



SUMMIT
ONLINE
JAPAN

KPMG Digital Audit X Blockchain Analytics

Junya Kondo
Senior Manager
KPMG AZSA LLC

Yoshinori Seki
Manager
KPMG AZSA LLC

Masatake Toyota
Director
KPMG Ignition Tokyo

Agenda

KPMG Japan Digital Audit

Case / Solution

Next Steps

KPMG Japan Digital Audit

KPMG Japan

KPMG AZSA LLC: あずさ監査法人は**KPMG**のメンバーファームとして、複雑な課題を有するクライアントや社会に対して価値ある監査・アドバイザーサービスを提供します。



注力すべき **3つの領域**



Data



Technology



Capability

Future of Audit

2025年、監査現場でのある2日間の出来事です。**Continuous Audit**が実現している未来の監査現場を描いています。(制作：KPMG UK)

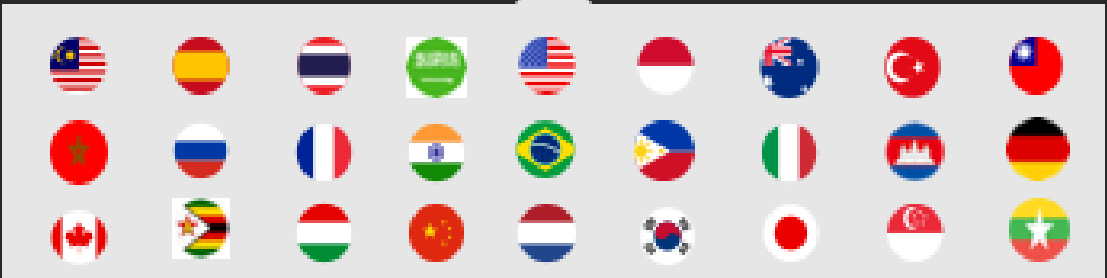




KPMG Japan

KPMG Ignition Tokyo

KPMG Ignition Tokyo : 約120名のデジタル人材集団



平均年齢



35歳

国籍



27カ国

ジェン
ダー
バランス



女性

30

:

男性

70



KPMG Ignition Tokyo (KIT) が注力する6つの技術領域



Secure Computing

監査情報・税務情報・アドバイザー情報などKPMGが取り扱う情報群を一元化し、より安全な状態で処理することを可能にする技術総称



Knowledge Processing

画像・文字・音声などの非構造データから情報を抽出・認識・データベース化
集約された構造データ間を結合し人間の知識・感覚に沿った意味的価値を獲得



Intelligent Agent

ある特定の分野において、集約された情報知識をもとに、人間との自然な対話を可能とする知的感覚を有するエージェント



Scientific Visualization

効果的な視覚・聴覚・触覚的フィードバック技術。

Business Intelligence toolsを始めとしたデータ分析・グラフ化技術



Smart Transaction

人間が検知不可能な異常の発見、意図的かつ悪意の処理の検出

KPMGの業務の根幹といえる部分への貢献を想定



Edge Computing & IoT

IoTを中心としたリアルタイムデータキャプチャー技術と高速処理のための次世代コンピューティング技術

技術ドメインを支える基盤

 Cloud

 DevOps

 Security

Case / Solution

仮想通貨分析ツール(特許出願中)開発の背景と要件

監査において、仮想通貨を対象に年間を通じた取引分析及び期末時点の残高を検証する必要性が出てきた。

要件

- 監査対象の通貨は複数ある。
- 監査対象アドレスは数百万件に達する通貨もある。
- 取引分析は1会計期間分（1年）のデータで十分だが、残高検証については、前期末残高という概念が仮想通貨に存在しないため、ジェネシスから期末時点までのデータを積み上げて計算する必要がある。
- 監査において扱う情報の信頼性、正確性と網羅性は担保する必要がある。

外部Explorerサイトの利用がダメな理由

- 監査対象アドレスは機密情報扱いのため、外部Explorerにアドレスを渡すことができない。
- 監査において、情報源の信頼性を評価する必要があるが、外部Explorerのソースコードは公開されているものの、バックエンドの運用管理状況は公開されておらず、信頼性を評価できない。

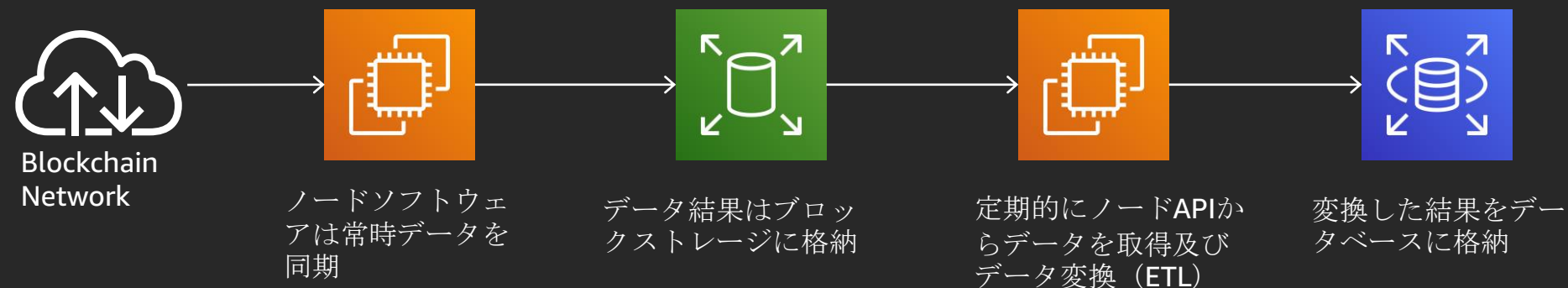
Explorerサイトの自社運用でもダメな理由

- 監査対象アドレスが数百万件存在するケースもあるため、**Web**インターフェースしかない**Explorer**では取扱が事実上困難。
- 過去の特定时点の残高を表示できる機能を持つ**Explorer**は極わずか。
- 結果の表示方法（**HTML, JSON**等）が千差万別であり、**Explorer**毎に検証方法を変えるのは監査人の負担が大きい。

当初の案

各通貨のノードはAPIを備えており、それを介して監査に必要な情報（主にブロックとトランザクション）をJSON形式で取得、分析しやすい形に加工するシステムを当初想定した。

当初のシステム構成：よくあるモノリシックなシステム構成



開発時における課題

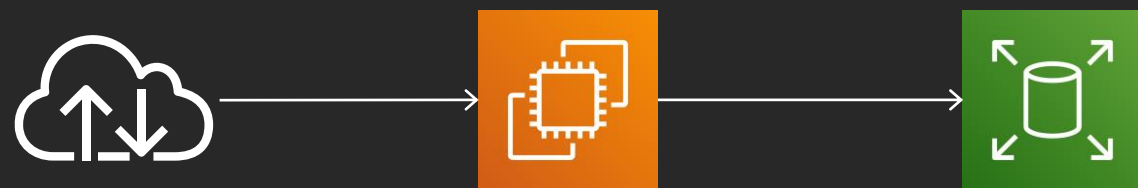
当初は2~3カ月で終わると思ったプロジェクトだが、開始したら課題が噴出した。

- 通貨ノードの運用コスト課題
- システム運用の課題
- 通貨仕様の理解不足
- データ加工の課題

通貨ノードの運用コスト課題

- ノードのストレージとしてSSDが要求されており、また容量がTB級になる通貨もあり、ストレージの運用コストが高額となる。
- ノードインスタンスも最低Large級のマシンパワーが必要で、インスタンスの運用コストも高額となる。

当初の構成



0.124USD/H
X 24H x 30D
≒ 90 USD

0.12USD/GB
x 1000 GB
= 120 USD

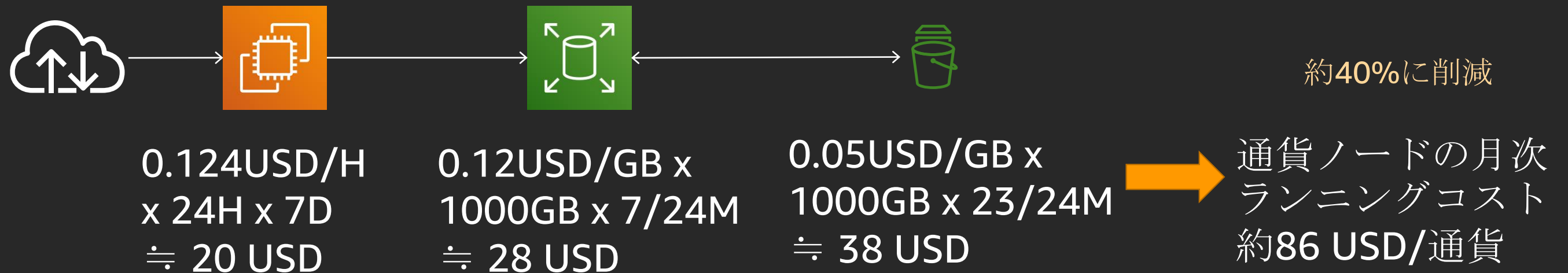


通貨ノードの月次
ランニングコスト
約210 USD/通貨

ノードの運用コストの解決策

- 毎日使うものではないため、ノードの同期及びデータ抽出は定期実行とし、通常時はインスタンスを停止し、ストレージもスナップショットに退避し、運用コスト削減。
- 不要なインスタンス、スペックは削除（タグ付けを活用）
- スポットを活用し、インスタンスの運用コストをさらに削減。

解決後の構成



システム運用の課題

- 現時点では、一部のチームが特定の時期に使用するのみのシステムであり、運用の手間はかけたくない。

システム運用の解決策

- 積極的にマネージドサービスを活用することにより、運用の手間を省力化。（細かいチューニングよりも運用の省力化を優先）
- 月次で動かすバッチシステムなので、ストレージ容量以外の監視系は無視。

通貨仕様の理解不足

ブロックに入っているトランザクションを取り出して、アドレス毎に金額フィールドを合算すれば残高が求められると思っていたが、そこまで単純な通貨は一つもなく、例えば

ビットコイン：ノードバージョンによってアドレス解釈が異なる。

イーサリアム：あるハードフォーク以前は、トランザクションデータの成功・失敗のフィールドが存在しない。

等々が開発途中で発覚。

通貨仕様の理解不足の解決策

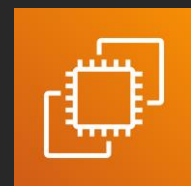
- ホワイトペーパーを隅から隅まで目を通す。
- ソースコードを直接読む。

この辺は力業。

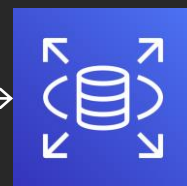
データ加工の課題

- ノードAPIから取得したデータのどの項目が検証に必要なのか良く分かっておらず、当初不要と思っていた項目が後から必要になるケースが出てきた。
- ノードAPIからのデータ取得は速度が上げにくく、データ変換の仕様変更対応に時間がかかる。

当初の構成



定期的にノードAPIからデータを取得及びデータ変換 (ETL)

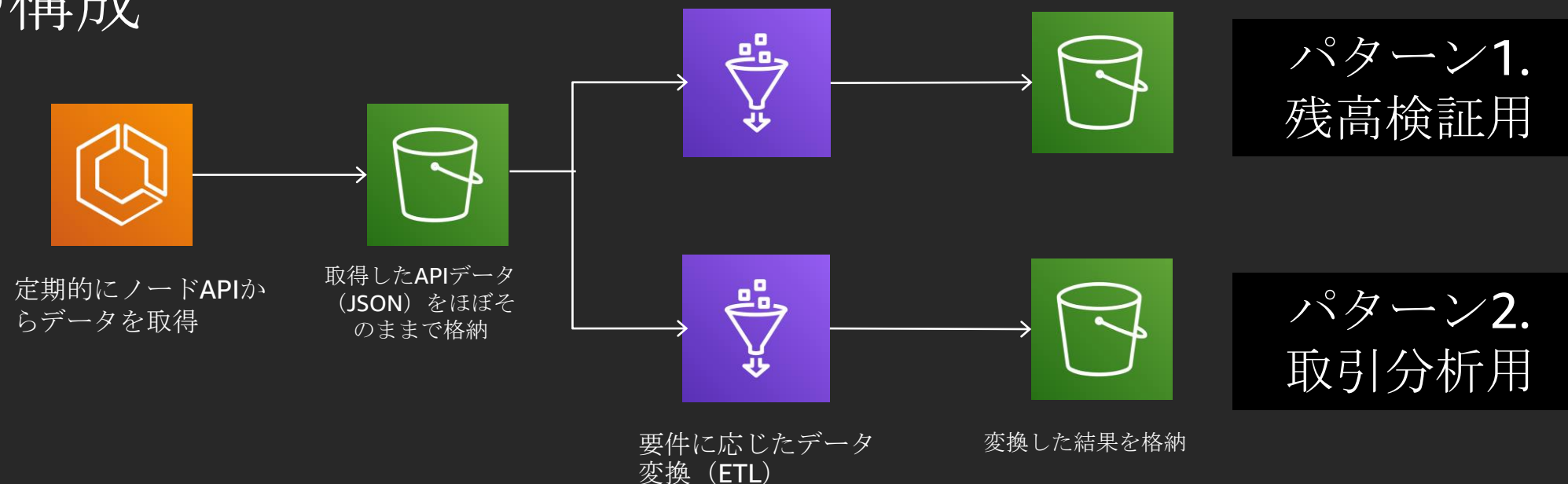


変換した結果を、リレーショナルデータベースに格納

データ加工の解決策

- ブロックチェーンの特性上、既存データの更新はあり得ないため、ストレージをリレーショナルデータベースからオブジェクトストレージに変更。
- APIから取得したデータは、オブジェクトストレージに貯めておき、要件決定後に**Spark**を使って必要な形にデータを加工するようにした。
(データレイク的思想)

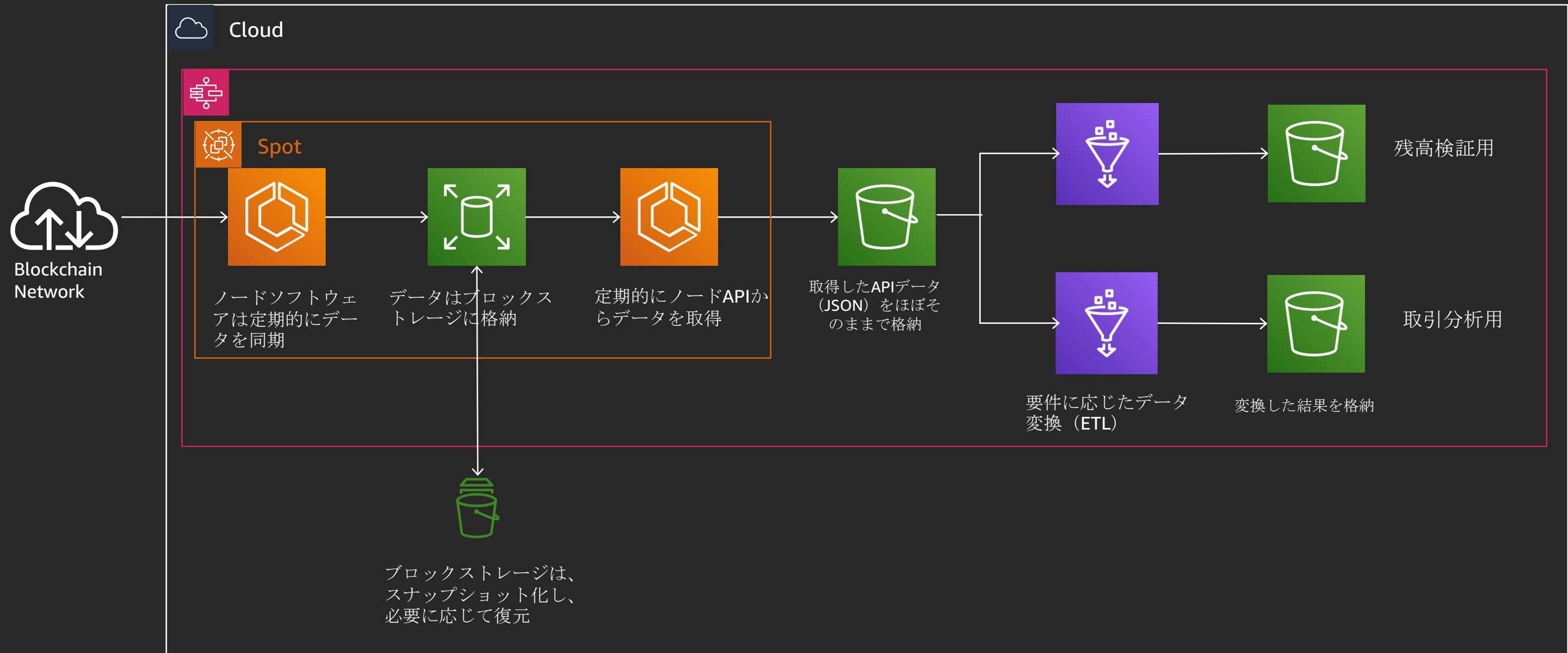
解決後の構成



要件に応じて後から変換パターンの追加が可能。

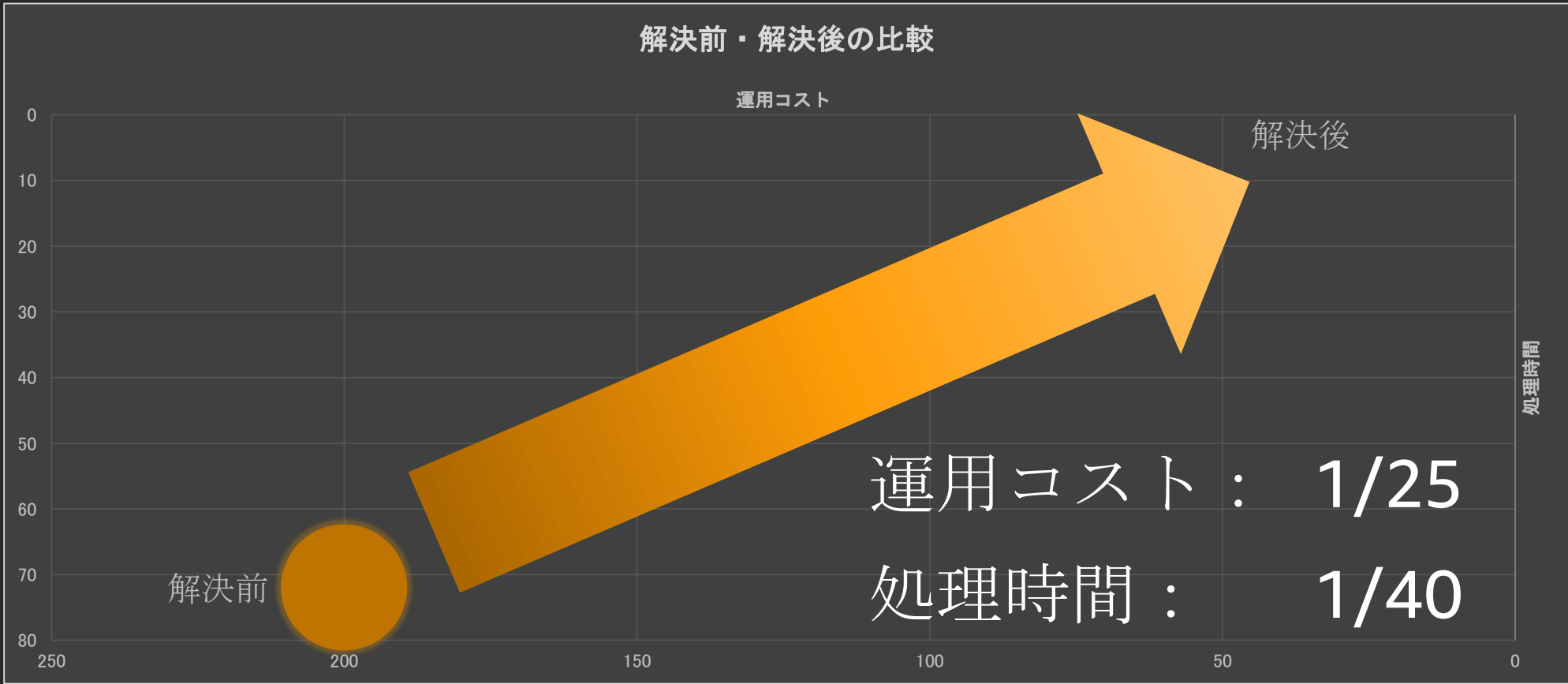
課題解決後のシステム構成

クラウドを活用したマイクロサービスの構成に。



課題解決前後の比較

アーキテクチャの変更により運用コスト及び処理時間の飛躍的圧縮が実現。



Next Steps

Next Steps

CAPP3

今後の予定

- 機能を拡張（バージョン3: CAPP3）

【多機能】
→ 多種データを組み合わせ検知機能化

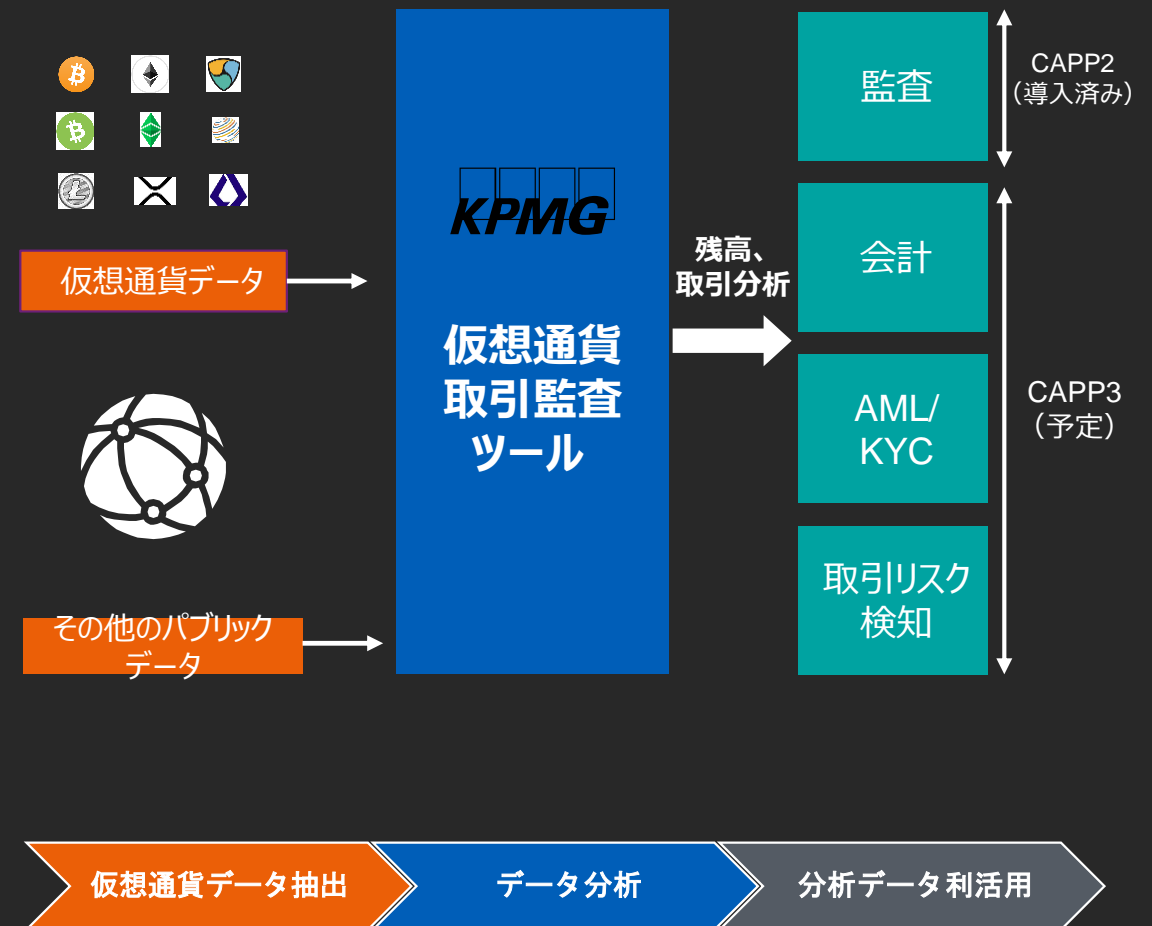
- 機械学習による取引リスクを検知

【高精度】
→ 全取引の機械学習で検知精度向上

- ハイリスク口座、ハイリスク取引のモニタリング

【即時性】
→ マネロン、テロ資金、違法売買のアラート

仮想通貨取引監査ツール（Crypto Audit Platform） 概要図



Thank you!

Junya Kondo

junya.kondo@jp.kpmg.com

Yoshinori Seki

Yoshinori.seki@jp.kpmg.com

Masatake Toyota

Masatake.Toyota@jp.kpmg.com