5Y-03

Ethereum 2.0におけるフルノードのワールドステートの信頼性向上手法

伊藤 悠斗 †
工学院大学 情報学部 コンピュータ科学科 †

真鍋 義文 ‡
工学院大学 情報学部 システム数理学科 ‡

1 はじめに

Ethereum[1] とは，Bitcoin を始めとする仮想通貨・ブロックチェーン技術の 1 つであり，スマートコントラクトと呼ばれる任意の関数のようなものを登録・実行でき，これを用いて構築したアプリケーションを非中央集権的アプリケーション (通称 DApp) と呼び，DApp には従来のアプリケーションと違い，高耐障害性・高持続可能性・高追跡可能性・非中央集権と言った優れた特徴がある．現在では上記の特性を活かして Ethereum 上で自立可動し続ける PKI や DNS が提案されている．DApp は World State(以降，状態とする) と呼ばれる従来のコンピューターの不揮発性ストレージに相当するものがあり，例えば DNS を DApp として作った際は状態にドメイン名と IP アドレスのマッピングが保存される．本稿ではこの状態に対する改竄攻撃を抑制し，状態の信頼性を向上させるために状態改竄に対して経済的ペナルティを科す提案をする．

2 Ethereum と DApp

2.1 ブロックチェーン概要

ブロックチェーンは一般的なシステムと違い，意思決定権を持つ中央サーバーの様なものが存在しない．ブロックチェーンでは共通のプロトコルを遵守したクライアントが P2P ネットワークにノードとして参加し，あらゆる意思決定をプロトコルに従って各クライアントが自律的に行うことでシステムを維持している．ネットワーク内の過半数のノードがプロトコルを遵守した振る舞いをすることでブロックチェーンは正常に動作する．ブロックチェーンのデータ構造はブロックと呼ばれるデータの塊をツリー状に繋いだ形になっている．ブロックには何らかの永続化したいデータとその前のブロックのハッシュが含まれている．チェーン内のブロックを少しでも書き換えるとそれ以降のブロックが全て連鎖的に変化するためプロトコルを無視した改竄を検知することができる．これによってブロックチェーンは高い改竄耐性を得ている．ノードは新たなブロックを作成した場合，他のノードにそれをブロードキャストする．受信したノードはブロックがプロトコルを遵守しているか確認し，正しければ自身のチェーンに繋げる．ブロックチェーンは中央となるサーバーが無いため各ノードがそれぞれ独立してチェーンを持つ．この場合，ノード毎にチェーンの差異が発生するように思えるが，例え分散していても同じプロトコルに従い，同じ順番でブロックを処理するため同じチェーンになる．

A reliability improve method for the world state of full nodes in Ethereum 2.0

† Yuuto Itou, Department of Computer Sience, Faculty of Informatics, Kogakuin University
‡ Yoshifumi Manabe, Department of Information Systems and Applied Mathematics, Faculty of Informatics, Kogakuin University

2.2 Ethereum 概要

Bitcoin は台帳をブロックチェーンに載せ，堅牢な分散台帳にしたものである．台帳をブロックチェーンに載せたものをブロックチェーン 1.0 と呼び，本稿の対象となる Ethereum はブロックチェーン 2.0 と呼ばれ，ブロックチェーン上で任意のプログラムを動かすことができる．これはブロックチェーンを改竄が困難なストレージとして扱い，それを操作するためのプログラムもブロックに記載するため非常に透明性が高く堅牢なアプリケーションが作れる．このプログラムはスマートコントラクトと呼ばれ，Ethereum では Ethereum Virtual Machine(以降，EVM とする) という仮想マシン上で実行される．EVM はチューリング完全な命令セットを持つため理論上は一般的な計算機と同じことができるが現時点では実装コストや実行コスト，実行時間は大きく劣る．スマートコントラクトでストレージに相当するものを状態と呼び，全てのフルノードがそれぞれ独立して最新の状態を保持する．状態はブロックに記載されることで永続化され，改竄耐性を得るように思えるがそうではない．状態は 2019 年 12 月時点で 200GB 以上あり，状態はトランザクションを処理する度に変化するため，その時々の状態を全てブロックに載せるとノード運用コストが激増してしまう．そのため状態はブロックチェーンの外部に保持され，ブロックチェーン自体には Merkle Patricia Trie[2] と言う木構造のルートハッシュのみが記載される．フルノードはネットワークに接続時し稼働を開始すると，最新の状態を得るために最初のブロックから全てのスマートコントラクトを順に実行して，状態を初期状態から最新状態に遷移させる．ネットワークから新たなブロックを得た場合は同様にスマートコントラクトを順に実行して最新の状態を得る．この時，各ノードが独立して状態を保持するが，前述のブロックチェーンと同じ理屈で，各ノードが同じスマートコントラクトを同じ順番で処理しているため最終的には同じ状態になる．

3 本研究の動機

DApp を利用するには Ethereum のネットワークに接続する必要があり，その方法は主にフルノードを運用する方法とライトノードを運用する方法の 2 種類に分かれる．フルノードは自身でトランザクションを処理し最新状態を得るため他者を信頼する必要がなく堅牢になるが，その代わりにある程度のマシンスペックが必要になり，低スペック PC やスマートフォンからの利用は今のところ現実的ではない．ライトノードは自身でトランザクションを処理せず，ネットワーク上のフルノードから最新状態をコピーする．これは先程とは反対で低スペック PC やスマートフォンなどの低スペック環境向けとなっており，その代わりに状態の信頼性をコピー元のフルノードに依存するというデメリットがある．DApp が広く普及し多くの利用者が様々な場面で利用するようになった場合，多くの利用者はコストのかかるフルノードではなく手軽なライトノードを選ぶと推測できる．しかし，ライトノードは前述の通り状態の信頼性をフルノードに依存するため，もしネットワー

ク内に悪意のあるフルノードが存在し，改竄した状態を広報していた場合，ライトノードは不正な状態を取得してしまう可能性がある．ブロックチェーンはその仕組み上ネットワークに対する改竄攻撃には強い耐性を持つが，個々のノードに関してはそうでもなく，自身が運用するフルノードに関しては状態の改竄が可能となる．利用者が運悪く，もしくは何らかの攻撃によって悪意のあるノードにのみ接続している状況では，不正な状態を不正だと判断できない．限られた状況ではあるが，将来的に PKI や DNS の様なクリティカルなサービスが DApp として実装された際のことを考えると，上記の様な状態改竄攻撃への対策が必要になる．

4 関連研究

この問題はノードの信頼・不信問題と捉えることもできる．Ethereum にはアカウントに信頼を付与する提案 ERC-1329 Inalienable Reputation Token[3] が既に存在する．これは譲渡不能な信頼トークンをアカウントに付与し，行動によってそれを増減するという提案である．信頼を付与するという点では参考になるが，この提案では不正を行った者に対するペナルティは信頼の減少のみであり，信頼そのものには価値がないため，前章で述べた攻撃に対する負のインセンティブにはなりえない．

5 不正摘発プロトコル

5.1 概要

我々の生活に欠かせないサービスの一つとして Domain Name System(以降，DNS とする) がある．DNS は hoge.example の様なドメイン名を 203.0.113.10 の様な IP アドレスに変換するサービスであり，これを DApp にした場合はドメイン名と IP アドレスのマッピングが状態に保存されることになる．仮に攻撃者が状態改竄攻撃を行った場合，状態に保存されていたドメイン名と IP アドレスのマッピングが改竄され，利用者が間違った IP アドレスを取得する危険がある．そこで本稿ではこの問題を軽減するために，パブリックチェーンの透明性を活かした状態改竄の発見・報告・懲罰の手法を提案する．懲罰では不正を行った者に経済的な損失を直接与えたほうが抑止力としての効果が高いと考えられるため，不正を行った者から Ethereum 内の通貨である ETH を強制的に徴収し，経済的な損失を直に与える．状態改竄に経済的リスクを発生させることによって不正を行うインセンティブを抑制できると考える．以降では状態改竄とその摘発のシナリオを役者毎に示す．役者は利用者・攻撃者・摘発者・懲罰執行者の 4 者とし，登場する DApp は前述の DNS とする．

5.2 利用者のシナリオ

利用者はこの DApp を用いて名前解決を行いたい

1. DApp を利用するために Ethereum のネットワークにライトクライアントして参加する
2. 必要な状態を得るために，ネットワーク上のフルノードから状態を取得する
3. DApp と取得した状態で名前解決を行う

5.3 攻撃者のシナリオ

攻撃者は DApp 利用者に間違った名前解決をさせたい

1. Ethereum のネットワークにフルノードとして参加する
2. フルノードとしてトランザクションを処理し，通常通り状態遷移するなかで，対象 DApp の状態のみを改竄する
3. 偶然もしくは何らかの攻撃を用いて，利用者にコピー元のフルノードとして選択される
4. 利用者に改竄した状態を提供する

5.4 摘発者のシナリオ

摘発者は賞金稼ぎのようなもので，不正なノードを発見して賞金を得たい

1. 適当なフルノードを検査対象とする
2. 状態が改竄されていないか確認する
3. 改竄を懲罰執行者に報告する

5.5 懲罰執行者のシナリオ

1. 摘発者の報告に対して，本当に改竄されているか確認する
2. 改竄が確認された場合，そのフルノードに懲罰を科し，摘発者に報酬を与える

5.6 懲罰の詳細

懲罰を科すにあたり，本稿では Ethereum 2.0 より導入される予定のデポジットの仕組を利用する．Ethereum 2.0 では従来の Proof of Work では無く Proof of Stake(以降 PoS とする) という手法で合意を得る．PoS には従来のマイニングに代わるステーキングと言うものがあり，これに参加するには 32ETH のデポジットが必要となる．デポジットはステーキングによって増加し，一定期間オフラインになるなどのプロトコルで定められた違反を犯すことで減少する．Ethereum 2.0 の PoS プロトコルは Casper と呼ばれ，デポジットの徴収・増加・減少を専用のスマートコントラクトが行う．Casper のスマートコントラクトは Ethereum 2.0 のプロトコルの一部であり，実装は通常のスマートコントラクトと同じであり，各ノードでそれぞれ処理される．このスマートコントラクトに懲罰執行者にあたるプログラムを追加し，摘発者はこのスマートコントラクトを実行することで改竄の報告をする．スマートコントラクト内では改竄の確認・懲罰執行・報酬支払いを自動的に行う．

6 終わりに

本稿では Ethereum と DApp の概要を説明した上で状態改竄攻撃の可能性を提起した．その軽減策として不正に対する経済的損失を与える仕組を Ethereum 2.0 に導入し，不正を行うインセンティブを低下させる提案をした．この提案は近い将来に実装予定の Ethereum 2.0 と親和性があり，不正を行った者への懲罰や摘発者に対する報酬支払いを Casper プロトコルのデポジットの仕組を流用することで実現難易度を下げている．

参考文献

[1] DR. GAVIN WOOD, ”ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER” https://ethereum.github.io/yellowpaper/paper.pdf (2019-10)
[2] ”Patricia-Tree” https://github.com/ethereum/wiki/wiki/Patricia-Tree (2019-03)
[3] ”ERC-1329: Inalienable Reputation Token” https://github.com/ethereum/EIPs/issues/1329 (2018-04)