DELIA設立一周年記念セミナー

最新ブロックチェーン事情とBBc-1

株式会社ゼタント
久保 健

ZETTANT

自己紹介

クボ　タケシ
久保　健

- 株式会社ゼタント 代表取締役
- (社) ビヨンドブロックチェーン 理事 (技術開発担当)
- (株) ブロックチェーンハブ シニアアーキテクト

- 大手通信会社の研究所および事業部に計16年在籍
  - IPネットワーク、認証システム、分散システム、ゲーム理論等の研究
  - 大規模サービス・インフラ開発のプロジェクトマネジメント
- 次世代ブロックチェーン基盤 BBc-1のメイン開発者

会社紹介

ZETTANT

https://www.zettant.com

- 2017年5月 創業（ブロックチェーンハブの支援を受け創業）
- セキュリティ技術、ブロックチェーン技術、ネットワーク技術、データ分析
- 自社サービス開発、コンサル、受託開発

blockchain hub

メンバー構成

研究・技術者：5名
マーケティング・営業：1名
CFO：1名

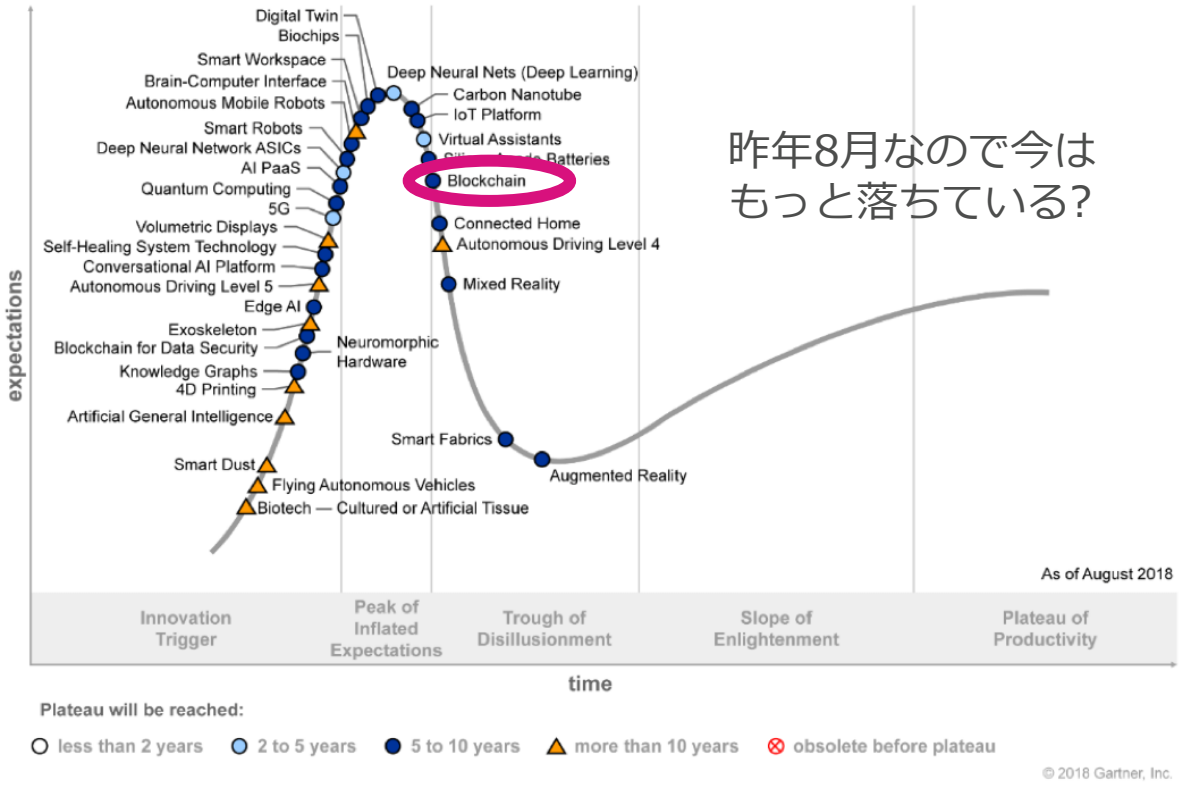
企業様向けのファイル交換サービス「iTransfy for biz」のトライアルを始めています。
操作がとてもシンプル、それでいて非常に安全という2点に特化しています。
ご興味のある方は是非ご連絡ください。

昨今のブロックチェーン事情

昨今のブロックチェーン事情
ブロックチェーンのビジネス＆技術動向
ブロックチェーン利用の2つの大きな方向性
Beyond Blockchain-1 (BBc-1)の位置付け
BBc-1事始め
まとめ

ZETTANT

ガートナー　ハイプ・サイクル

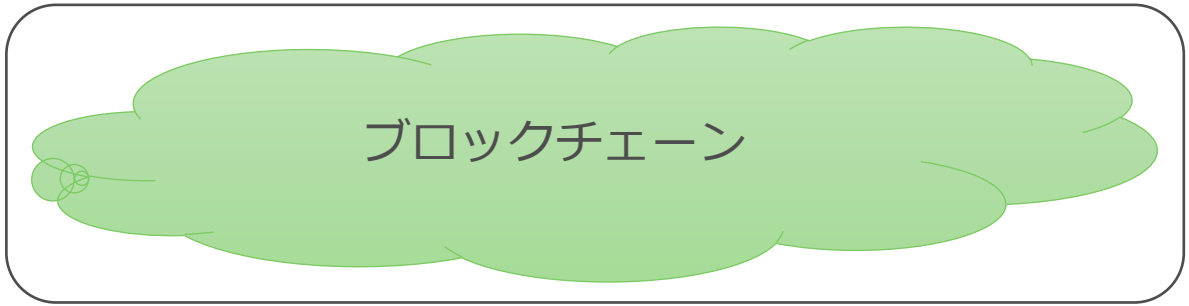


昨年8月なので今は
もっと落ちている?

ZETTANT

1年ぐらい前までの状況

解決したいビジネス課題



とりあえずブロックチェーンでしょ
（とはいえ半信半疑）

そしてICOバブル、仮想通貨バブル

ZETTANT

最近の状況

解決したいビジネス課題

ブロックチェーン

結局何ができるのか整理が必要

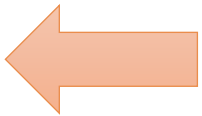
それ、ブロックチェーンいるんだっけ？

ZETTANT

そんなに悪い流れではない

- これまでの評価が過大だっただけ
- ようやく冷静になる人が増えた
- 今有力とみなされているものも、本当にいいのかどうかまだわからない

・ビジネス的な流れ
・技術の本質



この両方を見極めておけば、今からでも乗り遅れることはない

ブロックチェーンのビジネス＆技術動向

昨今のブロックチェーン事情
ブロックチェーンのビジネス＆技術動向
ブロックチェーン利用の2つの大きな方向性
Beyond Blockchain-1 (BBc-1)の位置付け
BBc-1事始め
まとめ

ZETTANT

業界動向

- プラットフォーム競争
- オフチェーン、セカンドレイヤ
- クロスチェーン
- ステーブルコイン
- STO
- トレーサビリティ、金融サービス

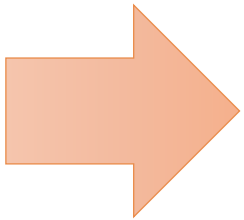
プラットフォーム競争

普及しているもの

Bitcoin

Ethereum

・
・
・



スケーラビリティ
ファイナライズ
ガバナンスなどの課題

新型プラットフォーム

- DPoS
  限定ノードによる
  ブロック承認
- ブロックなし
  そもそもブロック
  を生成しない
- ガバナンス改善
  フォークへの考慮

ZETTANT

新しいプラットフォームたち

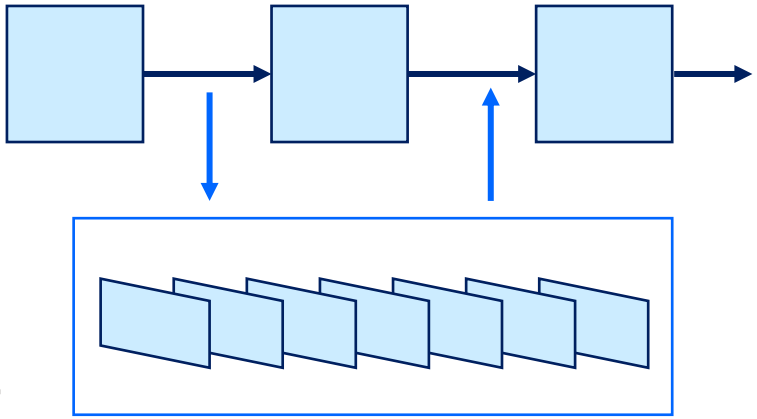
- EOS
  - DApp (Decentralized Application) プラットフォーム
  - 数万件以上/秒、取引手数料無料
- Tezos
  - 3つのプロトコル（ネットワーク、トランザクション、コンセンサス）を独立させることで、ハードフォークに左右されない仕組み
- DFINITY
  - 分散化されたクラウド「クラウド3.0」
- IOST
  - PoB (Proof of Believability) という新しい仕組みを導入
- Hedera Hashgraph
  - ゴシッププロトコルによる分散コンセンサスアルゴリズム
  - ブロックなし
- BBc-1
  - ブロック、マイニング無し

ZETTANT

オフチェーン（セカンドレイヤ）技術

期待
- スケーラビリティ問題の解決
- マイクロペイメント等のビジネスニーズへの対応

仕組み
- メインチェーンの外で大量のトランザクションを高速処理する
- その結果のみをメインチェーンに還元する



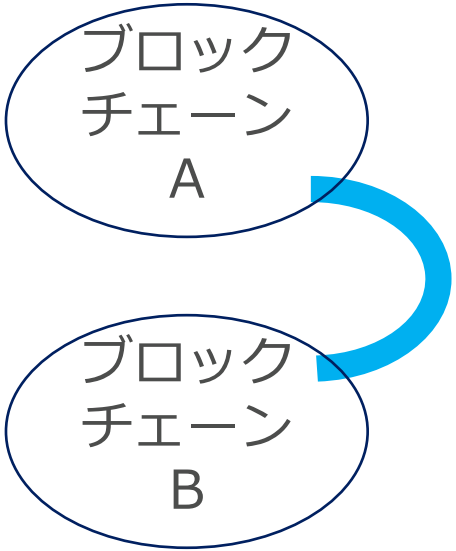
- ビットコイン
  - Lightening Network
- Ethereum
  - Plasma
  - Raiden Network

ZETTANT

クロスチェーン

異なるチェーンをつなぐ技術

- 取引所などの第三者を経由せず、異なる仮想通貨を直接交換可能に
- 取引所のセキュリティリスクや手数料等を回避



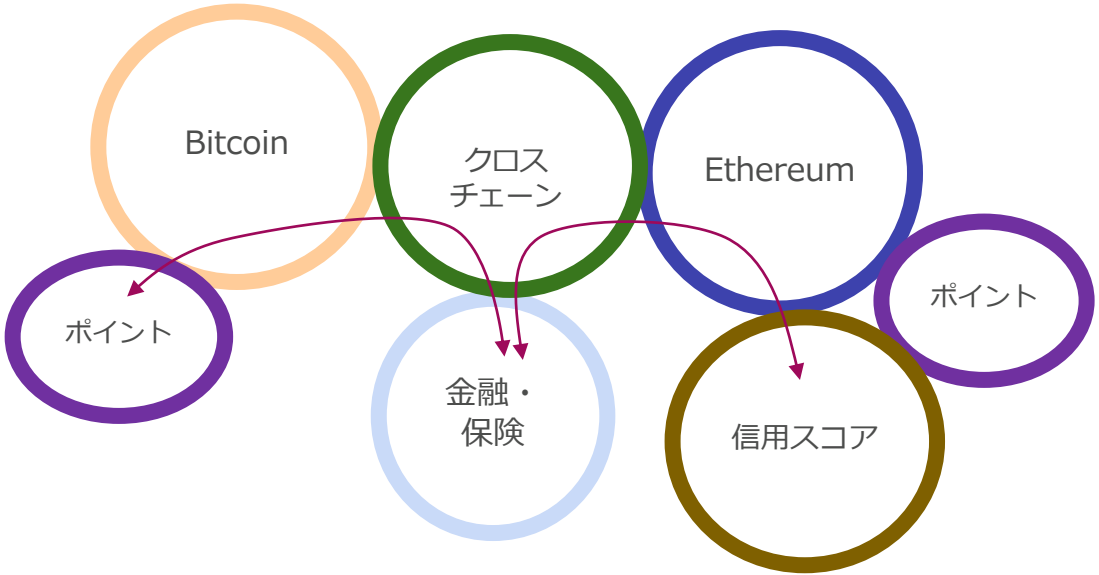
- Cosmos　異種チェーン間トークン移転
  - https://cosmos.network/
- Polkadot　BC間接続ネットワーク
  - https://polkadot.network/
- WanChain
  - https://wanchain.org/
- AION
  - https://aion.network/

ZETTANT

クロスチェーンへの期待

複数のブロックチェーンの上のサービス同士がつながる

- サービス間連携による利便性の向上



特定サービスにおける意味

サービス利用

↓

金融アプリと連携

↓

サービス利用実績を金融・保険会社等チェック

ZETTANT

ステーブルコイン

仮想通貨・トークンの問題である価格変動リスクを抑える工夫を施す

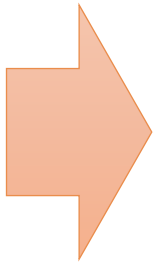
法定通貨担保	仮想通貨担保	需給調整
担保する法定通貨で価値裏付け	他の特定暗号通貨（ETH等）で価値裏付け	発行量を管理し価格を調整
Tether TrueUSD	DAI (Ether担保)	Basis Carbon Kowara

ZETTANT

STOによる健全なトークン流動性拡大へ

ICO
(Initial Coin Offering)

- ユーティリティトークン（利用権）という建前
  - 証券・規制対象とは曖昧な線引き
- 投機・詐欺が横行



STO
(Security Token Offering)

- 証券性を前提
  - 現実世界における資産価値による裏付け
- 米国SEC等の規制当局に対応

株式や不動産などを
トークン化して流通させる

ZETTANT

トレーサビリティ

サプライチェーン上の物資の流通過程の記録と共有
- 物資の流通とブロックチェーンの特性が適合している

- Food Trust
  - 米WalmartとIBMによって始まった食品トレーサビリティ
  - 他の企業も参加し始めている
  - Hyperledger Fabricを利用
- TradeLens
  - デンマークMaerskとIBMによって始まったコンテナ船による国際貿易の物流トレーサビリティ
  - 事務処理コストを低減が目的

ZETTANT

金融サービス

送金、証券取引、法定通貨代替 などを目的としたデジタル通貨

- リップル、JPMコイン
  - 法人向けの国際送金を主眼においた仮想通貨
- ステラ
  - 個人向けの送金を主眼においた仮想通貨
  - 中国から参加できない

保険

- 国際物流での貨物事故のための保険の事務処理の簡略化
- 少額短期保険（オンデマンド保険）
- 低所得者向け保険

ブロックチェーン利用の2つの大きな方向性

昨今のブロックチェーン事情
ブロックチェーンのビジネス＆技術動向
ブロックチェーン利用の2つの大きな方向性
Beyond Blockchain-1 (BBc-1)の位置付け
BBc-1事始め
まとめ

ZETTANT

仮想通貨・トークンとそれ以外

仮想通貨やトークンを中心
としたビジネスを考えたい

ブロックチェーン技術の特性を
活かしたビジネスを考えたい

仮想通貨以外
という意味

仮想通貨・トークンとそれ以外

仮想通貨やトークンを中心
としたビジネスを考えたい

ブロックチェーン技術の特性を
活かしたビジネスを考えたい

ブロックチェーンが必要なのかどうかとかは
あまり気にする必要はない（と思う）

- 仮想通貨はブロックチェーン上で運営されている
- ブロックチェーンを使わない仮想通貨はきっと受け入れられない

ZETTANT

仮想通貨・トークンとそれ以外

仮想通貨やトークンを中心
としたビジネスを考えたい

ブロックチェーン技術の特性を
活かしたビジネスを考えたい

- 何らかの仮想通貨やトークンそのものを作りたい
  - 法定通貨の代用品
  - ポイントの代用品
  - 証券の代用品

認知されるのか
法的な問題も（資金決済法、金商法など）

ZETTANT

仮想通貨・トークンとそれ以外

仮想通貨やトークンを中心
としたビジネスを考えたい

ブロックチェーン技術の特性を
活かしたビジネスを考えたい

- 何らかの仮想通貨やトークンを利用するサービスを作りたい
  - ウォレット
  - 支払手段
  - ポイント

どの仮想通貨に対応するのか
結局最後に法定通貨に勝てるのか
法的な問題も（資金決済法、金商法など）

ZETTANT

仮想通貨・トークンとそれ以外

仮想通貨やトークンを中心
としたビジネスを考えたい

ブロックチェーン技術の特性を
活かしたビジネスを考えたい

そもそもなぜブロックチェーンを使いたい
のかを吟味したほうがいい（と思う）

- ブロックチェーンは、そもそも効率が悪い仕組み
- 使いたい理由がないと、損しかしない

ZETTANT

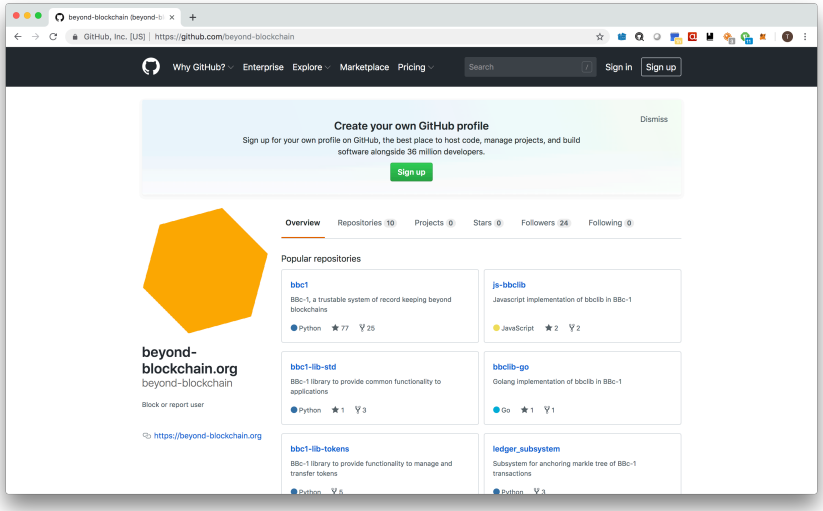
Beyond Blockchain-1 (BBc-1) の位置付け

昨今のブロックチェーン事情
ブロックチェーンのビジネス＆技術動向
ブロックチェーン利用の2つの大きな方向性
Beyond Blockchain-1 (BBc-1)の位置付け
BBc-1事始め
まとめ

ZETTANT

オープンソースプロジェクト

https://github.com/beyond-blockchain/bbc1



BBc-1のリファレンスシステムモデルをPythonで実装しています

- ご興味のある方は是非触ってみてください

一般社団法人ビヨンドブロックチェーンで開発・普及をすすめようとしています

- 協力してくださる方を絶賛募集中です！

連載記事もあります　技術評論社　bbc1　で検索

ZETTANT

BBc-1が取り組む課題

ブロックチェーンを何のために使うのかを１から考え直した

- 情報が「**改ざんされていない**こと」を**確認できる**ようにする
- 情報が「**存在**していたこと」を**否定できない**ようにする
- 上記2つを**誰でも実施**できるようにする

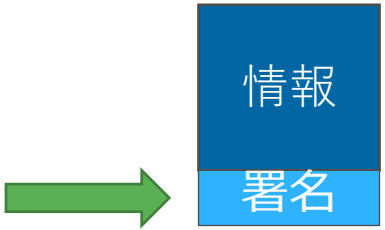
ZETTANT

BBc-1が取り組む課題

ブロックチェーンを何のために使うのかを１から考え直した

- 情報が「**改ざんされていない**こと」を**確認できる**ようにする
- 情報が「**存在**していたこと」を**否定できない**ようにする
- 上記2つを**誰でも実施**できるようにする

署名がついていれば
改ざんは検知できる

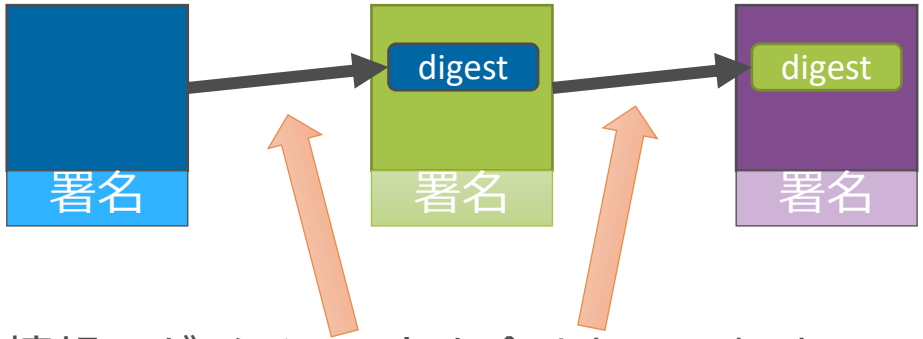


ZETTANT

BBc-1が取り組む課題

ブロックチェーンを何のために使うのかを１から考え直した

- 情報が「**改ざんされていない**こと」を**確認できる**ようにする
- 情報が「**存在**していたこと」を**否定できない**ようにする
- 上記2つを**誰でも実施**できるようにする



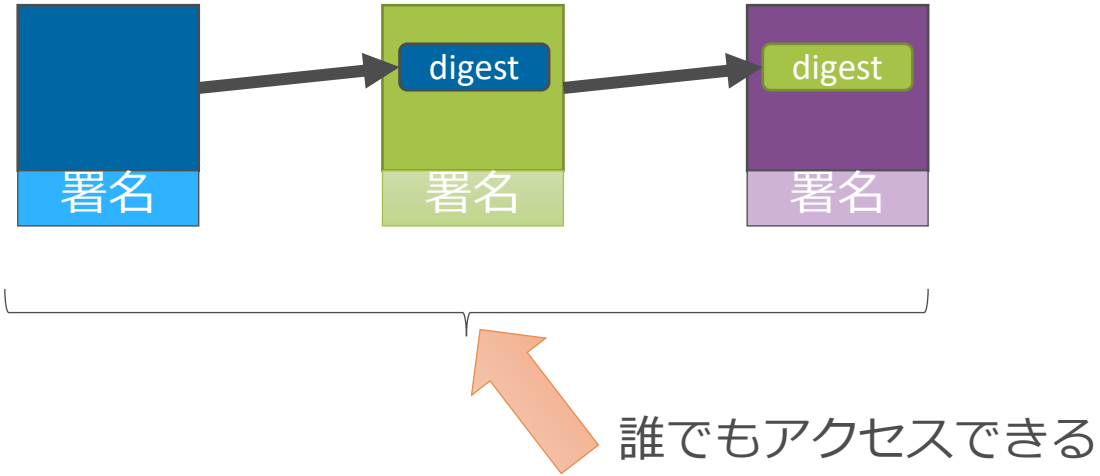
過去の情報のダイジェストを含めた、いわゆるDAG構造を
構成すれば、途中の情報が削除されるとそれを検知できる

ZETTANT

BBc-1が取り組む課題

ブロックチェーンを何のために使うのかを１から考え直した

- 情報が「**改ざんされていない**こと」を**確認できる**ようにする
- 情報が「**存在**していたこと」を**否定できない**ようにする
- 上記2つを**誰でも実施**できるようにする



ZETTANT

BBc-1が取り組む課題

ブロックチェーンを何のために使うのかを１から考え直した

- 情報が「**改ざんされていない**こと」を**確認できる**ようにする
- 情報が「**存在**していたこと」を**否定できない**ようにする
- 上記2つを**誰でも実施**できるようにする

これを実現するのに

必ずしも**分散システムである必要はない**

いわゆる**コンセンサスアルゴリズムも必ずしも必要ではない**

ZETTANT

BBc-1が取り組む課題

ブロックチェーンを何のために使うのかを１から考え直した
- 情報が「**改ざんされていない**こと」を**確認できる**ようにする
- 情報が「**存在**していたこと」を**否定できない**ようにする
- 上記2つを**誰でも実施**できるようにする

BBc-1はこれを実現することを第一義としている

これを実現するのに

必ずしも**分散システムである必要はない**

いわゆる**コンセンサスアルゴリズムも必ずしも必要ではない**

ZETTANT

BBc-1が取り組む課題

ブロックチェーンを何のために使うのかを１から考え直した

- 情報が「**改ざんされていない**こと」を**確認できる**ようにする
- 情報が「**存在**していたこと」を**否定できない**ようにする
- 上記2つを**誰でも実施**できるようにする

これを実現するのに

必ずしも**分散システムである必要はない**

いわゆる**コンセンサスアルゴリズムも必ずしも必要ではない**

必要に応じてBBc-1のアプリケーションレベルで実現する

ZETTANT

BBc-1が取り組む課題

「誰が何に合意すべきか」を精査すること！

パターン１

- 登録する情報（トランザクション）が正しいものでなければ損失を被る可能性がある人

- 情報＝契約の場合、契約の当事者（2者またはそれ以上）は、契約内容に間違いや偽りがあると損失を被る可能性があるので、しっかり確認してその内容を承認する必要がある

ZETTANT

BBc-1が取り組む課題

「誰が何に合意すべきか」を精査すること！

パターン２

- 登録する情報（トランザクション）が正しいものであることを主張したい人

- 情報＝存在を表すものの場合、その情報の所有者や、存在証明をサービスとして提供する人が、「確かにそれは存在していた」と主張するために、その情報を承認する

ZETTANT

BBc-1の肝

情報（トランザクション）に署名を付与すれば、署名した本人はその情報に記載された内容を承認したこととする

- 署名するために必要な「秘密鍵」は本人しか持ちえず、他人が勝手になりすまして署名されることはないため、「間違いなくその人が承認した」ことになる
- したがって、承認できない内容であれば、絶対に署名を付与してはならない

誰が合意する必要があるのかを精査すれば、分散システムやコンセンサスアルゴリズムは必要ない事例もたくさんあるはず

BBc-1の肝

つまり・・・

要件の検討が最も大切

考えるべき要件

- 情報を誰が保管するのか？
- 情報が正しくなかったときに被害を受けるor責任を取るべきなのは誰か？

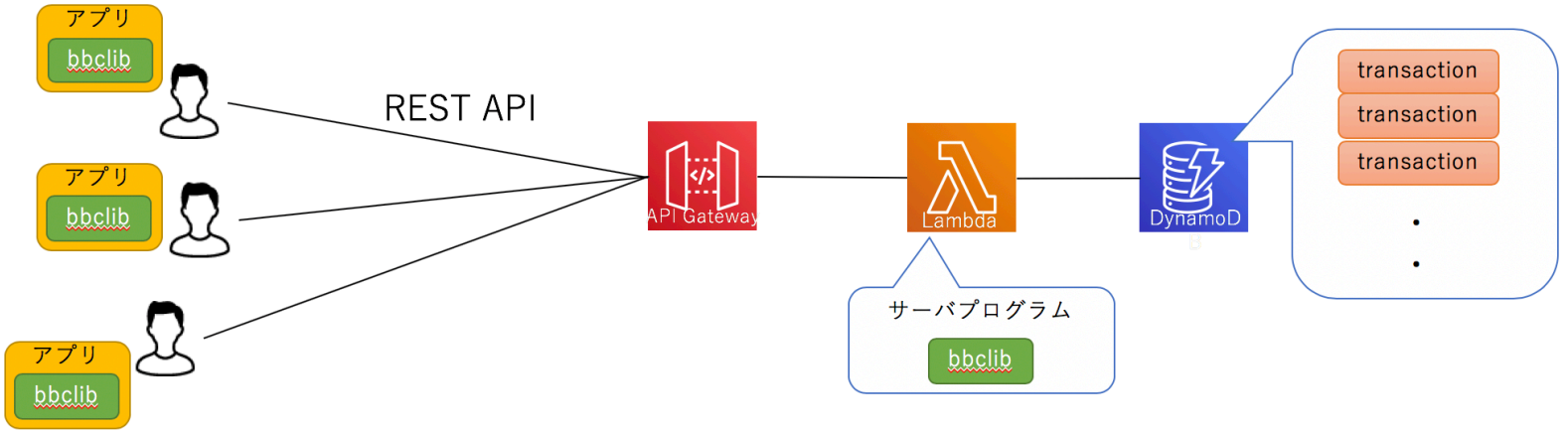
システムをもっと簡略化しパフォーマンスとコストを両立できるようになるはず

ZETTANT

場合によってはこんなシステムでもOK

AWS LambdaとDynamoDBを利用したシステム例

- トランザクションに複数の署名を付与したい場合は、メッセージングの仕組みが必要になる
- メッセージングのためだけにbbc_coreを利用するのは効率が悪いので、メッセージングの仕組みを別途開発/導入したほうがよいと考えられる
  - 例えば、Lambdaを経由する、Redisなどを利用する、など



ZETTANT

参考URL

ここでの考察の詳細は下記URLに公開しています

- https://github.com/beyond-blockchain/bbc1/blob/develop/docs/BBc1_system_design_guide_v1.0_ja.pdf

- https://github.com/beyond-blockchain/bbc1/blob/develop/docs/BBc1_consensus_consideration_v1.0_ja.pdf

気になる方はぜひ御覧ください

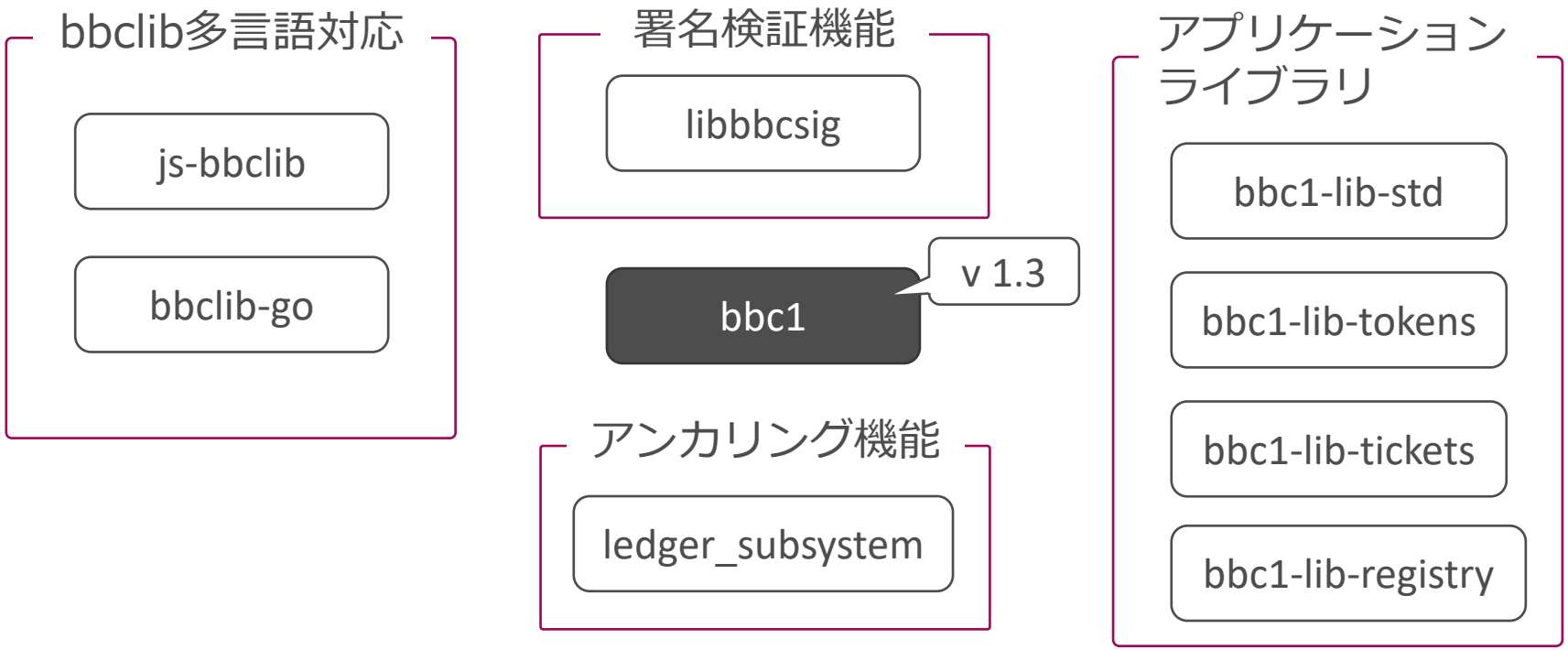
BBc-1事始め

昨今のブロックチェーン事情
ブロックチェーンのビジネス＆技術動向
ブロックチェーン利用の2つの大きな方向性
Beyond Blockchain-1 (BBc-1)の位置付け
BBc-1事始め
まとめ

ZETTANT

BBc-1 リポジトリ構成

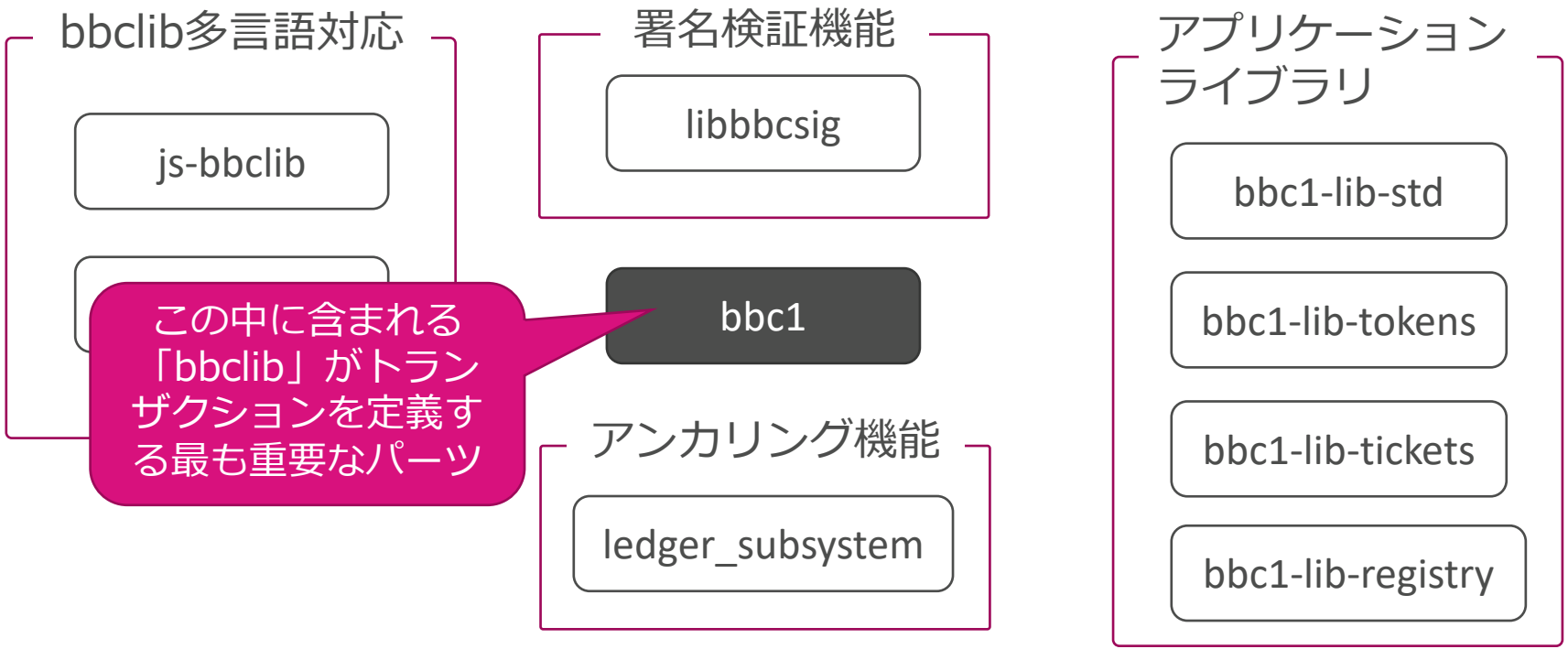
https://github.com/beyond-blockchain?tab=repositories



ZETTANT

BBc-1 リポジトリ構成

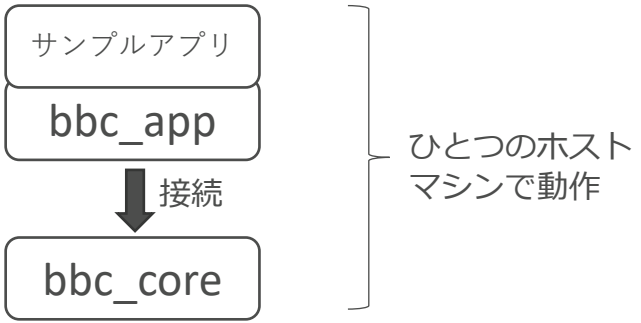
https://github.com/beyond-blockchain?tab=repositories



ZETTANT

BBc-1のはじめ方

- 簡単スクリプト
  - bbc1リポジトリにあるexamples/starter
- 目的
  - 最も簡単なシステム構成でトランザクションの登録と検索までを動作させる
  - BBc-1を使う上で重要なのはトランザクションの作成部分なので、この化暗澹スクリプトは、どのようなトランザクションを作るべきかを練習する土台になる
- システム
  - coreプロセスが1つ、クライアントアプリが1つ、同じホストで起動する



ZETTANT

利用手順

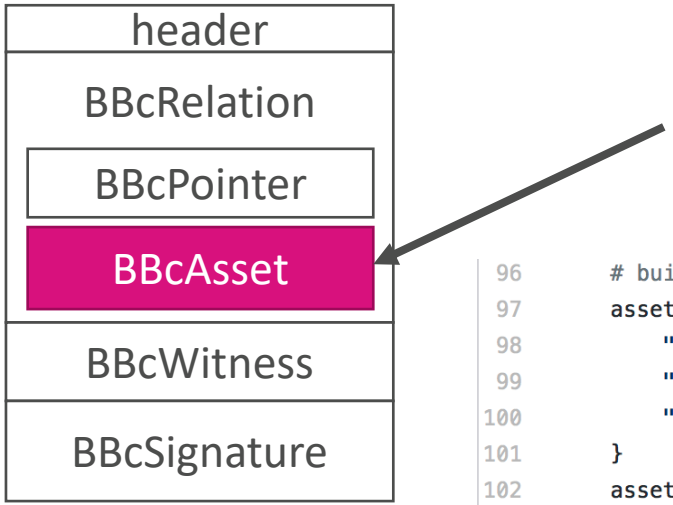
https://github.com/beyond-blockchain/bbc1/blob/develop/examples/starter/README.md

- 手順のとおりに実行するだけで、bbc_coreが起動し、トランザクションがDBに登録される
- Step 5 (トランザクションの生成と登録）は何度も実行すれば、何個でもトランザクションが登録される
- 登録したトランザクションを検索したり、一覧を表示することも可能

トランザクションの作成

- トランザクションを作っているスクリプトの場所
  - bbc1/examples/starter/scripts/register_a_transaction.py

- トランザクションの構成



この中に本当に保存したい
（合意したい）情報を書く

```
96      # build asset body, which is the main data body you want to register in the bbc_core
97      asset_body_dict = {
98          "item_a": 1000,
99          "item_b": "xxxx",
100         "item_c": binascii.a2b_hex("0123456789")
101     }
102     asset_body_data = msgpack.dumps(asset_body_dict)  # in this example, messagepack is u
```

スクリプト内の97行目以降

まとめ

昨今のブロックチェーン事情
ブロックチェーンのビジネス＆技術動向
ブロックチェーン利用の2つの大きな方向性
Beyond Blockchain-1 (BBc-1)の位置付け
BBc-1事始め
まとめ

ZETTANT

まとめ

何をやりたいか、つまりビジネス要件を明らかにするのが先決です

- 仮想通貨、トークンに関わりたい
  - ⇒ ブロックチェーン必須ですが、もしかすると法定通貨に駆逐されるかも
- データに外部監査可能な信頼性を与える必要がある
  - ⇒ 是非、ブロックチェーンの利用を考えましょう
- それ以外
  - ⇒ おそらくブロックチェーンは不要です

ZETTANT

まとめ

考えるべき要件

- 情報を誰が保管するのか？
- 情報が正しくなかったときに被害を受けるor責任を取るべきなのは誰か？

実はブロックチェーンに求める要件はシンプルでは？

- シンプルな要件に複雑な仕組みを採用するのはマイナスが大きい

ぜひ、BBc-1の利用を！

ZETTANT

ご清聴ありがとうございました

t-kubo@zettant.com
https://www.zettant.com

ZETTANT