

智能合约、区块链及第三代互联网

余陈杨律师行
2023年6月5日

何谓智能合约

智能合约是储存于区块链上的程序化合约，一旦满足预先设定的条件就会自动化执行。

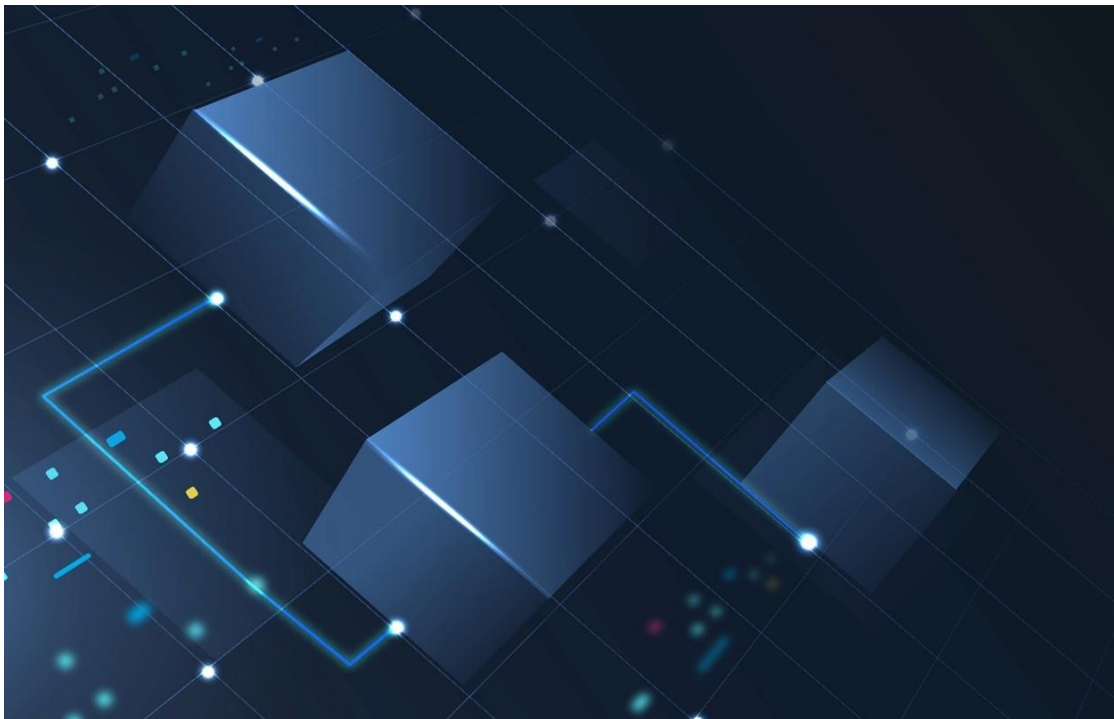
智能合约用于自动执行协议，毋须任何中介参与，合约各方亦可以预测结果。因此，与传统合约相比，智能合约更具成本效益及节省时间。

智能合约的概念最早由尼克·萨博于1994年提出。于1998年，他亦发明一种名为“比特金”的虚拟货币。而比特币则于10年后才推出。智能合约包含执行合约条款的计算机化交易代码。不同于传统合约，智能合约不载列任何法律语言或条款。相反，智能合约的语言属编程语言（例如：JavaScript），其条款亦被嵌入到相应的代码当中。



智能合约及区块链

区块链技术，作为一个点对点的网络，是通过去中心化及分布式分类帐的方式记录所有可能于网络中达成的交易。因此，区块链技术的关键是去中心化。与核心分类帐不同，分布式分类帐是一个由网络中的使用者共享的数据库，在该数据库中，每个使用者均能保留及同步更新数据副本。分布式分类帐允许使用者可安全地核证、执行及记录他们自己的交易，而毋须任何中介（例如：代表交易方的法律顾问）。



区块链容许网络使用者在没有集中化机构（例如：结算所）参与的情况下安全地移转加密货币，例如，以太坊就是以区块链为基础用于加密货币的网络。区块链技术通过纳入合约当事人之间的协议条款而与传统合约有所重合，但又因满足条件时在分布式环境中自动化执行协议而超越传统合约，成为智能合约。因此，于区块链上运行的智能合约，能便利、履行及执行网络使用者之间的协议。为避免合约被篡改，智能合约的副本亦将被复制并储存于区块链网络的每个节点。

区块链及第三代互联网

第三代互联网（即，**Web 3.0**）期待已久，其通过运行没有集中化机构的协议而实现去中心化。第三代互联网，作为一个点对点的网络，不存在任何集中化机构，并允许任何内容创建者对其持有私密钥匙的数据拥有全面的所有权。因此，这可能会导致一些大型的科技公司（例如：**Facebook**）失去对互联网核心能力的控制。

第三代互联网促使使用者能跟踪自己的数据，并查阅其决定使用的平台源代码。第三代互联网上的所有使用者均能持续了解与其相关的价值及商务。

鉴于第三代互联网将于去中心化的协议上运行，因此，于第三代互联网中找到与区块链可能的聚合点至关重要。并且，由于第三代互联网通过利用智能合约、无缝整合及储存对抗审查的点对点数据文件而体现其互相操作性，自动化。毫无疑问，区块链将作为第三代互联网的一个关键驱动力。

在区块链技术的支持下，第三代互联网将促使以区块链为基础的新应用及服务于当今被广泛使用。这些应用及服务，包括但不限于(i)非同质化代币（亦被称为 "**NFTs**"）；(ii)去中心化金融（亦被称为 "**DeFi**"）；(iii)加密货币（例如：比特币）；(iv)去中心化应用程序（亦被称为 "**dApps**"）；(v)智能合约；及(vi)分散式自治组织（也称为 "**DAOs**"）。

值得注意的是，随着第三代互联网的兴起，分散式自治组织提出一个开创性的去中心化之社交协议，以允许使用者协同创建一个类似电子邮件之分散式的社交网络。