設計ガイド：NFT を利用するアプリケーション

設計ガイドについて

ブロックチェーンを利用するアプリケーションは、従来のアプリケーションとは異なる特徴や制約を持ち、それらに対応した設計が必要です。設計ガイドでは、ブロックチェーンを利用するアプリケーションの開発に関する重要なポイントについて、ひとつずつトピックを取り上げ、説明していきます。今回のトピックは、NFT を利用するアプリケーションについてです。

ベストプラクティスや事例を交えながら、ブロックチェーンの基本原理や概念に沿って効果的にブロックチェーンを活用するための指針を示します。ブロックチェーンに関する一般的な内容は、ブロックチェーンの共通の特性や仕組みに基づいて説明します。東芝独自のブロックチェーン DNCWARE Blockchain+™ (BC+)に関する固有の視点は、このプラットフォームで利用可能な機能に触れながら紹介します。BC+固有の視点は、[BC+]というラベルを付けて区別します。

はじめに

この設計ガイドでは、NFT を利用したアプリケーションについて、以下のような観点で指針を示します。

- NFT について
- NFT の構成
- NFT とデジタル資産の"所有権"
- NFT の意味付け
- NFT の唯一性とトークン URI
- NFT の用途
- BC+における NFT
- NFT のオーナーであることの検証

NFT について

NFT (Non-Fungible Token) は、イーサリアム上で作成できるユニークなトークンです。NFT はデジタルアート販売、会員権、デジタル証明書、ゲーム、暗号資産、地域活性化などさまざまな用途で使用されています。NFT の利用範囲が広がっている理由として、用途に応じてさまざまな種類の NFT を作成できることが挙げられます。具体的には、NFT はイーサリアムのスマートコントラクトを利用して作成されています。スマートコントラクトはブロックチェーン上で動作するプログラムなので、目的に応じて動作を自由自在にカスタマイズすることができます。

しかし、NFT の開発者がそれぞれ独自に開発を進めると、NFT を相互利用することが難しくなります。そこで、ERC721 という標準的なインターフェースが定義されています。NFT の開発者がこのインターフェースに従ってスマートコントラクトを作成することで、さまざまな NFT の相互利用が容易になります。なお、ERC721 以外にも ERC1155 などの異なるインターフェースがあり互換性がありませんが、総称として NFT と呼ばれるため注意が必要です。

[BC+]

同様の NFT を BC+上でも実現できます。イーサリアム上の NFT と同様に、BC+でも NFT をスマートコントラクトで実装します。相互利用を促進するため、ERC721 に似たインターフェース定義を公開しています。ただし、イーサリアムと BC+ではスマートコントラクトの言語仕様が異なるため、ERC721 との完全な互換性はありません。

BC+における NFT の標準的なインターフェース定義
https://dncware-blockchain-plus.github.io/samples/practical/nft-spec.html
BC+における NFT のサンプルコードの説明
https://dncware-blockchain-plus.github.io/samples/docs/NFT_overview.pdf
BC+における NFT のスマートコントラクトの例
https://dncware-blockchain-plus.github.io/samples/practical/nft200.mjs

本書では、特に断りがない限り、ERC721 または前述の BC+のインターフェース定義に準拠した NFT について説明します。

NFT の構成

NFT を実装したスマートコントラクト内では、複数のトークンが管理されています。それらをスマートコントラクト内で一意に識別するために、トークン ID と呼ばれる識別子が用いられます。このトークン ID があることで、NFT のトークンは唯一無二の存在となります。具体的には、ブロックチェーン、スマートコントラクト、そしてトークン ID の 3 段階の ID を特定することで、NFT のトークンはグローバルに一意に識別されます。

一例として、競売会社クリスティーズのオークションで高額落札された NFT の"EVERYDAYS: THE FIRST 5000 DAYS"は、以下の情報で一意に識別されます。

ブロックチェーン：Ethereum Main Network
スマートコントラクト：0x2A46f2fFD99e19a89476E2f62270e0a35bBf0756
トークン ID：40913

NFT は一つ一つのトークンに対して、トークンのオーナーがブロックチェーンに記録されています。一つのトークンのオーナーは同時に一人までです。そして、オーナーは自身が所有するトークンを譲渡（Transfer）することができます。トークンが譲渡されると、ブロックチェーン上に記録されているオーナーが書き換えられます。

イーサリアムの場合、すべてのスマートコントラクトが公開されており、NFT の現在のオーナーを誰でも調べることができます。例えば、上の例のトークンのオーナーは、Etherscan で調べることができます。対象のスマートコントラクトを読み出す下記のページを開き、ownerOf のところにトークン ID を指定して問い合わせると、現在のオーナーのウォレットアドレスが表示されます。

上の例のスマートコントラクトを読み出すページ：
https://etherscan.io/address/0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756#readContract

Etherscan 上での NFT のオーナーの問い合わせ例：

あるいは別の方法として、NFT マーケットプレースである OpenSea のページを開いてオーナーを確認することができます。このページには、取引履歴などの他の情報も表示されます。このページにアクセスする下記 URL の後半部分は、スマートコントラクトのアドレスと、トークン ID で構成されています。

上の例のトークンの OpenSea 上のページ：
https://opensea.io/assets/ethereum/0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756/40913

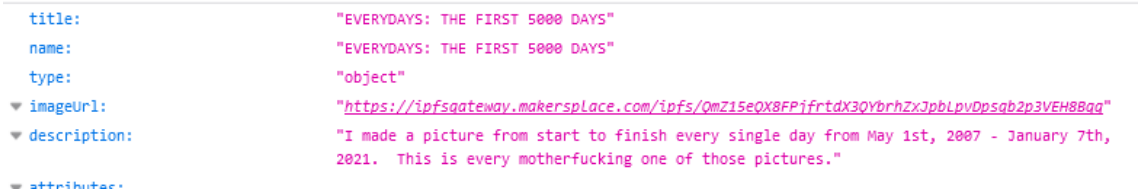
OpenSea のページを見ると、NFT には画像が付いていることがわかります。すべての NFT に画像があるわけではありませんが、特にデジタルアートの NFT ではほとんどの場合に画像が付いています。また、NFT の名前や説明も表示されています。これらの情報はメタデータとして NFT の外部に記録されているものです。メタデータの格納場所は、スマートコントラクト内のトークン URI という文字列として記録されています。

このトークン URI は、やはり Etherscan で調べることができます。対象のスマートコントラクトを読み出す下記ページを開き、tokenURI のところにトークン ID を指定して問い合わせると、トークン URI が表示されます。この例の場合では、トークン URI は IPFS 上のメタデータを指していることがわかります。メタデータの中に画像の URL が記載されており、この URL の先に NFT に割り当てられた画像があります。

上の例のスマートコントラクトを読み出すページ：
https://etherscan.io/address/0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756#readContract

Etherscan 上での NFT のトークン URI の問い合わせ例：

トークン URI が指す IPFS 上のメタデータ(JSON 形式)：
https://ipfs.io/ipfs/QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXDPvPx3VC5zUz



メタデータ中の imageURL：
https://ipfsgateway.makersplace.com/ipfs/QmZ15eQX8FPjfrtdX3QYbrhZxJpbLpvDpsgb2p3VEH8Bqq

デジタルアートの NFT の多くは、この例と同様の構成を持っています。具体的には、IPFS 上にデジタルアートの名前や説明、画像の URL などのメタデータを JSON 形式で格納しておき、そのメタデータの場所をトークン URI として NFT を作成します。つまり、デジタルアートの名前や説明、画像などのコンテンツ自体は NFT とは別に保存されており、ブロックチェーン上にはその場所を示すトークン URI が記録されるのです。

NFT を作成するアプリケーションを設計する際には、NFT のメタデータや画像などのデータをどのように格納するかを設計する必要があります。データが小さい場合、トークン URI の文字列に直接埋め込むか、NFT のスマートコントラクト内に格納することで、ブロックチェーン上に保管することが可能です。この方法を用いる NFT は「オンチェーン NFT」と呼ばれ、NFT 本体とデータが分離しないため、最も信頼性が高いです。

一方、データをオフチェーンに保存する場合、格納先の代表的な選択肢としては IPFS や Amazon S3 などのクラウドストレージがあります。これらの選択肢にはそれぞれ特徴があり、どれが最適かはアプリケーションの目的によって異なります。たとえば、IPFS はデータの変更不可・全公開です。一方、クラウドストレージはデータの変更可で、特定の管理者によって開示範囲が設定されます。こういった性質の違いを考慮して、NFT のデータの格納先を選択します。

[BC+]

BC+の NFT でも、トークン URI の宛先を選ぶ必要があります。データの格納場所としては、イーサリアムの場合と同様にオンチェーン、IPFS、クラウドストレージなどが選べますが、BC+ではさらにブロックチェーン・ノードを選択可能です。その場合の具体的な方法は 2 つあります。

1. 添付ファイル機能：数メガバイト程度までのファイルを、変更不可・削除不可なデータとしてブロックチェーン・ノードに保存します。

2. ストレージ機能：複数のブロックチェーン・ノードに割り当てられた領域に、任意のデータを秘密分散して保管します。この方法では、データは変更可能・削除可能です。（スマートコントラクト・バージョン 3.7 から利用可能）

NFT とデジタル資産の"所有権"

この章ではデジタル資産の NFT の意味について考えていきます。NFT はデジタル資産の所有権を表すものだという説明をよく見かけますが、これについて具体的に掘り下げていきます。まず、デジタルアートの NFT を取り扱っている競売会社クリスティーズのホームページの次の説明を見てみましょう。

> What is an NFT
> An NFT, or 'non-fungible token', is a unique, digital certificate that is stored on a blockchain and provides certain ownership rights in an asset, typically a digital one, such as a digital work of art. NFTs provide a powerful tool to establish and demonstrate ownership rights in the digital asset space where it is often hard to demonstrate such rights given how quickly and easily digital works can be replicated. [1] 以下省略

日本語訳：

NFT、つまり「非代替性トークン」は、ブロックチェーンに保存され、資産（通常はデジタルアート作品など）に対する特定の所有権を付与する固有のデジタル証明書です。NFT は、デジタル作品が迅速かつ容易に複製できるため、所有権を実証することが難しいことが多いデジタル資産分野で、所有権を確立して実証するための強力なツールを提供します。

このように、デジタルアートの取引の現場では、デジタル作品の"所有権”を実証するツールとして NFT が認知されています。つまり、デジタル作品は複製の中からオリジナルを区別することが困難ですが、それを逆手にとって、NFT のオーナーが持っている複製がオリジナルであると定義することにより、その課題を解決しようというわけです。

NFT がデジタル作品の"所有権”を表しているものであるとオークションの当事者が考えるのであれば、ＮＦＴが高額で落札される可能性が高まります。また、そのように信じる人が多ければ、その後も NFT の価値は維持されます。その意味で、この考えは妥当であるといえます。

一方で、法令で定義される所有権についてはどうでしょうか。無体物であるデジタル作品は（日本では）そもそも所有権の対象になりません。したがって、法令上は、デジタル作品の"所有権”には意味がなく、NFT のオーナーであることを理由にして、デジタル作品の"所有権"を第三者に主張しても、法的な効力は当然に無いでしょう。所有権という言葉から漠然とイメージされる法的な効力を NFT はもっていないのです。

NFT を利用するアプリケーションを設計する際には、上記の二面性を正しく理解していることが重要になります。

> 所有権のところを著作権と言い換えた場合についての考察
> 所有権と違い、デジタル作品は著作権の対象になり得ます。しかし、デジタル作品を販売した際に、著作権までもが自動的に譲渡されるわけではなく、著作者は著作権をそのまま保持するのが普通です。これは、本を買ってもその本の著作権が得られるわけではないことと同じです。したがって、NFT がデジタル作品の著作権を表している、として NFT を販売することは可能ですが、通常のケースではそのような形でデジタル作品を販売するということは、著作者がしないでしょう。

NFT の意味付け

前の章ではデジタル資産の NFT の意味の二面性について説明しました。この二面性はデジタル資産に限らず、そのほかの NFT を利用するアプリケーションにも一般に言えることです。NFT を設計する際には、以下の点について十分に検討することが重要になります。

・NFT になんらかの意味を持たせる。
・NFT の意味をアプリケーション利用者の共通の理解として浸透させる。
・NFT の意味を担保するための仕組みを開発する。

NFT の意味付けにおいては、社会に既に存在する概念や仕組みと衝突しないことが最低限必要です。デジタルアートの例では、従来はデジタル作品の"所有権"を実証することが難しいという背景があったため、NFT を導入しても既存の概念と衝突することがなく、うまくいきます。

一方、デジタルではない現物の作品にまでも同様の NFT を導入すると、現物の作品を所有しているという法令上の所有権と、NFT のオーナーであることによる"所有権"の概念が衝突するため、うまくいかなくなります。このような場合は、衝突が起きない別の概念に置き換えるのがよいでしょう。たとえば、その作品の「デジタル版」の"所有権"を表す NFT とするという手があります。

他の例としては、メタバース内のアイテムなどは現実世界とは隔離されているため、既存の社会的概念や仕組みと衝突しにくく、NFT 化に適しています。また、新しいビジネスを始める際に生まれる新しい概念も、既存のものと衝突しにくいため、NFT 化に向いています。特に、法令で定義されていないが、ある種の権利や価値を表す新しい概念は、NFT 化に適しています。

NFT の意味を定義した後、その意味に沿った機能を持つ仕組みを作る必要があります。例えば、特定のデジタル空間に参加できるデジタル会員証を NFT として発行した場合、その NFT を持っている人がそのデジタル空間にログインできるようにする仕組みが必要です。これを実現するシステムは NFT を作成するだけで勝手に現れるわけではないので、追加のシステムとして開発する必要があります。

NFT の効力をシステム的に実装するのが難しい場合もあります。そのような場合には、利用規約にルールを記載するなどして、包括的に NFT の効力を持たせる工夫が必要です。NFT の意味の解釈は人によって異なる可能性があるため、そのズレから生じる問題を想定し、利用規約などでガイドラインを設けておくことも大切です。

NFT の唯一性とトークン URI

NFT は唯一性が特徴ですが、これはトークン URI が重複しないという意味ではありません。つまり、異なる 2 つの NFT が同じトークン URI を持つこともあります。例えば、デジタルアートの NFT を作成する際に、1 つのデジタルアートに対して限定数のコピーを作り、それぞれに NFT を割り当てて販売することが考えられます。これは従来の版画作品の販売のアナロジーとして理解できます。このケースでは、これらの NFT のトークン URI は同じになっても問題ありません。

別のケースとして、第三者が無断で同じトークン URI を持つ別の NFT を作成することが考えられます。これは、いわば NFT の贋作で、技術的に容易に作成可能です。NFT 自体はユニークなので、これらの NFT を区別することは簡単ですが、どちらが本物かは知らなければわかりません。そのため、トークン URI だけを見て NFT を信用することはできません。本物の NFT がどのブロックチェーンの、どのスマートコントラクトの、どのトークン ID であるかを事前に知っておく必要があります。NFT の効力を実装するシステムは、この点に注意して設計する必要があります。ユーザが NFT を作成でき、その際にトークン URI をユーザが自由に指定できるようなアプリケーションを設計する場合にも、この点に特に注意が必要になるでしょう。

NFT の用途

NFT が応用できるさまざまな用途について、その代表的なものをいくつか紹介します。

・デジタル作品のオーナーシップ

最古の NFT として知られる CryptoPunks や、最高取引額として知られる"EVERYDAYS: THE FIRST 5000 DAYS"などが有名ですが、これ以外にも無数のデジタル作品が NFT 化されています。どのようなデジタル作品であっても、イーサリアムのガス代さえ払えば誰でも NFT 化することができますし、OpenSea などのブロックチェーン上のマーケットプレースを通して、その NFT を販売することができます。画像に限らず音楽や動画などあらゆるデジタル作品を NFT 化することができます。このタイプの NFT は、NFT のオーナーとなること自体に主要な価値があるため、それ以外の効力が明確になっていない場合が多い点に注意が必要です。

・デジタルトレーディングカード

野球やバスケットボールの選手の写真などをカードに印刷したものとしてトレーディングカードがありますが、これのデジタル版としての NFT が（米国の）各球団の公認つきで販売されています。典型的な NFT トレーディングカードでは、試合中の最高のシーンのショート動画などがコンテンツとなります。もともとトレーディングカードのコンセプトが NFT のそれに非常に近いため NFT 化しても違和感がなく、NFT の用途として適しています。

・会員権

NFT のオーナーとなることにより会員の資格を得られるというものです。最初期の NFT のひとつである"Bored Ape Yacht Club"は、この仮想クラブの会員権でした。NFT のオーナーとなり会員になると、さまざまな特典が得られます。たとえば、仮想通貨(ApeCoin)をエアドロップで取得できるなどです。ほかの例としては、DAO(分散型自律組織）のガバナンストークンとしての NFT があります。このタイプの NFT は効力が明確になっています。したがって、NFT の導入にあたってはその効力を実現するためのシステムも同時に開発する必要があります。

・地域活性化（NFT クーポン）

NFT を地域のお店で提示すると割引が受けられる、地域の神社にお参りすると NFT がもらえるなど、NFT を使ったさまざまなアイディアで地方の活性化を実現しようとする取り組みがあります。このタイプの NFT は、無料で配られることが多いです。NFT そのものの資産価値が低いため、NFT 導入の敷居も低くなります。ですが、アイディア次第では地域活性化に大きな効果を上げる可能性があります。

・デジタル証明書

NFT のコンテンツとして証明書を格納することにより、デジタル証明書とする使い方です。ブロックチェーンの耐改ざん性、不変性といった特徴を利用しています。証明書の内容をまるごとオンチェーンに格納するか、証明書の内容のハッシュ値をオンチェーンに格納して、証明書の内容が改ざんされないことを担保します。このタイプの NFT は譲渡することには意味がなく、譲渡を禁止する措置をスマートコントラクトに設定する場合もあります。

BC+における NFT

[BC+]

この章では、BC+における NFT に特有の点について説明します。

・トークンのオーナー

イーサリアムの NFT では、トークンのオーナーはウォレットアドレスやコントラクトアドレスで示されますが、BC+ではユーザ ID やコントラクト ID でオーナーを示します。これらの ID は、ブロックチェーンに記録された DID（分散型 ID）の一種です。オーナーをアドレスで直接に示すのではなく、抽象化された DID を使用することで、アドレスとトークンの関係が間接的になり、運用の柔軟性が向上しています。

・アクセス権

BC+では、アクセス権を設定できます。この機能を使って、NFT の流通範囲や取引の公開範囲を制限することが可能です。また、アクセス権を全体に開放することもでき、その場合はイーサリアムと同様にアクセス制限のない NFT となります。ここでは、NFT へのアクセス権の設定の具体例をいくつか示します。

NFT コントラクトの履歴開示先(disclosed_to)を制限することにより、NFT コントラクトのアクセス履歴の開示先を制限できます。NFT の取引履歴などを公開したくない場合などに有効です。

NFT コントラクトの実行許可先（accessible_to）を制限することで、NFT コントラクトへのアクセス自体を制限できます。具体的には、NFT コントラクトからのトークン情報の読み取りや、トークンの譲渡のトランザクション要求などの呼び出し元が制限されます。これにより NFT の流通範囲を事実上制限することができます。ただし、accessible_to の設定だけでは範囲外への譲渡は禁止できていません。これを禁止するためには、スマートコントラクト内のプログラムとして処理する必要があります。具体的には、trasferFrom の宛先(args.to)を accessible_to に設定した範囲に限定するには、たとえば下記のようにします。

```
if ( ! isAccessibleTo(getContractId(), args.to)) throw 'denied';
```

・トークン ID

イーサリアムの NFT ではトークン ID は整数値ですが、BC+ではトークン ID が文字列になっています。そのため、トークンの内容を表す文字列をトークン ID として設定することが可能です。これにより、NFT の人による識別が容易になります。

・転送履歴コントラクト

ERC721 では、トークンの譲渡（Transfer）がイベントとして定義されており、取引履歴を追跡できます。これに意味的に対応するものとして、BC+では転送履歴コントラクトがインターフェース定義に含まれています。直に NFT コントラクトのトランザクション履歴を追跡することでも取引履歴を確認できますが、それに比べて、アクセス権を個別に設定できる、複数の NFT コントラクトの取引履歴をまとめられる、引数型が検索しやすい形式になっているなど、転送履歴コントラクトの方が使いやすくなっています。

NFT のオーナーであることの検証

NFT を利用したアプリケーションを実装する際、NFT のオーナーであることを検証する仕組みが必要になることがあります。ここでは例として、会員限定のイベントに入場する際に、入場者が会員証として NFT を提示するケースを考察します。このようなオフチェーンでの検証は、オンチェーンでの検証ほど簡単ではありません。ここでは、この検証方法について、いくつかの例を示します。

簡単的な検証方法として、スマホのウォレットに NFT の画像を表示して入場時に提示することでオーナーであることを示します。しかし、この方法には大きな問題があります。典型的な NFT の画像は IPFS から誰でも取得できるため、同じ画像を使って偽の NFT を作成するとか、スクリーンショットを別のスマホで表示することが可能です。したがって、NFT のオーナーでなくても、この検証を通ることができます。この問題点を許容できるようなケースに限って、この方法を用いることが出来ます。

厳密な検証方法の一例として以下のような手順があります。

・入場ゲートにて、ワンタイムの乱数（チャレンジ）を含む QR コードが表示される。
・入場者は自身のスマホアプリでその QR コードを読み取る。
・入場者のスマホアプリは、所定の形式のトランザクションを作成し、NFT のオーナーのウォレットで署名する。作成するトランザクションには以下の情報が含まれる。
　会員証となる NFT のトークン ID
　読み取ったチャレンジ
・トランザクションが検証者のサーバに送られる。
・検証者のサーバは、以下の検証を行う。
　トランザクションが所定の形式であり、正しく署名されているか
　入場ゲートで表示したチャレンジと、トランザクションに含まれるチャレンジが一致すること
　ブロックチェーン上の NFT コントラクトに問い合わせて、トランザクションに含まれるトークン ID の NFT のオーナーのアドレスを取得し、それがトランザクションを署名したアドレスと一致すること
・上記検証がすべて成功した場合に限り、入場ゲートが開く。

この方法による検証は非常に正確ですが、トランザクションへの署名を利用するシステムが複雑であり、設計に比較的に高いコストがかかるという難点があります。厳密な本人確認が必要な場合には、このような方式になるでしょう。

第三の方法として、証明書 NFT を使って検証する方法があります。入場者はウォレットに会員証 NFT と顔写真 NFT を持っているとします。検証者はブロックチェーン上の NFT コントラクトに問い合わせて、これら 2 つの NFT が同じオーナーであることを確認し、顔写真 NFT の画像と入場者の顔を照合して検証します。
検証のチェーン：　会員証 NFT⇔オーナー⇔顔写真 NFT⇔入場者の顔

この方式は、設計が比較的に容易であり、また、さまざまな応用が可能です。

まとめ

ブロックチェーンを利用するアプリケーションの設計ガイドとして、NFT の構成や考え方、NFT の用途、BC+での NFT の利用方法などを説明しました。