学習ログとブロックチェーンによる多角的なプログラミング・スキルの証明書

富岡 真由[1,a)]　秋信 有花[2]　倉光 君郎[1,b)]

概要：オンラインジャッジは，もともと競技プログラミングの自動審判システムとして開発されてきた．一方，オンラインジャッジは教育システムとしても優れており，近年ではプログラミングの自習用，また大学等のプログラミング演習の教材として利用されるケースも増えている．
我々は，オンラインジャッジの学習ログからプログラミングスキルや他の能力を証明する仕組み作りを目指している．本稿では，ブロックチェーン技術を用いて，独立のオンラインジャッジに格納された学習ログに対し，スマートコントラクトで証明書を記述する新しいアーキテクチャを提案する．ブロックチェーン技術を用いることで，様々な観点から証明書を発行することが可能になり，その証明書の信頼性が担保されることを目指す．

1. はじめに

オンラインジャッジ [1] は，もともと競技プログラミングの自動審判システムとして開発されてきた．豊富な過去問アーカイブや提出プログラムの自動採点，優れた回答例の供給，学習歴の記録など，教育システムとしても優れているため，近年ではプログラミングの自習用にも利用されている．加えて，大学等のプログラミング演習としてオンラインジャッジを使うケースも増えている．

さらに，昨今のプログラミングの重要性の高まりもあり，企業側は採用時にプログラミング能力を基本スキルのひとつとして評価することが増えている．

しかしオンラインジャッジも，学習の達成度の評価という点では問題が残る．オンラインジャッジは，競技プログラミングの競技者の力量を示す観点からレーティングと呼ばれるスコアを出しているが，レーティングは動的計画法などの難度の高いアルゴリズムが解く能力の指標であり，プログラミングの一般的な力量を示すものとは異なる．またオンラインジャッジは，学生時代のプログラミング学習の記録が残されており，単純にスキルだけでなく，努力量やチャレンジ力など，様々な観点からの人物評価のデータが含まれている．

我々は，オンラインジャッジの学習ログから多様な評価観点にあわせ，プログラミングスキルや他の能力を証明する仕組み作りを目指している．

本研究では，ブロックチェーン技術を用いて，独立のオンラインジャッジに格納された学習ログに対し，スマートコントラクトで証明書を記述する新しいアーキテクチャを提案する．ブロックチェーン技術を用いることで，様々な観点から証明書を発行することが可能になり，その証明書の信頼性が担保されることを目指す．

本稿の残りの構成は以下の通りである．2 節では，想定シナリオを示す．3 節では，使用する技術について簡単に説明する．4 節では，提案システムである ManabiCert システムを紹介する．5 節では，本論文を総括し展望をまとめる．

2. 想定シナリオ

まず，我々のゴールを理解するため，典型的なシナリオを示してみたい．登場するアクターは，以下の通りである．

- オンラインジャッジでプログラミングを学んだ学生
- 最低限のプログラミングスキルを持った学生を採用したい企業

2.1 学生サイド

まず，日本女子大学理学部数物科学科の標準的な学生像から，学生側の立場でシナリオを示してみたい．

[1] 日本女子大学理学部数物科学科
Department of Mathematical and Physical Sciences, Japan Women's University, 2-8-1 Mejirodai, Bunkyo-ku, Tokyo 112–8681, Japan
[2] 日本女子大学大学院理学研究科数理・物性構造科学専攻
Graduate School of Science Division of Mathematical and Physical Sciences, Japan Women's University, 2-8-1 Mejirodai, Bunkyo-ku, Tokyo 112–8681, Japan
[a)] m1716065tm@ug.jwu.ac.jp
[b)] kuramitsuk@fc.jwu.ac.jp

List of solved problems

#	Problem ID	Date	Language	CPU	Code Size	#
1	0025	2020/08/18	Python3	0:02	323	4769824
2	1042	2020/08/09	Python3	0:02	228	4749776
3	NTL_1_B	2020/06/29	Python3	0:02	68	4626430
4	ALDS1_10_A	2020/06/16	Python3	0:02	127	4583001
5	0007	2020/06/15	Python3	0:02	119	4580811
6	ITP1_7_D	2020/06/15	Python3	0:83	753	4580224
7	1200	2020/06/08	Python3	0:19	501	4559467
8	ITP1_3_B	2020/05/15	Python3	0:15	109	4473339
9	0315	2020/05/14	Python3	0:02	47	4471070
10	0296	2019/08/03	C++	0:00	347	3789096
11	ITP1_7_C	2019/06/25	C++14	0:00	774	3685114
12	0511	2019/06/25	C++14	0:00	317	3684763
13	ITP1_6_C	2019/06/18	C++14	0:00	499	3663479
14	ITP1_8_A	2019/06/11	C++14	0:00	413	3643312
15	0029	2019/06/03	Python3	0:02	68	3622887
16	ITP1_6_B	2019/06/03	Python3	0:02	229	3621010
17	0173	2019/05/28	C++14	0:00	226	3604854
18	0195	2019/05/28	C++14	0:00	406	3604812
19	0219	2019/05/28	C++14	0:00	552	3604767
20	0218	2019/05/28	C++14	0:00	776	3604717

Page 1 of 6 20 View 1 - 20 of 109

図 1 オンラインジャッジの学習ログの例

- ２年次前期，オンラインジャッジを採用したプログラミング演習を履修する
- ２年次後期，プログラミングに関心をもち，授業外でも時々オンラインジャッジの問題に取り組む
- ３年次前期，友達に誘われて ACM ICPC に挑戦してみる．オンラインジャッジで練習するが，残念ながら予選落ち
- ３年次後期から４年次，IT 開発会社に興味をもって，就職活動を行う

ACM ICPC は，大学対抗のプログラミング競技会で，予選を通過してアジア大会に進めるのは全国で 100 人程度，原則，各大学の上位 3 人である．だから，ACM ICPC の予選通過は，高いプログラミング能力の指標となる．しかし，ACM ICPC の予選は通過しなかったとしても，プログラミングを学習してきた事実とその結果のスキルを評価してもらいたいと考えるのは当然である．

2.2 企業サイド

企業側は，学生を採用する立場で考えると

- プログラミング力は，ICPC 予選を通過したかどうかで測るしかない
- ICPC 予選参加は，学生のチャレンジ力の指標になるかもしれないが，基本，誰でも参加できるコンテストで予選の成績はわからない
- 結局，ほとんどの学生のプログラミングスキルはよくわからない

企業は，プログラミングスキルを測るため，GitHub ポートフォリオや独自のスキルテスト，ホワイトボードコーディング，コーディング経験を面接でなんとなく聞くに頼らざるを得ない．

読者は，オンラインジャッジに２年間の学習ログが記録されているのに，どうして活用しないのだろうかと疑問に感じるだろう．

2.3 学習ログと証明書

最後に，我々の提案する学習ログを活用するシナリオを述べる．

まず，学習ログとスキルに関する基準を定める．学生と企業が定められた基準に関して合意したとき，

- 学生は合意した基準を目標にオンラインジャッジに取り組み，基準に達したとき証明書が発行される
- 企業は学生のスキルの証明書を受け取る

この追加シナリオでは，スキル基準を定めるものが新たに登場する．スキルの基準を定めるものは，企業でも大学であっても，完全に第三者であっても構わない．むしろ，誰でも基準を定められるようにすることが，スキル評価の多様性に繋がる．

まとめると，以下のような性質を実現するシステムが必要となる．

- スキル基準は，明確かつ公平な形式で記述されており，人手によらず判定できるようにアルゴリズム化されているのが望ましい
- スキル基準や発行される証明書は，偽造不可能で十分に信頼されるものでなければならない

3. ブロックチェーン技術

我々は前述のシナリオを実現するために，ブロックチェーンとスマートコントラクトを使用する．本節では二つの技術について簡単に説明する．

3.1 ブロックチェーン

ブロックチェーンは，暗号通貨などに代表されるデジタル資産の取引データを複数の利用者や管理者にまたがって共有する分散システムである．特徴は以下の 3 点に集約される．

- 改ざんへの耐性が強い
- 非中央集権型
- 障害や攻撃に強い

3.2 スマートコントラクト

スマートコントラクトは，あらかじめ記述されたコントラクトに従って，ブロックチェーン上で自動的に実行されるプログラムのことである．スマートコントラクトを導入することによって，送金などの単純な暗号資産の取引だけでなく，複雑な取引が実現できるようになる．

しかし，スマートコントラクトは一つの大きな制約がある．それは，外部の情報に基づいたコントラクトを記述できないという点である．これは，ブロックチェーン上の世界から，外部の世界へ直接アクセスすることができないためである．外部の情報を参照したコントラクトが記述できないと，コントラクトの利用範囲が限られてしまう．

そこで近年注目を集めるのは，オラクル (Oracle) サー

```
contract example1 {
  string public id = 'sumire';
  string public name = 'Mejiro Hanako';
  uint public grade;

  /*オラクルサービスを呼び出すためのイベントの定義*/
  event Set(address from, string usr_name);

  function aojcheck(string _name) public returns(string
      ){
    emit Set(msg.sender, _name);
    return id;
  }

  /*オラクルサービスを経由して得られたスコアに基づいた判定*/
  function aojchecked(uint _score) public {
    if (_score >= 20) {
      grade = 1;
    }
    else {
      grade = 0;
    }
  }

  function getgrade() public constant returns (uint) {
    return grade;
  }
}
```

図 2 スマートコントラクトの例

ビス [2] である．オラクルサービスは，スマートコントラクトに外部の情報を提供するサードパーティ製のサービスのことである．オラクルサービスは，ブロックチェーンの世界と外部の世界の間でデータの橋渡しをしてくれる．このサービスによってスマートコントラクトを利用できる範囲が広がることが期待される．

4. ManabiCert システム

我々は，2 節で述べたシナリオを実現する ManabiCert システムを提案する．ManabiCert システムは，ブロックチェーン技術を採用したアーキテクチャとなっている．

4.1 証明書

ManabiCert システムは，スキル証明書をブロックチェーン上のスマートコントラクトで実現する．スキル基準は，図 2 に示す通り，Solidity などのプログラミング言語で記述され，オラクルサービスを用いることで，オンラインジャッジの結果を参照してスキルの判定をすることができる．なお，スマートコントラクト内に一度記述された値は改ざんが不可能であるため，スコア基準の明確さや公平性が保護されるようになる．

4.2 外部サービスとの連携

ManabiCert システムの特徴は，外部サービスであるオンラインジャッジを用いることである．学習ログをすべてブロックチーン上で管理する代わりに，ブロックチェーンのオラクル (Oracle) サービスの仕組みを用い，外部サービスとのセキュアな連携を行うことにする．

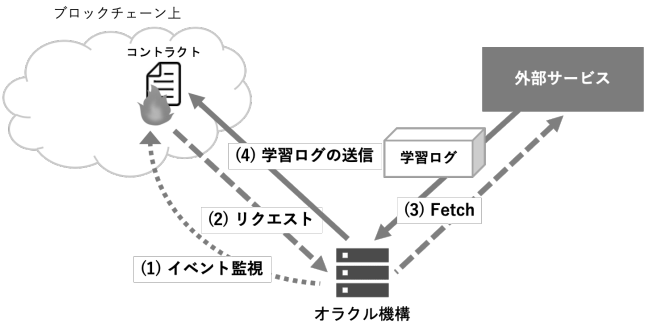

図 3 学習ログの取得

図 3 は，ManabiCert システムがオラクルサービスを用いて，コントラクトが外部サービスから学習ログを受け取るまでのフローを示したものである．それぞれのフローの詳細は以下の通りである．

(1) 常にコントラクト内のイベントを監視させておく
(2) イベント発生を検知したら，学習ログの取得をオラクル機構に要求する
(3) オラクル機構は指定された外部サイトから，学習ログを取得してくる
(4) オラクル機構からコントラクトに学習ログを送信する

このように，ManabiCert システムでは，ブロックチェーン技術を活用することで，様々な性質の実現を目指している．

5. むすびに

本稿では，ブロックチェーン技術を用いて，独立のオンラインジャッジに格納された学習ログに対し，スマートコントラクトで証明書を記述する新しいアーキテクチャを提案した．今後は，ManabiCert システムのプロトタイプの開発を進め，実用性の評価をしていく予定である．

謝辞 本研究は，第二著者がセコム株式会社 IS 研究所のインターンシップで学んだオラクルサービスの実装に基づいている．熱心にご指導いただいたセコム株式会社 IS 研究所の松本泰氏，佐藤雅史氏，長谷川佳祐氏に感謝いたします．

参考文献

[1] 渡部有隆：オンラインジャッジの開発と運用 -Aizu Online Judge-，情報処理，Vol. 56, No. 10, pp. 998–1005 (2015).
[2] Steve, E., Juels † Ari, Sergey, N.：ChainLink: A Decentralized Oracle Network (2017).