Hyper Ledger Fabricお勉強ノート

・目的

fabricがV1.0になって大きく仕様が変わったよって話少し勉強がてら要素をまとめて見たいと思った。

WordとかExcelって本当に嫌い（苦手なのでその勉強も兼ねて）

いや、メールでファイルとか送るのめんどくさい。チャットベースでドキュメントに修正とかHyperLedgerで使ってるの見て試したくなったから（うちの会社でもこんなの導入してくれないかなぁ。）。

そんだけそんだけ

・基本的方針

google docsでは他ユーザーに対して編集可能か参照可能を規定することができるけど、

基本的にチャットとか試したい。質問とか修正がある時は、提案モードにしてコメントを残してください。匿名にて提案をされる際には、コメントに名前を残してくれると嬉しい。

いや、コメント残してくれるだけでも嬉しいです(どんなコメントでも大歓迎です。質問とか提案とか)。楽しんでくれれば松ケ谷は本望です（泣いて喜びます）。。。ソーシャルドキュメンテーション！

仕様についてわからないところは聞いて確認してupdateします。

主にUpdateが多いのは土日です（笑）

・fabric V0.6について

ここは主要素ではないので簡単にまとめる。とわかりやすくまとめたURL貼るだけ。。。

<http://qiita.com/kyrieleison/items/ec5223bbe6140822df4a>

これは忘れていただきたい。

・fabricV1.0について

できるだけエンジニアじゃない感じで書きたい。

ここから本題。基本的に参考にする部分は

<https://hyperledger-fabric.readthedocs.io/en/latest/index.html>

重要な部分を中心に書きたい。。。

あ、いやこれも読む必要あるかな

<https://fabric-composer.github.io/>

<https://docs.google.com/document/d/1R5RtIBMW9fZpli37E5Li5_Q9ve3BnQ4q3gWmGZj6Sv4/edit#heading=h.z6ne0og04bp5>

# KEY CONCEPTS

## ledger

* 1. ledgerは全てのトランザクション（チェインコードの呼び出した結果）を表したレコードの集合体である。参加者によって呼び出された更新、削除の結果がキーと値のペアで持たれている。そもそもledgerは不変の、シーケンス化されたブロックに格納されているブロックチェーンと現在の状態を表す状態データベースで構成されている。チャネルごとに一つのledgerを持っており、各ピアはメンバーとなっている各channelごとのledgerを持っている
     1. Todo:そもそもchannelが新しく出てきた。これはなんだ。。。
  2. 検索と更新はキーを利用したもの、範囲を利用したもの、両方使ったものと結構使える。読み取りはクエリを利用して十分できるようにしているよ（couchDBを状態データベースに利用した時のみ）。
     1. info:　v0.6ではDB部分にRocksDBが使われていましたが、v1.0より、levelDBまたはcouchDBになりました（デフォはlevel）。ただし、couchDBのほうかリッチに検索機能を使えるようです。今後はRDBにも対応していく予定ですとのことです。当然ながらリッチな検索機能を持つ際には処理能力とトレードオフになっていることが考えられるのでそこは利用用途で考えるべきかなと思います(あくまで予想)。ちなみにv0.6は2000/secとトランザクション性能をうたっていましたが間違いなくあれは理想値です。v0.6にて上記性能が出るのは分散されたノードがIBMのデータセンターの同様の筐体にcontainerを四つ浮かべて試した時と言っていました。ノードを遠隔地に置いて試したらネットワークでスループットに影響出るよねとIBM担当者に聞いたところそれは出ますと言っていた。V1.0でどの程度改善されたかは知りませんが、あまりIBMがメデイアに言う〜トランザクションまで性能が出ますは現実値ではないと思います（むしろブロックチェーンの良い点を殺して実現したりしている）。
  3. ledgerのkeyベースの履歴検索はデータ由来のシナリオの検索を可能にするよ。いやこの部分の日本語訳きつい。おそらくchainに対しての検索はトランザクションの履歴を見れるでー的な感じなのだろうか。。Read-only history queries - Query ledger history for a key, enabling data provenance scenarios
  4. トランザクションにはread setと呼ばれるチェインコードのから読み取られたキーと値のものと、write set と呼ばれるチェインコードで書き込まれたキーと値のものがある。
  5. トランザクションには全てのendorser、処理を確定させたOrdering serviceの署名が含まれる。
     1. info: v1.0より新たにendorser,ordering serviceのpeerの役割が作られました。endorserは最初に処理を受け取り処理内容に問題ないか確認する主体、ordering serviceはその処理の内容を受け取って、各ノードのチェインに書き込む順序を指示するものです。ordering service自体はledgerを持っておらず（持たせることはできるのか❓）、事前に規定されたアルゴリズム（※）に従ってorderを出します。

※アルゴリズムにはsolo、kafka、SBFTが存在しています。以前まで

利用されていたPBFTとかはどっかいった❓

* 1. トランザクションはoridering serviceから各ピアに対してブロックに書き込むように指示が与えられる。またそれを受け取ったピアはendosmentのポリシーの確認を行い、ポリシーの実行を行う。またchainに書き込む前にバージョンチェックを行い、チェインコードが実行される間にキーと値が変更されていないか確認する。
     1. Todo:　endoserによるポリシーの確認はこの時点で行われるのか❓よく流れがわからん。例えばトランザクションを最初に受け取ったendoserは検証を行いその時点でendosementポリシーに反するものがあればトランザクションを否定するのでなく、全てのピアに連携される時点で検証が行われる❓
  2. 確認され問題がなければトランザクションは確定される。
  3. チャネルに属するledgerにはポリシーやアクセス制御リストやその他の情報が含まれている。
     1. Todo:channelごとにledgerが作られているようですといってる❓ここでアクセスコントロールしてるみたいだけど、１つのノードに対して、複数のlegerを持つことを許容している❓

## Privacy through Channels

チャネルによってプライバシーを規定するらしい。

* 1. fabricはチャネルごとにledgerを持っておりそれをチェインコードによって操作する。
  2. ledgerはチャネルのスコープ内に存在していて、ネットワーク全体にshareされる。またchannelを利用して、特定の参加者のみに共有されるように制御を行う。
  3. 特定の参加者のみに実施したい場合別々のチャネルを作成すること。それを利用してトランザクションとledgerを分離する。
  4. このチェインコードを利用してピアはledgerにアクセスする。つまり正しくアクセスするにはチェインコードは必須。またチェインコードによりledgerに書き込むデータは一般的な暗号化は可能。

## security & membership service

* 1. 全ての参加者のアイデンティティを管理してそれを利用したトランザクションの基盤になる。
  2. 公開鍵のインフラは組織、ネットワークコンポーネント、クライアントアプリに暗号証明書を生成するためのもの。チャネルを利用することでプライバシーと機密性を高めることができるとさ。

## 

## Consensus

コンセンサスの概念が書かれているwww学者ではないのでめんどくさいなぁ

コンセンサスとは要約するとブロックに追加される正当性を承認する一連のサークルでと考えてくださいとさ。ちょっと概念すぎてめんどくさいなぁ後回し。

# ARCHITECTURE

WIP

# USECASES

以下についてはfabricにて有効なユースケースとして紹介されているものを記載する。あくまでこのような実装が考えられるよレベルですかね。

## B2B CONTRACT

* 1. ビジネスの契約を信頼できる方法によって自動化する。ブロックチェーンについては公開されてしまうため、秘密情報についてはプライバシー管理を実施する必要がある
  2. 秘密契約についてはledgerが当事者間では容易に確認することができる環境が望ましい。例えばBITを行う際の契約書は定義的に誰からでも参照できる必要がある。
  3. これらのledgerは簡単に確認でき標準化される必要があるため、電子取引のプラットホームを利用して作成するのが良い。

persona

契約当事者、契約の完全性を保証する第三者のステークスホルダー

component

* 1. Multi-sig contract activation　複数署名による契約の履行とか訳せばいいかな契約の実施をカウンターパーティから実施されると契約は保留状態となり、他取引相手または、第三者の参加が必要となる
  2. Multi-sig contract execution　複数署名による契約の実行

契約の中では１つの署名の履行が必要になる場合が存在する。トレードファイナンスではサードパーティ側が船荷を確認した時のみ、支払いが実行可能になる。

* 1. Atomicity of contract execution 契約の原子性　うまい訳し方教えてww契約の原子性は資産の移転がDVPによって資産の移転が発生した時にのみ保証される必要がある。いかなるステップが失敗した場合にはトランザクション全体をロールバックする必要がある。
  2. contract to chaincode チェインコード間の通信契約

同一のledgerにあるchaincodeは一律に通信できる必要がある

* 1. Longer Duration contract 長期間の契約

長期間のB２Bの契約の際にはタイマーの設定が必要になる。

* 1. reuseale contract 　再利用される契約

利用頻度が高い契約については標準化することが可能

* 1. Auditable contractual agreement 監査上の契約の同意

全ての契約は第三者により監査可能となる

* 1. Contract life-cycle management 契約ライフサイクルのマネージメント

B２Bの契約は常にユニークであり、全て標準化できる訳ではない。ledger networkのスケーラビリティを高めるには効率的な契約管理システムが必要

* 1. validation access 検証用のアクセス

検証用の権限を与えられたもののみががトランザクションの検証が可能

* 1. view access 参照用のアクセス

　 B２Bの契約には機密情報が含まれる、そのため事前に参照権限を与えらアカウントのみが参照することができる。

## **Manufacturing Supply Chain**

最終集約事業者（自動車メーカーのような）はサプライチェーンを構築することができる。これは最終集約事業者がサプライヤーをより適切に管理することができるようになり、車両リコールなどのイベントに適切に対応できるようになる（例えばサプライヤーにより提供された部品が誤っていた場合など）fabricは標準的なプロトコル利用するchain networkを提供し、それを参加者が容認することで、特定車両に利用され、作られる番号付きの部品の入荷やトレースを実現する。

persona

final assembler

全ての製品を集めて実行（製品を作成する）ビジネスのエンティティ

part supplier

部品のサプライヤー、サプライヤーはサブサプライヤーから部品を受け取り組み立て、完成した製品をrootに送る

key components

* 1. Payment upon delivery of goods 　商品の送達に対する支払い

商品受け取り時に支払いが可能になるようにoff-chainなシステムと統合する必要がある

* 1. Payment upon delivery of goods 　第三者監査

全てのサプライヤーからの部品はサードパーティーによって監査可能でなかればいけない。例えば規制当局は特定のサプライヤーから提供された部品のトータルの数を追跡できる必要があります。租税の計算に利用。

* 1. Obfuscation of shipments　出荷の難読

残高は難読化する必要があります。何故ならばサプライヤーが他のサプライヤーのビジネスアクティビティを確認されないようにするため。

* 1. Obfuscation of market size 市場規模の難読化

総残高については難読かする必要がある。サプライヤーが契約の交渉を行う際にレバレッジを使用する際に自分たちの市場規模を知られないようにするため。

* 1. validation Access 検証用のアクセス

検証用の権利を与えられたもののみがトランザクションの検証をできる（部品の送達）

* 1. view access 参照用のアクセス

参照用のアクセス権を持ったもののみが、出荷された部品と可能な部品の残高を確認できる。

## **Asset Depository**

金融証券などの資産はblockChainのネットワーク上に電子化するようできる必要がある。それは資産のタイプ上の全てのステークホルダーがその資産に直接アクセスできるように、仲介のレイヤーを経由せずに取引に参加し、資産の情報を取得できるようにする為である。取引は全てほぼリアルタイムにて実施され、全てのステークホルダーはほほリアルタイムにて資産の情報にアクセスできるべき。ステークホルダーはオペレーションコストを下げるために自動化ロジックを利用する。その例としていかなる❓（任意の）資産に対して、ビジネスルールを追加する必要がある。

persona

投資家　資産の利益並びに法的所有者

発行者 　ledgerネットワークに電子化された資産を発行したビジネス事業体

カストディアン　投資家に彼らの資産を管理するために雇われたもの。また管理されている資産に付加価値サービスを提供するもの

証券保管所　電子化された資産の保管所

key component

asset to cash 資産の流動化（現金化）

発行体が支払いをできるように、また投資家から資産を受け取れるように、チェーンを利用しないシステムとの統合が必要

reference rate 参照レート

変動金利のレートなどのいくつかの資産は外部のデータにリンクされた属性（参照レート）を持つことがあり、それらの情報はledger networkに渡される必要がある。

asset auditor 資産監査人

資産取引はサードパーティが監査できる必要がある。例えば当局はマーケットのリスクを認識するために取引や資産の動きを監査したいと考える可能性があるから

## **One Trade, One Contract**

WIP

## **Direct Communication**

WIP

## **Separation of Asset Ownership and Custodian’s Duties**

WIP

## **Interoperability of Assets**

WIP