国際金融への仮想通貨の体系組込みと
PoW (Proof of Work)型認証方法への改良案 *

専修大学　小川健 **

＜報告要旨＞

近年急速に注目される様になってきた仮想通貨とその暗号技術であるブロックチェーンは，経済系でも例えば金融方面を狙う場合には決して無視できない．また，その代表格の 1 つ，ビットコインはデジタルな金（きん）とも呼ばれ，その価格の乱高下・高騰以外にも中央銀行のないお金として経済学教育の教材にも充分なり得るだけでなく，教えないという選択は学生に「真実を伝えない」教育ともとれる．そして，こういう事柄を（10 年前にはニュースに触れていなかった）学生が教員の手ほどき無しに勝手に学びだす際には，例えば 10 年ほど前に問題になった円天詐欺等のような項目に簡単に引っかかる危険性も高い．しかし技術系と異なり，経済系では例えば電子メール等での公開鍵暗号の仕組み等ですら教えられている訳ではなく，学生も多くは知らない．そこで，本報告では国際金融の学部生用講義を想定して，技術系ではない経済系では仮想通貨やビットコイン/リップル，そしてブロックチェーン等はどう教えたらよいか検討することで，国際金融の既存の体系の中に仮想通貨・暗号通貨をどのように組み込めるのか検討する．

また，2018 年 5 月よりモナコイン(MONA)，ビットコインゴールド(BTG)を初めとして，Proof of Work 型アルトコインには Block Withholding Attack/Selfish Mining，51%攻撃と言われるような Proof of Work 認証型ブロックチェーンの根幹を揺るがすような攻撃が行われだした．これを契機に（ビットコインを除く）小・中規模なアルトコインでは旧来の Proof of Work 型の認証方式には限界が来ているのではないか，とする説が取りざたされるようになり，モナコインは実際に保有量に応じた承認権限を与える Proof of Stake(PoS)型への移行を表明した．しかし，ビットコインに始まるパブリック・ブロックチェーンの持つ「非中央集権制」について，PoS では（事前には確保されても）事後には確保されない可能性がある．そこで Proof of Work 型暗号通貨認証方式の長寿命化についても本報告で考察する．

キーワード：仮想通貨教育，国際金融教育，Proof of Work(PoW)

JEL 区分：A22, E58, F31, F65, G12, G15

論文本体URL： http://u0u1.net/HRLh （随時更新予定）

---

* 本稿の基原稿に際し，橋本理博先生（帝塚山大学）及び高久賢也先生（広島市立大学）への討論者をかつてお願いいたしました．この場を借りて御礼申し上げます．商標侵害の意図はありません．本稿にありうる誤りについては執筆者に帰します．

** 〒214-8580 神奈川県川崎市多摩区東三田二丁目 1 番 1 号 生田校舎 9 号館 7 階 9710 号室
(044)900-7970, (090)4255-1796, takeshi.ogawa.123@gmail.com