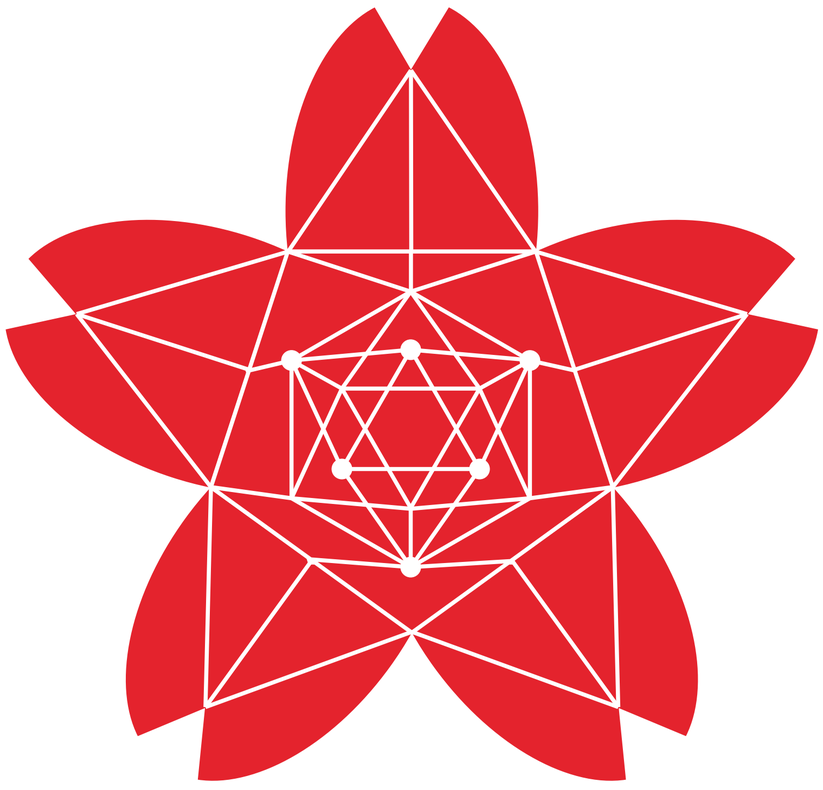


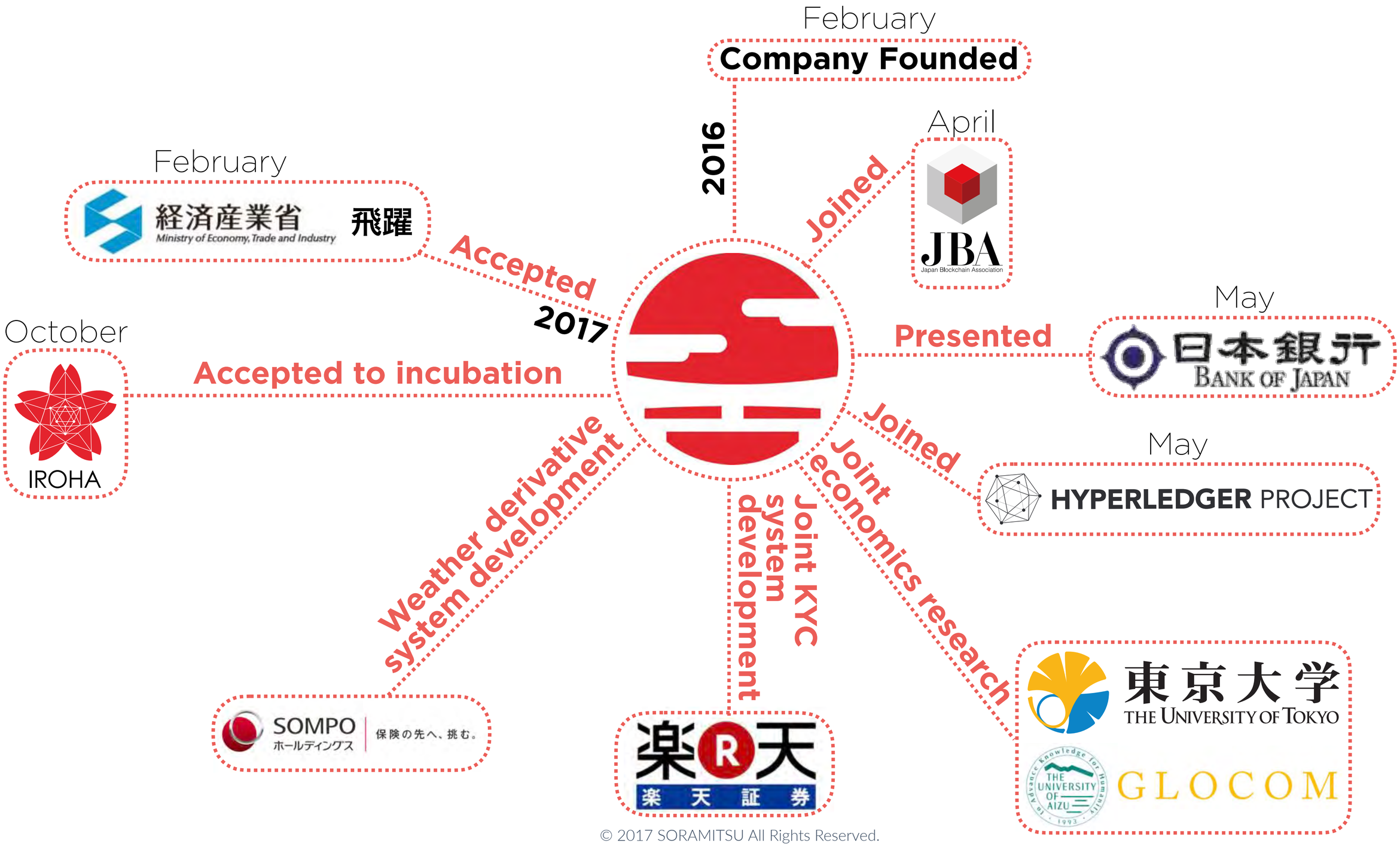
IROHA

平成29年2月28日

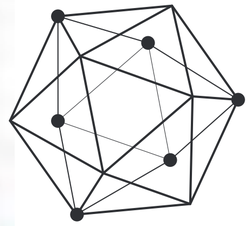
www.soramitsu.co.jp

About Soramitsu

ソラミツ株式会社は平成２８年２月に創立した日本のフィンテック会社である。



ハイパーレジャーとは



HYPERLEDGER PROJECT

ハイパーレジャーに採用された分散型台帳

ハイパーレジャーはソフトではなく、プロジェクトガバナンス機構である。現在いくつかのプロジェクトがあり、その中で以下の分散型台帳プラットフォームの開発が行なわれている。

プラットフォーム	最初の開発者	主な言語	ステータス
Fabric	IBM	Go	incubation
Sawtooth Lake	Intel	Python	incubation
いろは	ソラミツ	C++	incubation
Corda	R3	Kotlin	？？

分散型合意形成の基礎（1/2）

分散型台帳技術では複数技術の組み合わせに特徴があり、特に利用される分散型合意形成のアルゴリズムによってシステム運用に大きな影響を及ぼす。

アルゴリズムの種類	アルゴリズムの名称	採用しているプロジェクト	取引のFinality	所用時間
確率ビザチン合意形成（中本合意形成）	Proof of Work、Proof-of-Elapsed Time	ビットコイン、Hyperledger Sawtooth Lake	いいえ	数１０秒、数分
Broadcast-based BFT	PBFT	Hyperledger Fabric	はい	数秒、数１０秒
Chain-based BFT	スメラギ	Hyperledger Iroha	はい	数秒

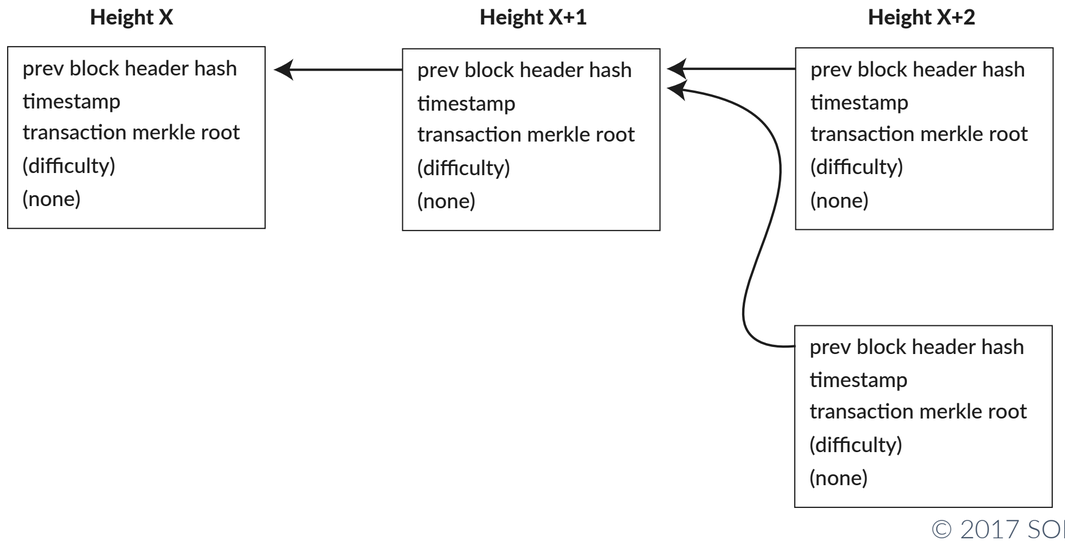
分散型合意形成の基礎（2/2）

サーバー停止、虚偽の処理、ランダムに応答がない等の状態はビザンチンfaultといい、分散型システムにとっては大きな課題であるが、分散型合意形成システムの利用により現実的に解決される。

中本合意形成

各サーバーはそれぞれブロックを作成する権利を獲得しようと競争する為、参加する台数の制限がない。但し、確率的にブロックが作成される為、常に台帳が一時的に分岐する可能性があり、取引の確定が困難。

例：



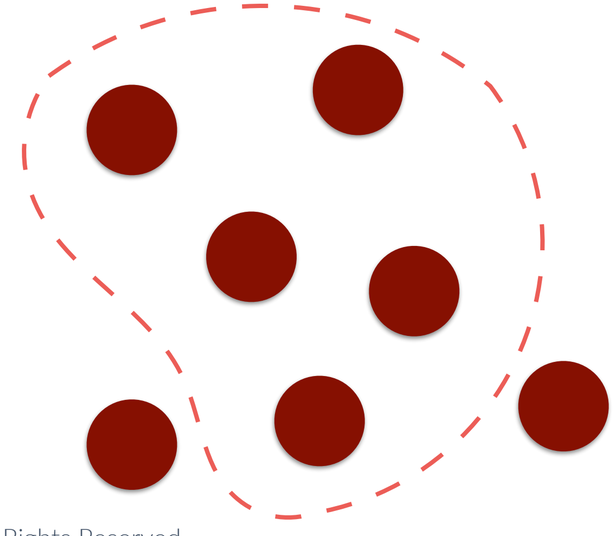
Byzantine Fault Tolerance

f := ビザンチンfaultyサーバーの数

最先端のアルゴリズムにおいては、3f+1台のサーバーが必要なため、参加するサーバーのアイデンティティを認証する必要がある。

例：f = 2

3f+1台 サーバーが必要



その中、2f+1台が認証することが必要

Hyperledgerいろはの特徴

日本初で唯一「Hyperledgerプロジェクト」に採用されているブロックチェーン。また、IBM、Intelに続いて世界で3番目のプロジェクト。

※日本のブロックチェーンスタートアップ企業である、ソラミツ株式会社は、ブロックチェーン技術の発展に寄与するために、Linux Foundationのオープン・ソース「Hyperledgerプロジェクト」にプロジェクトネーム「いろは（Iroha）」としてコードを提供しました。

平成28年9月26日：Hyperledgerプロジェクトに提案。
平成28年10月13日：Incubation Statusとして正式に受諾されました。

- **シンプル開発API**
- **デジタルアセットツール**
- **モバイルアプリ開発ライブラリー**

Hyperledgerいろはの特徴（Fabric/Sawtooth Lakeとの違い）

・高パーフォマンス構造

　　システム構造はユーザー向けのアプリに基づいており、
　　低レテンシーのシンプルな構造

・新しい合意形成アルゴリズム

　　Chain-based BFT algorithm: スメラギ

・モバイルアプリ開発向けのライブラリー

　　安価かつ安全にアプリを開発する事ができる

・アセット発行可能な取引種類

　　チェーンコードを実装せずにデジタルアセットを発行する
　　ことが可能

Hyperledgerいろはの特徴（バージョン1.0の目的）

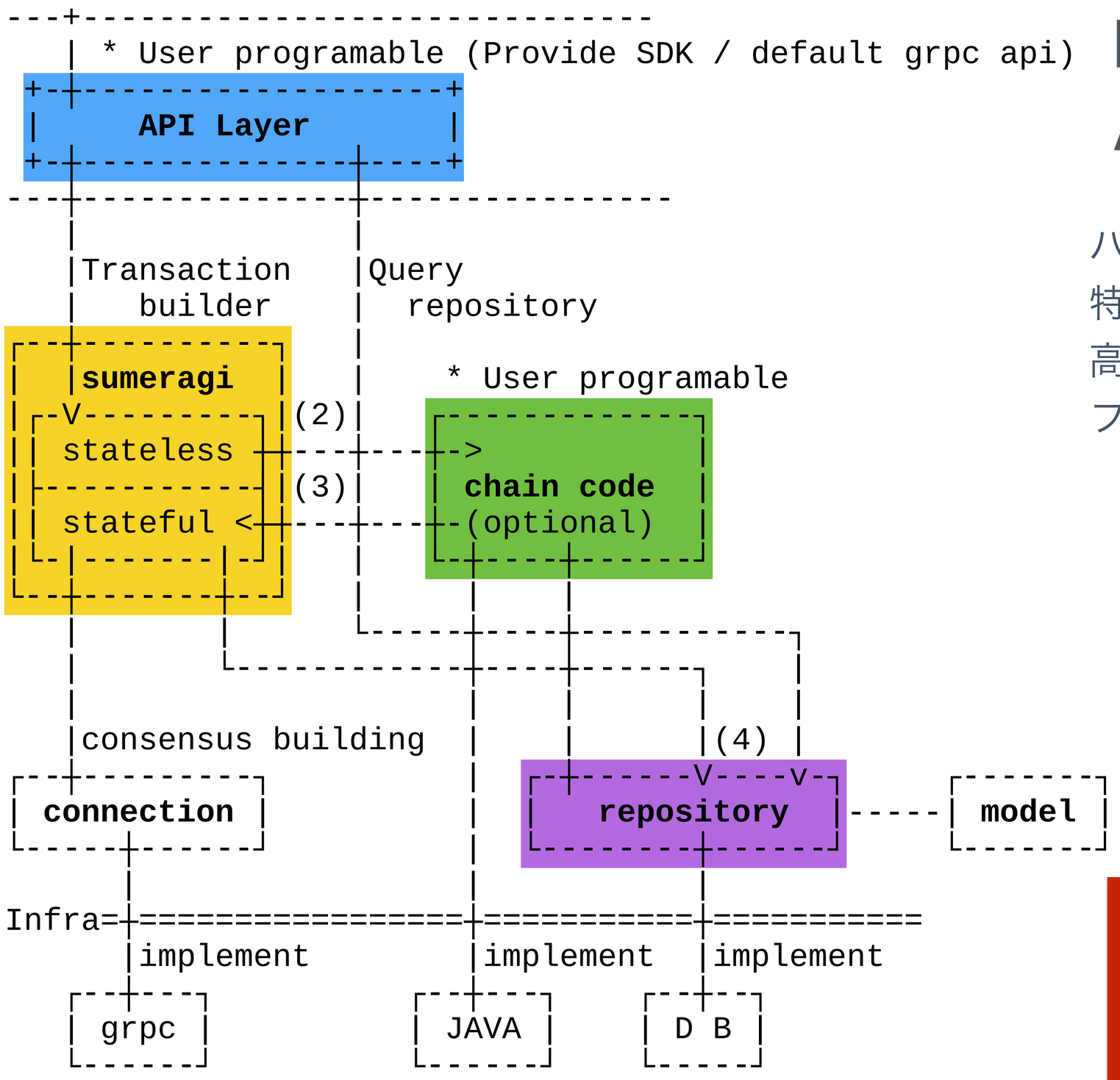
・高スループット
　　秒間数千件

・低レイテンシー
　　取引finality２秒以内を目標とする

・スケール可能
　　ビッグデータ対応

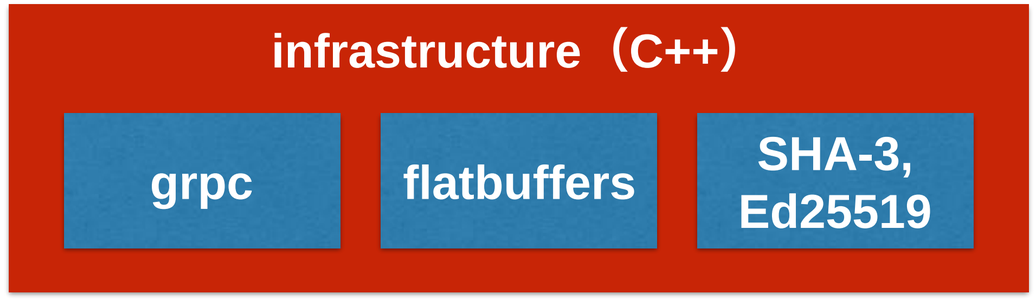
・モジュール化
　　コアな機能は他のプロジェクトでも利用可能な構造を作る

Hyperledgerいろはの構造



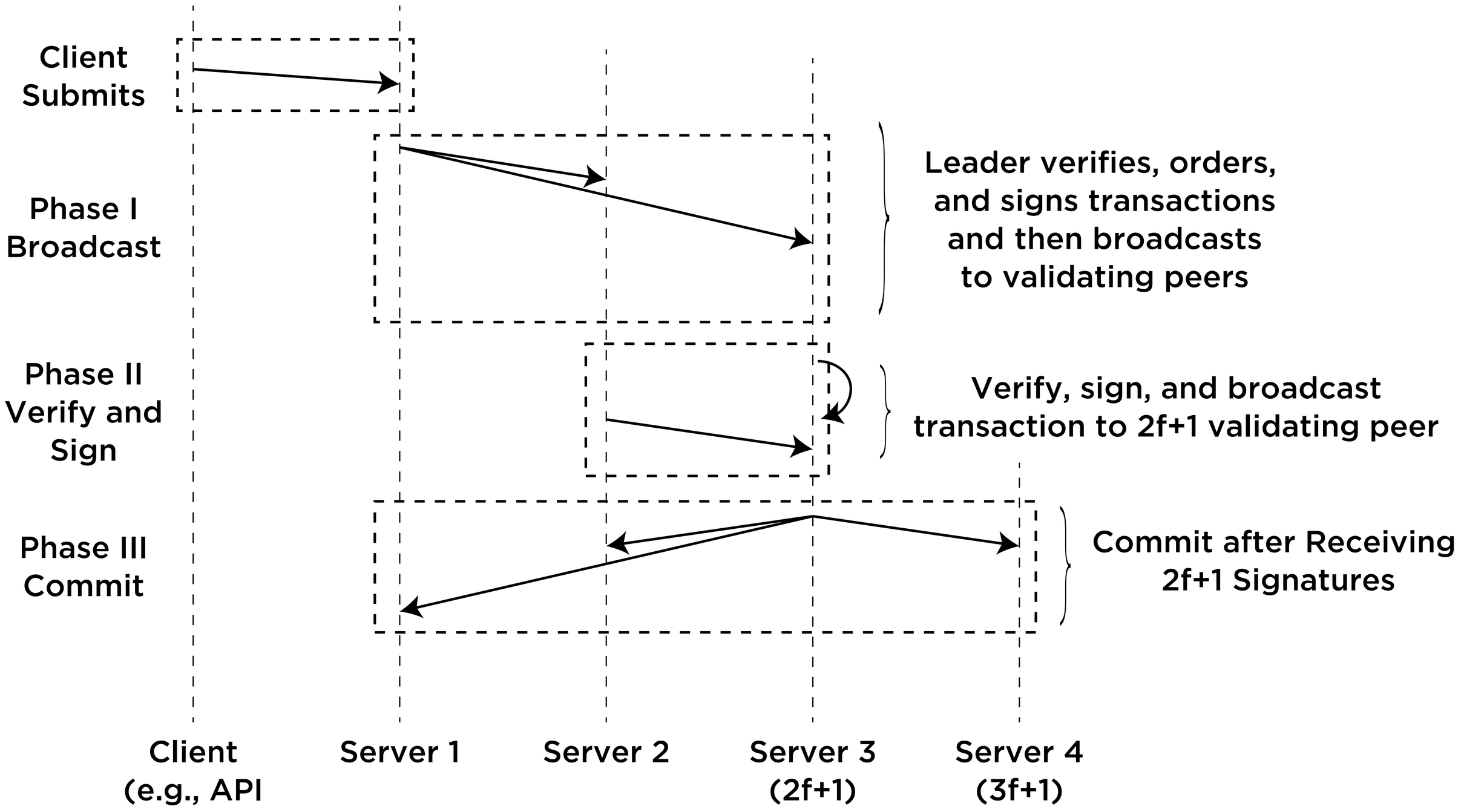
Hyperledger Iroha Architecture

ハイパーレジャーいろはのシステム構造は、特にモバイルアプリ等をサポートする為に高速度と低レテンシーが重要であり、高パーフォマンスなシステム構造が一番の特徴。



合意形成アルゴリズム（スメラギ）

Hyperledgerいろはの合意形成アルゴリズムはchain-based BFTのスメラギを採用しており、モバイルアプリに対応する為に取引を一件ごとに捌く。

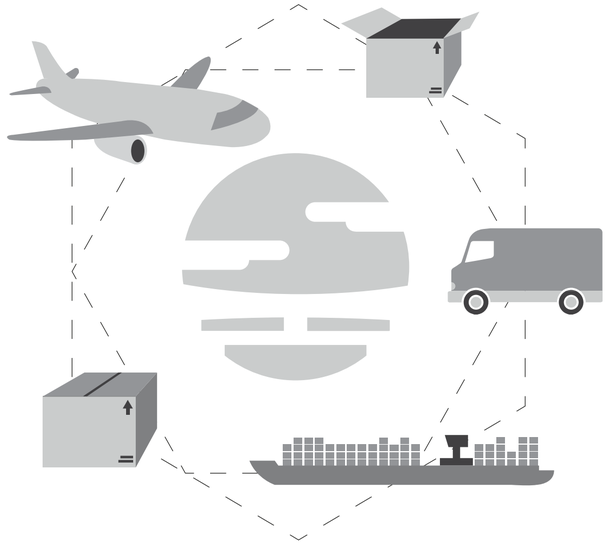


Hyperledgerいろはのユースケース

アイデンティティ

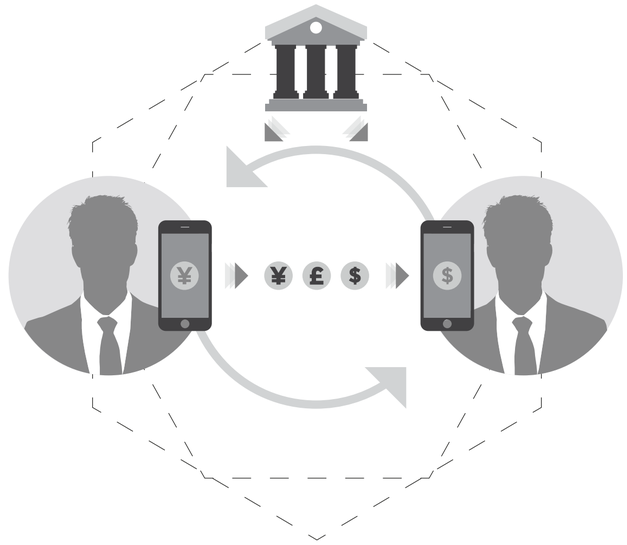
- 支払い・決済（対面型決済含む）
- 契約管理
- 証券取引
- 金融商品管理
- サプライチェーンマネージメント
- スマートグリッド

サプライチェーン



- 貿易金融
- 本人確認（KYC）
- 公証・タイムスタンプ機能
- シェアリングエコノミーサービス
- 医療
- IoT、その他

通貨管理



パーミッション・パーミッションレス分散型台帳

分散型台帳ではネットワークに参加するサーバーを制限する場合はパーミッションと呼び、制限がないシステムはパーミッションレスと呼ぶ。ユースケースに応じて、パーミッション・パーミッションレスはそれぞれ向き・不向きな点がある。

運用者への信用度

特徴	ユースケースの例	パーミッションレス DLT	パーミッション DLT	従来データベースシステム
信用性が大事	公証	◯	△	✖
低Latency	対面支払い	✖	◯	◯
多量取引	株のHFT	✖	△	◯
ビッグデータ	IoT	✖	△	◯
モバイル対応 高セキュリティ	発展途上国の CBDC等	✖	◯	△

ユースケースの例（KYC; 1/2）

弊社はHyperledgerいろは上でいくつかのサービスを開発しており、全てのサービスの基盤となるデジタルアイデンティティシステムの開発を進めている。特に犯罪収益移転防止法の特定事業者向けのアイデンティティのシェアリングプラットフォームの開発を行なっている。

ユーザーが個人情報を金融機関に共有する

金融機関は電子署名を含めた証明書を作成して、他の金融機関と共有する

ユースケースの例（KYC; 2/2）

Soramitsu Annouces Know Your Customer (KYC) Personal Identity System

Soramitsu Co. Ltd

PRESS RELEASE

JP, September 13, 2016 at 20:21 BST

Rakuten Securities, Inc. (President: Yuji Kusunoki, hereafter Rakuten Securities) and Soramitsu Co., Ltd. (CEOs: Makoto Takemiya and Ryu Okada; hereafter, Soramitsu) announce that they are working together to develop a KYC [1] system using blockchain technology [2].

Recently, complying with KYC requirements has posed many problems for financial institutions. To help comply with KYC regulations, Rakuten Securities and Soramitsu are developing a system using secure blockchain technology. The present work is exploring the possibilities of using blockchain technology for practical use in KYC and related systems.

Rakuten Securities is looking to maintain a safe environment where customers can feel secure making transactions, while using blockchain technology to create new and innovative services.

Press Contact

Name
Makoto Takemiya

Email address

Phone number
+81-03-5843-8978

http://www.coindesk.com/press-releases/first-japan-announcement-know-customer-kyc-personal-identity-system-co-development-regtech-high-technology-meets-fintech/

ユースケースの例（契約管理）

P&C Insurer Trials Blockchain for Catastrophe Coverage

Stan Higgins (@mpmcsweeney) | Published on September 26, 2016 at 19:30 GMT

NEWS

335 30 1

One of Japan's largest property insurers is co-developing a prototype blockchain system for insurance derivatives.

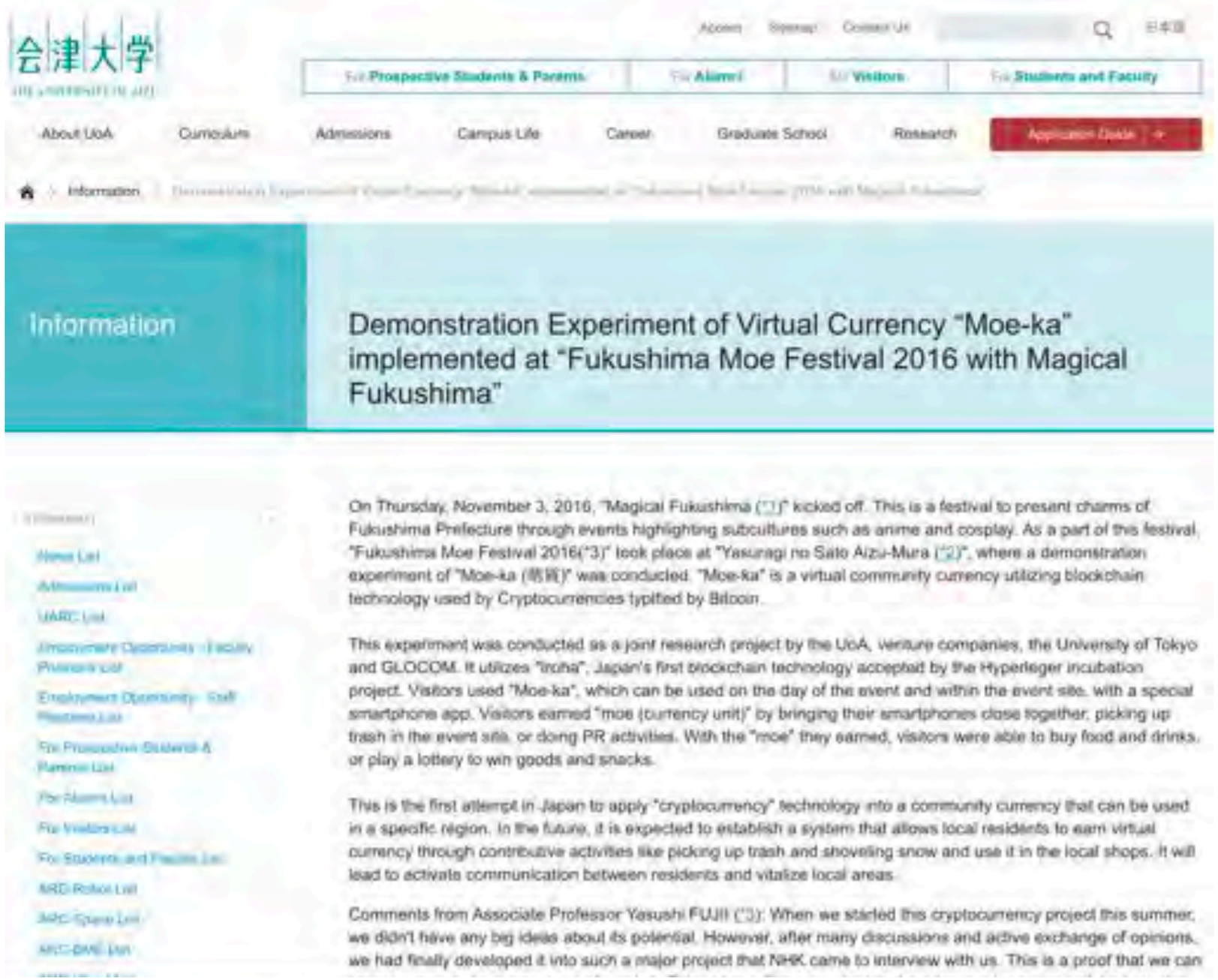
Sompo Japan Nipponkoa Holdings announced today that it is working with a firm called Soramitsu to develop a means to purchasing and exchanging insurance policies related to natural disasters and other catastrophic events.

The company said in a statement:

> *"The Derivative System Using Blockchain Technology (tentative name) that Sompo Holdings and Soramitsu have begun jointly developing aims to create a service that simultaneously shares data such as contract details on the blockchain to accurately and swiftly carry out every step in the insurance process, from managing risk aggregation for derivative products to determining whether or not to pay out on claims and implementing procedures to pay compensation."*

http://www.coindesk.com/pc-insurer-trials-blockchain-catastrophe-coverage/

ユースケースの例（デジタルアセット; 1/2）



http://www.u-aizu.ac.jp/en/information/moeka2016.html

ユースケースの例（デジタルアセット; 2/2）

その他のユースケースの例

Central Bank Digital Currency (CBDC)

中央銀行が電子通貨を発行し、台帳へのAPIアクセス手段を提供した場合、デジタル世界で生成され流通する日本円等を実現可能。

証券決済

中央銀行の電子通貨（CBDC）が実現すれば、即時証券決済の実現も可能となり、証券業界における効率が向上する。

上記のユースケースについて：

ブロックチェーンが向いている点

・透明性 （不正行為防止）

・Security（改竄困難・不正取引困難）

ブロックチェーンが向いてない点

・プライバシー（透明性によって全ての取引を見える可能性あり）

将来的に解決する可能性

・匿名取引（準同型暗号やOblivious Transfer）

・合意形成のバリデーションと合意形成を分けて行う

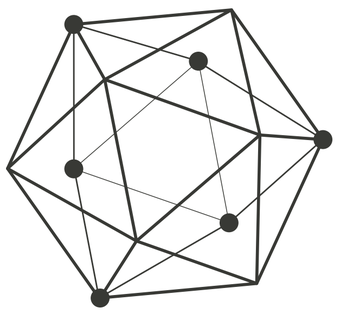
いろはのハッカソン

日時：平成29年3月11日（土）～3月12日（日）10：00～18：00

場所：東京大学　工学部２号館　92Bおよび93B教室

IROHA

http://www.gcl.i.u-tokyo.ac.jp/events/20170311-0312-global-design-hackathon/



HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

IROHA

https://github.com/hyperledger/iroha