12.おわりに

信頼に依存しない電子取引のシステムを提案した。我々は、デジタル署名から作られたコインという通常の枠組みから出発した。これは、所有権の強い管理を提供するが、二重消費を防止する方法がなければ不完全である。これを解決するために、我々はプルーフ・オブ・ワークを用いたピアツーピアネットワークを提案し、取引履歴を公開記録することで、誠実なノードがCPUパワーの大部分を支配すれば、攻撃者がすぐに変更できないような計算量になるようにした。このネットワークは非構造的でシンプルであるがゆえに堅牢である。ノードはほとんど協調することなく、一度にすべての作業を行う。メッセージは特定の場所に送られることはなく、ベストエフォートで配送されればよいので、ノードを識別する必要はない。ノードは自由にネットワークから離れ、再参加することができ、不在の間に起こったことの証明としてプルーフ・オブ・ワークチェーンを受け入れる。ノードはCPUパワーで投票し、有効なブロックは拡張して受け入れ、無効なブロックは拒否して取り組むことを表明する。必要なルールやインセンティブは、このコンセンサスメカニズムによって強制することができる。

参考文献

[1] W. Dai, "b-money", http://www.weidai.com/bmoney.txt, 1998.

2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure

timestamping service with minimal" [2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal 信頼性要件," 第 20 回情報理論シンポジウム in ベネルクス, 1999 年 5 月.
[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no
2, page 99-111, 1991.
[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping,".
In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference
on Computer and Communications Security, pages 28-35, April 1997.
[6] A. Back, "Hashcash - a denial of service counter-measure,".
http://www.hashcash.org/papers/hashcash.pdf, 2002.
[7] R.C. Merkle, "Protocols for public key cryptosystems," Inc. 1980 Symposium on Security and
プライバシー, IEEE Computer Society, pages 122-133, April 1980.
[8] W. Feller, "An introduction to probability theory and its applications," 1957.