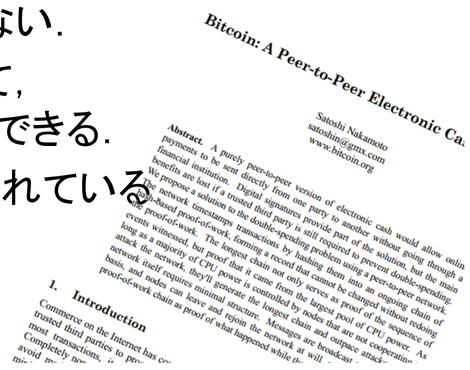
菊池研究室　*Bitcoin*の研究

明治大学総合数理学部先端メディアサイ

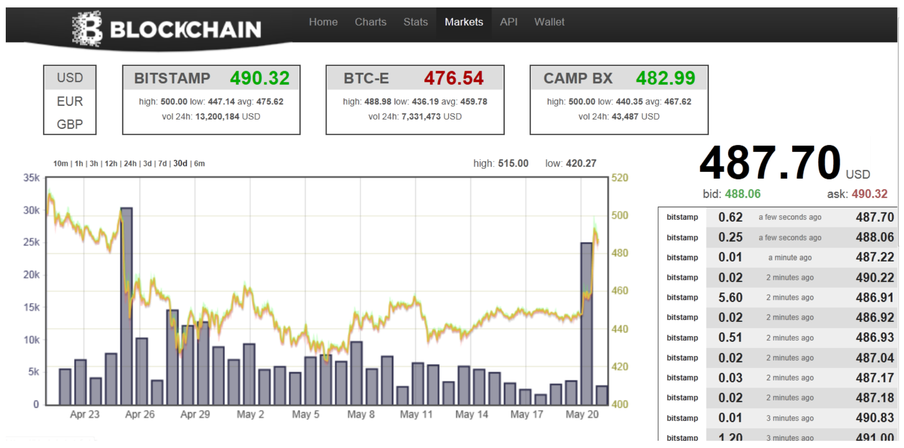
ビットコインとは何か？

- P2Pによるディジタル通貨
  - ナカモト サトシによる論文 “Bitcoin: A Peer-toPeer Electronic Cash System”, 2009
  - オープンソースによる開発，特定の開発者や製品があるわけではない．
  - 原理が公開されていて，誰でも「コイン」を採掘できる．
  - 投資対象として売買されている



ビットコインの相場

- 1BTC = 487.7 USD = **49,399円**



http://markets.blockchain.info/

疑問

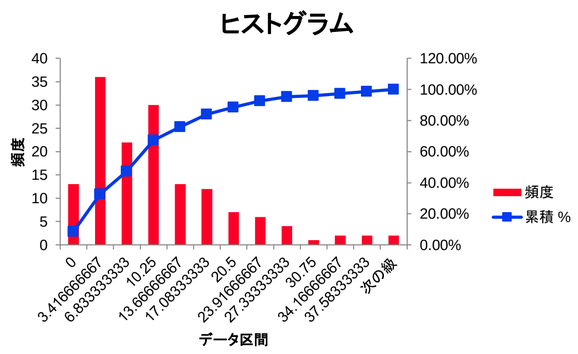
- どうやって「採掘」するの？
- なぜ採掘上限が決まっているの？
- コピーして何回も使えるの？
- 匿名なの？

電子マネーと現金の比較

	現金	電子マネー
発行者	中央銀行	サービス事業者 (JR, コンビニ)
不正対策	すかし（紙幣） 構成要素（硬貨）	ディジタル署名 MIC (Felica)
決済速度	×遅い	○早い
お釣り	×固定種類の通貨	○任意の額に分割
匿名性	○	×

平均発掘時間

- ブロック数
  - 2014年6月5日計　152ブロック
  - 平均間隔　9.14 分

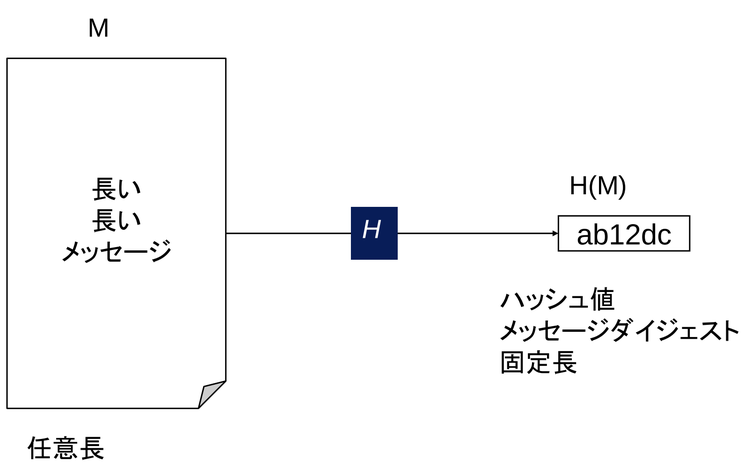


SHA256で「採掘」に挑戦

- 掘り当てたnonce候補

Nonce	入力値
000000 48c825029903b04d5146b6df546ee0f0a925630f414ee4f14692e1e549	2410917
000000 ac377abc57787764fa2acaa25d7baea194b93944bd45e3e247259def1c	11732505
00000 1dc633186945013fecbdc4689064aa252cadef5a92754d74e33e2b97e51	13401563
00000 3ade5d00c008b64c6fbc45a879e0b613dbb05976006058b8ad8dad0e445	15495479
00000 3f19d3c5076fa50297bc26636f3f70845b49ce2e37d0d470f83f865e3b8	1489124
0000 053d0f2f0a8b68881f582714c7629885377d5152927afb5a8f723175d4f2	8271493
00000 64617c99d31d0a916cf9657f4f5db48ea2d8ec56aab5426dc23de2e54b5	15163152

ハッシュ関数



「京」で採掘したら

- 性能
  - 10P FLOPS (10x 10^{15} 浮動小数点/s)
  - CPU数 88,128台

予測経過時間
T = 1.74 x 10^{11} / 88128 [秒]
= _____ [時間]