Hyperledger Fabric 1.0を用いた金融領域におけるブロックチェーン技術検証

鳥山 慎一　岡部 達也　田中 俊太郎　金子 雄介

要 旨

ブロックチェーンは、分散型台帳システムであり、中央集中管理機関を持たずに参加者間でデータの共有及び記録をする仕組みです。本稿では、品質面でシステム要件の高い金融機関のITシステムへのブロックチェーン適用性を見極めることを目的に、企業間連携の業務を一例に実施したPoCを紹介します。結果として、本PoCで採用したブロックチェーン基盤であるHyperledger Fabric 1.0は、運用/保守性やセキュリティの面で多くのシステム要件を充足することが判明した一方、現時点では改ざん耐性や暗号化機能など、未達成の項目も存在することが分かりました。

KeyWords　ブロックチェーン/Hyperledger Fabric/企業間連携

1. はじめに

ブロックチェーンは、サトシ・ナカモト氏により提唱されたBitcoinの基幹となる分散型台帳システムであり、中央集中管理機関を持たずに参加者間でデータの共有及び記録をする仕組みです[1)]。2018年時点では、金融業界に限らず、金融業界以外のさまざまな企業により研究開発や実証実験(Proof of Concept: PoC)が進められています[2) 3)]。

本稿では、ITシステムの信頼性やセキュリティなどの品質面でシステム要件の高い金融業界において、ブロックチェーンを用いたシステム実装で品質基準を充足できるかなどを見極めるべく、NEC、三井住友フィナンシャルグループ、日本総合研究所の三社合同で実施したPoCについて紹介します。

2. PoCの目的及び進め方

金融機関を含む企業間連携システムをユースケースとし、ブロックチェーンを活用したシステムの構築及び運用の実現性・有効性を見極めることをPoCの目的と設定しました。企業間連携に着目した理由は、以下に述べるブロックチェーンの性質との親和性が高いことにあります。

・真正性の高いチェック処理の自動化

・真正性の高いワークフロー実行履歴の保存

2.1 評価軸の選定

次に、金融業界のITシステムを実現する上で不可欠な以下2点を踏まえ、検証項目を定義しました[4) 5) 6)]。

(1) 運用/保守性

企業間連携ブロックチェーンシステムに必要な運用機能(ノード起動・停止、障害通知など)を洗い出すため、検証環境を構築し、実機での検証を実施しました。

(2) セキュリティ

企業間連携ブロックチェーンシステムで具備すべきセキュリティ機能(データ秘匿やアクセス制限、不正の追跡など)への整合性を見定めるため、検証環境で準拠性の検証を実施しました。

2.2 検証環境

以下に検証環境の概要、**図1**に全体概観を示します。

・2組織、各組織5台ずつ、計10台のサーバで構成

・AWS(Amazon Web Services)上に構築し、サーバのインスタンスタイプはすべてt2.medium(3.3GHz×2vCPU、4GBメモリ)を指定[7)]

ブロックチェーン基盤は、OSS(Open Source Software)のHyperledger Fabric 1.0(以下、Fabric

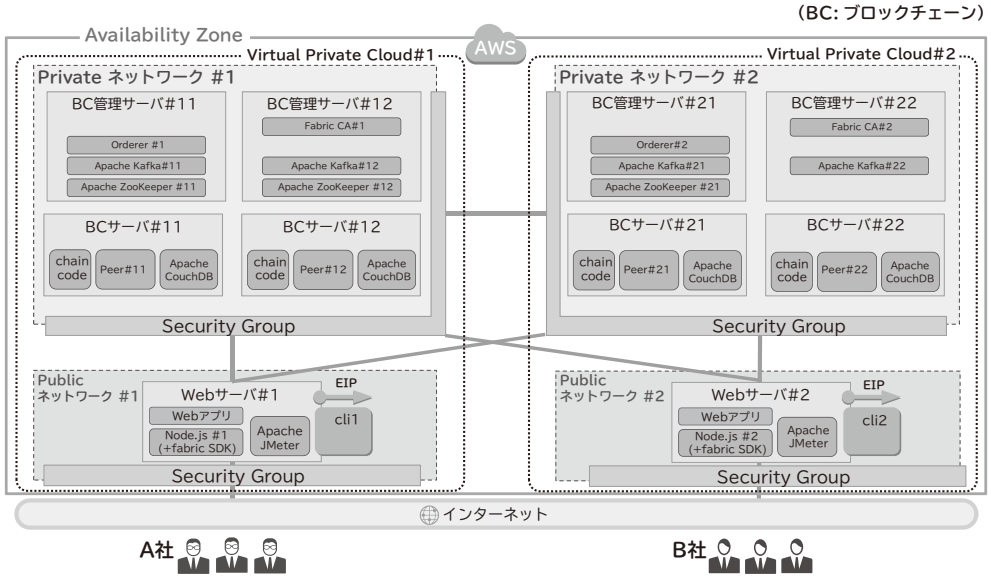


図1　検証環境の全体概観

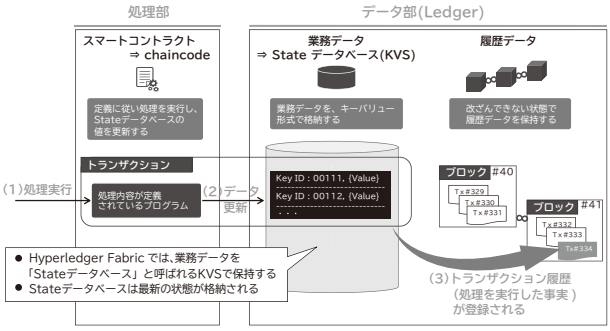


図2　Fabric 1.0におけるブロックチェーンの構成

1.0) を用いました[8) 9)]。Fabric 1.0は処理部とデータ部に大別でき、「スマートコントラクト」「業務データ」「履歴データ」の3つの要素で構成されます。Fabric 1.0では「スマートコントラクト」をchaincodeで記述し、「業務データ」をKVS (Key-Value Store) として保持します。**図2**に構成例を示します。

また、検証環境では、ユーザー操作画面の他に、以下の2つを開発しました。

- **呼出側アプリケーション**
  JavaScript言語で実装。ユーザー操作画面からのリクエストを処理し、chaincodeを呼び出す
- **chaincode**
  Go言語で実装。業務ロジックを実行する

3. PoCの結果

表1に結果概要を示します。Fabric 1.0は、運用/保守性やセキュリティの面で多くのシステム要件を充足することが判明した一方、現時点では未達成の項目も存在することが分かりました。それらについて、第3章各節で掘り下げて言及します。

3.1 運用/保守性

表2に結果詳細を示します。特筆すべき点として、保有するデータを改ざんされたノードは、改ざんされたことを自身で検知できないことが挙げられます。原因は、ノードがブロックを追加する時に、ハッシュチェーンを検証する処理が不十分なためです。ただし、改ざんされたデータが他のノードに伝播することはありません。また、実機検証にてFabric 1.0の仕様上の問題が2点判明しました。

3.2 セキュリティ

表3に結果詳細を示します。第3章1節でも改ざん耐性についての問題を指摘しましたが、Fabric 1.0は、データ秘匿やアクセス制限、不正の追跡などの機能が十分でないと言えます。なお、今後のHyperledger Fabricのバージョンアップによって、機能が追加される可能性があります。

表1　結果概要（全体サマリ）

	検証項目	ゴール（要件）	結果
1	データバックアップ、アーカイブの可否	10年分のデータを保存できること	△ 表2
2	アプリケーション追加・修正時のサービス影響	アプリケーション追加・修正時において、サービス停止とならないこと	○
3	ノード障害時の復旧可否	ノードDown時に、サービス影響がなく、ノード再参加が可能なこと	○
4	サービス監視の可否	サービス全体の監視方式が明確化されること	○
5	単一障害点の有無	単一障害においてサービス停止がないこと	○
6	単一組織障害のサービス影響	単一組織障害においてサービス停止がないこと	△ 表2
7	ノード障害の許容数	単一障害に伴うノード障害数が許容数より少ないこと	○
8	改ざん耐性	単一ノードの改ざんによって全ノードの改ざんができないこと	△ 表2
9	暗号化	データを秘匿できる仕組みが具備されていること	△ 表3
10	権限管理	アクセスを制限できる仕組みが具備されていること	△ 表3
11	改ざん検知	不正を追跡できる仕組みが具備されていること	△ 表3

（○:問題なし、△:問題あり＜回避策あり＞、×:問題あり＜回避策なし＞）

表2　未達成項目の結果詳細（運用/保守性）

検証項目	検証結果	表1参照
データバックアップ、アーカイブの可否	取引量が多い場合、Diskの追加やアーカイブが必要	1
単一組織障害のサービス影響	2組織では1組織の全サーバDown時にサービス停止が発生（分散メッセージングシステムのスプリットブレインにより、ブロック生成が停止する）	6
改ざん耐性	改ざんした内容は改ざんノード自身では検知せず、改ざんされた状態のまま、処理が継続 不正トランザクション発生時のハードフォーク方針の策定も必要	8
アプリケーションと基盤の分離	組織数を変更するたびに呼出側アプリケーションの修正が発生	※
トランザクションの排他制御	KVSでマスタデータ（読取）とトランザクションデータ（追記）の分離が必要	※

（※：検証にて追加で判明した項目）

表3　未達成項目の結果詳細（セキュリティ）

検証項目	検証結果	表1参照
暗号化	データ（履歴・KVS）は公開されるので、暗号化の仕組みが別途必要 秘密鍵も平文ではなく暗号化された状態での管理が必要	9
権限管理	一般ユーザーが操作する際にはユーザー認証が必要	10
改ざん検知	不正行為発生時の調査に監査ログが必要	11

4. PoCの結果に対する考察

PoCの結果から、金融サービスの基盤としてFabric 1.0を採用するには、現時点で不足している機能を補完するシステムを外部で実装するなどの検討・検証が必要と考えられます。**図3**に結果を鑑みたシステム構成例を示します。

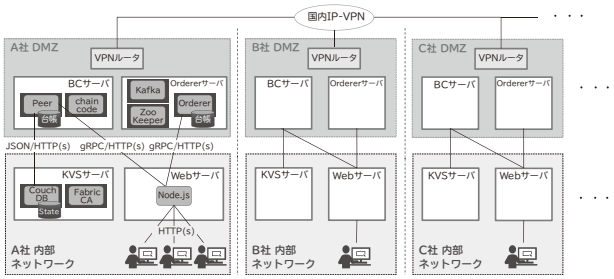


図3　結果を鑑みたシステム構成

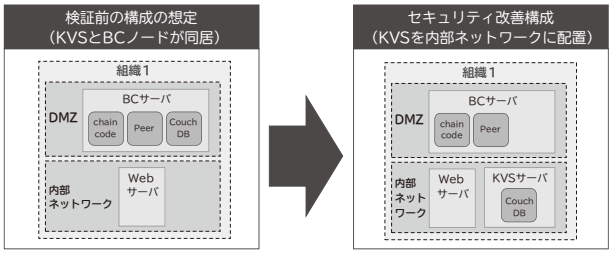


図4　配置セグメント

4.1 運用/保守性

(1)改ざん耐性

Fabric 1.0では、ブロックチェーンの改ざん耐性の肝となるハッシュチェーンの検証処理が不足しているため、金融機関のITシステムへ適用するには、機能追加が必須となります。

(2) データアーカイブ

Fabric 1.0においては、履歴データ、業務データのいずれにおいても、データは増加する一方であるため、ブロックチェーンを活用するシステムごとにデータの増加量、及び、増加に対する応答性能の劣化を測定し、アーカイブの必要性を検討する必要があります。

4.2 セキュリティ

(1)システム構成

Fabric 1.0におけるシステム構成においては、業務データを保存しているデータベースに対する攻撃耐性を向上させるため、KVSサーバを内部ネットワークに配置する必要があります（**図4**）。

(2)監査ログ

Fabric 1.0には監査ログを取る機能がありません。ただし、金融業界のITシステムにおいてはデータへの

アクセスの証跡を取ることが要件となる場合が多いため、別途、監査ログを取る仕組みを導入する必要があります。

(3) 鍵管理

Fabric1.0には秘密鍵の管理機能がありません。一般にブロックチェーン基盤では秘密鍵が盗まれないことを前提にしたセキュリティ保証であるため、金融サービスの基盤として採用する場合は、別途、秘密鍵の管理方式を検討する必要があります。例えば、PKCS（Public Key Cryptography Standards）を鍵管理に利用することで対応可能です。

5. おわりに

本稿では、企業間連携システムをユースケースとして、Fabric 1.0が金融業界で求められる品質基準を充足する部分と充足しない部分を明らかにし、ブロックチェーンを取り入れた金融機関のITシステム構築時の留意事項を示しました。ブロックチェーンの適用範囲は、仮想通貨の送金にとどまらず、価値ある情報の共有や、スマートコントラクト機能を活用したシェアリングエコノミーの社会実装など、その広がりが国内外のさまざまな業種で期待されています。しかし、本稿で紹介したPoCで明らかになった項目を含め、実業務への適用にはまだクリアすべき事項が存在しています。ブロックチェーン自体、いまだ仮想通貨以外のユースケースが少ないため、外部セキュリティ監査により、他に具備すべき機能の実装漏れがないかを改めて点検し、詳細にリスクを洗い出すことが必要であるとも考えられます。NECは、実業務へのブロックチェーン適用に向けて、PoCで明らかになった課題を補完するシステム構成での追加PoC、取り巻く社会環境の変化を鑑みた適用分野の拡大、Hyperledger Fabricへのノウハウ還元による普及促進を通じ、ビジネスの発展や豊かで明るい社会や未来を支える社会の実現に貢献していきます[10)]。また、三井住友フィナンシャルグループ及び日本総合研究所は一体となって新しいIT技術の積極的な活用に取り組むことで、時代の変化に対応しながら、企業競争力の高い先進的な金融グループを目指すとともに、お客様へのサービス向上に努めていきます。

参考文献

1) Satoshi Nakamoto：Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf
2) ガートナー、ブロックチェーンへの取り組みに関する調査結果を発表，ガートナー ジャパン株式会社，2018.4
https://www.gartner.co.jp/press/html/pr20180405-01.html
3) 鳥山慎一ほか：ブロックチェーンによる企業間連携の実用化に向けた取り組み，NEC技報，Vol.69 No.2，pp.20-24，2016.3
https://jpn.nec.com/techrep/journal/g16/n02/160205.html
4) FISC：FISC サイバーセキュリティ参考情報，金融情報システムセンター，2017.5
https://www.fisc.or.jp/isolate/?id=822&c=topics&sid=241
5) 経済産業省：ブロックチェーン技術を活用したシステムの評価軸 ver1.0，2017.3
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/pdf/010_s04_00.pdf
6) 独立行政法人情報処理推進機構：非機能要求グレード，2018.4
https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html
7) アマゾン ウェブ サービス（AWS）
https://aws.amazon.com/
8) Welcome to Hyperledger Fabric
https://hyperledger-fabric.readthedocs.io/en/release-1.0/
9) Hyperledger
https://www.hyperledger.org/
10) NECプレスリリース：NEC、世界最速 毎秒10万件超の取引を可能にするブロックチェーン技術を開発，2018.2
https://jpn.nec.com/press/201802/20180215_03.html

執筆者プロフィール

鳥山 慎一
金融システム開発本部
マネージャー

岡部 達也
金融システム開発本部
主任

田中 俊太郎
株式会社日本総合研究所
開発推進部門
先端技術ラボ

金子 雄介
株式会社三井住友フィナンシャルグループ
ITイノベーション推進部

関連URL

NEC 金融ソリューション
https://jpn.nec.com/financial/index.html

株式会社三井住友フィナンシャルグループ
http://www.smfg.co.jp/

株式会社日本総合研究所
https://www.jri.co.jp/

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.71 No.1　データを活用した持続可能な都市経営特集

データを活用した持続可能な都市経営特集によせて
データ利活用型スマートシティの始動

◇ 特集論文

データを活用した都市経営のビジョン
世界のデータ利活用型スマートシティ開発動向
持続可能な社会に向けた都市経営へのパラダイムシフト

データ利活用型スマートシティの実証・実装事例
データを活用した都市経営の海外事例
FIWAREを活用したスマートシティ向け共通プラットフォームの構築（高松市事例）
豊島区における「群衆行動解析技術」を活用した総合防災システム
訪日外国人向けのおもてなしサービスの高度化と地域活性化への取り組み事例
自治体データ活用事例 ～財務・子育て・地域振興などのさまざまなデータ活用～

シティマネジメント技術
データ利活用型都市経営を実現する情報プラットフォーム：FIWARE
FogFlow：クラウドとエッジを通じたIoTサービスのオーケストレーション
スマートシティIoTに求められるセキュリティ要件と技術
欧州におけるスマートシティとSociety 5.0の実現へ向けての標準化の動向
都市評価指標標準とその活用

地域共創
地域共創基盤としての「スマートシティたかまつ推進協議会」
枠を超えた共創活動「せとうちDMO」の立ち上げ
包括連携協定による地域共創
「新たな行政サービス共創研究会」が創るこれからのあたりまえ

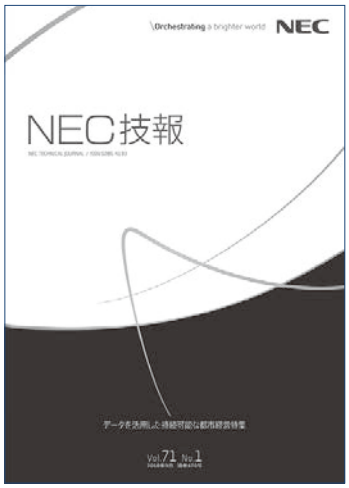
◇普通論文

スピン流熱電変換 ～インフォマティクスを活用した材料開発と適用領域～
NanoBridge-FPGAによるIoTデバイスの低電力・高性能化
IoTデバイス応用に向けたナノカーボンの材料開発
Hyperledger Fabric 1.0を用いた金融領域におけるブロックチェーン技術検証

◇ NEC Information

C&Cユーザーフォーラム＆iEXPO2017　Orchestrating a brighter world
基調講演
展示会報告

NEWS
2017年度C&C賞表彰式開催



Vol.71 No.1
（2018年9月）

特集TOP