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

多層ブロックチェーンを用いたNFTオークションアーキテクチャ

呉　俊豪† 　上山　憲昭†† 　宮地　秀至††

† 立命館大学 大学院 情報理工学研究科
〒567-8570 大阪府茨木市岩倉町 2-150
†† 立命館大学 情報理工学部
〒567-8570 大阪府茨木市岩倉町 2-150
E-mail: †gr0694hh@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし　近年，NFT (Non-Fungible Token) の普及に伴い，ブロックチェーン上での NFT オークションがデジタルコンテンツ取引の一形態として広く利用されている．NFT オークションでは，多数の参加者による入札が短時間に繰り返し行われるため，高頻度なトランザクション処理が要求される．しかし，従来の多くのオークションは単一のブロックチェーン上で実行されており，入札回数の増加に伴うガスコストの高騰や，ネットワーク混雑によるトランザクション処理遅延といった課題を抱えている．その結果，参加者の増加に伴ってシステム全体のスケーラビリティが制限され，大規模なオークションの実現が困難となる．本稿では，これらの課題に対して，多層ブロックチェーンを用いた NFT オークションアーキテクチャを提案する．提案手法では，NFT の保管および最終的な決済処理を主チェーン (Layer 1) で行い，入札処理を複数の Layer 2 チェーンおよびサイドチェーン上で並列に実行する構成を採用する．さらに，Relayer が各拡張チェーン上で得られた最高入札結果を収集して主チェーンへ送信し，主チェーン上でそれらを比較して最終的な落札者を確定することで，主チェーンへの負荷軽減を図る．評価では，複数の Layer2 チェーンおよびサイドチェーン環境において提案手法を実装し，従来の単一チェーン型 NFT オークションと比較した数値評価を行った．その結果，提案手法がガスコストおよび処理遅延の低減に寄与し，スケーラビリティを向上させることを示した．
キーワード　ブロックチェーン，NFT オークション，Layer2 チェーン，サイドチェーン,Relayer, スケーラビリティ

A Multi-Layer Blockchain Architecture for NFT Auctions

Junhao WU †, Noriaki KAMIYAMA††, and Hideaki MIYAJI††

† Graduate School of Information Science and Engineering, Ritsumeikan University
2–150, Iwakura-cho, Ibaraki, Osaka 567–8570
†† College of Information Science and Engineering, Ritsumeikan University
2–150, Iwakura-cho, Ibaraki, Osaka 567–8570
E-mail: †gr0694hh@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

Abstract　with the proliferation of Non-Fungible Tokens (NFTs), NFT auctions on the blockchain have become widely used as a form of digital content trading. NFT auctions require high-frequency transaction processing because bids from many participants are repeated in a short period. However, many conventional auctions are executed on a single blockchain, facing challenges such as soaring gas costs due to increased bidding and transaction processing delays caused by network congestion. Consequently, the scalability of the entire system is limited as the number of participants increases, making it difficult to realize large-scale auctions. In this paper, we propose an NFT auction architecture using a multi-layer blockchain to address these issues. The proposed method adopts a configuration where NFT custody and final settlement processing are performed on the main chain (Layer 1), while bidding processing is executed in parallel on multiple Layer 2 chains and sidechains. Furthermore, a Relayer collects the highest bid results obtained on each expansion chain and submits them to the main chain, where they are compared to determine the final winner, thereby reducing the load on the main chain. In the evaluation, we implemented the proposed method in an environment with multiple Layer 2 chains and sidechains and performed a numerical evaluation comparing it with a conventional single-chain NFT auction. The results showed that the proposed method contributes to reducing gas costs and processing delays, thereby improving scalability.
Key words　Blockchain,NFTAuction,Layer2chain,Sidechain,Relayer,,Scalability

1. はじめに

ブロックチェーンは，分散型台帳技術として改ざん耐性や透明性を備えたデータ管理を可能とし，暗号資産をはじめとする様々な分野で利用が進んでいる．近年では，この技術を基盤とした NFT (Non-Fungible Token) が注目を集めており，アート作品やゲームアイテムなどのデジタルコンテンツ取引に広く利用されている [2].

NFT の主要な取引方式の一つとして，スマートコントラクトを用いたオークションシステムがある．これにより，中央管理者を介さずに透明性の高い取引が可能となる．しかし，従来の多くの NFT オークションは単一のブロックチェーン（主チェーン）上で実行されており，入札回数の増加に伴うガスコストの高騰や，ネットワーク混雑によるトランザクション処理遅延といった課題を抱えている．これらの問題は，オークション規模の拡大とともに顕在化し，大規模な NFT オークションの実現を困難にしている [2], [8].

これらの課題に対し，近年では Layer 2 チェーンやサイドチェーンといった拡張技術が提案されている．Layer 2 は主チェーンのセキュリティを前提としつつ処理性能やコストの改善を図り，サイドチェーンは独自の合意形成により特定用途に最適化した処理を可能とする [6], [11]．しかし，NFT オークションにおいて，これら複数の拡張チェーンを同時に利用し，入札処理を分散して実行する構成については，その設計方針や有効性が十分に整理されているとは言い難い．

そこで本稿では，NFT オークションにおけるスケーラビリティとコストの課題を解決するため，多層ブロックチェーンを用いたオークションアーキテクチャを提案する．具体的には，NFT の保管および最終的な決済処理を主チェーンで行い，頻繁に発生する入札処理を複数の Layer 2 チェーンおよびサイドチェーンへ分散して実行する構成を採用する．さらに，オフチェーンの Relayer が各拡張チェーン上の入札結果を監視・収集し，主チェーンへ連携する仕組みを導入することで，主チェーンへのトランザクション集中を回避しつつ，システム全体の整合性と処理効率の向上を図る．

本稿では，提案アーキテクチャの実装および評価を行い，従来の単一チェーン型システムと比較してガスコストおよび実支払額が大幅に削減されることを示す．

2. 関 連 研 究

2.1 ブロックチェーン上のオークションシステム

ブロックチェーン上のオークションシステムは，スマートコントラクトを用いることで，入札，落札判定，および資産移転といった一連の処理を自動的かつ検証可能な形で実行できる．Ethereum を代表とする EVM 系プラットフォームでは，イングリッシュオークションやダッチオークション，第一価格封印入札方式など，従来のオークション形式を分散アプリケーション (dApp) として実装する試みが多くなされている [8]．また，入札の公平性や秘匿性に関する課題に対しては，コミット・リビール (commit-reveal) 方式等を用いて入札内容の即時公開を避ける設計などが提案されている [2], [3].

しかし，従来の多くの方式は単一のブロックチェーン（主チェーン）上で実行されるため，参加者数や入札回数の増加に伴いトランザクション数が増大するという特性を持つ．その結果，ガスコストの増大が利用者負担として顕在化し，ネットワーク混雑による確定までの遅延が発生しやすい．既存研究の多くはオークションプロトコルの改善に主眼を置いており，ブロックチェーン構成そのものを拡張して大規模利用時のコストや遅延を解決する検討は十分ではない．

2.2 マルチレイヤ型ブロックチェーンとスケーラビリティ

ブロックチェーンのスケーラビリティ向上を目的として，主チェーン (Layer 1) を基盤に複数の層を組み合わせるマルチレイヤ型アーキテクチャが検討されている．Layer 2 (L2) は，主チェーンのセキュリティを前提としつつ，トランザクション処理を主チェーン外で実行し，結果のみを反映することでスループット向上やコスト削減を図る技術であり，Optimism や Arbitrum などのロールアップ系ネットワークが代表的である [6], [11]．一方，サイドチェーンは Layer1 チェーンの外と独立して動作し，特定の処理を分担する．

また，異なるチェーン間で資産や状態を連携させるクロスチェーン技術も研究されており，アプリケーションの展開範囲を拡張する基盤となっている．特に Miyaji-Kamiyama らはクロスチェーン間におけるセキュアな通信方式を実現した [5]．しかし，アプリケーションとして NFT オークションを想定した場合，複数の Layer 2 チェーンやサイドチェーンを同時に活用して入札処理を水平分散する構成については，設計上の論点や評価が体系的に整理されているとは言い難い [1]．さらに，Miyaji-Kamiyama らの方式上で NFT オークションを実現できておらず，並列に得られる入札結果をどのように集約し，主チェーンでの最終処理と整合させるかという点は，明確な設計が求められている．

3. 提 案 方 式

3.1 システムモデルと設計目標

本稿では，NFT オークションを対象として，主チェーン（Layer1 チェーン）と複数の拡張チェーン（Layer2 チェーン・サイドチェーン）からなるマルチレイヤ型構成を用いたオークションアーキテクチャを提案する．対象とする環境では，主チェーンは資産の最終確定（finality）を提供する基盤として位置付けられ，拡張チェーンは主チェーンの処理負荷を軽減しつつ，アプリケーション処理を分散して実行する基盤として用いる．

登場主体は，出品者（seller），入札者（bidder），リレイヤ（Relayer），およびブロックチェーンネットワークである．出品者はオークション対象の NFT を所有し，オークション開始前に主チェーン上で NFT を安全に管理可能な状態に移行する．入札者は，いずれかの拡張チェーン上で入札を行い，オークション終了後に主チェーン上で確定する落札結果に従って取引が成立する．Relayer は各拡張チェーン上のオークション結果を収集し，主チェーン上の最終確定処理に必要な情報を送信する役割を担う．

従来の多くの NFT オークションは単一の主チェーン上で入札処理を実行するため，参加者数や入札処理数の増加に伴い，ガスコストの増大や処理遅延が課題となる．これに対して本稿では，入札処理を複数の拡張チェーン上で並列に実行し，主チェーンには最終処理に必要な最小限の情報のみを反映することにより，主チェーンへの負荷集中を抑制しつつ，オークション全体のスケーラビリティ向上を目指す．

本提案の設計目標を以下に示す．

- **主チェーン負荷の軽減**：主チェーン上で高頻度な入札処理を行わず，主チェーンのトランザクション数とガスコストを抑制する．
- **拡張チェーンの並列活用**：複数の Layer2 チェーンおよびサイドチェーンを同時に利用し，入札処理を分散して実行できる構成とする．
- **結果の整合性確保**：拡張チェーン上で得られた入札結果と，主チェーン上で確定する最終結果が整合するよう，オークション手順と状態遷移を明確化する．
- **実装可能性**：既存の EVM 系実行環境を前提に，スマートコントラクトとスクリプトにより再現可能な実装とする．

3.2 入札方式（コミット・リビール方式）

本稿では，拡張チェーン上の入札方式として，コミット・リビール方式（commit–reveal）に基づく封印入札（first-price sealed-bid）を採用する．入札者は，入札額 b と乱数 s から $h = \mathrm{keccak256}(b, s)$ を計算し，コミット期間に h のみを登録する．その後，リビール期間に入札額 b と乱数 s を提示し，コントラクト側で h との一致を検証することで入札の正当性を確認する．この方式により，入札期間中に入札額が公開されないため，公開入札に比べて追随入札やフロントランニングの影響を受けにくい [3].

各拡張チェーンでは，リビール期間終了後にリビール済み入札の中から当該チェーン内の最高入札者と最高入札額を決定し，ローカル結果として確定する．最終的な落札結果は，複数拡張チェーンから得られるローカル結果を主チェーン側で比較し，最高入札額を与える結果を採用することで確定する．落札者は，主チェーン上で確定した落札額を支払うことで NFT を受領する．

3.3 全体アーキテクチャ

本節では，提案するマルチレイヤ型 NFT オークションアーキテクチャの全体構成と，各要素の役割および情報の流れを示す．図 1 に提案アーキテクチャの概略を示す．提案手法は，主チェーン（Layer1 チェーン），複数の拡張チェーン（Layer2 チェーン・サイドチェーン），およびそれらを接続するリレイヤ（Relayer）から構成される．基本方針は，NFT の保管と最終確定処理は主チェーンで実行し，高頻度に発生し得る入札処理は拡張チェーンに分散させることで，主チェーン上のトランザクション負荷を抑制する点にある．

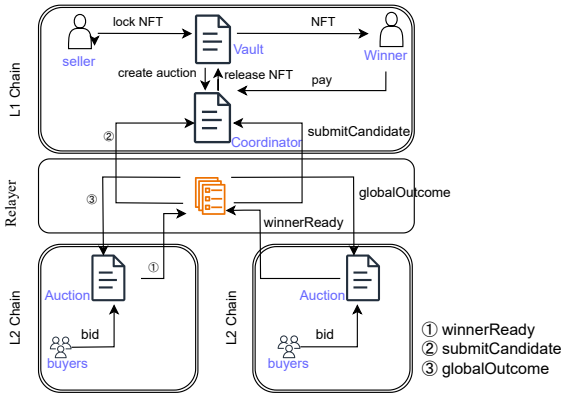

図 1　提案アーキテクチャの概要

3.3.1 主チェーン（Layer1 チェーン）

主チェーンは資産の最終確定（finality）を提供する基盤であり，(1) オークション対象 NFT の保管，(2) オークション終了後の落札結果の確定，(3) 取引成立に伴う NFT の移転および支払い処理を担う．本稿では，主チェーン上に NFT の保管を担う *NFTVault* と，最終結果の確定を担う *L1Coordinator* を配置する．*NFTVault* は，出品者が保有する NFT をオークション期間中ロックし，主チェーン上で所有権が保持される状態を提供する．*L1Coordinator* は，オークション識別子や出品者，対象 NFT，期限等のメタ情報を管理し，Relayer により報告された拡張チェーン上の入札結果に基づいて，主チェーン上で落札者および落札額を確定する．

3.3.2 拡張チェーン（Layer2 チェーン・サイドチェーン）

拡張チェーンは，入札処理を分散して実行するための実行基盤である．拡張チェーン上では，オークションに関する処理を扱う *AuctionHub*（または同等のコントラクト）を配置し，入札受付，入札状態の更新，および当該拡張チェーン内の最大入札候補（candidate）の算出をする．本提案では，複数の拡張チェーンを同時に利用することを前提とし，入札者は任意の拡張チェーンを選択して入札処理を実行できる．これにより，単一チェーンへのアクセス集中を緩和し，参加者の増加に対して処理を水平分散できる構成とする．

拡張チェーン上のオークションは，主チェーン上のオークションと同一の識別子（AuctionID）により紐付けられる．各拡張チェーンは独立に入札処理を進めるため，オークション期間中はチェーン間で逐次的な同期を行わない．一方で，オークション終了時には，各拡張チェーン上で得られた結果（最高入札情報）を主チェーンに集約する必要がある．このため，拡張チェーン側では，オークション終了後に当該チェーン内の最高入札情報を確定し，主チェーンへ送信可能な形式に整形する処理をする．本稿では，この最高入札情報を候補結果（*candidate result*）として扱い，典型的には「拡張チェーン識別子，AuctionID，最高入札者アドレス，最高入札額，結果確定時点」などから構成されるデータとして定義する．

3.3.3 リレイヤ（Relayer）

Relayer は，拡張チェーン群と主チェーンを接続し，データの集約を行う中継ノードとして機能する．具体的には，各拡張チェーンの AuctionHub から発行されるイベントログを監視し，オークション終了後に各チェーンにおける最高入札額および入札者情報を取得する．Relayer はこれら複数の並列結果を一つのトランザクションに集約して L1Coordinator へ送信する．これにより，主チェーン側は入札の全履歴を検証する必要がなくなり，最終決済に必要な最小限のデータのみをオンチェーンで処理する効率的な構成を実現している．

3.3.4 情報の流れ

提案アーキテクチャにおける情報の流れを以下に整理する．まず，出品者は主チェーン上で NFTVault に NFT をロックし，オークションを開始可能な状態を作る．次に，拡張チェーン上で *AuctionHub* によりオークションを開始し，入札者は任意の拡張チェーン上で入札処理をする．オークション期限到来後，各拡張チェーンは当該チェーン内の最高入札情報を確定し，Relayer がそれらを収集する．最後に，Relayer は複数チェーンの候補結果を主チェーンへ送信し，*L1Coordinator* はそれらを主チェーン上で比較して最大値を採用し，最終的な落札者・落札額を確定する．

3.3.5 オークション手順

本提案におけるオークション手順を時系列に整理する．まず出品者は主チェーン上で NFTVault に対象 NFT をロックし，取引対象をオークションに供する準備をする．次に入札者は任意の拡張チェーン（Layer2 チェーン・サイドチェーン）上の AuctionHub を選択して入札を行い，本稿では入札額の事前露出を抑制するためコミット・リビール方式（commit–reveal）により入札を確定させる．オークション期限到来後，各拡張チェーンは当該チェーン内で入札を集計し，最高入札者と最高入札額からなるローカル確定結果を得る．Relayer は複数の拡張チェーンから得られたローカル確定結果を収集し，それらを比較して最も高い入札額を与える結果を主チェーンへ送信する．主チェーン側では L1Coordinator が受信した結果に基づいて落札者と落札額を最終確定し，落札者は主チェーン上で落札額を支払うことで取引を成立させる．最後に L1Coordinator が NFTVault を介して NFT を落札者へ移転し，オークション

処理を完了する．

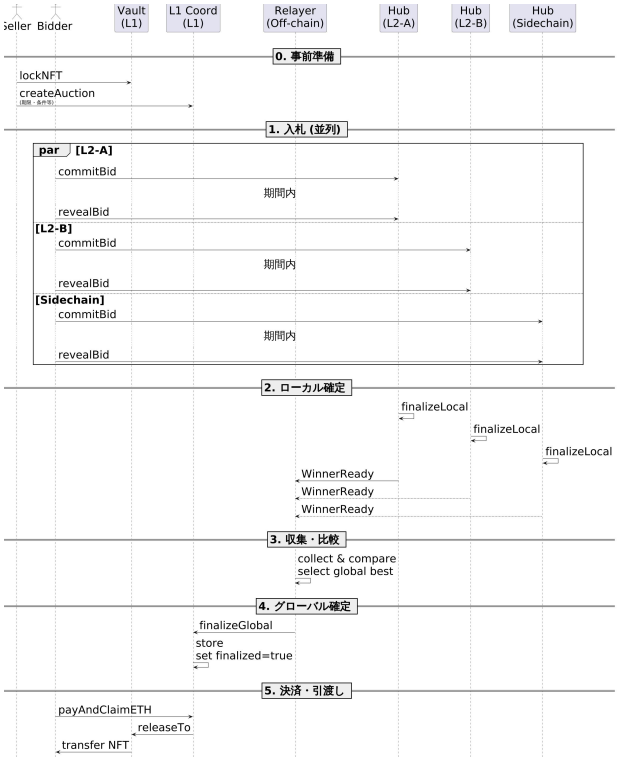

図 2　提案手法におけるオークション手順

3.4　スマートコントラクト設計

提案アーキテクチャを実現するために実装したスマートコントラクトの設計を示す．本稿では，主チェーン（Layer1）に NFT の保管と最終確定・決済を担うコントラクトを配置し，拡張チェーン（Layer2 チェーン・サイドチェーン）に入札処理を担うコントラクトを配置する．各コントラクトはオークション（出品ロット）の識別子として *lotId* を共有し，主チェーン側では最終確定に必要な情報（落札者・落札額・状態フラグ）を管理する一方，拡張チェーン側では入札処理を独立に実行する構成とする．以下では，*Vault*，*AuctionHubL2*，*CoordinatorL1* の 3 つのコントラクトについて，主要な状態変数と関数，および処理の要点を擬似コードとともに説明する．

3.4.1　Vault（Layer1）

Vault は，オークション対象の NFT を主チェーン上で一時的に保管するためのコントラクトである．出品者は事前に対象 NFT を Vault にロックし，*lotId* と *tokenId* を紐付けて管理する．最終確定後は，`CoordinatorL1` からの呼び出しにより Vault が NFT を落札者へ移転する．

3.4.2　AuctionHubL2（Layer2 チェーン・サイドチェーン）

AuctionHubL2 は，拡張チェーン上で入札処理を実行するためのコントラクトである．本稿では，入札額の事前露出による不公平を抑えるため，コミット・リビール方式（commit–reveal）を採用する．入札者はまずコミットとして入札情報のハッシュを登録し，その後にリビールとして入札額と乱数を提示する．オークション終了後は，リビール済み入札者集合を走査し，当該拡張チェーン内の最高入札者と最高入札額を候補として算出し，ローカル候補結果として通知する．

3.4.3　CoordinatorL1（Layer1）

CoordinatorL1 は，拡張チェーン上で得られた候補結果を受け取り，主チェーン上で最終結果を確定し，決済と NFT 引き渡しを実行するコントラクトである．主チェーン側では入札履歴全体を保持せず，`lotId` ごとに落札者・落札額および状態（確定・決済）だけを管理する．Relayer は各拡張チェーンの候補結果を `submitCandidate` として登録し，`FinalizeGlobal` は提出された複数チェーンの候補結果を主チェーン上で比較して最大値を採用し，最終的な落札者・落札額を確定する．`PayAndClaim` は落札者による支払いを確認した上で，Vault に NFT の解放を要求する．

本章では，マルチレイヤ型 NFT オークションアーキテクチャを提案し，主チェーンと拡張チェーンの処理分担，ならびにチェーン間情報伝搬の設計を示した．提案方式では，各拡張チェーンが当該チェーン内の最高入札結果（ローカル最大値）を出力し，Relayer がそれらを主チェーンへ報告する．主チェーン上では，報告された複数チェーンのローカル最大値を比較して全体の最高入札結果を確定し，決済および NFT の移転を実行する．この構成により，入札履歴全体を主チェーンへ集約することなく，複数拡張チェーンを同時に利用したスケーラブルなオークション処理を実現する．

4.　性 能 評 価

4.1　評価の目的と方針

本節では，提案方式が NFT オークションの実行コストに与える影響を定量的に示す．従来方式として，単一の主チェーン（Layer1）上で入札から確定までを実行する方式（Single-Layer1）を比較対象とし，提案方式として，入札処理を拡張チェーン（Layer2 チェーン，サイドチェーン）に分散し，主チェーンでは最終確定と決済のみをするマルチレイヤ型方式（1 つ Layer2，Multi-Layer2，Sidechain 併用）を評価する．

本稿の基本方針は，主チェーン上で高頻度に発生し得る入札処理を行わず，拡張チェーン側で入札処理を処理し，主チェーンには最終確定に必要な情報のみを反映することである．このとき，主チェーン側で発生する処理は主として最終確定および決済に限定されるため，入札者数の増加に対して主チェーン負荷がどの程度抑制されるかが重要となる．そこで本章では，処理をフェーズに分解し，各フェーズの GasUsed と手数料を測定し，方式間で比較する．

4.2　評 価 指 標

4.2.1　GasUsed

GasUsed は，スマートコントラクト実行に要した計算資源量を表す指標であり，トランザクション実行時に消費されたガス量（`gasUsed`）としてレシートに記録される．ガスは EVM（Ethereum Virtual Machine）上の命令実行コストを抽象化した単位であり，ストレージ書き込みやログ出力などの操作に応じて消費量が決まる．そのため GasUsed は，ネットワーク混雑や通貨価格の影響を受けにくく，方式間で「処理そのものがどれだけ重いか」を比較するのに適している．

本稿では，入札処理を `commitBid`, `revealBid`, `finalizeLocal`，主チェーン側の最終処理を `finalizeGlobal`，`payAndClaim` としてフェーズ分解し，各フェーズの GasUsed を集計する．なお，`commitBid` と `revealBid` は入札者ごとに 1 回発生するため，入札者数の増加に伴う GasUsed の増加傾向（スケーラビリティ）を観測しやすい．

4.3　評価環境と条件

4.3.1　使用ネットワークと実装構成

提案方式の有効性を検証するため，EVM 互換の複数テストネットを用いて評価環境を構築した．主チェーン（Layer1）には Ethereum Sepolia を採用し，資産の最終確定（final-

ity）を担う *NFTVault* および *L1Coordinator* コントラクトを配置した．ここでは NFT の保管（`lockNFT`），最終結果の確定（`finalizeGlobal`），および決済（`payAndClaim`）を実行する．拡張チェーン（Layer2/サイドチェーン）には Arbitrum Sepolia，Optimism Sepolia，Polygon Amoy を採用し，入札処理を担う *AuctionHub* コントラクトを配置した．ここでは入札（`commitBid`, `revealBid`）およびローカル確定（`finalizeLocal`）を実行する．これにより，コスト特性の異なるネットワーク（L1，L2，サイドチェーン）間での機能分散とコスト削減効果を検証する．

4.3.2 計測条件

各シナリオでは，処理を実行してガス消費量（`gasUsed`）を集計し，前節の定義式に基づいて実支払額を算出した．コスト算出にあたっては，ネットワーク間の比較条件を統一するため，2026 年 1 月時点の市場価格に基づく代表値（表 1）を用いた．

表 1　評価パラメータ（2026 年 1 月基準）

ネットワーク	Gas Price (Gwei)	Token Price (USD)
Ethereum (L1)	0.4	3,350 (ETH)
Optimism (L2)	0.001	3,350 (ETH)
Arbitrum (L2)	0.02	3,350 (ETH)
Polygon (Sidechain)	360	0.16 (POL)

4.4 実験結果と考察

本節では，提案方式における主要処理のガス消費量（gasUsed）を整理し，ネットワークごとのガス手数料（gasfee）および実支払額（USD）を比較する．ここで gasUsed はトランザクション実行により実際に消費されたガス量であり，gasfee は gasUsed にガス単価を乗じて得られる支払コストを表す．さらに，ネットワーク間で支払通貨（Token）が異なる点を考慮し，gasfee をトークン価格で換算した実支払額（USD）も併記する．

本稿の評価はテストネット上で実施したが，gasfee および USD 換算に用いるガス単価・トークン価格は，後続の比較を現実の運用コストに近い形で解釈するために，各ネットワークの本番環境（Mainnet）における代表値を採用する．以降では，(i) 主チェーン（Layer1）で実行する処理，(ii) 拡張チェーン（Layer2 チェーン・サイドチェーン）で実行する処理，の双方について，シナリオ別にガス消費と支払額の傾向を示す．特に，提案方式では入札処理（commit–reveal）とローカル確定を拡張チェーン側へ移す一方，主チェーン側には最終確定と決済に必要な最小限の処理のみを残すため，処理配置の違いが総コストに与える影響を明確化する．

4.4.1 単一チェーン方式との比較

入札者 5 名（各 EOA）条件で，単一チェーン方式（Sepolia のみ）と提案方式（Sepolia ＋ Arbitrum Sepolia）を比較する．提案方式では，主チェーンで `lockNFT` を実行後，入札者は拡張チェーン上で `commitBid`/`revealBid` を各 1 回実行し，`finalizeLocal` によりローカル確定する．その後，主チェーンで `finalizeGlobal` により最終確定し，落札者が `payAndClaim` を実行する．gasUsed は各トランザクションレシートから取得し，入札者 5 名分の入札処理は合算した．表**??**に gasUsed を示す．

表 2　gasUsed の比較（入札者 5 名，処理別）

処理	提案方式（Sepolia + Arbitrum）	単一チェーン（Sepolia のみ）
`lockNFT`	91,608（Sepolia）	–
`commitBid`（5 名分合計）	224,188（Arbitrum）	263,333
`revealBid`（5 名分合計）	349,417（Arbitrum）	359,900
`finalizeLocal`	74,985（Sepolia）	–
`finalizeGlobal / finalizeAuction`	99,525（Sepolia）	128,433
`payAndClaim`	67,241（Sepolia）	67,873
合計	**906,964**	**819,539**

次に，平均 Gas Price（Sepolia: 0.4 Gwei，Arbitrum: 0.02 Gwei）を適用して gasfee を算出し，さらに換算レート（ETH=3,350 USD）に基づき USD 換算額を求めた．結果を表 3 に示す．単一チェーン方式は 1.10 USD, 提案方式は 0.39 USD となり，約 65% の費用削減を確認した．

表 3　gasfee・実支払額の比較（入札者 5 名）

方式	合計 gasUsed	gasfee（ETH）	実支払額（USD）
単一チェーン（Sepolia のみ）	819,539	0.0003278	1.10
提案方式（Sepolia ＋ Arbitrum Sepolia）	906,964	0.0001163	0.39

なお，提案方式でもロック・最終確定・決済は主チェーンに残る一方，入札者数に比例して増加する `commitBid`/`revealBid` は拡張チェーン側で実行されるため，参加者増加時に単一チェーンとの差が拡大することが期待できる．

4.4.2 2 つの Layer2 チェーンにおける入札者数の影響

本節では，拡張チェーンとして Arbitrum Sepolia と Optimism Sepolia の 2 本を同時に用いる構成について，入札者数の増加がガス消費に与える影響を整理する．入札者は 2 つの拡張チェーンへ概ね均等に分配し（合計入札者数 N に対し各チェーン $N/2$ 程度），各入札者が `commitBid` と `revealBid` を各 1 回実行する．入札終了後，各拡張チェーンでローカル確定を行い，Relayer が候補結果（各チェーンの最高入札結果）を主チェーンへ集約し，主チェーン上で `finalizeGlobal` により最終結果を確定する．

表 4 に入札者数別の gasUsed 集計結果を示す．主チェーン側では `lockNFT` と `payAndClaim` が出品ごとに 1 回のみ実行されるため，入札者数によらず主チェーン側コストは概ね一定となる．一方，拡張チェーン側では `commitBid`/`revealBid` が入札者ごとに発生するため，入札者数に対して概ね線形に増加する．また，本構成では主チェーン上で 2 本の候補結果を比較する必要があるため，主チェーン＋ 1 本構成に比べて `finalizeGlobal` の処理負荷が増加し，主チェーン側の確定処理コストが高くなる傾向がある．一方で，入札処理を 2 本へ分散できるため，アクセス集中の緩和や並列実行による混雑回避が期待でき，参加者数が大きい条件ほど分散の有効性を示しやすい．

表 4　主チェーン＋ 2 つの拡張チェーンにおける入札者数別 gasUsed

入札者数（各 L2）	主チェーン合計	Arbitrum Sepolia 合計	Optimism Sepolia 合計	全体合計
1	280,334	214,551	214,537	709,422
5	280,334	641,243	641,243	1,562,820
10	280,334	1,236,353	1,236,329	2,753,016

4.4.3 サイドチェーン併用における入札者数の影響

本節では，Layer2（Arbitrum Sepolia）とサイドチェーン（Polygon Amoy）を併用する構成について，入札者数の増加がガス消費に与える影響を整理する．入札者は 2 つの拡張チェーンへ概ね均等に分配し（合計入札者数 N に対し各チェーン $N/2$ 程度），各入札者が `commitBid` と `revealBid` を各 1 回実行する．入札終了後，それぞれの拡張チェーン上でローカル確定を行い，Relayer が候補結果（各チェーンの最高入札結果）を主チェーンへ集約し，主チェーン上で `finalizeGlobal` により最終結果を確定する．

Polygon Amoy 側で取得した gasUsed 集計結果を表 5 に示す．主チェーン側は `lockNFT` と `payAndClaim` が出品ごとに 1 回のみ実行されるため，入札者数によらず主チェーン側コストは概ね一定となる．一方，拡張チェーン側では `commitBid`/`revealBid` が入札者ごとに発生するため，入札者数に対して概ね線形に増加する．また，本構成では候補結果が 2 本

（Layer2 + Sidechain）となるため，主チェーン上で比較を伴う `finalizeGlobal` が必要であり，本実験では `finalizeGlobal` の gasUsed は 36,582 であった．

表 5　Polygon Amoy における入札者数別 gasUsed

入札者数	gasUsed 合計
1	187,509
5	641,649
10	1,209,324

4.5　入札者数に対する実支払額推移

本節では，各シナリオで取得した gasUsed 集計値を，実行ネットワークに対応する平均 Gas Price と支払通貨単価に基づいて換算し，gasfee（支払通貨量）および USD 換算額を算出する．提案方式では処理が複数ネットワークに分散して実行されるため，処理が実行されたネットワークに応じて換算基準を切り替える．具体的には，主チェーン（Sepolia）上で実行される処理（例：`lockNFT`，`finalizeGlobal`，`payAndClaim`）は Sepolia 側の基準（ETH の平均 Gas Price と ETH 建ての支払）で換算する．一方，Layer2（Arbitrum/Optimism）上の入札処理（`commitBid/revealBid`）およびローカル確定は，各 Layer2 の基準（平均 Gas Price，支払は ETH 建て）で換算する．さらに，Sidechain（Polygon Amoy）上の処理は Polygon 側の基準（平均 Gas Price，支払は POL 建て）で換算し，USD 換算では POL の単価を用いる．入札者の割り当ては，チェーン数に応じて概ね均等に分配する方針とした（例：2 本構成では N を半数ずつ）．

表 6　各シナリオにおける gasfee（支払通貨量）の比較

シナリオ	$N=1$	$N=2$	$N=5$	$N=10$	$N=15$	$N=20$
単一チェーン	0.00011612	0.000169	0.000327	0.000592	0.000857	0.001121
L1+L2	0.00010672	0.00010912	0.000116	0.000128	0.000140	0.000152
L1+2 つの Layer2	–	0.00012152	–	0.000131	–	0.000144
L1+L2 + Sidechain	–	ETH: 0.000121 POL: 0.067503	–	ETH: 0.000130 POL: 0.230993	–	ETH: 0.000142 POL: 0.435356

表 7　各シナリオにおける実支払額（USD）の比較

シナリオ	$N=1$	$N=2$	$N=5$	$N=10$	$N=15$	$N=20$
単一チェーン（ETH）	0.3890	0.5663	1.0980	1.9850	2.8710	3.7580
L1+L2（ ETH）	0.3575	0.3656	0.3897	0.4299	0.4701	0.5103
L1+2 つの L2（ ETH）	–	0.4071	–	0.4409	–	0.4830
L1+L2 + Sidechain（ETH+POL）	–	0.4173	–	0.4756	–	0.5486

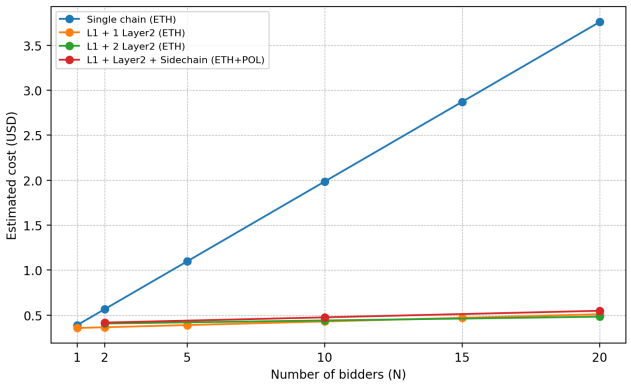

図 3　入札者数 N に対する実支払額（USD）の推移

表 7 と図 3 より，入札者数 N が増加するほど単一チェーン構成では実支払額が大きく増加する一方，Layer2 を用いる構成では増加が緩やかである．これは，入札処理（`commitBid/revealBid`）が主に拡張チェーン側で発生し，Layer2 の低い Gas Price により入札回数増加時の費用増分を抑制できるためである．また，サイドチェーンを含む構成では Gas Price が高くても支払通貨（POL）の単価が低いことから，USD 換算の費用が相対的に小さくなる傾向が現れる．さらに，いずれの構成でも主チェーン側の処理（ロック・最終確定・支払い）は必須であるためコストの下限を形成するが，参加者数が増えるほど入札部分の比率が増し，結果として拡張チェーン活用による相対的な優位性が大きくなる．

5.　ま　と　め

本稿では，主チェーンと複数の拡張チェーン（Layer2・サイドチェーン）からなるマルチレイヤ型 NFT オークションアーキテクチャを提案した．提案方式は，NFT の保管および最終確定・決済を主チェーンで行い，入札処理を拡張チェーンへ分離して並列実行することで，主チェーンへの負荷集中を抑制しつつスケーラビリティ向上を図る．実装では，主チェーンに Vault と Coordinator，拡張チェーンに AuctionHub を配置し，拡張チェーン側で commit–reveal により入札を受け付けた後，各チェーン内で最高入札結果を確定し，主チェーンで最終確定と決済を行う構成とした．評価では，EVM 互換テストネット（Sepolia，Arbitrum Sepolia，Optimism Sepolia，Polygon Amoy）上で提案方式を実装し，単一チェーン構成と比較した．その結果，入札処理を拡張チェーンへ分散することで，入札者数が増える条件ほど費用面の優位性が大きくなる傾向を確認した．以上より，複数ネットワーク環境における実装・評価を通じて，本提案の有効性を示した．

謝辞　本稿は JSPS 科研費（25K03113, 23K28078）の助成を受けたものである．

文　　献

[1] H. Guo, et al., “A framework for efficient cross-chain token transfers in blockchain networks,” Journal of King Saud University Computer and Information Sciences, 2024.
[2] Z. Shi, et al., “Integration of Blockchain and Auction Models: A Survey, Some Applications, and Challenges,” IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 497-537, 2023.
[3] K. Chin, et al., “A Sealed-Bid Auction With Fund Binding: Preventing Maximum Bidding Price Leakage,” IEEE Blockchain, 2022.
[4] K. B. Nikitha, et al., “E-Auction Using Blockchain Mechanism,” ICAECA, 2023.
[5] H. Miyaji and N. Kamiyama, “PPSCCC: Privacy-Preserving Scalable Cross-Chain Communication Among Multiple Blockchains Based on Parent-Child Blockchain,” ACISP, 2025.
[6] M. R. Hossain, et al., “A Comprehensive Analysis of Blockchain Technology and Consensus Protocols Across Multilayered Framework,” IEEE Access, 2024.
[7] H. Desai, et al., “A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions,” IEEE Blockchain, 2019.
[8] C. Pop, et al., “An Ethereum-based implementation of English, Dutch and First-price sealed-bid auctions,” IEEE ICCP, 2020.
[9] G. Sharma, et al., “Anonymous Fair Auction on Blockchain,” NTMS, 2021.
[10] H. Watanabe, et al., “Verifiable M1st-Price Auction without Manager,” CSS, 2020.
[11] H. Huang, et al., “DecoupleChain: A Two-Layer Blockchain Sharding System Enabling Frequent Shard Reconfiguration,” IEEE ICWS, 2025.