CurrencyPort

分散型合意元帳の実用に向けた開発現場の最前線

カレンシーポート株式会社
代表取締役・CEO　杉井　靖典

2016年3月17日

日本銀行　第17回 決済システムフォーラム

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	370万円（資本準備金を含む） 〈2016年1月1日現在〉

【創業メンバー】

代表取締役	杉井　靖典
取締役	伊藤　みゆき
取締役	志茂　博
執行役員	金田　東陽

【事業目的】

1.電子財布システムの開発および応用サービスの提供
2.資金決済・送金システムの開発および応用サービスの提供
3.外国為替両替システムの開発および応用サービスの提供
4.自動売買アルゴリズムの研究開発および応用サービスの提供
5.分散合意形成アルゴリズムの研究開発および応用サービスの提供
6.越境商取引システムの開発および応用サービスの提供
7.店舗向け販促・販売システムの開発および応用サービスの提供
8.前各号に附帯関連する一切の事業

代表取締役　杉井 靖典

取締役　伊藤 みゆき

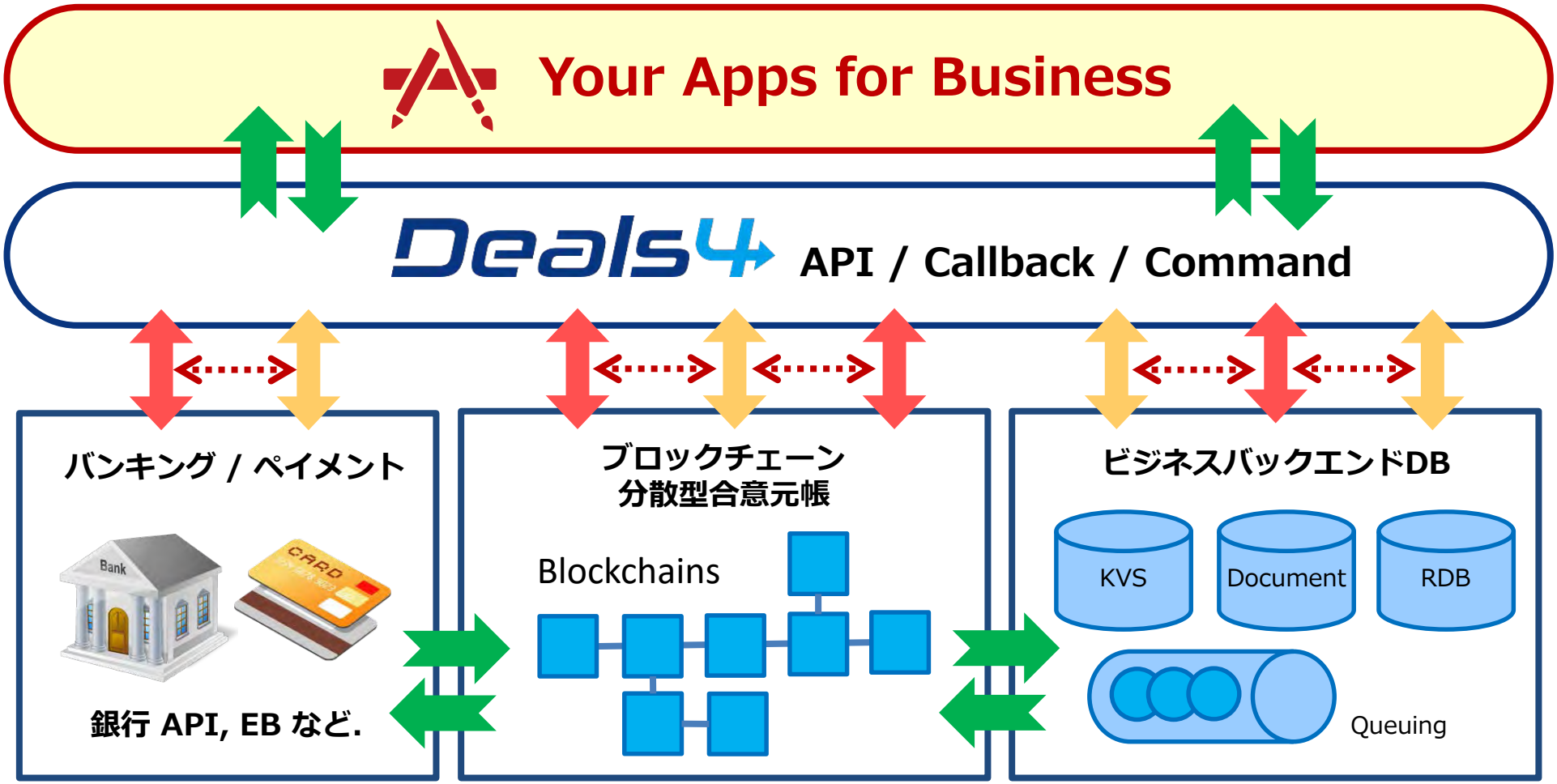
取締役　志茂 博

執行役員　金田 東陽

価値の発行・移転・交換を伴うビジネスアプリ開発用 I/F

CurrencyPort

資金決済、取引契約、監査証跡が必要な業務アプリ向け開発支援ミドルウェア



ブロックチェーンの特性

リレーショナルデータベースや分散型データベースとの根本的な違い

- ✓ 価値そのものを、デジタルデータとして発行できる。
- ✓ 発行されたある価値を、特定の利用者のみに保有させることができる。
- ✓ 保有しているある価値を、別の利用者に宛て移転させることができる。
- ✓ 同一価値の複数同時利用や、多重移転を排除する機構をもつ。
- ✓ 価値記録が正しいことは、数学的、暗号学的な手法を用いて証明できる。
- ✓ 価値記録の内容を改ざんしようとしても、それが困難なデータ構造をもつ。
- ✓ 万が一価値記録の内容が改ざんされても、自動的に無効になる機構をもつ。

貨幣（トークン）機能

✖

監査証跡機能

ブロックチェーンの利活用が期待されるビジネス分野

CurrencyPort

価値や権利の発行・保有・移転・交換・契約を伴うビジネス領域で特に有効

- ✓ 金融（銀行、資金移動、有価証券取引）
- ✓ 流通・小売（物流、デジタルコンテンツ流通）
- ✓ エスクローが有効な資金回収リスクの回避手段となる取引

  例）業務委託契約、貿易、不動産売買、中古品売買
- ✓ 予約を伴う各種産業 宿泊施設、交通機関、医療機関、学習施設、サロン等
- ✓ 時間利用、使用料等、従量課金を伴う各種産業やサービス

  例）駐車場、駐輪場、レンタカー、貸し会議室、貸金庫、貸し倉庫、貸しロッカー

  デジタルコンテンツ利用、カラオケボックス、スポーツクラブ、スーパー銭湯など多数
- ✓ センサーネットワーク、IoT等を活用した自動取引を伴う産業

  例）ガス、水道、電気、通信、交通、農業、畜産
- ✓ 内容証明、商業登記、不動産登記（事実事項証明）

ブロックチェーン上にあらゆる価値を発行して取引を記録

CurrencyPort

法定通貨、仮想通貨、地域通貨、企業通貨等の価値発行・移転・交換に対応

銀行

入金／出金

API

Deals4

- ✓ 価値発行
- ✓ 価値移転
- ✓ 価値交換

ウォレット


akPrCt...mKrdqd


akBbdP...tLbtkR

ブロックチェーン

Blockchains

デビットカード
クレジットカード

入金（支払い）

暗号通貨ウォレット

入金／出金

証券口座

入金／出金（振替え）

価値発行に適するブロックチェーン上の実装

CurrencyPort

パブリックブロックチェーンにおける価値発行プロトコルの例

	Bitcoin系	Ethereum系	nem系
価値発行プロトコル	✓ OpenAssets ✓ Colu ✓ CounterParty など	✓ Coin contract	✓ Mosaic tile
ビルドインコイン	BTC	ETH	XEM
合意形成アルゴリズム	Proof of Work	Proof of Work (将来:Proof of Stake)	Proof of Importance

パブリックチェーンとプライベートチェーンの相互連携

CurrencyPort

どちらか一方だけよりハイブリッドで使う方が互いに有する特性を補完できる

パブリックチェーン		プライベートチェーン
Bitcoin	派生	MultiChain
Ethereum	派生	eris　HydraChain
nem	派生	mijin
低速処理、無信頼の分散合意形成 原則情報全公開、高度な外部監査性		高速処理、信頼基準による合意形成 権限管理が充実、情報制御が可能

パブリックとプライベートを相互連携する際のポイント①

CurrencyPort

主に、プライベートチェーン側の外部監査性を担保するため

- ✓ **プライベートチェーン側の「取引存在証明」**
  プライベートチェーン側のブロックのハッシュ（一方向関数）値を、
  一定毎にパブリックチェーン側のトランザクションにアンカリングする

- ✓ **プライベートチェーン側の「事実否認防止」**
  パブリックチェーン側のブロックのハッシュ（一方向関数）値を、
  一定毎にプライベートチェーン側のトランザクションにアンカリングする

双方向アンカリング

プライベートチェーンの弱点補完

パブリックとプライベートを相互連携する際のポイント②

CurrencyPort

発行された価値の技術的保証手段

- ✓ **価値（トークン）発行はパブリックチェーン側のみに限定**
- ✓ **パブリックからプライベートチェーン側に移転した価値はパブリック側で自由に利用できないようロックする**

  例）プロトコルまたはコントラクトレベルでのロック制御
- ✓ **プライベートからパブリックチェーン側への価値の移転時プライベート側の価値を無効化する**

  例）１．プライベートチェーンから外部へ出金または送金を行う際は、
  価値転出専用のウォレットに転送する
  ２．上記を条件にパブリック側のロック解除するトランザクションを発行する

2 Way ペッグ

発行価値の信託保全と監査機能

発行された価値の公正明大な把握、自律監査・外部監査を両立

- ✓ **発行済みの価値（トークン）の数量**
  = パブリックチェーン上に**発行された価値の総数**
  = **保全すべき価値（金額）**

数学的に証明可能

- ✓ **信託保全残高ステートメントの謄写**にタイムスタンプと電子署名を施し**ブロックチェーン上に参照情報を公開**

改ざんが実質不可能

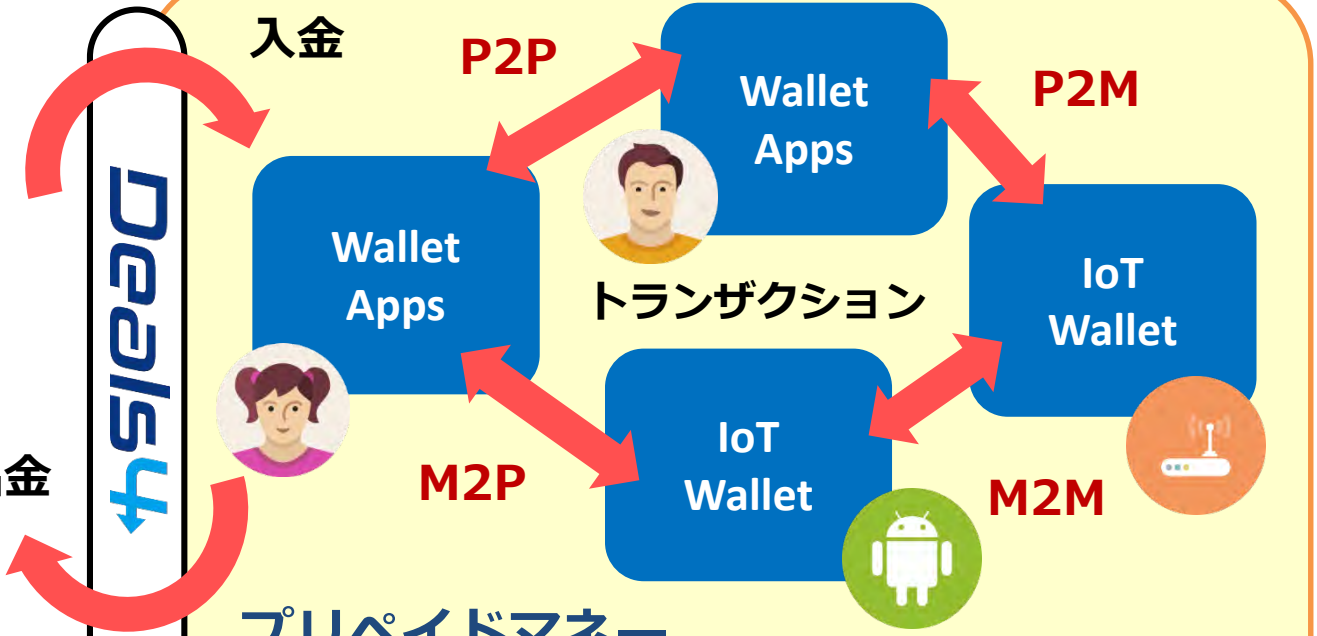
利用者はより安心してプリペイドマネーを利用可能に

プリペイドマネー／トークンエコシステムを展開

CurrencyPort

人と人との取引はもちろん、人と機械、機械と機械の取引決済にも対応

銀行APIより
柔軟でビジネスにより
踏み込んだAPIを提供



参照系中心

実行系を開放

すごいアプリケーション!
まだ見ぬサービス!!

入金, 出金, 通貨両替, 送金,
オーソリゼーション, 支払い, エスクロー, 契約 etc.

ビジネスロジックのプログラミングインターフェイス

CurrencyPort

口座管理、資金移転、支払い、両替、エスクローなど取引に必要な機能を提供

Deals4 ※開発予定の機能を含みます

- ✓ アカウント管理
- ✓ ウォレット管理
- ✓ 商品管理（価格、ロケーション）
- ✓ 権限管理（トークナイゼーション）
- ✓ 残高確認（アセット毎）
- ✓ 金銭の入金、出金（銀行・カード等連携）
- ✓ オーソリゼーション（残高、受入れ、口座状態）
- ✓ 資金移動（送金）
- ✓ 資金決済（支払い）<ワンショット、タイマー、バスケット>
- ✓ マルチカレンシー対応の通貨両替（手元、支払い時）
- ✓ エスクロー、コントラクトの実行
- ✓ 見積書、請求書
- ✓ 権利移転、名義管理
- ✓ 取引履歴、監査証跡
- ✓ 秘密分散ストレージ
- ✓ 秘匿検索、秘匿計算

BBaaS

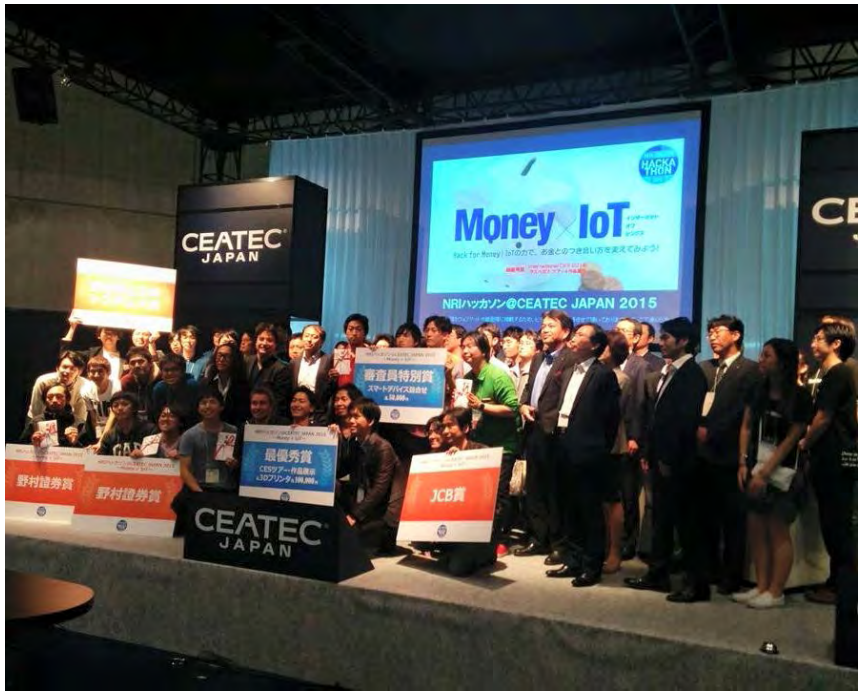
（ビジネスバックエンド・アズ・ア・サービス）

APIは随時追加

API技術提供「Money×IoT」 NRIハッカソン@CEATEC JAPAN2015

CurrencyPort

決勝進出9チーム中、4チームが採用（素材最多採用）うち3チーム受賞!!



「IoT × Money」というテーマのハッカソンなのに、
直接Moneyをいじれる APIは、
当社しか提供していなかった…

採用作品例）

- ✓ ある商品を購入すると、当該商品メーカーの端株（ファンド）が購入できるサービス
- ✓ エスクローを活用した募金の使途の明瞭化
  エスクローを担保にした銀行融資の可能性も
- ✓ ストリートパフォーマーの投げ銭ハット
  遠隔地（TV等）を通じての投げ銭もできる

超高速開発が可能

カードプロセッシング・イシュアのバックヤード

従来の決済プロセシングの手順を変えずに仮想通貨を含むカード決済を実現

生活者

通常のカード決済プロセシングの手順

例) お勘定 ¥

Mercahant（加盟店） ¥ → Acquirer（加盟店開拓） ¥ → Payment Network ¥ → Issuer（カード発行）

¥ ← Acquirer ← Payment Network ← Issuer

カード

又は

モバイルウォレット

VISA JCB MasterCard AMERICAN EXPRESS

（支払い通貨を選択）

$ € ฿

Deals4

- ✓ ウォレット機能
- ✓ アカウント機能
- ✓ オーソリ機能
- ✓ 通貨両替機能

$ € ฿ ¥

Exchange Market

両替市場

ブロックチェーンだけでは解決しない技術課題

CurrencyPort

自社開発または、研究所組織をもつ大手企業との共同開発

✓ **秘密分散共有制御技術**

海外先行プロジェクト：Storj

- ブロックチェーンと連携可能な秘密分散ストレージサービスの開発

✓ **秘匿計算技術**

海外先行プロジェクト：ɛnigma

- 準同型暗号等を用いた秘匿検索・秘匿計算をブロックチェーン上で利用可能にする技術の開発

実は国内の基礎研究が先行している分野

✓ 複数署名の自動収集技術

✓ 時限駆動式契約自動執行技術

- スマートコントラクトの応用
- ブロックチェーン技術の拡張
- 外部サービスとの連携

ブロックチェーン分野において日本が示せる技術力

CurrencyPort

ブロックチェーン技術との親和性の高い世界に対する日本優位の先進例

- ✓ 秘密分散ストレージ
  NTT、東京大学、インテック、NRIセキュア、パナソニック　等
- ✓ 秘匿検索
  NTTソフトウェア、日立、三菱電機、富士通研究所
- ✓ 秘密計算
  富士通研究所、NEC、日立、NICT

ブロックチェーンとの連携・応用をオファーして行く

エンタープライズ用途には必須の機能

ブロックチェーンの課題

CurrencyPort

ブロックチェーンの原理や構造的理由または、外部要因により生じる課題

- ✓ 署名鍵の保管および署名方法に関する課題
- ✓ 時刻の取扱いに関する課題

  各ノード・各トランザクションの申告ベースによる紳士協定

  - 原子時計を運用する時刻配信業務認定事業者等が署名した時刻を使う？
  - 時刻取扱いに特化したブロックチェーンチェーンの開発と相互運用

- ✓ 取引のファイナリティに関する課題

  取引確定のタイミングが明確に定義できない（数学的確率に依存・紳士協定）

- ✓ 法的証拠能力に関する課題

  電子署名及び認証業務に関する法律に定める運用基準に適合可能か？

ブロックチェーン開発に従事できるエンジニアはどこに？

CurrencyPort

囲い込みとは正反対の世界。競合とは敵対するより協調合意する方が合理的

- ✓ 世界規模の開発コミュニティで技術は日進月歩
- ✓ 数学、暗号学、コンピュータサイエンスの素養が必要
- ✓ 原理的な理解ができていないと、応用も難しい
- ✓ 大手研究所組織に眠っている技術とのマッチング機会が重要
- ✓ どのブロックチェーンも開発途上で仕様通りに動かないことも日常茶飯事。ドキュメントも未整備で未実装な機能も多いので手を動かしながら技術を身に着ける根気が必要
- ✓ 基礎研究開発者への支援が必要

ご清聴、ありがとうございました。