分散台帳技術の実装の形式検証

Formal Verification of DLT Consensus Algorithms

齋藤 新 * その他 †

あらまし 分散台帳技術の安全性を形式仕様記述フレームワークで行った。定理証明を用いて検証。2 段階のリファインメントによりモデル化と検証を行った。TLA の使用で得た知見も紹介。

Summary. To appear.

1 Introduction

背景を書く。分散台帳技術は暗号資産の実装プラットフォームとして広く用いられるようになった。

形式検証することの意義:

- 正確な実装の保証。バグの回避。暗号資産に適用する場合などには、バグによる被害は大きい。
- 実装が満たす性質を厳密に定義することにより、分析や改良が進む。
- 実装を作る参考になる。たとえば Fabric ではチェーンコードや world state、コンセンサスアルゴリズムはプラグイン可能になっている。実装者がプラグインを作成する際に形式的に書かれた仕様があれば安心・安全である。

2 分散台帳技術

分散台帳技術の概要を説明。

2.1 Hyperledger Fabric

Fabric の説明。コンソーシアム型であることなどの特徴。コンセンサスの特徴。

3 形式検証支援系

Z 記法、VMS、Event-B (B-Method)、Coq、

プログラムの検証としてみる: 関数型状態遷移系の検証としてみる: 状態遷移系型時相論理。

3.1 TLA$^+$

4 安全性の形式検証

何を検証するか書く。

4.1 表と図

表の例を表 1 に，図の例を図 1 に示します.

謝辞 test 本フォーマットを作成して頂いた方々に感謝します.

*Shin Saito, IBM Research-Tokyo

†Others, other

表 1　表の例

FOSE2013	ソフトウェア工学の基礎 XX	岡野 浩三，関澤 俊弦 編
FOSE2014	ソフトウェア工学の基礎 XXI	花川 典子，尾花 将輝 編
FOSE2015	ソフトウェア工学の基礎 XXII	青木 利晃，豊島 真澄 編
FOSE2016	ソフトウェア工学の基礎 XXIII	阿萬 裕久，横川 智教 編
FOSE2017	ソフトウェア工学の基礎 XXIV	吉田 敦，福安 直樹 編
FOSE2018	ソフトウェア工学の基礎 XXV	伊藤 恵，神谷 年洋 編

図 1　図の例 (**FOSE2005** のロゴを使わせてもらっております)

参考文献

[1] 鵜林 尚靖，亀井 靖高 編:ソフトウェア工学の基礎 XIX, 日本ソフトウェア科学会 *FOSE2012*, 近代科学社, 2012.
[2] 岡野 浩三，関澤 俊弦 編:ソフトウェア工学の基礎 XX, 日本ソフトウェア科学会 *FOSE2013*, 近代科学社, 2013.
[3] 花川 典子，尾花 将輝 編:ソフトウェア工学の基礎 XXI, 日本ソフトウェア科学会 *FOSE2014*, 近代科学社, 2014.
[4] 青木 利晃，豊島 真澄 編:ソフトウェア工学の基礎 XXII, 日本ソフトウェア科学会 *FOSE2015*, 近代科学社, 2015.
[5] 阿萬 裕久，横川 智教 編 : ソフトウェア工学の基礎 XXIII, 日本ソフトウェア科学会 *FOSE2016*, 近代科学社, 2016.
[6] 吉田 敦，福安 直樹 編 : ソフトウェア工学の基礎 XXIV, 日本ソフトウェア科学会 *FOSE2017*, 近代科学社, 2017.
[7] 伊藤 恵，神谷 年洋 編 : ソフトウェア工学の基礎 XXV, 日本ソフトウェア科学会 *FOSE2019*, 近代科学社, 2018.
[8] 伊藤 恵，神谷 年洋 編 : ソフトウェア工学の基礎 XXVI, 日本ソフトウェア科学会 *FOSE2019*, 近代科学社, 2019. （to appear）