2ZA-02

ブロックチェーンによる分散型タイムスタンプとその折り紙著作権保護への応用

高　月菲[†]　　張　丘平[†]　　延原　肇[†]

所　属[†]　　筑波大学 システム情報工学研究科

現行の著作権登録制度は 1) 手続きが煩雑、2) 申請完了までの時間が長い、3) 費用が高いため、大量の電子データを取り扱うサービスにおける著作権保護には適用困難である。この問題を解決するため、ブロックチェーン技術を利用した分散型タイムスタンプサービスを提案する、提案する分散型タイムスタンプは手軽・安全・安価・即時というメリットがある。提案手法では、電子データの関連情報をアドレスとしてブロックチェーンに格納させることで、最大 40 バイトしか格納できなかった点を解消している。提案手法の有効性を確認するための評価実験として、折紙の折り図の著作権保護支援へ適用し、提案手法による申請は 0.4 円というコスト及び申請完了まで平均 10 分で完了という結果を得た。

キーワード：ブロックチェーン、分散型タイムスタンプ、折り図、著作権保護支援

1. はじめに

電子データの改ざんと偽造は痕跡を残さずに比較的容易にできるため、著作権侵害の問題が発生しやすい。それに対して、文化庁による著作権登録制度があるが、現行の制度は、1) 手続きが煩雑、2) 時間が長い、3) 費用が高い、といった問題点がある。一つの解決策は第三者機関であるタイムスタンプ認証局、時刻認証局などにより発行され、電子データの存在性と非改ざん性を証明する信頼できるタイムスタンプ(Trusted Timestamping)という技術がある。しかし、タイムスタンプ認証局のサーバへのハッキングにより時刻が改ざんされた場合、安全性と信頼性の問題が発生する。この問題点に対して、P2P 電子通貨ビットコインのインフラ「ブロックチェーン（Blockchain）」による信頼できるタイムスタンプサービスが登場している[2]。しかし、現存サービスの手法 Proof of Existence[1]は最大 40 バイトのデータしか格納できない。

本研究では手軽・安全・安価・即時な分散型タイムスタンプに加えて、格納できるデータ量を増加させる手法を提案する。ここでは、電子データの要約および関連情報をビットコインの N 個アドレスに変換し、この N 個アドレスに小さい金額を送金する。取引がブロックチェーンに記録される時点はタイムスタンプとする。提案手法により、最大 N*40 バイトの 電子データを格納するができる。

提案手法を折り図（折り紙の手順を表す図）の著作権保護支援に応用し、N を 3 に設定し、評価実験を行う。提案手法による取引がブロックチェーンに格納されたことにより、提案手法は有効であることが証明できる。さらに、提案手法を実現するため必要な費用と平均時間を評価する。

2. 関連研究

ビットコインは P2P の暗号化電子通貨であり（Nakamoto，2009）、第三者機関に依存せず、分散的に存在する。ビットコインの全て承認済みの取引がブロックチェーンに記録されている。ブロックチェーンは第三者機関に依存せず、ビットコインの約 500 万人の利用者によって共有され、新しいデータを書き込む際、複数の利用者の合意が必要である。このような仕組みにより、ブロックチェーンの記録の改ざんと偽造はほぼ不可能である。ブロックチェーンには約 40 万のブロックがあり、１つのブロックには主に含まれている情報は：１）前のブロックのハッシュ値；２）タイムスタンプ；３）乱数；４）約 500 個承認済みの取引情報である。

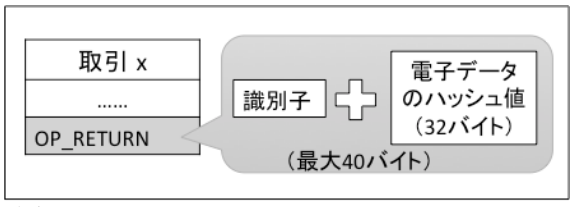


図 1　Proof of Existence によるタイムスタンプ

現存サービスの１つ Proof of Existence[1]はビットコインのスクリプト言語 data output (OP_RETURN)というスクリプトを利用する。入力した電子データの 32 バイトのハッシュ値を識別子「DOCPROOF」の後につけ、それを OP_RETURN にエンコードする手法である（図１）。しかし、この手法は最大 40 バイトのデータしか格納できない。

3. 提案手法

電子データのハッシュ値以外の情報もブロックチェーンに格納させるため、OP_RETURN を利用せず、電子データのハッシュ値及び関連情報（作品名、作者名など）を N 個のビットコインのアドレスに変換し、この N 個のアドレスに小さい金額を送金する取引をブロックチェーンに格納する手法を提案する。図２は提案手法の中心を示す。

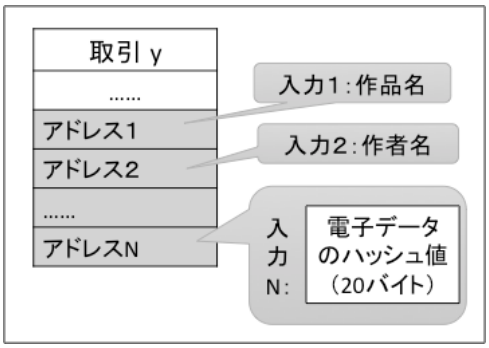


図 2　提案手法の概要

ステップ１：ユーザーはウェブ画面で N 個の情報を入力する。例えば、入力１：電子データとの名前；入力２：作者の名前；…入力 N：作品の電子ファイル。

ステップ２：第 1 から N-1 の入力は 16 進数に変換し、第 N 個の入力のハッシュ値をハッシュ関数 RIPEMD-160 で計算する。

ステップ３：Base58 というエンコード手法で第１から N 個の入力を N 個のビットコインのアドレスに変換する。

ステップ４：N 個のアドレスに小さい金額を送金し、特殊な取引をビットコインのネットワークにブロードキャストする。この取引がブロックチェーンに記録された時点は分散型タイムスタンプとする。これで、40*N バイトの電子データのハッシュ値、関連情報（作品名、作者名など）がブロックチェーンに格納された。

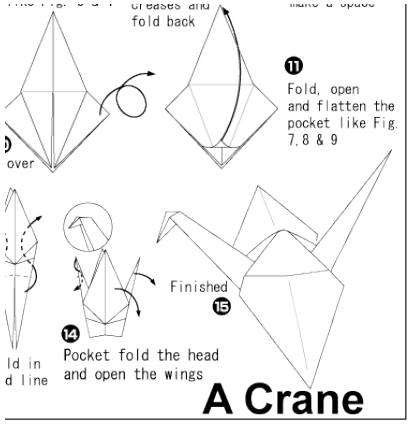
ステップ５：取引検索用の ID が出力とする。

記録時点以後、この電子データの存在性と非改ざん性を検証することができる。４章は評価実験で提案手法の時間と費用を評価する。

4. 評価実験

折り図とは、折り紙の手順を表す図である（図３）。折り図は創作者の知的財産、守るべきだと考えられる。本実験では、折り紙の折り図の著作権保護を対象とし、N＝３に設定する。

ユーザーは３つの情報を入力する。入力 1 は折り図の名前と作者の名前、入力 2 は関連情報（ウェブサイト、利用許可など）、入力 3 は折り図の電子ファイル（本研究では鶴の折り図 1 枚の png ファイルを利用する）。



入力 1 と 2 の情報は十六進数に変換した後、入力 3 の折り紙のファイルをハッシュした後、Base58 というエンコード手法で 3 つビットコインのアドレスに変換する。このアドレスに小さい金額を送金する取引をブロードキャストし、ブロックチェーンに記録した時点をタイムスタンプとする。

実験１：費用の評価実験

５つ費用が異なる折紙取引を生成し、それらをブロードキャストした後、ブロックチェーンに格納状況を記録する。結果は表１に示す。結果から、費用が低すぎる場合ブロックチェーンに記録することができない可能性があることがわかる。

表 1　費用の実験結果（BTC：ビットコイン JPY：円）

費用	BTC	$1x10^{-3}$	$1x10^{-4}$	$5x10^{-5}$	$1x10^{-5}$	$5x10^{-6}$
	JPY	38.92	3.89	1.95	0.39	0.19
格納結果		成功				失敗

実験２：時間の評価実験

実験１で成功した４つの費用に基づき、４組（合計 16 回）の実験を行った。ブロードキャスト時点から記録時点までの時間を記録する。提案手法の分散型タイムスタンプは平均 10 分で完了していることがわかる。

5. まとめ

従来電子データの著作権登録制度の 3 つの問題点と現存タイムスタンプサービスの 40 バイトの格納データの制限に対して、本研究では手軽・安全・安価・即時な分散型タイムスタンプを実現し、それを折紙創作の折り図の著作権保護支援に応用した。

参考文献

[1] *Proof of Existence.* Retrieved from http://www.proofofexistence.com/

[2] Nakamoto, S. 2009. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf