Hyperledger Projectのセキュリティと方向性

平成28年8月23日
日本アイ・ビー・エム株式会社
グローバル・ビジネス・サービス事業
アソシエイトパートナー
高木　隆

ブロックチェーンのセキュリティインシデント

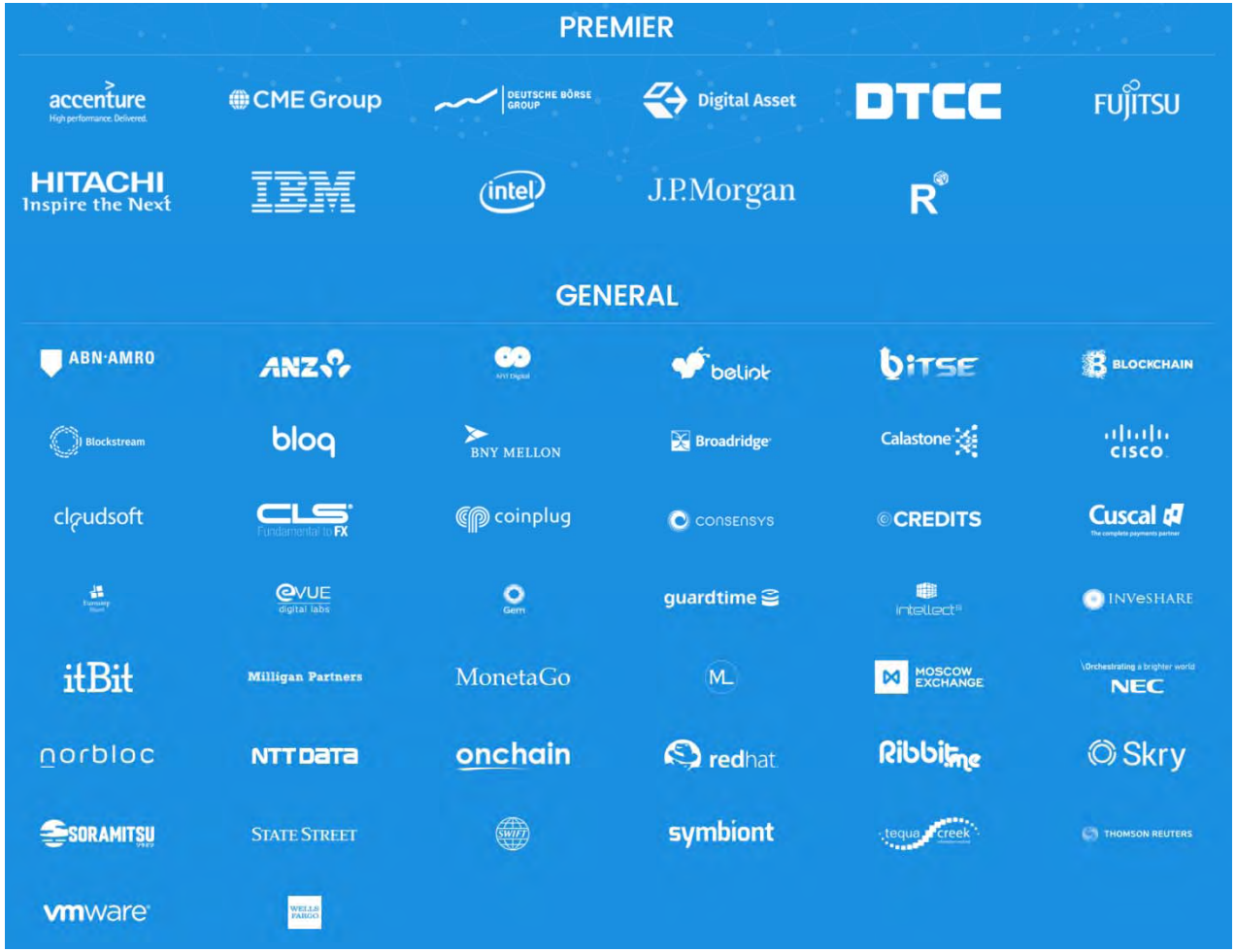
- ハッキング等により相応の仮想通貨資産が流出

情報セキュリティの3要素		関連インシデント
機密性	•許可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また開示しない特性	•**Mt. Gox**：**$450m**相当のビットコイン預かり資産を喪失（2014年） •**Bitfinex**：Multisig対策を施していたにも関わらず、**$60m**相当のビットコイン預かり資産を喪失（2016年7月）
完全性	•正確さ及び完全さの特性	•**The DAO**：**$50m**相当の仮想通貨イーサリウムが流出（2016年6月）
可用性	•許可されたエンティティが要求したときに、アクセス及び使用が可能である特性	–

課題
① **ブロックチェーンの入口・出口（鍵管理）**
② **取引の正確さ及び完全さの検証（コンセンサス）**

Hyperledger Project

- Linux Foundationのもと、業界横断でブロックチェーンのオープンスタンダードを検討

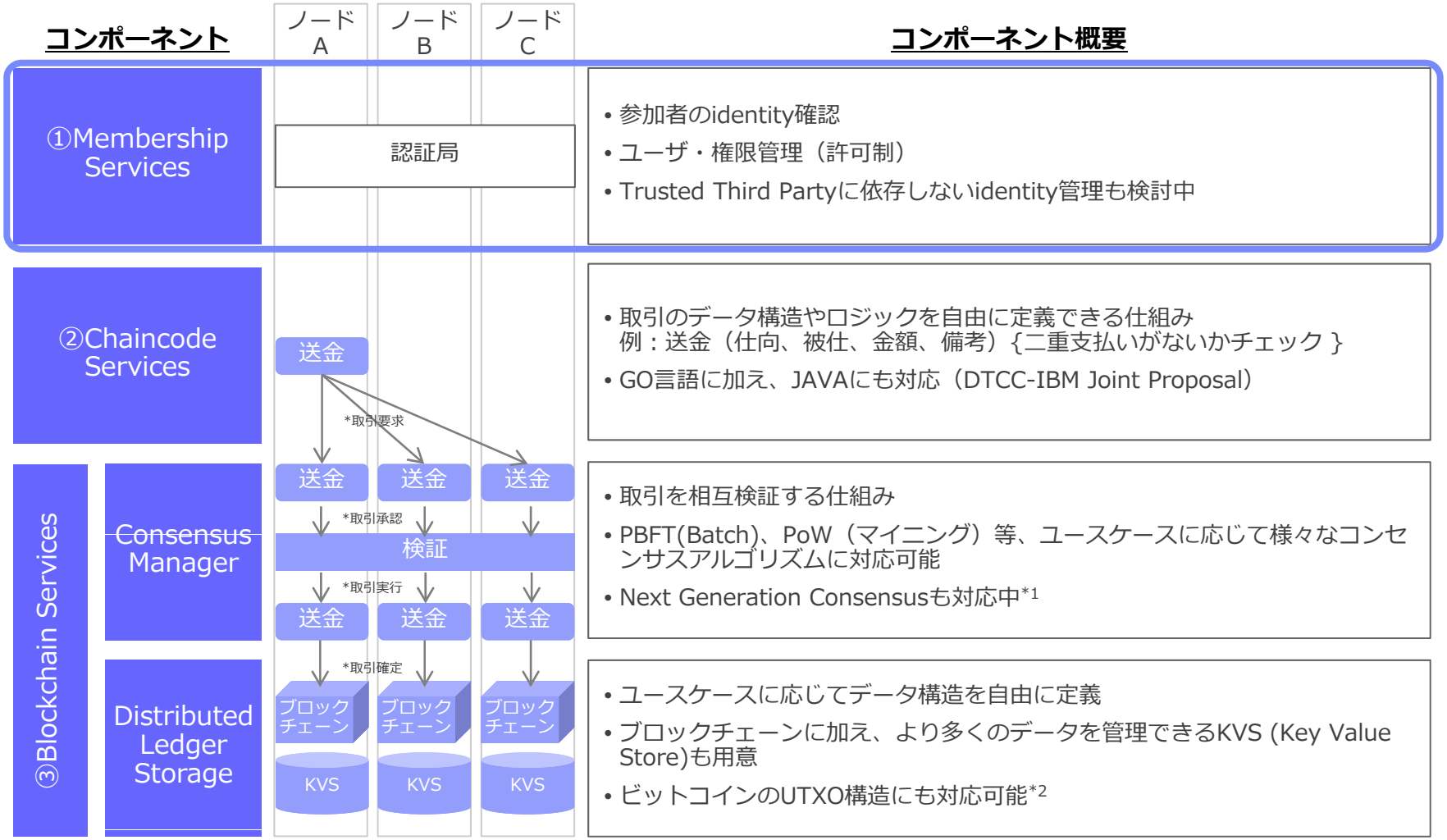


IBMの取組み

- ✓プライバシー要件にも対応したブロックチェーン基盤**OBC (Open Block Chain)**をコード提供
- ✓IBM OBCをDAH社のブロックチェーン基盤と統合（**Hyperledger Fabric**）
- ✓Hyperledger Fabric v.1に向けて対応中
- ✓DTCCと共同でスマートコントラクトのJAVA言語対応を実施

Hyperledger Fabric

- 機密性を確保する為の仕組みとして**Membership Services（認証局）**を導入

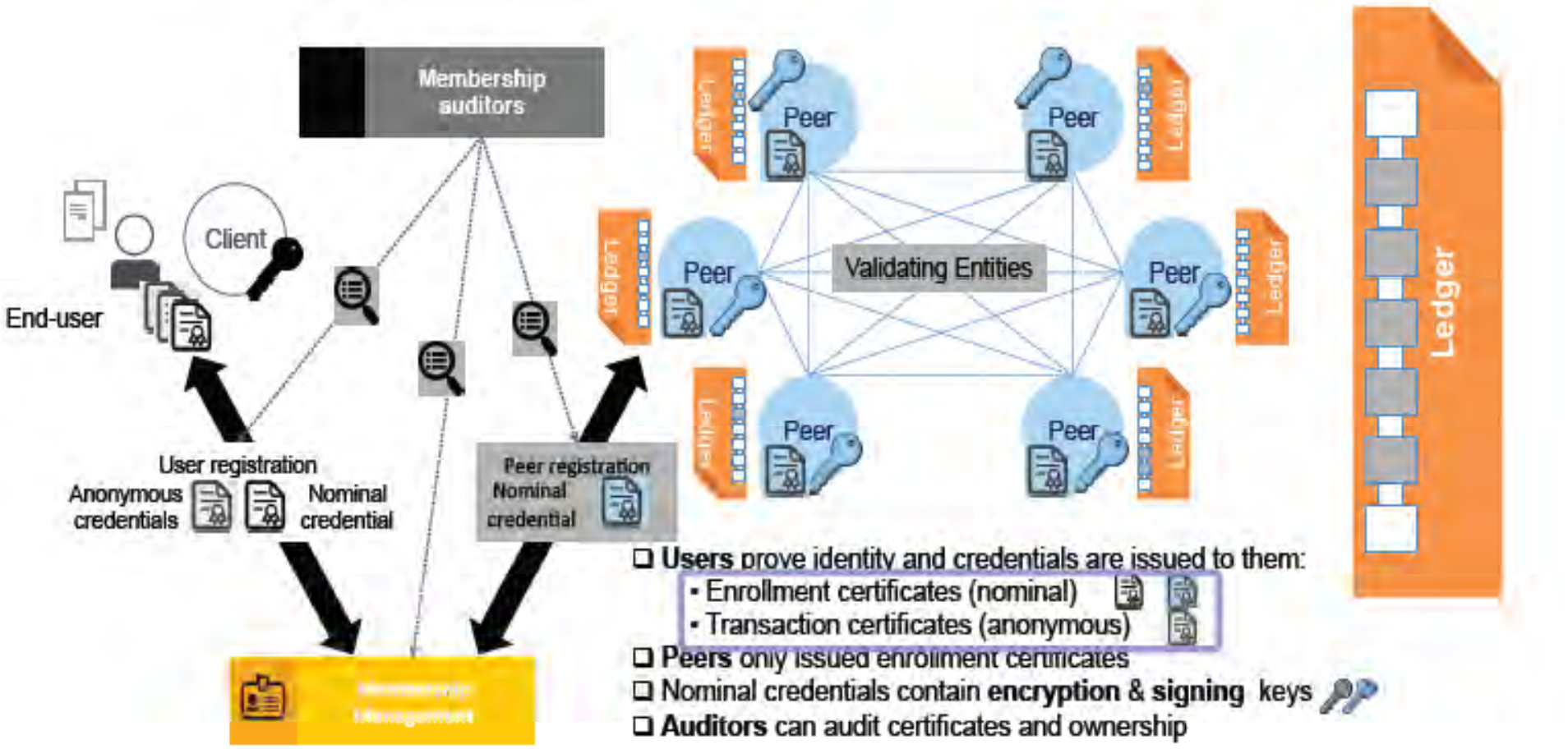


Hyperledger Fabricコンポーネントアーキテクチャー

*1 https://github.com/hyperledger/fabric/wiki/Next-Consensus-Architecture-Proposal
*2 https://github.com/hyperledger/fabric/tree/master/examples/chaincode/go/utxo

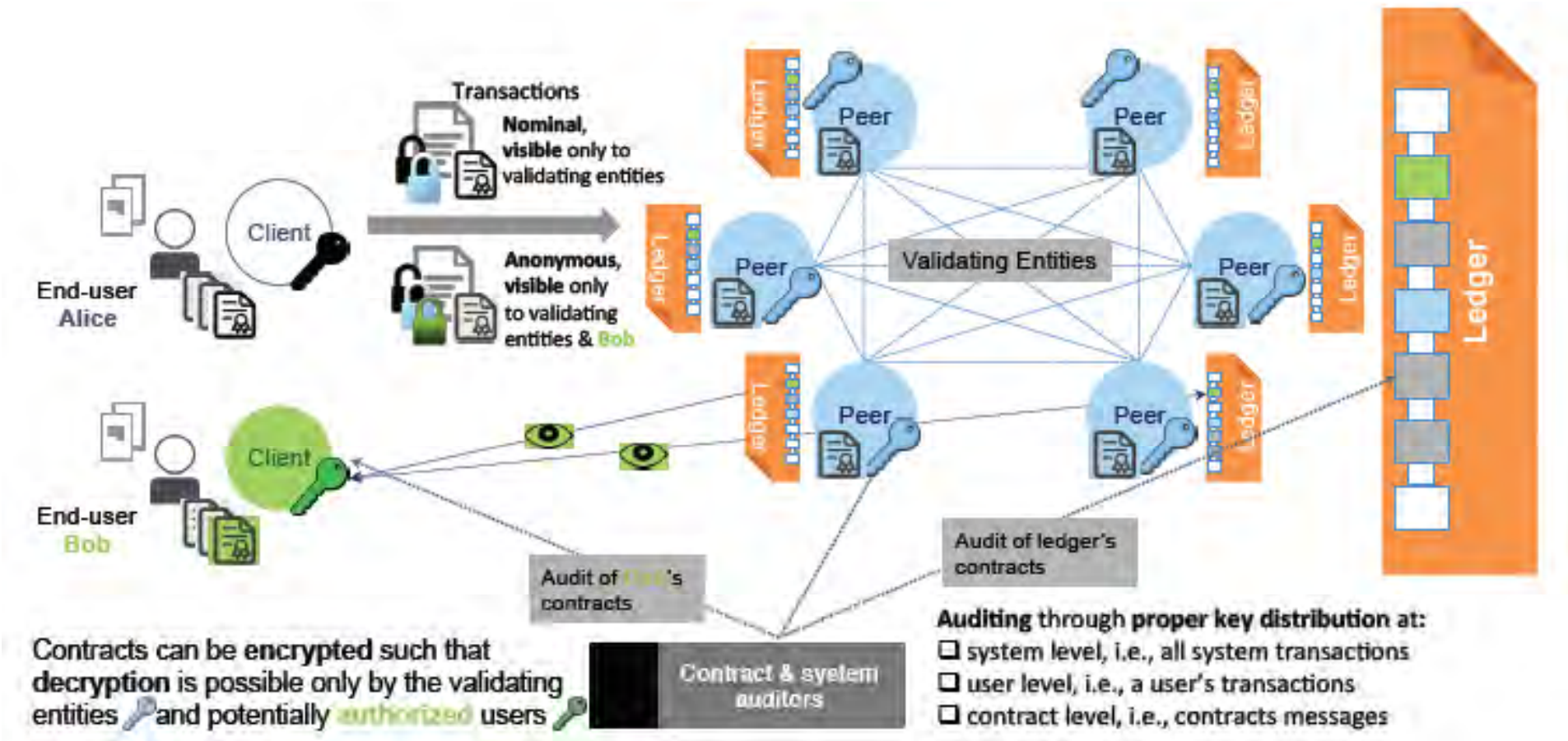
Membership Servicesの仕組み

- **Ecert**とは別に、期限が設定可能なワンタイム証明書**Tcert**を導入することで、鍵漏洩・紛失に伴うセキュリティリスクを低減



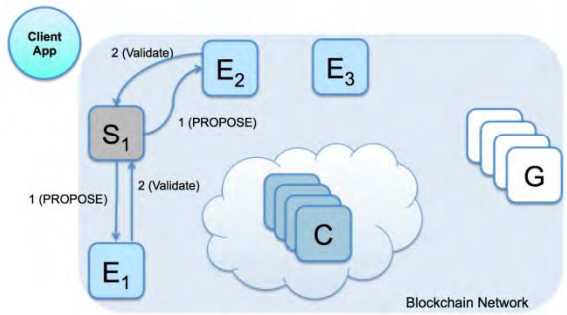
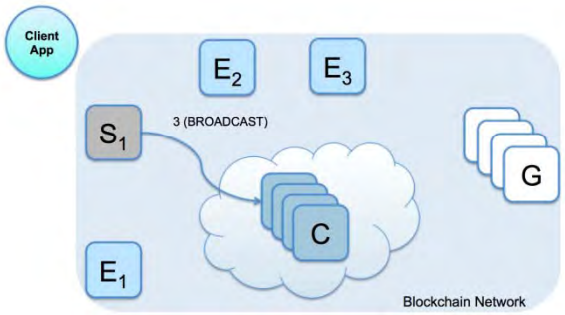
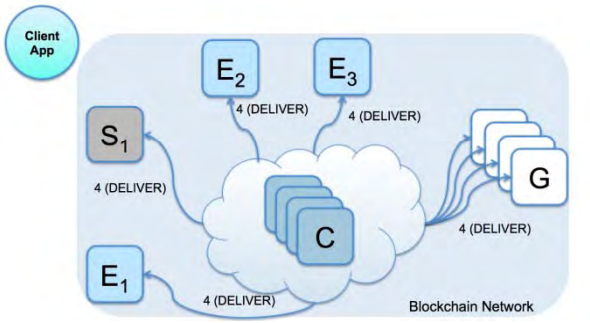
Membership Servicesの前提

- 検証ノードは検証用の鍵を保有する為、**既存の金融システムと同等のセキュリティ対策が行なわれていることを前提**とする



Next Generation Consensus

- 機密性・完全性・可用性を高めた新コンセンサスアルゴリズムをHyperledger Project内で検討中
- **取引の正確さ及び完全さを検証する仕組み**を整備することも検討
  （The DAO事件のようなスマートコントラクトの不正検知含め）

一次検証	二次検証	取引確定
		
• Submitting Peer S_1が Endorsement Peer E_1/E_2に一次検証を依頼 • Endorsement Peer E_1/E_2が一次検証を実施	• Submitting Peer S_1が取引をハッシュ化の上、Concentorに二次検証を依頼 • Concentorが二次検証を実施	• Concentorがブロックを配布

https://github.com/hyperledger/fabric/wiki/Next-Consensus-Architecture-Proposal参照

High Security business network for IBM Blockchain

- IBMからはハードウェアによる鍵管理も提供

ニュースルーム › ニュースリリース ›

IBM、業界最高水準のセキュアなITインフラが支える 新たなブロックチェーン向けクラウド・サービスを発表

企業間ネットワークのための新しいクラウド環境で、ブロックチェーン・エコシステムの性能、プライバシー、および相互運用性の検証が可能に
EverledgerがIBM Blockchainを活用してダイヤモンド等の高価な品物を追跡
IBM LinuxONEが、クラウドによる厳格な業界の規制やセキュリティーおよびコンプライアンス要件への対応を支援

Select a topic or year

↓ ニュースリリース　↓ 関連する resources

↓ 関連する XML feeds

TOKYO - 20 7 2016:
2016年7月20日

[米国ニューヨーク州アーモンク - 2016年7月14日（現地時間）発]

IBM（NYSE：IBM）は本日（現地時間）、ブロックチェーン・ネットワーク用のセキュアな環境を必要とする組織のための、新たなクラウド・サービスを発表しました。規制産業に属する企業にとって理想的なこの環境で、お客様は個人情報を扱うブロックチェーン・プロジェクトの検証と運用ができます。

サービスの特徴

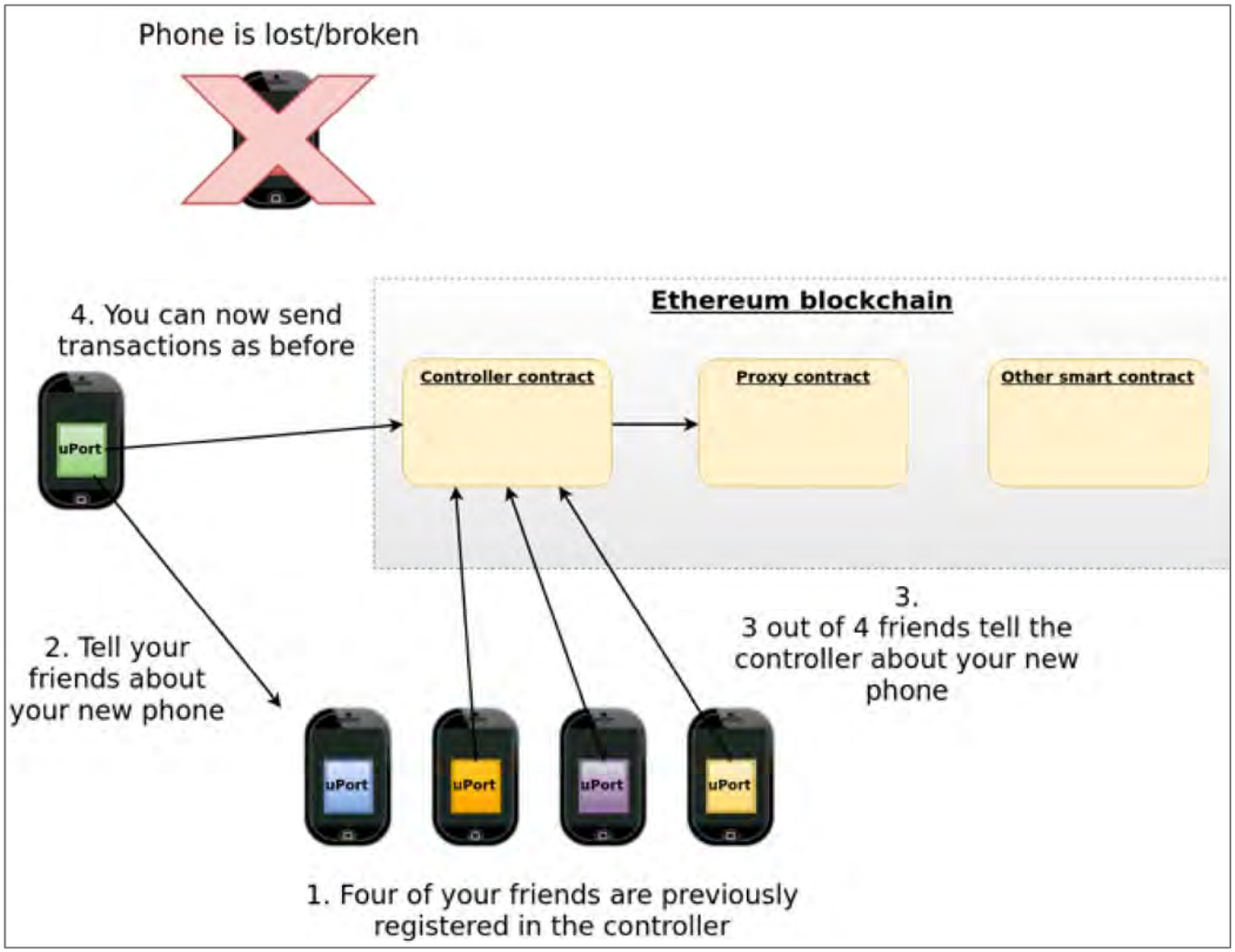
- ✓ セキュリティ機能が充実したIBM LinuxOne Emperorサーバーを活用したブロックチェーンサービス
- ✓ ブロックチェーンを活用してダイヤモンドなどの高価な品物の追跡と保護を行う**Everledger**がセキュアなインフラストラクチャーに支えられたIBM Blockchainでソリューションを構築

LinuxOne Emperorの特徴

- ✓ Hardware encryption with built-in accelerators for blockchain hashing, signing and security
- ✓ Faster responses with hipersockets
- ✓ Global Security Standards compliant
- ✓ **Tamper proof crypto keys in firmware/crypto cards**
- ✓ Unlimited random keys to encode transactions

uPort

- Hyperledger Project Identity WGではuPortの鍵管理も調査



『Ethereum & uPort』（ConsenSys Christian Lundkvist）より抜粋

安全性を踏まえたフェージング戦略例

- 安全性の観点から、**プライベートブロックチェーン+既存システム**から取り組むことを検討されている欧米金融機関も存在