CurrencyPort

金融分野へのブロックチェーン利活用に際する実装課題と安全対策

カレンシーポート株式会社
代表取締役・CEO　杉井　靖典

2016年8月23日

日本銀行　第1回　FinTechフォーラム

登壇者プロフィール／杉井 靖典（Yasunori Sugii）

- ✓ 経済産業省　　ブロックチェーン検討会　委員
- ✓ 日本銀行　　決済システムフォーラム　プレゼンター
- ✓ ブロックチェーン推進協会（BCCC）　副理事長
- ✓ 日本ブロックチェーン協会　会員
- ✓ 書籍「ブロックチェーンの衝撃」
  第４章　ブロックチェーン産業へのインパクト寄稿

会社概要

カレンシーポート株式会社 - CurrencyPort Limited

【会社情報】

本　社　　東京都 千代田区 丸の内
設　立　　2015年10月1日
資本金　2700万円（資本準備金を含む）
メンバー 12名
〈2016年8月 現在〉

【事業目的】

1. 電子財布システムの開発
2. 資金決済・送金システムの開発
3. 外国為替両替システムの開発
4. 自動売買アルゴリズムの研究開発
5. 分散合意形成アルゴリズムの研究開発
6. 越境商取引システムの開発
7. 店舗向け販促・販売システムの開発

FINOLAB
THE FINTECH CENTER of TOKYO

私たちが関与した実証実験・事例

ブロックチェーン技術の実証実験　～国内企業4社協働による取り組み～

2016-02-16 プレスリリース

みずほフィナンシャルグループ
シンジケートローン業務に関する要件提示

電通国際情報サービス
業務システム設計、業務シナリオ作成、プロトタイプ開発

カレンシーポート
ブロックチェーン技術、スマートコントラクト開発支援

日本マイクロソフト
Azure BaaS（ブロックチェーンクラウドサービス）の提供

私たちが関与した実証実験・事例

低トランザクション市場を想定した、技術的な限界や可能性について評価

2016-04-07 プレスリリース

証券取引所

JPX JAPAN EXCHANGE GROUP

証券会社

野村證券 NOMURA

MUFG

SBI GROUP SBI証券

他（非公表）、数社

技術協力

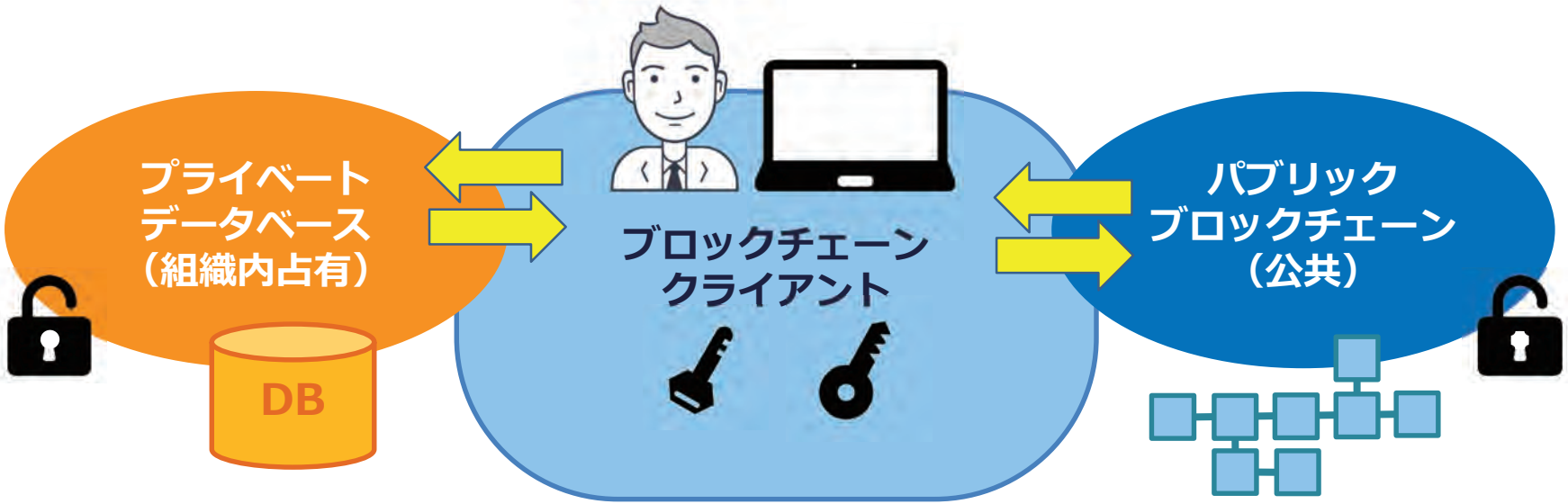
NRI 未来創発 Dream up the future.

CurrencyPort

ブロックチェーン活用システムの構成例（1）

CurrencyPort

組織内にあるドキュメントの存在証明・公証等に活用したい場合に検討例



- ✓ 組織固有の業務
- ✓ 組織内の機密情報
- ✓ 複雑で高度な処理
- ✓ 高速な処理
- ✓ 即時のファイナリティ

実装例）

factom

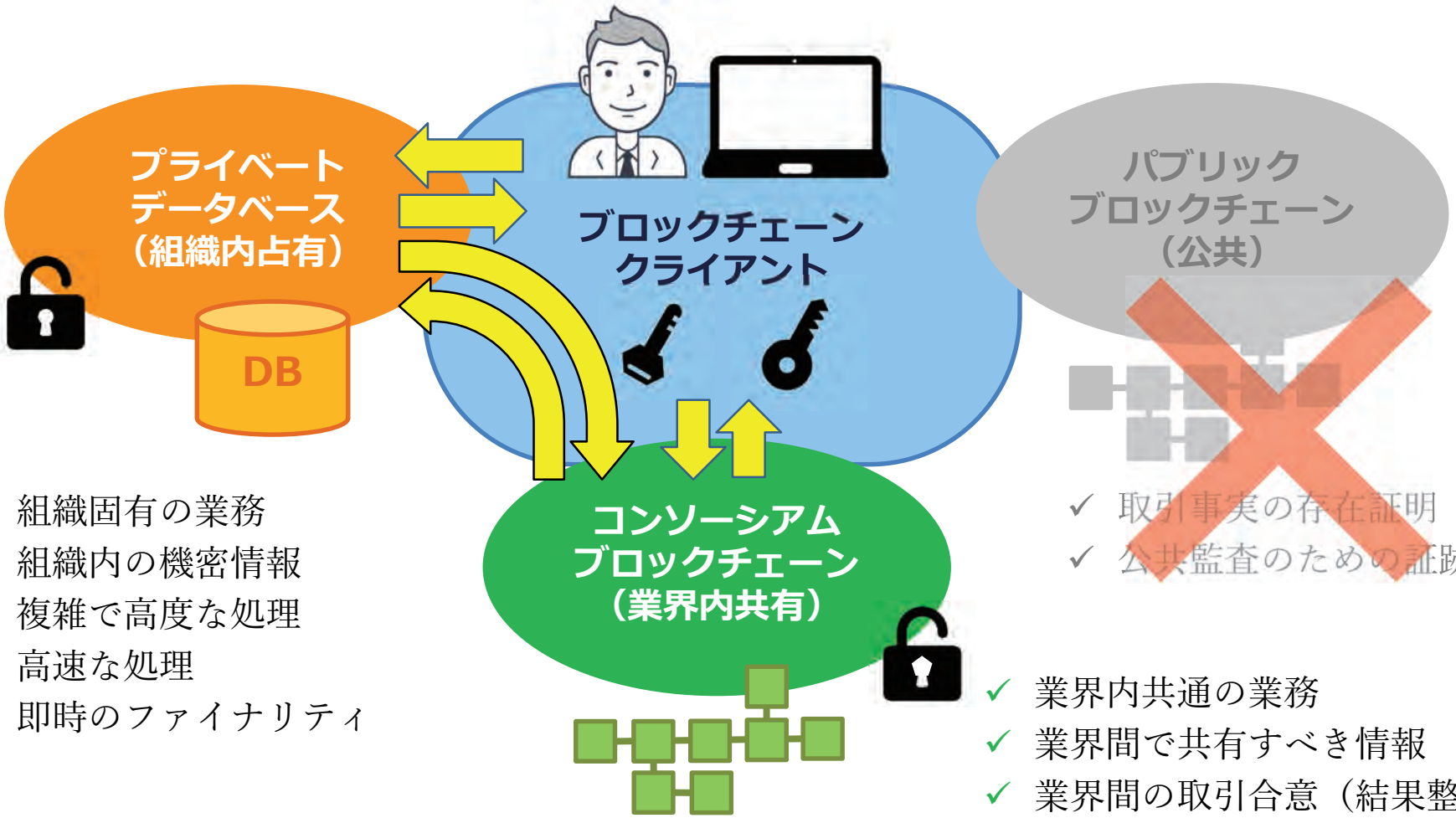
※実際には外部の分散ストレージとの併用が必要

- ✓ 取引事実の存在証明
- ✓ 公共監査のための証跡

ブロックチェーン活用システムの構成例（2）

CurrencyPort

コンソーシアムの規模が小さいと、ブロックチェーンの特性が十分に活きない



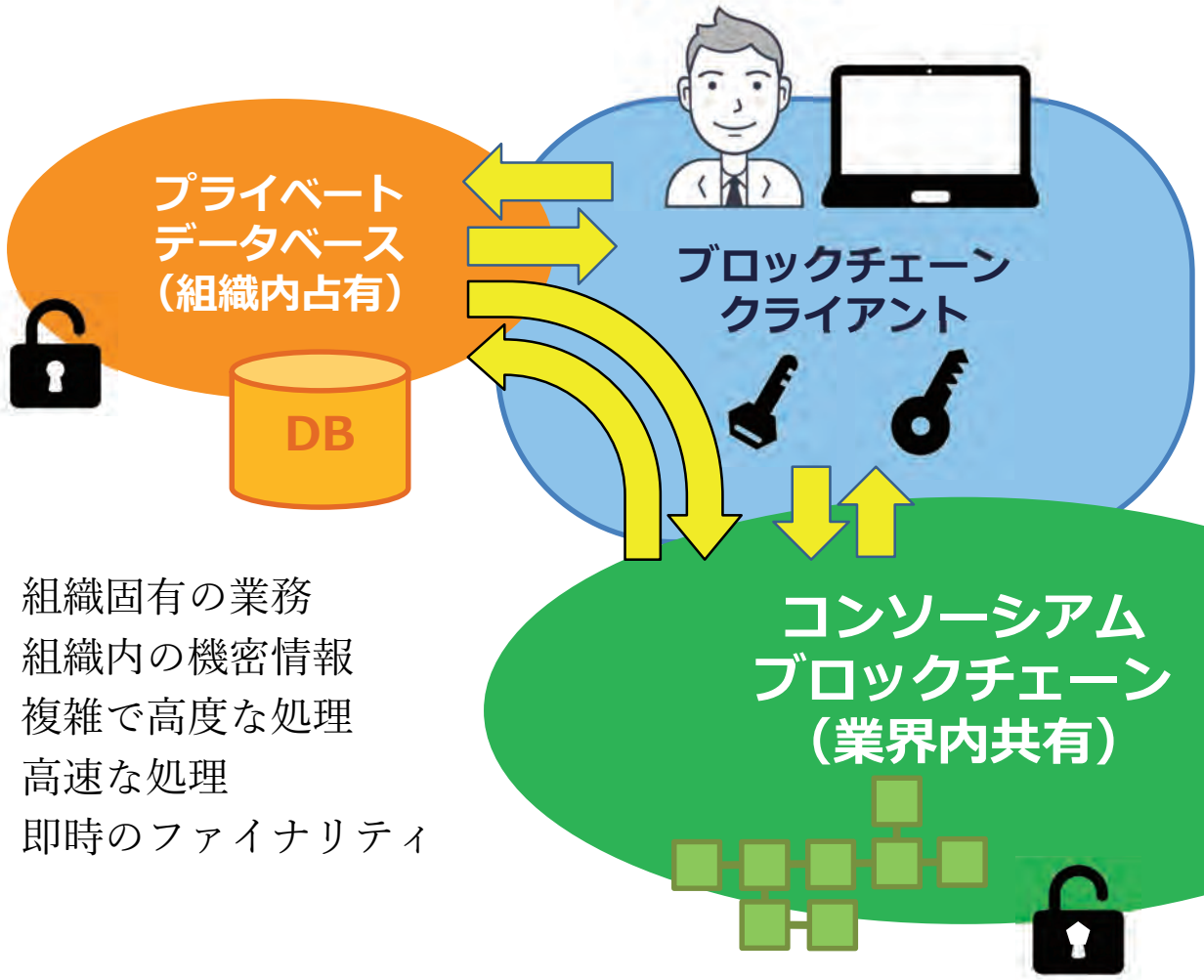
- ✓ 組織固有の業務
- ✓ 組織内の機密情報
- ✓ 複雑で高度な処理
- ✓ 高速な処理
- ✓ 即時のファイナリティ

- ✓ 取引事実の存在証明
- ✓ 公共監査のための証跡

- ✓ 業界内共通の業務
- ✓ 業界間で共有すべき情報
- ✓ 業界間の取引合意（結果整合性）

ブロックチェーン活用システムの構成例（2-2）

コンソーシアムの規模が大きくなると、パブリック性をもつようになる



- ✓ 組織固有の業務
- ✓ 組織内の機密情報
- ✓ 複雑で高度な処理
- ✓ 高速な処理
- ✓ 即時のファイナリティ

- ✓ 取引事実の存在証明
- ✓ 公共監査のための証跡
- ✓ 業界内共通の業務
- ✓ 業界間で共有すべき情報
- ✓ 業界間の取引合意

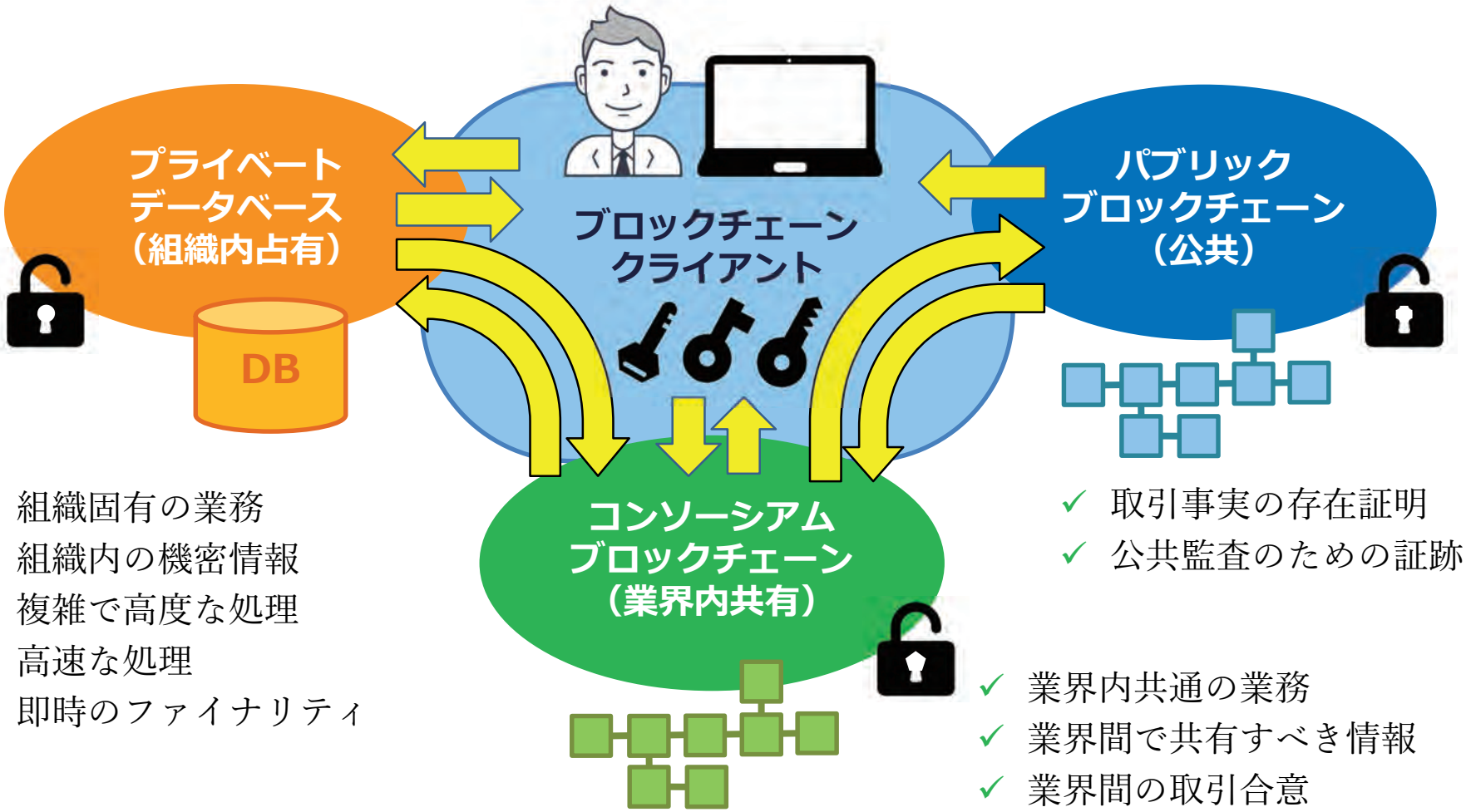
例えば数百・数千の組織が加入するネットワークならパブリックになる

例）全国・全世界規模の
銀行間ネットワーク
証券会社間ネットワーク

ブロックチェーン活用システムの構成例（3）

CurrencyPort

小さなコンソーシアムでのブロックチェーン活用想定した場合の実用的な例



- ✓ 組織固有の業務
- ✓ 組織内の機密情報
- ✓ 複雑で高度な処理
- ✓ 高速な処理
- ✓ 即時のファイナリティ

- ✓ 取引事実の存在証明
- ✓ 公共監査のための証跡

- ✓ 業界内共通の業務
- ✓ 業界間で共有すべき情報
- ✓ 業界間の取引合意

データベースとブロックチェーンの共存（CAP定理の補完）

CurrencyPort

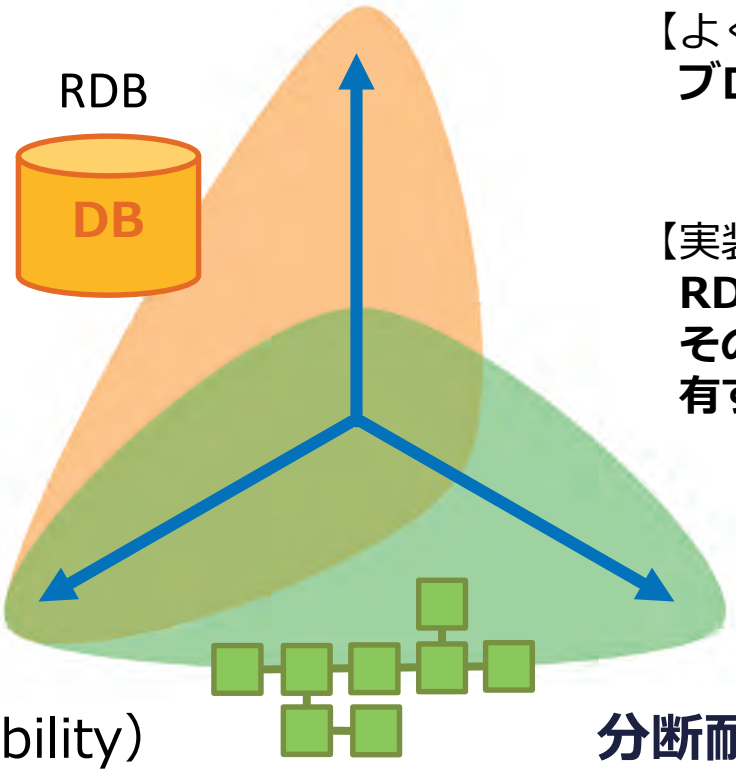
ブロックチェーンはデータベースを置き換えるような技術ではない

一貫性（Consistency）

例えば
行内勘定系

RDB

DB



可用性（Availability）

分断耐性（Partition-tolerance）

Blockchain

例えば
銀行間ネット

【よく言われるブロックチェーンの課題】
ブロックチェーンのファイナリティは不明瞭

【実装案】
**RDBでトランザクションの一貫性を担保し
その結果をブロックチェーンに分断耐性を
有する監査付きの取引ログとして記録する**

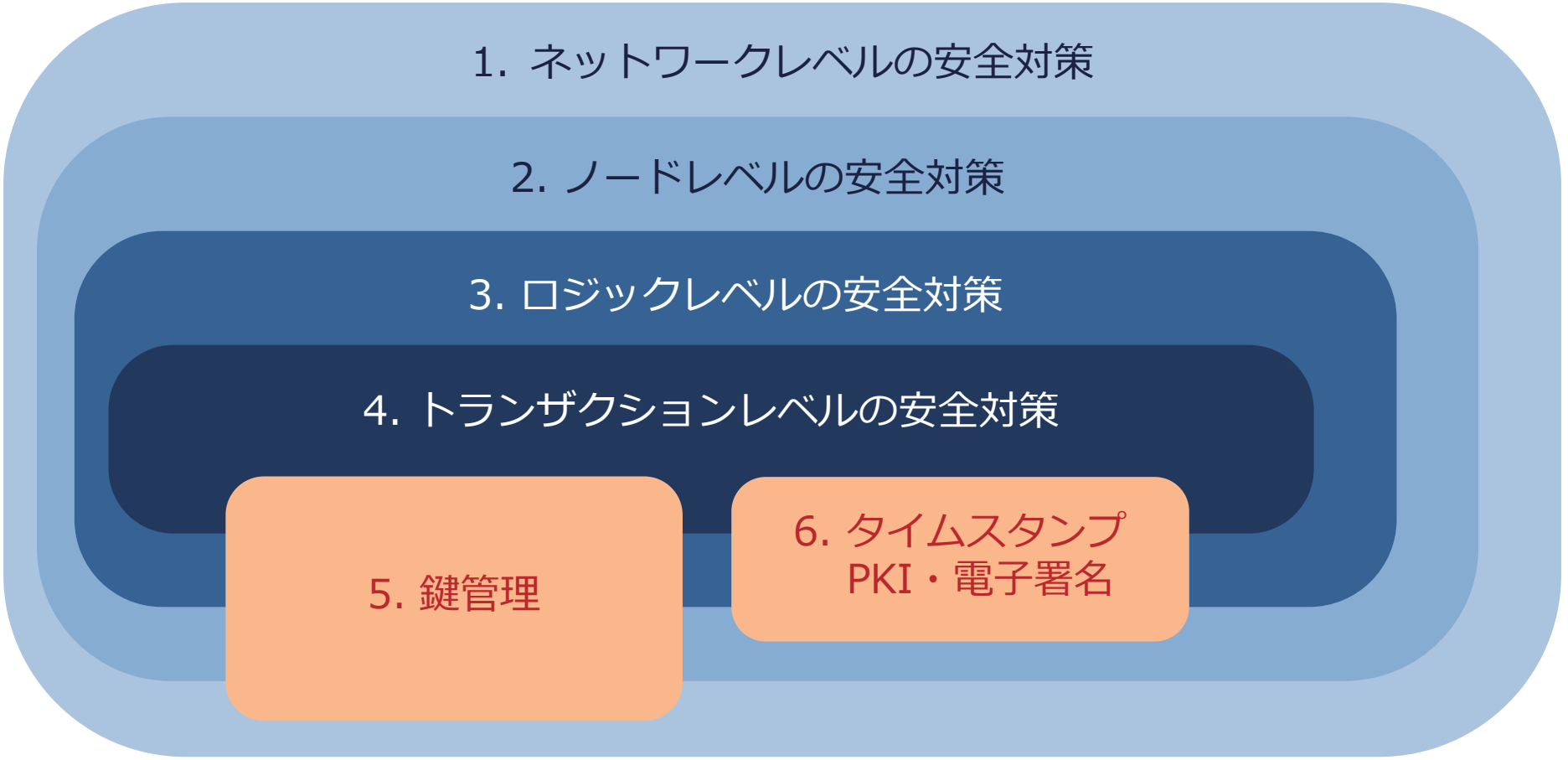
（例：ポストトレード処理）

**RDB + Blockchain
ハイブリッドで実用化をめざす**

ブロックチェーンのセキュリティ

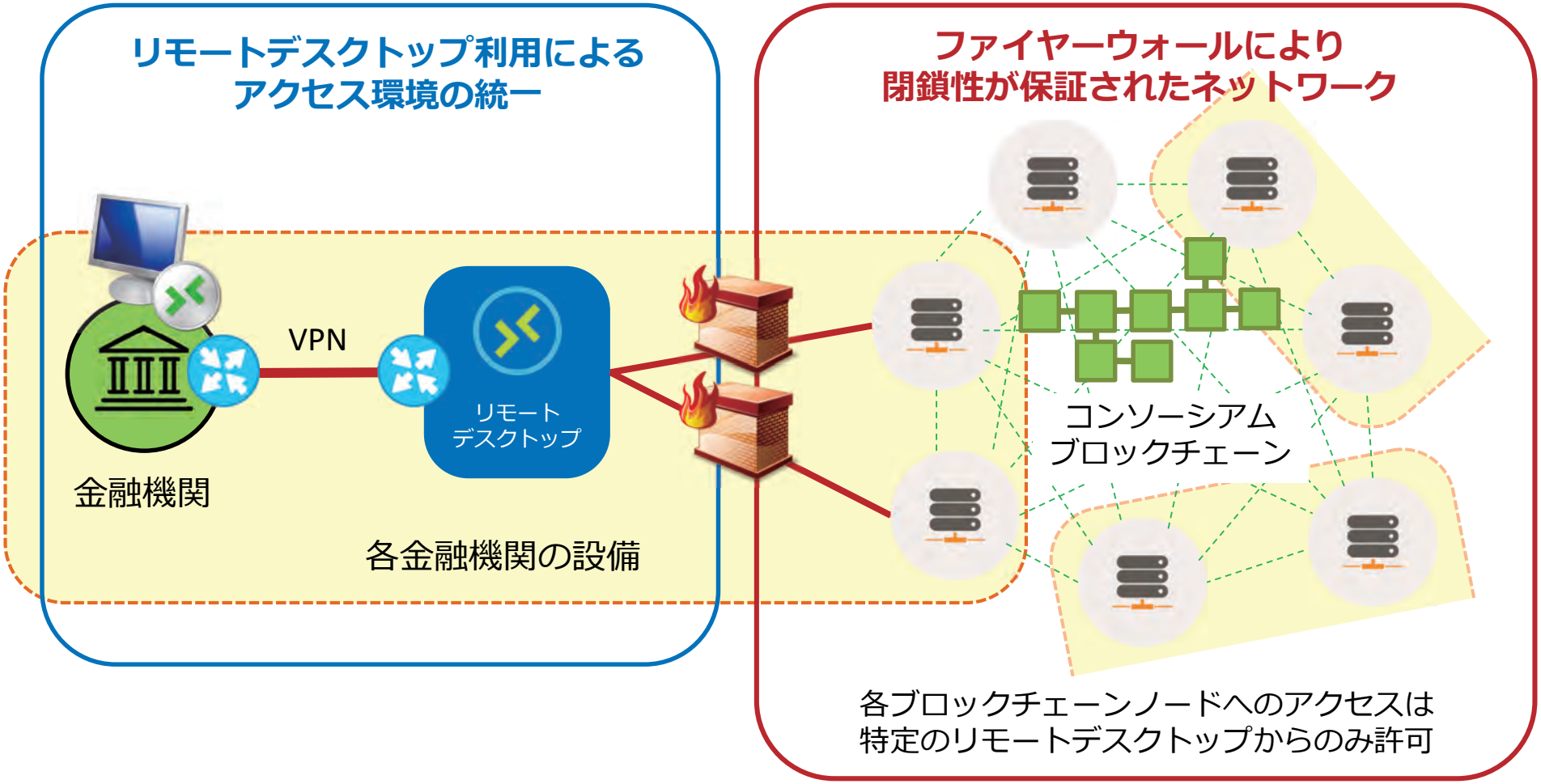
CurrencyPort

従来のシステムと同様に「多層防御」による安全対策が有効



ブロックチェーンのセキュリティ

1. ネットワークレベルの安全対策（RDP・ファイヤーウォール）



ブロックチェーンのセキュリティ

2. ノードレベルの安全対策

エンタープライズ向けに開発されたブロックチェーンでは、
以下のような細かなアクセス権限設定が可能なものもあります。

- ✓ **トランザクションを送れるか否か**
- ✓ **コントラクトコードを呼び出せるか否か**
- ✓ **コントラクトを作れるか否か**
- ✓ **アカウントを作れるか否か**
- ✓ **承認に参加できるか否か**　など

パーミッションド
ブロックチェーン

実装例）

eris INDUSTRIES

ブロックチェーンのセキュリティ

3-1. ロジックレベルの安全対策（ドキュメントの閲覧制御）

ブロックチェーンで取扱うデータを必要のある参加者にのみ閲覧可能にするため、
以下のような手順でドキュメント処理を行う「暗号デーモン」を実装する

1. コンソーシアムの各参加者は、各自公開鍵暗号用のキーペア（秘密鍵と公開鍵）を作成し、特に**秘密鍵は他者がアクセス不能な安全な場所に保管**しておく。

2. 秘密文書を送信したい者は、文書送信時に**ランダムな共通鍵を作成**し、その共通鍵を用いて当該文書を暗号化し、**分散ストレージに保管**する。

次ページ

3. 秘密文書にアクセス許可を与えたい他の参加者の公開鍵を取り寄せ、2.で暗号化に用いた**共通鍵を暗号化**し、当該参加者宛に送付する。

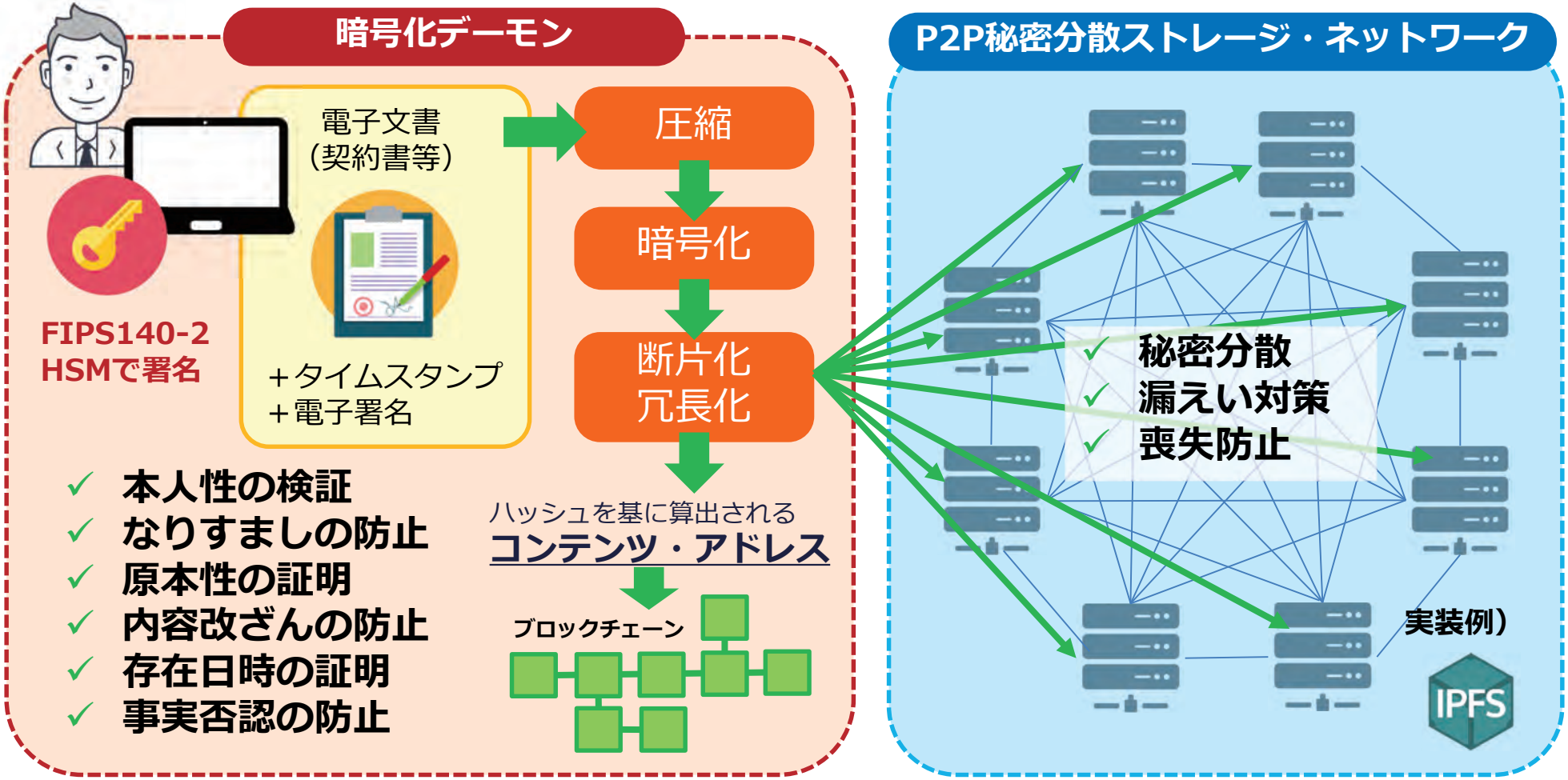
FIPS140-2
HSM

4. 暗号化された共通鍵を受信した参加者は、1.で保管した自身の**秘密鍵を用いて復号**することで、秘密文書を復号するための共通鍵を得られ、**分散ストレージ上に保管された秘密文書**にアクセスできる。

次ページ

ブロックチェーンのセキュリティ

3-2. ロジックレベルの安全対策（ドキュメントの秘密分散）

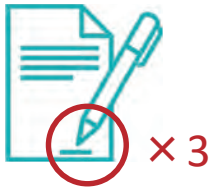


ブロックチェーンのセキュリティ

4-1. トランザクションレベルの安全対策（取引権限制御）

「マルチシグネチャ技術」

送信者



ブロックチェーンにより
実装方法は異なる

例）署名者グループ5名のうち、
3名がサインすれば有効となる取引

3 of 5 multi-signature transaction

受信者

実用例）ADR

高額取引のエスクロー取引を行う際「販売者」「購入者」「仲裁人」の三者を予め署名者に指名しておき、通常取引の際は販売者と購入者の双方のサインがあれば自動的に約定させたいが、何かトラブルが生じた際、紛争解決のため仲裁人がその裁定を可能とする権限を与えたい。

（ 2 of 3 multi-signature ）

4-2. トランザクションレベルの安全対策（トレード・シークレット）

「リング署名技術」

送信者

関連技術として署名グループのうち
署名生成事実のない者は否認できる
技術も併せて研究されている

署名者グループのメンバーのうちの
誰かが署名したことは保証できる

しかし、
それが**誰であるかは特定できない**

受信者

第三者

受信者も第三者も
同様に署名検証可能

CurrencyPort

4-3. トランザクションレベルの安全対策（トレード・シークレット）

「秘匿トランザクション技術」

Input	Output
1.2 ＋ 1.0 ＋ 0.8	2.4 ＋ 0.6

3.0 = 3.0

Input	Output
1.2 *x G* ＋ 1.0 *x G* ＋ 0.8 x G	2.4 x G ＋ 0.6 x G

3.0*G* = 3.0*G*

離散対数問題の困難性に依存

楕円曲線における離散対数ベースポイント ***G***
を各入出力に掛けて、両辺を比較する。

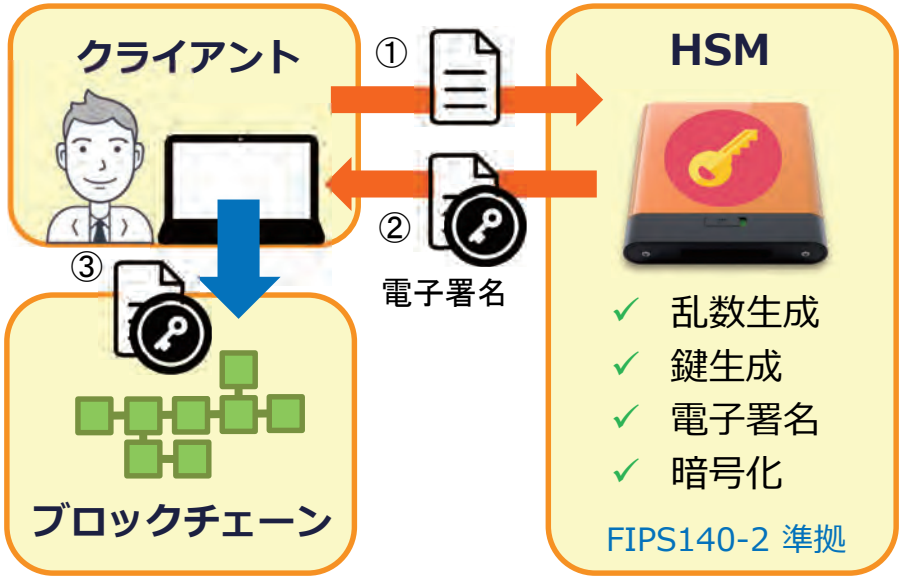
Input と Output の「等号性」が示せれば、正常な取引勘定が行われたと言える

ただし、プロトコルレベルでの実装が必要

ブロックチェーンのセキュリティ

5. 鍵管理（HSM／ハードウェア・セキュリティ・モジュールの活用）

- ✓ 鍵管理等、暗号処理業務専用のハードウェアを用いる
- ✓ 耐タンパ性（機密解析困難性）のあるIC（セキュアエレメント）上に鍵を保管する
- ✓ 汎用コンピュータのメモリ上に鍵をロードしない（HSMの外部に鍵が一切露出しない）
- ✓ 乱数生成、鍵生成、トランザクションの電子署名、暗号化はハードウェア側で行う
- ✓ FIPS140-2 暗号モジュールのセキュリティ要件（米国連邦標準規格）への準拠



HSMデバイスの例）

アプライアンス型

USBドングル型

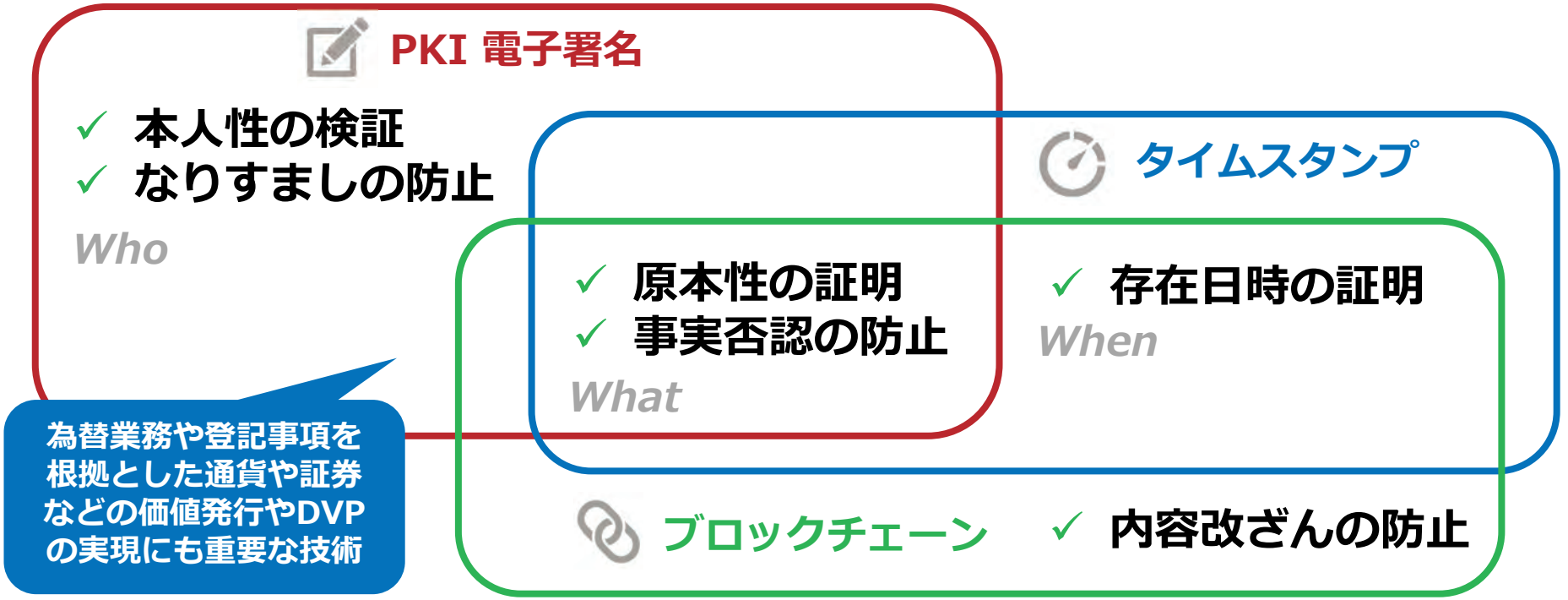
クラウドHSMサービスの例）

- ✓ Microsoft Azure key vault
- ✓ Amazon Key Management Service

ブロックチェーンのセキュリティ

6. タイムスタンプ + PKI・電子署名 + ブロックチェーン

オリジナルのブロックチェーンシステムは「トラストレス」を標榜する実装が一般的なので電子署名の際に公開鍵暗号基盤（PKI）を利用しませんが、業務上 KYC/AML が必須となる金融分野の「トラステッド」なブロックチェーンシステムでは特に、PKIの利用が有効 です。



スマートコントラクト

ブロックチェーン上に自律執行性のある契約をプログラミングできる技術

例）あらかじめ取り交わされた貸借契約の内容に基づき、
借り手の口座からローン貸し手の口座に毎月の返済を自動的に行う。

例）サービス予約時、利用者が資金のエスクローを行った時点で自動的にバウチャートークンを発行する。サービス履行後、履行状況によりエスクローがリリースされ、事業者口座に資金が移動される（予約キャンセルなどの条件付き一部払戻しにも対応）

【パブリックチェーンのオリジナル実装】

ethereum

【プライベートチェーン向けの派生実装】

eris INDUSTRIES

HydraChain

2016年上半期における国内金融機関の実証実験では
Ethereum系（プライベートチェーン向けの派生実装）が選択されることが多かった。

スマートコントラクトシステムに潜む罠

The DAO Attack 事件の例

➢ 何が起きたのか？

The DAO は、Ethereum のスマートコントラクト によって構築された 自律分散組織（DAO） に対する投資を目的とした仮想通貨(ETH)建てのファンドで、約150億円相当を調達した。

当該ファンドの割当てを管理するプログラムの部分に発見された再帰性ループの脆弱性が突かれ 2016年6月17日～18日に掛けて、調達した約1/3にあたる 仮想通貨（ETH）が流出 した。

➢ どうして起きたのか？

※バージョン管理による工夫は可能

- ✓ ブロックチェーンに記述されたコントラクトは、バグがあっても変更できない （Immutable）
- ✓ チューリング完全を実現 ⇒ プログラミングの自由度が高い ⇒ バグを含みやすい
- ✓ Ethereum ではチューリング完全のコントラクトと不可変のブロックチェーンが蜜結合
- ✓ 不特定多数が参加するパブリック・チェーンでは、仕様改定したい際の合意形成が困難

Ethereum 固有の問題ではなく、
Bitcoin でも問題になっている（ブロックサイズ変更の議論等）

安全なスマートコントラクト基盤の実現に向けた考察

CurrencyPort

The DAO Attack 事件から学べること

「コードは法だ」
の主張は正当なのか?

➢ 何が問題なのか？

プログラミングされている内容は、契約書と同義か?

技術と業務と法律のすべて長けていないと、コントラクトの内容を精査できない。

結局は「非中央集権組織（DAO）」の実現だと言いながらも、
実際には「開発者の信用や稼働実績」など従来通りに充分な評価が成されたコントラクトでなければ、安全に利用できないことが早晩実証された格好。

➢ 技術的に解決可能なのか？

Case1.

- ✓ コントラクトとブロックチェーンの分離
- ✓ 合意用チェーンと計算用サイドチェーン

HYPERLEDGER PROJECT　Lisk

Case2. ※2016年8月時点・構想中

- ✓ 想定外の状態遷移が発生しないステートチャート
- ✓ 企画者や法律家が記述可能なビジネスルール（BRMS）

nem　mijin

金融分野におけるブロックチェーンの安全対策・まとめ