浅谈区块链技术及其应用

漆　楚
（西南大学商贸学院，重庆 402460）

摘要：基于区块链技术的发展现状，文章介绍了区块链相关概念及应用场景。从区块链的起源出发，给出了区块链的本质和定义，重点分析了区块链的技术原理，并对区块链的应用与发展前景进行说明，同时还提出区块链技术在发展过程中存在的挑战，最后给出了发展建议。

关键词：区块链；应用；发展前景；挑战；建议

一、区块链技术的起源和技术原理

（一）区块链技术的起源

“区块链”一词是由中本聪提出来的，最早出现在《比特币：一种点对点的电子现金系统》这篇论文中，论文介绍了以区块链技术为代表的多种架构理念，在电子现金系统领域有着划时代的意义，标志着比特币的产生。虽然世界对比特币的态度一直都不太一致，但是区块链技术，这一比特币的底层技术，却逐渐成为人们关注的焦点。在比特币的发展过程中，区块起到存储信息的作用。在一定时间内区块节点的交流信息由一个个区块记录，区块之间的链接通过哈希算法来实现，前一个区块的哈希值被保存在后一个区块当中。信息交流不断扩大，各个区块相继接续，区块链由此形成。

从本质上看，区块链技术是对网络数据进行存储、交流、验证的技术手段，它不依赖于第三方，是通过自身分布式节点来实现的。所以，不少人从金融会计领域来理解区块链技术，他们认为区块链技术是一种大型的网络记账簿，而且这本记账簿具有分布式、去信任化、去中心化的特点。如果从数据存储的视角来定义区块链，区块链可以被视为一种分布式的、去中心化的账本数据库。

（二）区块链的技术原理

1. 分布式账本。分布式账本技术在去中心化自治交易中发挥着至关重要的作用，这种技术能够有效地将某一节点的信任转化为计算机协议的信任，促进去信任化对等网络的快速发展。作为分布式账本的一个子集，区块链的工作机制与分布式账本的共性是一致的。区块中各种交易记录采取默克尔树（储存哈希值）的结构方式进行排列，至于前后区块则是按时间的先后顺序排列。与传统的记账簿相比，这种分布式的交易账簿具有不可篡改性、匿名性等特性，应用价值相当高。

2. 智能合约。智能合约本质上是一组计算机程序，它采用信息化的方式传播、验证和执行合约。区块链内各个节点都参与合约的制定，合约明确了参与双方的权利及义务，同时会触发合约自动执行的条件也被包含在代码中。当区块链网络出现上传的合约时，验证节点首先会对其进行验证，成功验证并安装到区块链系统后，智能合约就会被发现和启动。

3. 非对称加密算法。区块链采用非对称加密算法，在这项技术中含有一组密钥（即公钥和私钥）。显然，公钥是可以公开获取的，而私钥则为交易者私有。一组密钥可以对彼此进行解密，在对明文的加密和解密过程中必须要两者的配合才能发挥作用，这样有效保证了此算法在密码学上的安全性。该算法最基本的应用就是对信息加密，其工作原理可以理解为用特定信息接收者的公钥对信息进行加密，形成密文，将其发送至信息接收者，在接收到信息后，对方采用私钥对密文进行解密。

二、区块链技术的应用与挑战

（一）区块链技术的应用

1. 在金融领域的应用。区块链技术最早产生于比特币平台，与金融行业的联系十分紧密。在智能记账领域里，该技术安全性高的优势十分突出。正因如此，金融领域广泛采用区块链技术。例如，信贷用户的诚信记录可以通过区块链技术加以保存，这样金融管理机构的成本会大幅度下降。将用户与其投资方向的金融数据通过区块链技术呈献给金融机构的管理者，能够有效提高管理效率，提升机构的运营能力。

2. 在食品安全领域的应用。近年来，食品安全问题越来越被人们重视，但由于食品供应的流程复杂，我国很难建立有效的食品安全监督体系。通过区块链技术可打造食品数据流通的大型统计网络。通过该网络，建立高效率的食品安全监管体系将不再只是一句口号。例如，食品监管部门可以建立食品安全数据库，将各种食材的相关信息记录在数据库中。通过层层推进，消费者可以很轻松地查询到所购买食品的安全信息。

3. 在社会管理的应用方向。应用于各种智能的运输平台，借助区块链的智能合约技术，利用计算机的强大计算能力，精准匹配乘客和车辆，有效达到车辆和乘客的供求平衡，去掉中间商，减少乘客和司机的损失，实现互利共赢。另外，对于造假和盗版问题，通过区块链技术可以将授权的技术保护起来，这样被剽窃的概率几乎为零，当然这种方式也存在一个明显的缺陷，那就是更改起来的技术难度会增加。

（二）区块链技术的挑战

1. 拓展挑战。为了验证数据，区块链技术必须存储所有的数据信息。然而，随着事务量的不断增长，区块链中的区块数量会越来越多，这样一来，整个区块链系统会越来越复杂。所占用的存储空间是难以想象的，一般存储设备无法承受。除此之外，区块的增多也会导致验证时间的增加，每秒处理的数据量可能无法满足庞大的交易需求，从而造成更高的成本。

2. 隐私挑战。区块链技术的不可篡改性使其具有很高的安全性，尽管如此，还是存在一定的隐私问题，仅以比特币为例，在交易进行过程中不需要提供真实身份，只需要有用户生成的地址即可，包含的用户地址信息是无法修改的。所以一旦某个用户的地址被泄露，将导致该用户的所有交易信息被泄露。

3. 法律监管挑战。区块链技术作为一项新的技术，在改变经济、生活的同时，必然伴随着和法律制度的磨合。尤其是在区块链发展初期，对其发展态势还缺乏明确的判断，而且法律的规范化与技术进步之间存在时间差，所以法律很难对其潜在的问题进行制约和规范。

三、结语

安全是首先要考虑的问题，要保证系统的可靠性，不可盲目建设区块链平台。同时，要加大对网络安全技术算法的投入力度，提高信任生成的保护力度。在区块链发展的过程中，政府应该了解区块链的潜在用途，构建区块链发展的生态体系，形成有效的监管机制。

参考文献：

[1] 宋伟阳，徐海水．区块链关键技术与应用特点．
[2] 蒋润祥，魏长江．区块链的应用进展与价值探讨．