# スマートコントラクトを活用した 電子書籍の分散型流通システムの設計と試作

広島大学 情報科学部 情報科学科 B184362 尾形 啓悟

## 1 はじめに

電子書籍は国内でも広く利用されているが、購入した書籍は基本的に電子書籍ストアの管理下にあり、サービス終了やアカウント停止などで購入した書籍を失う可能性が存在する。また、基本的にはクライアントサーバ方式が採用されており、単一障害点やハッキングへの弱さがある。そこで、ブロックチェーン上で動作するスマートコントラクトを活用した非中央集権的で分散型の新しい流通システムを設計、試作を行った。

## 2 既存研究

Jeonghee Chi らの研究では、B_Chain と C_Chain の 2 つのブロックチェーンでそれぞれ電子書籍情報と電子書籍購入のトランザクションを管理する安全で信頼性の高い電子書籍取引システムが提案されている [1]。また、株式会社 Gaudiy とコミックスマート株式会社との共同プロジェクトでは、パブリックブロックチェーンを利用した自立分散型の流通システムを構築、提供するとしている [2]。しかし、これらの研究では依然として電子書籍データの配信はデータサーバに依存しているため、サーバが停止したり、サーバの所有者がその運用をやめた時にシステムが機能しなくなってしまう問題を孕んでいる。

## 3 ブロックチェーン

Bitcoin などで知られるブロックチェーンとは、暗号技術を用いて情報が格納されたブロックをチェーンのようにつなげていくデータベースである。特に P2P ネットワーク上で誰でも参加ができるものはパブリックブロックチェーンと呼ばれ、大きな特徴として改竄耐性、ゼロダウンタイム、透明性が上げられる。

### 3.1 スマートコントラクト

スマートコントラクトとはブロックチェーン上で動作するプログラムである。イーサリアムではイーサリアム仮想マシン (EVM) によりチューリング完全のスマートコントラクトが実行される。スマートコントラクトにより、新規チェーンを作ることなく新しい暗号通貨を作ったり、NFT(非代替性トークン) を作ることができる。

### 3.2 NFT

NFT(非代替性トークン) は唯一性をもち、偽造が不可能なデジタルデータであり、絵や動画、ゲームアイテム、その他様々なデジタルコンテンツに結びつけられ、OpenSea をはじめとする NFT マーケットプレイスなどで取引されている。ただし、そのデジタルコンテンツ自体のコピーや不正利用を防ぐものではないことに注意をする必要がある。ERC721 は EIP721[3] で議論で提案された NFT の標準であり、多くの NFT がこれにしたがって実装されている。

## 4 WebRTC

WebRTC は主要なウェブブラウザやモバイルアプリケーション間でリアルタイム通信をプラグイン無しで行う機能を追加するオープンソースのプロジェクトである。ブラウザ間で P2P 通信を行うことでカメラの映像やマイクの音声、その他任意のデータを仲介なしで送受信することができる。WebRTC で P2P 通信を開始するには SDP(Session Description Protocol) を互いに交換する必要があり、交換にはシグナリングサーバを利用することが一般的である。

### 4.1 dataChannel

WebRTC には標準で DTLS によって暗号された任意のデータを送信できる dataChannel という API が用意されている。dataChannel では UDP 上に SCTP が実装されている。SCTP はメッセージ指向型であり、到達保証や順序保証を切り替えることができる。

## 5 提案手法

提案システムは販売と配信の二つのパートに分かれている。

### 5.1 販売

販売パートでは、ブロックチェーン上に電子書籍の所有権付きの NFT をユーザの暗号通貨と引き換えに鋳造するスマートコントラクトを作成する。スマートコントラクトを通じて作者は作品のハッシュ値と価格の登録を行うことができ、ユーザは NFT を購入することで電子書籍の所有権を得ることができる。

### 5.2 配信

著者は従来のようなサーバによる配信を含め、複数の配信方法を用意することができる。ここでは配信手段の一つとして所有権保有者同士を繋ぐハイブリッド P2P 型ファイル共有システムによる配信を提案する。前提として、所有権保有者同士でのデータ共有は違法アップロード、違法ダウンロードには当たらないものとしている。システムは中央サーバ (ブローカー)、不特定多数のノード (配信者)、中央サーバの用意したスマートコントラクトによって構成される。スマートコントラクトは残りダウンロードリクエスト回数および料金を管理する。残りダウンロード回数はクライアントがダウンロード料、仲介手数料、担保からなる料金を支払うことで増やすことができる。中央サーバはクライアントからのダウンロードリクエストに対し、ノードと

クライアントが所有権を保持していることとクライアントの残りダウンロード回数が 0 でないことを確認したのちに配信を行うノードを手配する。また、手配したノードをスマートコントラクトに記録する。この際にクライアントの残りダウンロード数は 1 減らされる。クライアントはノードからデータを受け取るとそれをハッシュ化して中身を確認し、スマートコントラクト上で手配されたノードを承認する。その際に、ノードと中央サーバにそれぞれダウンロード料と仲介手数料が報酬として、また、クライアントに担保がスマートコントラクトから送金される。このシステムの中央サーバは誰もが自由に立てることができ、仲介手数料やノードの選び方なども自由に設定することができる。また、配信するコンテンツの所有権とコンテンツデータを保持していれば誰でもノードとして参加することができる。

## 6 実装方法

### 6.1 販売

スマートコントラクトを記述できるプログラミング言語 Solidity、イーサリアムで動作するスマートコントラクトの開発を補助するツールである Hardhat を使用してスマートコントラクトを作成し、Mumbai テストネットにデプロイした。コントラクトは OpenZeppelin により公開されている ERC721.sol[1]を継承しており、それを拡張する形で所有権の管理機能を加えた。著者は register 関数を使用して作品の価格、ハッシュ値、また任意でロイヤリティや作品のメタデータを保存した URI などの情報を登録でき、ユーザは mint 関数を設定価格の暗号通貨の支払いを含めながら実行することで所有権付き NFT を鋳造することができる。

### 6.2 配信

React で Web アプリケーションを作成した。ユーザはこれを用いてノードの登録や、データの送信、スマートコントラクトを実行するトランザクションの作成を行うことができる。ユーザは事前に Chrome 拡張機能として提供されている仮想通貨ウォレット Metamask をインストールしている必要がある。また、ノードからクライアントへのデータ送信はブラウザ間で WebRTC　DataChannel を利用する。中央サーバは Node.js によって実装されており、Socket.IO を活用して WebRTC 接続におけるシグナリングの役割も担う。NAT 超えに必要とされる場合がある STUN、TURN サーバは skyway によって提供されているものを使用した。

## 7 評価実験

初めに、リクエストからダウンロードまでの時間を測るため、自宅のネット環境で実験を行った。中央サーバは Heroku に構築した。1MB, 10MB, 100MB, 1GB のデータを作品として登録し、それらを配信するノードを一つ用意した。コンテンツリクエストを送り、受信した内容のハッシュ値を確認するまでの時間を計測した。その結果、1MB では 1.58 秒、10MB では 2.72 秒、100MB では 14.92 秒、1GB では 141.57 秒で完了した。

次に、モバイルワークステーションを活用して ubuntu_server の仮想マシン上に中央サーバをたて、性能実験を行った。仮想マシンにはプロセッサ数を 2、メモリを 2GB 割り当てた。ユーザの増加がレスポンスに与える影響を調べるため、Socket.IO の接続後、クライアントとしての登録を行う仮想ユーザを作成し、秒間クライアント登録数の変化に伴うレスポンスの変化をテストした。その結果、秒間 100 登録数を超えたところからレスポンスに遅れが生じることがわかった (図 1 参照)。

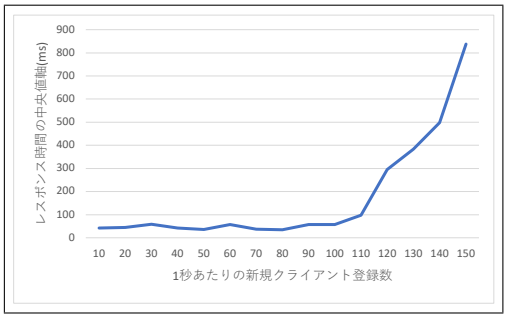


図 1: 秒間クライアント登録数とレスポンス時間の中央値

## 8 終わりに

### 8.1 まとめ

本研究ではスマートコントラクトを活用した電子書籍の非中央集権的で分散型の新しい流通システムの設計を行い、webRTC 等の技術を用いてその試作と評価実験を行った。

### 8.2 今後の課題

販売システムにおいては、実際には作者ではない人が作品を登録するなどの詐欺への対策が課題である。配信システムにおいては、スケーラビリティが問題になることが評価実験により明らかになった。また、ブロックチェーン自体もスケーラビリティを課題としており、高速なチェーンを用いる、できる限りオフチェーンで情報を処理するなどの工夫が必要である。

## 参考文献

[1] Chi J, Lee J, Kim N, Choi J, Park S: “Secure and reliable blockchain-based eBook transaction system for self-published eBook trading.” PLoS ONE 15(2): e0228418. (2020)
https://doi. org/10.1371/journal.pone.0228418

[2] 【プロジェクト#3】NFT × 電子書籍 — 株式会社 Gaudiy
https://hp.gaudiy.com/medias/364

[3] William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs “EIP-721: Non-Fungible Token Standard ” (2018)
https://eips.ethereum.org/EIPS/eip-721

[1]https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC721/ERC721.sol