Internet Week 2017

～君は本当のブロックチェーンを知っているか？～

# エンジニアのための ブロックチェーン基礎講座

株式会社ゼタント
久保 健

2017/12/27

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**
**https://www.zettant.com**

- (株) ブロックチェーンハブ シニアアーキテクト
- (社) ビヨンドブロックチェーン 技術開発担当理事
- Yume Cloud Inc. 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



zettant

# 最近の活動

## BBc-1の公開

新しいブロックチェーンプラットフォームBBc-1をオープンソース(※)として公開。メイン開発者としてプロジェクトに参画

## 鍵/PW管理技術

暗号鍵やパスワードの管理コストを劇的に下げる仕組みをBBc-1を応用して実現

**Blockchain＋Network＋Security技術で**
**Fintech、非金融、IoTを新たなステージに**

(※) https://github.com/beyond-blockchain/bbc1

# アウトライン

- ビットコインとブロックチェーン
- ビットコインの概要
- イーサリアムの概要
- ブロックチェーンの課題
- まとめ

01

# ビットコインと
# ブロックチェーン

# ビットコイン

## 取り組む課題

自分のお金をいつでも自分の好きに送金することを誰にも止めさせない

## ソリューション

- P2Pでコインを授受
- デジタル署名で検証可能性、否認不可能性を担保
- みんなで二重消費を防ぐ

**この実現のために発明されたのが「ブロックチェーン」**

# ブロックチェーンとは

ブロックと呼ばれる順序付けられたレコードの連続的に増加するリストを持つ分散データベースである

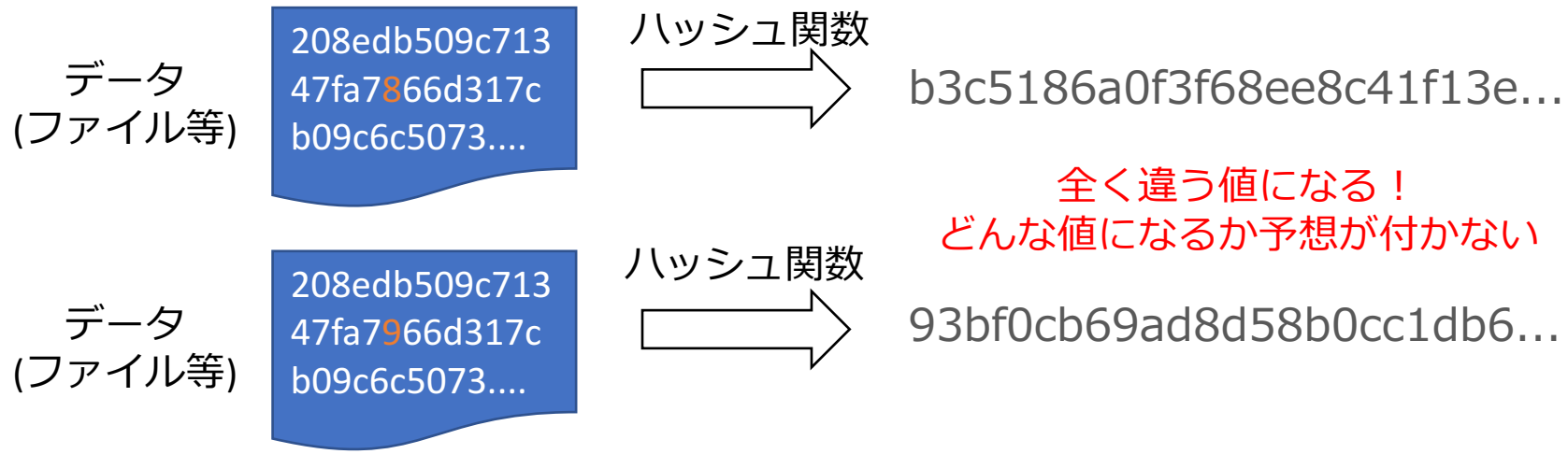
by Wikipedia




zettant

# ハッシュ計算

## 任意のデータを固定長のバイト列（ダイジェスト）に変換する




ビットコインではSHA256などのハッシュ関数が用いられ、256bit = 32Byteのダイジェストが算出される

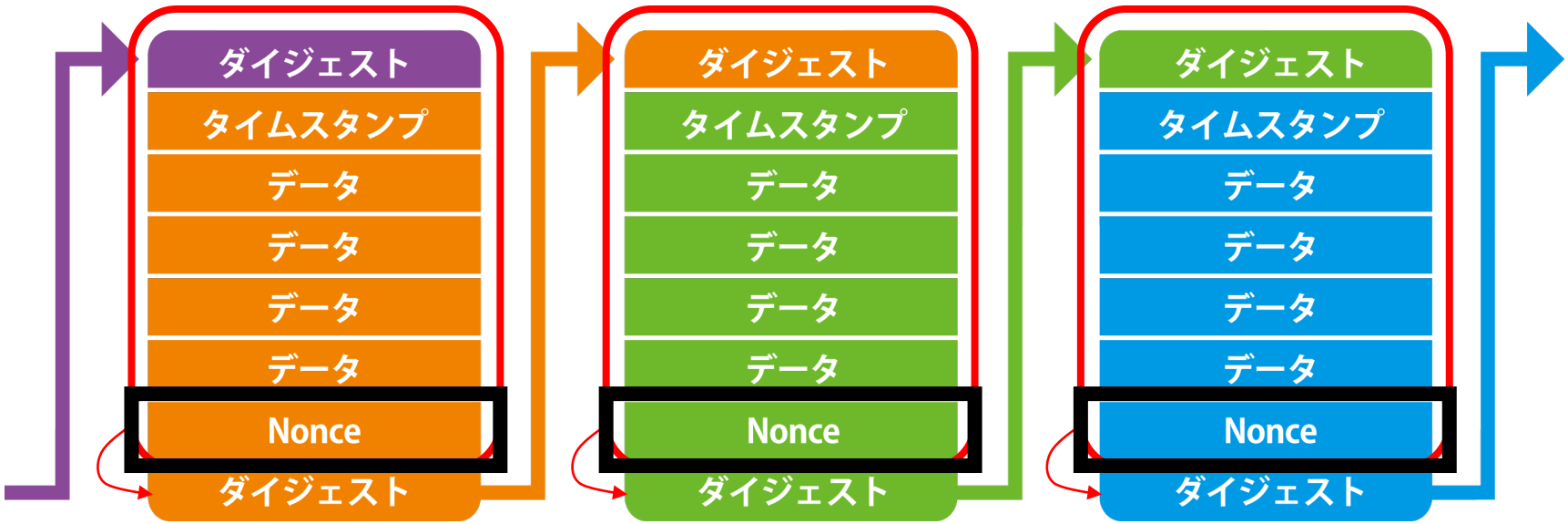


zettant

# ブロックチェーンとは

## しかも、過去のデータを改ざんすることを非常に困難にするしくみを持つ

例：ダイジェストの値に制約を設ける（上位xx桁は0であること）




条件を満たすような**都合のいいNonce**を見つけなければならない



zettant

# ブロックチェーンとは

**改ざんしたら、その後に続く全てのブロックのNonceも探し直さなければならない！**

**→そんなのほぼ無理**

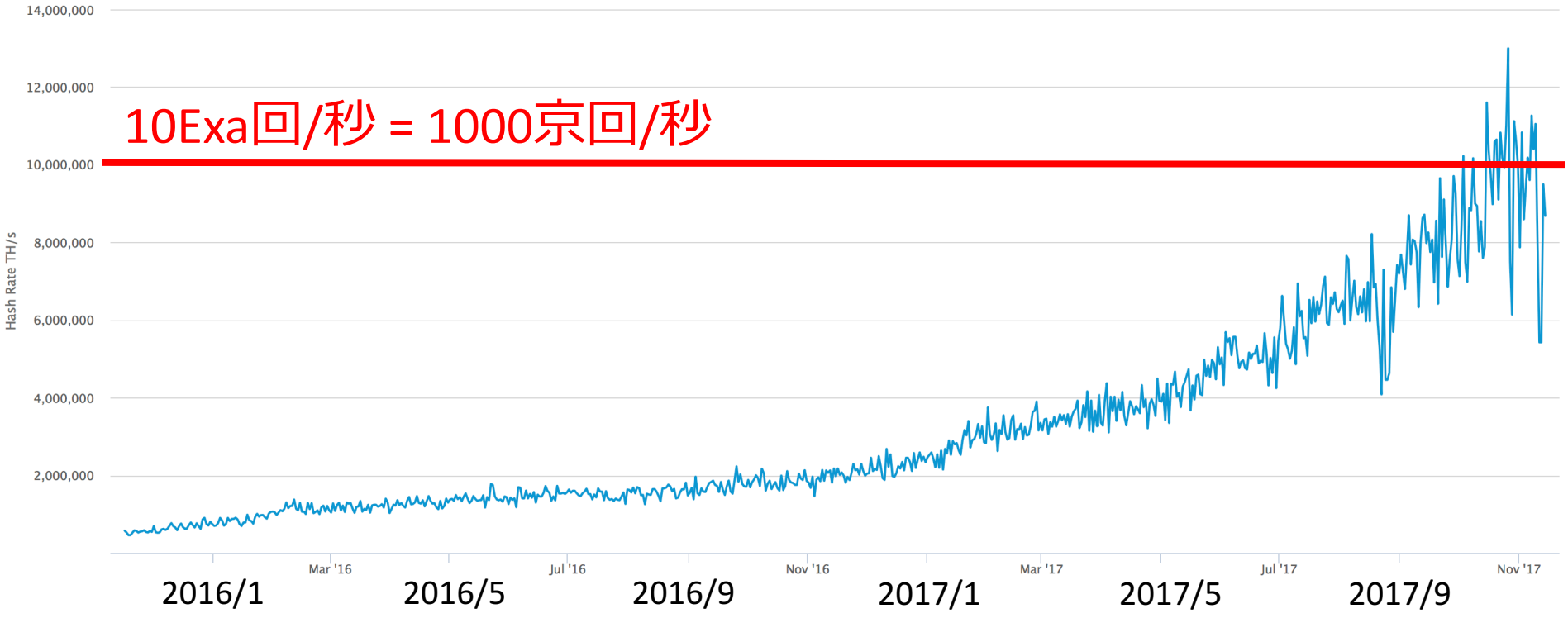

1つのNonceを見つけるだけでも、大量の計算が必要



zettant

# ハッシュレート

ビットコインシステム全体の計算リソースをハッシュレートという値（ハッシュ計算を毎秒何回できるか）で評価している



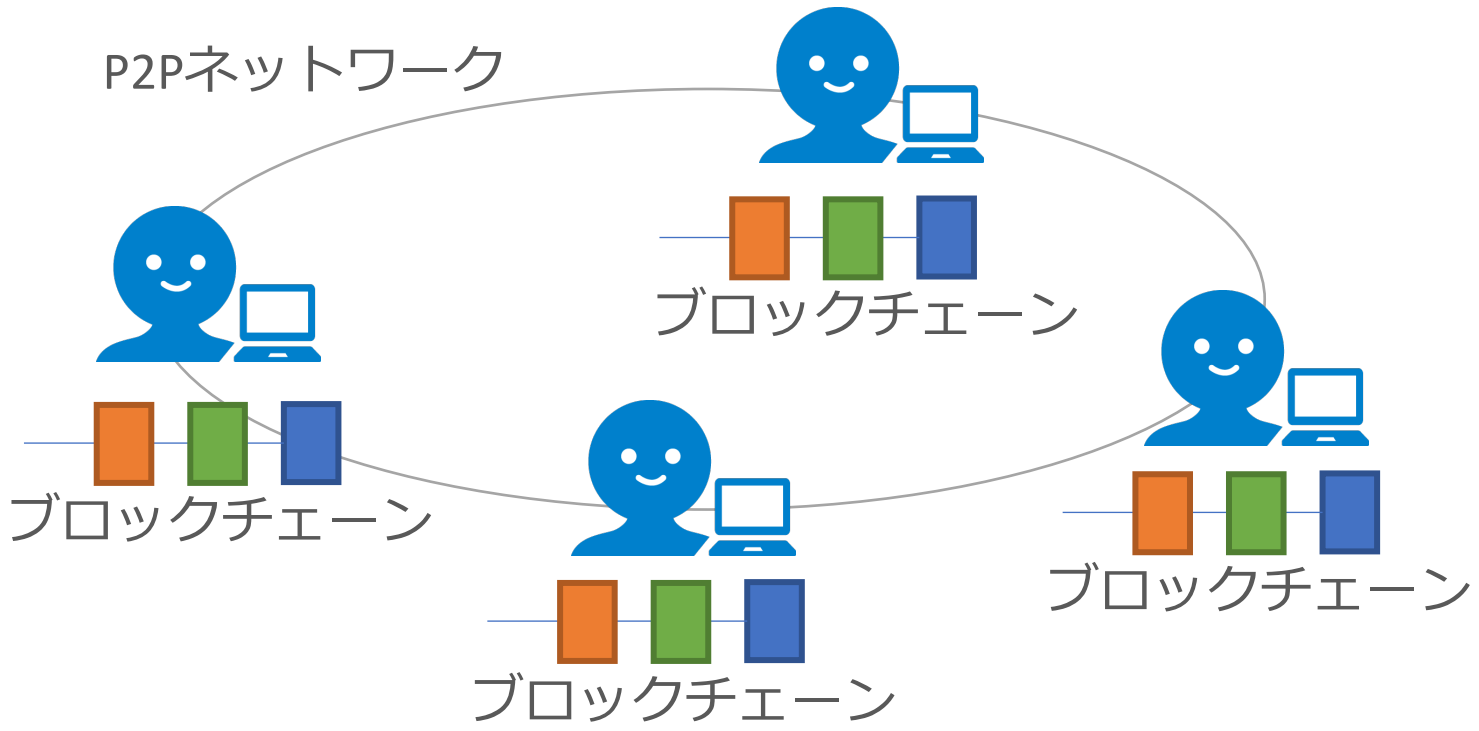

[出展] https://blockchain.info/ja/charts/hash-rate?timespan=2years



zettant

# ブロックチェーンとP2P

**P2Pネットワークを使って参加者みんなでブロックチェーンを保持し、だれでも中身を確認できる**

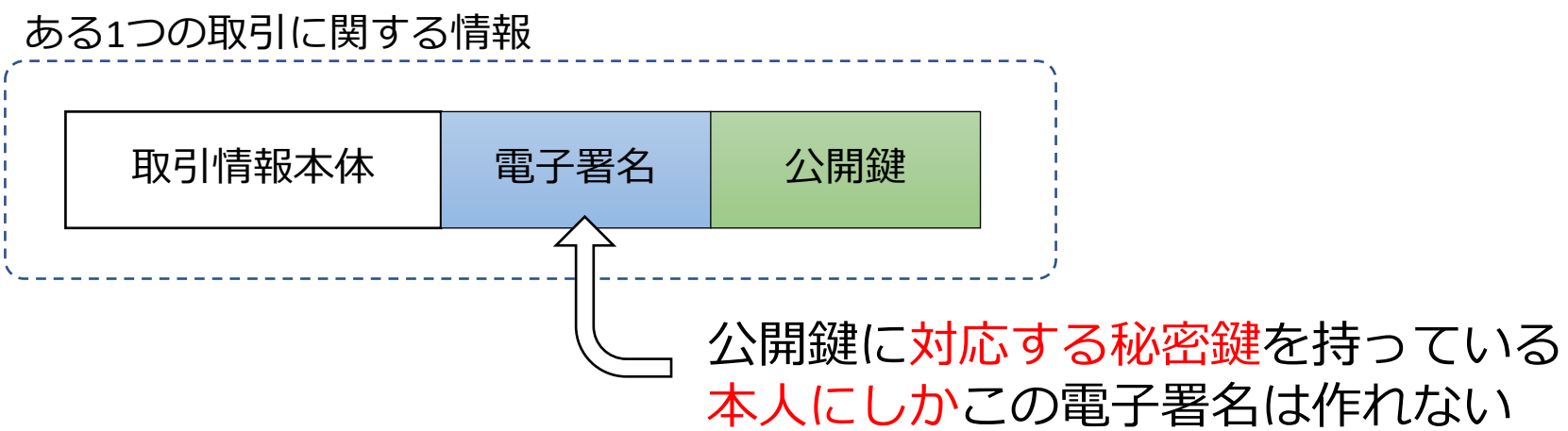





zettant

# ブロックチェーンと電子署名

## 電子署名とそれを検証するための公開鍵をセットにしてブロックチェーンに保存する



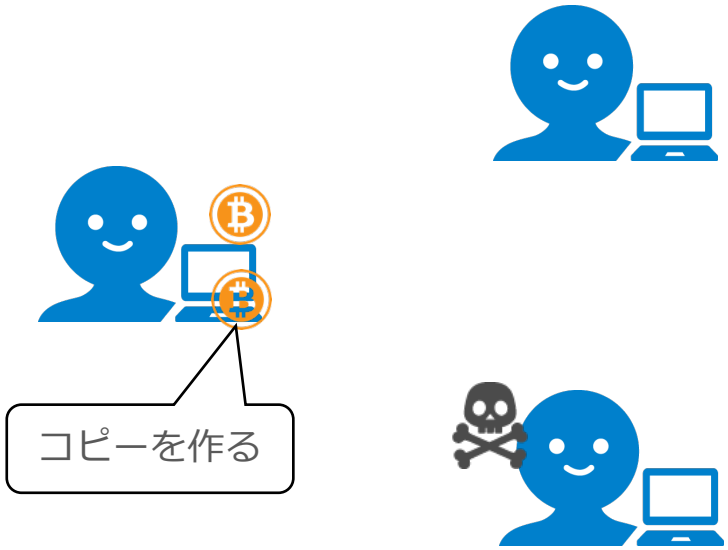

誰が作った情報なのか、改ざんされていないかは、
電子署名の正当性を検証することで確認できる



zettant

# ブロックチェーンと2重消費

## 同じビットコインを2回以上使えてしまうこと



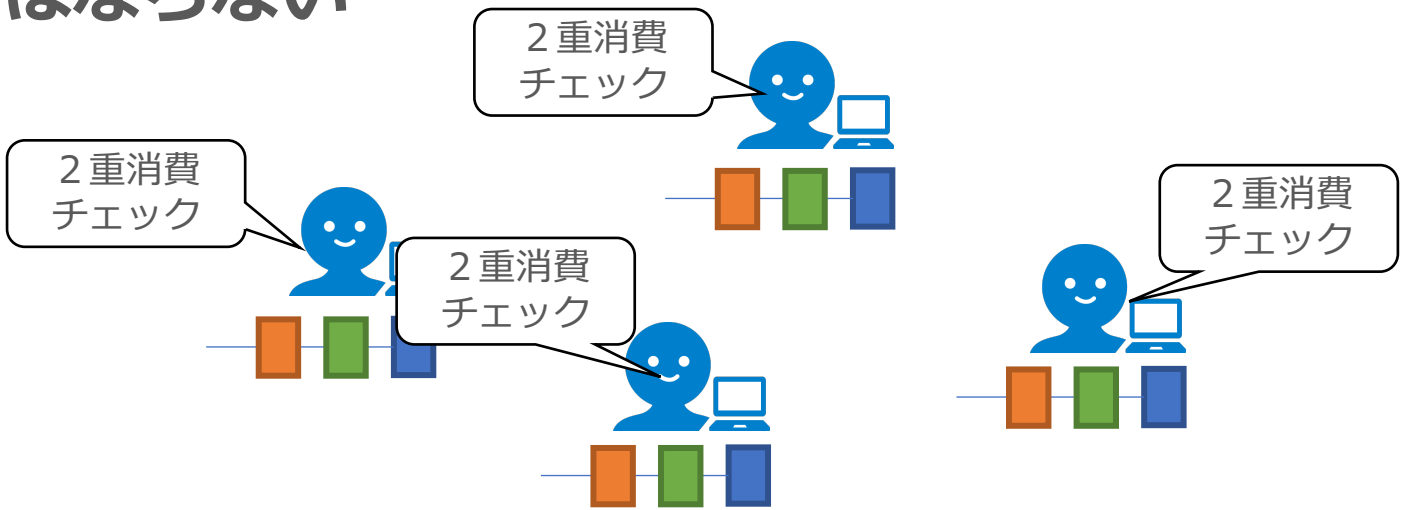

いくらでもお金を増殖させることが出来てしまい、
**価値を維持できなくなる**



zettant

# 2重消費を防ぐためのルール

**ブロックチェーン全体のなかには、同一コインについて「受取」と「支払」の取引情報が1回ずつしか入ってはならない**




ブロックチェーンをみれば**誰でも確認**できる。
2重消費の取引はブロックに**組み込まない**。



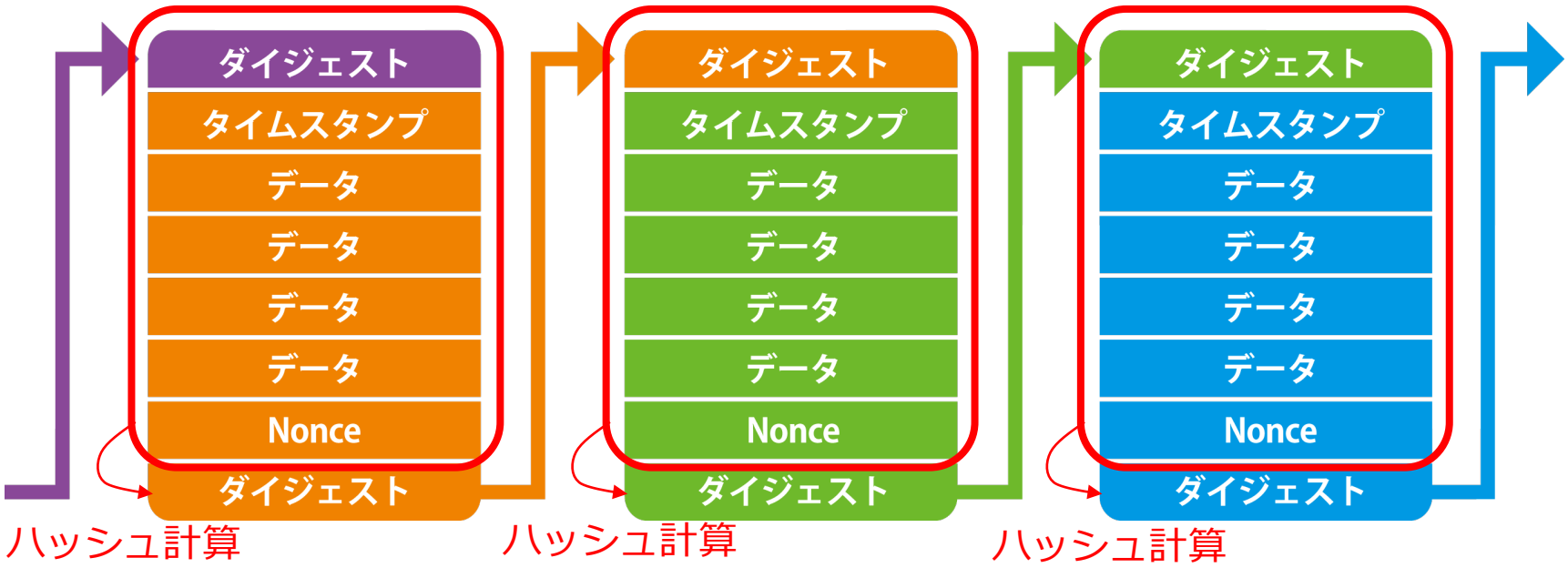
zettant

# ブロックチェーンとは

- 誰もが同じ情報を参照できる
- 過去のデータが容易には改竄できない
- 分散型台帳

# ブロックチェーン(もう一度)

**複数の取引データを1つの束（＝ブロック）にしたものをダイジェストという数字を使って繋いだものをみんなで共有する**




10/21現在、ビットコインのブロックチェーンは145GB程度



zettant

02

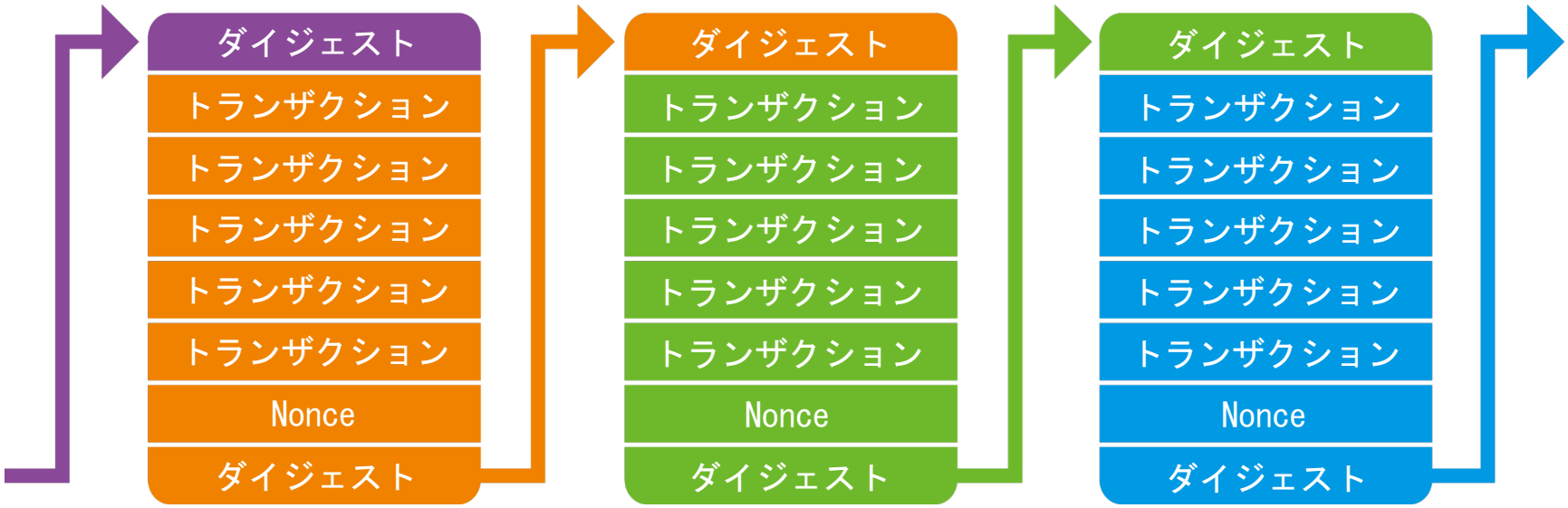
# ビットコインの概要

# ビットコインの概要

| | |
|---|---|
| **発行される総量** | 約2100万BTCと決まっている |
| **マイニング** | 約10分に1回、取引情報がブロックにまとめられる |
| **報酬** | マイニングに成功すると12.5BTCもらえる<br>各取引から手数料も徴収する |
| **取引の確定** | ブロックに「確実に」組み込まれた取引のみ「確定した」とみなせる |

# ビットコインとブロック

- 取引情報はトランザクションと呼ばれる
- ブロックを作るノードをマイナーという



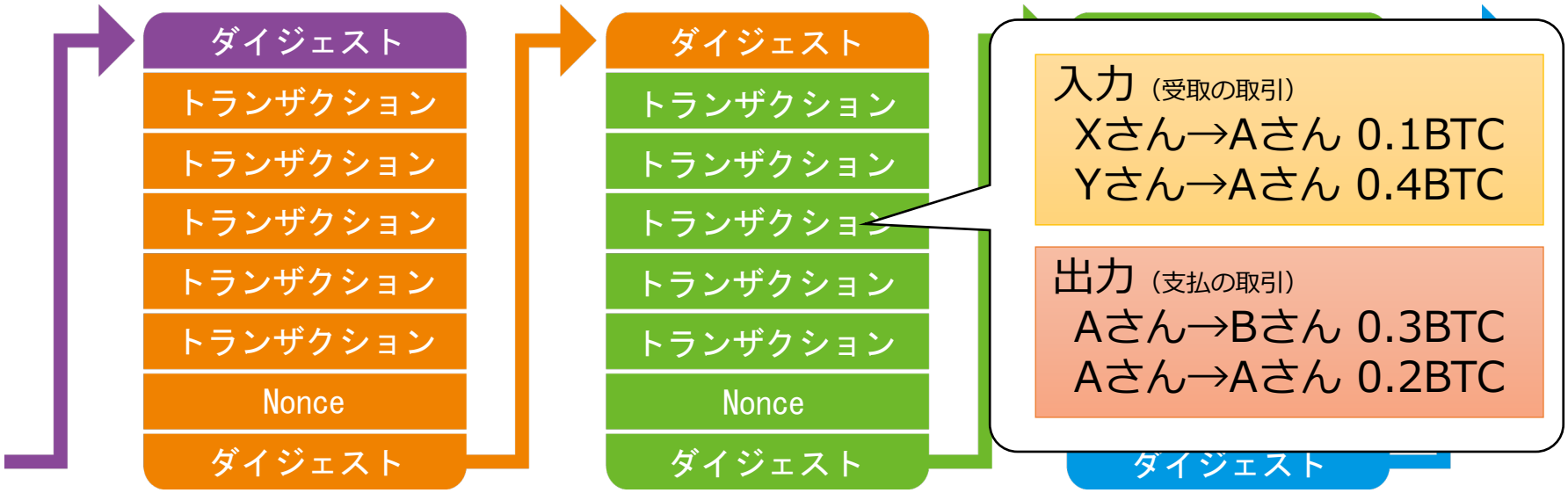

マイナーがトランザクションを束ねてブロックにする



zettant

# ビットコインとブロック

- 取引情報はトランザクションと呼ばれる
- ブロックを作るノードをマイナーという




マイナーがトランザクションを束ねてブロックにする

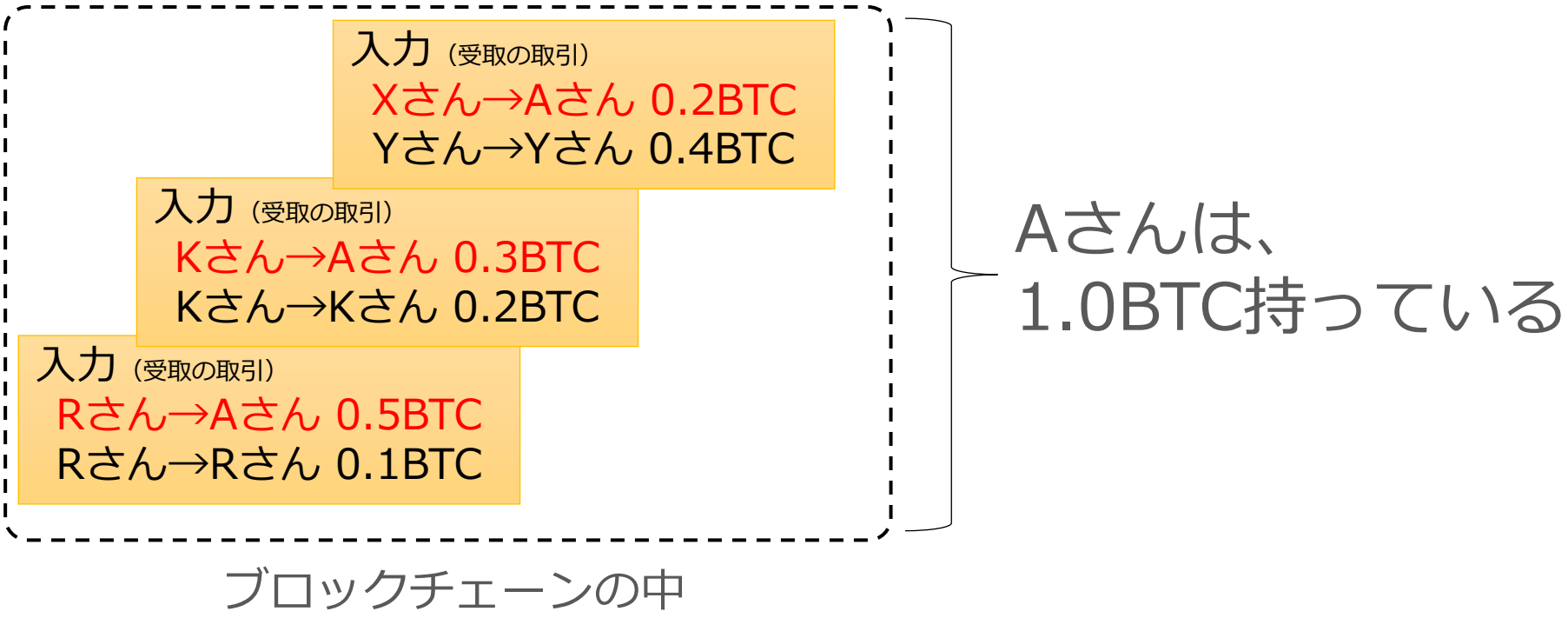


zettant

Aさんが0.9BTCをBさんに払う

# ビットコインの受取と支払

**支払いをするときは、ブロックチェーンの中から**
**受け取りの取引情報を必要な金額分かき集める**

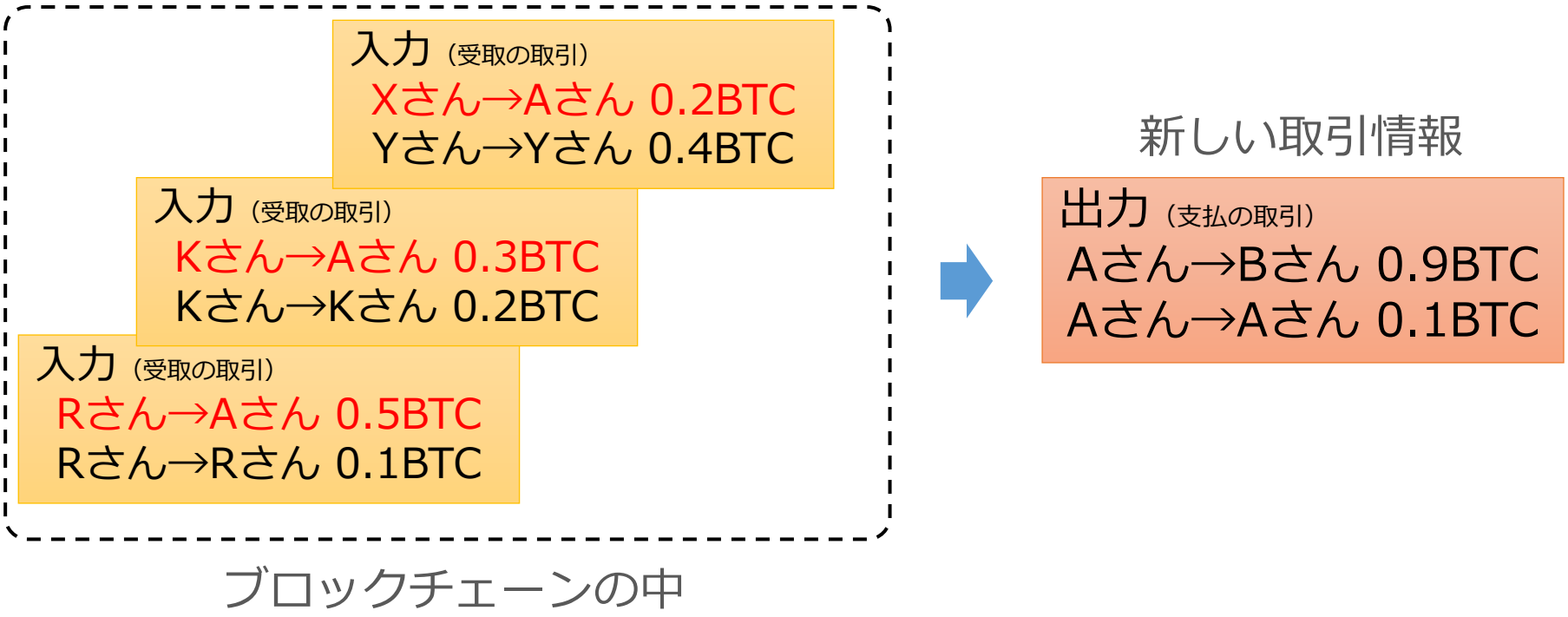





zettant

# ビットコインの受取と支払

**支払いをするときは、ブロックチェーンの中から**
**受け取りの取引情報を必要な金額分かき集める**






zettant

# ビットコインの受取と支払

「入力→出力」という取引情報を新たに生成し、ブロックに書き込む

入力（受取の取引）
Xさん→Aさん 0.2BTC
Yさん→Yさん 0.4BTC

入力（受取の取引）
Kさん→Aさん 0.3BTC
Kさん→Kさん 0.2BTC

入力（受取の取引）
Rさん→Aさん 0.5BTC
Rさん→Rさん 0.1BTC

新しい取引情報

出力（支払の取引）
Aさん→Bさん 0.9BTC
Aさん→Aさん 0.1BTC

# ２重消費を防ぐには

**受取**に関する取引情報

**支払**に関する取引情報

同じ情報はそれぞれ一回しか認めない

NG 同じBTCを2回受け取る
同じBTCを2回支払う

- 上記ルールを満たさない取引のトランザクションはブロックに組み込まない
- ブロックに組み込まれないと支払いに使えない



zettant

# マイナーの役割

**ブロック作成**

トランザクションを束にしてブロックにする

**ブロック伝搬**

ブロックを他のノードに転送し、全員で共有する

**ブロック検証**

署名の正しさや2重消費の有無をチェックする

**マイナー＝ビットコインシステムの運営者**

# マイナーへのインセンティブ

## マイニング報酬

マイニング（Nonceの発見）に１番乗りすると、12.5BTCがもらえる

約2500万円!! (12/27現在)

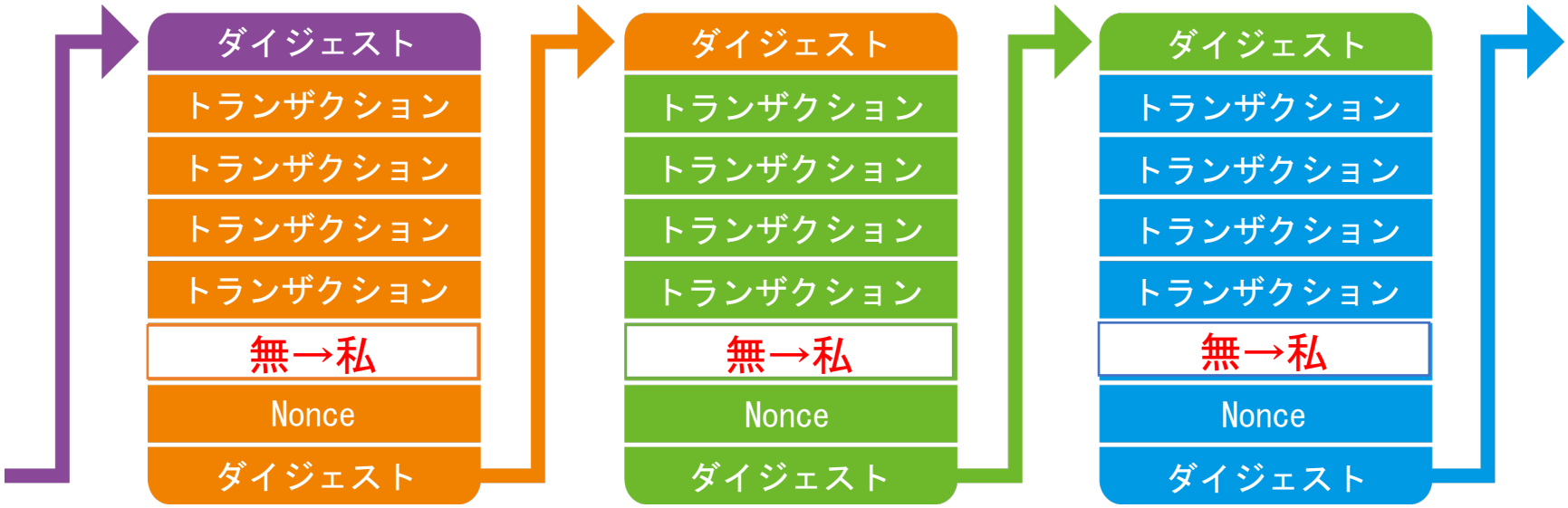
## 取引手数料

各トランザクションから少額の手数料を徴収する

**これらの報酬を目当てに、マイナーは電気代、設備代を費やしてマイニングを行う**

# マイニング報酬

マイナーは、「無→私」というトランザクションを含めることができる



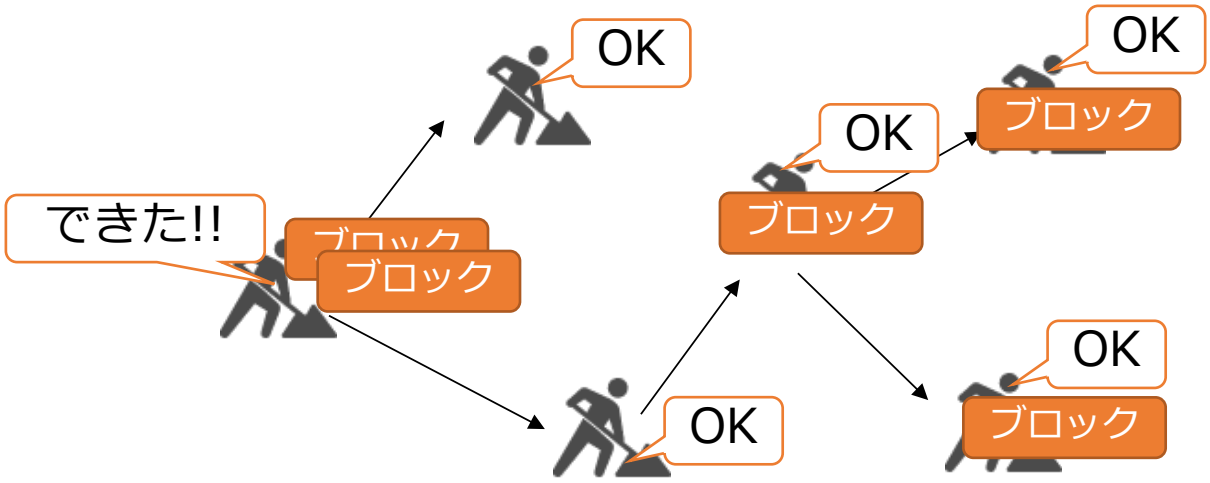

何もないところから価値が生み出される



zettant

# マイニングは早い者勝ち

**ブロックには番号がついていて、各番号のブロックを作れるのは、ただ一人のマイナーのみ！**




早い者勝ちなので、皆一番乗りを狙う。
負けたらすぐに次のブロックを作り始める。



zettant

# なぜブロックなのか

## 見るべき対象を1つに

取引情報を１つのブロックチェーンに集結することで、それを見れば誰でも**必ず確認できる**

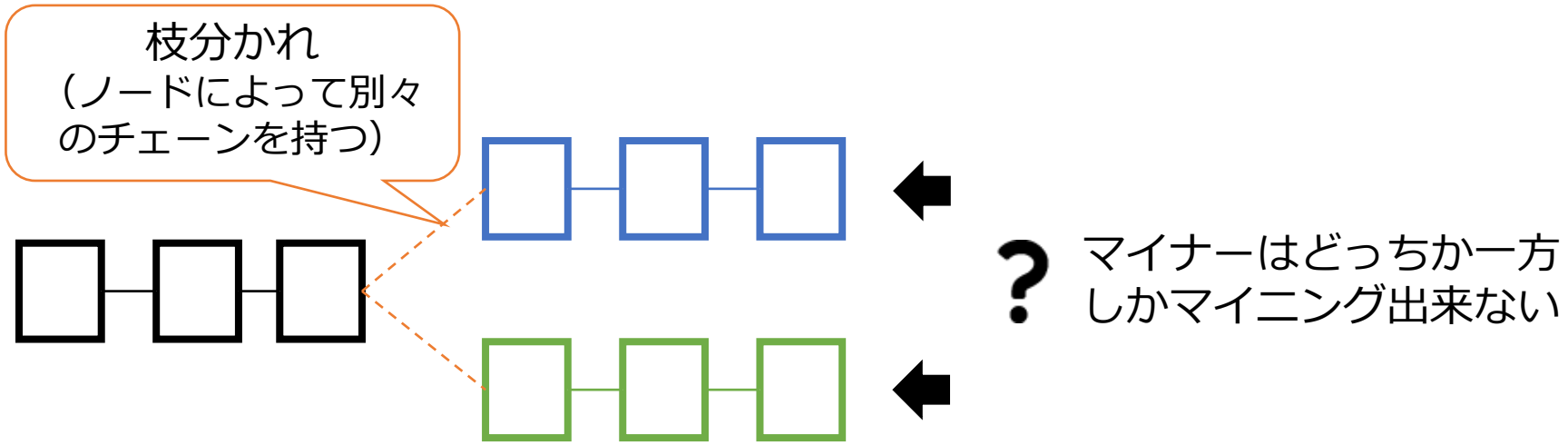
## 参加者に競争させる

勝ち負けが明確になる「レース」を作り出し、勝者にBTCを与えるという**明確なインセンティブ**を実現する

**2つを一挙に解決する仕組みになっている！**

# フォーク

## 複数のチェーンが存在する状態




最近話題になっているフォークとは、

- ソフトウェアの仕様変更によって
- 互換性のない全然別のブロックチェーンが出来上がる



zettant

# ソフトウェアアップデート

不具合修正や機能向上させたくても・・・・

**大多数の合意**　　**新バージョンの適用**

すべてのノードが**同じブロックチェーン**を
維持管理しないといけないから

でも・・・

人によっては、好ましくない機能の場合もある

お金が絡むとなおさら



zettant

# ソフトウェアアップデート

異なる機能をもつソフトウェアを動かす
グループが現れると

異なる複数のチェーンにフォークしてしまう

Bitcoin / BitcoinCash / BitcoinGold / etc...

03

# イーサリアムの概要

# スマートコントラクト

**デジタルに表現される資産を予め定められた**
**ルールに従って自動的に移転させる仕組み**

プログラムのこと

契約のこと

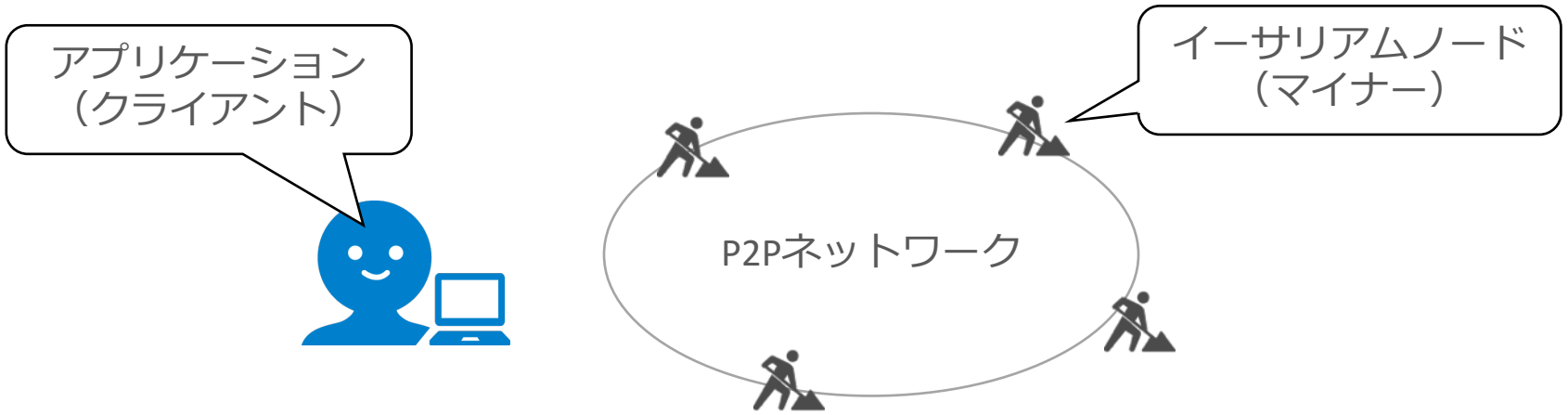
端的にいいえば

**契約プログラムを自動実行すること**

ブロックチェーンの技術として語られることが多いが
本質的にはブロックチェーンとは関係ない

# イーサリアム（Ethereum）

「結果を偽れない分散コンピューターを作る」という思想

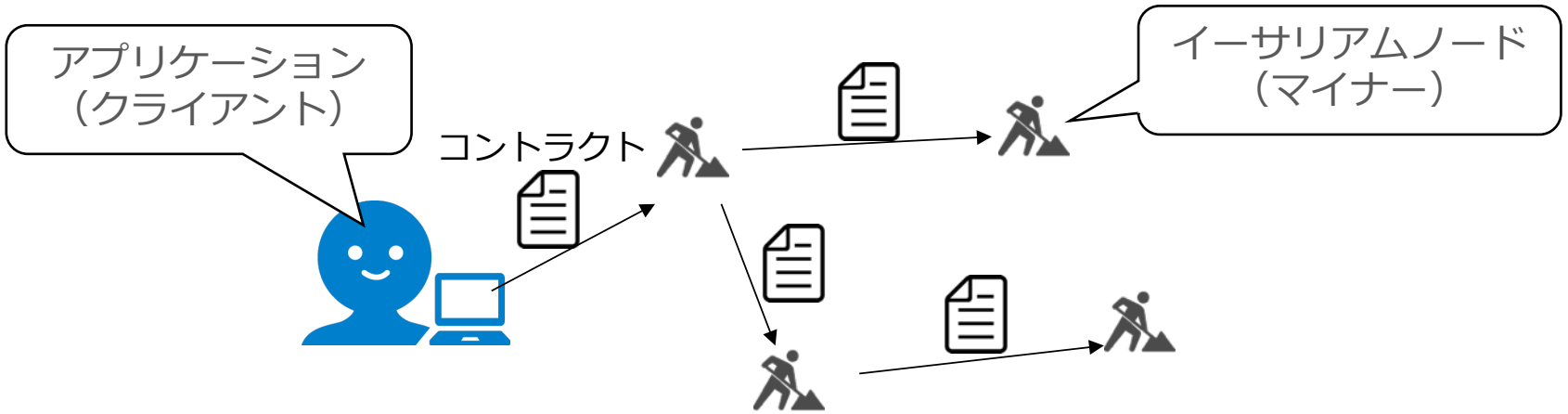





zettant

# イーサリアム（Ethereum）

「結果を偽れない分散コンピューターを作る」という思想



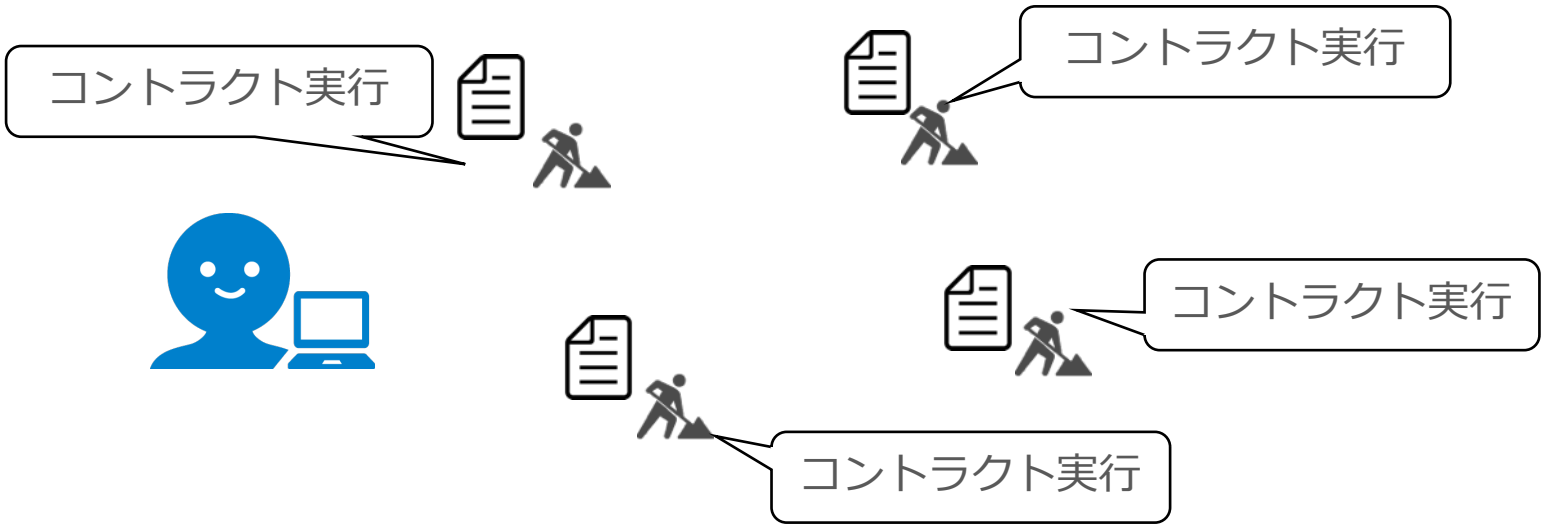

コントラクトは計算ルールとデータを記述したもの



zettant

# イーサリアム（Ethereum）

## 「結果を偽れない分散コンピューターを作る」という思想




全てのノードが同じコントラクトを実行する。

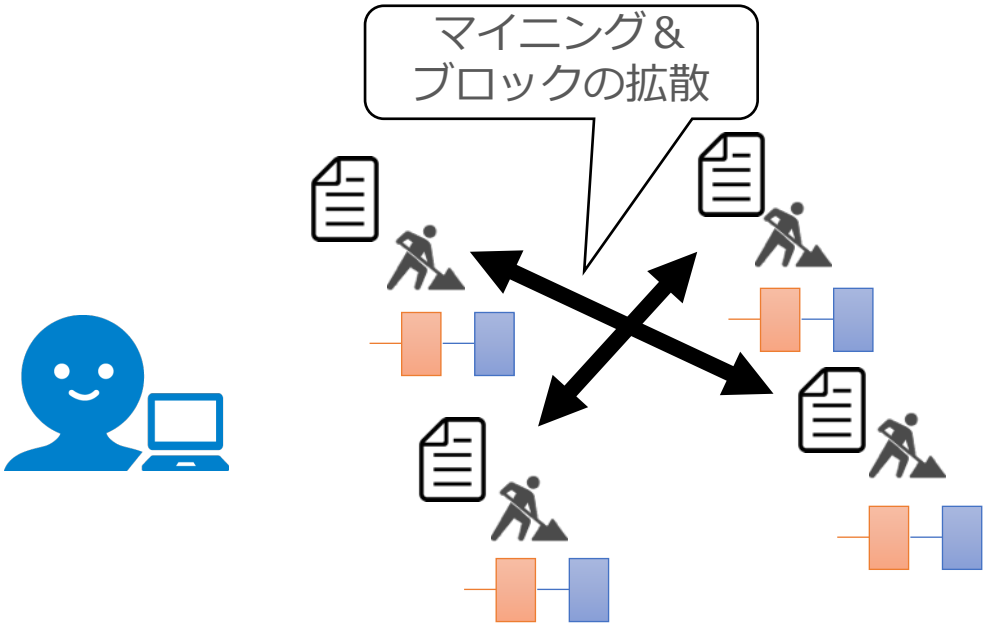
正しい計算を行わないと、あとでマイニングした時に損をする。



zettant

# イーサリアム（Ethereum）

**「結果を偽れない分散コンピューターを作る」という思想**



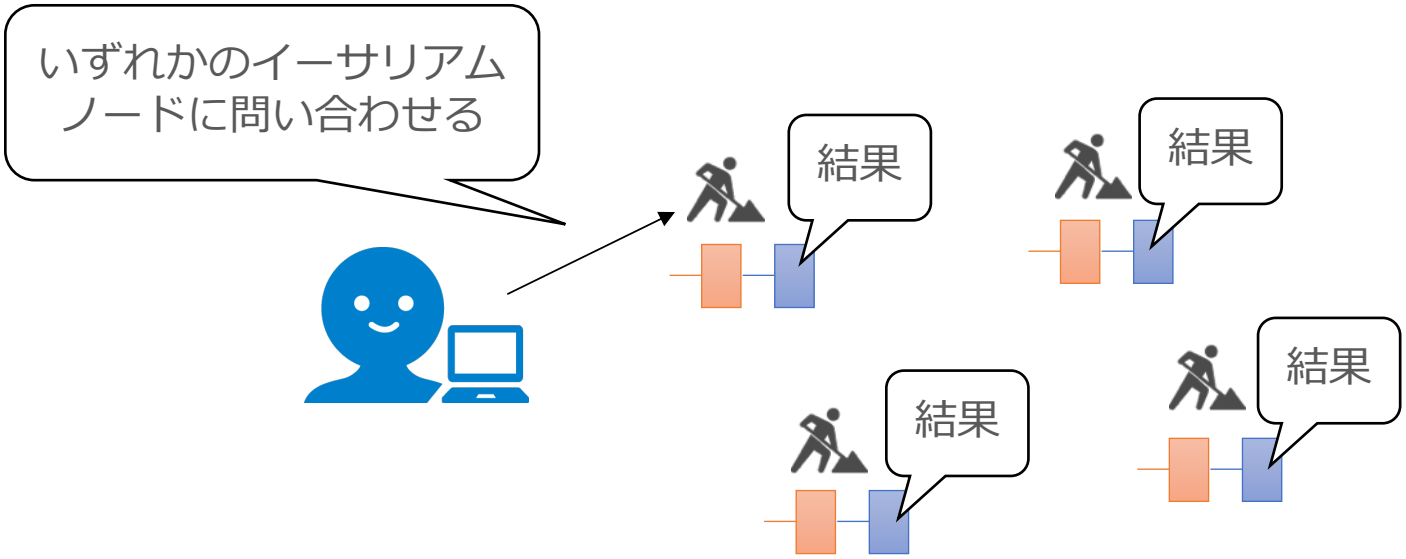

結果をブロックに書き込み、ビットコインと同様にマイニングを行い、１番乗りを目指す



zettant

# イーサリアム（Ethereum）

「結果を偽れない分散コンピューターを作る」という思想



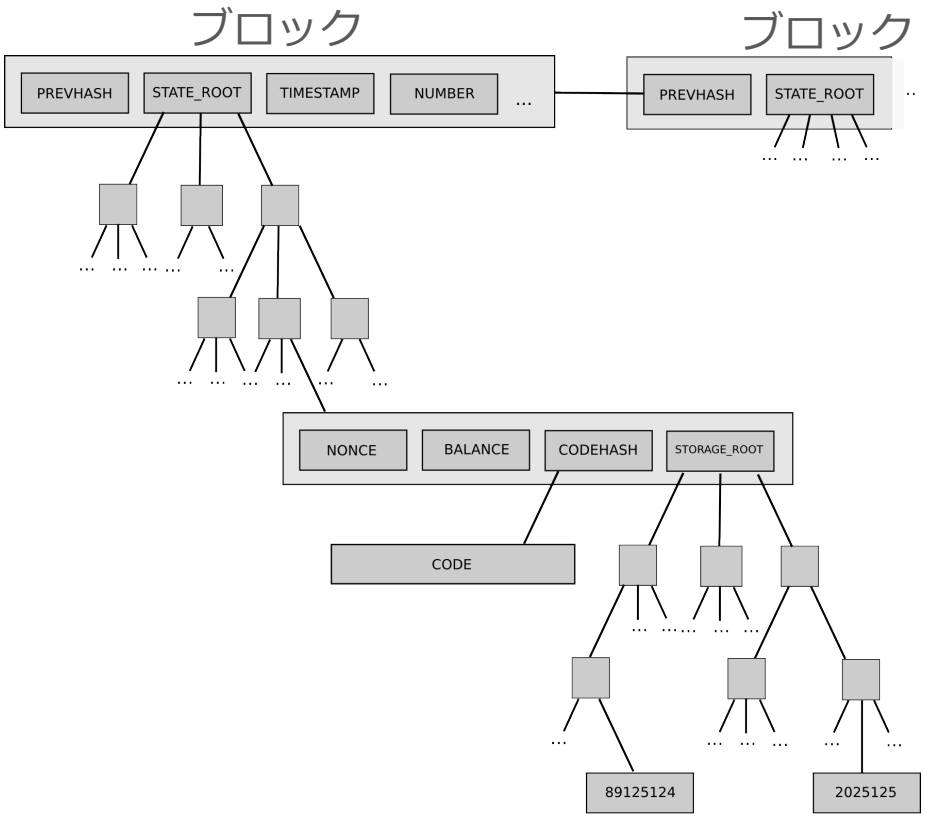

ブロックチェーンを見れば結果がわかる



zettant

# イーサリアムのブロックチェーン

## ブロックチェーンには、コントラクトの計算結果やパラメータなどが格納される




各ブロックは、パトリシア木というデータ構造をもち、それぞれの要素が１つのアカウント（コントラクトなど）を表す

[出展]
https://github.com/ethereum/wiki/blob/master/%5BJapanese%5D--Ethereum-Development-Tutorial.md



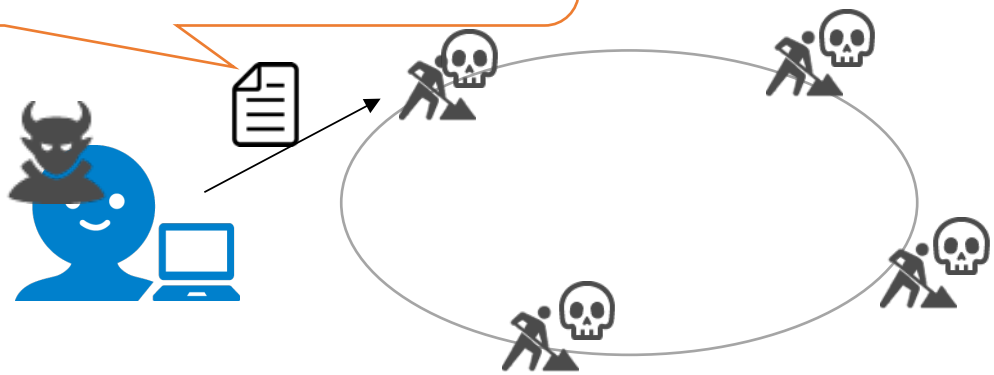
zettant

# 無限ループとか

## もし、こんなコントラクトを投入されたらどうなる？

コントラクト

次の計算を無限に繰り返せ
→ 1+1=?



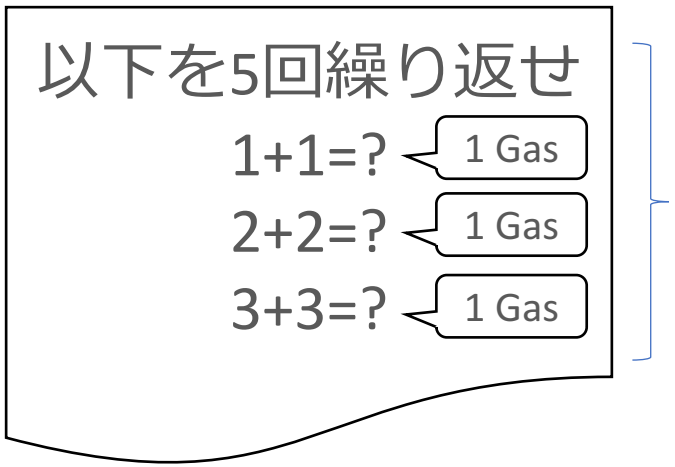
計算が終わらず、他のコントラクトが全く
実行できなくなり、システムが停止する



zettant

# Gas

## 命令を1つ実行するたびにGasという手数料が必要




3 Gas x 5 = 15 Gas 必要

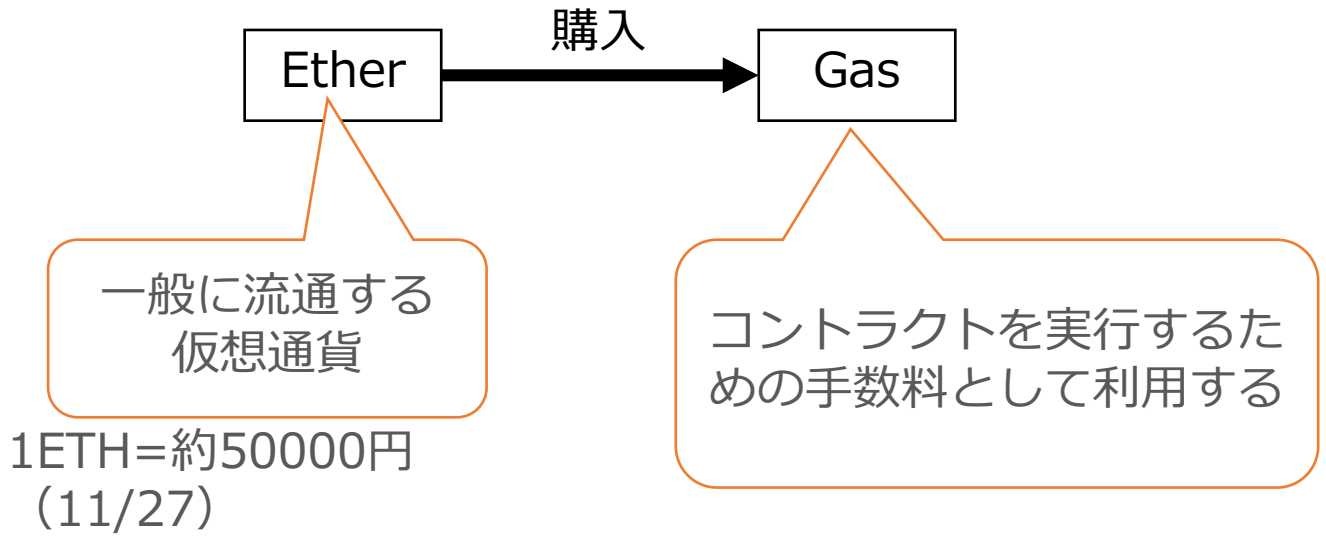
Gasはマイナーへの手数料になる。
手数料が足りなければ実行してもらえなくなる。



zettant

# EtherとGas

**コントラクト（＝プログラム）を、他人に実行してもらうには、相応の対価が必要**




Etherはマイニングまたは法定通貨と交換することで手に入れられる



zettant

04

# ブロックチェーンの課題

# ブロックチェーン技術の課題

| | |
|---|---|
| **処理速度** | 単位時間あたりに処理できるトランザクション数 |
| **ファイナリティ** | 合意（トランザクションの確定）に至るまでの過程（時間、確率） |
| **秘匿性** | 情報を全体で共有することによる秘匿性の毀損 |
| **インセンティブ** | システム運営のインセンティブとシステム利用対価のミスマッチ |
| **ガバナンス** | システムアップデートのポリシー策定や実施の困難さ |

# ブロックチェーンシステムの種類

## パブリック型

インターネット上に広く構築され、不特定多数が自由に参加/離脱可能なシステム

ビットコイン、Ethereum、NEM・・・

## プライベート型

企業・コンソーシアム内など特定の参加者によって運営されるシステム

Hyperledger、Corda、Ripple・・・

**ユースケースが異なるため取り組むべき課題も異なる**

# ブロックチェーンのメリット？

こんなことをよく耳にする

- **安全**
- **信頼性が高い**
- **スマートコントラクトが世の中を変える**
- **安い**

これらの文言には
注意が必要

**本当に「ブロックチェーンならでは」なのか？**

# ブロックチェーンのメリット？

こんなことをよく耳にする

- **安全**
- **信頼性が高い**
- **スマートコントラクトが世の中を変える**
- **安い**

ブロックチェーンを使わなくてもほとんどのことが実現可能

なぜか？？

**ブロックチェーンシステムは、その殆どが既存のデータベース技術などの組み合わせだから**



zettant

# ブロックチェーンのメリット？

こんなことをよく耳にする

- 安全
- 信頼性が高い
- スマートコントラクトが世の中を変える
- 安い

みなさん
気になりますよね？

これはこれで結構
価値はありますが

- 新規企業の参入機会になっているから
- システムの組み直しで簡素化できるから

# では、ブロックチェーンに意味はないのか？

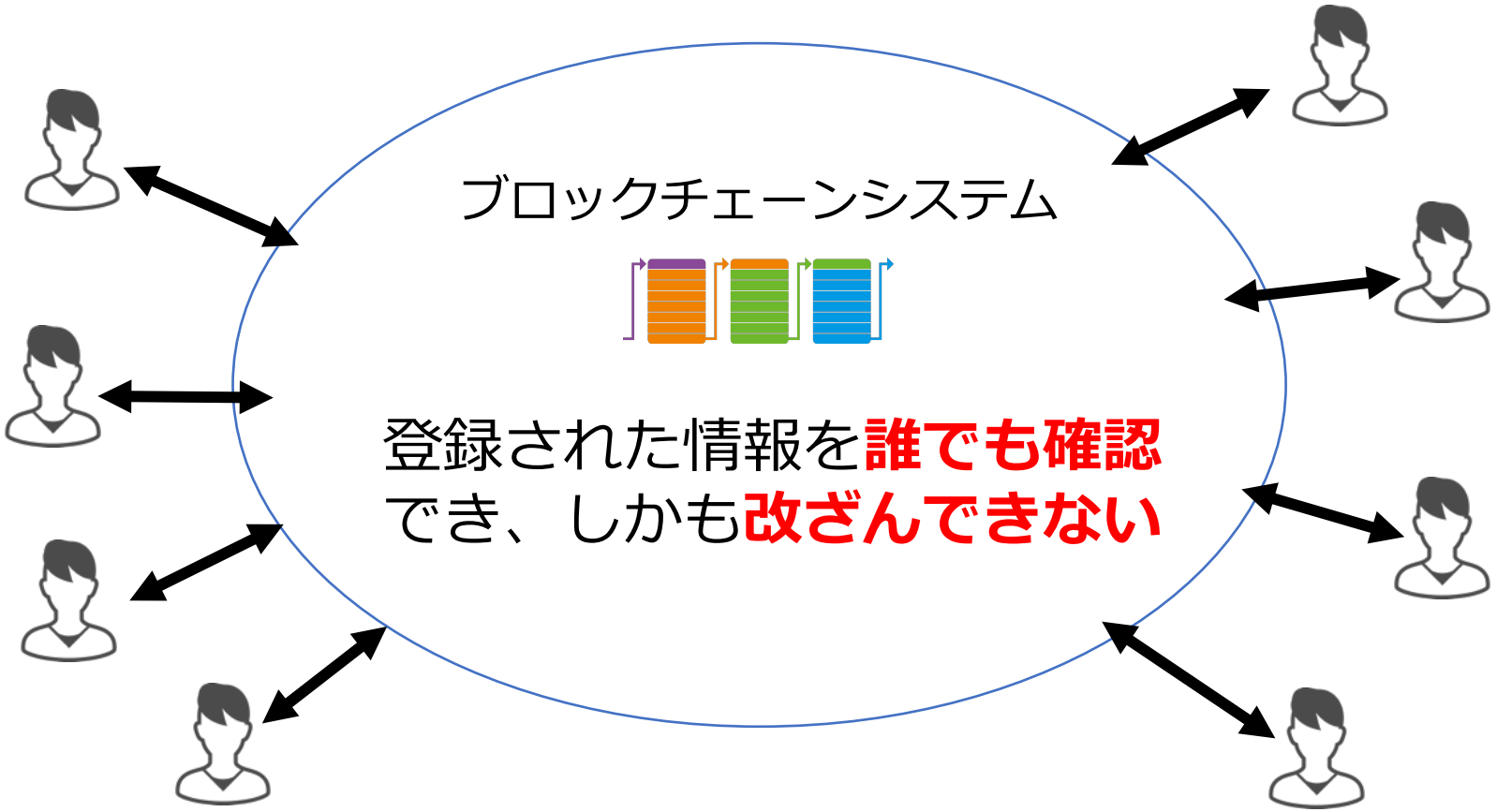
# 否

# ブロックチェーンの最大の発明

- **複数のステークホルダ**がいる中で
- **特定の誰か**を信頼の基点にすること無く
- 価値の**保存や移転**を可能にした

この要件を満たす仕組みは、現在のところ
ブロックチェーンしか存在しない！！

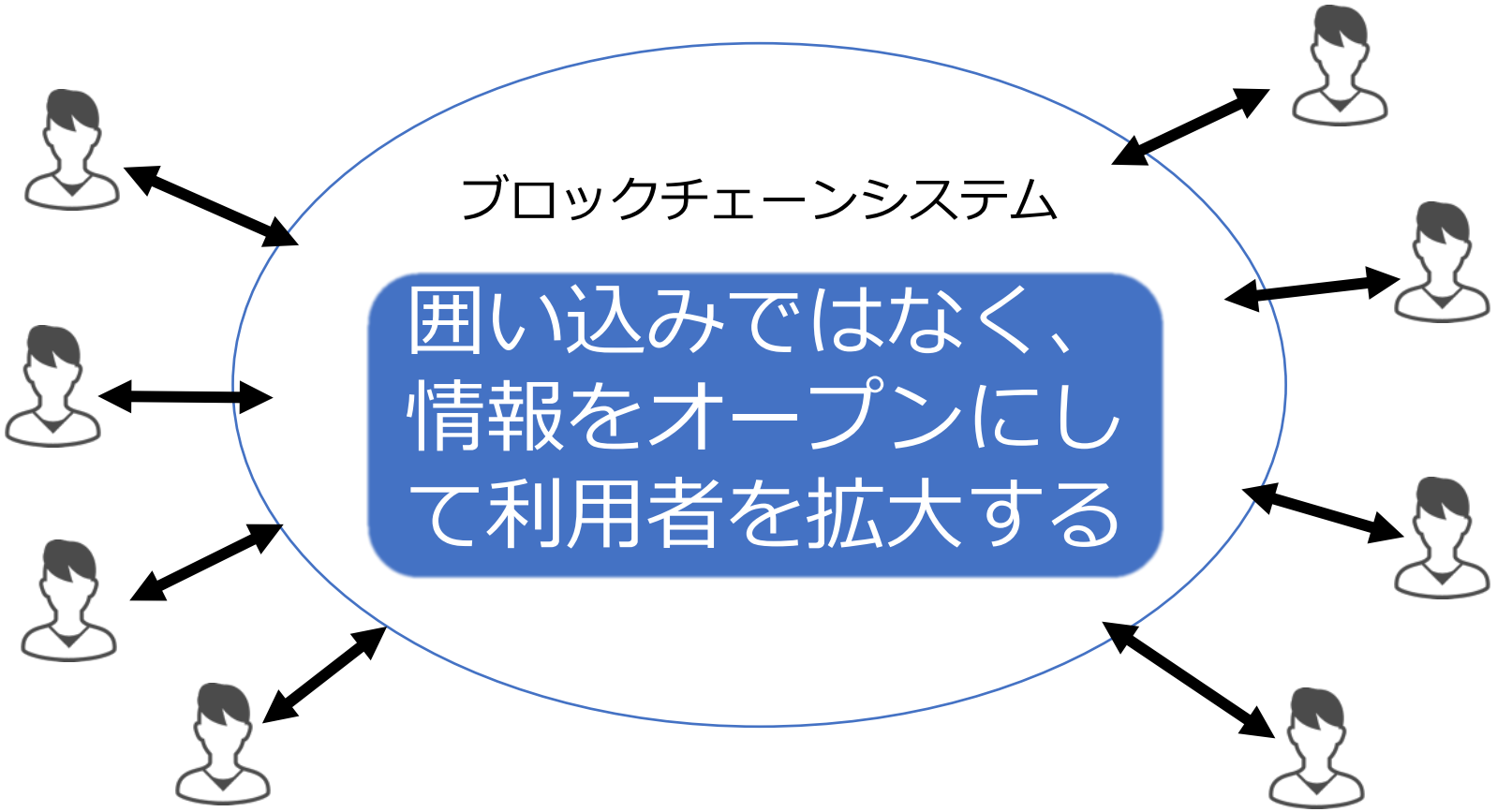
# ブロックチェーンが実現する世界






zettant

# ブロックチェーンが実現する世界






Azettant

# 向いているサービス

## 存在・来歴証明

あるデジタル情報が本当に存在していること、誰の手にあるのかを証明する必要があるもの

## 価値移転

デジタル情報の所有権を移転する

ビットコインもその一例

**いずれにしても、透明性が本質的に求められるようなサービスに向いている**

05

# まとめ

# 使いどころ

ブロックチェーンは「信用に関する問題」を
解決する唯一の技術

- **複数のステークホルダ**がいる中で
- **特定の誰か**を信頼の基点にすること無く
- 価値の**保存や移転**を可能にしたい

まだ発展途上で、ここまでに挙げた課題を
解決すべく、様々な研究開発が進んでいる

# もう少し具体的に言うと・・・

## 信頼の分散

とにかく透明性を上げるられる（みんなを信頼するし、信頼しない）

## リスクの分散

単一故障点を無くすことができる

## コストの分散

誰か一人が大きなコストを負担してシステムを作らなくて良い

**こんなメリットを享受したいときに使えます**

# Beyond-Blockchain

## 新しいブロックチェーンプラットフォーム
## Beyond Blockchain One（BBc-1）

- 10/31にオープンソースとしてgithubに一般公開
- シンプルな仕組みでブロックチェーンの課題を解決する

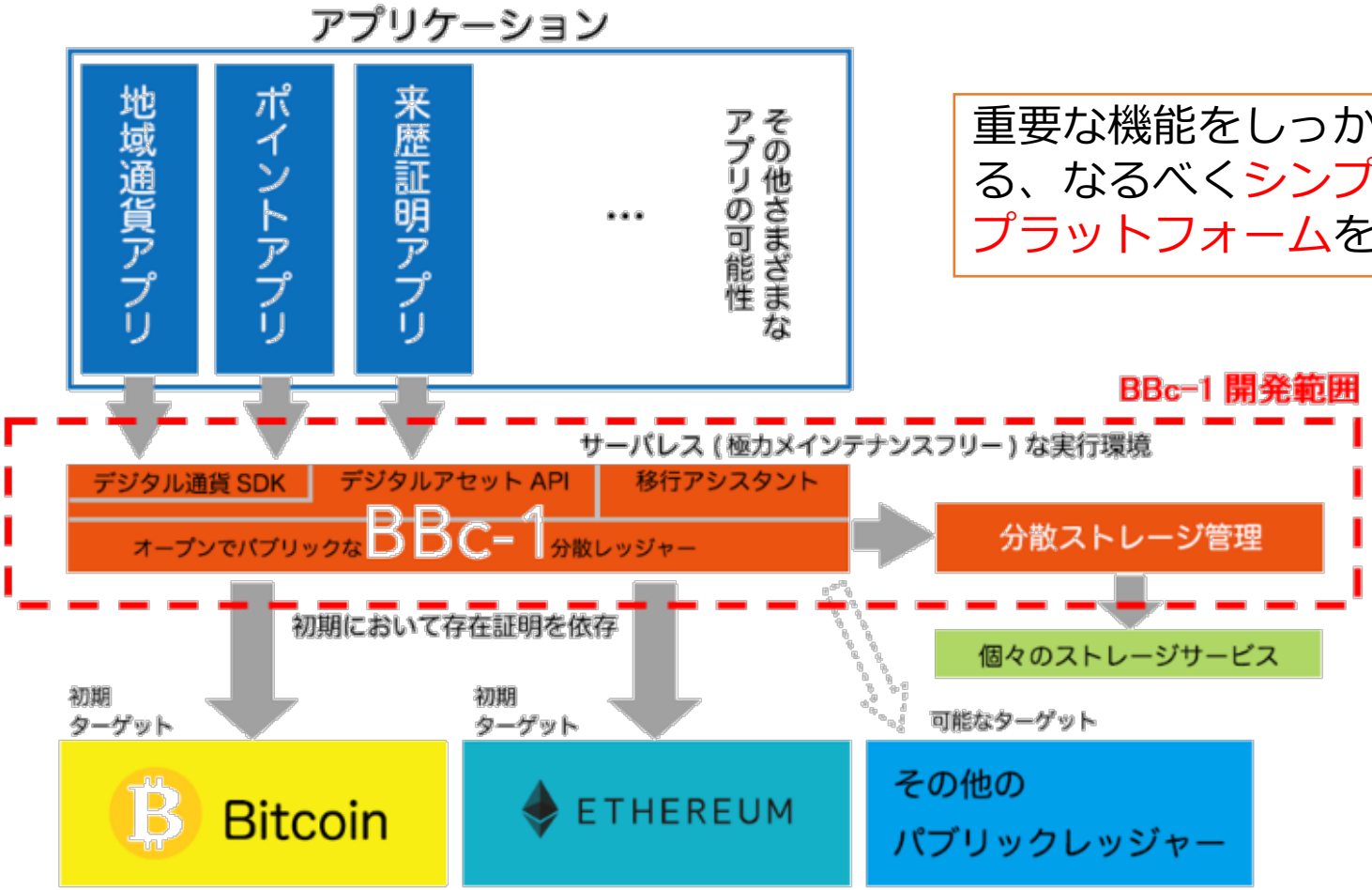
## 一般社団法人ビヨンドブロックチェーン

- より多くの人に利用してもらい、より良いプラットフォームに発展させるために設立
- 企業/個人会員を募集しておりますのご検討ください！



zettant

# BBc-1のアーキテクチャ




重要な機能をしっかり提供できる、なるべくシンプル・軽量なプラットフォームを目指します

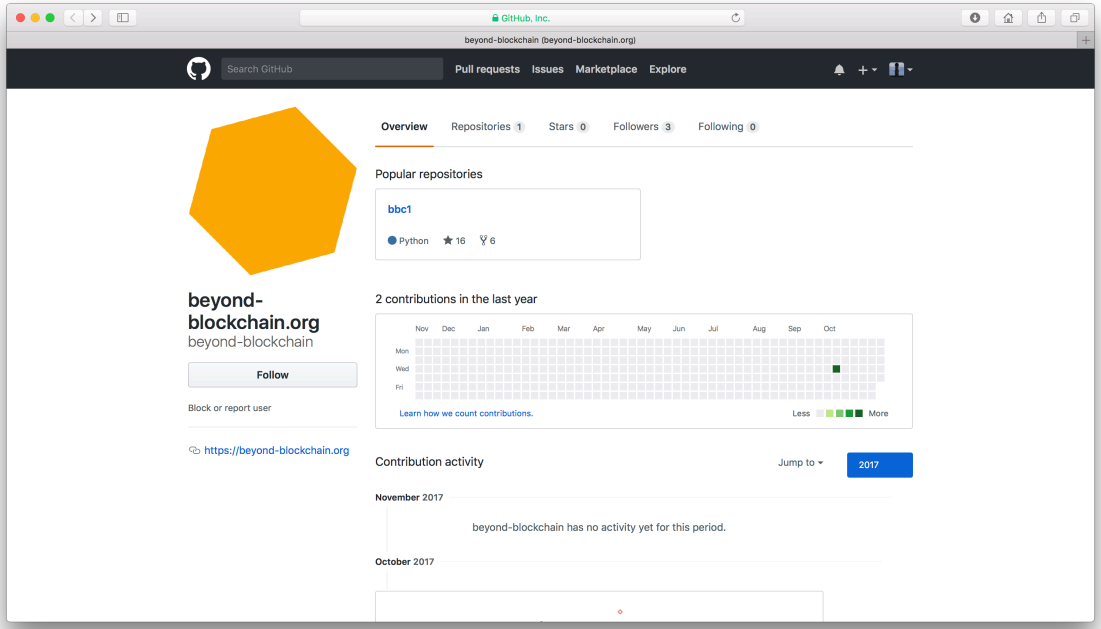
https://beyond-blockchain.org



zettant

# GitHubに公開しています

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




BBc-1のリファレンスモデルとして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。プルリク大歓迎です！



zettant

# ご清聴ありがとうございました



zettant