一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
NS2019-205(2020-03)

ブロックチェーンを用いた個人信用度評価方式

許斐　健太†　　上山　憲昭††

† 福岡大学 大学院 工学研究科 電子情報工学専攻　〒 814–0180 福岡市城南区七隈 8–19–1
†† 福岡大学 工学部 電子情報工学科　〒 814–0180 福岡市城南区七隈 8–19–1
E-mail: †td192003@cis.fukuoka-u.ac.jp, ††kamiyama@fukuoka-u.ac.jp

あらまし　近年中国では個人の信用スコアを，融資，賃貸，シェアサイクルなどの様々な場面で活用する動きが高まっている．また海外や日本でも信用スコアを使用する動きが高まっている．現在は一企業が個人ごとに個人の信用スコアを算出しているため，個人の信用スコアの算出方法は企業に依存しているのが現状である．また信用スコアの提供サービスを特定の企業や団体が運営しており，その企業や団体が信用スコア算出などで個人情報を管理するためプライバシィの問題がある．一方，暗号通貨の核となる Blockchain を用いることによって，第三者を通さずに通貨の受け渡しが可能である．Blockchain はシステム管理者も含めデータの改ざんが困難であり，利用者がアドレスで管理されているためプライバシィ情報も秘匿できることから，IoT データの管理など様々な分野での応用が期待されている．さらに Ethereum と呼ばれる通貨には通貨の受け渡し以外にスマートコントラクトと呼ばれる自動契約を第三者を必要とせず履行できる仕組みを有してている．そこで本稿では Ethereum を使用することで，個人の信用スコアの算出方法を一企業に依存せず誰もが個人の信用スコアを評価するしくみと，そのシステムを使用したビジネスモデルを提案する．そして実験室環境で実装した Ethereum 上で提案システムを動かした動作検証結果について述べる．
キーワード　信用スコア，ブロックチェーン，イーサリアム

Providing Personal Credit Rating System Using Blockchain

Kenta KONOMI† and Noriaki KAMIYAMA††

† Graduate School of Engineering, Fukuoka University
8–19–1, Nanakuma, Jounan, Fukuoka 814–0180
†† Department of Electronic and Information Technology, Faculty of Engineering, Fukuoka University
8–19–1, Nanakuma, Jounan, Fukuoka 814–0180
E-mail: †td192003@cis.fukuoka-u.ac.jp, ††kamiyama@fukuoka-u.ac.jp

Abstract　In recent years, there has been an increasing movement in China to use personal credit scores in various situations such as lending, leasing, and share cycles. The use of credit scores is increasing overseas and in Japan. At present, one company calculates the individual's credit score for each individual, so the method of calculating the individual's credit score depends on the company at present. In addition, there is a privacy problem because a specific company or group manages personal information such as credit score calculation. On the other hand, by using the blockchain, which is the core of cryptocurrency, it is possible to transfer currency without passing through third parties. Blockchain is difficult to falsify data including system administrators, and privacy information can be concealed because users are managed by address. Therefore, applications in various fields such as IoT data management are expected. In addition, the currency called ethereum has a mechanism that can execute automatic contracts called smart contracts without requiring a third party, in addition to the transfer of currency. Therefore, in this study, we propose a system that evaluates an individual's credit score by using ethereum and does not depend on a single company for calculating an individual's credit score, and proposes a business model using the system. We also show numerical results of the proposed scheme executed on the ethereum implemented in our laboratory.
Key words　credit score, blockchain, ethereum

1. はじめに

近年中国では芝麻信用，米国では FICO スコアなどの個人の信用スコアを使用したサービスが注目されている．芝麻信用のシステムでは個人の信用スコアが 350 点〜950 点の範囲で，身分，取引履歴，資産，交友関係などを元にクラウドコンピューティングや機械学習を用いて算出され，算出された信用スコアを使用してクレジットカード，不動産，公共サービスなど様々

なサービスに提供されている．FICO スコアは支払い履歴や借入額，クレジットなどの金融情報を元にスコアが算出されローンや電気やガス，賃貸などの契約などに使用されてる [1]．日本でも FICO スコアのような金融情報を元に信用スコアを算出し，信用スコアをサービスに利用しようとする動きが高まっている．現在の信用スコアではある企業がある個人の信用スコアを機械学習などを使用し算出している．これによって企業に信用スコアが依存するという問題がある．

また近年 Bitcoin を始めとした仮想通貨の基盤システムとしてのブロックチェーンが注目されている．データをブロック単位で保存し，通貨の取引データやスマートコントラクトと呼ばれる契約プログラムを一定時間ごとに保存していくシステムであり，ブロックは一つ前のブロックのハッシュ値を保存し，一本のチェーン状にデータが保存されるため，ブロックチェーンと呼ばれている．またこのシステムは管理する人によって 3 種類に分かれ，プライベートチェーン，コンソーシアムチェーン，パブリックチェーンがある．プライベートチェーンは基本的に一企業，一個人など限られた人がブロックチェーンを管理するものである．コンソーシアムチェーンは予め選出された複数の管理主体のみがブロックチェーンを管理するが，IBM が開発している Hyperledger Fabric がこれにあたる．パブリックチェーンは管理したい人がいれば誰でも管理することが可能なブロックチェーンであり，暗号通貨の取引で使用される Bitcoin や Ethereum がこれにあたる．

Ethereum は通貨の送金以外にスマートコントラクトを保存することができるブロックチェーンである．コンセンサスアルゴリズムと呼ばれるブロックチェーンにブロックを新しく保存する場合にブロック内のデータを改ざんされないためのアルゴリズムが存在する．Ethereum は Bitcoin と同じ PoW (proof of works) と呼ばれるアルゴリズムで Ethash と呼ばれるハッシュ計算を行い，最も早く答えを出した人に対し，ブロックを保存した時に支給される通貨と保存ブロックの Gas がインセンティブとして，Ethereum の通貨である ETH で支給される．現在は PoW でブロックチェーンが管理されているが，次期大型アップデートで PoS (proof of stake) と呼ばれるアルゴリズムに変更されることが予定されている．またブロック生成時間が 15 秒と早い特徴がある．

本研究では Ethereum を用いたブロックチェーン上に信用スコアシステムを構築し，一企業が一個人の信用スコアを決めるのではなく，一個人の信用スコアを不特定多数の人が評価することが可能な仕組みを提案する．提案方式を用いることで，企業に依存することなく信用スコアを評価することが可能である．本稿の貢献は以下にまとめられる．

- Ethereum を用いて個人信用スコアを評価し提供するシステムを提案し，そのビジネスモデルやスマートコントラクト，ステークホルダー間のデータと貨幣の流れを示す．
- 実験室環境で構築した Ethereum 上に提案システムを実装し，動作検証を行った結果を示す．

以下，2 節で関連研究について述べ，3 節で提案方式の詳細について説明した後，4 節で実機システムを用いた性能評価を示し，最後に 5 節で全体をまとめる．

2. 関 連 研 究

ブロックチェーンを初めて使用し通貨の取引を可能にしたシステムとして Bitcoin がある [2]．Bitcoin は 2008 年に Satoshi Nakamoto によって提案されたシステムで 2009 年に Genesis ブロックと呼ばれる最初のブロックが記録されてから現在まで一度も止まることなく動作しているシステムである．また Bitcoin ではプログラムとして 80Byte しかデータを入れるスペースがないため，通貨のやり取り以外あまり汎用性がない．そこで通貨の取引以外にスマートコントラクトをブロックチェーンに格納しようとして生まれたブロックチェーンとして Ethereum [4] がある．

Ethereum を応用した様々な研究が見られるが，例えば IoT デバイスを Ethereum を用いて管理する方法が提案されている [3]．使用するユーザや端末である SAMC，使用するデバイスである OAMC，SAMC が OAMC をどのように使用するかの情報である PMC，SAMC や OAMC と PMC をつなぐための情報である ACC，の 4 種類のスマートコントラクトを作成し，IoT デバイスを管理する [3]．

また文献 [5] では Ethereum を使用し，ブロックチェーン上で電子投票を行うことが可能であることが述べられている．これは選挙を管理する中央機関がなくなることで投票する票を操作されることがなくなり，投票者が地理的にどこにいても投票することが可能になると言う 2 つの点が Ethereum を使用する利点と位置付けている．

さらに文献 [7] はブロックチェーンを用いた分散交通システムを提案している．分散交通システムとは道路の交差点から交差点までをセグメントとし，その道路の脇にビーコンと呼ばれる IoT 機器を配置し車が通るたびに車のデータをブロックチェーンに記録し，車の通行量を管理する．またブロックチェーンに記録されたデータから事故の発生などで通行不能箇所が発生したときはブロックチェーンが分離し，通行可能になるとブロックチェーンが合併するシステムである．

3. 提 案 方 式

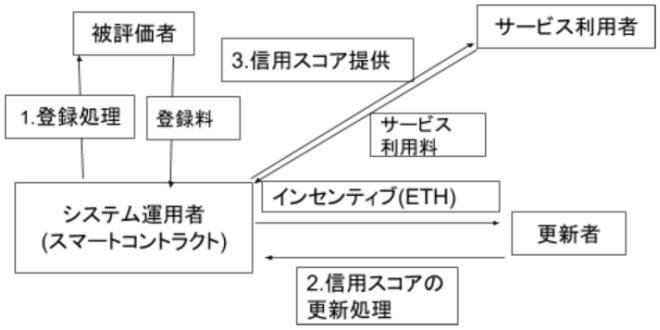

図 1　個人信用スコアシステム

本稿では Ethereum を用いた個人信用スコア提供システムを提案する．提案システムは，1．システム登録，2．信用スコア評価，3．信用スコア提供，の 3 つの機能から構成される．1 のシステム登録機能は，ユーザが初めて信用スコアシステムを使用する際にユーザを登録する機能であり，被評価者がシステム運用者に登録料を払いユーザ登録を行う．2 の信用スコア評価機能は 1 を行った任意のユーザが，他の任意の登録ユーザの評価を行う機能である．信用スコアを評価する人の信用スコアと，新たに申告された評価値によって，被評価者の信用スコアを更新する．評価したユーザには評価を行ったインセンティブとして暗号通貨を受け取る．3 の信用スコア提供機能は，システム登録の有無とは無関係に，どのユーザでも可能であり，1 を行ったユーザの現在の信用スコアを活用したいユーザが使用料を支払うことでユーザの信用スコアを取得可能とする．この時 gas と使用料を支払うが，後述するように使用料より Gas 料が圧倒的に少ない．

提案システムにおけるステークホルダ間の動作を図 1 に示す．

提案システムの 3 つの機能を実行するためには，あらかじめスマートコントラクトとしてブロックチェーンに書き込む必要があるが，これは提案システムを構築する主体が行うことを想定する．ただしスマートコントラクトの設定が完了し，システムが稼働を開始した後は，提案システムの構築者はシステムに関与しない．またユーザの識別は ETH のアドレスで行う．1，2，3 の 3 つの各機能を利用する際には，Gas と呼ばれる Ethereum を利用するための手数料が発生する．次に 3 つの各機能の動作の流れを説明する．

3.1 システム登録

システム登録においては，登録希望ユーザからブロックチェーンのシステム運用者（以後，単にシステム運用者と表記）に対して ETH アドレスが通知され，アカウントを作成したことがあるかの有無を確認し，無い場合は信用スコアが初期値に設定される．そして登録ユーザはシステム運用者に登録料を払う．図 2 にシステム登録のスマートコントラクトのコードを示す．

```
function make_account() public payable {
  require(personal_score_management[msg.sender] == 0);
  personal_score_management[msg.sender] = 100;
  amount += msg.value;
}
```

図 2　システム登録のスマートコントラクトのコード

3.2 信用スコア評価

登録ユーザは他の任意のユーザの信用スコアを評価値をシステム運用者に通知することで更新することが可能である．信用スコアの更新式としては様々なものが考えられるが，更新するユーザ i の信用スコアを R_i，被更新ユーザ j の信用スコアを R_j，ユーザ i がユーザ j に対して時刻 t でつけた評価値を $S_{ij}(t)$ で定義し，ここでは信用スコアの更新式を次式で与える．

$$R_j(t) = R_j(t-1) + (1 + R_i(t)/1000)S_{ij}(t) \qquad (1)$$

信用スコアが高いユーザからの評価ほど，より強く信用スコアの更新値に評価値が反映される．また，意図的に他のユーザの信用スコアを操作することがないよう，30 日といった一定の期間以内に同一ユーザから同一ユーザに対する信用スコアの更新が複数回あった場合は，更新を受け付けない処理を行う．信用スコア評価のスマートコントラクトのコードを図 3 に示す．ここでは例として，評価値は 1〜6 の値で入力されること，信用スコアは 1〜1,000 の範囲の値をとることを想定する．入力値 person_score から式 (1) によって被評価者の信用スコアが更新される．

3.3 信用スコア提供

任意のユーザは提案システムに登録している任意のユーザの信用スコアを参照することが可能である．図 4 に，信用スコア提供のスマートコントラクトのコードを示す．入力値は信頼度を取得したいユーザのアドレスであり，アカウントが存在するかを確認し，サービス利用者は利用料を支払うことで，信用スコアを受け取る．

3.4 通貨の流れ

ここでは 3 つの各機能を実施したときの，各ステークホルダ間の通貨の流れを整理する．1．システム登録の際は，登録ユーザはシステム運用者に登録料を支払う．また 2．信用スコア評価の際は，システム運用者から評価者に対してインセンティブが支払われる．さらに 3．信用スコア提供の際は，信用スコア参照者からシステム運用者にサービス利用料が支払われる．またこれらに加え，1 の動作の際は被登録者から，2 の動作の際は評価ユーザから，3 の動作の際は個人信用スコアの利用者から，各々，ブロックチェーンのシステム運用者（マイナー）へ Gas が支払われる．表 1 に各機能におけるステークホルダ間の通貨の流れをまとめる．

```
function evaluation (address person, int8 person_score)
private {
   require( 0 < person_score && person_score < 7);

   int calc;
   int x;

   psc[1] = -10; psc[2] = -3; psc[3] = -1;
   psc[4] = 1; psc[5] = 3; psc[6] = 10;

    calc = int(personal_score_management[person]) +
    psc[person_score] +(psc[person_score] *
    int(personal_score_management[msg.sender]) /
    1000);

    if(calc > 0 && calc < 1000) {
    personal_score_management[person] = uint(calc);
    } else if(calc > 1000) {
         personal_score_management[person] = 1000;
    } else { personal_score_management[person] = 1;
    }
}
```

図 3　信用スコア評価のスマートコントラクトのコード

```
function consultion(address person) public returns
 (uint) {
  require(personal_score_management[person] != 0);

  amount += msg.value;

  return personal_score_management[person];
}
```

図 4　信用スコア提供のスマートコントラクトのコード

表 1　個人信用スコアシステムの通貨の流れ

	支払者	受益者
1. システム登録	被評価者	システム運用者
2. 信用スコア評価	更新者，システム運用者	システム運用者，更新者
3. 信用スコア提供	サービス利用者	システム運用者

3.5 ビジネスモデル

提案システムは，サービス利用者とシステム登録者の支払い料金を原資として，更新者にインセンティブを払うビジネスモデルである．サービス使用料を p，更新者に支払うインセンティブを q，更新者から受ける更新処理の発生頻度を r(回/秒)，サービス利用者数を N，サービス利用者 1 人あたりのサービス利用頻度を x(回/秒)，更新者数を M とすると，システム登録料を無視した場合にビジネスとして本システムが成立する条件は $Npx > Mqr$ となる．例えば $p = 50$，$x = 0.001$，$M = 10,000$，$q = 50$，$r = 0.003$ とすると，$N > 30,000$ であれば本条件が成立する．

4. 性能評価

実験室環境でプライベートチェーンによる Ethereum を実装し，提案システムの動作の検証を行った．評価では Ubuntu18.04 のメモリ 16GB，Corei3 × 4 の PC を 1 台使用し，Miner と使用者の動作を同時に行った．また Ethereum でスマートコントラクトを作成するための言語は Solidity であり，動作のシミュレーションは Javascript で作成した．Ethereum のプライベートチェーン上にスマートコントラクトを作成し，ユーザ 10 人を作成し，ランダムなユーザがランダムなユーザの信用スコアを評価し，式 (1) の信用スコアの更新式を用いた時の信用スコアの推移を検証した．ユーザが入力する値は 1〜6 の 6 種類とし，信頼できる順に降順にスコアをつける．信用スコアの値は 1〜1,000 までとし，初期値を 100 とした．また各ユーザに対し真の信用スコアを 1 から 1,000 の範囲の一様分布でランダムに設定した．

評価ユーザ i は，被評価ユーザ j の真の信用スコア $\hat{R}_j$ と現在の信用スコア R_j によって信用スコアを設定した．すなわち評価値 $S_{ij}(t)$ を，$R_j < \hat{R}_j - 100$ のとき -10，$\hat{R}_j - 100 \leqq R_j < \hat{R}_j - 20$ のとき -3，$\hat{R}_j - 20 \leqq R_j < \hat{R}_j$ のとき -1，$\hat{R}_j \leqq R_j < \hat{R}_j + 20$ のとき 1，$\hat{R}_j + 20 \leqq R_j < \hat{R}_j + 100$ のとき 3，$R_j \geqq \hat{R}_j + 100$ のとき 10 に設定した．

ある 1 人のユーザの真の信用スコアを 1,000 回，2,000 回評価時点で各々，800 と 300 に変化させたときの，このユーザの真の信用スコアと評価スコアの時系列を図 5 に示す．真の信用スコアが変化しても評価信用スコアが真の信用スコアに漸近している様子が確認できる．

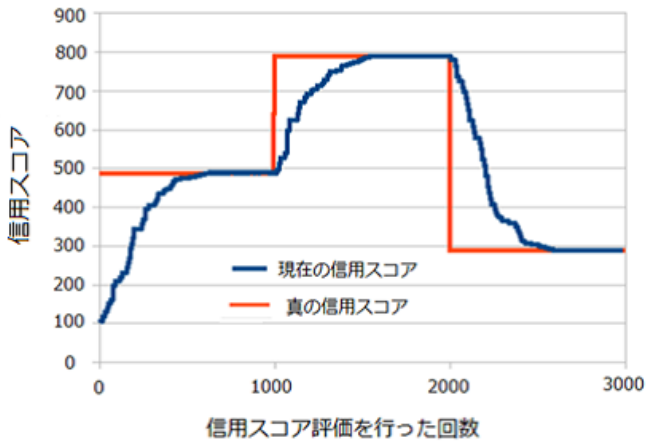

図 5　サンプルユーザの真/評価信用スコアの時系列

CPU の 1 コアでマイニングの動作をさせ，ある程度 Difficulty が安定したブロックを始まりとして，任意のユーザが，他の任意のユーザを評価する動作を 1Step とし，1 つのシミュレーションにつき 100Step 動作させた．このようなシミュレーションを行うプロセスを複数，並列処理で動作させた時の 1 秒あたりに処理できたトランザクション数を並列プロセス数に対し，図 6 にプロットする．並列実行数が増加するほど，1 秒間あたりに処理可能なトランザクション数が増加しているが，70 程度まで並列に動作させたところで，それ以上，並列動作数を増やしてもスループットは増加しなくなった．そのため今回，実験に用いた環境においては，1 秒間あたり 10 程度のトランザクションが処理可能であることが確認できた．

1．2．3．の各機能を実際に動作させた時に支払われた Gas 量と，令和元年 12 月 11 日現在のレートに基づき価格に換算し

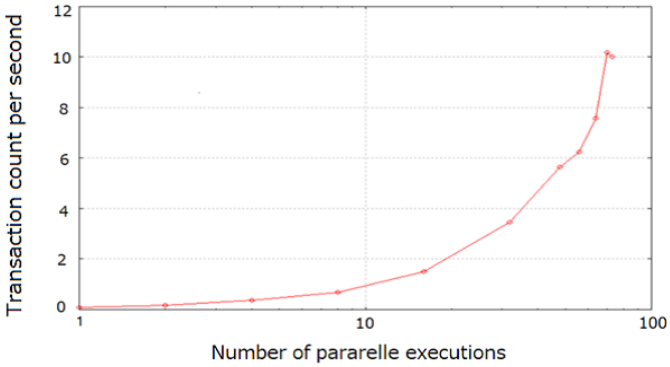

図 6　並列実行数あたりの TPS(1 秒あたりのトランザクションの処理数)

た値を表 2 に示す．2 の信用スコア評価の動作の Gas 料金は 6.53 円なので，この額を超えたインセンティブを与える必要がある．

表 2　Gas 量と価格

スマートコントラクトの動作	Gas 量	価格
デプロイ	696498 gas	141 円
登録	52193 gas	10.57 円
信用スコアを評価	32248 gas	6.53 円
信用スコア提供	42291 gas	8.57 円

5. まとめ

本稿では Ethereum 上にスマートコントラクトとして信用スコアシステムを構築することと，そのビジネスモデルを提案した．実験室環境における実機を用いた提案方式の動作検証を行い，真の信用スコアが変化しても，変化に追随して信用スコアが推定できること，また 1 秒あたり 10 個程度のトランザクション処理が可能であることを明らかにした．今後の課題として，セキュリティの強化，ユーザの評価値設定モデルの検証，より現実に即した環境での実験に取り組む予定である．また Ethereum のコンセンサスアルゴリズムが現在の PoW から PoS に変更が予定されているため変更後の評価も行いたい．

謝辞　本研究成果は，SCAT 研究費助成 180047 の援助を受けたものである．ここに記して謝意を表す．

文　献

[1] 大屋　雄裕，“個人信用スコアの社会的意義”，総務省学術雑誌『情報通信政策研究』第 2 巻第 2 号

[2] “Bitcoin:A Peer-to-Peer Electronic Cash System” available at https://bitcoin.org/bitcoin.pdf

[3] G. Sagirlar, et al., Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains, IEEE Blockchain 2018

[4] “A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM” available at http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[5] 豊 美玲, 張 元玉, 笹部 昌弘, 笠原 正治 ”IoT のための柔軟な分散型属性ベース・アクセス制御の実現” NS2018-251

[6] E. Yavusz et. al., ”Towards secure e-voting using ethereum blockchain”2018,2018 6th International Symposium on Digital Forensic and Security (ISDFS) https://ieeexplore.ieee.org/abstract/document/8355340/citations#citations

[7] 藤原 明広 ”ブロックチェーン技術を用いた分散型交通情報システムの提案” IN2017-138