区块链发展的应用与挑战

2008年，中本聪在*Bitcoin: A Peer-to-Peer Electronic Cash System* 中提出了区块链的最初概念，并使用区块链实现了比特币这一最著名的区块链应用。而在今年，区块链技术不断收到了全世界越来越多的关注，随着 Vitalik Buterin 所提出的有智能合约这一特点的以太坊的出现，区块链的更多应用也开始被社会所重视。

那么什么是区块链呢？区块链的的本质是按时间顺序增长的数据集合区块所构成的链条，每一个区块与前一个区块都有着通过密码学保证的联系。在每一个区块中，主要包含了上一区块的哈希值，以 Merkle 树形式保存的交易数据以及时间戳。对于交易记录的验证区块链使用了非对称加密机制进行，通过这种机制要通过遍历找到某一钱包的私钥是非常困难的，因此可以达到一定的安全。

区块链在最常用的分布式账本场景下，由一个 P2P 网络进行组织，每个节点地位平等，在同一共识机制下，进行节点间的交流和对新区块的验证。对于已写入区块链中的数据，除非改变从该区块往后的所有区块数据，否则无法改变， 所以有着难以篡改的特性。

区块链的应用

区块链去中心化，难以篡改、集体维护以及可编程等特点使其发展出了多种可能的应用，其中最广泛的就是以比特币和以太坊为代表的基于分布式账本的 Cryptocurrency。 比特币在发布至今的过程中其价值经历了非常大的变化，最高达到了近20000 美元，在2018年9月23日的价值为6,733.01 美元。加密货币依靠算法所建立的信用体系已经对全球经济产生一定影响，在未来这影响可能会更加深远。

除了加密货币外，区块链还有很多在各个领域中的可能的应用空间，尤其在智能合约概念出现后，几个例子如下：

1. 通过区块链在政治选举、董事会投票等场景中进行应用，使这些场景可以更高效地进行，且难以篡改结果，以此可以帮助减少投票中出现的舞弊欺诈等情形。纳斯达克便已在爱沙尼亚进行区块链投票平台的测试
2. 以区块链版权项目 po.et 为例，通过在区块链上注册数字内容所有权的元数据，记录并认证数字内容的授权信息及其他条款，且防止欺诈。内容所有者可以编写或直接使用现有的授权证书，来规定使用其创作内容的使用授权细节。这些授权利用区块链智能合约强制执行，可以直接降低内容所有者对其创作内容维权的成本。
3. 区块链的难以篡改、伪造数据的特性使其可广泛应用于数据公证和审计的场景，将各类需要进行公证的记录存至区块链中可以保证持久的安全存储，并提升需要使用这些记录进行审计核查时的效率。

The Linux Foundation 主导发起了Hyperledger, 一个推动区块链跨行业应用的开源项目，该项目成员包括金融，银行，物联网，供应链，制造和科技行业的领头羊。该项目推动了区块链在金融、医疗、供应链及其他面向企业领域的应用发展。

区块链面临的挑战

区块链尽管有着非常多优良的特性，但是也面临着许多挑战，这些挑战对区块链未来的发展都可能造成影响：

1. 众多加密货币剧烈的涨跌幅吸引了很多人加入“炒币”大军，也使得其泡沫不断膨胀。甚至社会上还出现打着区块链旗号的金融诈骗项目，利用加密货币进行逃税、洗钱、勒索等违法行为的可能也为各地区监管机构带来担忧。这些现象可能在舆论上对区块链带来负面影响，也会对各地区对区块链及其相关技术的监管政策产生消极影响。
2. 区块链面临许多安全性威胁，51%攻击问题是使用 PoW 共识的区块链最大的威胁，尽管对比特币等区块链发动此类攻击的成本极高，但这也是一个可能的安全威胁。对于共识机制在安全方面的提升仍然需要更多的研究。
3. 加密算法也存在潜在威胁，Shor's algorithm 若在未来量子计算机得到应用后进行实现，则会使得现在被广泛应用的 RSA 算法被非常有效率地破解，其他的加密算法也会受到类似的威胁。因此区块链的发展也需要应对加密算法方面所可能面临的问题。
4. 区块链加密货币的“挖矿”可能带来大量的算力和资源的浪费。以比特币为例，在2017年 ASIC 矿机还未被广泛用于挖比特币的时候，全球“矿工”主要使用 GPU 来进行“挖矿”。GPU 的需求量也由此大幅提升，英伟达和 AMD 公司当年所推出的 GPU 也因此出现了大规模缺货或涨价。这些被“矿工”买走的 GPU 在挖矿过程中主要进行的是无实际价值的 SHA256哈希运算，因此可以认为这些 GPU 的算力都被浪费了，而且在挖矿过程中会耗费大量电力 。对于区块链，尤其是基于 PoW 共识的区块链而言，解决资源浪费会是未来发展的一个实际问题。
5. 区块链的效率仍然需要提升，比特币目前每秒仅能处理7笔交易，以太坊每秒约20笔交易 ，相比之下，PayPal 2017年每秒钟平均处理240笔交易, Visa 可容纳65000笔以上的交易 ，较低的效率很可能会对区块链未来的发展产生制约。
6. 全节点区块链要求每个节点保存完整区块链数据，对于比特币这类已经长期产生新区块的区块链应用而言这会导致各节点需要存储非常大量的数据。虽然这样的冗余可以保证数据完整性，但是可能会带来性能等问题。

区块链作为一个新兴的技术有着光明的应用前景。其去中心化、难以篡改、安全可信以及可编程的特点使得它有改变当今社会经济、生产模式的潜力。然而，区块链的发展会面临许多技术上以及社会经济文化上的挑战。学术界以及与区块链相关的企业对于区块链的许多问题仍然要寻求解决之道，在基础技术理论上推进区块链的发展。