点对点通信协议) 来解锁。通过让所有 Slocks 在相同的区块链上运行，简化了计费。

基于同样的主题，在能源领域，物联网与区块链的整合允许建立一个点对点市场，根据用户定义的标准，机器可以自动买卖能源。例如，TransActive Grid 正在纽约布鲁克林的一个社区试验点对点可再生能源市场的概念。太阳能电池板在区块链上记录它们的过剩产出，然后通过智能合同卖给邻近的企业。

区块链在物联网中的作用还不止于此。考虑供应链的典型例子：一个集装箱离开了制造商 (A 点), 通过铁路运输到邻近的港口 (B 点), 然后被运到目的港 (C 点), 再次被运输到分销商 (D 点), 直到它最终到达零售商 (E 点)。这个过程涉及到几个部分，所有这些参与者都如图 4a 所示。每个参与者通常会维护自己的数据库，以跟踪资产，并根据链上其他参与者的输入对其进行更新。建立了一个区块链网络跟踪这个资产，意味着现在有一个共享数据库，其中的更新具有加密可验证性，可以沿着网络自动传播，并拥有可审计的信息。例如 (图 4 b), 当船只到达目的港时, 他们发送消息到一个预先确定的公认的智能合约，使得链上的每个人都知道集装箱现在在点 c。因为这笔交易被签署了，它将以密码验证的方式证明集装箱到达了港口。港口收货人也将发消息给同一个智能合约，确认了集装箱的所有权。

或者，如果链遵循比特币交易模型 (参见第二章第三部分)，则整个过程可以通过原子的点对点的令牌交换来完成[①]。在创建区块链时，允许制造商发出 “我有个集装箱” 的令牌; 允许所有其他参与者发出 “我已收到集装箱” 的令牌。当制造商将集装箱交给货运转运公司，由该公司将其从 A 点移动到 B 点时，它将创建一个具有两个输入和两个输出的事务 (参见第二章第三部分)。输入 1 指向制造商自己的 UTXO(“我有集装箱” 令牌)，输出 1 创建一个新的 UTXO，将此令牌锁定在运输者的公钥，有效地将所有权传递给它。输入 2 指向运输者自己的 UTXO(“我已经收到集装箱” 令牌)，输出 2 创建一个新的 UTXO，将该令牌传输给制造商。制造商签署了他们的部分，然后发送这个不完整的交易，运输者签署了自己的部

① 参见 Greenspan 关于 “交付对支付” 以及区块链是如何促进它的优秀指导书。

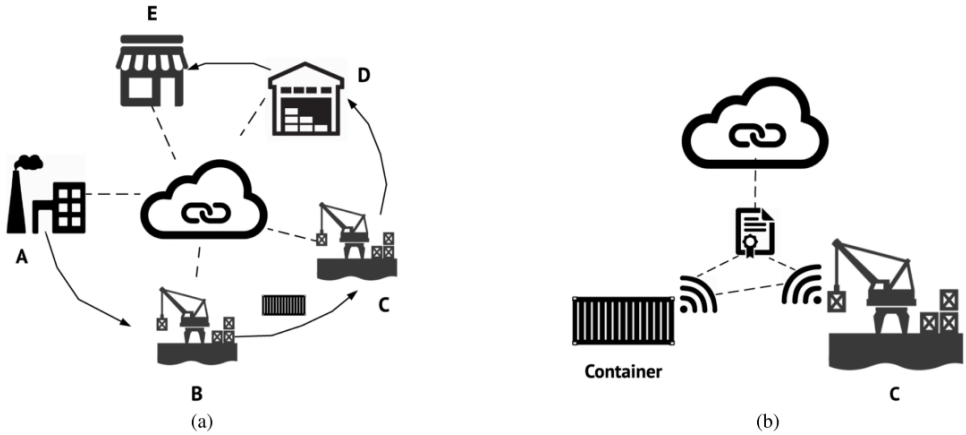

图 4 这是一个利用智能合约和物联网进行资产跟踪的示例。在 4a（左）中，集装箱离开制造工厂（A），通过铁路到达邻近的港口（B），被运输到目的地港口（C），然后到达分销商（D），最后到达零售商（E）。在 4b（右）中，我们着重关注 B 到 C 的阶段。集装箱承运人与目的地码头（C）进行握手，确认集装箱送达预期位置。这之后，它会发送消息到智能合约以签署交付。目的地港随后确认接收。如果 C 在一定时间范围内没有发送确认，承运人将得到消息并可以开始调查出现了什么问题。

分，然后将它发布到区块链。当这个交易被添加到区块链时，制造商已经从运输者收到了 “我已经收到集装箱” 令牌，运输者现在持有 “我有集装箱” 令牌。类似的原子交换将在 B 点的运输和船运公司, 直到零售商在 E 点最终接收 “我有集装箱” 令牌。在这会有一个完整的、密码验证、用于跟踪资产的时间戳记录，减少发生纠纷的可能。

上述是对过去实践的升级，也是区块链有用性的证明，但在物联网上可以更进一步，成为完全自动化的系统。假设每个参与者都有一个带蓝牙的智能跟踪器，或 GSM/LTE 装置以接入互联网。在集装箱上也有类似的跟踪器。当两个参与者在场且集装箱也在场时，比如在 A 点，设备可以在没有任何用户输入情况下自动发送交易至区块链，这个过程就可以进行到下一个阶段了。

在我们的情景中，蓝牙是必需的，这样设备就可以知道它们什么时候彼此接近，什么时候通过互联网在区块链上进行交易。这只是众多情形中的一种。例如，Filament 就为传感器提供了被称为 “Taps” 的远距离无线电。Taps 可以形成网状网络，通过一种称为 telehash 的协议以分布式的方式安全地相互通信，并通过公共区块链上的智能合约相互交互。传感器本身不连接到互联网以减少部署成本，但可以连接到提供连接的网关节点。

A.4 应用注意事项

在这一节中，我们将讨论当物联网制造商试验区块链并让物联网设备参与到一个区块链网络中时可能出现的几个问题。我们就讨论了这些问题的可能解决方法和这方面正在进行的工作。

与正确配置的集中式数据库相比，区块链解决方案通常性能较差，导致事务处理吞吐量较低和延迟较大。我们建议读者参考，它侧重于协商机制的灵活性方面，但也涉及性能问题。这一问题在 PoW 机制的公共网络中尤为突出 (参见第二章第五节和第二节)，尽管诸如 Bitcoin-NG 等新研究中展现了好的可能性。通常，这种性能损失是对缺乏信任的分布式的代价。在区块链中，每个节点执行相同的任务，没有并行任务执行的空间。这种情况在执行智能合约的区块链中更加明显，第二章第五节中提到了并发问题。至少有一个主要的区块链平台正在朝着可并行化的方向努力，尽管实现和测试仍有很长的路要走; 参见以太坊改进方案 105。

在区块链上维护隐私是一个复杂的问题。每个参与设备都是由它们的公钥 (或其哈希) 标识的。参与者不需要知道其他人的密钥; 他们只需要交易对方公钥[①]。然而，区块链中的所有交易都是公开的。通过分析这些数据，相关方可以识别并创建地址之间的连接，并最终对它们背后的实际身份做出明智的推断-。如果隐私对应用很重要，有两种方法可以缓解 (但不能完全消除) 这个问题:

（1）让您的设备为每个事务使用一个新密钥，或为每个交易对手使用一个不同的密钥，以使模式识别变得困难。以比特币上的 “分层确定性钱包”BIP0032 标准为例，该标准允许以可管理且安全的方式产生无限数量的公钥。“每笔交易一个新密钥” 方法的一个问题是，每笔交易都必须将这个新密钥传递给相关的交易方，这是个麻烦耗时的过程。

（2）在私有区块链的情况下，如果另一个参与者可能通过跟踪你的设备的活动获得竞争优势，就不要对所有交易使用相同的区块链。通过只与需要合作的实体建立区块链，并只将其用于需要合作的流程，最小化设备的暴露。诚然，与单一区块链相比，这增加了协调成本，但这是维护隐私的必要代价。介绍了区块链分析的方法和使这些分析技术失败的方法。

同样，交易也很难保密，因为每个交易的内容都暴露给网络上的每个节点，以便对其进行验证。正如所指出的，同态加密可能是解决这个问题的一种方法; the Elements Alpha 实验链允许使用附加同态承诺进行保密交易。零知识证明可能

① 但是请注意，在私有网络中，维护列表的人应该知道每个成员的身份，否则无法正确进行审查。

是另一种形式，它是一种密码原语，允许一方向另一方证明语句的有效性，而不披露其内容; 更多信息请参考 Hawk 模型。然而，这些方法是资源密集型的，因此它们在资源受限的物联网设备上的适用性有限。与维护设备隐私的情况一样，区块链可被设置为服务于特定的进程，在使用之后被丢弃，这可能是一种可接受的解决方案。

另一个在部署 (或参与) 区块链网络时要考虑的问题是决定 (或检查) 矿工集合。回想一下 (第二章第二节)，虽然一个矿工不能伪造一个事务或重写历史，但它可以阻止一个新的、有效的交易被添加到区块链。共识机制对拜占庭节点的容忍度有限; 如果参与合谋的矿工数量超过这一门槛，风险就会很大。需要明智地选择矿工节点，最小化它们之间相互勾结的机会。在私有网络中，应签订合法的合同，以使串通行为受到适当的惩罚。

智能合约的法律效力有限。正在努力使智能合约的技术规则具有法律效力和约束力。在此之前，虽然整个流程是可验证的，但交易实体对智能合约操作的结果有争议，该怎么办? 增加法律可执行性的一种方法是在智能合约中包含对真实世界合同的引用，反之亦然。这是一个被称为 “双重整合” 的过程，其工作原理如下: (a) 部署所述智能合约，在区块链上记录其地址，并将该地址包括在真正的合同内；(b) 对相应的现实世界契约进行散列，记录其散列摘要，将真实契约存储在安全空间中 (可以是集中式的，也可以是分散式的)；(c) 向智能合约发送一个交易，该交易应在其元数据中包含真实合约的散列; 然后，合同将该信息存储在自己的内部数据库中[①]。在发生法律纠纷时，可以使用存储在智能合约中的哈希值，然后显示真实世界的合同 (由该哈希唯一标识)，并证明区块链上的操作与物理世界中的预期结果之间的联系。参照 CommonAccord 和 Legal Markdown ; 这两个工具都打算通过使用模板来创建合法的真实世界和相应的智能合约。

另一个是标记资产的预期价值问题。区块链用于交易与一些财产相关联的令牌。如果设备拥有链上的令牌，并且希望在现实世界中兑换该令牌 (例如接收现金)，这种情况下有什么保证? 在不支持智能合约的区块链中，不支持双重集成。也许答案就在类似的方法中，它哈希了一个现实世界的合同，并将这个哈希作为元数据嵌入正在交易的令牌 (即通过哈希来公证)。无论如何，参与者需要事先检查交换资产的保证。

Complete Autonomy（完全自动）是一把双刃剑: 在把一份智能合约放在区块链上之前，应该仔细检查它的逻辑，代码中的故障安全机制，以防止出现死角。

① 这需要一个具有适当的允许一个可识别 (通过公钥) 用户在契约中存储数据的智能合约。

正如我们在 II-D 节中所述，有的智能合约 (或 DAOs) 的行为可能会根据用户输入而改变。或者可能有一个函数允许特权用户 (通过他们的密钥标识) 销毁已部署的合约并将其从区块链的分布式虚拟机中删除。然而，如果都不被支持，我们所面对的是一个永远无法改变的系统。这本身可能不是一件坏事。但是，如果合约上的某个函数写错了，与它的任何交互都无法撤消。一个简单的例子，考虑一个智能合约，它充当链上的一个储蓄罐。可以向它存入资金 (加密货币)，也可以从中提取资金。无论是谁在区块链上部署了它，都没有包含任何故障安全措施，比如“自毁” 功能，该功能允许删除合约并收回资金。如果合同的 “取款” 功能写错了，那么存入其中的资金将不可挽回地消失。

最后，区块链网络可能还需要以下机制来补充其功能，同时这些机制需要去中心化，以免满足网络的特性:

（1）保存指向资源的指针的 DNS 服务。例如，Blockstack 在比特币网络上提供了这样的服务。用户在比特币区块链上发送一笔适当的交易，在 Blockstack 上创建或修改一条记录。区块链的节点过滤区块链数据，获得与有效的 Blockstack 交易对应的数据，并使用它们修改对应的数据库。

（2）安全的通信和文件交换。如前所述，每个网络参与者都要读取区块链中的消息。需要专用通信通道时，应该使用 telehash、或 Whisper 等协议。网络的文件共享需求可以通过内容寻址的 P2P 文件系统来解决，如 IPFS，。

A.5 总结

综上所述，区块链和物联网的结合非常强大。区块链为我们提供了灵活的、分布式的点对点系统，以及以不可靠环境下、可审核的交互方式。智能合约我们自动化复杂的多步骤流程。物联网生态系统中的设备是区块链与物理世界的接触点。当所有这些结合在一起时，我们就可以用新的、独特的方式自动化耗时的工作流程，在加密和可验证性的条件下节省大量的成本和时间。我们相信，在物联网领域，区块链的加入将在多个行业引发重大变革，带来新的商业模式，并让我们重新考虑如何实现现有的系统和流程。

书面翻译对应的原文索引

[1] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016. doi: 10.1109/ACCESS.2016.2566339. URL https://doi.org/10.1109/ACCESS.2016.2566339.