様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ５ 月 ３０ 日現在

機関番号：１４４０１
研究種目：基盤研究(C)（特設分野研究）
研究期間：2018～2021
課題番号：１８ＫＴ００９８

研究課題名（和文）形式検証によるスマートコントラクトとその実行基盤に対するトラスタビリティの実現

研究課題名（英文）Using formal verification to establish the trustability of smart contracts and their platforms

研究代表者
土屋　達弘（Tsuchiya, Tatsuhiro）

大阪大学・情報科学研究科・教授

研究者番号：３０２８３７４０

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究では，モデル検査を中心とした検証手法を，スマートコントラクト，および，その実行基盤であるブロックチェーンに適用することによって，これらの応用におけるトラスタビリティを実現することを目標とした．研究では，特にこれらの基礎となるコンセンサスアルゴリズムに注目し，不具合を検証する新しい手法を開発した．提案手法では，通常の逐次的なプログラムによって，メッセージ遅延や故障を含めたアルゴリズムの動作を模倣し，逐次プログラムに対するモデル検査手法を適用する．実際のアルゴリズムを対象に，安全性の違反を検出できることを示すことができた．

研究成果の学術的意義や社会的意義
スマートコントラクトやブロックチェーンを利用するアプリケーションは，それらが高い信頼性を提供できること前提としている．分散環境上での信頼性の実現の中核を担うのがコンセンサスであり，そのアルゴリズムには欠陥がないことが強く求められる．本研究で開発した手法では，分散アルゴリズムであるコンセンサスアルゴリズムを通常の逐次プログラムとして模倣するというアイデアにより，逐次プログラムに対する強力な形式手法を適用することを可能とした．

研究成果の概要（英文）：The goal of this research was to achieve trustability by applying formal verification methods, such as model checking, to smart contracts and blockchains. During the course of the research, a focus was placed on the correctness of consensus, which is at the heart of the applications above mentioned. As a result, a new verification method has been developed. The unique feature of this method is that it can make full use of verification techniques for sequential programs by simulating distributed consensus algorithms using sequential, ordinary programs. Using existing consensus algorithms, the research showed that the proposed approach is capable of finding safety defects.

研究分野：情報学

キーワード：コンセンサス　形式検証　ブロックチェーン　モデル検査　スマートコントラクト

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

暗号通貨等に加え，種々のデータの改ざんを防ぎ，信頼性高く共有する目的で，ブロックチェーンの応用が進んできた．そのような背景において，ブロックチェーン上で動作し，その内容を読み書きするプログラムであるスマートコントラクト，および，その動作を支えるブロックチェーン自体の信頼性の実現は，大きな問題であった．

スマートコントラクトに関しては，たとえば，代表的なブロックチェーンであるイーサリアム上のスマートコントラクトの設計不具合により，多額の暗号資産が窃取されるといった事態が生じていた．

また，ブロックチェーンのコアとなるコンセンサスアルゴリズムについては，しばしばアルゴリズムの不具合が報告されていた．コンセンサスアルゴリズムのようなアルゴリズムは，分散アルゴリズムとよばれ，ネットワーク上のコンピュータが非同期的に動作しながら協調することで，所定のサービスを提供する，このような分散アルゴリズムの設計は，一般に非常に難しく，さらに，ブロックチェーンでは種々の故障や攻撃に対しても耐性を有し，そのような状況下でも正しく動作することが求められる．

２．研究の目的

先述したように，特に信頼性が必要とされるスマートコントラクトやブロックチェーンに対し，形式検証手法を適用することで，その正しさを示す，あるいは，不具合の存在を明らかにすることで，これらの応用におけるトラスタビリティを実現することが，本研究の目的である．

形式検証手法とは，数学的な正しさでシステムを検証する手法を意味する．種々の方法が存在するが，研究ではモデル検査と呼ばれる技術を適用することを想定していた．モデル検査は，検証の対象となるシステムやアルゴリズムを，状態遷移システムとして解釈し，コンピュータを用いて状態を探索することで，期待される仕様（性質）が成り立つか否かを調べることができる．種々のモデル検査ツールや手法が知られており，本研究の検証対象を適切にモデル化し記述することで，これらの既存技術を有効活用して，形式検証を実現することを目標とした．

３．研究の方法

研究の過程では，まず，当該分野の研究動向の調査を行った．その結果，特にスマートコントラクト自体の検証については，多くの研究成果が本研究課題の開始と並行して公表され始めていることが分かった．そこで，本課題では特にコンセンサスという，スマートコントラクトの実行やブロックチェーン自体の維持の中核を担う問題にフォーカスし，この問題を解くアルゴリズムの形式検証に注力することとした．

コンセンサスアルゴリズムの検証に関しては，近年，独自のモデル化言語と方法論を利用することで，アルゴリズムの正しさを証明する手法が開発されていた[1,2]．これらの手法は不具合の存在ではなくアルゴリズムの無欠陥性まで示すことができるという点で優れているが，一方で，手法が依拠しているモデル化方法に検証対象のアルゴリズムが限定されることや，その検証手法に通じた研究者でないと利用できないといった問題がある．

このような背景を踏まえて，本研究では，誤りの検出を目的とし，かつ，容易にアルゴリズムをモデル化，検証できる手法を開発した．開発した手法では，コンセンサスアルゴリズムを，通常の逐次プログラムとして表現する．そして，逐次プログラムに対する既存のモデル検査手法を適用することで，不具合を検出する．

(1) 逐次プログラムとしての表現．分散アルゴリズムであるコンセンサスアルゴリズムを逐次プログラムとして表現するために，分散システムを構成するコンピュータ間メッセージの授受を行う非同期のステップを，逐次プログラム上での通常のループとして表現した．また，メッセージの遅延や喪失は，乱数を用いて対応するデータをエラー値に書き換えることで表現した．コンピュータの故障は，そのコンピュータが送信するメッセージがすべて喪失する可能性を残すことでモデル化できる．

(2) プログラムの検証．逐次プログラムとして表現したアルゴリズムの検証には，有界モデル検査を用いた．有界モデル検査は，プログラム中のループ構造を一定回数展開することで，ループのないプログラムに変換する．その上で，プログラムの実行をブール式によって記号的に，すなわち，変数などに具体的な値を設定することなく，すべての可能性を含む形で表現する．このことにより，エラーとなる実行が１つでもあれば，ブール式の充足性，すなわち，ブール式全体が真となる可能性を判定することで，その実行を検出することができる．

４．研究成果

開発した手法をいくつかのコンセンサスアルゴリズムに適用した．モデル化では C 言語の逐次プログラムを用いて，これらのアルゴリズムを表現した．また，有界モデル検査を実現するツールとして，CBMC を用いた．乱数は任意の場合が非決定的に得られるように表現し，アルゴリズムのすべての可能な動作が表現できるようにした．

One-third-rule と LastVoting[3]という 2 つアルゴリズムに対する検証時間(秒)を，それぞれ表 1, 2 として示す．LastVoting はよく知られたコンセンサスアルゴリズムである Paxos を抽象化したアルゴリズムである．実験では，CPU として Xeon E3-1245 (3.5GHz)，メモリ 8GB を有する Windows 10 PC を用いた．また，タイムアウト(TO)の時間を 5 分とした．

表 1．One-third-rule

	n=4	n=4	n=6
r=1	0.5	0.7	1.1
r=2	1.8	4.2	8.9
r=3	3.9	9.9	26.0
r=4	6.2	15.8	69.8

表 2．LastVoting

	n=4	n=4	n=6
r=4	2.3	5.4	22.9
r=8	4.7	13.9	91.0
r=12	9.8	42.9	TO

ここで，n はコンピュータ（プロセス）の数，r は検証できた非同期ステップの数を表している．LastVoting は，4 ステップを 1 フェーズとして繰り返す構造をしているため，ステップ数を 4 の倍数とした．これらのアルゴリズムは[1]で正しさが示されており，当然不具合は検出されなかった．

一方，不具合の検出が可能なことを例示するため，これらの実験とは別に，Paxos アルゴリズムの変種について意図的にパラメータを変化させたアルゴリズムを対象に検証を行った．その結果，期待通り不具合として検出できることが分かった．

[1] O. Maric, C. Sprenger, and D.A. Basin, “Cutoff bounds for consensus algorithms,” Computer Aided Verification- 29th International Conference, CAV 2017, vol.10427, pp.217-237, Lecture Notes in Computer Science, 2017.
[2] Oded Padon, Giuliano Losa, Mooly Sagiv, and Sharon Shoham. 2017. Paxos made EPR: decidable reasoning about distributed protocols. Proc. ACM Program. Lang. 1, OOPSLA, Article 108, October 2017.
[3] B. Charron-Bost and A. Schiper, “The Heard-Of Model: Computing in Distributed Systems with Benign Failures,” Distributed Computing, vol.22, no.1, pp.49-71, April 2009.

5．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

1．著者名 土屋達弘	4．巻 104，DC2021-66
2．論文標題 コンセンサスアルゴリズムに対するラウンドモデルに基づいた簡易的なテスト・検証手法の提案	5．発行年 2022年
3．雑誌名 信学技報	6．最初と最後の頁 13-17
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 土屋達弘	4．巻 120，SS2020-40
2．論文標題 逐次プログラムのテストによる分散フォールトトレラントアルゴリズムのバグ検出	5．発行年 2021年
3．雑誌名 信学技報	6．最初と最後の頁 73-77
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 土屋達弘
2．発表標題 SATソルバを利用した分散アルゴリズムの検証・テスト
3．学会等名 2022年度 人工知能学会全国大会
4．発表年 2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関