比特币白皮书阅读感想 （谨代表个人观点）

一、精巧的链式结构

比特币白皮书于 2008 年正式提出，彼时数字签名以及非对称加密技术已经发展多年，并非独属于比特币的“重大的发明”，因此单一的一笔或几笔运用加密技术的交易并不足以让人称道。但在我看来，基于此的链式网络结构的的确确是该系统最核心最精巧的设计之一。 与其说比特币是技术的创新，不如说是系统设计的创新。几乎所有比特币的核心特质都依赖于此链式结构实现：可追溯性（可以追溯到第一个区块），双花（最长的链），不可篡改性（POW 机制，也即如何在能附上一个新的区块）。随着链越来越长，安全性也越来越高，越早的数据越不容易被篡改。现在尽管丰富的产品和系统可以让人们可以自由定义其中的部件，比如共识机制，区块执行（block execution）等，其根本仍是基于链式结构。

二、近乎完备的系统考量

白皮书包括简介和结论共有 12 个章节。虽然总共只有 9 页，但是几乎考量到该系统设计运行时的方方面面，不光阐述了基本的原理和核心的部件，在安全性（AttackerSuccessProbability）、经济模型（Incentives）、隐私性甚至可扩展性（Reclaiming Disk Space）都有考量，足见这是很严谨的思维。整个系统并不复杂但却及其稳定：中本聪说：The network is robust in its unstructured simplicity。同时，比特币网络至今已经稳定运营了 13 年也是佐证。在没有进行现实实现（至少没有体现在白皮书里），仅靠设计概念就呈现出如此完备和稳定的系统，让人印象深刻。

三、广阔的发展前景

白皮书并非完美，但却做了开创性的基础性的工作，甚至是开发了 blockchain 这一个新兴的行业并催生了长足的发展。比如为了解决 POW 过于耗费能源的问题出现了其他共识机制 POS，DPOS 等，为了解决比特币用途单一的问题（比特币只用于交易）发展出了以太坊，智能合约，Defi 等等。这些未必是中本聪预料到的，但确实因此发展而来。同时，不光在区块链本身做更新，跨行业的结合也有很大的想象空间。

2021.05.13

Kai