Blockchain and Smart Contract: Notes

Hailiang Zhao @ ZJU.CS.CCNT
hliangzhao@zju.edu.cn

区块链简介

1 核心优势：去中心化

2 通过运用**数据加密、时间戳、分布式共识、激励机制**，在**结点无需相互信任的分布式系统**中实现点对点交易、协同与合作。

3 血亲信用 → 贵金属信用 → 央行纸币信用 → 基于区块链构建的去中心化信用

4 狭义的定义：区块链是一种**按照时间顺序**将数据区块以链条的方式组合成特定数据结构，并以**密码学**方式保证的不可篡改和不可伪造的**去中心化共享总账**（decnetralized shared ledger），能够安全存储简单的、有先后关系的、能在系统内验证的数据。

5 广义的定义：区块链是

（1）利用加密链式区块结构来验证和存储数据、

（2）利用分布式节点共识算法来生成和更新数据、

（3）利用自动化脚本代码（智能合约）来编程和操作数据

的一种去中心化基础架构与分布式计算范式。

6 特点：

（1）去中心化：采用纯数学方法在分布式节点之间建立信任关系

（2）时序数据：采用带有时间戳的链式数据结构进行存储，可验证、可追溯

（3）集体维护：系统内所有节点均可参与数据区块的验证

（4）可编程性：灵活的脚本代码系统，以太坊提供了图灵完备的脚本语言

（5）安全可信：非对称密码学加密，共识算法

7 区块链是具有普适性的底层技术框架：

1.0模式：可编程加密数字货币体系（比特币等） →

2.0模式：可编程金融系统（股权众筹、P2P借贷） →

3.0模式：可编程社会

比特币简介

1 2010年5月，弗罗里达程序员用1万比特币购买了价值25美元的披萨优惠券，从而诞生了比特币的第一个**公允汇率**。

2 比特币的发行依赖于分布式网络节点共同参与的一种称为**工作量证明**（Proof of Work，PoW）的共识过程。

3 PoW共识过程：**参与挖矿的**各节点（矿工）贡献自己的算力来竞争解决一个**难度可调整的**数学问题，成功解决该问题的矿工将获得区块的记账权，并将**当前时间段（时间段的长度的是多大？自上一个区块上链时的时间戳到当前时刻吗？自由决定。）的所有比特币交易（是否存在部分交易没有来得及广播到获得记账权的该矿工？如果存在这一现象，如何处理？存在的，每个人打包自己想打包的。未被打包的就游离在池子里面。一个交易甚至有可能过了很久很久都没有打包。）打包**记入一个新的区块、按照时间顺序连接到比特币主链上。获得打包权的矿工将收到（*i*）比特币系统给予的奖励以及（*ii*）被打包的交易所支付的手续费。这会激励比特币的持有者持续参与到记账权的争夺中。

4 区块链系统为比特币系统解决了数字加密货币所面临的两个重要问题：

（1）双花：两次或多次使用“同一笔钱”，有第三方机构（如银行），自然可以避免

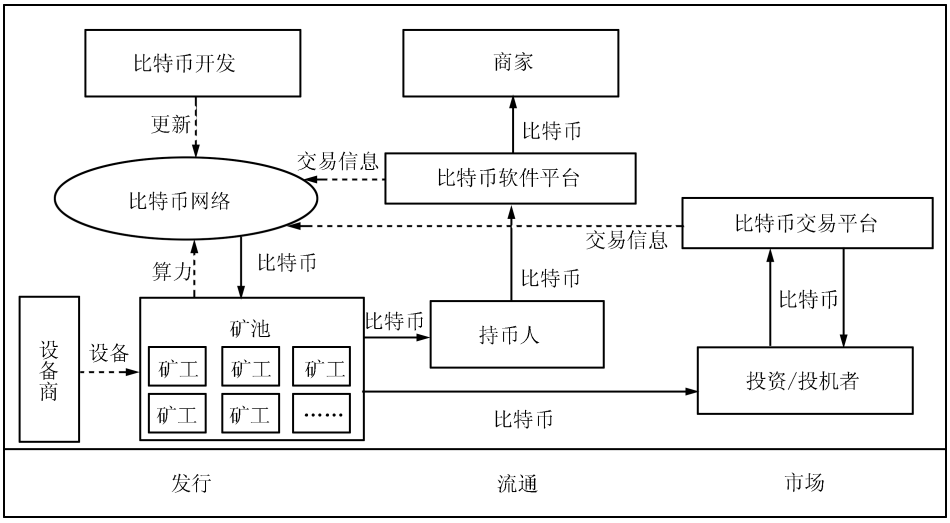
（2）拜占庭将军问题：在缺少可信任的中央节点的情况下，分布式节点如何达成共识、建立互信

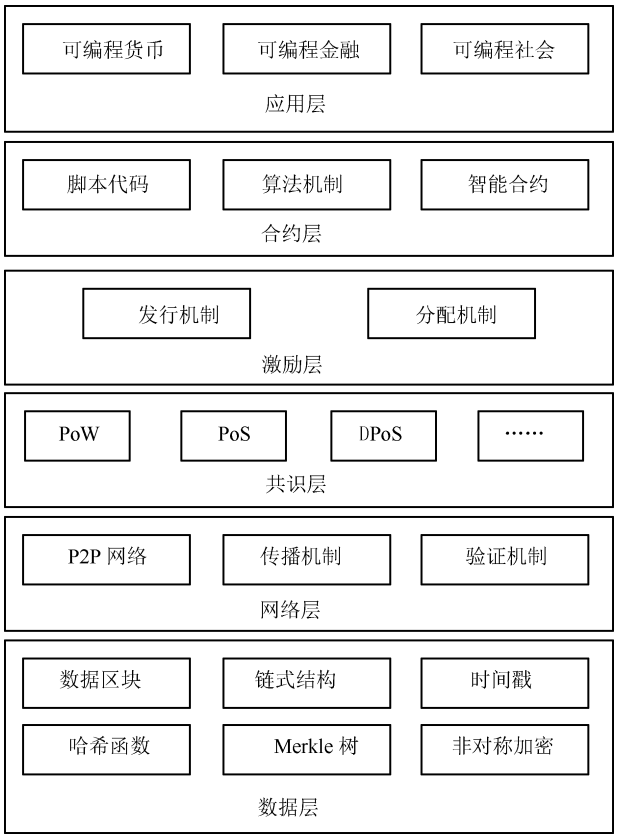
实现了**中心化的信用背书机制 → 软件（数字加密+共识算法）定义的信用**的转变。

5 比特币的生态圈

比特币经发行后进入流通环节，持币人可通过特定的软件平台（比特币钱包）进行比特币交易（购买商品，支付服务），这使得比特币具备了货币的属性。比特币和法币之间存在公允汇率，这使得其具备涨跌机制。因此出现了比特币的交易平台，方便持币人投资、投机比特币。任何交易都会被记录在比特币所对应的区块链网络中，等

待着拥有记账权的矿工打包并上链。（注册了一个比特币账户，是否就意味着成为了比特币的区块链网络中的一个节点？作为其中一个节点，有权决定自己是否参与记账权的争夺？参与PoW过程的服务器和对应的账户之间是什么关系？谁才是区块链中的节点？注册一个比特币的账户并不意味着成为比特币区块链系统中的一个节点。需要将整个账本拷贝到本地，通过广播的方式告知现有的节点，这样你就是比特币区块链系统中的一员了！）



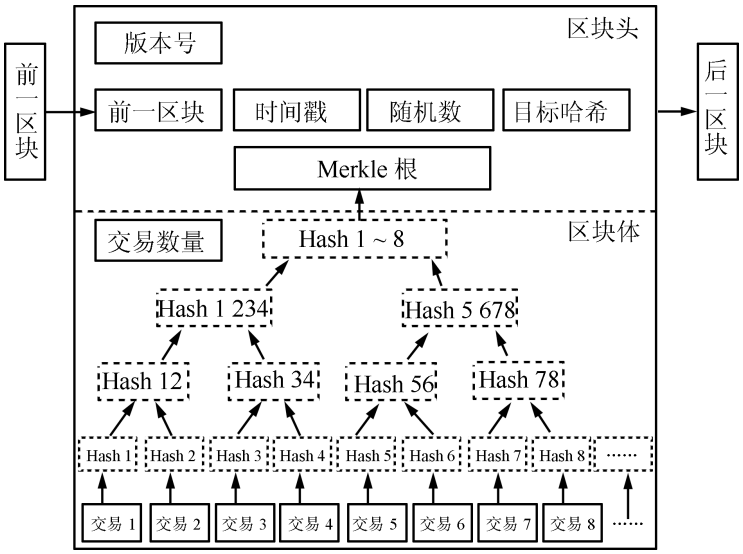


区块链模型

1区块链的基础架构模型

2 数据层

（1）区块结构



（2）链式结构：如果短时间内（多久的时间是“短时间内”？自己决定自己想要打包的。）有两个矿工同时挖出了两个新的区块并链接到主链上，那么区块主链会出现暂时的“分叉”现象。对于比特币而言，解决方案为：矿工总是选择延长累计工作量证明最大的区块链。（因为是先争夺打包权，后将当前时间段内的全部交易打包进区块，所以不存在有交易被漏掉的现象？存在的，因为打包哪些交易是由用户自己决定的。）

（3）时间戳：可以作为区块数据的存在性证明（proof of existence），计算机系统对时间的记录是铁面无私的。（这个时间戳好像是一个区块加盖一个，但是一个区块内有众多交易，每一笔交易难道没有时间记录吗？有的。每一笔交易的原始数据也会被存放进来，它们才是真正的叶子节点。）现有的交易记录也是包含一笔交易的时间信息的，甚至不仅仅是时间，交易对象和交易地点均有记录。交易是毫无隐私可言的，对我们所信任的中心化机构是完全透明的。

（4）哈希函数：原始数据被编码为特定长度的哈希值计入区块链（*Trans_i* → *Hash_i*），原始数据和交易记录不保存。哈希函数具有以下特征：（*i*）单向性；（*ii*）定时性；（*iii*）定长性；（*iv*）随机性。比特币采用双SHA256哈希函数，具有巨大的散列空间，抗碰撞性极强（也就是说，还是有可能发生碰撞的！）。

（5）Merkle树：快速归纳并校验数据的存在性和完整性。优点：（*i*）区块头仅需包含根哈希值而不必封装所有底层数据（这样的话，我们可否将区块头和区块体进行分离式的存储呢？二者之间当然可以借助一些手段实现一一对应和认证。现有的比特币系统就是分离式存储的。）（*ii*）简化支付验证：想要验证一条交易的可靠性，仅需沿着该子树向上追溯到根哈希即可，别的树节点无需接触（复杂度为*logN*）。

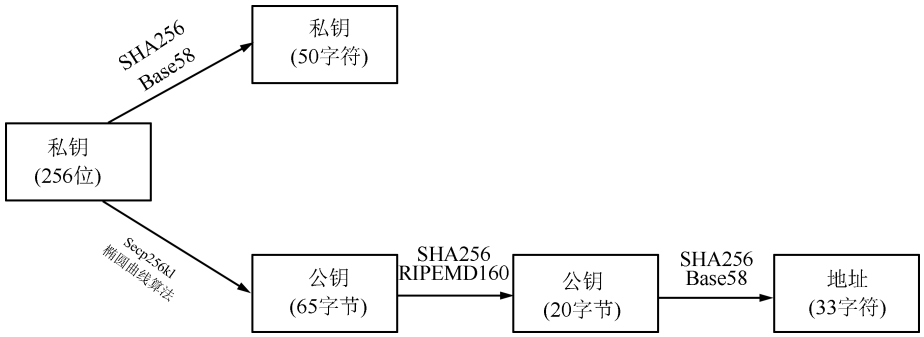
（6）非对称加密：假设A发送信息给B

（*i*）信息加密（A用B的公钥加密数据，B用自己的私钥进行解密）

（*ii*）数字签名（A用自己的私钥加密数据，B用A的公钥验证数据是否来自A）

（*iii*）登陆认证（客户端使用私钥加密登录信息发送给服务器，服务器采用该客户端的公钥解密并认证登录信息）

公钥的生成过程是不可逆的，比特币的公钥和私钥保存于比特币钱包，丢失私钥就意味着丢失了自己的比特币财产。



对于比特币而言，地址即公钥，公钥即地址。

3 网络层

对于比特币而言，每一个节点均能参与区块数据的校验和记账过程，仅当区块数据通过全网大部分节点（>50%）验证之后，才能计入区块链（这个验证的操作是节点自动执行的吗？是否存在“在线”这种说法？是否有可能错过验证交易？存在“在线”的说法。验证交易是由用户来决定是否参与的一个行为，是很有可能错过的。）。

（1）采用对等网络来组织散步全球的参与数据验证和记账的节点。每个节点地位对等、以扁平式拓扑结构相互连通。每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点的功能。

（2）节点分为全节点和轻量级节点。

（3）如果交易节点是与其他节点无连接的新节点，比特币系统会将一组长期稳定运行的“种子节点”推荐给新节点建立连接，或者推荐至少一个节点连接到新节点。（什么叫和其他节点无连接？这涉及到P2P网络是如何组网的。怎样定义“临近节点”？将自己成为区块链中的一个节点这件事广播出去即可。只要有一个网络内的节点接收到这个信息，那么这个节点就算是其中的一员了。）

4 共识层

（1）区块链技术的核心优势：在决策权高度分散的去中心化系统中使得各节点高效地针对区块数据的有效性达成共识。

（2）类型：

比特币：高度依赖节点算力的工作量证明（PoW）；

点点币：权益证明（Proof of Stake，PoS）；

比特股：授权股份证明（Delegated Proof of Stake，DPoS）。

（3）PoW共识：根据当前难度值，各个矿工节点通过搜索一个合适的随机数（Nonce），使得区块头中各元数据的双SHA256哈希值小于或等于区块头中的目标哈希。

Procedure（对于各个矿工）：

1：搜索当前时段全网未确认的交易，增加一个用于发型新比特币奖励的Coinbase交易，形成当前区块体的交易集合；

2：计算区块体交易集合的Merkle根，将该值计入区块头。填写区块头中的前一区块、版本号、时间戳等其他元数据，将随机数Nonce置零。

3：随机数Nonce++，计算当前区块头的双SHA256哈希值，如果小于或等于区块头的目标哈希（显然这个目标哈希是由比特币系统设立的，矿工节点对该数据没有修改权），则意味着成功搜索到合适的随机数并获得了该区块的记账权，否则继续该步骤。

4：如果一定时间内未计算成功，则更新时间戳和未确认交易集合，回到步骤1（是否有可能各个矿工节点所形成的当前区块包含的交易不完全一致？就是说有些交易并未被广播到当前矿工节点？可能的，所以要按照最长主链的原则来保证链的一致性。）。

显然，目标哈希数值越小，Nonce的搜索就越困难。假设目标哈希有x个前导零，则期望上至少需要16^x次搜索才可以找到符合要求的Nonce。

（4）比特币系统的安全性和不可篡改性是由**PoW共识机制的强大算力**所保证的，任何对于区块数据的攻击或篡改都必须**重新计算该区块及其后的所有区块的SHA256难题**，且计算速度必须要达到**伪造链的长度超过主链**才算是成功篡改。这种攻击难度导致的成本是巨大的。如果真的可以成功篡改，那么收益如何呢？事实上，攻击一旦成功，那么比特币的公允汇率必然会一跌到底，形同废币，没有任何价值了。所以，这种攻击即使成功了也是没有任何收益的，反而有巨额亏损。这样理解是否正确？正确。

（5）PoW带来的问题：（i）资源浪费；（ii）过长的交易确认时间不适合小额交易的商业应用。

（6）PoS共识：系统中具有最高权益的节点获得记账权。权益体现在节点对特定数量货币的所有权，即币龄（币天数，coin days）。

币龄：特定数量的币预期最后一次交易的时间长度的乘积。

系统在特定时间点上的币龄总数是有限的。其共识过程的难度与交易输入的币龄成反比。

（**PoS过程是怎样的？这个过程中的“挖矿”代表了什么行为？**每个人按照自己的意愿拿出一部分币参与到打包权的争夺中来。如果获得了记账权，那么自己的这部分币的币就会被扣除，这部分币的币龄就没了。也就是说，参与到打包权的争夺是有成本的行为。甚至有可能“入不敷出”，这就涉及到一个博弈的过程。）

（7）DPoS共识：“董事会决策”

系统中的股东节点将其持有的股份权益作为选票授予一个代表，获得选票最多且愿意成为代表的前101个节点将进入“董事会”，按照既定的时间表轮流对交易进行打包结算并签署（生产）一个新区块。

进入董事会成为授权代表节点需要缴纳不菲的保证金（打包一个区块收入的100倍），和金融系统一致，授权代表节点必须对全体股东节点负责。其通常需要保证99%的在线时间以保证不会错过签署对应的区块。

PoW：必须信任最高算力节点；

PoS：必须信任最高权益节点；

DPoS：每个节点能够自主决定其信任的授权节点（显然，权益较小的股东实际上并无决定权。因此这个说法是否不够准确？的确如此。）。参与验证交易的节点只能来自董事会，所以这将大幅减少参与验证和记账的节点数量，从而实现快速共识验证。

5 激励层

（1）区块链的共识过程本质上参与共识的节点之间的任务众包过程，最大化自身收益是各节点参与数据验证和记账的根本目标。所以，必须设计合理的激励机制让广大节点在最大化自身受益的同时保障整个系统的安全和有效性。（只要有众包，就可以有区块链（激励层）。从这个角度出发，联邦学习如果想要用户提供自身的隐私数据，就可以将区块链用进来。但是，真实情况是，谷歌根本就没有征求用户的同意就直接把联邦学习用在谷歌输入法上了。为基于edge的分布式机器学习设立激励机制似乎也只能停留在了学术和理论层面。）

（2）发行机制

成功取得记账权的节点将会在打包区块时获得系统提供的奖励以及每笔被打包的交易的手续费。随着比特币发币数量的减少（直至停止发行），手续费将成为驱动节点争夺打包权和记账的唯一动力。

手续费可以防止大量微额交易发起的“粉尘攻击”。这是因为：交易再小，也需要为其成功被打包支付手续费，大量微额交易意味着攻击发起方需要支付大量的手续费，成本过于高昂。

（3）分配机制

小算力节点通常会选择加入矿池，通过“汇聚算力”来提高挖矿成功的概率。主流矿池存在多种分配机制，如PPLNS（Pay Per Last *N* Shares）、PPS（Pay Per Shares）、PROP等。

矿池依据各节点贡献的算力按照比例划分成不同的股份。

矿池的出现是对比特币和区块链去中心化趋势的潜在威胁。

（难道各个互联网巨头或者政府不会通过购买或建造矿池来使自己成为最大算力节点？当前是否有出现这样的事件？为什么没有？对于政府而言，这样做不就以一种合法的方式将比特币“收归国有”了吗？这种事情还真就发生过。首先，这种行为就算成功了，带来的收益也不一定能够超过成本。其次，任何增加比特币不稳定的因素都会导致其公允汇率降低，从而使自己的比特币“不值钱”。综合各种因素，这种行为还真就不一定是获益的。）

6 合约层

数据层：数据表示

网络层：数据传播

共识层：数据验证

以上三者可以看作是区块链系统的虚拟机。

约合层：建立在虚拟机之上的商业逻辑和算法，是实现区块链系统灵活编程和操作数据的基础。

（1）非图灵完备的脚本代码（e.g. 比特币）→ 以太坊（图灵完备的脚本语言）

（2）比特币脚本（附着在比特币交易上的指令的集合）

锁定脚本：使用比特币接收者的公钥实现阻止输出功能

解锁脚本：使用比特币接收者的私钥对应的数字签名加以解锁

可以实现：延迟支付，担保交易，博彩与预测，多重签名（公司决策、财务监督、中介担保、遗产分配，etc.）。

7 区块链应用场景

（1）数字货币

（2）数据存储（分布式、高冗余、去中心化、隐私保护）：个人健康数据 → 人类思想意识

（为什么区块链可以实现隐私保护？这是因为数据并非存储在中心化的机构内，可避免因为遭受攻击或权限管理不当造成数据丢失或泄露。但是数据全部存在区块链上啊，区块链是公开的啊？区块链存储的不是原始交

易，而是其哈希值，那所谓的可追溯性如何体现？区块实际上存储了原始交易。区块链实际上无法做到隐私保护。数据都是公开的，总可以被查询甚至绘制用户画像。区块链不在于隐私保护，而在于不可篡改。）

（区块链如何存储数据？被打包的是交易，数据又并非交易。更何况，区块链存储的不是原始数据哈希之后的数值吗？哈希运算是单向性的，那么问题又来了，如何得知一开始存进来的到底是什么？区块实际上存储了原始交易。）

（3）数据鉴证（共同验证和记录、带有时间戳、不可篡改和伪造）：数据公证、审计

（4）经融交易（自发产生的信用和契约）：股权众筹、P2P网络借贷、互联网保险、资金清算交割

（5）资产管理：有形和无形资产的确权、授权和实时监控

（如何实现供应链管理和产品溯源？描述一下这个过程。区块实际上存储了原始交易，有了这个的确是可以做到溯源的。）

（6）选举投票

8 区块链的三种应用模式

公有链

联盟链：共识过程受到预定义的一组规则控制

私有链：适用于特定机构的内部数据管理与审计，写入权限由中心机构控制，读取权限选择性开放

区块链的现存问题

1 安全

（1）51%攻击问题

中国大型矿池的算力占全网总算力的60%以上，理论上可以通过合作实施51%攻击，从而实现双花。（但是收益不敌成本，说一说成本有哪些？这是一个复杂的、高风险的政治行为，当然不是想做就做的。）

（PoS如何在一定程度上缓解了51%攻击问题？因为不是靠算力来争夺记账权的，自然可以避免因为算力的集中带来的问题。）

（2）量子计算机的发展有暴力破解非对称加密的可能性

（3）隐私保护：区块链中的各节点并非完全匿名，针对部分公钥地址开展用户画像分析仍有可能取得蛛丝马迹

2 效率：7笔交易每秒（为什么？在比特币的系统代码中是如何实现的？），10分钟区块验证。

3 资源：应当汇聚分布式节点的算力解决实际问题，设计行之有效的交互机制来汇聚和利用分布式共识节点的群体智能。

4 博弈：各个矿池可通过区块截流攻击的方式、伪装为对手矿池的矿工等手段，不贡献完整的PoW来攻击其他矿池。

（基于区块链的）智能合约

1 定义

（1）狭义：运行在分布式账本上预制规则、具有状态、条件响应的，可封装、验证、执行分布式节点复杂行为，完成信息交换、价值转移和资产管理的计算机程序。

（2）广义：无需中介、自我验证、自动执行合约条款的计算交易协议。

2 智能合约是一组情景-对应型的程序化规则和逻辑，是部署在区块链上的去中心化、可信共享的程序代码。智能合约可以任意复杂。

3 分类

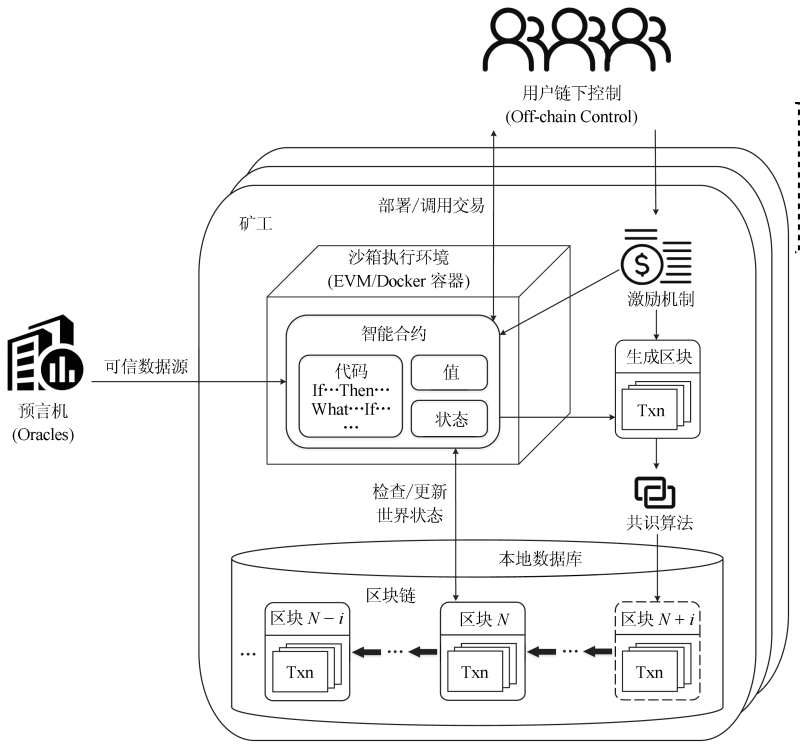
智能法律合约：作为法律的替代和补充

智能软件合约：作为功能型软件

智能替代合约：引入新型合约关系

4 运作机理和机制

智能合约经多方共同协定、各自签署后随用户发起的交易提交，经P2P网络传播、矿工验证后存储在区块链特定的区块中，用户得到返回的合约地址及合约接口等信息后即可通过发起交易来调用合约。矿工收到系统预设的激励机制的激励，将贡献自身算力（或权益）来验证交易：在本地沙箱执行环境（以太坊虚拟机）中创建合约or执行



合约代码，合约代码根据可信外部数据源（预言机）和世界状态信息自动检查判断当前所处场景是否满足合约出发条件以严格执行响应规则并更新世界状态。交易验证有效之后被打包进新的数据区块并更新到区块链主链。

4 通过将房屋和车辆等实体资产进行非对称加密，并嵌入含有特定访问控制规则的智能合约后部署在区块链上，使用者符合特定的访问权限或执行特定操作（如付款）后就可使用这些资产，这能够有效解决房屋或车辆租赁商业模式中资产交接和使用许可方面的痛点。（这个操作想要实现的最大困难在于如何建立实体资产到数字信息的映射。这是否需要国家意志来贯彻？需要。）

5 智能合约面临的问题

研究挑战	典型问题	涉及到的模型要素	要素层次
隐私问题	可信数据源隐私问题	预言机	基础设施层
	合约数据隐私问题	分布式账本及其关键技术	
		交互准则	合约层
法律问题	难以追责或事后救济	分布式账本及其关键技术	基础设施层
	意思表示真实性不足	法律条文/商业逻辑/意向协定、情景—应对型规则	合约层
	存在不可预见情形		
安全问题	漏洞合约	分布式账本及其关键技术	基础设施层
		开发环境	
		预言机	
		情景—应对型规则	合约层
	恶意合约	法律条文/商业逻辑/意向协定	
机制设计问题	机制设计	机制设计	运维层
性能问题	区块链性能问题	分布式账本及其关键技术	基础设施层
	待优化的智能合约	情景—应对型规则	合约层
	待优化的机制设计	机制设计	运维层

6 应用：经融、管理、医疗、物联网与供应链

7 “默顿”社会系统（不确定性、多样性、复杂性） → “牛顿”社会系统（可全面观察、可主动控制、可精确预测）

References

[1] 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481−494
[2] 欧阳丽炜, 王帅, 袁勇, 倪晓春, 王飞跃. 智能合约: 架构及进展. 自动化学报, 2019, 45(3): 445−457