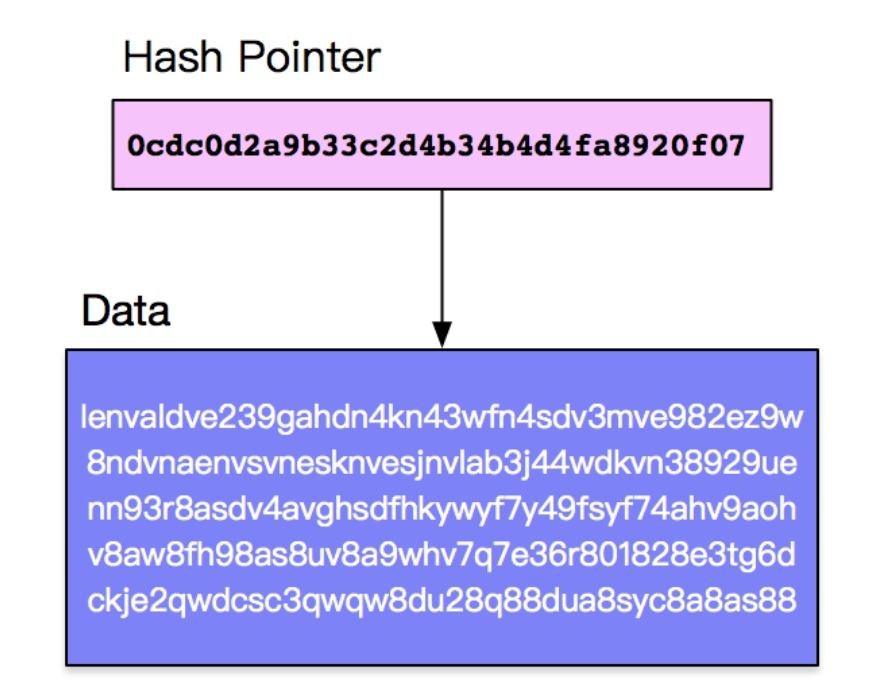
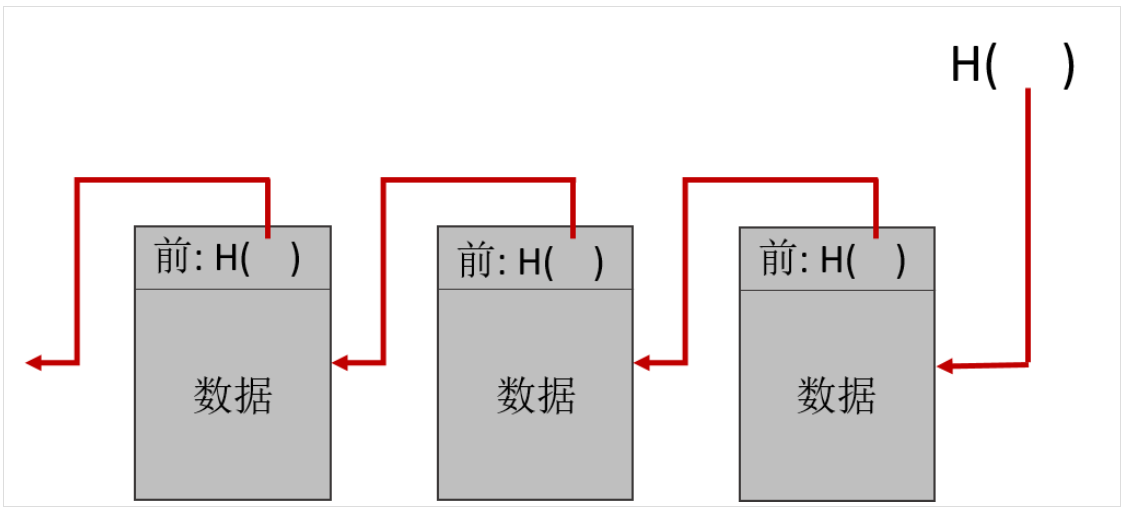
## 8.1 体系架构

### 8.1.1 区块链数据结构

#### 8.1.1.1 链型区块链

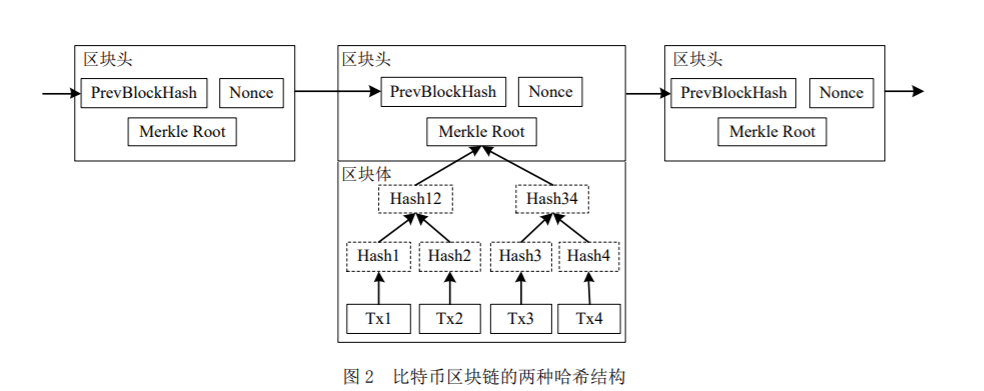
  为了实现数据的不可篡改性，区块链引入以区块为单位的链式结构。区块链简单来说就是按时间顺序将数据区块通过哈希指针的方式连接起来的一个链表。哈希指针是区块链里最常用的数据结构，一串数据的哈希值就是这串数据的指纹/摘要，因此就可以用这个哈希值来指向这串数据，如下图：

  区块链的每一个区块都有对应本区块的哈希指针，除了创世区块（即第一个区块）之外，其他每个区块都存储了前一个区块的哈希指针，从而形成如下所示的一个链条，即区块链：

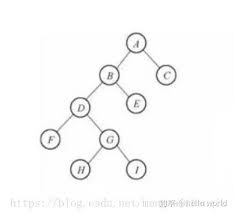


  这样的数据结构可以保证数据无法篡改，一旦篡改任何区块的数据，对应的哈希指针就会出错被检测到。

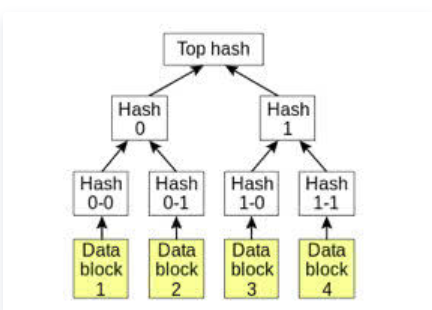
#### 8.1.1.2 树形区块链

  以比特币为例，每个区块由区块头和区块体两部分组成，区块体中存放了自前一区块之后发生的多笔交易；区块头中存放了前块哈希（PreBlockHash）、随机数（Nonce）、Merkle 根等，区块链基于两种哈希结构保障了数据的不可篡改性，即Merkle树和区块链表，下图描述了比特币的区块链数据结构： 

  Merkle tree是一种哈希二叉树，1979年由Ralph Merkle发明。在计算机科学中，二叉树是每个节点最多有两个子树的树结构，每个节点代表一条结构化数据。通常子树被称作“左子树”（left subtree）和“右子树”（right subtree）。二叉树常被用于实现数据快速查询，二叉树如下图所示：



  Merkle树由一个根节点（root）、一组中间节点和一组叶节点（leaf）组成。叶节点（leaf）包含存储数据或其哈希值，中间节点是它的两个孩子节点内容的哈希值，根节点也是由它的两个子节点内容的哈希值组成。所以Merkle树也称哈希树。叶节点存储的是数据文件，而非叶节点存储的是其子节点的哈希值（Hash，通过SHA1、SHA256等哈希算法计算而来），这些非叶子节点的Hash被称作路径哈希值（可以据其确定某个叶节点到根节点的路径）, 叶节点的Hash值是真实数据的Hash值。因为使用了树形结构, 其查询的时间复杂度为0(logn)，n是节点数量。



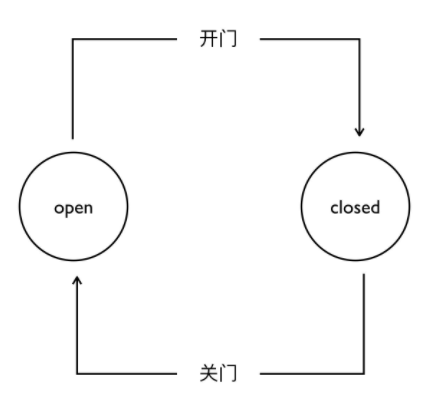
### 8.1.2 网络模型

#### 8.1.2.1 全局网络建模方法

**状态机**

  状态机是有限状态自动机的简称，是现实事物运行规则抽象而成的一个数学模型。现实事物是有不同状态的，例如一个自动门，就有open和closed两种状态。通常所说的状态机是有限状态机，也就是被描述的事物的状态的数量是有限个，例如自动门的状态就是两个open和closed。

  状态机，也就是State Machine，不是指一台实际机器，而是指一个数学模型。一般就是指一张状态转换图。例如，根据自动门的运行规则，可以抽象出下面这张图。



  切换成区块链内部视角，区块链除各个区块外，本质上还是离不开网络。可以将区块生产节点理解为生态系统中的生产者，其他节点基于区块完成交易，验证，广播等各个动作，可以理解为消费者。每个节点都有不同的状态，通过状态机能描述清楚区块链的网络节点部分。例如，智能合约接收外界输入，内部执行代码（执行动作，进行状态转换），最终达到一个新的状态。

**网络模型**

  比特币网络中的节点主要有四大功能：钱包、挖矿、区块链数据库、网络路由。每个节点都会有路由的功能，但是其他功能并不一定全部具备，一般属于比特币核心节点才会全部包含四种功能，包含所有功能的节点也叫全节点。

  以太坊网络和比特币一样，以太坊也具备钱包、挖矿、区块链数据库、区块路由四大功能，也存在不同类型的节点，与比特币P2P网络结构最大的不同在于，以太坊的P2P是有结构的。其网络采用 Kademlia（Kad）算法实现，使用该算法可以快速而又准确的路由、定位数据的问题。

**维护全局状态的一致性**

  全局状态的一致性可以分成强一致性和最终一致性，以下介绍PoW/PoS共识算法如何来维护全局状态的一致性： 1. PoW（工作量证明）：矿工通过把网络尚未记录的现有交易打包到一个区块，然后不断遍历尝试来寻找一个随机数，找到满足条件的随机数就相当于获得区块链的本轮记账权。矿工把满足条件的区块在网络中广播出去，全网其他节点在验证该区块满足挖矿难度条件，同时区块里的交易数据符合协议规范后，每个节点将该区块链接到自身维护的区块链上，从而在全网形成对当前网络状态的共识，达成全局状态的一致性； 2. PoS（权益证明）：要求节点提供拥有一定数量的代币证明来获取竞争区块链记账权的一种分布式共识机制，从而可以达成全局状态的一致性。

  全局网络建模是指区块链中所有全节点通过共识机制对等协商，共同维护区块链。全局网络建模方法下的区块链节点存储完整的账本数据（账户模型下还包括状态数据），并执行所有交易，这种建模方法对系统的存储、计算和网络造成了较大压力，对参与的节点提出了更高的配置要求。

#### 8.1.3.2 账户数据模型

**账户模型介绍**

  以太坊中的账户使用的是Account模型，并不是比特币中的UXTO模型，以太坊中有两类账户：外部账户（EOA）和合约账户。

  外部账户由私钥控制，每个账户都有自己的余额。拥有者可以通过创建和签名一笔交易从自己的外部账户发送消息，而接受方账户则不计入该金额，外部账户的地址是由公钥决定的。

  合约账户由代码控制。在一些情况下，当合约账户收到一条消息，合约账户的代码就会被激活，允许它对内部存储进行读取和写入，发送其他或者创建合约。合约账户的地址是创建合约时确定的，合约账户地址由合约创建者的地址和该地址发出过的交易数量计算得到，地址发出过的交易数量也被称作nonce。 

**账户内部结构**

  账户由四个组成部分，不论账户类型是什么，都存在这四个组成部分： \* nonce：如果账户是一个外部账户，nonce代表从该账户地址发送过的交易数量，该数量会出现在交易的字段中，起到防止双花的目的。如果账户是一个合约账户，nonce代表由该账户创建过的合约数量。 \* balance：该账户拥有的余额，以Wei为单位。 \* storageRoot：该账户的存储内容是Merkle Patricia树的根节点哈希值。Merkle树会将此账户存储内容的哈希值进行编码，默认为空值。 \* codeHash：如果是外部账户，codeHash是一个空字符串的哈希值，如果是合约账户，codeHash是该账户EVM code（编译后的智能合约字节码）的哈希值。和账户的其他字段不同，codeHash是不可变的，可以用来从状态数据库中获得相应的EVM code。

**基于账户模型的加密货币**

  以太坊选择了无现金的基于账户的系统。一个地址被看作一个账户，一个交易将一个值从一个账户转移到另一个账户。每一笔交易都有一个唯一的nonce，以防止双花攻击。为了允许只创建货币并将其分配给接收者或只从发送者那里取钱并将其作为使用的交易，因此发送者和接收者都是可选的(Zahnentferner 2018)。

#### 8.1.3.3 区块链数据库模型

  比特币、以太坊和超级账本三大应用平台的主要功能是针对数字货币与智能合约，但是数据管理性能较弱，近年来，许多研究力图将区块链技术与传统的数据库技术相结合，提升数据管理的性能，同时兼顾区块链去中心化、数据可回溯、防篡改的特性。

  BigchainDB的设计始于分布式数据库，并通过一系列创新增加了区块链的特征：分散控制、不可篡改以及数字资产的创建和移动。BigchainDB继承了现代分布式数据库的特性：吞吐量和容量与节点数量的线性校准，功能齐全的NoSQL查询语言，高效的查询和许可。由于建立在现有的分布式数据库上，因此它还继承了其大部分代码库的企业强化代码，可扩展的容量意味着具有法律约束力的合同和证书可以直接存储在区块链数据库中，许可系统支持从私有企业区块链数据库到开放的公共区块链数据库的各种配置(McConaghy et al. 2016)。BigchainDB是对像以太坊这样的分散处理平台和星际文件系统（IPFS）这样的分散文件系统的补充。

  Dinh等提出了第一个基准测试框架Blockbench，用于评估私有区块链系统，包括区块链应用的一致性算法、数据模型、执行引擎和链上应用的测试方法，并且分析了以太坊、超级账本、Parity以及 UStore的读写以及查询能力，对于区块链的设计以及瓶颈发现和解决带来了极大的帮助(Dinh et al. 2017)。

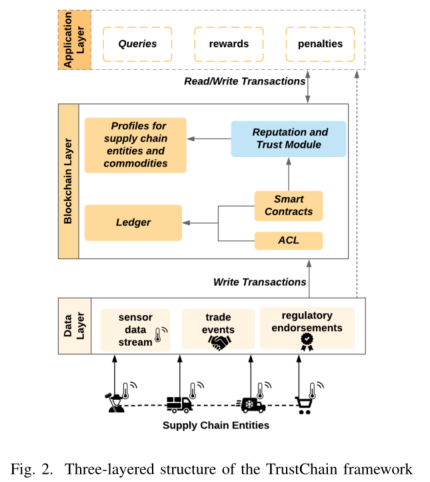
  焦通等提出08133区块链数据库系统框架，兼顾数据查询以及数据回溯。通过限制中心机构对数据记录的操作，来达到防篡改和去中心化的目的。git该数据库中有多条区块链，每一条区块链相当于传统数据库中的一张表，所有的中心机构充当数据的存储节点，所有的存储节点根据共识算法生成区块链，所有节点（包括用户）存储区块头信息，可以由区块头信息检索到记录并验证记录的正确性(焦通 et al. 2019)。

## 8.3 互操作和跨链

### 8.3.1 区块链链上链下融合

#### 8.3.1.1 数据融合

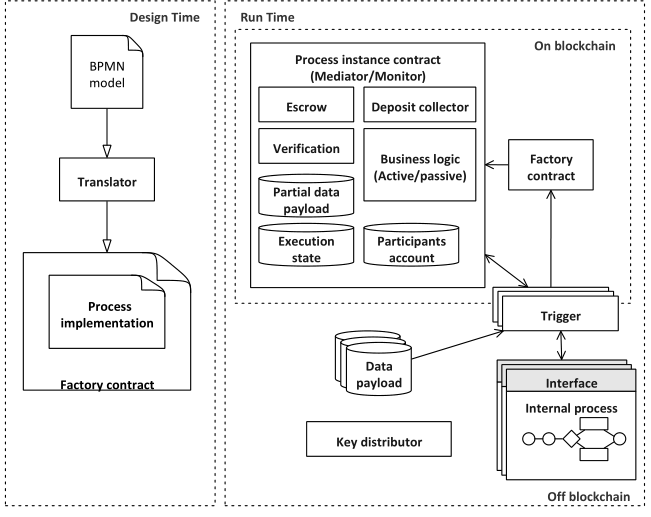
  数据融合指通过链上存储数据的关键信息、链下存储数据内容实现信息系统和区块链各存储部分数据的情况下实现业务融合。以下简要介绍几个例子：

1. Juan Benet于2014年提出星际文件系统（InterPlanetary File System，IPFS），IPFS是一种点对点分布式文件系统，旨在将所有计算设备与同一文件系统连接起来。在某些方面，IPFS与Web相似，但是IPFS可以看作是一个BitTorrent群，可以在一个Git存储库中交换对象。IPFS中的存储证明包括复制证明和时空证明。复制证明（Proof of Replication，PoRep)是一个新型的存储证明,可以让证明人提供存储证明给用户，证明用户的数据已经被复制存储到证明人唯一的专用物理存储设备上。时空证明POST（Proof of Spacetime，PoSt）是Filecoin项目采用的共识机制,使用用户存储的数据本身作为算力大小的证明。IPFS技术架构如下图所示：
2. Azaria等提出基于区块链的分布式电子医疗记录（electronic medical records，EMRS）管理模型MedRec。该系统为患者提供了全面、不变的日志，患者可以跨提供商和治疗地点轻松访问其医疗信息。MedRec利用独特的区块链属性使身份验证、机密性、问责制和数据共享，模块化设计与提供商现有的本地数据存储解决方案集成在一起，促进了互操作性。MedRec激励医学利益相关者（研究人员，公共卫生当局等）以区块链“矿工”的身份参与网络，访问汇总的匿名数据作为挖掘奖励，以换取通过工作量证明维持和保护网络。总之，MedRec促进了数据经济学的兴起，提供了大数据来增强研究人员的能力，同时让患者和提供者选择发布元数据的选择(Azaria et al., n.d.);
3. Malik等人提出基于区块链结合IoT的供应链信任管理模型，用于解决与商品质量以及在区块链上的实体记录数据相关的信任问题。模型使用Consortium区块链来跟踪供应链参与者之间的交互，并根据交互动态分配信任和信誉分数。该框架有助于提供代理和资产的信誉模型，可以为同一参与者分配特定产品的声誉， 使用智能合约实现自动化和效率(Malik et al. 2019)。

#### 8.3.1.2 流程融合

  流程融合指信息系统与区块链系统各执行部分流程的情况下实现业务融合，主要包括：链下执行，链上存储结果、链上链下混合执行。

  然而，在融合的过程中缺乏信任问题成为避免不了的障碍之一，因此Weber等人设计了一种基于区块链的链上链下流程协同机制。通过区块链技术在不受信任的参与者网络上进行去中心化和事务数据共享，该机制可以用来找到关于协作各方共享状态的协议，而不需要信任一个中央权威机构或任何特定的参与者。

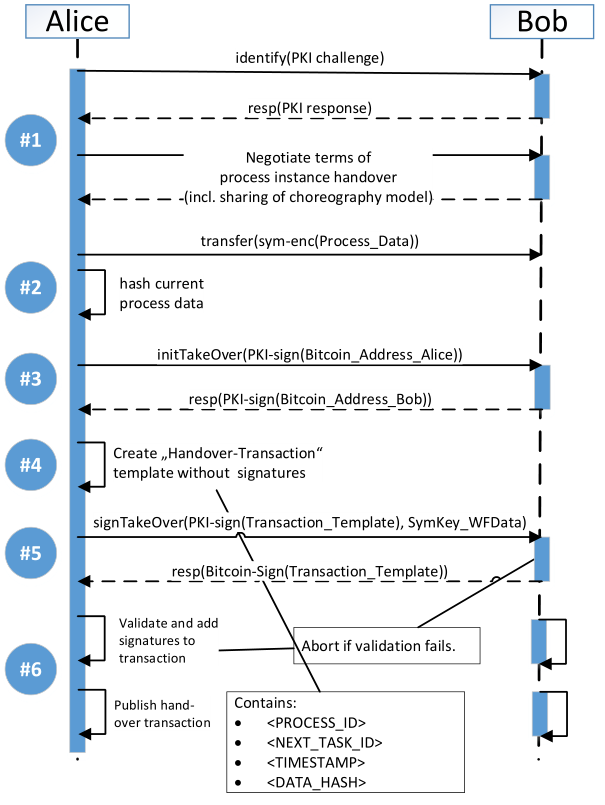
  方法概述如图1所示，通过区块链的两种方式来促进融合过程： 1. 区块链作为编排监视器，通过观察消息交换来存储所有相关参与者的流程执行状态。在此设置中，区块链充当不可变数据存储，以共享流程执行状态来创建审计跟踪。智能合约检查交互过程是否符合编排模型。另外，编排监视器可以用于管理自动付款点和托管； 2. 区块链作为参与者之间的主动中介，协调协同过程的执行。使用智能合约驱动流程并实现数据转换或计算(Weber et al. 2016)。 

  另外，在编排过程中，对流程实例的控制是在独立各方之间共享的，在流程运行时期间，没有一方拥有完全的控制权。然而，为了记录文档、记帐，有必要在运行时监控和验证流程实例。因此，为了实现业务流程运行时验证，Prybila等人基于比特币区块链设计了一种运行时验证的业务流程机制，通过探索了比特币区块链的适用性，以创建一个新的编排解决方案。以下为该方法的概述，流程图如图2所示：

  流程所有者在新流程实例的开始选择一个免费的比特币输出，作为编排的控制令牌。这个控制令牌存储进程的执行状态。同时，区块链成为令牌的去中心化存储。拥有令牌的人负责执行编排的一部分，即一个活动/任务。要在流程实例中启用并行性，可以拆分和联接令牌。参与者可以通过提交传播令牌的新事务来记录进程和移交给其他参与者的过程。

  每个事务都添加了流程当前状态的附加元数据。由于比特币交易是基于推送的，令牌发送方通过发布各自的交易来批准从一个参与者到另一个参与者的交接。然而，令牌接收方的批准也必须记录在事务中。因此，令牌接收者的签名也被嵌入到存储在事务中的流程元数据中。

  如果该交接令牌的过程以某种方式违反编排契约的约定，流程所有者可以从涉及的参与者处进行惩罚。同时，参与者也有可能证明他们成功地参与编排，从而获得奖励。为保持编排的灵活性，参与者并不是在流程设计时预先确定的，而是在流程运行时动态地选择。不利的一面是妨碍正确流程序列的执行。因此，流程所有者可以通过观察区块链来监视实例的进度。如果某个流程实例的执行偏离给定的流程模型，那么流程所有者和该实例的所有其他编排参与者可以检测到这一点并对其作出反应(Prybila et al. 2020)。



#### 8.3.1.3 输入输出融合

  区块链是一个确定性的、封闭的系统环境，目前区块链只能获取到链内的数据，而不能获取到链外真实世界的数据，区块链与现实世界是割裂的。一般智能合约的执行需要触发条件，当智能合约的触发条件是外部信息时（链下），就必须需要预言机来提供数据服务，通过预言机将现实世界的数据输入到区块链上，因为智能合约不支持对外请求。区块链是确定性的环境，不允许不确定的事情或因素，智能合约不管何时何地运行都必须是一致的结果，所以虚拟机（VM）不能让智能合约有 network call（网络调用），这可能导致结果就是不确定的。目前链上链下数据的协同主要有以下4大发展方向：

1. 大规模高性能点对点网络。围绕区块链应用，原来大规模点对点的网络，这个才是最重要，因为区块链本来就是点对点传输的。如果说网络技术没有突破，区块链系统性能是很难提升。
2. 模块化安全密码学协议。本来区块链就是分布式加上密码。安全密码学协议模块化，区块链子系统嵌入不同的，模块化安全密码学协议也是研究方面。
3. 高性能可编程计算引擎。我们希望用户不同的智能合约用不同的编程语言来编，既然用不同的编程语言，那你就需要高性能可编程计算引擎。
4. 可定义的数据分发协议。

**预言机（Oracle）是什么？**

区块链链下信息写入区块链的机制，一般被称为预言机（Oracle Mechanism）

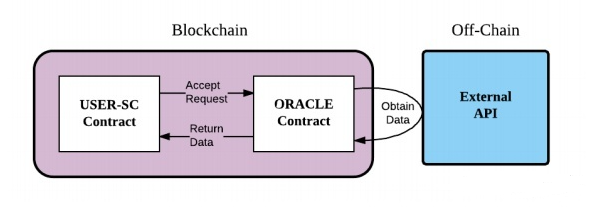
  预言机的功能就是将外界信息写入到区块链内，完成区块链与现实世界的数据互通。它允许确定的智能合约对不确定的外部世界作出反应，是智能合约与外部进行数据交互的唯一途径，也是区块链与现实世界进行数据交互的接口。

  在《精通以太坊（Matering Ethereum）》一书中，提出了三种预言机的设计模式，分别是：

* 立即读取（immediate-read）
* 发布/订阅（publish–subscribe）
* 请求/响应（request–response）

**预言机的工作流程**

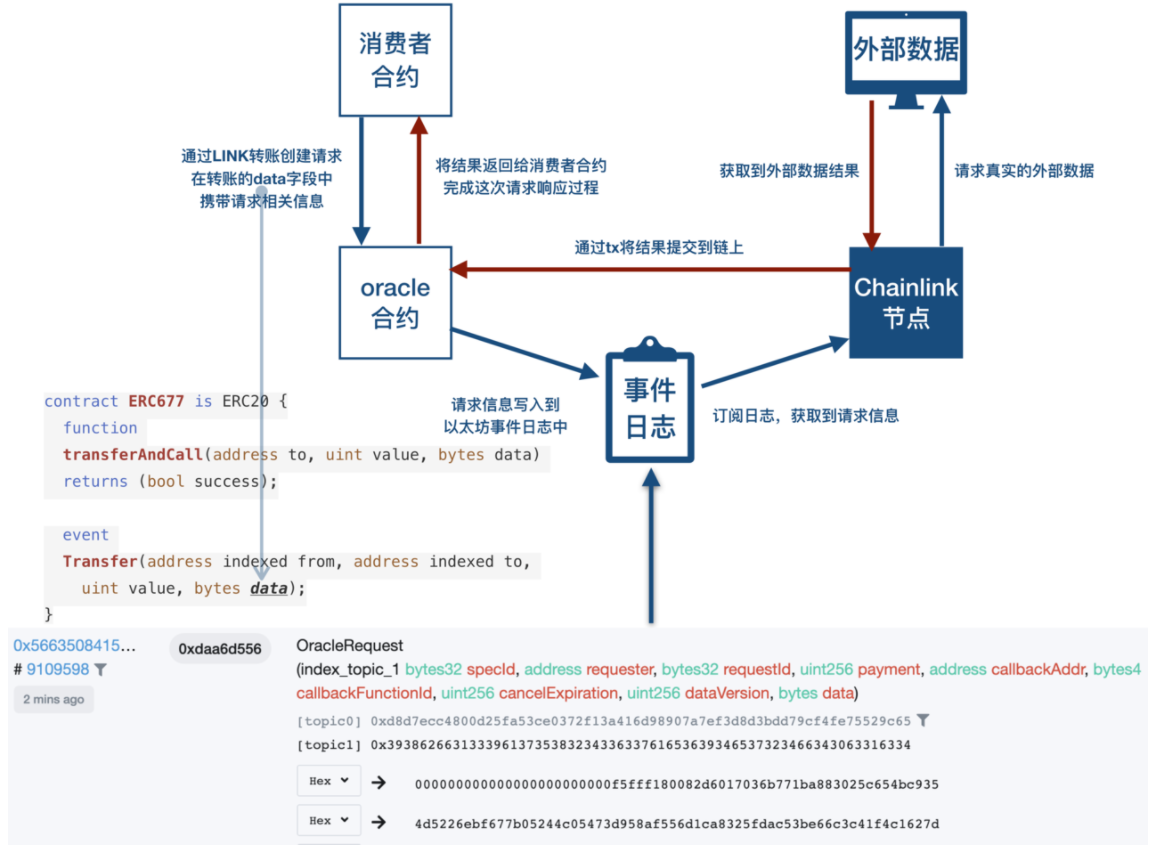
  链上的智能合约把相应的请求发给链上的Oracle合约，然后通过链下的API接口获得外部数据。即外部数据给链上的Oracle合约，Oracle合约再把数据回传给用户的智能合约。这与传统互联网中的直接代码获取数据不同，因为区块链与外部世界进行数据交互是不允许这与操作的。



**Chainlink**

  Chainlink是一个去中心化的预言机项目，它的作用就是以最安全的方式向区块链提供现实世界中产生的数据。Chainlink在基本的预言机原理的实现方式之上，围绕LINK token通过经济激励建立了一个良性循环的生态系统。Chainlink预言机需要通过LINK token的转帐来实现触发。LINK是以太坊网路上的ERC677合约。

  基于LINK ERC677 token完成的预言机功能，就属于 **请求/响应模式** 的设计模式。这是一种较为复杂的模式，图中展示的是一个不含有聚合过程的简单请求/相应流程。



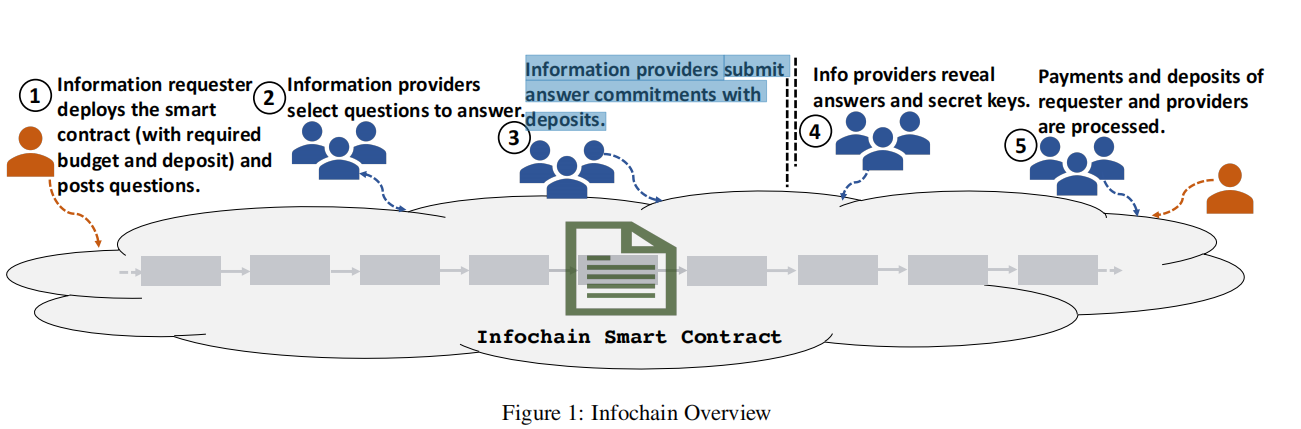
以Chainlink提供的TestnetConsumer合约中的一个requestEthereumPrice方法为例来简单讲一下请求响应的流程。这个函数定义如下：

function requestEthereumPrice(address \_oracle, string \_jobId) public onlyOwner  
{  
 Chainlink.Request memory req = buildChainlinkRequest(stringToBytes32(\_jobId), this, this.fulfillEthereumPrice.selector);  
 req.add("get", "https://min-api.cryptocompare.com/data/price?fsym=ETH&tsyms=USD");  
 req.add("path", "USD");  
 req.addInt("times", 100);  
 sendChainlinkRequestTo(\_oracle, req, ORACLE\_PAYMENT);  
}

  该实现的功能就是从指定的API (cryptocompare)获取ETH/USD的交易价格。函数传入的参数是指定的Oracle地址和JobId。将一些列的请求参数组好后，调用sendChainlinkRequestTo方法将请求发出。

**Infochain**

  Infochain是基于区块链的分布式、不可信、可见的预言机，在以太坊区块链上实现去中心化、无信任和透明的区块链预言机。与传统的去中心化系统的实现方式不同，Infochain通过实施博弈论的同行一致性机制来解决真实性问题，证明即使当代理有外部动机误报信息，对等一致性机制可以得出引出真实的信息。



08313115-3 Infochain 架构

Infochain是基于预言机的去中心化的分布式问答模型，其工作流程分为5步：

1. 信息请求者部署智能合约(包含所需的预算和定金)并发布问题。
2. 信息提供者选择问题来回答。
3. 信息提供者提交回答承诺与存款。
4. 信息提供者揭示答案和秘密密钥。
5. 处理请求者和提供者的付款和存款。

由此可以保证通过Infochain获取的数据是真实的。

### 8.3.2 跨链

#### 8.3.2.2 公证人模型

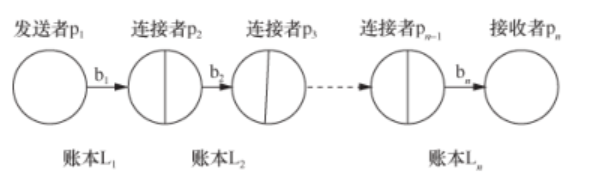
  公证人模式是基于interledger协议创造的一种技术框架，与现实世界中的中介机制类似，引入交易双方能够共同信任的第三方充当公证人来作为中介，公证人既可以自动的监听和响应来自链上的交易请求和确认信息，也可以主动地对发生的事件或请求进行监听和响应。公证人模式分为单签名公证人¸多签名公证人和分布式签名公证人（分布式签名公证人模式采用安全多方计算的思想，安全性更高，但实现难度也更大。以下分别展开介绍这三种公证人模式：

1. 单签名公证人模型：也叫中心化公证人模型，通常由单一指定的独立节点或者机构充当，它同时承担了数据收集、交易确认、验证的任务。这是最简单的模式。其优点在于处理速度较快，技术结构相对简单，但是这种方式的问题也很明显，即中心化的公证人的安全风险；
2. 多签名公证人模型：通常由多位公证人在各自账本上共同签名达成共识后才能完成交易，多重签名公证人的每一个节点都拥有自己的一个密钥，只有当达到一定的公证人签名数量或比例时，跨链交易才能被确认；
3. 分布式签名公证人模型：分布式签名公证人模型和多签名公证人模型最大的区别在于签名方式不同，它采用了多方计算（Multi-Party Computation）的思想，安全性更高，实现也更复杂。对于跨链交易，系统仅产生一个密钥，密钥以碎片形式发送给每个公证人节点。

  无论使用哪种签名方式，公证人模型核心解决的问题体现在两方面：

1. 保障跨链交易原子性：即跨链交易要么发生，要么不发生，否则两条链的不一致和不同步状态将成为跨链交易最大的系统漏洞，是跨链交易必须要解决的难点。
2. 完成对另一条链交易确认：包含了两个层次的问题，一是确认交易已经发生并且上链，写入了区块账本；二是该交易已经获得了系统足够多区块的确认，这样由于系统发生重构而导致交易无效的概率将非常低。

  瑞波的InterLedger协议中原子模式的实现方式是典型的公证人模型，在InterLedger协议中，包括发送者、连接者、接收者和公证人等角色。发送者把资产转给公证人组多签地址进行资产托管，接收者确认收到转账后在收据上签名。当前账本公证人根据收据将资产转给连接者(郭朝 et al., n.d.)。支付链如图1所示。



## 8.5 区块链与其他信息技术的融合

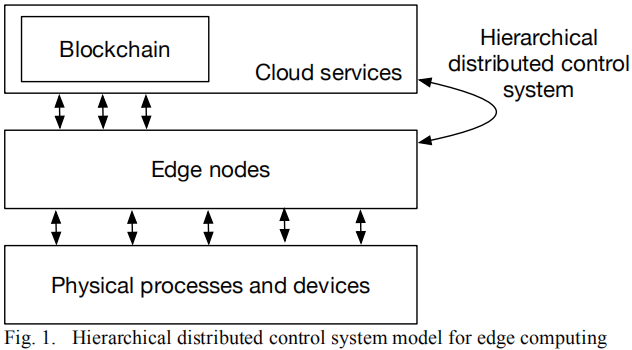
### 8.5.2区块链与云边端体系结构

  边缘计算可以在网络边缘处理或预处理终端收集或产生的数据，无需将全部数据上传云端，从而减轻云计算中心的网络负载与计算能耗、降低服务延迟与隐私泄漏风险。但在处理复杂统计与分析任务时，边缘计算服务有限的计算和存储能力不能满足任务的需求，需要将边缘计算和云计算结合，互为补充，同时结合终端设备产生的海量数据建构几个层次型的云边端结构来满足复杂任务的需求。在云边端融合架构中，由于边缘服务器或不同的云服务节点等可能分属不同利益方，且在复杂环境下云边端系统易受到攻击，引入区块链技术为解决这些问题提供了新思路。

#### 8.5.2.1 融合区块链的云边端体系架构

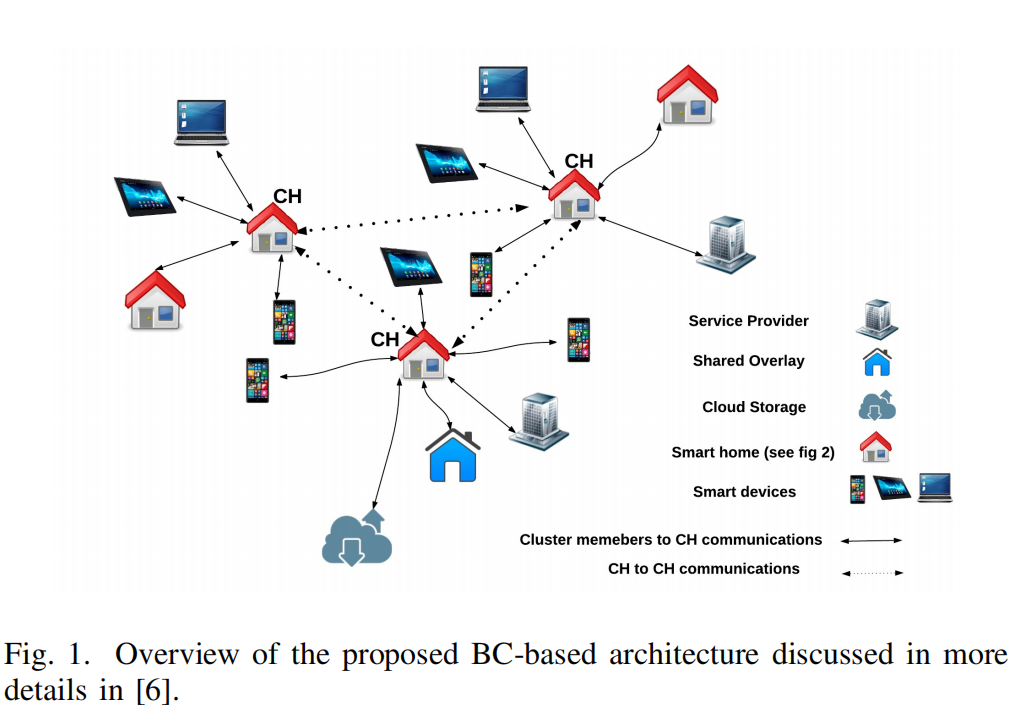
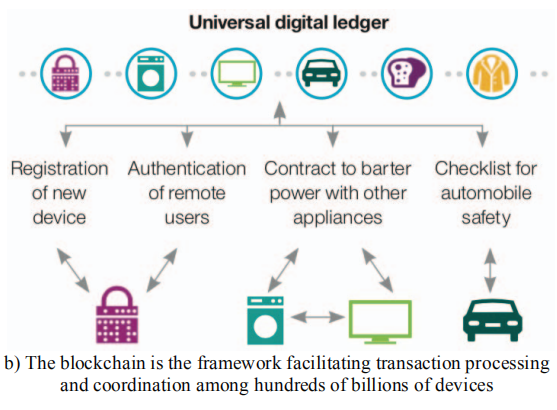
  边缘计算与区块链融合能提高物联设备整体效能。以物联网设备群为例，一方面移动边缘计算可以充当物联设备的“局部大脑”，存储和处理同一场景中不同物联设备传回的数据，并优化和修正各种设备的工作状态和路径，从而达到场景整体应用最优。另一方面，物联终端设备可以将数据“寄存”到边缘计算服务器，并在区块链技术的帮助下保证数据的可靠性和安全性，同时也为将来物联设备按服务收费等多种发展方式提供了可能性。

1. Stanciu提出的一个分层分布控制系统，用于在连接到网络的终端设备附近提供计算资源，在物联网、智能电网、医疗保健、智能家居等领域有着广泛的应用。该系统为三层架构，分别是云服务层、边缘层以及物理层。其中，云服务层和边缘层是基于Hyperledger Fabric的区块链解决方案，其中的功能块将作为主管级的智能合约实现。与在执行层执行的负责实际过程控制的边缘节点的集成是基于微服务架构的，Docker容器实现功能块，而Kubernetes平台用于协调容器跨边缘资源的执行。这种类型的架构被用于边缘计算模型，既可以为监测环境的大规模传感器网络提供计算资源，也可以提供基于数据处理和云资源集成的智能服务。具体如图085211-1所示。



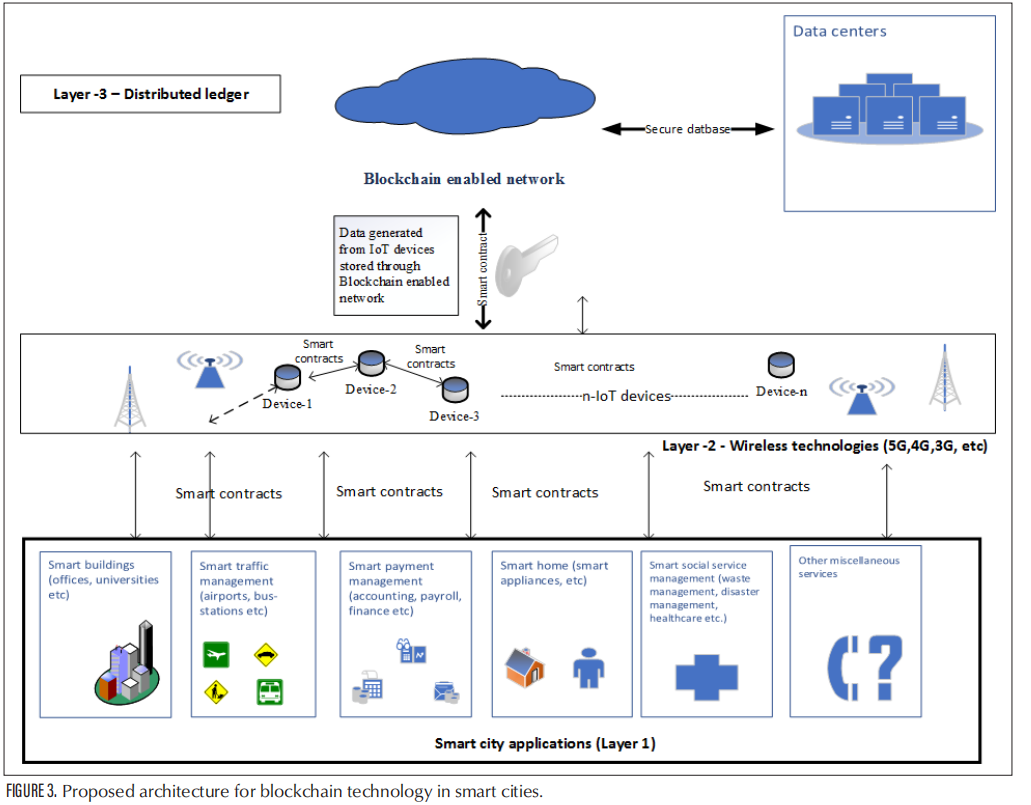
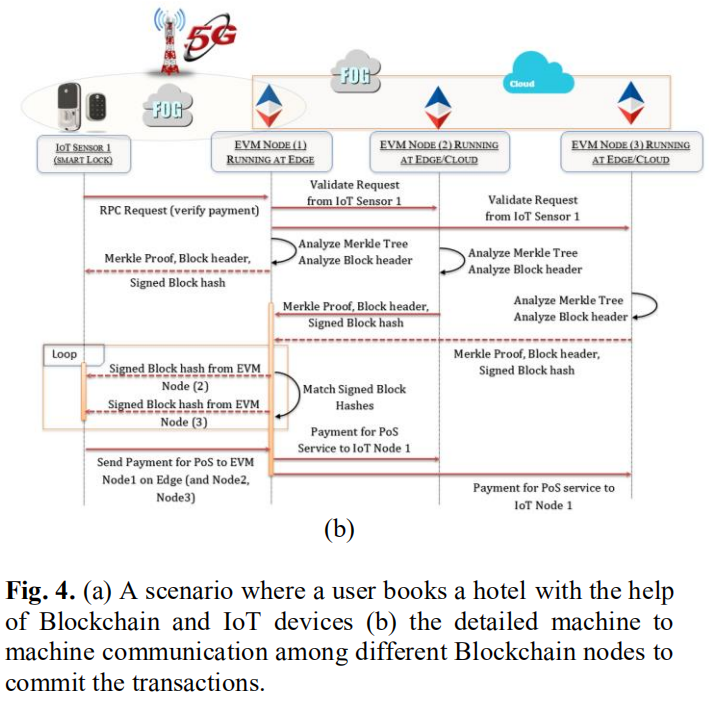
#### 8.5.2.2 智能家居

  随着物联网技术的发展，家具的智能化和联网化趋势愈发明显，随之而来的安全问题也越来越得到重视。区块链以及智能合约被广泛认为是能够解决大量智能终端联网的方案之一。

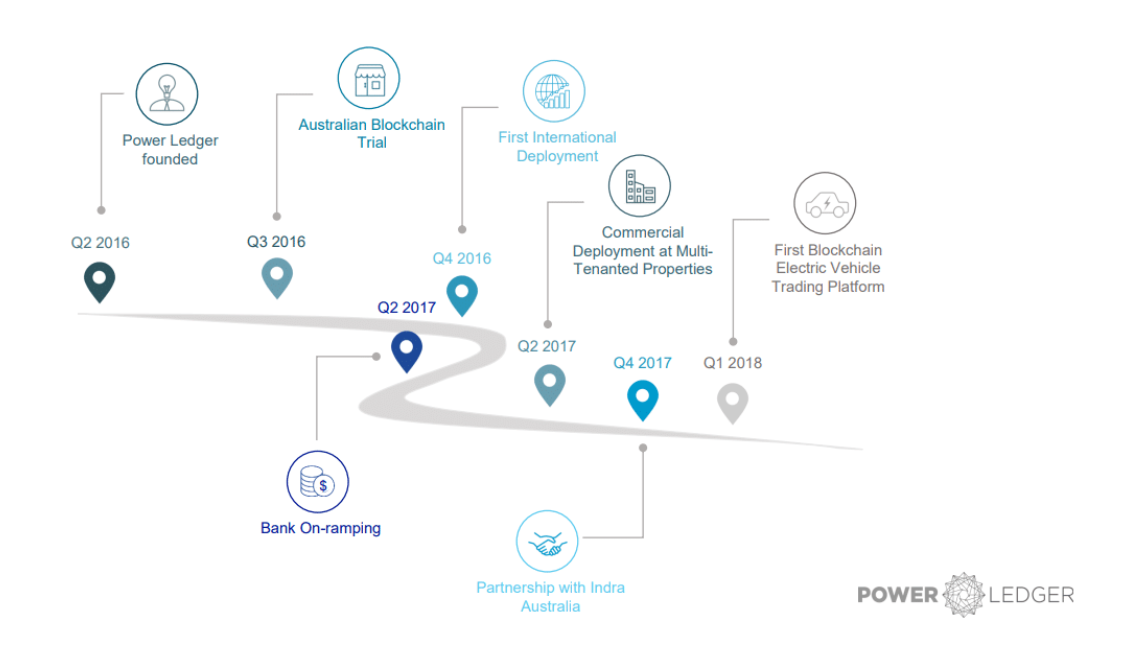
1. Dorri提出一个轻量级的区块链实例化架构，适合在物联网中使用。该架构在智能家居环境中得到较好的表现，由三个主要部分组成，即:云存储、覆盖网络和智能家居。在这个架构中每个智能家居系统都配备一个随时在线的高计算资源设备，称为“矿工”，负责处理与家居内外的所有通信。为实现用户对智能家居事务的控制，该矿工设备会给相应的设备分发秘钥，设备之间的通信通过秘钥进行安全同行。该计算设备还保留一个私有的、安全的区块链账本，用于控制和审计通信。根据机密性、完整性和可用性等基本安全目标对该系统进行安全性分析，结果表明Dorri的基于区块链的智能家居框架是安全的。 
2. 如今，智能家居系统的众多应用为用户提供选择，包括降低能耗、设备故障的警告、高可用设备和软件、诊断等。智能家居环境的互联网连接、动态和异构特性带来新的安全、认证和隐私挑战。在智能家居系统中，用户优先考虑设备便利性和连通性，反而不会太重视设备以及用户个人的隐私。针对此问题，Thanh提出一种基于区块链技术的智能家居数据隐私保护方法，即基于物联网区块链的智能家居，即SHIB。SHIB体系结构具有数据私密性、可信访问控制和高扩展性等优点。该体系结构明确并解决了智能家居环境中数据隐私、信任访问控制、扩展能力等方面的挑战。允许用户在智能控制合约中建立隐私策略，并存储在以太坊区块链网络上，只有合约的创建者可以在合约中添加新策略、更新或删除隐私策略，保证智能家居的数据隐私安全。 

#### 8.5.2.3 智慧城市

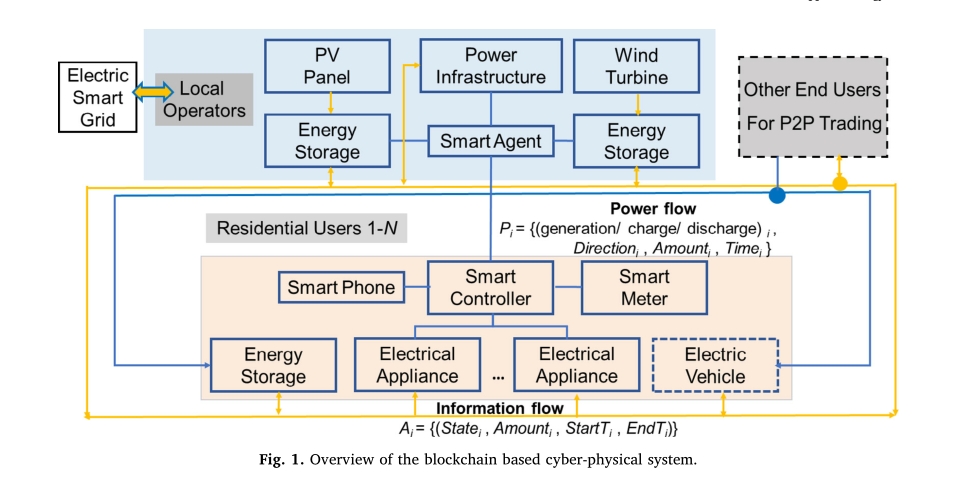
  近年来，在智慧城市领域开展了前所未有的工作。发展智慧城市的目的是提高居住在其中的人们的生活质量。为了实现这一目的，人们利用了物联网和云计算等技术。区块链技术也是有前途的技术之一，可以为其最终用户提供无数有价值的服务。作为新兴技术，区块链在智慧城市的诸多领域有较大应用潜力。在基础设施方面，与新型智慧城市相结合，探索在信息基础建设、智慧交通、能源电力等领域实现赋能，提高城市管理智能化，标准化。

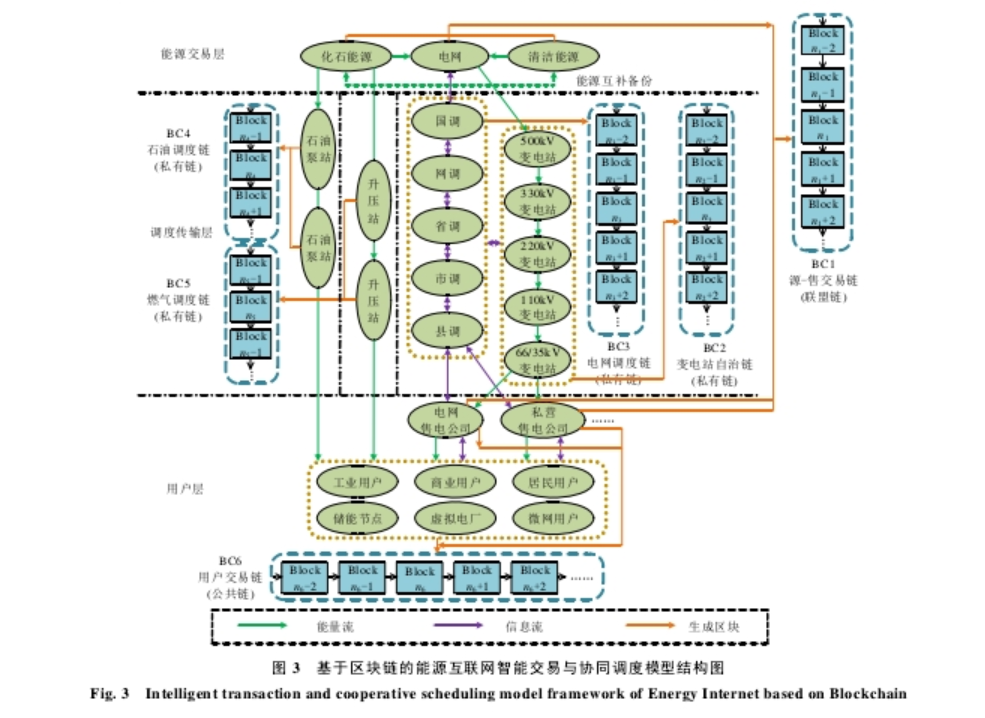
1. Saqib Hakak提出一种基于区块链的智慧城市架构，该架构分为三层，第一层包括所有潜在的应用，这其中包含了智慧大厦、智慧交通、智慧支付、智能家居、智慧社会服务等；第二层作为信息载体，由异构互联网和通信技术组成，包含5G、4G等现今通信技术；第三层为基于区块链的存储保护层，用于可信节点达成共识后验证信息块。智慧城市中每个参与节点都包含一份智能合约，该智能合约包含各节点参与信息交换的特定规则，所有交换的信息将被存在第三层。基于区块链的智慧城市架构可以记录每个参与者的访问控制记录，考虑到由于智慧城市有众多设备参与，数据的产生需要征税，区块链则可以提供部分或者完全的数据。其次区块链的激励机制可以激励公民使用不同的智慧城市应用，加速智慧城市建设。目前已有相关应用，如法国城市大脑、智慧迪拜以及柬埔寨首都金边智慧城市项目。 
2. Rahman提出了一种基于区块链的基础设施，以面向安全和隐私的时空临时智能合约服务，以实现大型智能城市中可持续物联网（IoT）支持的共享经济。该基础架构利用边缘的认知雾节点来托管和处理来自移动边缘IoT节点的有效负载和交易，并使用AI处理和提取重要事件信息，同时生成语义数字分析，最后将结果保存在区块链和分散的云存储库，以促进智慧城市共享经济服务。该框架提供一种可持续的激励机制，可以潜在地支持安全的智能城市服务，例如共享经济，智能合约以及与区块链和物联网的网络物理交互。以满足智慧城市物联网数据服务，该服务提供网络物理共享经济服务，通过智能合约，该框架可以向提供复杂的金融服务，而不需要中央审核机构。 

#### 8.5.2.4能源互联网

  能源互联网和区块链都具有开放、互联、共享、对等的共同理念。因此，区块链将有望成为解决能源互联网发展瓶颈问题的突破口。目前，国内外已有少数公司开始探索并实践区块链技术在能源互联网中的应用，下面将简要介绍几个区块链技术在能源互联网中应用的实例： 1. Power Ledger由澳大利亚的区块链软件公司Ledger Assets创立。Power Ledger构建了全球首个使用区块链的P2P电力交易系统，这套系统的出现是分布式能源交易的一次伟大尝试，为减少交易成本提供了有效途径。不同于比特币采用的Pow(工作量证明)机制，PowerLedger采用的是POS(权益证明)机制，利用自己的区块链Ecochain，使电能在产生的时候系统就能确定电能的所有者，然后通过一系列交易协议完成电能所有者和消费者之间的交易，住户可以直接将剩余电能卖给其他住户，出售价格高于直接出售给电力公司的价格，电能的生产者获得了更大的收益，电能的消费者也获得了更低的用电成本; 

1. 利用区块链自治协同管理和智能交易技术，可研究和解决多能源系统在交易完全去中心化下产能、用能、节能等各互补能源节点的能效自主智能交易。例如，Noor构建了基于区块链的网络物理系统，下图所示。参与者包括住宅用户以及来自商业和工业领域的其他最终用户，他们都与本地运营商相互联系。每个最终用户都有自己的智能控制器，可以与P2P网络中的其他用户交换信息和价值。运营商将P2P电力交易系统作为一个社区来运行，而电网将这个社区作为一个单独的用户使用，但是自治性要远高于该社区中的任何个人。运营商可以通过协商的价格从电网中为那些未满足的需求购买电力，这有助于减少社区对电网的影响，并且通过区块链智能合约交易实现边缘侧设备及存能元件需求侧管理及对等交易(Noor et al. 2018);



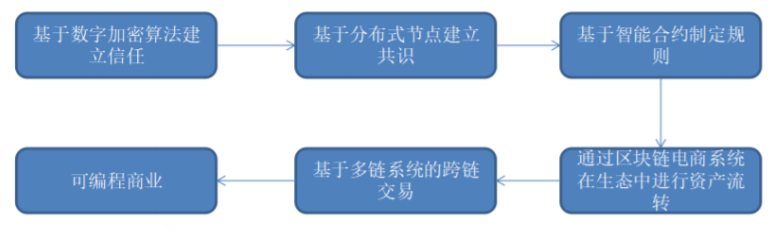
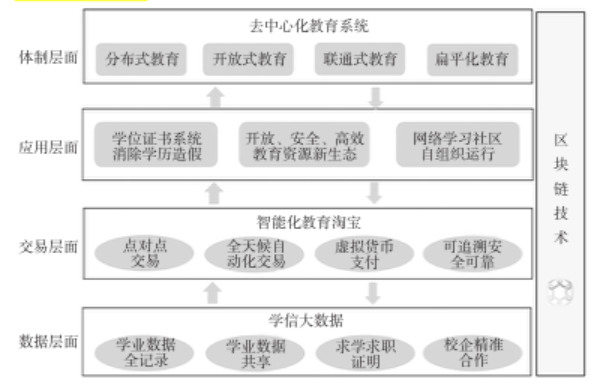
3. 利用区块链去中心的分布式决策与调度机制，可研究和解决在能源系统调度部分去中心化下源–网荷–储各节点主动参与能量流的分布决策、协同调度与潮流分配。龚钢军等从多能源系统的物理拓扑结构和逻辑协议层次分析，考虑能源节点区块链算力不匹配问题，提出了基于区块链技术的能源互联网物理层次架构和逻辑协议层模型,如下图所示。在调度部分去中心化后，提出了基于区块链的垂直分级调度系统和多级变电站的协同调度模式，并定义了该模式下各级调度、电厂、变电站、售电公司与各类用户的节点属性和任务职能，以及处在不同层级、由不同节点所构成的各区块链的类型。形成了以“交易完全去中心化，调度部分去中心化”为特点，基于区块链技术构建的智能交易与协同调度模式，为实现能源互联网高效安全运行贡献了方案及思路(龚钢军 et al. 2019)。 

#### 8.5.2.5 共享经济

  共享经济是应用经济学的专业术语，最早由美国德克萨斯州立大学社会学教授马科斯·费尔逊（Marcus Felson）和伊利诺伊大学社会学教授琼·斯潘思（Joel.Spaeth）于1978年提出。共享经济可以定义为以获得一定报酬为主要目的，基于陌生人且存在物品使用权暂时转移的一种新的经济模式。这种经济模式已经渗透到社会和人们生活的方方面面，使人们开始关注共享经济。

  基于对共享经济概念的充分理解，再结合区块链技术的特点——去中心化、点对点网络、时间戳、不可篡改、共识机制、智能合约，可以发现，共享经济和区块链技术有着在本质上共通的属性。因此区块链+共享经济的优势可以归纳为：去中心化降低成本、智能合约促成平台自治、公开透明保证资源合格、时间戳解决纠纷。

  综合来说，在区块链系统中，“区块链+共享经济”的基础主要如下有几点：首先，基于数字加密和分布式节点签名等技术建立系统角色之间的信任和共识；其次，系统中资产的交易使用、违约赔付、到期核算等具有规则属性的业务可以借助于智能合约公平自动进行，用户的不合规行为会受到对应的处理，用户有利于生态建设的行为则会受到奖励。正是在智能合约的这种支撑下，链上用户可以直接交互，根据既定的生态规则，实现平台的自治；另外，在解决信任问题的基础上，依托共享平台的电商系统，加之通证激励的设计，可以有效推动共享资产在多链之间的交易流转，实现共享经济的可编程商业生态，以下举出两个案例进行说明：

1. 目前，民宿、共享乘车（汽车合乘）等提供剩余资源并实现有效利用的共享经济已经得到了人们的关注，我们也期待能够通过使用区块链技术来构筑分布式的共享经济服务。通过平台上代币的激励形成不存在中央服务提供者的网络，并且能自律地持久运行，同时对法律法规有一定的耐受性的共享经济平台也开始出现。共享经济和区块链的结合让P2P租赁共享平台出现是一个典型的例子，例如：Airbnb、HomeAway、GSENetwork、FlipKey16以及OneFineStay等。这类平台有类似特点，如用户将闲置的社会化资源暂时交给别人共享使用、供求双方基数较大、供求一体化、供求主体是个人或小型经济组织等。这类平台的主要作用是将闲散的社会化资源加以整合共享，让供给和需求双方直接对接，实现供应和需求的最优匹配，进而达成资源的高效流动。 
2. 区块链技术有望在互联网+教育生态的构建上发挥重要作用，其教育应用价值与思路主要体现在六大方面：建立个体学信大数据、打造智能化教育淘宝平台、开发学位证书系统、构建开放教育资源新生态、实现网络学习社区的“自组织”运行以及开发去中心化的教育系统。图2显示了基于区块链技术构建的互联网+教育新生态体系。区块链技术有助于推动教育体系变革，加速教育系统进化发展。下图为基于区块链技术的互联网+教育新生态图： 

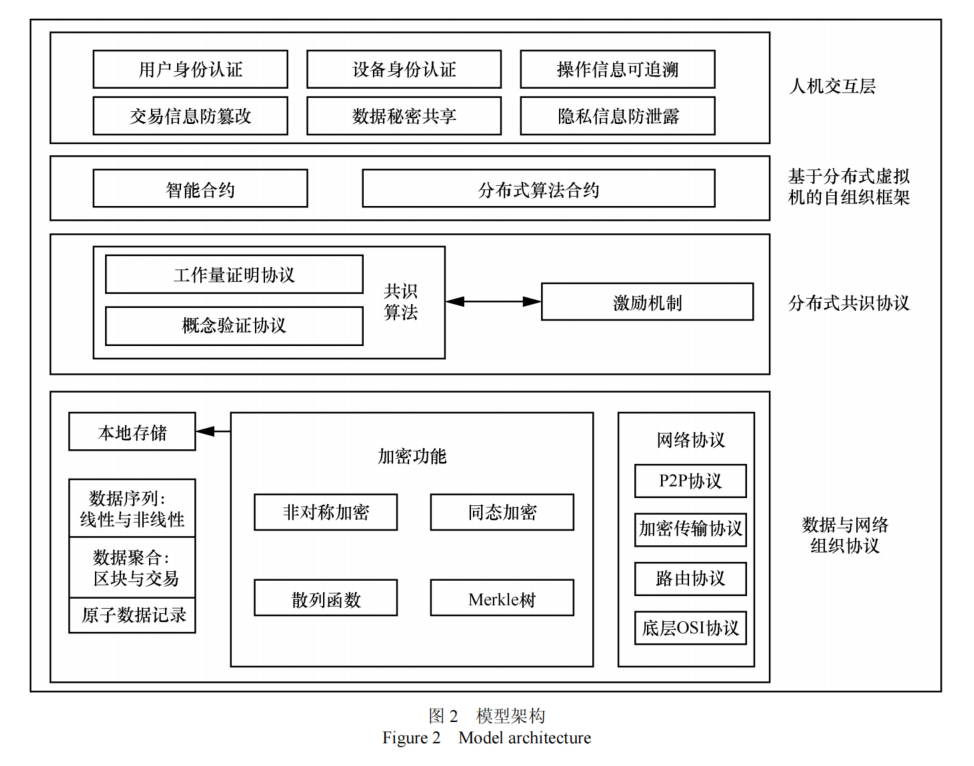
* 建立个体学信大数据架起产学合作新桥梁：区块链技术在教育领域可以用做分布式学习记录与存储，允许任何教育机构和学习组织跨系统和 跨平台地记录学习行为和学习结果，并永久保存在云服务器，形成个体学信大数据，有助于解决当前教育领域存在的信用体系缺失和教育就业中学校与企业相脱离等实际问题；
* 打造智能化教育淘宝平台，实现资源与服务的全天候自动交易：通过嵌入智能合约，区块链技术可以完成教育契约和存证，构建虚拟经济教育智能交易系统。该系统中各种服务的购买、使用、支付等工作全部由 系统自动完成，无需人工操作，同时购买记录无法篡改、真实有效，所有的交易和合约数据都将被永久保存；
* 构建安全、高效、可信的开放教育资源新生态：
  + 应用区块链技术加强资源版权保护：基于非对称加密算法保护的版权信息其安全性与可靠性更高，同时鉴于区块链公开透明的特点，任何资源创建信息都可以被使用者查询、追踪、获取，进而有助于从源头上解决版权归属问题；
  + 应用区块链技术降低OER运营成本：将区块链技术的去中心化应用到OER建设中可节省大量中介成本。用户与用户间可直接通过点对点的传播方式进行资源共享，从而减少在大量中介平台上研发与管理维护的投入，改变OER运行机制，有效降低OER运营成本；
  + 应用区块链技术促进资源共享：利用区块链的分布式账本技术，将教育资源分布式存放在不同的区块中，通过点对点的传播方式，所有节点将通过特定的、达成共识的软件协议直接共享学习课件和工具软件等资源，既有助于提高共享效率，又可以解决资源孤岛问题；
  + 实现网络学习社区的真正“自组织”运行，主要体现在：使用虚拟币提高社区成员参与度，形成社区智慧流转体系、保护社区成员智力成果，生成观点进化网络、净化社区生态环境，实现社区成员信誉度认证；
  + 开发去中心化教育系统，全民参与推动教育公平：利用区块链技术开发去中心化教育系统，有助于打破教育权利被学校或政府机构垄断的局面，使教育走向全面开放，形成全民参与、协同建设的一体化教育系统。未来，除了政府机构批准的学校、培训单位等教育机构具有提供教育服务的资质外，将有更多的机构、甚至个体承担专业教育服务提供商的角色，并且基于区块链的开源、透明、不可篡改等特性能保证其教育过程与结果的真实可信(杨现民 et al. 2017)。

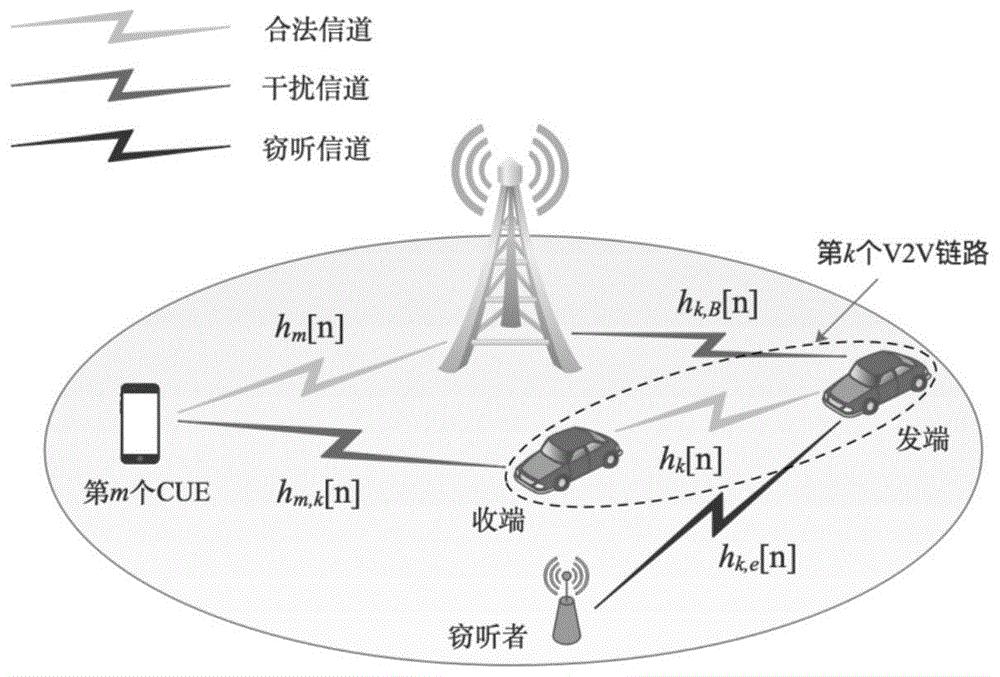
#### 8.5.2.6 车联网

  随着城市智慧化的加速发展，车联网为人类提供了交通管理和出行等方面的便利，成为智慧城市的重要标志，并被写入国家“十三五”规划中(Dennis, Owenson, and Aziz 2016)。越来越多人员和车辆的参与和高度动态的拓扑结构，导致车联网中个人信息可用性和用户隐私保护重要性之间不协调的矛盾，车辆人员信息或车辆位置信息泄露等安全风险对车联网的广泛应用形成了桎梏。

  因此，车联网在提供服务的同时需要重点设计隐私保护模型，使用户既能享有高质量的服务，又能避免自己的隐私信息被第三方非法获取。区块链技术中的去中心化、匿名化特性为解决车联网中相关的问题提供了思路。

  区块链技术是集加解密、数字签名、密钥分存、分布式存储及一致性问题和共识算法于一体的复合技术。区块链将各个数据块进行链接，在每个区块中，都存在区块头和区块体两个结构。区块头包含了版本号、目标散列值、前一个区块地址、时间戳等信息，而区块体中封装了当前所有交易的数据结构。这种数据结构能够从预先选择的节点跟踪每个块的信息并且影响后续节点的信息,其加密方法确保恶意攻击难以篡改信息。根据区块链的可追溯性，车联网用户可以查看所有的交易记录，同时区块链的匿名性保证了人们无法匹配其他人的账户。区块链信息的高度透明、防篡改，可有效降低隐私泄露的风险。王瑞锦等通过设计车联网区块链的块数据结构、网络构建、节点之间协同工作等机制，保证了车联网用户信息的隐私(王瑞锦 et al. 2020)。区块链在车联网中的应用如下：

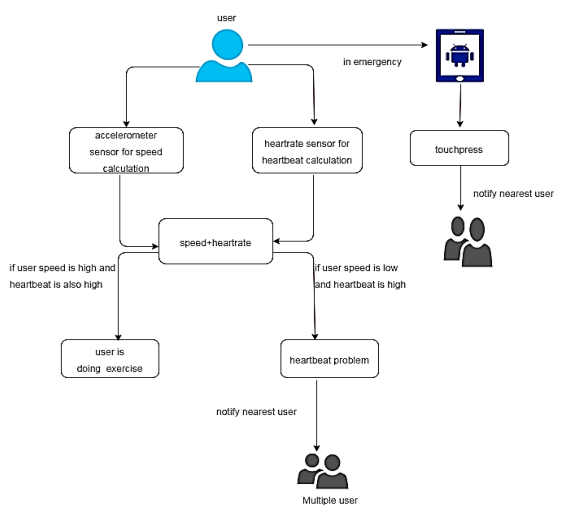


1. 车险理赔。在生活中，经常出现的套牌、冒牌问题可以通过区块链技术轻易处理。GPS和北斗能帮助车辆准确地定位到一个经纬度上，联网的车辆也会像比特币系统里面的余额一样，可以进行精确追踪。通过追踪每一辆车的位置信息，利用智能合约规定每一辆车的义务与权力，从而实现避免套牌、冒牌车辆的上路。在车险理赔过程中，一旦发生交通事故，区块中的每一个节点都能够记录事故车辆的详细位置信息和时间戳，从而可以实现快速有效的事故责任认定，提高理赔的效率且保障各方的合法权益(杨柳青 2018)；
2. V2V通信。车辆网络是一类特殊的移动自组网（MANET），目前国内外对车辆网络的研究大多基于车载自组网（VANET）。车载自组织网络（VANET）采用 ad-hoc 的网络形式以便实现车与车（V2V）的直接通信(Mir and Filali 2017)。路基设施与车的通信在顶层是靠路侧单元（RSU）与车载单元（OBU）完成。为了实现网络的负载均衡，避免出现因路侧单元负荷过大而造成的单点故障影响整个系统，利用RSU和OBU的通信实现车与车的直接对话机制，V2V也越来越倾向在一定程度上实现去中心化的功能。将车牌作为全网内的唯一标识应用到车联网中，再利用标志密码算法，可以保障车辆之间共享信息的私密性，同时满足在车联网系统中实现快速身份认证。区块链技术还可以通过智能合约来约束通信车辆双方的权利和义务，其去中心化的理念适合小范围内车辆自组织网络中实现内车与车的直接通信(刘博 and 周华平 2018)。

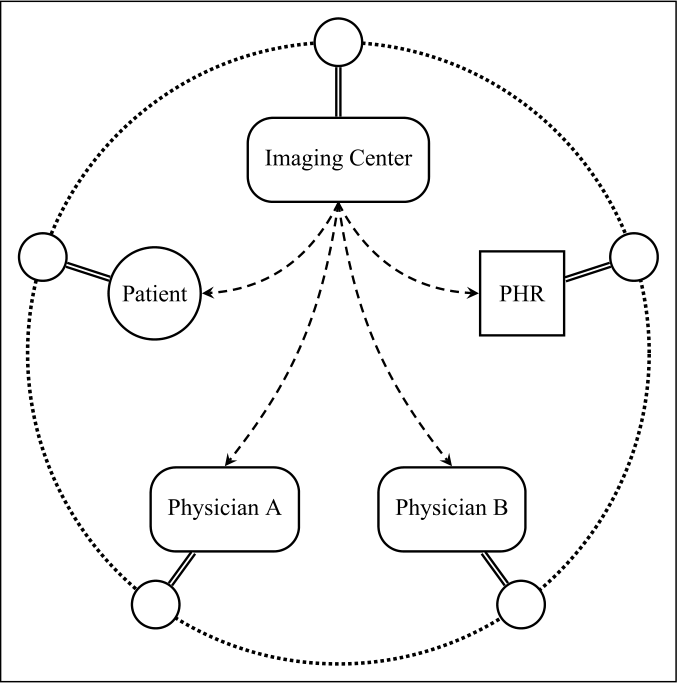
#### 8.5.2.7 智慧医疗

  区块链已发展多年，并应用到了现实生活中的方方面面，比如智能医疗、食品药品安全溯源、类似“绿码”功能的治安防控等，而对于医疗行业的影响可以渗透到多个环节，比如药品药理的科研创新、药品的可信追溯、医疗保险的管理与服务、医保支付改革、基于隐私保护的个人健康管理等。以下举出几个区块链在医疗行业的例子进行阐述：

1. 米希尔·特里坎德等人在2019年设计了一套基于移动用户控制区块链的个人健康数据共享与协作系统。该系统实现了数据与数据集样本的匹配。根据用户行为生成用户模式，该模式是一个需要网络节点验证的许可区块链，实现了一个基于隐私保护且从终端设备到云端覆盖范围更广的个人医疗保健系统，并强调用户对健康数据的所有权。该系统还部署了移动应用程序，该应用程序可以从个人可穿戴设备、手动输入和医疗设备收集健康数据，并将数据同步到云，以便与医疗保健提供商和健康保险公司共享数据。为了保证健康数据的完整性，每个记录都可以从云数据库永久的检索出该记录数据完整性和验证的证明，并将其保存在到区块链网络(**???**)。下图为该系统的体系结构图：



1. 帕特尔等人在2019年设计了一套基于区块链共识安全和分散共享医学影像数据的系统，该系统通过区块链来存储每一个做过影像检查患者的名字，患者可以被授权访问每一组影像，以及该影像对应的医院。该系统的使用者可以由以下成员组成：进行这项研究的影像中心、医院、门诊、患者以及任何医疗服务提供者、PHR供应商、云服务或是其他委派单位。下图为患者操作影像的流程图：



  每个参与者在图片共享区块链的网络上操作一个节点。患者通过发布区块链事务来访问所选择的实体。影像数据直接从来源转移到这些授权接收方，不需要通过中介机构(**???**)。

Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. n.d. “Medrec: Using Blockchain for Medical Data Access and Permission Management.” In *2016 2nd International Conference on Open and Big Data (Obd)*, 25–30.

Dennis, Richard, Gareth Owenson, and Benjamin Aziz. 2016. “A Temporal Blockchain: A Formal Analysis.” In *2016 International Conference on Collaboration Technologies and Systems (Cts)*, 430–37. IEEE.

Dinh, Tien Tuan Anh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan. 2017. “Blockbench: A Framework for Analyzing Private Blockchains.” In *Proceedings of the 2017 Acm International Conference on Management of Data*, 1085–1100.

Malik, Sidra, Volkan Dedeoglu, Salil S Kanhere, and Raja Jurdak. 2019. “Trustchain: Trust Management in Blockchain and Iot Supported Supply Chains.” In *2019 Ieee International Conference on Blockchain (Blockchain)*, 184–93. IEEE.

McConaghy, Trent, Rodolphe Marques, Andreas Müller, Dimitri De Jonghe, Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto. 2016. “Bigchaindb: A Scalable Blockchain Database.” *White Paper, BigChainDB*.

Mir, Zeeshan Hameed, and Fethi Filali. 2017. “Large-Scale Simulations and Performance Evaluation of Connected Cars-a V2v Communication Perspective.” *Simulation Modelling Practice and Theory* 73. Elsevier: 55–71.

Noor, Sana, Wentao Yang, Miao Guo, Koen H van Dam, and Xiaonan Wang. 2018. “Energy Demand Side Management Within Micro-Grid Networks Enhanced by Blockchain.” *Applied Energy* 228. Elsevier: 1385–98.

Prybila, Christoph, Stefan Schulte, Christoph Hochreiner, and Ingo Weber. 2020. “Runtime Verification for Business Processes Utilizing the Bitcoin Blockchain.” *Future Generation Computer Systems* 107. Elsevier: 816–31.

Weber, Ingo, Xiwei Xu, Régis Riveret, Guido Governatori, Alexander Ponomarev, and Jan Mendling. 2016. “Untrusted Business Process Monitoring and Execution Using Blockchain.” In *International Conference on Business Process Management*, 329–47. Springer.

Zahnentferner, Joachim. 2018. “Chimeric Ledgers: Translating and Unifying Utxo-Based and Account-Based Cryptocurrencies.” *IACR Cryptol. ePrint Arch.* 2018: 262.

刘博, and 周华平. 2018. “区块链技术在车联网中的应用研究.” *收藏* 40.

杨柳青. 2018. “区块链技术在车联网中的应用研究.” *收藏* 6.

杨现民, 李新, 吴焕庆, and 赵可云. 2017. “区块链技术在教育领域的应用模式与现实挑战.” *现代远程教育研究* 2 (34): r45.

焦通, 申德荣, 聂铁铮, 寇月, 李晓华, and 于戈. 2019. “区块链数据库: 一种可查询且防篡改的数据库.” *Journal of Software* 9: 2671–85.

王瑞锦, 唐榆程, 张巍琦, and 张凤荔. 2020. “基于同态加密和区块链技术的车联网隐私保护方案.” *网络与信息安全学报* 6 (1): 46.

郭朝, 郭帅印, 张胜利, 宋令阳, and 王晖. n.d. “区块链跨链技术分析.” *物联网学报* 4 (2): 35.

龚钢军, 张桐, 魏沛芳, 苏畅, 王慧娟, 吴秋新, 刘韧, and 张帅. 2019. “基于区块链的能源互联网智能交易与协同调度体系研究.” *资源环境与工程*, 1278–89.