5V-04

ブロックチェーン上のスマートコントラクトを利用した NTMobile システムの基礎的検証

木村　信裕 †1　柳瀬　知広 †2　田中　久順 †2　鈴木　秀和 †1　内藤　克浩 †3　渡邊　晃 †1
†1 名城大学理工学部　†2 名城大学大学院理工学研究科　†3 愛知工業大学情報科学部

1　はじめに

IPv4/IPv6 混在環境において，移動透過性を実現する技術として，NTMobile（Network Traversal with Mobility）が提案されている [1]．しかし，NTMobile を実装した端末とサーバ間及びサーバとサーバ間に依存関係があるため，サーバ障害などによりシステムが利用不能になる可能性がある．そこで，上記の課題を解決するとともに，端末の認証や暗号鍵の交換を簡単にするため，ブロックチェーンを導入した新たな仕組みを検討している．本稿では，ブロックチェーンのスマートコントラクトを用いた NTMobile システムの基礎的実装を行い，その有用性を確認する．

2　NTMobile の概要

NTMobile は，NTM 端末（NTMobile を実装した端末）の他，NTM 端末の管理や経路指示を担当する DC（Direction Coordinator），NTM 端末間で直接通信できない場合に通信を中継する RS（Relay Server），NTM 端末の認証を行う AS（Account Server）などで構成される．DC と RS は複数台設置可能であるが，AS は NTMobile ネットワーク内に 1 台のみ設置可能である．全ての DC が 1 台の AS に依存しており，また NTM 端末が特定の DC に依存し，その依存関係を変更できないという課題がある．このため，DC や NTM 端末は，依存している AS や DC に障害が発生した場合に，その障害を回避できず，NTMobile システムを利用できない可能性がある．

3　検討手法

図 1 に検討手法の概要を示す．検討手法では，各 DC をブロックチェーンで接続し，スマートコントラクトによって Node Transaction を管理する．Node Transaction は NTM 端末が発行する，発行端末自身の情報である．

検討手法では新たに，NTM 端末は楕円曲線暗号の秘密鍵および公開鍵を持つ．また，NTM 端末は公開鍵のハッシュ値から生成される端末 ID で識別される．

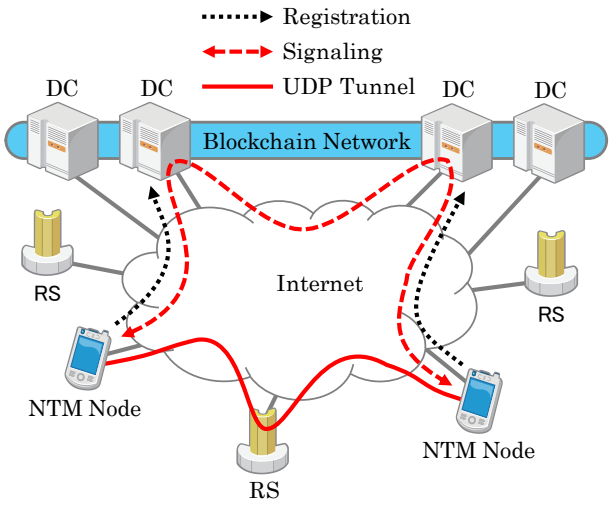

図 1　検討手法の概要

表 1　Node Transaction のフィールド

フィールド名	内容
端末 ID	端末の公開鍵のハッシュ値から生成された ID
収容 DC	端末を管理する DC のホスト名
タイムスタンプ	トランザクションの生成時刻
失効フラグ	端末の有効性を示すフラグ
署名	端末の秘密鍵による上記情報の署名

表 1 に Node Transaction に含まれるフィールドを示す．Node Transaction には発行端末の端末 ID および署名を含む．楕円曲線暗号では署名から公開鍵が算出できるため，公開鍵と端末 ID の対応関係から Node Transaction に含まれる端末 ID が署名端末自身のものであるかどうか検証が可能である．この検証に，公開鍵証明書は必要ない．

スマートコントラクトとは，Ethereum[2] などのブロックチェーン基盤が持つ，データの処理などのプログラムを確実に実行することができる仕組みである．

3.1　端末登録処理

NTM 端末は自身の Node Transaction を作成し，接続したい任意の DC に対し送信する．DC は，Node Transaction を検証することで送信端末の端末 ID を認証し，検証した Node Transaction をスマートコントラクトに送信する．また，NTM 端末は DC に対して，認証に利用する Node Transaction の他に，自端末の公開鍵や IP アドレスなどの情報も送信し，DC に保管される．

A Basic Examination of NTMobile System Using Smart Contract on Blockchain

Nobuhiro Kimura†1, Tomohiro Yanase†2, Hisayoshi Tanaka†2, Hidekazu Suzuki†1, Katsuhiro Naito†3 and Akira Watanabe†1
†1 Faculty of Science and Technology, Meijo University
†2 Graduate School of Science and Technology, Meijo University
†3 Faculty of Information Science, Aichi Institute of Technology

3.2 シグナリング処理

NTM 端末は自端末の収容 DC（以後，自 DC）に相手端末の端末 ID を送信する．自 DC はスマートコントラクトで相手端末の端末 ID を検索し，相手端末の収容 DC（以後，相手 DC）を特定する．自 DC は相手 DC から相手端末の IP アドレスや公開鍵などの端末情報を取得する．自 DC はお互いの端末の端末情報を元に，トンネルの経路を計算し，お互いの端末に経路指示を送信する．経路指示は，場合に応じて RS を経由する経路が指示される．

3.3 トンネル構築処理

それぞれの端末は，経路指示に含まれる相手端末の公開鍵と自端末の秘密鍵を元に楕円曲線 Diffie-Hellman 鍵共有を行い，トンネルを暗号化するための鍵（エンド鍵）を生成する．また，受信した経路指示に含まれる接続先 IP アドレスとポート番号，役割（受信待機やホールパンチングなど）に応じた処理を行い，通信を確立することで，エンド鍵で暗号化されたトンネルを構築する．

なお，相手端末の公開鍵は DC から取得しているが，公開鍵から相手端末の端末 ID を求めることができることから，公開鍵証明書なしに相手端末を識別することができる．また，悪意のある端末が他端末の公開鍵を騙った場合，秘密鍵がない限りエンド鍵を生成できず，中間者攻撃は行えない．

4 実装および動作検証

4.1 実装

Go 言語と Ethereum を用い，検討手法の基礎的実装を行い，動作検証を行なった．Ethereum は，ブロックチェーンを利用した分散アプリケーション基盤である．Ethereum では Solidity と呼ばれる専用の言語を用いてチューリング完全なスマートコントラクトを記述し，独自の P2P ネットワーク（Ethereum ネットワーク）上で動作させることができる．今回は，Node Transaction を扱うスマートコントラクトを Solidity で実装し，各 DC で構築した Ethereum プライベートネットワークで動作させた．Ethereum ネットワークはブロックチェーンネットワークであり，合意アルゴリズムによって対改ざん性が保証される．DC には，NTM 端末の認証，スマートコントラクトへの接続，RS を経由した経路指示の送信を実装した．RS には，トンネルの中継処理を実装した．NTM 端末には，秘密鍵の生成，DC への位置登録，経路指示を元にした他の NTM 端末と暗号化トンネルの構築，トンネルを用いたパケットの送受信を実装した．

4.2 動作検証

実装した DC および RS を Amazon Web Services の仮想プライベートサーバサービスである Amazon Lightsail で構築し，動作検証を行なった．NTM 端末から DC に接続し，Node Transaction とスマートコントラクトを用いた認証を行った後，NTM 端末同士でトンネル通信を行えることが確認できた．また，一方または両方の NTM 端末が DC を変更した場合でも，スマートコントラクトによって情報が共有され，トンネル構築を行えることを確認できた．

表 2　従来手法と検討手法の比較

	従来手法	検討手法
システム全体の可用性	△	○
NTM 端末の可用性	△	○
認証情報管理の容易さ	×	○
エンド鍵交換の容易さ	×	○

5 評価

表 2 に従来手法と検討手法の比較表を示す．従来手法では，NTM 端末は AS にアカウントを用いてログインする必要があったが，検討手法では AS は必要ないため，認証の可用性が向上している．また，アカウント管理が不要となり，NTMobile を運用する側としての有用性も高い．検討手法ではアカウントがない代わりに，新たに NTM 端末が公開鍵を持つが，公開鍵証明書は必要ない．そのため，NTM 端末は内部で秘密鍵と公開鍵を生成するだけで NTMobile の利用を開始できる．

従来手法では，端末の ID として，DC のホスト名を含む FQDN を利用していたため，端末の ID を変更せずに収容 DC を変更することができなかったが，検討手法では可能である．このため，NTM 端末は収容 DC に障害が発生した場合，他の DC に端末登録を行うことで，システムを継続して利用することが可能となる．

従来手法では，複数の一時共通鍵を利用することでエンド鍵の交換を行っていた．しかし，検討手法ではお互いの NTM 端末の公開鍵を交換するだけで完了するため，必要なシーケンスが従来手法より簡易である．

以上のことから，可用性や運用管理の容易さの点で，検討手法の有用性を確認できた．

6 まとめ

本稿では，ブロックチェーン上のスマートコントラクトを利用した NTMobile システムについて，基礎的実装と動作検証を行った．従来の NTMobile と比較することで，システムの可用性が高く，運用管理が容易であることを確認した．

参考文献

[1] 上醉尾ほか：情報処理学会論文誌，Vol. 54，No.10，pp.2288–2299 (2013).
[2] Ethereum. https://ethereum.org
[3] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf