ブロックチェーン上のアプリケーション移植性に向けて

首藤 一幸　神田 伶樹　斉藤 賢爾

本論文は我々の国際会議論文 [1] の日本語版要約である．
要約ではない日本語版，および，国際会議論文は，以下の URL から入手できる．
日本語版：
http://www.shudo.net/publications/201808-JSSST-2018-app-port/shudo-JSSST-2018-app-port.pdf
国際会議論文：
http://www.shudo.net/publications/201808-HotICN-2018-app-port/shudo-HotICN-2018-app-port.pdf
発表スライドは，以下の URL から入手できる．
日本語版：
http://www.shudo.net/publications/201808-JSSST-2018-app-port/
国際会議論文：
http://www.shudo.net/publications/201808-HotICN-2018-app-port/

1 要約

パブリックブロックチェーンは，我々が**インセンティブ不整合**と呼ぶ問題を抱えている．つまり，ブロックチェーンを支えるノード群とブロックチェーン上アプリケーションに共通の動機がないのである．

アプリケーションは，ブロックチェーンが提供する存在証明といった能力を活用したい．一方で，ブロックチェーンを支えるノード群，その運用者は，ただただコインが欲しいだけであり，ブロックチェーンの能力はそうした経済的な動機に支えられている．それゆえ，ノード群に対して経済的な動機を与えられないパブリックブロックチェーンは，トランザクションの安全な承認ができない．例えば，コインの価値低下はノード群の離脱を招き，ひいては承認能力の低下を招き，様々な攻撃に対して脆弱となる．

アプリケーションとノード群の動機を整合させられればそれに越したことはない．しかしその方法は知られておらず，未解決問題である．せめて，依って立つブロックチェーンが危うくなった際に他のブロックチェーン上に脱出できれば，アプリケーションは破綻を免れる．

同一のブロックチェーンミドルウェア間や，共通の API およびスマートコントラクト言語をサポートするミドルウェア間であれば，アプリケーションを異なるブロックチェーン上で実行し直すことは可能である（動作可能／ Runnable）．しかし，ブロックチェーンを利用するそもそもの意義はデータの存在証明やデータ変化の検証であるので，実行し直せるだけでは不足である．存在証明や検証に必要なログの移行も必要である（移行可能／ Migratable）．

本論文は，そうした移行を可能とするミドルウェアの構成法や移行の手順を提案する．

参 考 文 献

[1] Shudo, K., Kanda, R., and Saito, K.: Towards Application Portability on Blockchains, *Proc. IEEE HotICN 2018*, August 2018.

Towards Application Portability on Blockchains.

Kazuyuki Shudo, Reiki Kanda, 東京工業大学 情報理工学院 数理・計算科学系, Dept. of Mathematical and Computing Science, Tokyo Institute of Technology.
Kenji Saito, 慶應義塾大学 SFC 研究所, Keio Research Institute at SFC, Keio University.