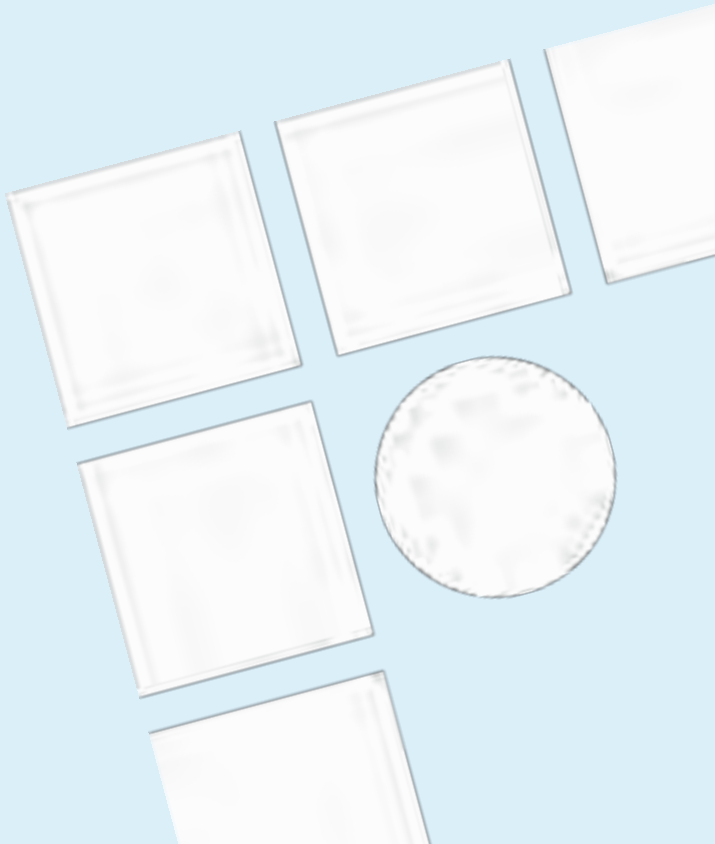
bitFlyer

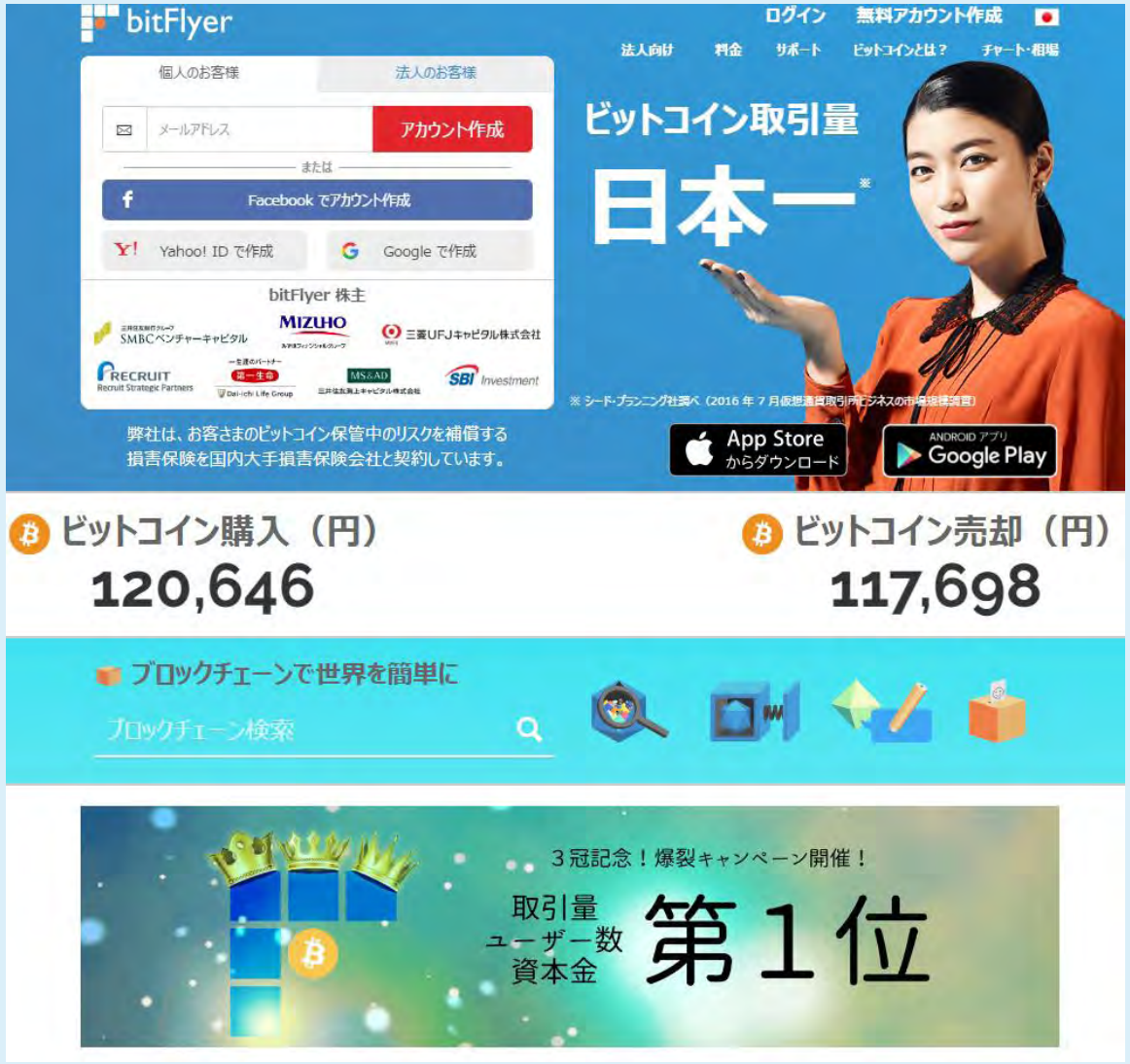
bitFlyerオリジナルブロックチェーン「miyabi」について



株式会社bitFlyer
ビットコイン・ブロックチェーン　ベンチャー企業

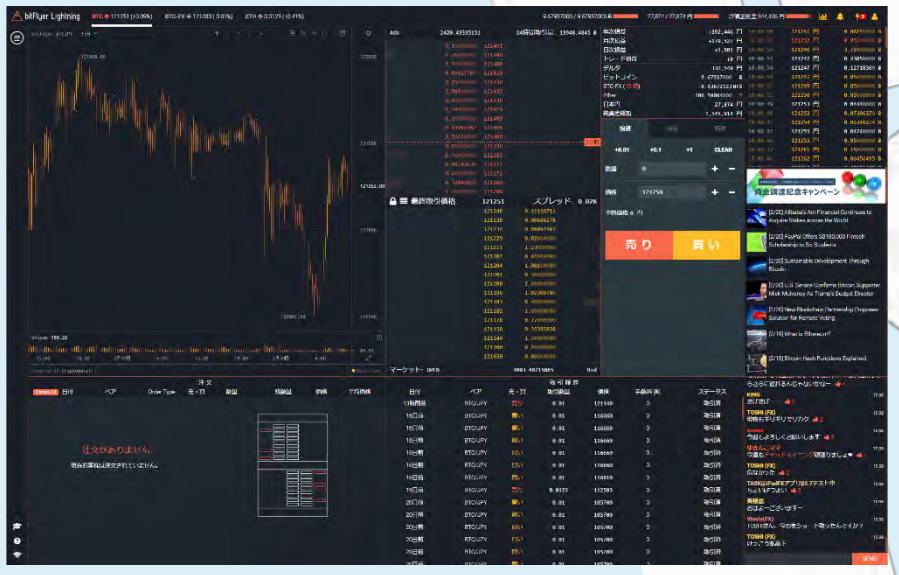
bitFlyer

bitFlyer – 透明な価格でビットコインを簡単売買



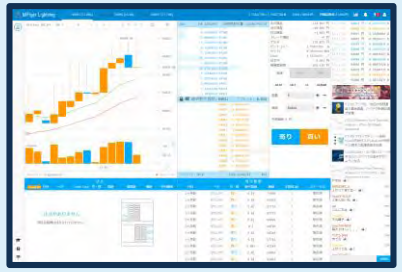
ユーザー数 50 万人超
月間取引量 3,000 億円超
資本金40 億円超

日本最大の
ビットコイン・ブロックチェーン企業



bitFlyer

会社情報



株式会社bitFlyer

設立	2014 年 1 月
資本金	41 億 238万円（資本準備金含）
本社所在地	東京都港区赤坂
海外拠点	米国、シンガポール、ルクセンブルク
取引銀行	三井住友銀行
会計監査人	新日本有限責任監査法人
弁護士事務所	森・濱田松本法律事務所、西村あさひ法律事務所、AZX 総合法律事務所、創法律事務所
税理士法人	EY 税理士法人
従業員	40 人
投資家（一部掲載）	SMBCベンチャーキャピタル、MIZUHO、三菱UFJキャピタル株式会社、第一生命 Dai-ichi Life Group、MS&AD 三井住友海上キャピタル、RECRUIT Recruit Strategic Partners、VENTURE LABO Investment、SBI Investment、Dentsu Digital Holdings、Quick、GMO PAYMENT GATEWAY、GMO VENTURE PARTNERS、B DASH VENTURES、DIGITAL CURRENCY GROUP、East Ventures、IncubateFund

国内事業者で唯一サイバー保険に加入

仮想通貨の盗難補償
三井住友海上が保険

インターネット上でやりとりする仮想通貨を安心して利用できる環境が整い始めた。三井住友海上火災保険は11月中に国内で初めて仮想通貨を巡るトラブルに対応する保険を売り出す。仮想通貨がサイバー攻撃などで盗まれたり、なくなったりした時に被害を補償する。仮想通貨の取引量は増えているが被害も広がっている。保険で安心感が高まれば、普及に弾みがつく。

仮想通貨ビットコインの取引所の国内最大手ビットフライヤー（東京・港）の協力を得て開発した。同社の月間取引高は1千億円を超えている。

仮想通貨の利用者はビットフライヤーのような専門の取引所に口座を設け手数料を支払って仮想通貨を売買している。今回の保険は取引所が加入対象で、サイバー攻撃などで仮想通貨が盗難・消失した際の損害額を補償する。取引所自身の被害だけでなく、口座に預けてあった利用者の仮想通貨も補償の対象となる。

補償額は1000万～10億円で、保険料は取引所の手数料収入の額に応じ数十万～数百万円。サイバー攻撃のような不正アクセスだけでなく、取引所の従業員のミスや不正なども補償範囲に含まれる。被害者への通知や海外からの賠償請求にも対応する。海外では一部で仮想通貨が盗難・消失した際の損害額を補償する保険があるが、国内では初めてだ。

ビットコインの販売や取引を手掛ける事業者は国内では小規模な企業が多い。一方、サイバー攻撃による被害額は一件あたり数十億円にのぼる場合もある。資本力の小さい企業では被害をまかないきれず、口座を持つ利用者の財産が補償されないリスクがあった。

bitFlyer　MS&AD 三井住友海上

2016年11月24日

各 位

株式会社 bitFlyer
三井住友海上火災保険株式会社

【国内初】ビットコイン事業者向けサイバー保険を共同開発

株式会社 bitFlyer（代表取締役：加納 裕三、以下「bitFlyer」）ならびにMS＆ADインシュアランスグループの三井住友海上火災保険株式会社（社長：原 典之、以下「三井住友海上」）は、今般、ビットコイン事業者向けに、サイバー攻撃等によるリスクを包括的に補償する専用保険を共同開発しました。

ビットコイン市場は今後大きな成長が見込まれており、ビットコイン関連のサービス運営事業者の数も増加を続けています。同時に、インターネットをビジネスの基盤とする運営事業者は、利用者が安心して取り引きできるようさまざまな対策を講じる必要がありますが、昨今の企業・団体に対するサイバー攻撃の増加と被害の深刻化を受けて、サイバーリスク対策は重大な経営課題となっています。

日本最大のビットコイン取引所を運営する bitFlyer は、従来から一般社団法人日本ブロックチェーン協会（ＪＢＡ）を通じてビットコインの利用者保護の取り組みを推進してきましたが、安心・安全なビットコインのサービスの普及と発展を図るため、三井住友海上と連携し、国内初となるビットコイン事業者向けサイバー保険を共同開発しました。

1．ビットコイン事業者向けサイバー保険の特長

（1）幅広い損害をカバー
サイバー攻撃等によって発生したビットコインの盗難、消失等に対する損害賠償のほか、事故対応に必要となる各種対策費用（見舞金費用・コンサルティング費用・原因調査費用・被害拡大防止費用など）まで補償します。

（2）充実したサポート
サイバー攻撃等により被害が発生した際は、専門知識・技術を要する原因調査や証拠保全等の事故対応について、運営事業者からのご要請に基づき、経験豊富な専門事業者を紹介します。

（3）サイバーリスク対策サービスの提供
サイバー攻撃による被害を未然に防止するために、標的型メール訓練や情報漏えいリスクに関するセキュリティ診断、従業員向けのチェックリスト等のサイバーリスク対策サービスを提供します。
また、ご要望に応じて、セキュリティ管理体制の整備等の個別コンサルティングも実施します。

三井住友海上火災保険とビットコイン事業者向けサイバー保険を共同開発

サイバー攻撃等によって発生した仮想通貨・円の盗難、消失等に対する損害が補償対象

bitFlyer

ビザンチン耐性（BFT）

ブロックチェーンが実現したもの

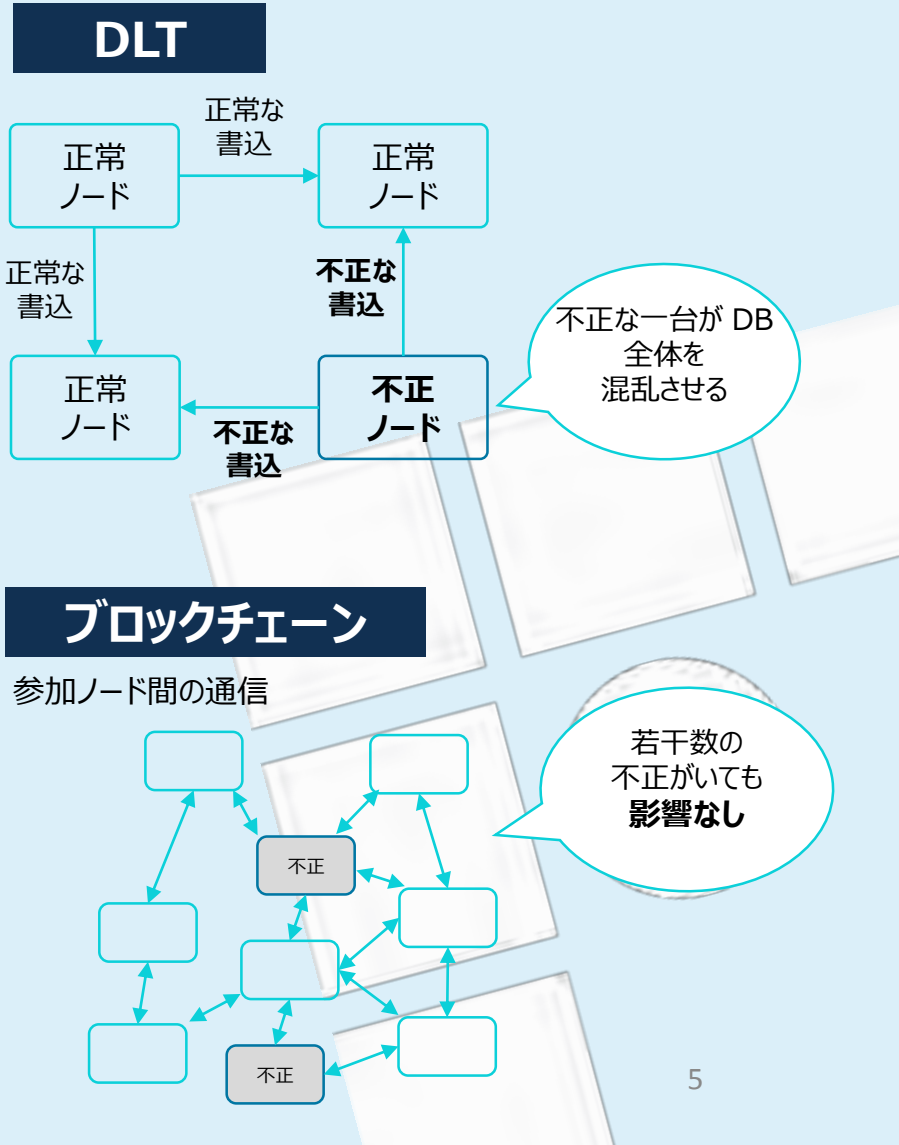
ビザンチン障害の実用的な解決

ビザンチン将軍問題とは …

コンピュータ ネットワークで、その参加ノードが意図的に / ソフトウェア バグによりエラーや不正が起きるような通信をする状況においても、ノード全体でデータの同期を正しく取れるかという問題のこと。長らくその解決方法が研究されてきました。

ブロックチェーンの特長: 正当な取引だけを受理する堅牢性

正しい取引を受理しない、または不正な取引を受理しようとするノードがあっても、全体には影響なく、正常に動作します。



bitFlyer

当社オリジナルブロックチェーン「miyabi」の位置づけ

スマートコントラクト搭載、ファイナリティーを確保し秒間1,500トランザクションを達成

中央集権型データベース

RDBMS

NoSQL

VS

分散型データベース
Availability

複数のノードで管理することで
・可用性向上（「落ちない」）
・単一障害点の存在

分散型台帳 (DLT)
Immutability

構造上データの書き換えができない（改竄不可能）

ブロックチェーン
BFT (ビザンチン耐性)

ブロックチェーンでは
「嘘つき」のノードがいても
システムが動き続ける

従来型ブロックチェーン
（含むビットコイン）
秒間～100tx

VS

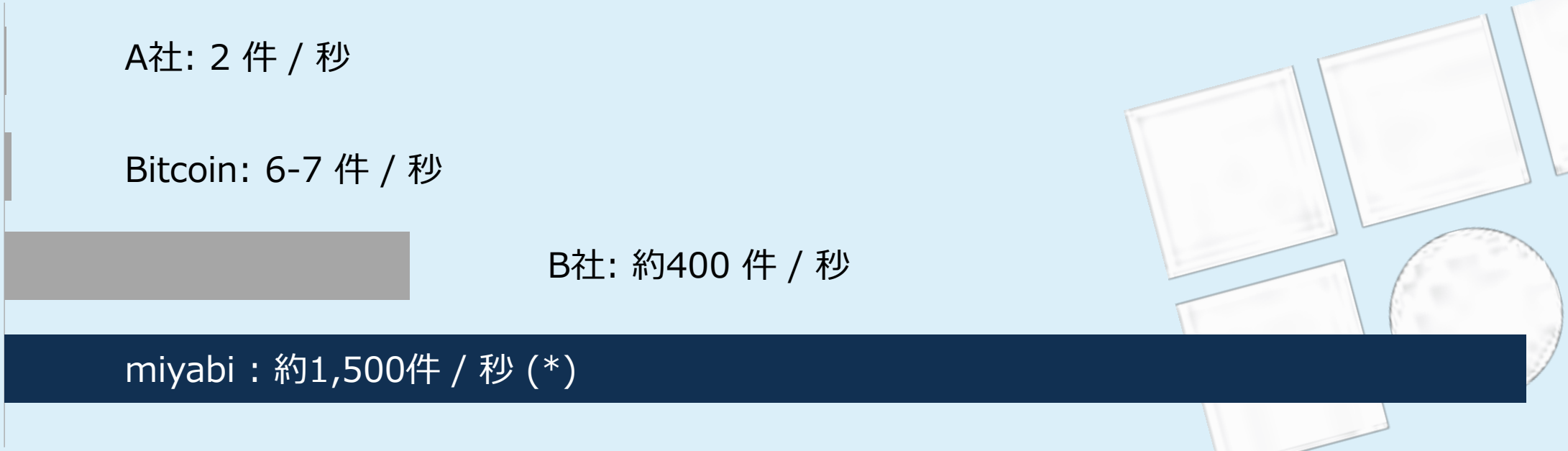
miyabi
秒間1,500tx
+スマートコントラクト

miyabi
miyabi では処理速度が速くなり
実用にも耐えうる性能に
さらにスマートコントラクトも
実行可能

bitFlyer

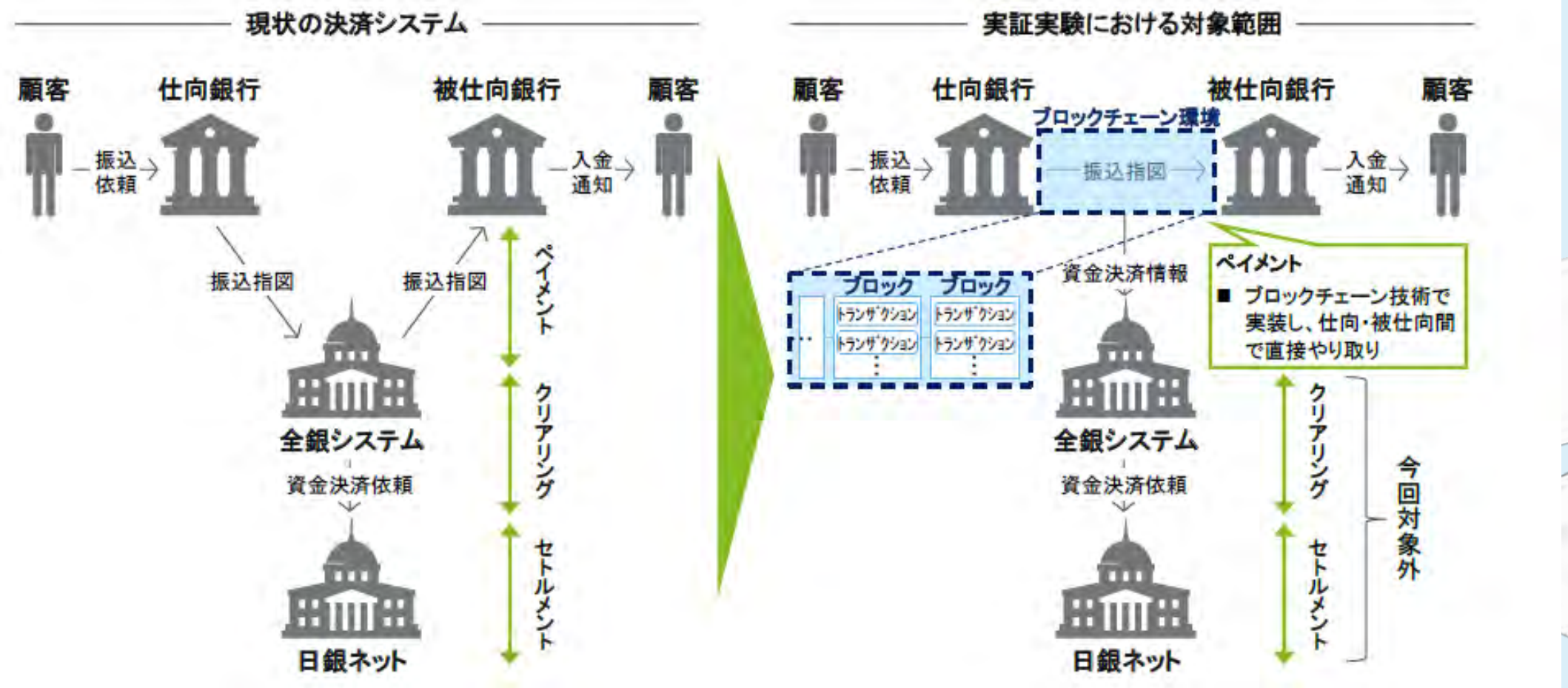
世界最速のパフォーマンス

既存ブロックチェーン製品（ビザンチン耐性を持つもの）と比較して圧倒的な処理能力を達成



＊ 2016年11月30日付けブロックチェーン研究会「国内の銀行間振込業務におけるブロックチェーン技術の実証実験に係る報告書」より
(デロイト トーマツ グループならびに株式会社みずほフィナンシャルグループ、株式会社三井住友銀行、株式会社三菱UFJフィナンシャル・グループ)

金融機関による実証実験の概要

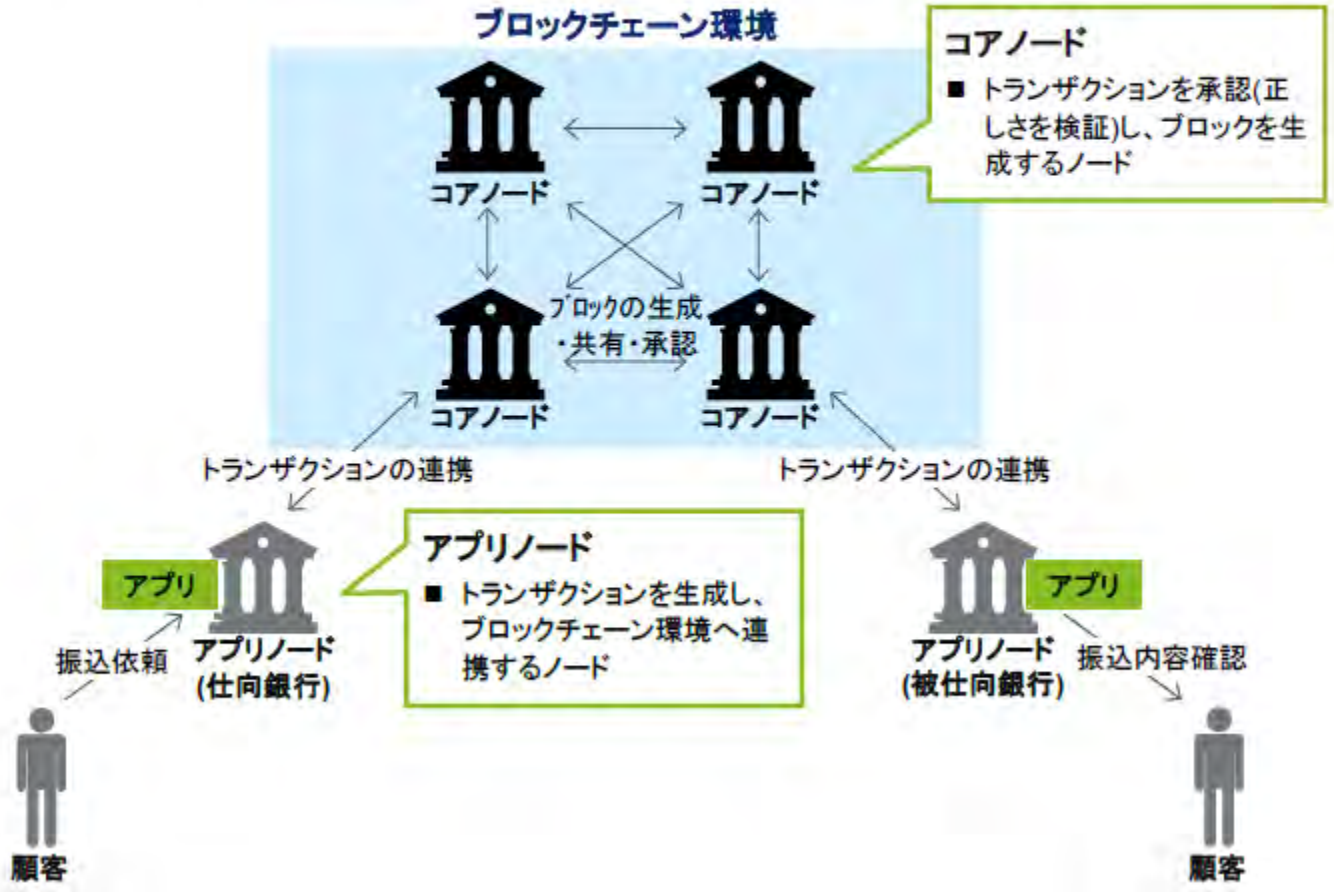


2016年11月30日　ブロックチェーン研究会
「国内の銀行間振込業務におけるブロックチェーン技術の実証実験に係る報告書」より一部抜粋

bitFlyer

構築した実験環境

アプリノード：　振込の実施者である銀行が担う想定
コアノード：　　信頼できる中立的な機関が担う想定



2016年11月30日　ブロックチェーン研究会
「国内の銀行間振込業務におけるブロックチェーン技術の実証実験に係る報告書」より一部抜粋

bitFlyer

技術的観点での検証結果

凡例) ○:検証の結果、必要な水準を満たしている △:検証の結果、必要な水準を満たすために課題あり
－:未検証であり、必要な水準を満たすために課題あり N/A:検証の対象外

検証の軸		銀行間振込業務で必要な水準 (想定)	実験環境における検証結果
可用性	サービス稼働率[10]	■ 社会的影響が極めて大きい重要インフラであり、高いサービス稼働率が必要	－ ■ コアノード増設により高稼働率が期待できるが、**具体的な数値は未算定**
	ディザスタリカバリー[11]	■ 災害等に備え、正センターの遠隔地にバックアップセンターの整備が必要	△ ■ コアノード設置の拠点分散化により対応可能だが、**分散拠点数・分散方式は未検討**
性能	レスポンスタイム	■ 業務の性質によるが、クライアント・サーバ型では画面レスポンス3秒が一般的	△ ■ 取引の承認時間に数秒程度必要であり、**実業務に適応可能かの検証要**
	スループット	■ 全銀システムにおけるピーク時の処理能力は1,388件／秒	○ ■ 実験環境では1,500件／秒以上 (国内1拠点での計測値)
拡張性	性能拡張性	■ 業務量は急激な増加は予想されないが経年で微増しており、一定程度の拡張性が必要	－ ■ 業務量の増加に備えた**スケールアップ・スケールアウトの方式について、今回は未検証**
	機能拡張性[12]	■ 参加銀行からの機能追加要望に備え、拡張性の高い機能構成としておくことが必要	－ ■ スマートコントラクトによる**機能拡張性を保持しているが、今回は未検証**
保守性	機器保守性	■ 機器故障に対して迅速な交換・復旧が可能な態勢整備が必要	N/A ■ 基盤管理等により同等レベルを確保可と想定 (ブロックチェーン技術に係らない範囲)
	アプリ保守性[13]	■ アプリの不具合、想定外の機能追加要望に対して柔軟・迅速に対応できることが必要	N/A ■ プログラム管理等により同等レベルを確保可と想定(ブロックチェーン技術に係らない範囲)
セキュリティ	攻撃・侵入耐性	■ 完全に排除可能であることが必要	N/A ■ FW[14]、閉域網等により同等レベルを確保可と想定 (ブロックチェーン技術に係らない範囲)
	データ秘匿性	■ 完全に排除可能であることが必要	△ ■ 暗号化により対応可能だが、実装簡易化のため**一部情報に対しては暗号化していない**
データ完全性	改ざん耐性	■ 完全に排除可能であることが必要	○ ■ ブロックチェーンの分岐が発生しないため、51%攻撃による改ざん攻撃を排除可能[15]
	データ完全性	■ 処理の過程において、データは不備・欠損・不整合がなく、一貫していることが必要	○ ■ ブロックチェーンの分岐が発生せず、全体で一貫した原簿の共有が可能

2016年11月30日　ブロックチェーン研究会
「国内の銀行間振込業務におけるブロックチェーン技術の実証実験に係る報告書」より一部抜粋

bitFlyer

想定される「 miyabi」の活用事例

既存のシステムの置き換え （低い送金手数料でいつでも使える）	銀行	証券会社
シェアリングエコノミーの 基幹システム	空き家の活用	カーシェアリング
IoT時代のデータ管理	食品 トレーサビリティ	不動産登記
政府システム	マイナンバー	電子政府