デジタルサイネージ分野におけるブロックチェーン利用の検討

ccatak / https://cc-res.com**管理人**
Email: ccatak@cc-res.com
Website: https://cc-res.com

講演資料の公開場所： https://cc-res.com/dsgnenjiss_attachment_20190629/

Agenda

ブロックチェーンについて

- 原義的なブロックチェーン
- しくみ
- 特徴
- 拡張性（スマートコントラクトとオラクル）
- パーミッションレスブロックチェーンとパーミッションドブロックチェーン

デジタルサイネージについて

- システムモデル
- 用途（広告配信と情報提供）
- ステークホルダー
- 拡張技術

デジタルサイネージにおけるブロックチェーンの利用について

- メタデータ管理
- 広告枠細分化と動的プライシング
- 公共性担保

ブロックチェーンについて

Satoshiは始まりの論文で何を語ったか

- 「信頼できる第三者機関」を介することによる不可逆性の問題と、「信頼できる第三者機関」がいないと発生してしまう二重支払い問題を同時に克服する電子決済システムを提案した。
- 暗号理論を基盤にP2Pネットワークが処理する機構とすることで、「信頼できる第三者機関」を排する。

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Satoshiの問題意識

「信頼できる第三者機関」を介する電子決済は、だいたいうまくいくが、信頼ベースのモデルの弱点＝取引の不可逆性がないことの問題に悩まされている。例えば…
- 少額決済ができない。
- 顧客に多くの情報を求める。
- 一定割合の詐欺は不可避である。

電子署名を利用することで一部解決できるものもあるが、二重支払い防止のために「信頼できる第三者機関」が間に入ってしまうと、結局信頼ベースモデルの弱点が露顕する。

Satoshiの提案

「信頼できる第三者」を介さず、「暗号理論の裏付け」に基づいて二者間の直接取引が可能で、かつ二重支払いも防ぐ電子決済システム。
⇒信頼ベースモデルの弱点を克服しつつ二重支払いも防ぐ。

P2Pネットワークがトランザクションをハッシュ化し、タイムスタンプを押してプルーフオブワークのチェーンに記録する。プルーフオブワークをやり直さない限り記録を変更することはできない。
さらに最長のチェーンが正であるので、ハッシュパワーの半数以上を良心的なノードが掌握している限り、良心的なノードの行うプルーフオブワークの速度が攻撃者のプルーフオブワークの速度を上回るので攻撃者は改竄できない。

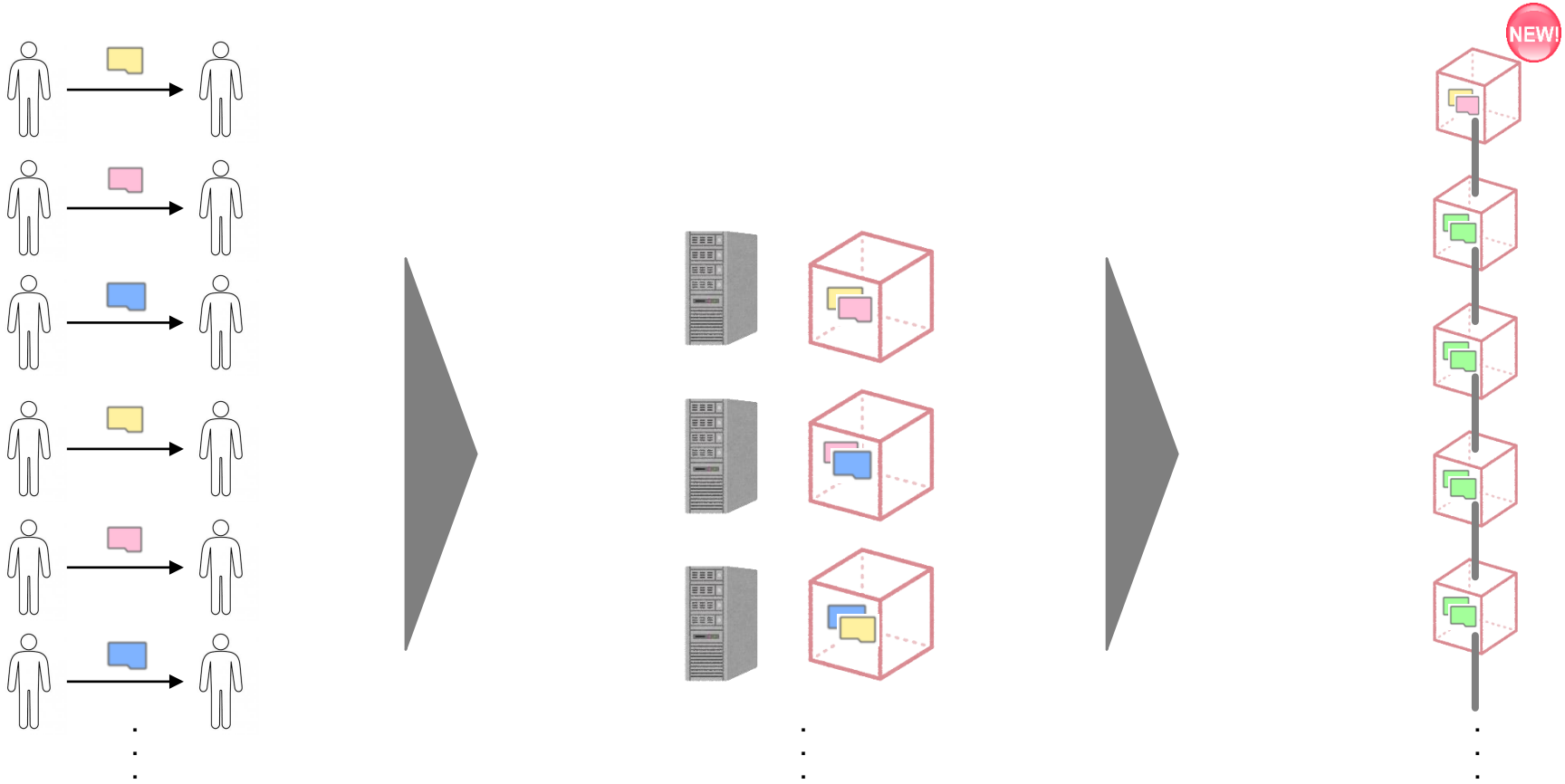
用語の定義

- 押さえておきたい主な用語を以下に整理。噛み砕いて表現した「ざっくり理解」のイメージだけ持っていればひとまず困ることはない。（注：以降、しばらくビットコインのブロックチェーンについて見ていきます。）

	用語	本稿での定義	ざっくり理解
1	ブロックチェーン	✓ ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装	✓ ブロックの積み重ね ✓ 改竄が難しい性質を持つ
2	ブロック	✓ 自身と直前のブロックを説明する情報並びにいくつかのトランザクションを主な成分として含む構造体	✓ トランザクションの集まり
3	トランザクション	✓ あるユーザから他ユーザへの価値の移転を主な成分として含む構造体	✓ 何らかの移動（今回は特に送金）
4	P2Pネットワーク	✓ 不特定多数の「ノード」からなる ネットワーク	✓ ノードがつながったもの
5	ノード	✓ ブロックチェーンにおいてブロックの生成やメッセージの伝達等を含む複数の役割を担うもの	✓ 縁の下の力持ち、便利屋さん
6	コンセンサス	✓ データのステートに関してノード間で行われる合意	✓ 合意

ブロックチェーンに1つブロックがつながるまでのざっくりした流れ

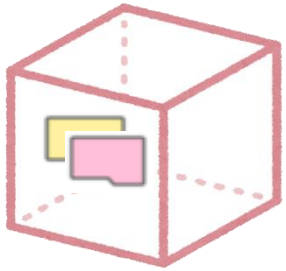
- ①たくさんのユーザがトランザクションを発行する。
- ②複数のノードがそれらのトランザクションを各々自由に見繕ってブロックにまとめる。
- ③そのうちの1つだけが有効とされてブロックチェーンにつなげられる。



理解：なるほど！トランザクションを発行するとブロックにまとめられて、そのうちの1つがブロックチェーンにつながるんだね！
疑問1：あれ？でも、「つながる」ってどういうことだろう。URLのリンクでも貼ってるのかな？（⇒p7）
疑問2：あれ？どうやってたくさんあるブロックの中から1つを決めるのかな？（⇒p8）

ブロックの構造

- ブロックの構造を表に整理。
- ブロックヘッダ（メタデータ）内にある「親ブロックのハッシュ」により、親ブロック（前のブロック）につながる。



これが前のブロックの参照。
つまり、前ブロックの表2の情報
を要約したデータを持っている。

表1 ブロックの構造

フィールド名	説明	データサイズ
マジックナンバー	0xD9B4BEF9固定、ネットワークを識別	4バイト
ブロックサイズ	ブロックヘッダ～トランザクションまでのブロックサイズ	4バイト
ブロックヘッダ	ブロックのヘッダ情報。メタデータ、	80バイト
トランザクションカウンタ	ブロック内のトランザクション数	1-9バイト
トランザクション	トランザクションのリスト	可変

表2 ブロックヘッダ（メタデータ）の構造

フィールド名	説明	データサイズ
バージョン	ブロックのバージョン	4バイト
親ブロックのハッシュ	親ブロックのブロックヘッダをハッシュ化したもの	32バイト
マークルルートハッシュ	ブロック内の全トランザクションをハッシュ化したもの	32バイト
タイム	ブロック生成時のタイムスタンプ	4バイト
ビット	ブロック生成時のプルーフオブワークの難易度	4バイト
ナンス	0から始まる32ビットの数字	4バイト

※ハッシュとは、あるデータを不可逆的に要約したもの。少しでも元データが変わると、ハッシュも全く異なるものになる。右にSHA-256でハッシュ化した例を示す（戻り値は32バイト→64文字）。

SHA-256(ccatak) ⇒BEBEFB94BE7D44DE87492B704DDCD2B0AD80C900C0E53E815918424175C9B37B
SHA-256(cca_tak) ⇒584BB788DAF7CD8E3AC91C080B239470F300D125F13D3CFB9F3BF84BDF930888
SHA-256(cc_atak) ⇒A39C2D004DA56DA16DAE065075393855CFEC8035BCA82105E85F8D74D64DA421
SHA-256(https://cc-res.com/) ⇒7CCCEBBB93B9096DF9B9B45657889D12C4414CE4788BEAC6264FC1FC93253D6A

理解:なるほど！前ブロックのブロックヘッダを要約したデータを持つことでつながるんだね！元のブロックヘッダの情報を直接持つよりもデータサイズはより小さくなる(80バイト⇒32バイト)し、エコだね！

ブロックの選び方(プルーフオブワーク)

- ブロックヘッダ内にある「親ブロックのハッシュ」、「マークルルートハッシュ」、「ナンス」の3つをハッシュ化して予め決められている値より小さな値を見つける競争を行う。最初に見つけたノードがブロックを生成できる。

ネットワーク

ネットワーク：
0が最初から17個続くハッシュを見つけたノードを勝ちとする。

表2 ブロックヘッダの構造

	フィールド名	説明	データサイズ
	バージョン	ブロックのバージョン	4バイト
全ノード共通 →	親ブロックのハッシュ	親ブロックのブロックヘッダをハッシュ化したもの	32バイト
ノードごとに異なる →	マークルルートハッシュ	ブロック内の全トランザクションをハッシュ化したもの	32バイト
	タイム	ブロック生成時のタイムスタンプ	4バイト
	ビット	ブロック生成時のプルーフオブワークの難易度	4バイト
試行回数ごとに異なる(1ずつ増やしていく) →	ナンス	0から始まる32ビットの数字	4バイト

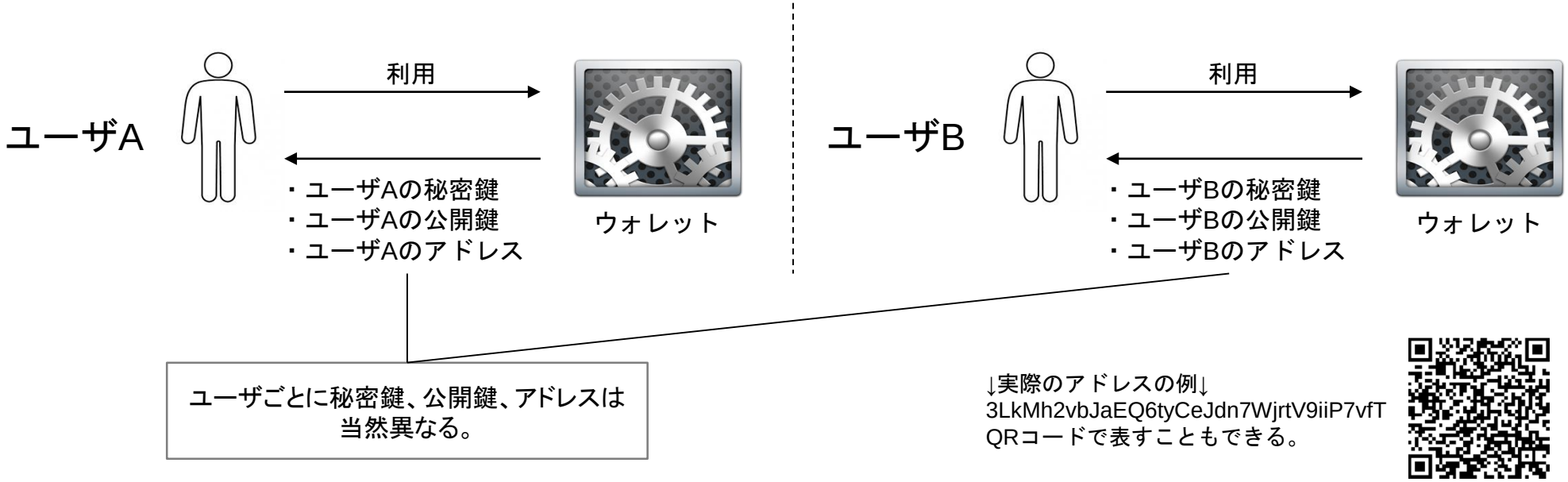
	Proof-of-Work	1回目	2回目	…	740825940回目
ノードA	親ブロックハッシュ	DFA73B59D0…	DFA73B59D0…		DFA73B59D0…
	マークルルートハッシュ	3D3BEED2BA…	3D3BEED2BA…		3D3BEED2BA…
	ナンス	0	1		740825940
	結果(ブロックハッシュ)	14045AA295DD2… ✖	954088627AAD… ✖		0000000000000000F… ○
ノードB	親ブロックハッシュ	DFA73B59D0…	DFA73B59D0…		DFA73B59D0…
	マークルルートハッシュ	859DD5DB85…	859DD5DB85…		859DD5DB85…
	ナンス	0	1		740825940
	結果(ブロックハッシュ)	A7845095F0090… ✖	0008DDFAFACC… ✖		96540FCCDBB… ✖
ノードC	親ブロックハッシュ	DFA73B59D0…	DFA73B59D0…		DFA73B59D0…
	マークルルートハッシュ	9AC21989CD	9AC21989CD		9AC21989CD
	ナンス	0	1		740825940
	結果(ブロックハッシュ)	004357FFADCD… ✖	54829DDF44C8D… ✖		ADF000890470… ✖

※実際の計算速度はハッシュパワー依存なので同じ時間当たりの計算回数はノードごとに異なります。Aが100回計算している間にBは10000回計算しているということもあります。

理解:なるほど！最初に条件を満たす小さなハッシュを見つけたノードだけがブロックを生成できるんだね！
疑問3:あれ？でも、トランザクションってどうやって相手に届くの？ブロックに取り込まれて、ブロックチェーンに刻まれたけど、まだ相手に届いてないよね。というかそもそも相手ってどうやって分かるんだっけ？(⇒p9)

ユーザの識別：アドレス

- ユーザはアドレスで識別する。
- アドレスは公開鍵をもとに作られる。公開鍵は秘密鍵から作られる。
- ウォレットというソフトウェアを使うと秘密鍵・公開鍵のペアとアドレスを作ってくれる。



理解：なるほど！アドレスでユーザが分かるんだね！
疑問4：あれ？でも、そのユーザが持っている所持金ってどうやって分かるの？それが分からないと送金できないよね。銀行みたいに、アドレスが口座のような役割を果たすの？（⇒p10）

トランザクションの構造

- アウトプットトランザクション（Tx-out）では、金額と、相手先の情報と相手が利用するための条件（ScriptPubKey）を記述する。
- インプットトランザクション（Tx-in）では、自分宛てに送られた未使用のTx-outを指定し、そこに記載された利用条件を満たすよう情報を提示する（ScriptSig）。

トランザクションの構造

フィールド名	説明	データサイズ
バージョンナンバー	バージョン	4バイト
フラグ	あれば0001で、Wウィットネスがあることを示す	あれば2バイト、なければ0バイト
インプットカウンタ	Tx_inの数	1-9バイト
インプットリスト	Tx_inのリスト	Tx_inの数による
アウトプットカウンタ	Tx_outの数	1-9バイト
アウトプットのリスト	Tx_outのリスト	Tx_outの数による
ウィットネス	あれば1インプットにつき1ウィットネス	可変
ロックタイム	トランザクションのロックが解除されるブロック高かタイムスタンプ、ロックなしの場合は0	4バイト

インプットトランザクション(Tx_in)の構造

フィールド名	説明	データサイズ
前Tx_outのハッシュ	このインプットが参照している前Tx_outのハッシュ	32バイト
前Tx_outのインデックス	このインプットが参照している前Tx_outのインデックス	4バイト
入力者のスクリプト長	入力者の署名スクリプトの長さ	1-9バイト
入力者の署名スクリプト（ScriptSig）	入力者を確認するためのスクリプト、入力者の秘密鍵による電子署名と公開鍵を含む	可変
シーケンス	送信者が定義するトランザクションのバージョン	4バイト

アウトプットトランザクション(Tx_out)の構造

フィールド名	説明	データサイズ
値	トランザクションの送金額	8バイト
出力先のスクリプト長	出力先のスクリプトの長さ	1-9バイト
出力先のスクリプト（ScriptPubKey）	出力先の公開鍵を用いて値を引き出すための条件を記述したスクリプト	可変

（補足）
①あるユーザAがユーザBに送金するとき、Tx-outに送金額を含むユーザBの情報を記述する。Tx-inに過去に誰かからユーザAに送られた未使用のTx-outを指定して送金に十分な金額を引き出す。
②トランザクションも別のトランザクションを参照するような構造をとっている。各ユーザのその時点の所持金の計算は、過去のトランザクションを遡って行う。
③履歴を辿り計算するのではなく、銀行口座のようにアカウントを設けて管理しているブロックチェーンもある。

理解：なるほど！トランザクションもブロックみたいに参照構造を持っていて、それを使って送金したり、履歴を辿って計算して所持金を求めたりするんだね！

ブロックチェーンの特徴（主に機能面）

❑ 機能面の主な特徴として、下記に挙げるようなものが考えられる。

	特徴	説明
1	記録のテクノロジであるが 物理的に何かを生成する技術ではない	✓ ブロックチェーンは基本的には何らかのデータ、並びにデータの変化を記録する技術 ✓ 物理的な何かを生成する技術の代替は不可（当然車やPC等を制作することはできない）
2	電子データの生成やロジックの記述ができるが 大きなデータや重たいロジックは扱えない	✓ スマートコントラクトを利用して電子的なデータの生成やデータの処理ロジックを記述可能 ✓ ノード側のリソースの問題から大量のデータを書き込んだり重いロジックを実行することは困難
3	透明性と追跡性があるが プライバシーの心配がある	✓ トランザクションは全て記録され、誰でも閲覧できる状態に置かれており高い透明性と追跡性があり不正がないことを証明可能 ✓ ひと度現実のアイデンティティと紐づくとブロックチェーンの解析によりかなりのプライバシー情報を推測可能
4	耐障害性があるが 設計に注意が必要	✓ ノードにブロックチェーン自体を持たせることで、ネットワークに障害が発生しても正常に動作 ✓ ブロックチェーンを維持するノードのふるまいやネットワーク分裂時の対応などに関して繊細な設計が必要
5	入力を正しいものとして処理するが 入力自体の正しさを保証しない	✓ 入力を正しいものとして処理し、記録し、正しく処理されたことを保証 ✓ 入力自体が正しいかどうかについては保証不可（例えばX⇒Yの送金トランザクションがあったとして、本当に送信者がXさんか分からない）
6	改竄耐性を持つが ロールバックができない	✓ コンセンサスアルゴリズムに基づいてファイナライズによる高い改竄耐性 ✓ トランザクションの内容に間違いがあったり後から変更を加えたい場合でもブロックに取り込まれると後戻り不可
7	非中央集権により検閲耐性を得るが 多くのステークホルダーが絡む	✓ ブロックチェーンは中央で管理する主体を持たず、プロトコルに基づきネットワークが維持 ✓ プロトコルの更新等を行う場合、開発者だけでなくネットワークに参加しているノードの合意を得る必要があるなど、多数のステークホルダーが関係し改修が容易でない側面がある。

メリットか
デメリットかは
文脈依存

=

メリットが
デメリットを
上回る箇所で
使えるとよい

※より汎用的かつ抽象的に特徴をまとめるならば、最近のブロックチェーンには**「電子データの生成とロジックの記述」「データとデータ遷移の記録」「データとデータ遷移の追跡性」**が備わっている。これらはかなり普遍的なので様々な分野に応用できるポテンシャルを秘めている。

拡張性：スマートコントラクト/オラクル

- スマートコントラクトによりブロックチェーンがプログラマブルなものになる。オラクルにより、ブロックチェーン外の情報に基づいたスマートコントラクトの実装も可能になり適用領域がいっそう広がる。
- 拡張には課題もあるが、パーミッションドブロックチェーンはその性質から課題が相対的に軽い。

ブロックチェーンの拡張	説明
スマートコントラクト （チェーンコードと呼ばれることも）	✓端的に言ってしまえばブロックチェーン上のプログラム。 ✓データの処理ロジックと処理を行う条件を記載してブロックチェーン上にデプロイする。条件が満たされると、ブロックチェーンに参加するノードが処理ロジックを実行する。処理結果やステートはブロックチェーン上に保存される。 ✓処理不正の検出、処理結果の信頼性向上、処理結果の透明性などの点でメリットがある。実行の手数料（GAS）、処理の遅さなどは一般的なコンピューティングと比較した時のデメリットになると思われる。パーミッションドブロックチェーンでは高速コンセンサスアルゴリズムにより、処理の遅さが緩和される可能性がある。
オラクル（※）	✓ブロックチェーン外の情報に関するデータの正しさを検証し送信するフィードのような役割を果たすエンティティ。 ✓オラクルを利用することでブロックチェーン外の情報をトリガとするスマートコントラクトを実装可能になり、適用領域が広がる。 ✓オラクルに対する信頼を前提とする点に課題があると言われるがIntel SGXの利用やTLSnotaryの利用など、課題解消に向けた取り組みは存在する。また、そもそも中央集権的な主体（信頼できる主体）を想定しているパーミッションドブロックチェーンでは課題として認識されないかもしれない。

※DBやパッケージベンダのオラクル社のことを指すものではない（ただし、オラクル社がブロックチェーンに関する取り組みを行っている点は付け加えておく）

パーミッションレスブロックチェーンとパーミッションドブロックチェーン

- ブロックチェーンはパーミッションの違いで2つのタイプ（パーミッションレス/パーミッションド）に分類できる。
- 既存のビジネスシステムの置換や応用を目的とする場合、管理方式や処理速度の点で類似しているパーミッションドブロックチェーンが用いられやすい。

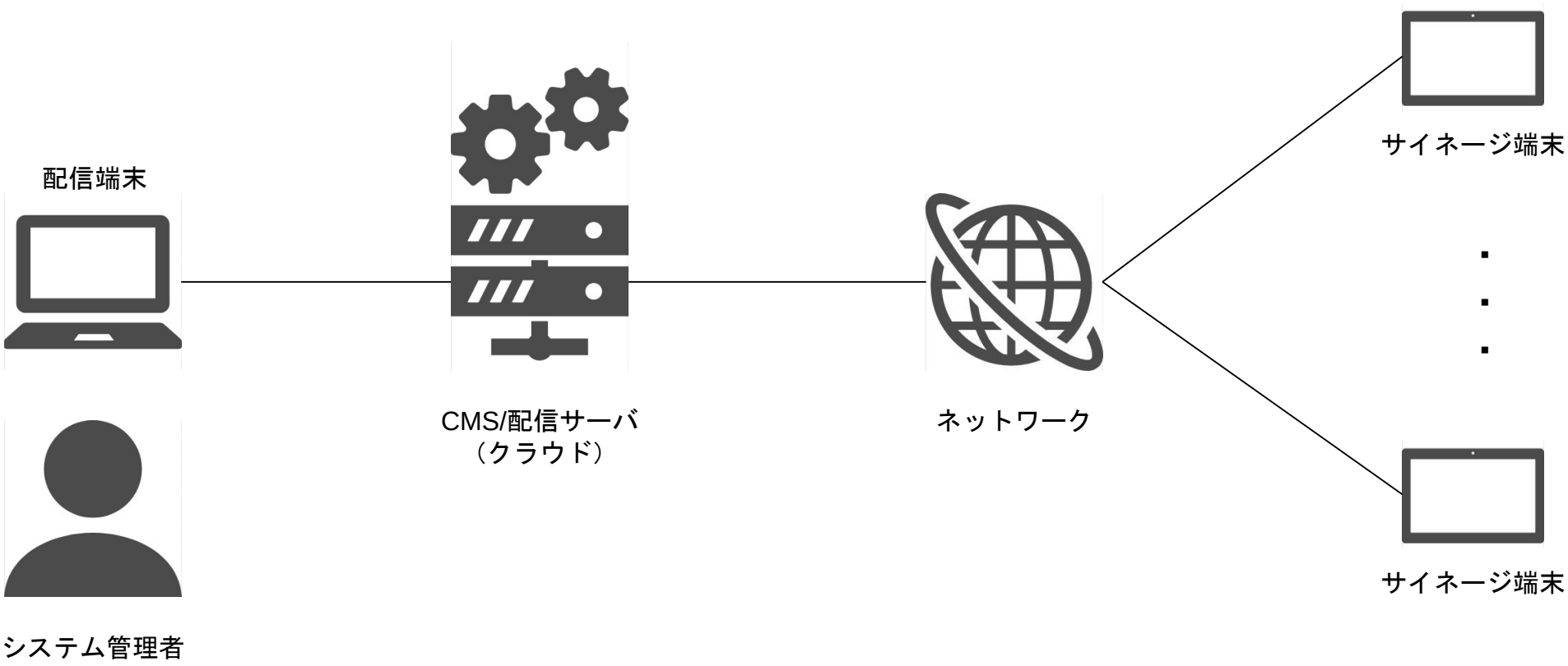
		パーミッションレス	パーミッションド
管理	1 管理主体	なし（プロトコルとインセンティブスキームにより制御）	あり
	2 ノード	身元が定かでない不特定多数のノードが自由に参加/退出	ノード数は少数で（定数があることも多い）、登録制であり、基本的に身元は明らか
スペック	3 改竄耐性	あり（ファイナリティはコンセンサスアルゴリズムによる）	あり（ファイナリティはコンセンサスアルゴリズムによる）
	4 処理速度	不特定多数のノードの合意が必要なため、基本的に低速	合意形成に関わるノードの少なさや高速コンセンサスアルゴリズムの採用により、比較的高速
	5 スマートコントラクトの利用	実装による（Bitcoinのようにないものもあれば、Ethereumのように実装されているものもある）	実装による（Hyperledger Fabricなど基本的に実装されているものが多い印象）
	6 オラクルの利用	実装による	実装による

※ブロックチェーンをパブリック型/コンソーシアム型/プライベート型に分ける考え方もある。

デジタルサイネージについて

システムモデル

- コンテンツの配信にかかる一連の業務はシステム管理者により行われる。
- コンテンツの管理や更新、配備などはクラウド上で行われる。
- クラウドサーバからデジタルサイネージへの端末はインターネットやLAN経由で行われる。最近主流となっているWeb-Basedサイネージでは、通信プロトコルとして双方向のインタラクションに優れたWebSocketを用いることが多い。



用途：広告配信と情報提供

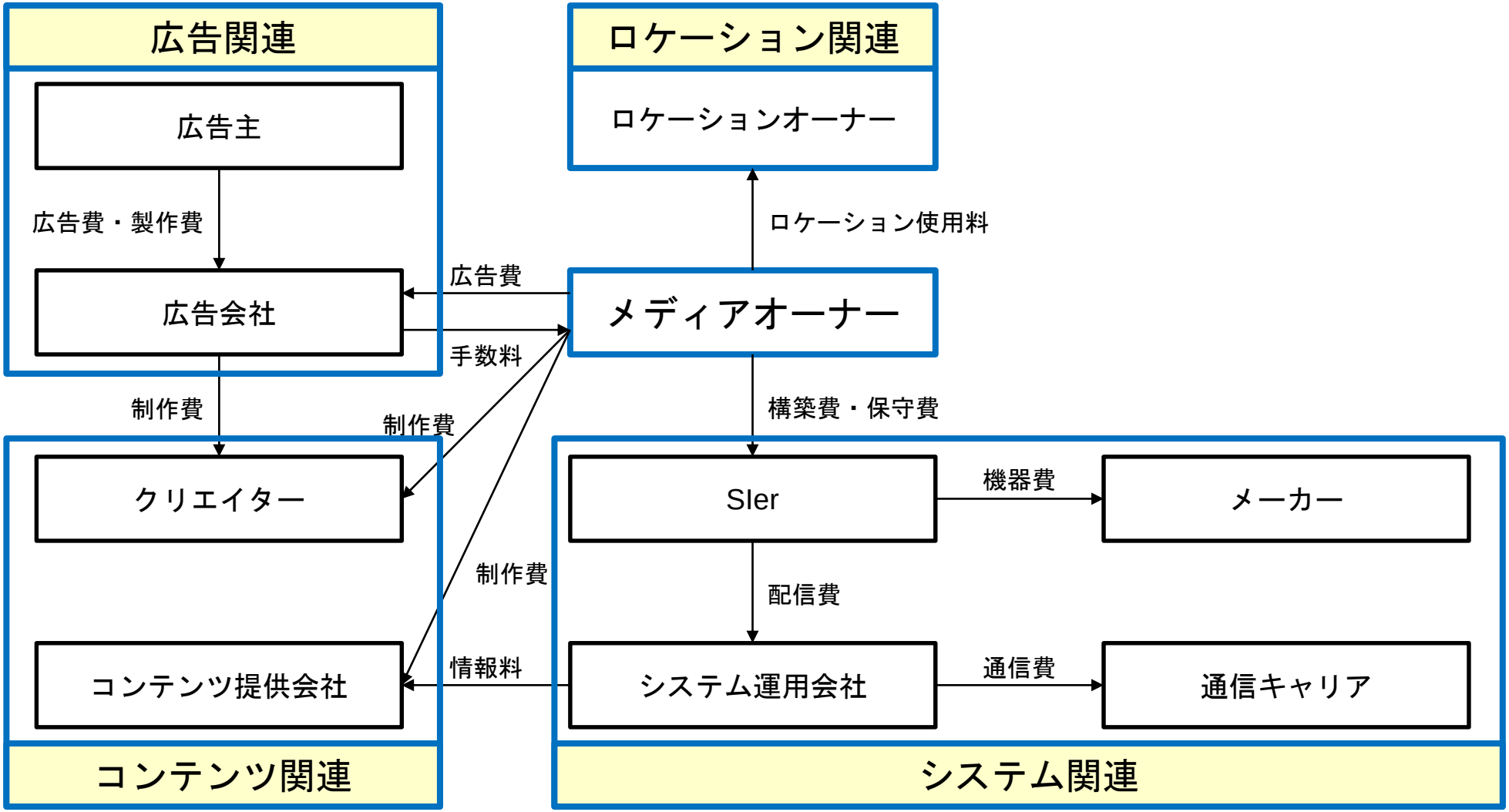
- デジタルサイネージの主な用途として広告配信と情報提供がある。
- 本稿で想定しているデジタルサイネージは広告配信と緊急時の情報提供を主な用途とするもの。緊急時の情報提供は政府の想定するユースケースでもある。

	広告配信	情報提供（平時/緊急時）
用途	企業あるいは店舗が持つ製品やサービスの特徴や利点をターゲットに認知させること。	(平時)ユーザの求める情報、公共交通機関の時刻表・遅延情報等の公共性の高いお知らせの提供。 (緊急)災害情報・避難指示・避難経路等の緊急性の高い情報の提供。
利用者の期待	利用者は広告主。求めるのは広告効果の高さ。 人数で測定するとすれば、接触人数×視認率がどれだけ高いか（と価格との対比）。	(平時)利用者は市民。直観的で分かりやすいUI/UXや要求に対する適切なコンテンツ。 (緊急)利用者は政府/自治体。求めるのは一目瞭然のコンテンツ、災害耐性の高い運用体制。
指標	接触人数⇒機器周辺の通行量や立地等 視認率　⇒画面サイズ、輝度等スペック等	(平時)インタラクション性、操作や音声の認識、提供コンテンツの精度等 (緊急)文字の見やすさ（フォントや大きさ）、ネットワーク障害耐性・非常用電源有無など運用の継続性等
立地	電車のドアの上部、駅構内の柱の側面等。	電車のドアの上部、駅構内の柱の側面等。

※他の用途も考えられるが、本稿の前提としているデジタルサイネージのイメージ外なので除く。

広告のステークホルダー

- デジタルサイネージの使い方を決められるメディアオーナーを中心として、概念的に広告、ロケーション、コンテンツ、システムの4つのセクションにステークホルダーがいる。ただし、各ステークホルダーが同一であるケースも少なくない。



※DSCの「デジタルサイネージ2020」をもとに作成。

展望

- テクノロジによるデジタルサイネージはますます強化される。
- 開発が容易になるとともにデジタルサイネージの端末コストが下がる。
- 映像の高精細化が行われる。それに伴うデータ容量の増加問題も5Gにより緩和・解消される。
- AIやIoT等の技術との融合が進み、コンテキストやパーソナル情報に基づいたサービスが実現可能となる。

テクノロジによる強化

①開発の易化	②表現の高精細化	③通信速度の高速化	④サービスの高度化
・HTML5により端末の依存性が排除され、高度なコンテンツの開発が容易になる ・デジタルサイネージ自体の単一障害点が減る	・4Kや8Kが標準として取り込まれるに従い、高精細な画像や映像表現が可能になる	・5G通信網が整備されることにより、高容量データでも安定して高速に通信できる	・AIやIoTなどのテクノロジと結びつくことで動的/インタラクティブなコンテンツ生成や属性情報に基づくパーソナライズドサービスが実現可能になる

デジタルサイネージにおける
ブロックチェーンの利用について

メタデータ管理　～問題意識～

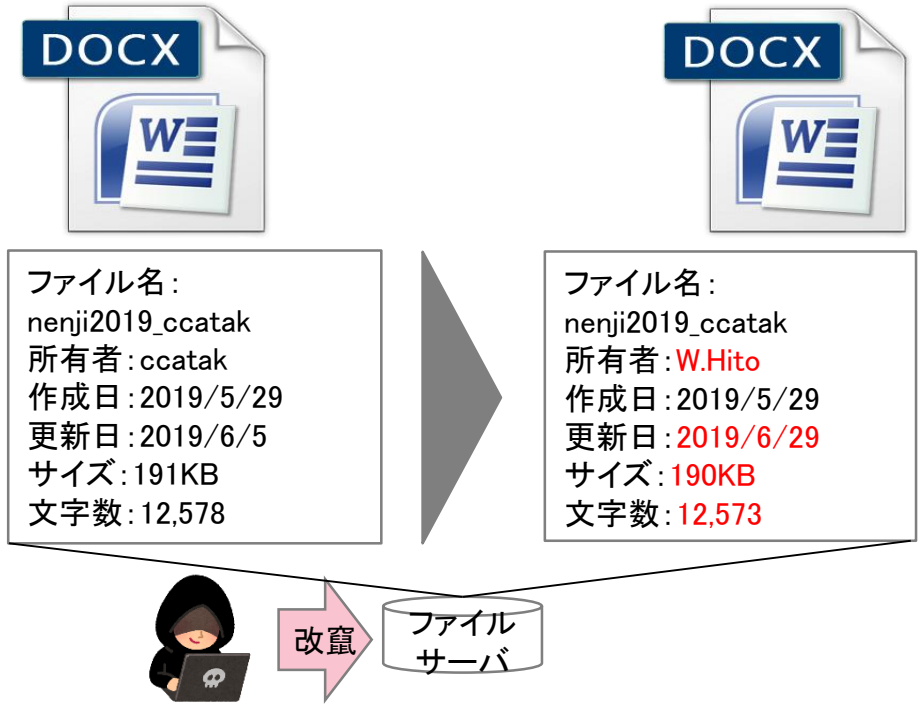
- コンテンツのメタデータが意図せず変更されたり、悪意を持って改竄される可能性がある。
- 権利等も広義のメタデータと捉えることができる。広義のメタデータの管理は煩雑かつ不透明である。

コンテンツのメタデータ管理

課題概要

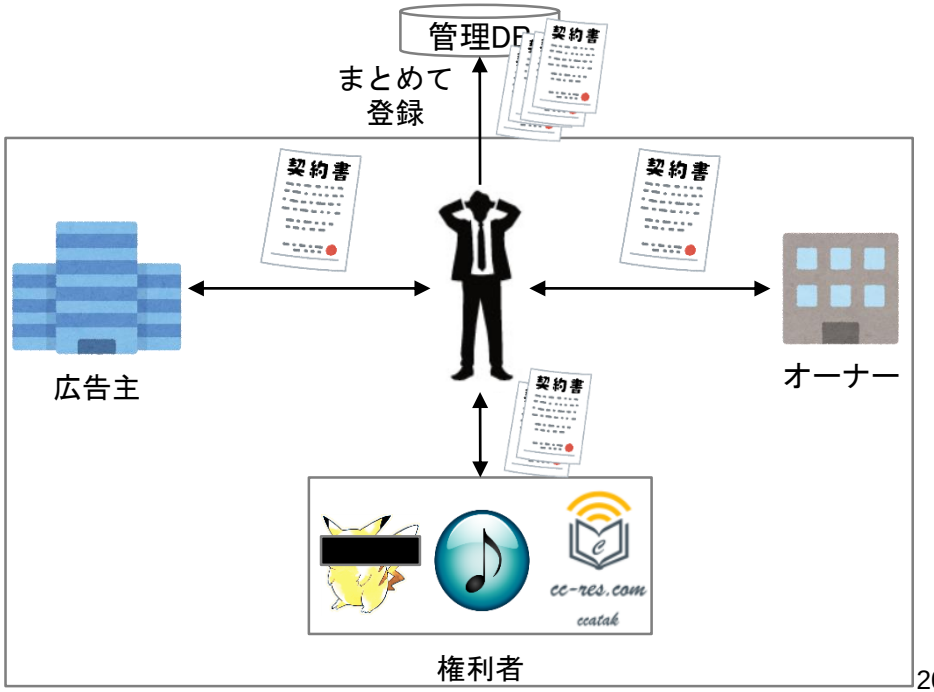
コンテンツの作成者、作成日時、データサイズ、アクセス権などのメタデータが暗黙裡に変更（改竄）されてしまう可能性がある。

イメージ



権利等広義のメタデータ管理

コンテンツの制作フローは、キャラクター、楽曲、ロゴなど権利処理にまつわる契約の連鎖ともいえる。広告会社を間に挟む構造で、契約の締結や管理が煩雑になりがちである。また、契約の内容は通常オープンにはされず、取扱いが不透明な場合もある。



メタデータ管理　～ブロックチェーン利用案～

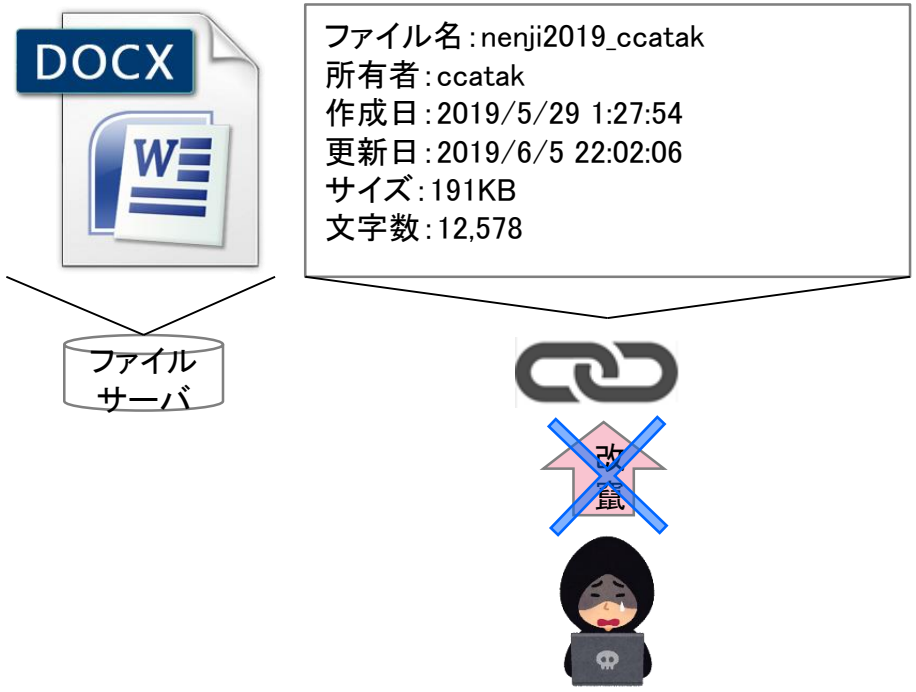
- コンテンツのメタデータをブロックチェーンで管理することで改竄耐性を向上させる。
- プレイヤーや契約内容もブロックチェーンに集約することで直接的なやりとりと透明性を確保する。

コンテンツのメタデータ管理

案

コンテンツのメタデータ部分をブロックチェーンで管理することで改竄の難易度を上げるとともに検出を容易にし、改竄耐性を高める。コンテンツ自体はこれまで通りクラウドサーバで管理（データサイズ等を考慮するとブロックチェーンでの管理に向かない）。

イメージ

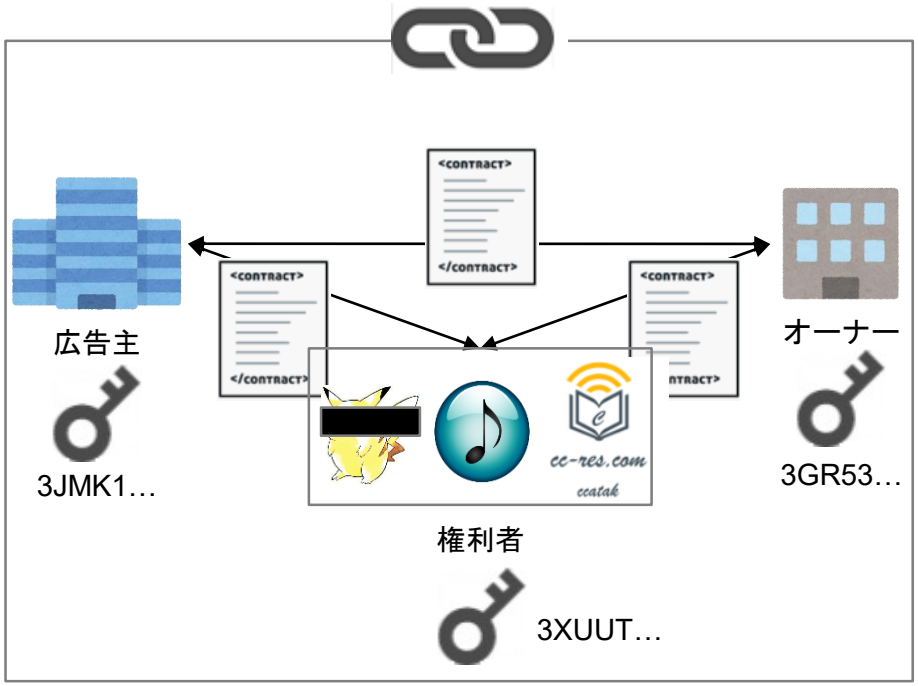


権利等広義のメタデータ管理

案

プレイヤーも契約も全てブロックチェーンに集約する。プレイヤー同士で直接的かつ明白な契約管理ができ可監査性もあってリスク・コンプライアンスに寄与する。また煩雑な契約管理から広告会社は抜け出ることができ、広告効果などより付加価値の高いサービスにリソースを傾注できる。

イメージ



広告枠細分化と動的プライシング　～問題意識～

- 広告掲載期間の選択肢の狭さが広告主とオーナーの双方にとって不都合になっている可能性がある。
- プライシングの手法に正当性はあるものの、広告主とオーナーの双方にとってより相応しい価格を追求する余地がある。

現在の在り方	課題	概要	案
【広告の掲載期間】 1枠の期間が1週間～1年という単位で販売されている。 ただし、1週間～1年の間で自由に選択できるわけではない。1週間、2週間、1カ月間、6カ月間、1年間などと定められており、その中から選択する形式である。 【配信の仕組み】 複数の広告コンテンツはまずロールという形にまとめられる。ロールの長さは決まっている。 ロールを組み合わせてプレイリストという1日の配信スケジュールが決定される。 プレイリストに従ってデジタルサイネージで配信が行われる。 【プライシング】 接触人数×視認率ベース	掲載期間	✓ 掲載期間の選択肢が狭く資金的余力のない広告主や特定のタイミングをピンポイントで狙って広告を出したい広告主には不都合。 ✓ オーナー側もこれらの潜在顧客をロスト。	広告主にとってもオーナーにとっても、 ①掲載期間について広告主により柔軟な選択肢が提供（それこそ1回単位で広告を打てるなど）されている方がよいのではないか？ ②そのうえで、広告の時間的変化と需給バランスを考慮した動的プライシングができればよいのではないか？
	プライシング	✓ 定型的な掲載期間の関係もあり広告枠の価値の時間的変化を十分に反映していない価格設定の可能性がある。 ✓ 広告主とオーナー側の需給バランスを反映した価格設定になっていない可能性がある。	

広告枠細分化と動的プライシング　～ブロックチェーン利用案～

- 広告枠細分化と動的プライシングをブロックチェーンで実現した時のPros/Consを以下に示す。価格根拠やデータの信頼性や透明性の観点で強みがあるが、そのための体制や設計、ビジネスモデルなど懸念も存在する。

Prosの例

- ✓ 広告枠の細分化により掲載期間の柔軟な選択肢（それこそ10秒1回のみなど）を与えることで生じる決済額の極小化に対してマイクロペイメントで対応可能である。
- ✓ オラクルを利用してデジタルサイネージ周辺の接触人数などの価格に影響するデータを動的かつ精度高く入手し利用できる。
- ✓ スマートコントラクトにより価格算出ロジックとオークションの仕組みを導入することで、これまでの接触人数×視認率に加えて広告主のニーズを取り込んだ透明な価格設定ができる。
- ✓ （KYC済みという前提だが）投資でいうところの“見せ玉”に似た手法による価格操縦が難しい。

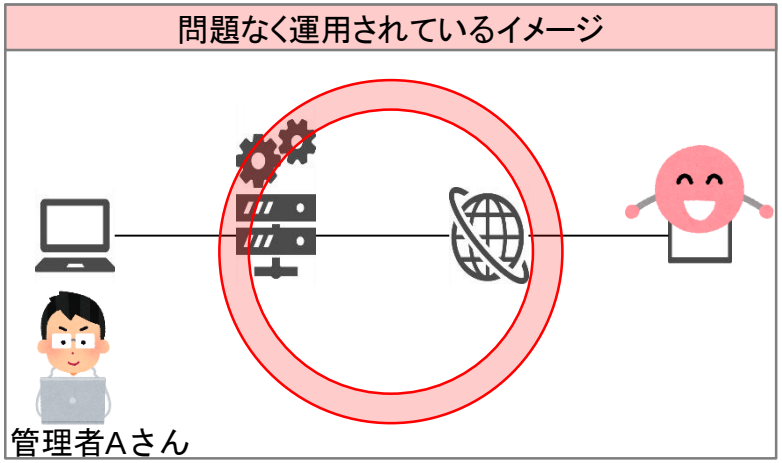
Consの例

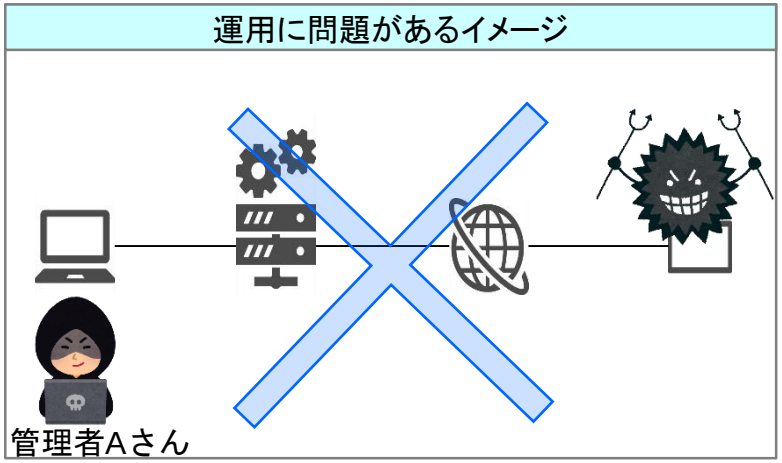
- ✓ オラクルの利用にあたって、データの信頼性を担保するためにブロックチェーンとオラクルの管理主体は別である方が望ましい。別でないとProsで挙げた精度の高いデータに疑義が生じる。
- ✓ オラクルを通じて接触人数などのデータを動的に集める場合、センサーなどの機器が追加で必要になると思われる。これらのコストを補っても利益を上げられるだけのビジネスモデルを作れるかは不明。
- ✓ 広告枠細分化によるベースとなる出稿依頼の増加、イベント等による一時的な出稿急増、将来的なデジタルサイネージの増加など、スケーラビリティ面を考慮した設計が必要だが前例がない。

広告枠細分化/動的プライシング自体はブロックチェーンでなくてもできる。
上は全てブロックチェーンで実現しようとした極端な例で、価格根拠やデータにどの程度の透明性・信頼性が必要か、掛けられる予算はどれくらいかなど、要件はさまざまあるはずで、それに照らしてブロックチェーンが適切なら用いればよい。

公共性担保　～問題意識～

- システム管理者が不正を冒すリスクはデジタルサイネージでも変わらず存在する。集権的なシステム管理体制となっていることに課題がある可能性がある。





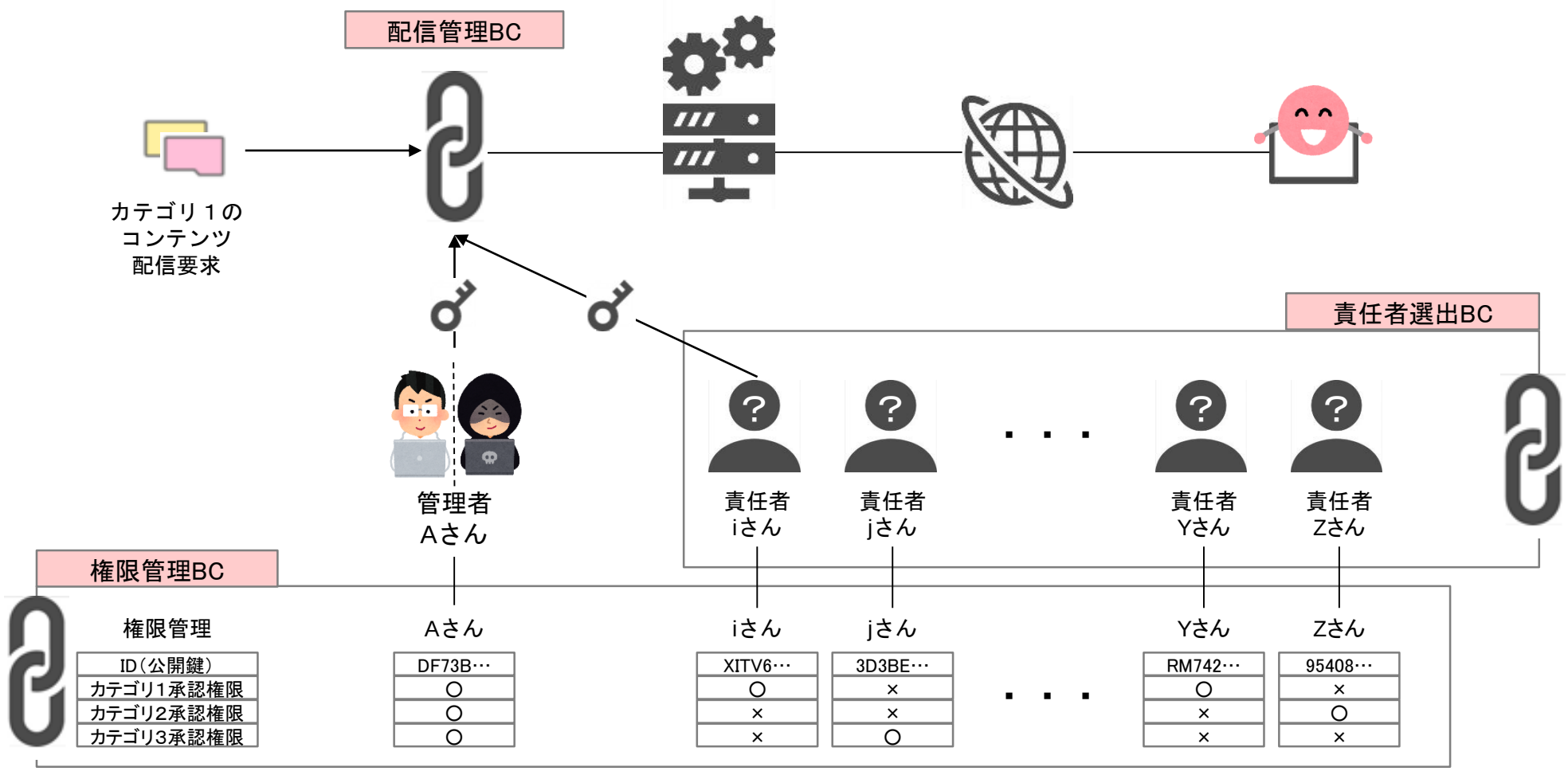
なぜAさんは  から  になってしまったのか？
どうすればよかったのか？

✓ 不正のトライアングル理論によれば、「動機・プレッシャー」「機会」「不正の自己正当化」が揃ったから。これらが揃わないようにすればOK。そのためにセキュリティポリシー、運用ガイドラインなどを定めて防ごうとする。
✓ とはいえ、日々の業務上の都合から権限が暗黙のうちに管理者に集中する、ルールの欠陥や他者との結託などにより不正が行われるといったリスクはやはり存在する。

集権的なシステム管理に課題があるのでは？

公共性担保　～ブロックチェーン利用案～

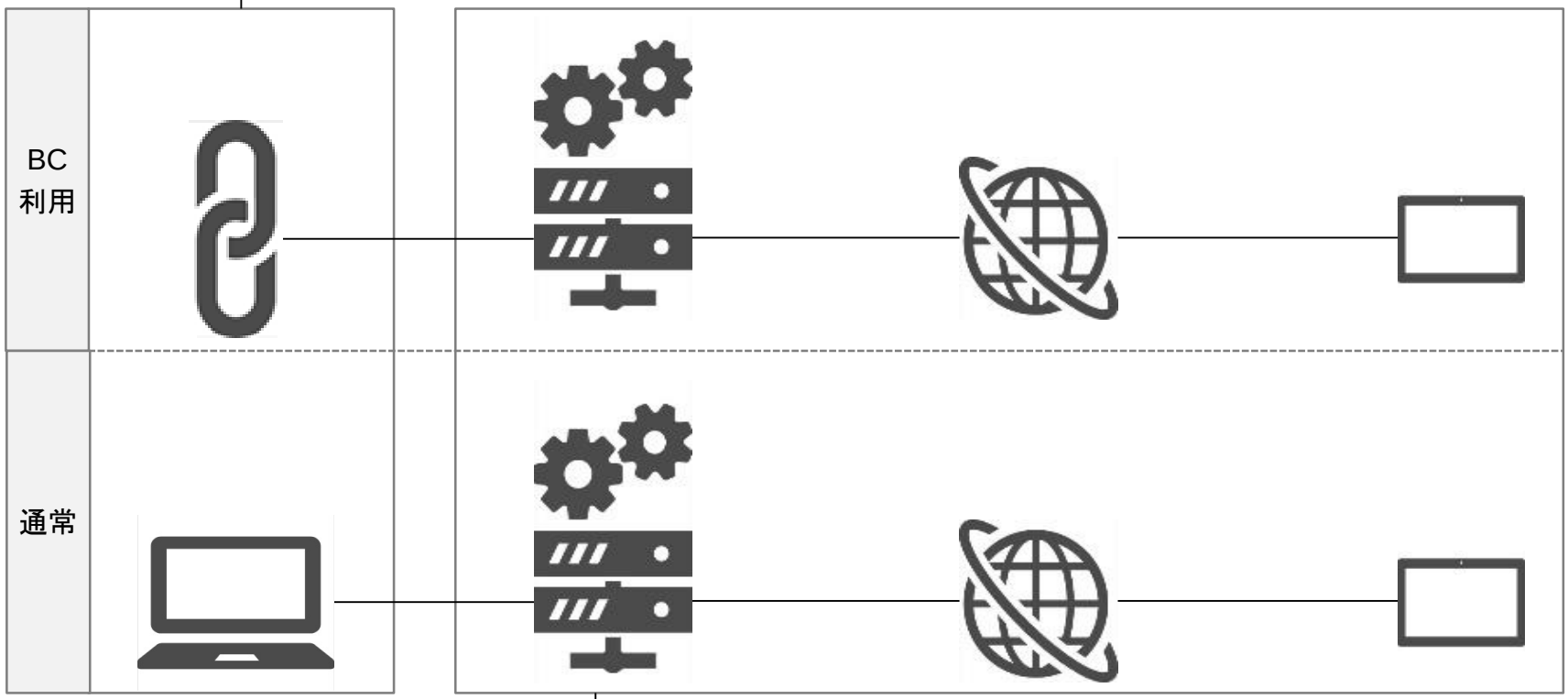
- 配信管理BCでは、コンテンツ配信に管理者と責任者の電子署名を必須とし、承認を多重化する。
- 責任者選出BCは、配信要求に署名する権限を持つ適切な責任者をランダムに選ぶ（結託リスクの低減）。
  選んだ責任者が一定期間署名しないなど不正を働いた場合、その証拠を記録して別の責任者を選ぶ。
- 権限管理BCは各人の権限を管理する。
- 変更履歴が全て記録されていること、誰もが確認できること等、可監査性が重要。



配信承認でブロックチェーンを利用するもう一つの側面

- 政府はデジタルサイネージを緊急時の情報提供インフラとしてみなしている。システムモデルを見れば大規模災害時にシステムが機能しなくなる余地は多くあるが、ブロックチェーンを配信承認に用いることでこの部分に関しては実効性を高めることができる。

被災により一部ネットワークが使えなくなってもブロックチェーンは動き続けることが可能。
配信承認部分はダウンしないため災害時情報提供の実効性は高まる（同一ロケーションにノードを配置しているとあまり効果がない）



サーバがクラッシュする、サーバとサイネージをつなぐネットワークに障害が起きる、サイネージ端末自体が壊れるといったケースではもちろんシステムとして機能しなくなる。

まとめ

ブロックチェーンについて

- ブロックチェーンは暗号理論に基づいて非中央集権性や改竄耐性を担保している。
- 研究が進む中で多様なブロックチェーンが登場している。
- スマートコントラクトやオラクルなど拡張性も高まっている。
- パーミッションレスタイプは新しい分野で、パーミッションドタイプは既存の分野の応用で用いられる傾向にあるようだ（組織体制や管理体制との親和性のため）。

デジタルサイネージについて

- デジタルサイネージの利用例として広告配信と情報提供がある。特に災害時の情報提供は政府の想定するユースケースでもある。
- HTML5、5G、8K、AI等の技術と結びきデジタルサイネージの応用可能性は広がる。

デジタルサイネージにおけるブロックチェーンの利用について

- デジタルサイネージのシステムモデルやステークホルダーの関係性について見ると、インフラ周りでいくつかの課題があるように見受けられる。メタデータ管理、広告枠細分化と動的プライシング、公共性担保などは課題の解決に向けてブロックチェーンの採用が考えられる領域である。

個人的な願望

- 一見無関係そうな分野でもブロックチェーンの応用の余地はあるので、ますます浸透してたくさんの価値を創出していってほしい。

デジタルサイネージ分野におけるブロックチェーン利用の検討

ccatak / https://cc-res.com**管理人**
Email: ccatak@cc-res.com
Website: https://cc-res.com

講演資料の公開場所： https://cc-res.com/dsgnenjiss_attachment_20190629/

おわり