CHAPTER 11

UPCOMING BLOCKCHAIN NETWORKING PROBLEM

Besides the abovementioned blockchain network deployment issues, there is one more concern that needs to be overcome and that is the blockchain network security concern. Since the blockchain technology is in its nascent stages, this concern has not surfaced as evidently as it might in the near future. Nevertheless, it is one of those pressing concerns that by all means must be addressed.

With every new networking technology, there are going to be bugs but that cannot stop innovation, can it? If so, we would not have had HTTP and then HTTPS in the world of the internet. So, although there are security problems, we need to keep fixing the loopholes. For now, we know that block validation rules which are trust-based need some serious attention. Both Bitcoin's 2010 overflow bug[21] and Ethereum's 2016 DAO issue[22] (arguably the largest failing in each case) were caused by bugs in the trust-based validations of block contents, and not by issues in the trustless network.

So, in the future, we must remember that there could be similar issues in future blockchain-based applications, regardless of the technologies and techniques used. So, even if applications are supported by excellent, proven, and well-supported trustless blockchain network, they would still remain susceptible to attacks. So, the issue is not at the network level and therefore cannot be fixed through the networking protocol. However, what it can definitely do is enable others to innovate.

Each time technology evolves, it is overshadowed by some skepticism and failure, which in this case takes place in the form of invalid headers and blocks. Particularly, in the form of invalid blocks attached to valid headers. Currently, such information is generally discarded: if either the block header or the block contents are found to be invalid by any node in the network, they are simply discarded. Well, that need not be the case, and here's what can be done. Open-source projects and bug bounty programs can be used to effectively identify and fix vulnerabilities. This can be done by enabling others to build new network security systems that mitigate security risks that have been detected or may arise in the future.

[21] See https://en.bitcoin.it/wiki/Value_overflow_incident
[22] See https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee