



Innovative R&D by NTT

スマートプロパティの概要と コンテンツ管理への適用

2016年5月18日

NTTサービスエボリューション研究所

大橋盛徳

- スマートプロパティとは？
- NTTサービスエボリューション研究所のスマートプロパティ型コンテンツ管理への取り組み

- ブロックチェーン技術の最初の実装は仮想通貨
ビットコイン
 - ビットコインとしての実装は2009年から無停止で稼働し続けている(=技術の壮大な実証実験)
- ブロックチェーン技術の有効性の証明



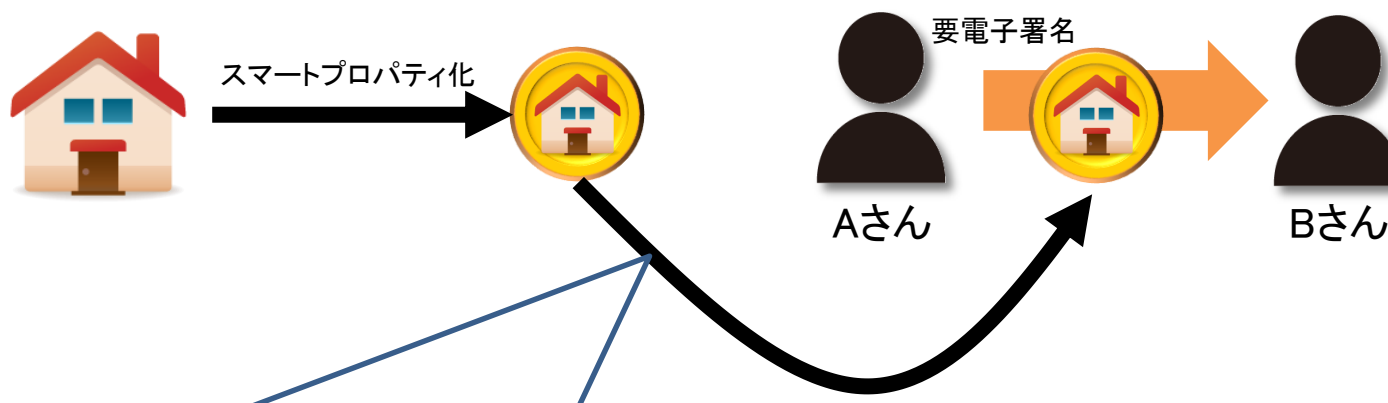
通貨だけでなく、広く資産の流通に応用できるのではないか

→ スマートプロパティへ注目

スマートプロパティとは何か？

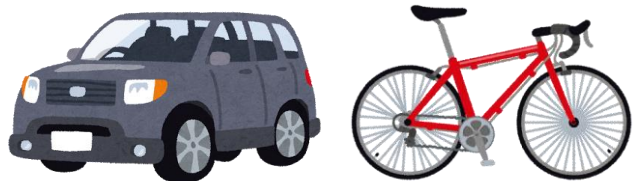


A. ある資産（プロパティ）を仮想通貨のようにコンピュータネットワーク上で流通できるようにしたもの



プロパティの情報を含むコインを生成し、
そのコインをブロックチェーン上で流通。
ブロックチェーン技術の高い改竄耐性で、資産情報を保護

スマートプロパティ化が検討される 資産の一例



車両

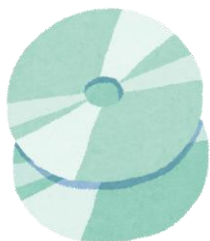
(売買、レンタル、シェアリングなど)



株式



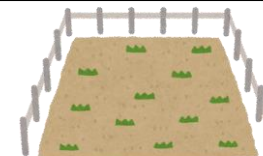
債権



映像・音楽作品



センサーデータ



土地



ライフログ



チケット



建物

(売買、レンタル、
シェアリングなど)

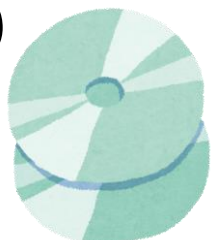
→ ブロックチェーン技術ならではのキラーサービスはまだない

スマートプロパティ化するには？



A. ある資産（プロパティ）を一意に特定する情報を
コインに記載する

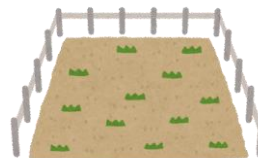
例)



映像・音楽作品



ハッシュ値



土地

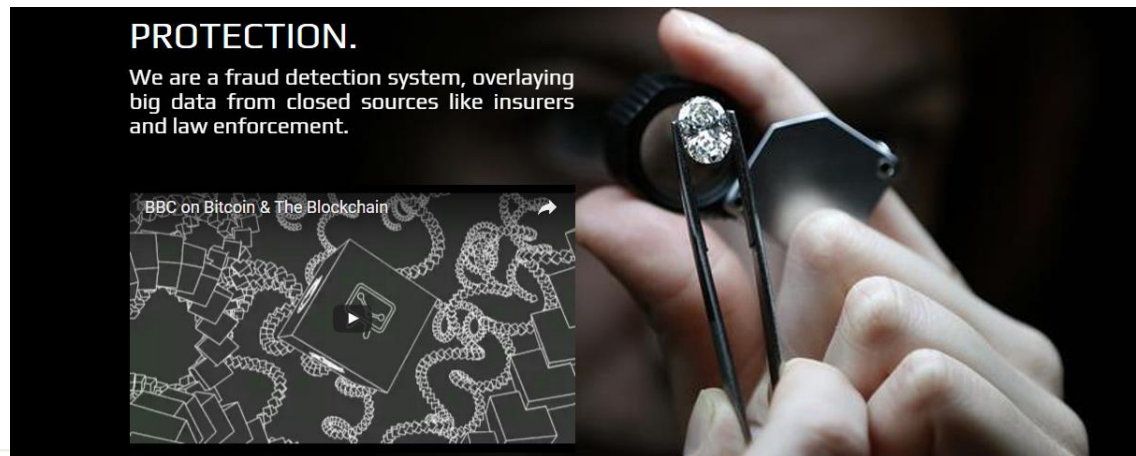


地番



ただし、問題もあり、
だれでも登録できたら架空のコインを作れてしまう
→ 初期情報の登録が大きな課題

- ダイヤモンドの盗難やダイヤモンドに関する保険金詐欺に対抗する目的のプロジェクト
- ダイヤモンドを特定するためにその特徴をメタデータとして記録する
- メタデータとして4C以外に40もの特徴量をメタデータとして記録する



引用： <http://www.everledger.io/>

仮想通貨とスマートプロパティの違い

	仮想通貨	スマートプロパティ
	 <p>ブロックチェーン</p>	 <p>ブロックチェーン</p>
紐づく対象の有無	<ul style="list-style-type: none">通貨のため特定の対象に紐づかない	<ul style="list-style-type: none">ブロックチェーン外に紐づく対象がある
コインとしての性質	<ul style="list-style-type: none">二重支払いはNG価格の最小単位で分割可能	<ul style="list-style-type: none">プロパティによっては多重複製は有効プロパティによっては単位が固定で分割や結合ができないものも
コインの生成	<ul style="list-style-type: none">マイニング(ブロックチェーンの維持管理のため系に内在する仕組み)	<ul style="list-style-type: none">人の手による情報登録/発行 → 対象のない架空のコイン発行の可能性あり

→ 仮想通貨専用のブロックチェーンプラットフォームではスマートプロパティを実現するのは困難であり様々なプラットフォームが提案されている

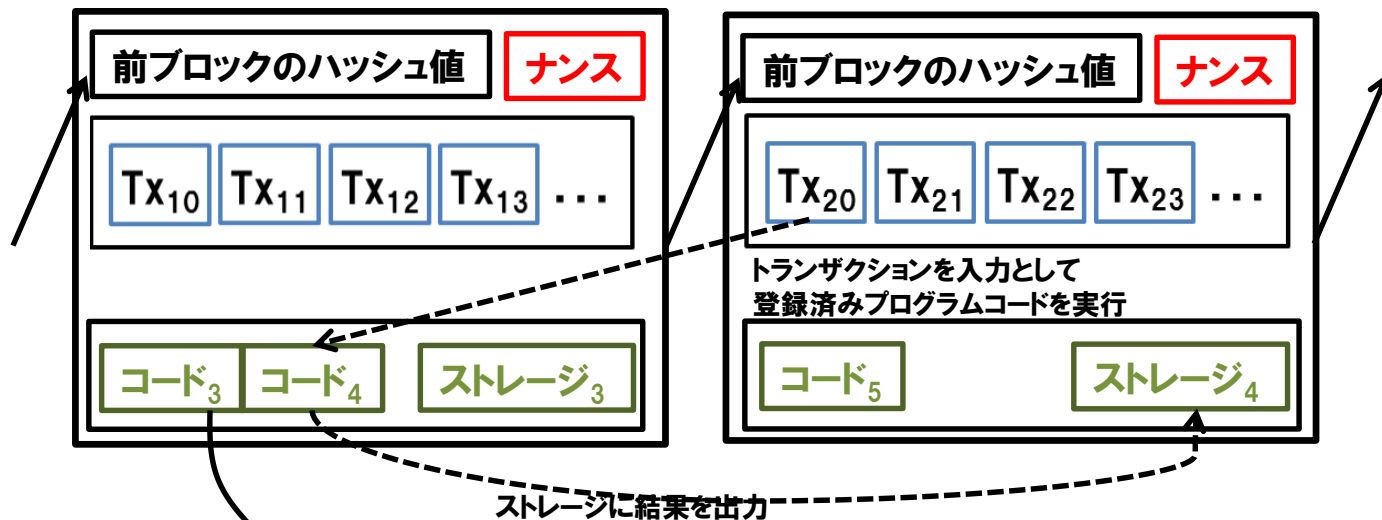
プログラムコードを埋め込める ブロックチェーンの登場



スマートプロパティでは、プロパティに応じて載せる情報や流通に伴う処理が各々異なる

- プログラムコードをブロックチェーンに埋め込み、任意の処理を実行させられる新しい概念のブロックチェーンの登場
- 代表例「Ethereum」

■ プログラムコード埋め込み型ブロックチェーンのデータ構造イメージ



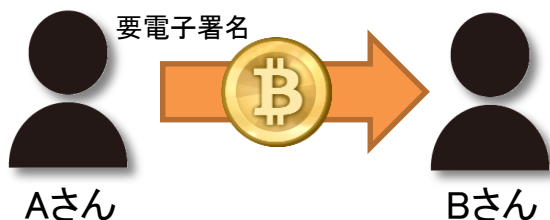
利用者はプログラムコードをブロックチェーンに登録可能
トランザクションを介して登録済みのコードを実行する

プログラムコード埋め込み型ブロックチェーン登場前はどのようにしてたか？



ビットコインのトランザクションにはスクリプト領域があり、その中で自由記述可能な部分がある。その領域を工夫して利用。

■ トランザクション



■ 実データ(バイト列)

基本的には入金額=出金額(お釣りは手数料)

入力	直前のトランザクションハッシュ	
	署名検証スクリプト	Aさんの公開鍵 署名値(上記を暗号化した値)
出力	出金額	
	宛先(Bさんアドレス)指定スクリプト	

この中に自由記述可能部あり

実現可能な
アプリケーション

- ・ファイルのハッシュ値を記載 → ある時点での存在証明サービス
- ・数値を記載 → 独自のポイントサービス

- スマートプロパティとは？
- NTTサービスエボリューション研究所のスマートプロパティ型コンテンツ管理への取り組み

背景:コンテンツの生成と消費の変化



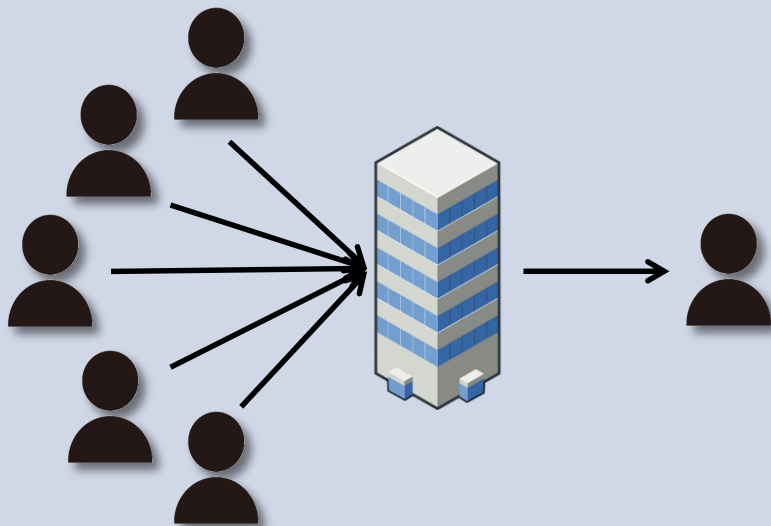
一般消費者は単なる消費者から情報の発信者へ

→ 一般消費者も含めた制作者の権利を保護しながら流通を支援する仕組みが求められる



- 既存の中央集権型のコンテンツ流通ではあらゆる権利者のニーズを同時に満たすことは難しい
- ブロックチェーン技術を活用することで、多くの関係者が関与した場合でも、特定の組織に依存しない柔軟な形態を実現可能

中央集権型コンテンツ流通



ブロックチェーン応用コンテンツ流通

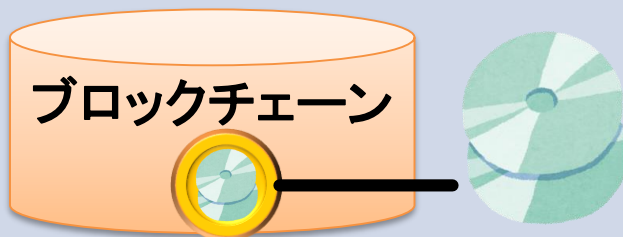


個対個の構造にも中央集権構造にもできる！

コンテンツのスマートプロパティにおける特徴と実装の工夫



スマートプロパティ



紐づく対象の有無	<ul style="list-style-type: none">ブロックチェーン外にコンテンツファイルがある
コインとしての性質	<ul style="list-style-type: none">利用権としてのコインは権利者が自由に複製し、流通できる
コインの生成	<ul style="list-style-type: none">コンテンツ制作者による情報登録/発行→ 他人のコンテンツを自身のコンテンツとして登録することを防ぐ必要がある

ハッシュ値を一意的IDとして利用

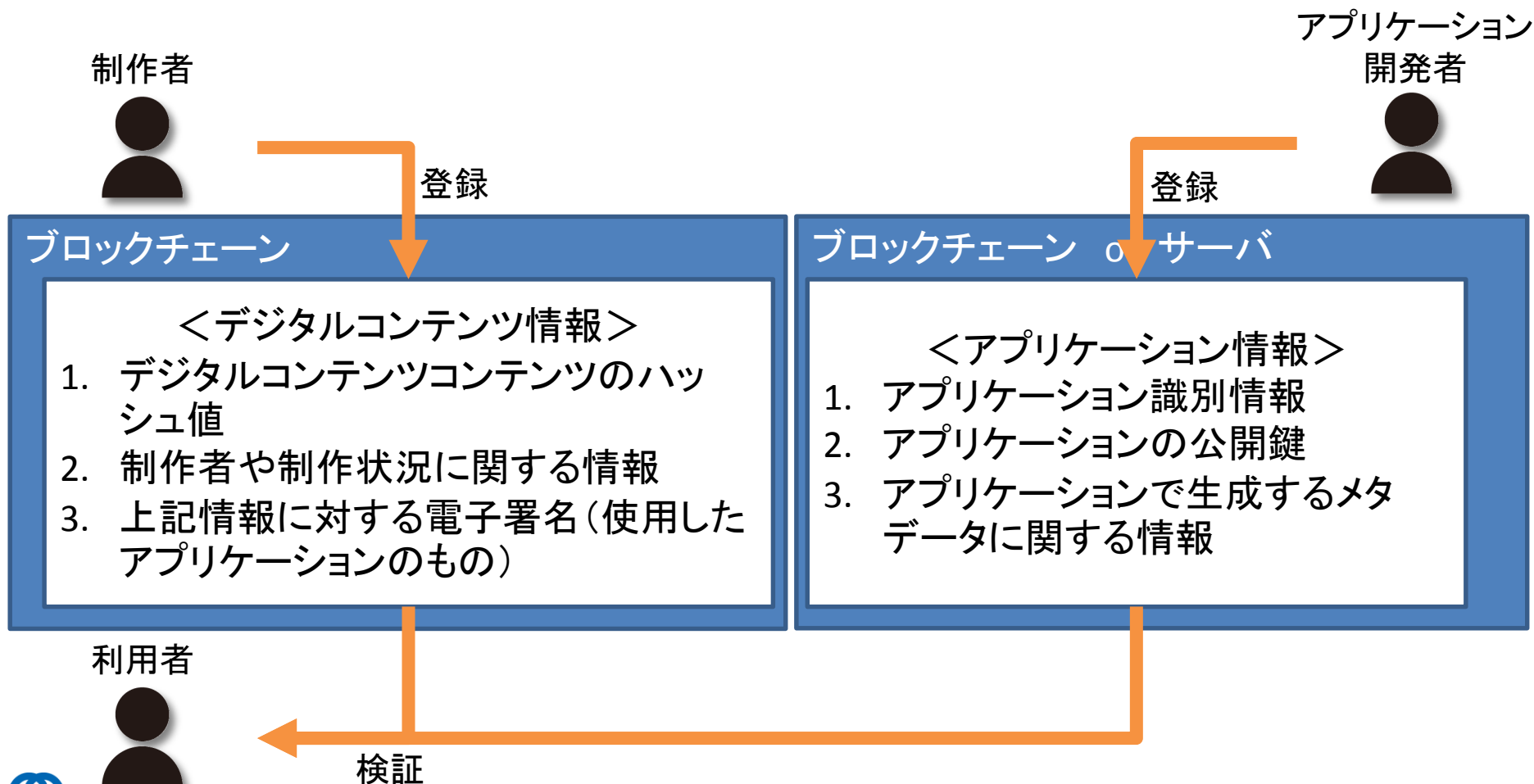
ブロックチェーン内に埋め込むプログラムコードによる処理で実現

特定のアプリで生成した瞬間にコンテンツを登録しコイン化。その際に、生成状況メタデータとアプリの電子署名も付与させることで、情報偽装を防ぐ

情報偽装を考慮した登録方式



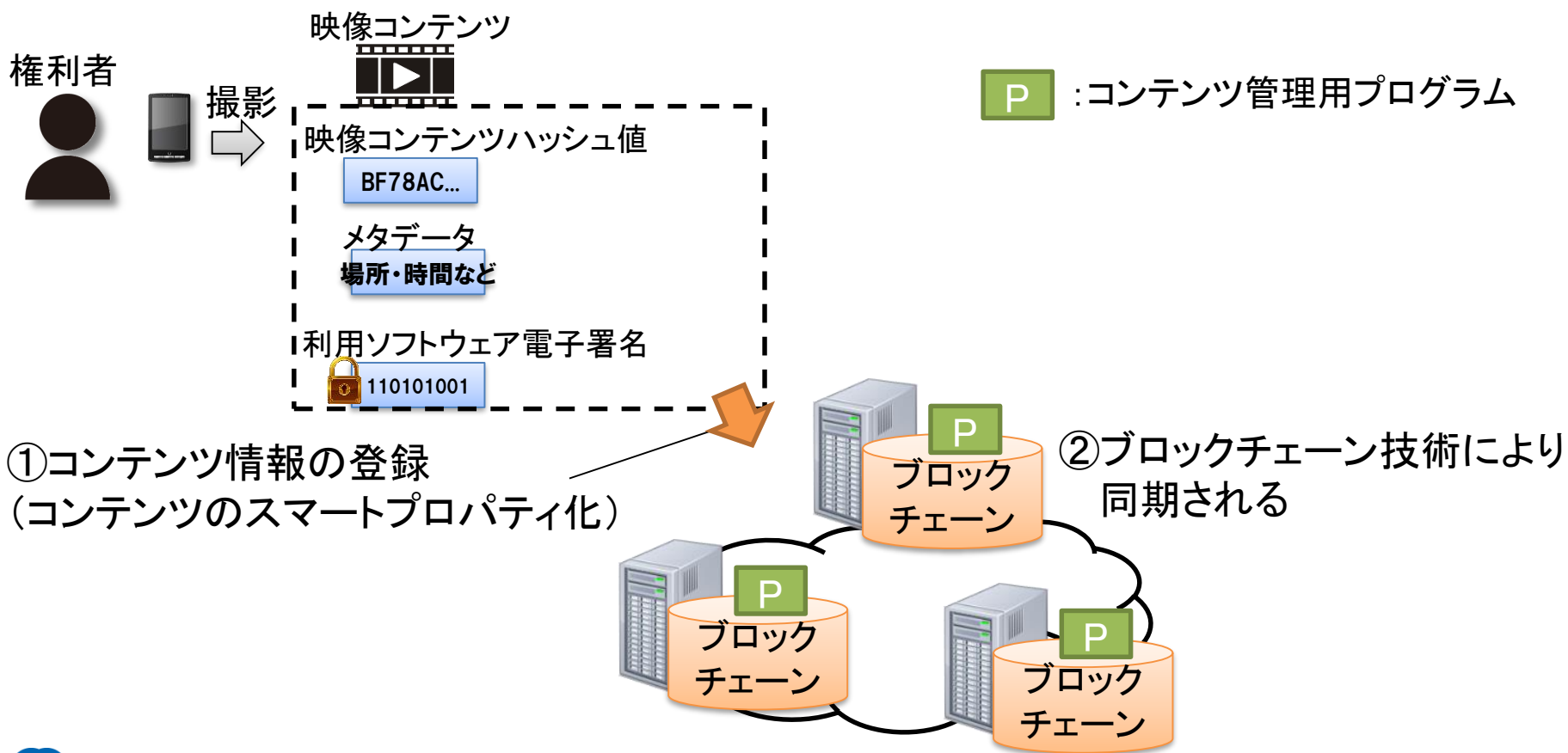
電子署名付きのデジタルコンテンツ情報をブロックチェーンに登録し、アプリケーション情報を利用し、検証可能にする



ブロックチェーンを利用した コンテンツ管理方式の概要（登録時）



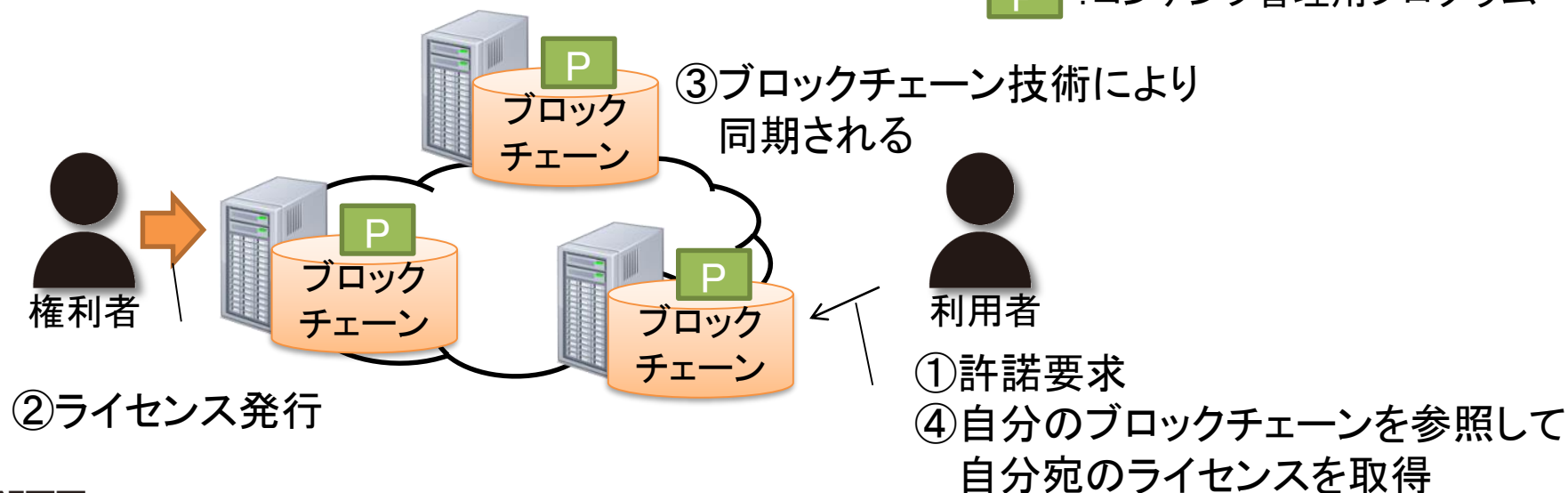
- コンテンツを作成した瞬間にコンテンツのハッシュ値とメタデータと利用したアプリの電子署名を付けてブロックチェーンに登録



ブロックチェーンを利用した コンテンツ管理方式の概要(利用時)

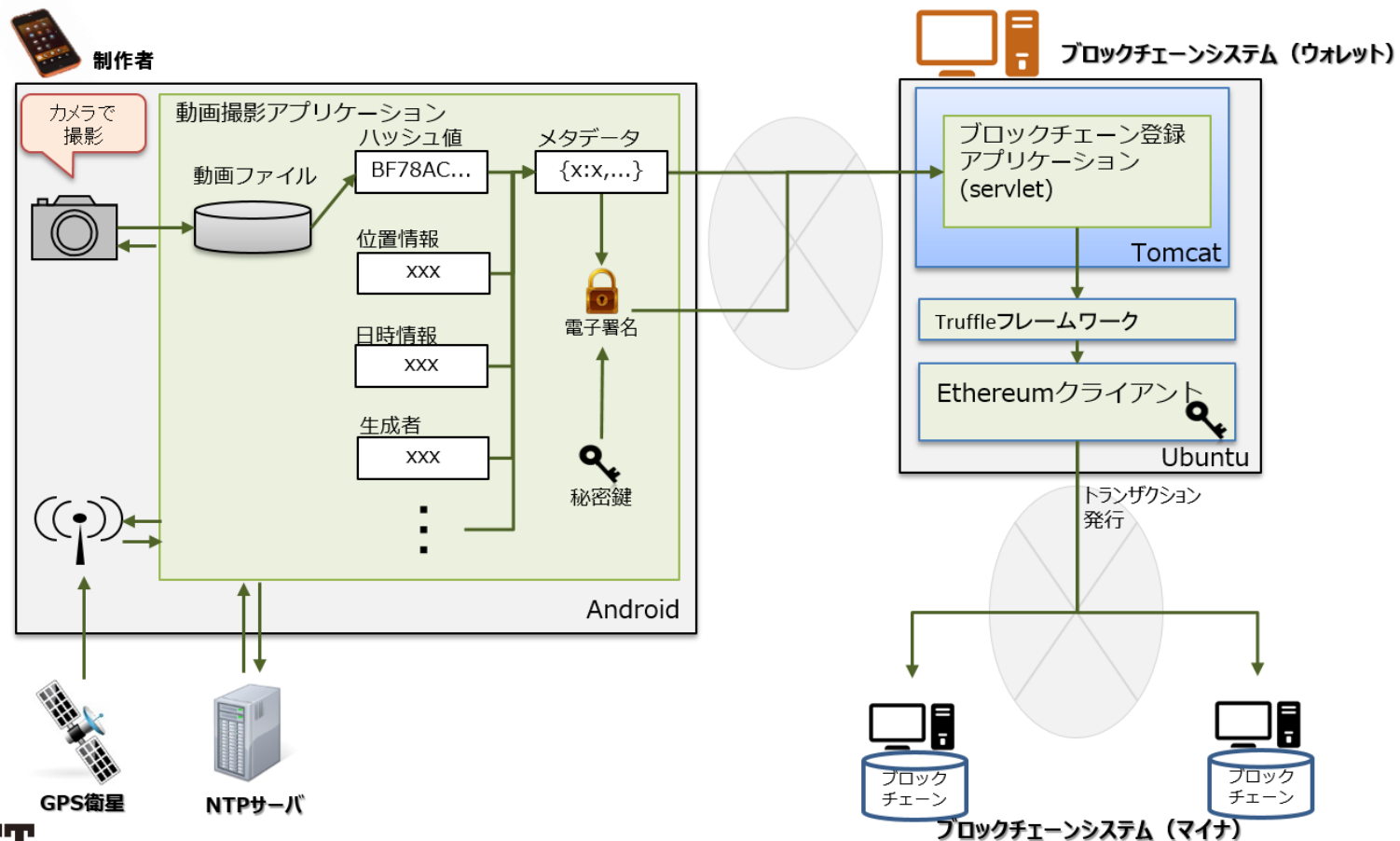
- 利用者は権利者を知らなくともブロックチェーンを介して許諾要求を行える
- 権利者は利用者からの許諾要求に対して直接ライセンス発行を行える
- ライセンスや復号鍵はブロックチェーンに記録され、ライセンスサーバを用意する必要が無い

P : コンテンツ管理用プログラム



コンテンツ管理方式の実装概要

ブロックチェーンプラットフォームとしてプログラムコードを埋め込める特徴のあるEthereumを使用し、実装した。Androidアプリで登録情報を作成し、その登録情報をEthereumのブロックチェーンに書き込んでいる。

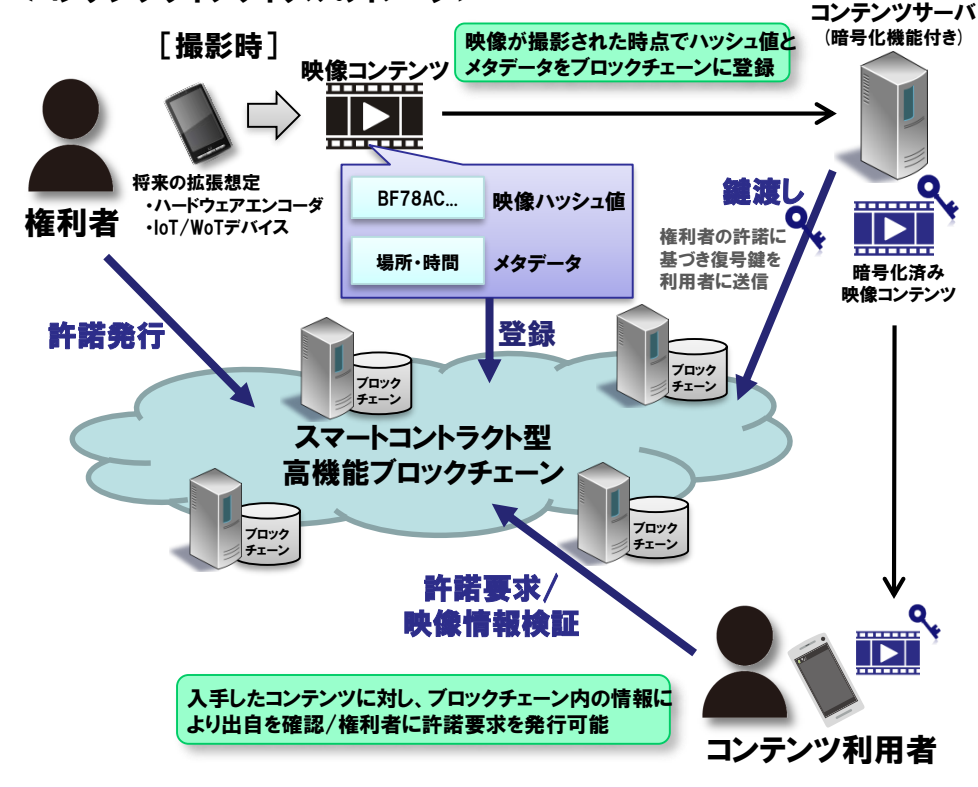


コンテンツの信憑性を検証可能な仕組み

Verifiable mechanism for content authenticity

超高臨場感サービスでは画像処理により加工した映像や複数素材を合成した映像を活用することがあり、オリジナルコンテンツの情報や権利処理が正当に行われていることを誰でも検証可能であることが求められます。また、無加工・無改竄なコンテンツであることが重要な場面もあります。ブロックチェーン技術^(※1)を活用した仕組みで、コンテンツの正当な権利許諾や編集の履歴を保証します。

<コンテンツライフサイクルのイメージ>



特徴

- 映像が撮影された瞬間にメタデータと共にブロックチェーンに情報が登録されることで制作者やオリジナリティを保証可能
- 入手したコンテンツの出自をブロックチェーン内の情報から検証可能
- コンテンツの制作者自身が直接的にコンテンツの利用許諾や譲渡等の権利処理を実行可能

利用シーン

- コンテンツの真正性や権利処理が正当に行われていることを証明するためのサービス
- いつ・どこで・誰が撮影した映像かを明確化し、イベント主催者が限定的なコンテンツ流通を許可することで、イベントの更なる活性化に貢献
- 作業完了証明やドライブレコーダーなど証拠性が重要な映像の記録

※1 ブロックチェーン技術: 公開ネットワーク上で全ての履歴を記録した台帳(ブロックチェーン)を中央集権機構によらずに堅牢に形成するための技術

NTT R&Dフォーラム 2016 デモ風景



F-11 コンテンツの信憑性を検証可能な仕組み

Verifiable mechanism for content authenticity

超高解像度サービスでは画像処理により加工した映像や複数素材を合成した映像を活用することがあり、オリジナルコンテンツの信憑性や権利処理が正当に行われていることを誰でも検証可能であることが求められます。また、加工・合成されたコンテンツであることが重要な要素もあります。ブロックチェーン¹⁾を活用した仕組みで、コンテンツの正当な権利処理や複製の検知を可能にします。

1) ブロックチェーンとは、分散型ネットワーク上でデータの複製を必要としない状態で、ブロックチェーンを利用することで、複製検知が容易に実現できる仕組みです。

2) 複製検知は、複製された映像にメタデータと共にブロックチェーンに情報を登録することで制作者やクリエイターを証明します。

3) 入手したコンテンツの出発をブロックチェーン内の情報から検証可能

4) コンテンツの制作者自身が直接的にコンテンツの利用許諾や譲渡等の権利処理を実行可能

5) コンテンツの真正性と権利処理が正当に行われていることを証明するためのサービス

6) いつどこでも誰が撮影した映像かを明確化し、イベント主催者が限定したコンテンツ流通を許可することで、イベントの更なる活性化に貢献

7) 作業完了証明やライブレコーダーなど信頼性が重要な映像の記録

- 開催日: 2016/2/18(木)・19(金)
 - 会場 : NTT武蔵野研究開発センター
- Copyright©2016 NTT corp. All Rights Reserved. 20



- スマートプロパティとは、ある資産（プロパティ）を仮想通貨のようにコイン化したもの
- 資産との紐付けが重要なポイント
- 高度なブロックチェーンプラットフォームも出てきており実装できる土壌は整いつつある