博士学位論文審査要旨

２０２２年1月１２日

論文題目：　Study on the Highly Reliable and Secure Data Management System under Weak ICT Environment by Blockchain Technology
（ブロックチェーン技術を用いた貧弱なICT環境下での高信頼・高セキュアデータ管理システムの研究）

学位申請者：　AGODA-KOUSSEMA RAGOUGUELABA

審査委員：

主　査：　理工学研究科　教授　　芳賀　博英
副　査：　理工学研究科　教授　　片桐　滋
副　査：　理工学部　　准教授　小野　景子

要　　旨：

本論文は貧弱な情報通信（ICT）環境下での，ブロックチェーン技術を用いた高信頼データ管理システムの設計と実装について述べたものである．申請者の母国（トーゴ）などの開発途上国ではICT環境が整備されていないが，そのような環境下でも住民サービスの向上が求められている．本論文では，住民データの管理を具体的対象として，ブロックチェーンを使ってデータの信頼性を担保する方法を提案している．ブロックチェーンの本質は改ざんが極めて困難な追記型データベースである．第１章は序論であり，本論文が目指す最終目標について述べ，その後に実現のために利用する方法について述べている．第２章は本論文の関連研究の紹介と，ブロックチェーンの技術的説明を行っている．第３章では住民データの登録・削除・変更などとともに，登録されたデータに基づいて，出生証明などの書類をユーザに提供するシステムを目標として設定したことを述べている．さらにユーザインタフェースとして，Web アプリの形式を提供すること，そしてWebアプリ構築のためにPrimeFacesというJavaベースのwebアプリ開発用のフレームワークを用いることも述べられている．第４章ではスクラッチからブロックチェーンを実装し，システムを開発する方法を述べている．第５章は既存のブロックチェーンフレームワークの一つであるMultiChainを用いたシステムの設計と実装について述べている．第６章はもう一つのフレームワークであるHyperledger Fabricを用いたシステムの設計と実装について述べている．第７章は本システムで用いたユーザインタフェースを実装するための Web アプリケーションフレームワークであるPrimeFacesを紹介している．PrimeFacesはJavaベースのWebアプリフレームワークであり，Javaによるシステムに容易に組み込めることが述べてある．第８章は３つの開発方法の比較であり，結論的にはスクラッチからの開発が最も効率的で適切であると結論づけている．第９章は本論文のまとめである．

本論文は現場のニーズを捉えてそれを情報システムを使って解決するという，情報システム研究の王道と言える手法に基づいた課題解決法であり，情報システム開発において，学術的に十分な価値を有するものと認める．よって，本論文は，博士（工学）（同志社大学）の学位論文として十分な価値を有するものと認められる．

総合試験結果の要旨

２０２２年1月１２日

論 文 題 目： Study on the Highly Reliable and Secure Data Management System under Weak ICT Environment by Blockchain Technology
(ブロックチェーン技術を用いた貧弱な ICT 環境下での高信頼・高セキュアデータ管理システムの研究)

学位申請者: AGODA-KOUSSEMA RAGOUGUELABA

審 査 委 員：
主　査：　理工学研究科　教授　　芳賀　博英
副　査：　理工学研究科　教授　　片桐　滋
副　査：　理工学部　　准教授　小野　景子

要　　旨：

2022 年 1 月 6 日の午後 1 時から 2 時 30 分までの 1 時間半に渡り, Zoom システムを用いてオンラインで博士論文公聴会を実施した．学位申請者からの学位論文内容の発表後に，主査と副査によって論文の内容及び関連分野についての口頭による質疑応答を実施した．主査と副査からのさまざまな質問に対して学位申請者から的確な解答がなされ，学位申請者が十分な専門知識を持っていることを確認できた.

学位申請者は修士論文及び博士論文を英語で執筆していること，さらに英文の論文を論文誌に２編，国際学会に１編発表し，学会において英語で口頭発表を行なっていることにより，十分な英語力を持っていることが確認できた．よって，総合試験の結果は合格であると認める.

博 士 学 位 論 文 要 旨

論 文 題 目： Study on the Highly Reliable and Secure Data Management System under Weak ICT Environment by Blockchain Technology
（ブロックチェーン技術を用いた貧弱なICT環境下での高信頼・高セキュアデータ管理システムの研究）

氏　　名： AGODA-KOUSSEMA RAGOUGUELABA

要　　旨：

本論文はブロックチェーン技術を用いた，貧弱な情報通信(ICT)環境下での高信頼なデータ管理システムの設計と実装について述べたものである．本論文の内容は出身国であるトーゴ共和国（トーゴ）の現状と深く関連している．トーゴは世界最貧国のひとつであり，生活に必要なさまざまなインフラが十分整備されているとは言い難い状況である．特に現代生活に欠かせない情報通信インフラは貧弱である．有線通信網の構築には多大な費用がかかるが，トーゴは経済的に必ずしも恵まれていないため，一部の地域を除いてほとんど整備されていない．そのためICTを活用した住民への各種のサービスはこれまで限定されていた．しかし近年携帯電話に代表される無線通信網が急速に整備され始めてきた．無線通信網は有線に比べると投資額が格段に低く，地理的な条件に影響されにくいため急速に整備が進み，現在では国民の多くが携帯電話を利用できるようになってきた．従って，今後国民にICTによる恩恵をあまねく広めることが求められている．その最も基礎的なサービスが，各種行政機関が提供するサービスである．

国家等の最も基本的なデータの一つが住民データである．これは日本の戸籍や住民登録に相当するデータであり，住民の誕生や死亡，居住地などのデータが含まれる．そこで本研究では，この住民データを管理する情報システムをターゲットとして研究を開始した．住民データ管理システムの構築において最も重要な点の一つが，データの信頼性である．データを電子化して記録するときには，特にデータの改ざんが大きな課題になる．従ってデータの改ざんが起こらないこと，少なくとも改ざんされたことを検知することが必須となる．そこで着目したのがブロックチェーン技術である．ブロックチェーン技術は暗号資産の出現とともに注目されているものであるが，暗号資産に固有の技術ではない．ブロックチェーンの本質は，改ざんが原理的には不可能ではないが実質的には極めて困難な追記型データベース技術である．そこでその特性を利用して，信頼性の高い住民情報管理用のデータベースを構築できると考えた．またこの住民情報管理システムへのアクセスの手段としては，現地でのスマホの普及を考慮して専用端末や専用アプリなどの形式ではなくWebアプリケーションの形式で提供することにした．これによって住民はサービスを受けるときに役所などへ赴く必要がなくなり，自分の居住地でインターネットを利用して手軽にサービスを受けることができる環境を実現することを目指した．以下本論文の構成を述べる．

第1章は序論であり，上記に述べた状況を説明したのちに，本論文が目指す最終目標について述べ，その後に実現のために利用する方法について述べている．

第2章は本論文の関連研究の紹介と，ブロックチェーンの説明を行っている．ブロックチェーンが最初に注目されたのはSatoshi Nakamotoという匿名の研究者が発表した，信頼できる中央集権的な存在がなくても，個々のステークホルダー間の情報のやりとりを保証することができるメカニズムである．このメカニズムを決済手段に適用したものが暗号資産である．そしてこれを決済手段以外に利用したものとして，ヨーロッパのエストニアにおけるKeyless Signature Infrastructureがある．これはエストニア全土で国民の情報を管理するにあたって，全ての国民

に個々のハッシュ値と呼ばれる値を割り当て，これをもとにしてブロックチェーンを実現している．また小規模な適用例として，やはり高度な信頼性が求められる医療分野への応用について紹介している．ブロックチェーンの説明においては，ブロックチェーンがブロックと呼ばれるデータの集合をポインタで連結したものであることを述べている．そしてポインタで結合するときに，そのデータを繋ぐために各ブロックのハッシュ値を使う．あるブロックのハッシュ値は前のブロックの全てのデータを使って計算される．従って前のブロックのデータの改ざんがあった場合には，その改ざんが異なったハッシュ値を生成するので，改ざんされた場合にはすぐに検出することができる．正しいハッシュ値を計算するには，膨大な計算が必要であり，実質的には改ざんが不可能であることが説明されている．そしてブロックチェーンの形態として関与者の数に応じてプライベート，コンソーシアム，パブリックの三つの種類があることが述べられ，その上で対象のアプリケーションにはコンソーシアム型あるいはプライベート型のブロックチェーンが適していることが述べられている．さらにブロックチェーンを実現するために，既にいくつか提供されているフレームワークのうちのいくつかもこの章で紹介している．

第3章では設計と実装の対象としたシステムの概要が述べられている．このシステムは住民データの登録・削除・変更などとともに，登録されたデータに基づいて，出生証明などの書類をユーザに提供するシステムを目標として設定したことを述べている．さらにユーザインタフェースとして，Web アプリの形式を提供すること，そして Web アプリ構築のために PrimeFaces という Java ベースの web アプリ開発用のフレームワークを用いることも述べられている．データの格納に用いるリレーショナルデータベースのスキーマ設計の概要についても示している．

第4章は，ブロックチェーンの実現のために特定のフレームワークを用いないで，スクラッチからブロックチェーンを実装して，当該システムを実現することについて述べてある．これは特定のフレームワークを用いないで，自分に必要な機能のみを実装することにより，開発の工数とシステムの可視性を向上させることを目的としている．Web アプリケーションの開発に用いた PrimeFaces が Java ベースのものであるので，ブロックチェーンの開発にも Java を用いている．ブロックチェーンは原理がさほど複雑ではないので，Java を用いてスクラッチで開発することもさほど難しいことではない．本章ではブロックチェーンと RDBMS，PrimeFaces との接続を実現し，システムを実装した経緯の詳細が述べられている．

第5章は既存のブロックチェーンフレームワークの一つである MultiChain を用いたシステムの設計と実装について述べている．MultiChain フレームワークは主としてプライベートブロックチェーンの実装を目的としている．今回のシステムは国家あるいは自治体という一つの組織がデータの管理に関与するものであるので，組織の規模は大きいが形態上はプライベートブロックチェーンと考えることもできる．MultiChain は実装言語として Java もサポートしているので，全てを Java で実装している．基本的には第4章で実装したシステムのブロックチェーンの部分を MiltiChain に変更しただけであるので，システムの実装そのものはさほど工数はかからずに実装され，想定した機能を実現できたことが報告されている．

第6章は Hyperledger Fabric を用いたシステムの設計と実装について述べている．Hyperledger Fabric は Linux Foundation が主導する Hyperledger プロジェクトの一つであり，複数のフレームワークを提供しているが，Fabric はその中で最も多く使われているフレームワークである．Fabric は基本的には複数の関与主体が存在するコンソーシアム型をサポートしているが，目標システムにおいて，個々の自治体等を一つの参加主体と考えた場合には，そのネットワークはコンソーシアム型と考えられるので，Hyperledger Fabric を用いて実装することができる．今回の実装においても第5章と同じように，システム全体の構成要素の中のブロックチェーンの部分だけを Fabric に入れ替えるだけであり，システムの実装について大きな問題はなかったことが述べてある．

第7章はシステムのユーザインタフェースを実装しているフレームワークである PrimeFaces

について述べている．PrimeFaces は Java ベースの Web アプリフレームワークであり，Java によるシステムに容易に組み込めることが述べてあり，その後 PrimeFaces を用いて実装した Web インタフェースのスクリーンショットが示されている．

第 8 章は第 4 章から第 6 章に述べられている三つのシステムの実装の比較を行なっている．そこでは二つのフレームワークを利用した開発においては，それぞれのフレームワークのインストールが完成さえすれば，その上での特定のプリケーションの開発にさほど困難はないが，フレームワークのインストールそのものがかなり困難であることが明らかになったことが述べられている．特にフレームワークに利用している様々なソフトウエアのバージョンの関係がかなりクリティカルで，指定されたバージョンのサポートソフトを利用しないと，一見するとインストールが成功したように見えて，実は重要なポイントが動作しないというエラーが発生したこと，フレームワークは多様なアプリをサポートするために，当該アプリには不要なコンポーネントもインストールされるが，その不要なコンポーネントのインストールのために，全体がインストールできず開発が進まない，という課題があったことが述べられている．そして結論的には，開発者側にある程度の技術力があれば，スクラッチからの開発が全体を見ると最も好ましいと結論している．

第 9 章は本論文のまとめである．