Summary for “Bitcoin: A Peer-to-Peer Electronic Cash System”

Hou, Jue

[jue.hou@helsinki.fi](mailto:jue.hou@helsinki.fi)

In the article of this week, the author introduced a framework for an electronic currency and transaction mechanism. Motivations for the Bitcoin, as author claims, are to get rid of trusted third party for transection process and to reduce the problems and cost caused by that. The solutions for that are to public all the transactions record with some privacy and security control which are based on cryptography algorithm. A transaction between a payer and payee will require previous transaction id, payer’s signature and payee’s public key for verification. Another assumption, which is critical for the framework, is that most of the nodes in the network are honest and hold the majority of CPU power. They will verify transection properly and refuse suspicious payment. In this way, the attacker will have to assemble great number of resources to compete with honest nodes so that he can jeopardize the security and certainty of a transaction. Also, author gives the mathematical proof that it is hard for the attacker to change the fact of what has been accepted. However, even possible, with such amount resources, working for verification as a cluster of honest nodes seems to be more profitable.

Overall, I think this article is rather interesting. And it also reminds me the conclusion drawn from the article of Sybil Attack. The data structure of a block is a little bit confusing but the whole transection and verification mechanism is still quite straightforward.