从拜占庭将军问题到区块链

我们认知并改造这个世界的方式一直在变，而技术一直是其中最大的推动力。

区块链从诞生到最近的大热，短短几年时间，它的重要性其实已经可以与互联网相提并论了。

而每一本跟区块链有关的书籍，都会提到一个问题——**拜占庭将军问题。**

但对大多数人来说，并不能很好地理解这个问题所要表达的意思。

今天这篇文章就带你通俗地学习拜占庭将军问题——这一区块链与加密货币的起源性问题。

拜占庭将军问题

1982 年，Leslie Lamport 等在论文 The Byzantine Generals Problem（拜占庭将军问题）中提出了这样一个问题：

设想在中世纪，拜占庭帝国的几位将军各自带兵共同围困一座城市。

这座城市的防守非常坚固，只有他们一起进攻才能攻下来。

也就是说，他们要么一起进攻，要么一起撤退，否则都是灾难性后果。

但是，因为各位将军分处城市不同方向，没法坐在一起讨论，只能通过信使告诉彼此自己投票进攻还是撤退。

于是，每位将军都是根据得到的所有别的将军的投票，做出自己进攻还是撤退的决定。

如果所有将军都是忠诚的，当然没有问题，根据大多数将军投票结果就好了。

但是问题在于，将军中可能有叛徒。

假设 9 位将军投票，4 人投进攻，4 人投撤退，剩下 1 人是叛徒，他选择告诉进攻的 4 人他投进攻，告诉撤退的 4 人他投撤退，那么结果就悲惨了。

所以需要有一种算法，以保证即使将军中有叛徒，忠诚的将军们依然能通过多数决来做出决定，也就是拜占庭容错。

然而要实现拜占庭容错并不容易，直到 1999 年，Miguel Castro 和 Barbara Liskov 提出了实用拜占庭容错算法（PBFT）。

使用拜占庭容错法能够实现只要叛徒不超过三分之一，忠诚的将军们就一定能达成一致结果，这已经是当时科学家能实现的最好结果了。

二

后来，一直到中本聪提出比特币，拜占庭将军问题的解决才有了一种新的思路。

我们这里不讨论技术算法和结构，简单来说，中本聪的思路就是，如果要做叛徒，攻击整个网络，需要付出相应的成本。

而这个成本在比特币的 PoW（Proof of Work）工作量共识机制下，就是要掌握整个网络 50%以上的算力——换句话说，有 50%以上的叛徒才行。

这是比 PBFT 高得多的容错率，而且大家可以想象一下这是多高的成本。

接下来，绝妙的是，如果真的掌握那么大的算力的话，用这些算力维护网络（诚实地挖矿）获得的收益其实会高于破坏网络。

三

其实在中本聪提出比特币的 PoW 工作量共识机制之前，学术界对于解决拜占庭将军问题已进行了了很长时间的探索。

1985 年

Neal Koblitz 和 Victor Miller 分别提出椭圆曲线密码学（Elliptic Curve Cryptography，ECC），首次将椭圆曲线用于密码学，建立公开金钥加密的演算法。

相较于 RSA 演算法，采用 ECC 好处在于可用较短的金钥，达到相同的安全强度。

1990 年

David Chaum 基于先前理论打造出不可追踪的密码学网路支付系统，就是后来的 eCash，不过 eCash 并非去中心化系统。

Leslie Lamport 提出具有高容错的一致性演算法 Paxos。

1991 年

Stuart Haber 与 W. Scott Stornetta 提出用时间戳确保数位文件安全的协议，此概念之后被比特币区块链系统所采用。

1992 年

Scott Vanstone 等人提出椭圆曲线数位签章演算法（Elliptic Curve Digital Signature Algorithm，ECDSA）

1997 年

Adam Back 发明 Hashcash（杂凑现金），为一种工作量证明演算法（Proof of Work，POW）。

此演算法仰赖成本函数的不可逆特性，达到容易被验证，但很难被破解的特性， 最早被应用于阻挡垃圾邮件。

Hashcash 之后成为比特币区块链所采用的关键技术之一。

1998 年

Wei Dai 发表匿名的分散式电子现金系统 B-money，引入工作量证明机制，强调点对点交易和不可窜改特性。

不过在 B-money 中，并未采用 Adam Back 提出的 Hashcash 演算法。

Wei Dai 的许多设计之后被比特币区块链所采用。

Nick Szabo 发表去中心化的数位货币系统——Bit Gold，参与者可贡献运算能力来解出加密谜题。

2005 年

Hal Finney 提出可重复使用的工作量证明机制（Reusable Proofs of Work，RPOW），结合 B-money 与 Adam Back 提出的 Hashcash 演算法来创造密码学货币。

2008 年

区块链技术是从比特币开始的，所谓的区块链 1.0，也就特指在数字货币领域的创新。

具体的创新包括货币转移、兑付及支付和交易系统等等。

在这一阶段，区块链的主要表现形式为 Token 的点对点交易，在这一阶段区块链的发展也催生了大量货币交易平台，目标是实现货币的去中心化与支付手段。

2012 年

受到数字货币的影响，区块链 2.0 时代更多是涉及商业合同交易方面合约的创新，在这一时代中，以太坊是其中的典型代表。

与比特币不同，以太坊让区块链技术脱离了单纯的发币，而是提供了更广泛的金融领域应用场景，让区块链技术得以在包括股票、清算、私募股权等众多金融领域崭露头角。

2014 年

随着前两个阶段的不断完善，区块链也正在迎来它的 3.0 时代。

其“去中心化”功能及“数据防伪”功能在其他领域逐步受到重视。

在这一最新阶段，区块链将更多地应用于人类组织形态的变革，包括且不限于医疗健康、科学、文化和基于区块链的司法、行业互信等问题。

四

在对区块链的研究中，经常听到有人说 PoW 算法浪费了大量的电力资源、GPU 资源等，是不可取的做法。

但区块链使用 PoW 共识算法来保证系统的去中心化，成就可信网络，凡事都是有得有失，达成信任这一目标不管以何种方式完成，成本永远不可能为零。

而在以比特币为首的区块链网络中，电力资源、GPU 资源等就是达成信任需要付出的成本。

由多门技术糅合在一起的区块链技术，它摒弃了口头协定与书面协定的诸多问题。使用非对称加密算法、PoW 等共识算法，构建了一套分布式系统，至善至美的解决了拜占庭将军问题，也为未来的世界提供了无限的可能性。