ConsensusBase

ブロックチェーンにおける ID/DID、認証の最新動向

2019/07/01 時点での資料です。

目次

自己紹介 / 会社紹介

DID / SSI / Verifiable Claimsとは?

IDが使われる分野(人、会社、モノの認証)

マイクロソフトのIONとは?

業界の最新動向（DIFやW3C）

大手認証企業とのID実証実験について

コンセンサス・ベイス事業紹介

目次

自己紹介

ブロックチェーンに関わる活動

- 経済産業省「ブロックチェーン検討会」委員
- IBC（International Blockchain Consultants）メンバー
- 日本ブロックチェーンユーザ会（JBUG） 代表

メディアへの出演・寄稿

- 年鑑：日経Fintech世界年鑑2017-2018/イーサリアムを執筆
- 雑誌：「日経BPムック/ブロックチェーン＆ビットコイン」
- 雑誌：「日経コンピュータ」(2016年7月7日号)
- テレビ：日経CNBC「ザ・金融闘論」に出演

イベントでの登壇

- 日本銀行主催「第1回 FinTechフォーラム」
- 日本FIX委員会トレーディングサミット2016
- FIBCイベント　セミナー「ブロックチェーンは金融をどう変えるのか」
- 青山アクセラレーションセンター イベント「ブロックチェーンが創る世界」

コンセンサス・ベイス(株)
代表取締役　志茂博

コンセンサス・ベイス株式会社のご紹介

国内でも有数の実績を誇るブロックチェーン技術の専門企業

プロフィール

社名	コンセンサス・ベイス株式会社
代表	志茂 博
創業	2015年 4月
事業内容	• コンサルティング • システム開発 • ブロックチェーン教育 • 自社サービスの開発・運営

大手企業との開発実績多数

SoftBank	国際募金プラットフォームの開発
大和総研 Daiwa Institute of Research	ミャンマー資本市場実証実験
CTC Challenging Tomorrow's Changes	社内開発の実験システム
GlobalSign GMO INTERNET GROUP	本人認証システム開発
Confidential	著作権管理システム開発
Confidential	データ改ざん防止システム開発

コンセンサス・ベイスの開発・コンサルティング実績の一例

クライアント企業(順不同、敬称略)

金融	野村総合研究所	2016年4月	証券分野の実証実験
	大和総研	2016年6月	ミャンマー資本市場の証券実証実験
	Confidential	2017年10月	ブロックチェーンによる信頼証明
IT	伊藤忠テクノソリューションズ株式会社	2016年7月	社内開発の実験ポイントシステム
	GlobalSign GMO INTERNET GROUP	2016年12月	ブロックチェーンにおける本人認証システム
	伊藤忠テクノソリューションズ株式会社	2019年4月	農作物のトレーサビリティ

クライアント企業(順不同、敬語略)

通信	SoftBank	2016年1月	国際募金プラットフォームの実証実験
	SoftBank	2018年11月	MR空間における信頼証明システム
	Confidential (大手上場企業)	2018年12月	IoTデバイスを利用した情報管理
エンタメ	Confidential (大手上場企業)	2018年6月	著作権管理システムの開発
	Confidential	2019年3月	ウェブメディアSNSシステム
	Confidential (大手上場企業)	2019年4月	ファン向けポイントシステム開発
	Confidential (大手上場企業)	2019年5月	ブロックチェーンゲームの開発

目次

DID … 非中央集権ID（Decentralized Identifier）

SSI … 自己主権的ID（Self Sovereign Identity）

- 2017年ぐらいからブロックチェーンを活用したID管理のプロジェクトが増えた
- 直近ではマイクロソフトなどの大手企業も参入しているが、まだ本格運用のフェーズには至っていない
- 2017年に国際的な団体であるDIF（Decentralized Identity Foundation）が設立され、国際規格の統一に取り組んでいる
- ID共通化の主目的に鑑みて、現在ではパブリックチェーンを活用したプロジェクトが中心になっている
- 今取り組んでいるプロジェクトは「個人IDの利便性」を追求するプロジェクトが多いが、5～10年先を見据えた際には、IoTデバイス、ドローン、自動運転車などの機器の認証の重要性が高まってくると見込まれる

SSI（Self Sovereign Identity）・DID（Decentralized Identifier）

SSI
- 自己主権型アイデンティティ
- 個人は自分のアイデンティティを所有し制御できるべきである、という考え方

DID
- 非中央集権型のデジタルID
- SSIを実現する手段の一つ。
- 分散台帳（≒ブロックチェーン）を利用

DIDs
- W3C Credentials community groupによって提案されているDIDの標準仕様
  W3Cは、HTML、XML、CSS、DOM等の規格を提唱した団体

Verifiable Claims（暗号技術で証明可能な個人・法人情報）

DID	基本ID、Ethereumアドレスをそのまま使用可能
DID Documents	JSON-LD(リンクドデータが入っているJSONファイル)に書かれたID情報。公開鍵等を含むがただし個人情報は含まれない
Verifiable Claims	個人情報のピース ある主体が他の主体について作成した、暗号学的に信用性のあるの記述データ。
Verifiable Credential	Verifiable Claimsが束になったもの 検証可能な個人情報の一単位(一集合体)であり、用途に合わせて作成できる

DIDの構造

DID

```
did:ethr:0xb9c5714089478a327f09197987f16f9e5d936e8a
```

① URLスキーム識別子（the URL scheme identifier (did)）
② DIDメソッド識別子（the identifier for the DID Method）
③ DIDメソッド固有識別子（the DID Method-specific identifier）

DIDは永続的かつ不変。

識別子のみで、個人情報は含まれません。（次項）

DIDの構造

DID Documents

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // this key can be used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----
\r\n"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

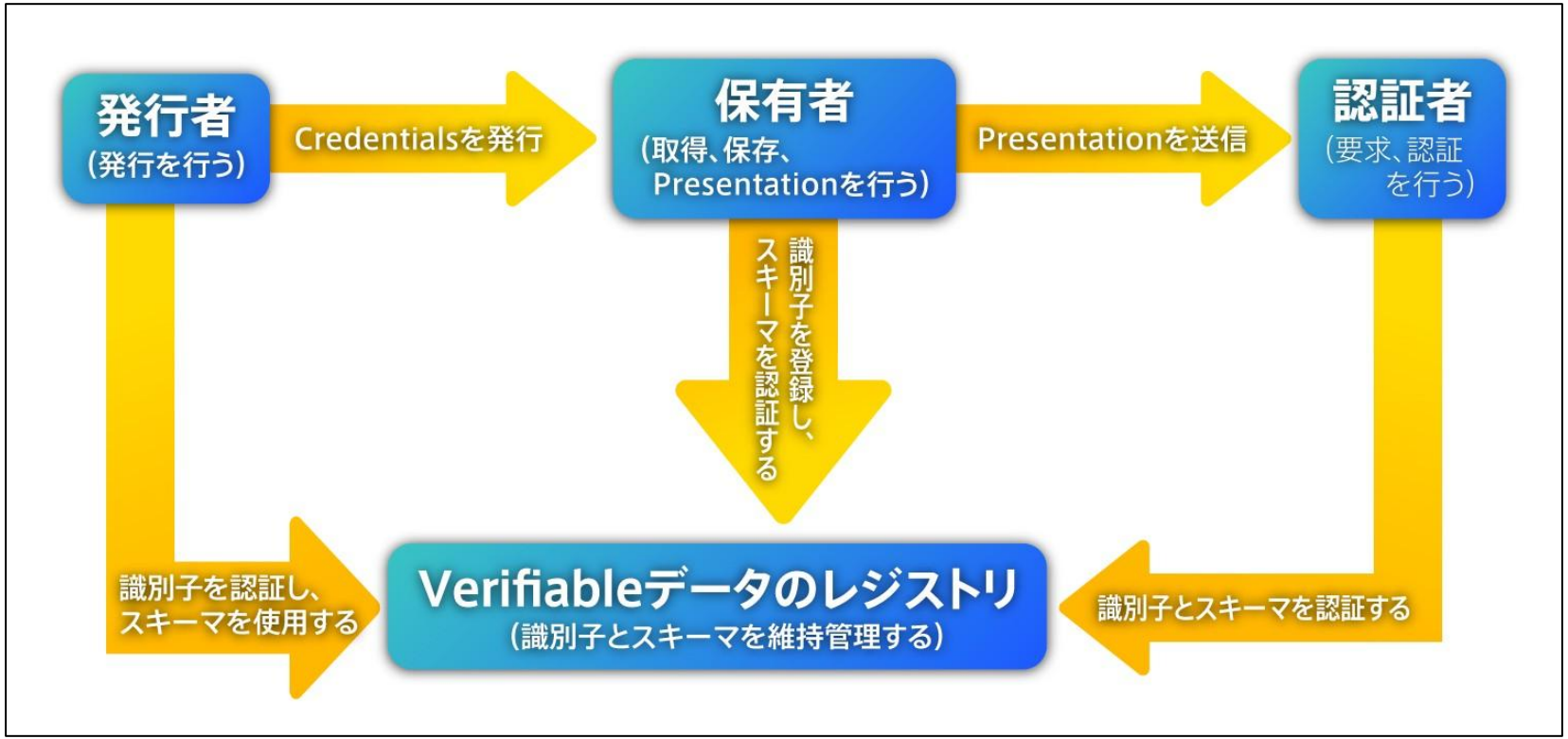
- DIDの管理下にあるエンティティを暗号的に認証する方法など、DIDに関連する情報を含む
- ユーザー名、住所や電話番号などの個人情報が入っていない
- 暗号化されておらず、誰でも閲覧可能
- ブロックチェーンに記録するため、改ざんが不可能で、半永久的に保存

Verifiable Claims

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.com/credentials/4643",
  "type": ["VerifiableCredential"],
  "issuer": "https://example.com/issuers/14",
  "issuanceDate": "2018-02-24T05:28:04Z",
  "credentialSubject": {
    "id": "did:example:abcdef1234567",
    "name": "Jane Doe"
  },
  "proof": { ... }
}
```

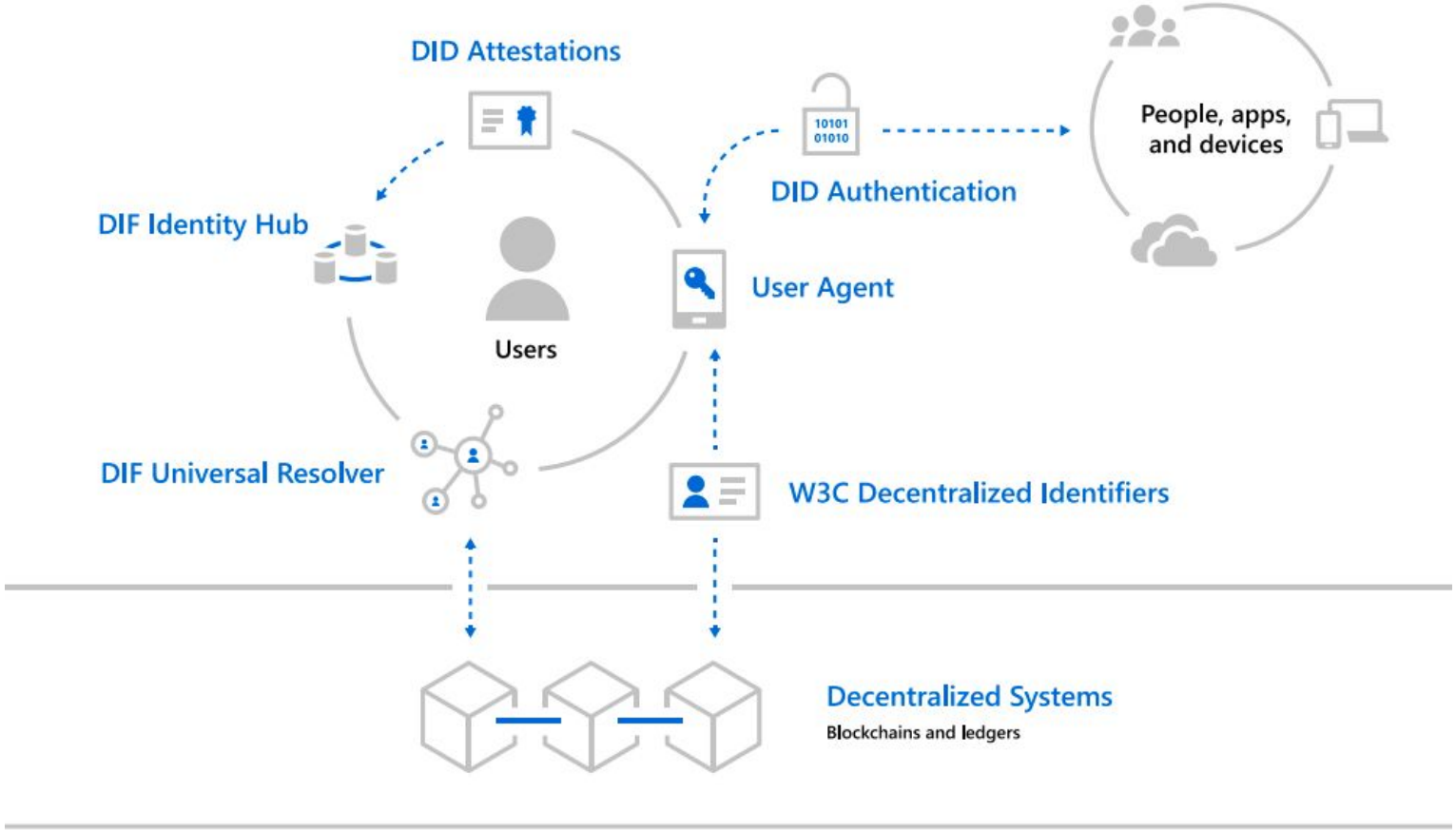
- 個人情報における特定の事実を証明するためのデータ形式
- 例えば、氏名、住所などの個人情報が入っています
- 暗号化されている
- W3Cが開発している規格です

Verifiable Claims（暗号技術で証明可能な個人・法人情報）



出典：DID（Decentralized Identifiers：非中央集権型識別子）、Verifiable Claims（暗号技術で証明可能な個人・法人情報）とは？

DIDに関連するネットワーク見取り図



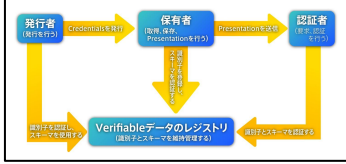
出典：マイクロソフト　ホワイトペーパー

構成要素の説明

コンポーネント名	概要
User Agent	いわゆるIdentity Wallet。スマホアプリやブラウザ Extensionとして実装される。鍵ペアの生成とDID（Decentralized Identifier/識別子）の登録、DID Authにおける認証器の役割を果たす。
Identity Hub	DIDに関連するIdentity情報を保存する。
Distributed Ledger	DIDとDID Documentを記録する分散台帳。 （ブロックチェーンなど。ブロックチェーンが必須な訳ではない。）
Universal Resolver	他の台帳上にあるDID　Documentを解決する（複数の系の分散台帳で運営される前提）
Verifiable Credentials	第3者から発行された検証可能なアイデンティティ情報（を表すデータ構造の標準）

出典 : これからの KYCとIdentity on Blockchainの動向

DID Auth（ユーザ認証） ~Credentials共有



・あなたの年齢を確かめて、Credentialsを共有したいです。

・ビールを配達

WEB SHOP
業者

① Challenge

④

User Agent

Aさん

③ 検証

② Response

・Challengeに対応するResponseを生成し、ユーザーの秘密鍵で署名
・自分のVerifiable CredentialsとDID Documentを渡す。

・公開されているAさんの公開鍵を使って署名を検証する。
・受け取ったVerifiable CredentialsのDID Documentの公開鍵でCredentialsを検証する。

Distributed Systems

＜Aさんが WEB SHOP 業者にビールを注文するケース＞

① ビールを注文すると、WEB SHOP業者が Challengeを発行する。
② Aさんは、業者を信頼してVerifiable Credentialsと個人識別子(DID Document)共有する。
③ 業者はAさんと共有した情報からブロックチェーンにアクセスすることで、その信頼性を確認する。
④ 認証成功したら、ビール配送スキームを実施。ビールが配達される。

目次

これまでの本人確認・ID管理における課題

個人ID

- 新しいサービスを利用する際には、同一の個人情報を毎回入力しなければならない
- どの企業に、どこまでの情報を開示するか決められない
- 一度情報を提出してしまうと、自分で削除することができない
- 単一の組織に全ての個人情報が管理されているため、情報漏洩・データ消失のリスクがある

組織・法人

- 企業間の取引開始時や、新規融資を受ける度に、登記簿や財務情報を提出する必要がある
- 財務情報などの機密情報を、誰にどこまで開示するか
- 一度情報を提出すると、自分で削除することができない
- 個人情報漏洩時の被害が大きいので、個人情報を保有したくない

機器・デバイス

- データを送信している機器・デバイスは本物か
- 機器・デバイスから送信されたデータは、途中で改ざんされてはいないか
- 機器・デバイスが提示してくる支払先情報（口座名義・ETHアドレスなど）は正しいか

個人と法人の課題意識と、機器・デバイスの課題意識は若干異なっている

個人ID	組織・法人	機器・デバイス
▪ 新しいサービスを利用する際には、同一の個人情報を何度も入力しなければならない	▪ 企業間の取引開始時や、新規融資申込時など、登記簿や財務情報を提出する必要がある	▪ データを送信している機器・デバイスは本物か
▪ どの企業に、どこまでの情報を開示するか決めたい ▪ 一度情報を提出してしまうと、自分で削除することができない	▪ 財務情報などの機密情報を、誰にどこまで開示するか ▪ 一度情報を提出すると、自分で削除することができない	▪ 機器・デバイスから送信されたデータは、途中で改ざんされてはいないか （左記の三つの課題もあるが） 暗号技術を活用した機器認証や、データの改ざん防止など ▪ 機器・デバイスが提示してくるアドレス（払い出し時に登録したアドレスなど）は正しいか
▪ 単一の組織に全ての個人情報が管理されているため、情報漏洩・データ消失のリスクがある	▪ 個人情報漏洩時の被害が大きいので、個人情報を保有したくない	

提供する情報の規格統一と適用性の向上
（Applicability）

自分自身で、誰にどの情報を開示するかを決定
（Access Control）

情報セキュリティ
（Security）

課題と分散型ID管理による解決策

	既存のサービス利用時の課題	ブロックチェーン分散型ID管理では
Applicability	▪ 新しいサービスを利用する際には、同一の個人情報を毎回入力しなければならない	▪ ブロックチェーンに保存された単一の個人情報を、全てのサービスに提供して認証を実施する
Access control	▪ どの企業に、どこまでの情報を開示するか決められない ▪ 一度情報を提出してしまうと、自分で削除することができない	▪ 自身が管理主権を持ち、最低限必要な情報だけをサービス提供者に与える ▪ 提供した情報を、自分で削除することができる
Security	▪ 単一の組織に全ての個人情報が管理されているため、情報漏洩・データ消失のリスクがある	▪ ブロックチェーンに保存されることで、企業側での情報漏洩・データ消失が起きない

目次

MicrosoftによるIdentity Overlay Network（ION）

Identity Overlay Network（ION）とは

概要
- 中央管理者に個人情報を預けることなく、自分が管理する非中央集権型の ID管理システム
- ストレージに保管されたPII（個人識別情報）に対し、第三者にアクセス権を渡して参照させる

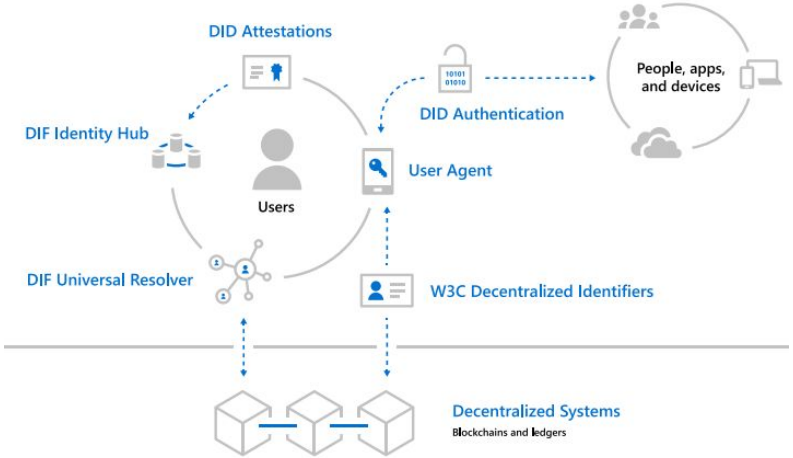
対象
- （現在の想定は）個人ユーザー

BC基盤
- ビットコインブロックチェーンのセカンドレイヤー（Sidetree）を活用

処理能力
- 1秒当たり数千～数万トランザクションを処理（これに対して、ビットコインは 1秒間で7-10トランザクション程度の処理能力）

開発状況
- ビットコインのテストネットに β版プロダクトを公開中

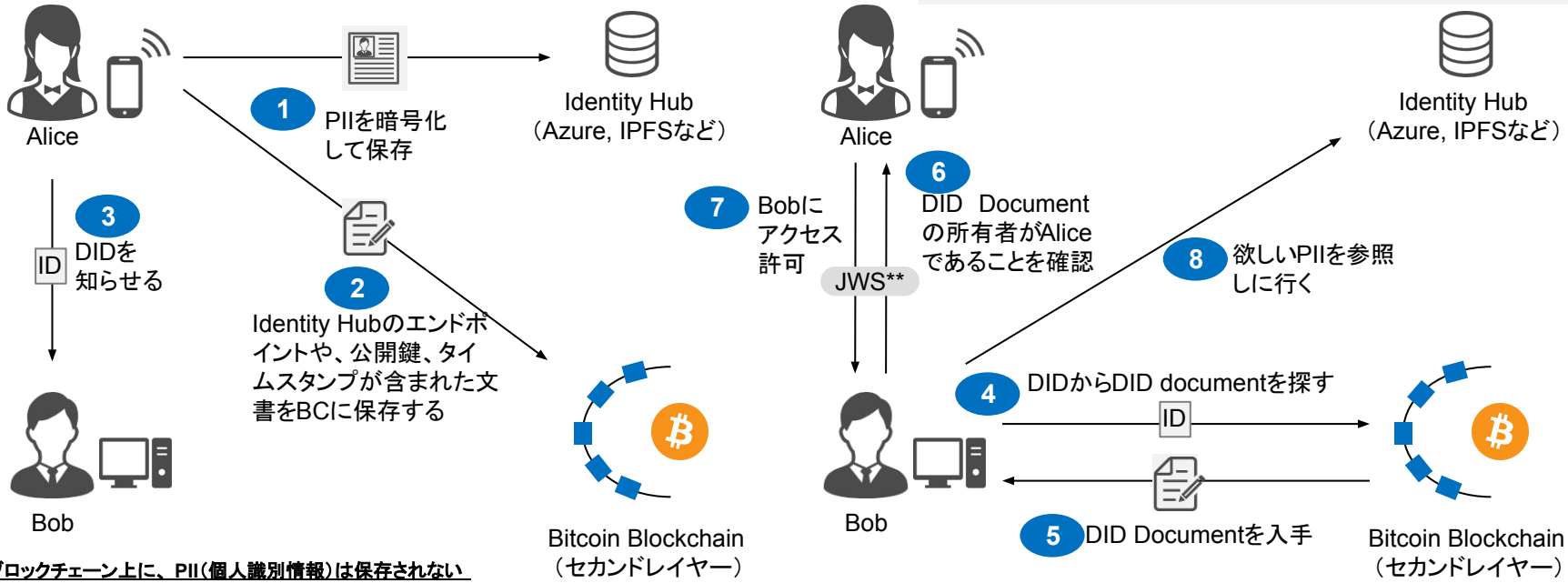
IONの仕組み



Source：Microsoft Official page（https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY）

IONの仕組み（自身のPII*（個人識別情報）を公開する場合）

DID：保存されるPII（個人識別情報）に付けられるD
DID Document：そのDIDに関連する情報（PIIの保存場所、公開鍵、タイムスタンプなど）が保存された文書

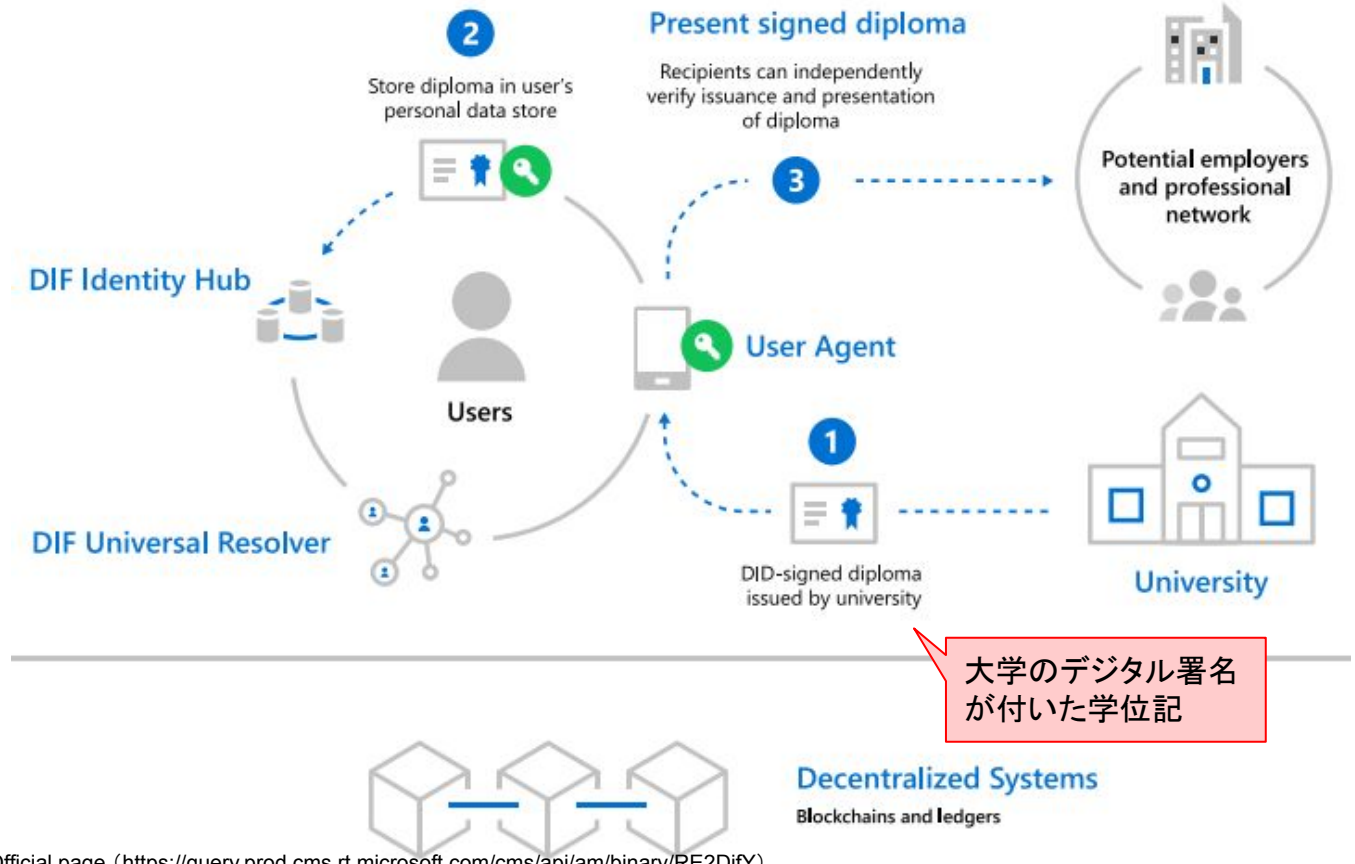


※ブロックチェーン上に、PII（個人識別情報）は保存されない

*PII（Personally Identifiable Information）：電話番号、マイナンバー、メールアドレスなどの個人を識別可能な情報
**JWS（JSON Web Signature）：公開鍵/秘密鍵のペアを使って、セキュアにアクセス権を付与する技術。 DID Documentに公開鍵が記録されているため、 Aliceの持つ秘密鍵にて所有権を証明し、Bobにアクセス権を付与することができる

Source：Microsoft Official page（https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY）

IONの仕組み（第三者による証明履歴を公開する場合）



Source：Microsoft Official page（https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY）

目次

DIF（Decentralized Identity Foundation：分散型ID財団）とは？

DIFの概要

概要

- ブロックチェーンを活用し、業界横断の認証用IDの標準化を目指して2017年設立

対象

- 個人だけではなく、組織、デバイスなど

活動内容

規格の統一

- プロトコル・構成要素・データフォーマットの規格を開発

相互運用性の確立

- 参加するプロジェクトの異なる規格同士を相互に参照可能にする規格の統一

企業間連携

- 分散IDの業界団体として、参加者の共通利益の保護を目的とする

加盟企業

Source：DIF Official page（https://identity.foundation/）

パブリックチェーンを活用したID管理と、プライベートチェーンを活用したID管理のアプローチ

	主要なプロジェクト	活用するチェーン	実施企業
パブリックチェーン	▪ uPort	▪ Ethereum	▪ Consensys
	▪ Civic	▪ Bitcoinのセカンドレイヤー（Rootstock）	▪ Civic開発チーム
	▪ ION（Identity Overlay Network）	▪ Bitcoinのサイドチェーン（Sidetreeプロトコル）	▪ Microsoft
	▪ ERC725（分散型IDの規格）	▪ Ethereum	▪ Ethereum開発者
	▪ ERC721（NFT）	▪ Ethereum	▪ Ethereum開発者
プライベートチェーン	▪ Hyperledger Indy	▪ Hyperledger Indy	▪ Sovrin Foundation
	▪ ID2020（難民支援ID）	▪ Enterprise Ethereum	▪ 国連、Accenture
	▪ KYC一元化プラットフォーム	▪ Hyperledger Fabric	▪ 日系金融機関

デバイス認証に利用する分散型ID「Ockam」とは?

概要

- ブロックチェーンを活用して、IoTのデバイス認証を行います。独自に「 Ockam Blockchain」を運営。

参加方法

- 「Ockam SDK」を利用することで、Ockamネットワークに参加できる。

特徴

相互運用性

- Ockamは相互運用性があり、マルチパーティIoTネットワーク用に構築されている。

簡単な価格設定でサーバーレス

- 開発者は、コードに組み込まれている単純な機能でネットワークと対話し、利用した分だけ支払う。
- SDKを使うとサーバーが必要ありません。

解決

セキュリティ

- Ockamの規格・ネットワークを利用することで、安全にIoT機器を管理できます。
- ネットワークがマイクロソフトのAzureを利用してクラウドインフラストラクチャ上に構築される。

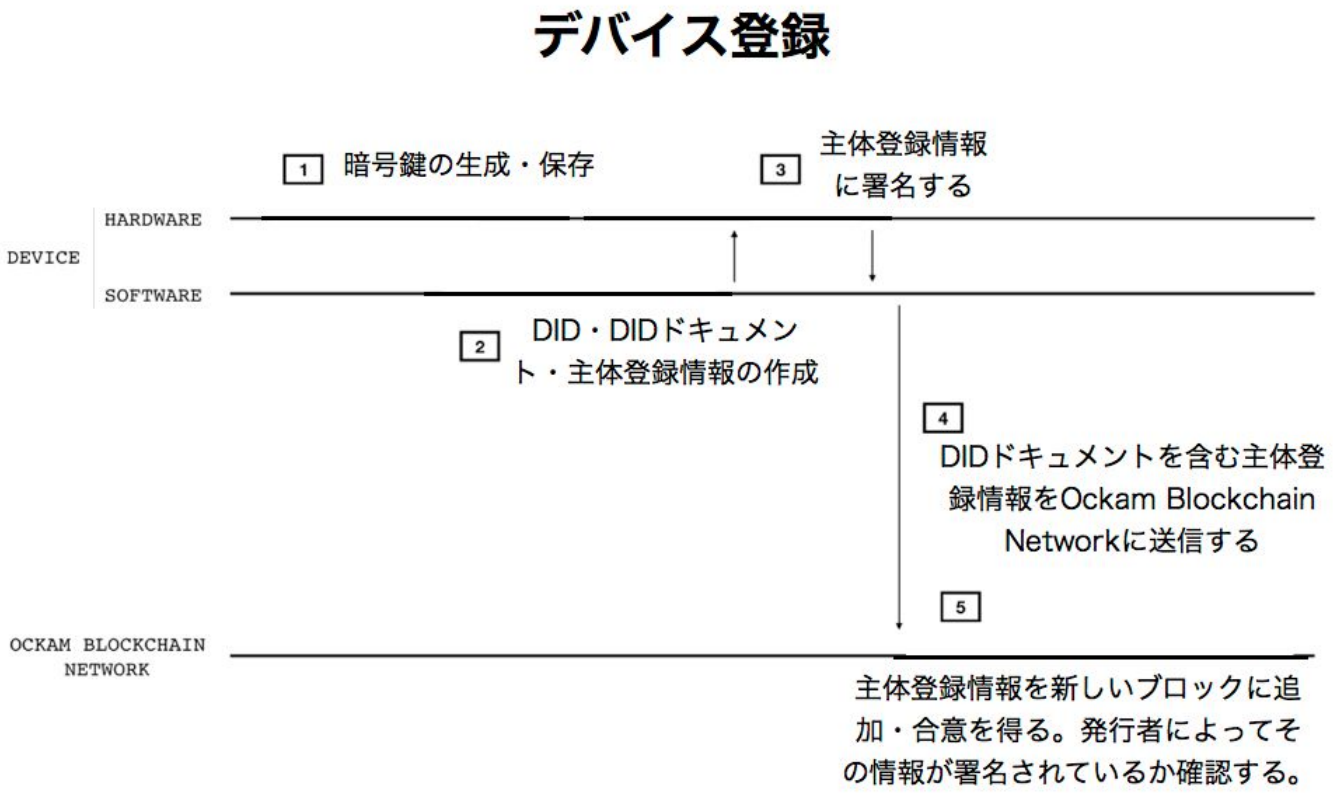
コスト面

- 独自のIoTインフラストラクチャーを構築しなくてすみます。

相互運用性

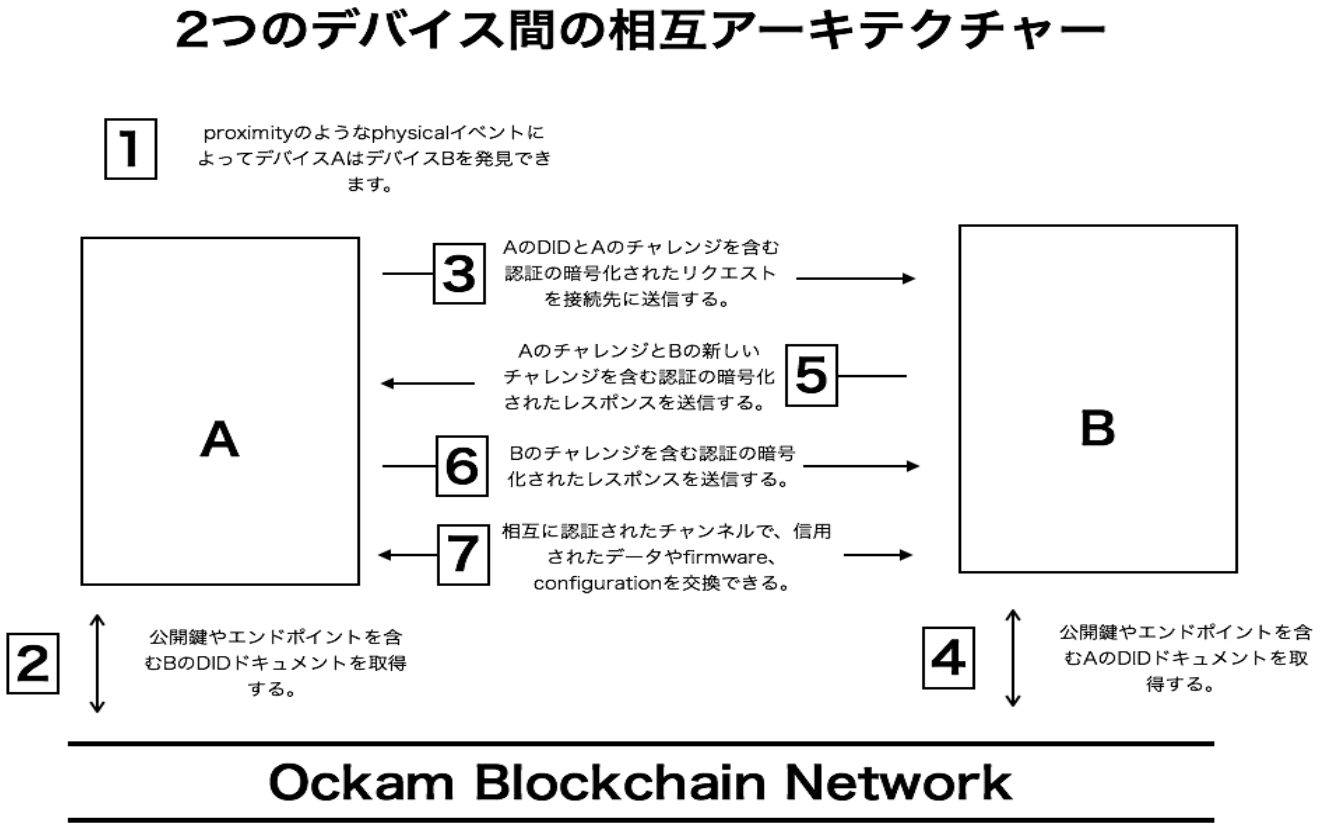
- 複数のIoTプラットフォームに接続する必要がありません。

デバイスの登録とデバイス認証流れ



出典：Ockamドキュメント

デバイスの登録とデバイス認証流れ



出典：Ockamドキュメント

目次

CB社とGMOグローバルサイン社による2017年の実証実験では、スマートコントラクトにより送金先ETHアドレスの認証を実現した

課題

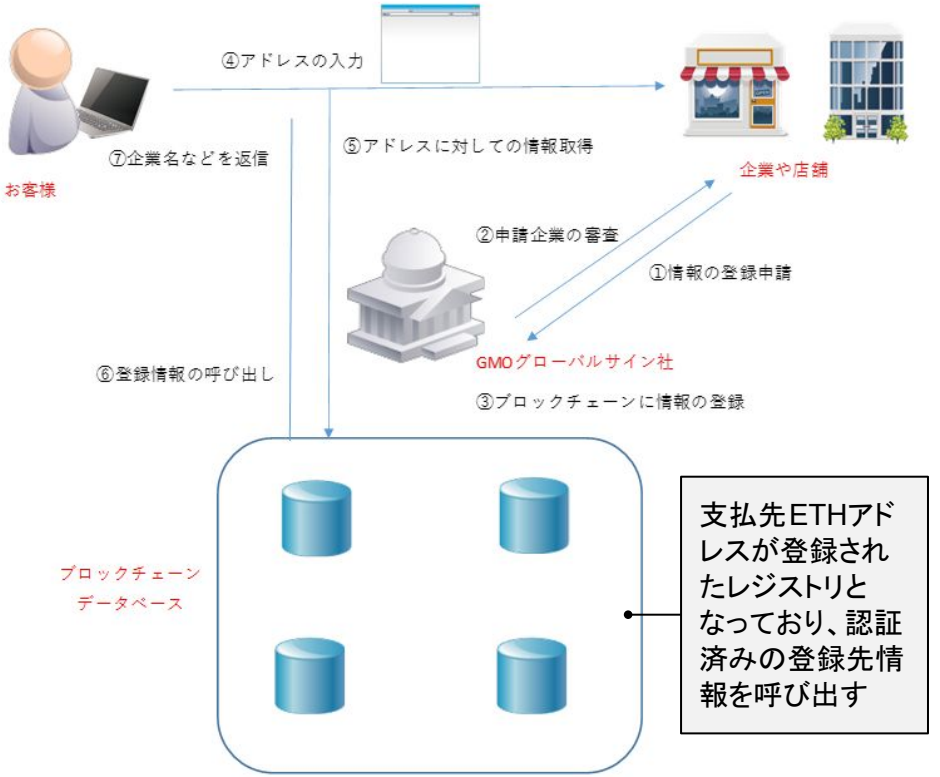
- Ethereum上での料金支払いにETHアドレスを提示されるが、本当にそのETHアドレスが目的の組織のものか判断がつかない

解決策

- GMOグローバルサインが事前に企業を審査し、スマートコントラクトにETHアドレスと企業情報を紐づけて登録
- 利用者は、支払う前に適切なETHアドレスかどうかを確認できる（SSL認証の考え方）

将来展望

- GMOグローバルサイン1社だけでは中央集権の仕組みだが、複数企業のコントラクトが認証すれば、非中央集権の仕組みになるのではないか



Source：GMO Global Sign（https://jp.globalsign.com/info/detail.php?no=1481523125） CB社内資料

ソフトバンクによる「AR/MR空間でのブロックチェーンを活用したIoT機器認証」の実証実験を技術支援

以下の3つの技術要素を検証

1. クラウドを活用したAR/MR空間と現実空間のリアルタイム同期
2. ブロックチェーンを活用した機器認証・認可情報の証明と記録
3. 指紋認証カードと、秘密分散技術（シャミア）による秘密鍵の管理

注：弊社は、2 3 術支援

Source：YouTubeにプロジェクト紹介ビデオ有り（https://www.youtube.com/watch?v=dn2q2gGue1A&feature=youtu.be）

目次

ブロックチェーン導入をお考えの企業様へ提供可能なサービス

ビジネスコンサルティング	• ブロックチェーン企画・開発のためのコンサルティング • ビジネス・技術の両面からブロックチェーン特有の課題抽出と、現在の技術における現実的な解決策を提示
技術コンサルティング・アドバイザリー	• ブロックチェーン開発過程における、技術面でのアドバイスを提供
受託開発	• ブロックチェーン開発において、ブロックチェーン部分の開発を受託（ブロックチェーン以外の部分は、ゲーム会社様にて開発いただく）
発行・取引プラットフォーム提供	• 弊社開発プラットフォーム（KARUTA / ICO launchdesk）をカスタマイズ提供

弊社の特徴

最も古く実績多数のブロックチェーン専門企業

1. 国内トップクラスの実績から得られた知見

2. 数多くビジネスとコンサルティング、開発の経験、ノウハウ

3. 幅広いブロックチェーン実装への知見

- 実際の事例からよくある問題点、落とし穴を熟知
- より意味のあるブロックチェーン活用方法を提供
- 無意味な検証を回避して、無駄な時間とコストをカット
- コンサルティングチームと開発チームの有機的な連携


ConsensusBase