
ソラミツ株式会社

武宮誠

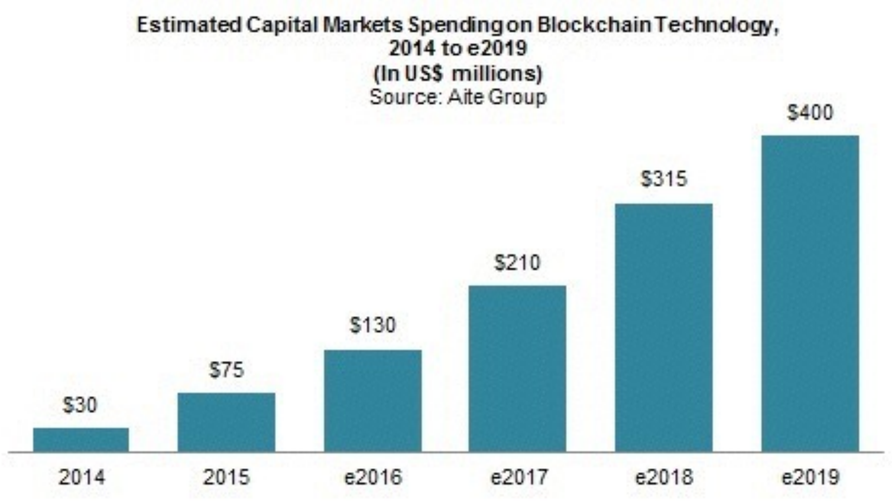
takemiya@soramitsu.co.jp


平成28年4月26日

# ブロックチェーンの可能性（概要）

ビットコインが生まれた2008年から2013年までは、ビットコインしか存在しなかったため、ビットコイン関連のベンチャーに投資が行われてきたが、2013年に発表されたEthereumでは、記録対象は、取引記録だけではなく、プログラム、データも含むようになり、この他にも、様々なパブリックチェーンが開発されてきた。2014年～のブロックチェーン技術への投資額は以下のとおりであり、今後拡大していくことが見込まれています。


（ブロックチェーンへの投資額）

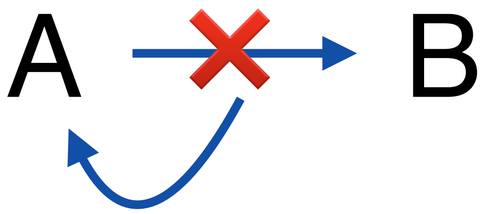


# ブロックチェーンの仕組み（概要）

ブロックチェーンは、各ブロックに1つ前のブロックのハッシュを入れて、新しいブロックを作成し、それをチェーンのようにつなげていくことで構築される。
また、ブロックの作成者はブロックの全体の内容に対して電子署名した上でネットワークに公開するため、仮に悪意あるものがブロックの内容を改竄した場合には、誰でもわかるしくみになっている。なお、1つのブロックを改竄するためには、関連するチェーン全ての改竄が必要になるため、改竄が実質的に困難なしくみで運用されている。
さらに、ブロック内の取引リスト（複数の取引を集約）が重要な情報であるが、この取引リストは、個別取引ごとに電子署名されているため、取引の発行者が誰かということが明瞭にわかる上に、ブロックと同様に個別取引及び取引リストの改竄も難しいしくみになっている。

# ブロックチェーンの仕組み（不正防止）

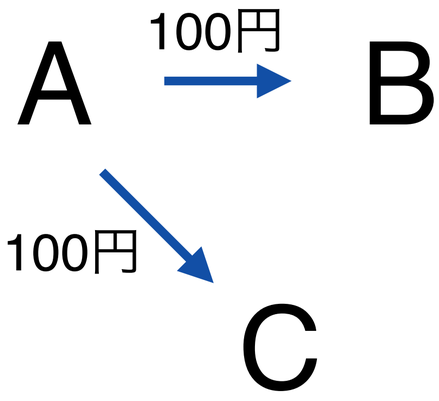
## 取引の改ざん




公開鍵技術によって、取引を電子署名するため、悪意あるものが内容を変更した場合は、不正な取引だとわかる。

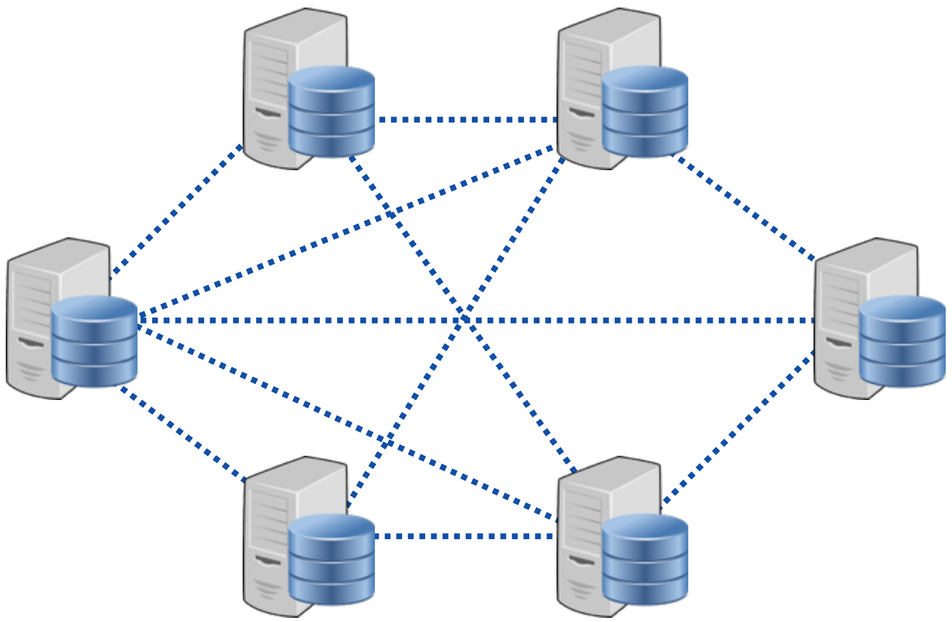
※　数式によって確認が行われるため、中央管理者は不要である。

## 二重取引（Double Spend）




ネットワークに参加するサーバーは全員同じデータをもつため、あるアカウントが保有残高以上のお金を送金しよう（二重取引）とした場合、参加者全員が二重取引していることがわかる。

# ブロックチェーンの仕組み（P2Pバイナリーデータ通信）



## システム停止防止

ブロックチェーンはP2Pネットワークを利用することで２４時間、停止することなく運用できる。仮に数台のサーバーが停止されたとしても、ネットワーク全体としては動き続ける。

## コスト削減

仮に数台のサーバーが停止されてもネットワークが総合的に運用できるため、特別仕様の信用性が高いサーバーやシステム環境でなく、安価なコンピュータハードウェアを利用することができる上に、管理者の人件費のコストも削減できる。

# ブロックチェーンの強み（1/2）

コストや開発の困難性から、実質的に不可能だったデータベースが実現できるようになった。複数の暗号技術等の組み合わせで機密性が高く、ゼロダウンタイムな環境へ。

**従来の技術**　複数の暗号技術とDBがバラバラであった

**ブロックチェーンの技術**　複数の暗号技術とDBが一体型の技術が生まれた

（新旧比較）

| | 従来の技術 | ブロックチェーン技術 |
|---|---|---|
| 公開鍵暗号方式 | 個別に組込開発 | ★一体型 |
| 電子署名 | 個別に組込開発 | |
| P2Pネットワーク | 個別に組込開発 | |
| データベース（DB） | 個別に組込開発 | |

# ブロックチェーンの強み（2/2）

ブロックチェーンの特徴の一つは中央管理者がいないことであるが、ノードの参加者と制限したプライベートな環境でコンプライアンスを確保することも可能である。

**パブリック** 制限なし、誰でも参加できる

**プライベート・パーミッション** 制限あり、選んだサーバーだけが参加可能もしくAPIをアクセスできる

セキュリティー・コンプライアンス・プライバシーを確保するため、プライベートブロックチェーンが企業に適している

# デジタルアセット管理システム（公開鍵暗号方式）

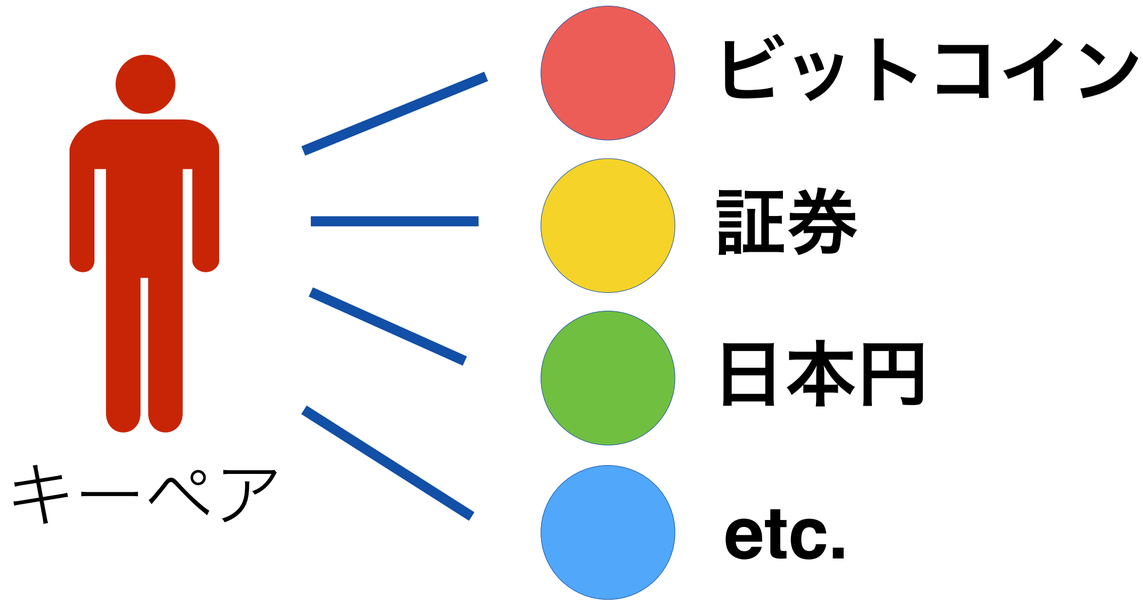
ブロックチェーン上では、すべての口座は公開鍵キーペア（楕円曲線暗号）で定義され、保有している通貨・デジタルアセットはキーペアに帰属する仕組みとなっている。

## 公開鍵の例

71fc5b675058d55fd81eb6fe91f6e3bc321bab75272041 6fb38aa7a0d1d0515a

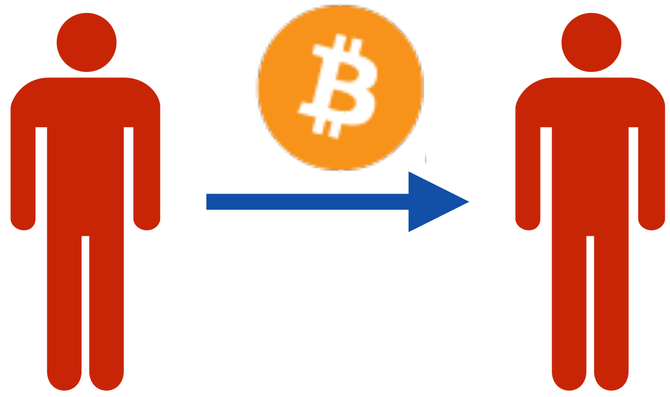
## 秘密鍵の例

00b3b8cf802ea687ee1e0f249e442ae82ee02b8b82e4cb3900092601603c658351

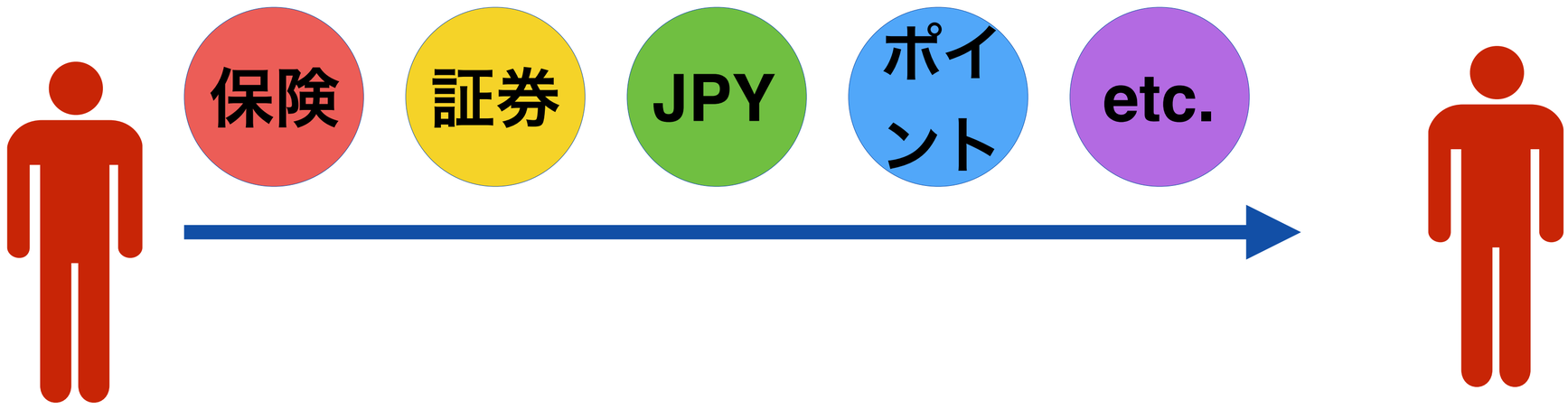


# デジタルアセット管理システム（フレキシブル化）

**２００９年：**従来のブロックチェーンでは一つの通貨（ビットコイン）のみが流通し、他のアセットの流通はできなかった



**現在：**一つの通貨だけではなく、様々なデジタルアセットの流通が可能になった。
∴ブロックチェーンの強みは価値をデータとして取扱い、データを通信（流通）できることであるため



# デジタルアセット管理システム（プラットフォーム）

2008年にビットコインという仮想通貨が生まれた。ビットコインはあくまで”通貨”であるが、ビットコインと同じしくみで「中身」を変えることにより、証券、ポイント、ギフト券、車や家の権利、デリバティブ商品などあらゆるasset（資産）をデジタル上で管理できるようになった。

ビットコイン2.0と言われるプロジェクトで、ビットコインにいわゆるスマートプロパティやユーザー独自通貨の発行機能を実装するものとなっており、2013年ごろから、Colored Coins、counterparty 、NEMlightwalletなどのプロジェクトが始まった。

これらのプロジェクトの出現により、**企業や個人は、デジタルアセットを簡単に発行・流通・管理することが可能となっている。**




2008


2012


2014

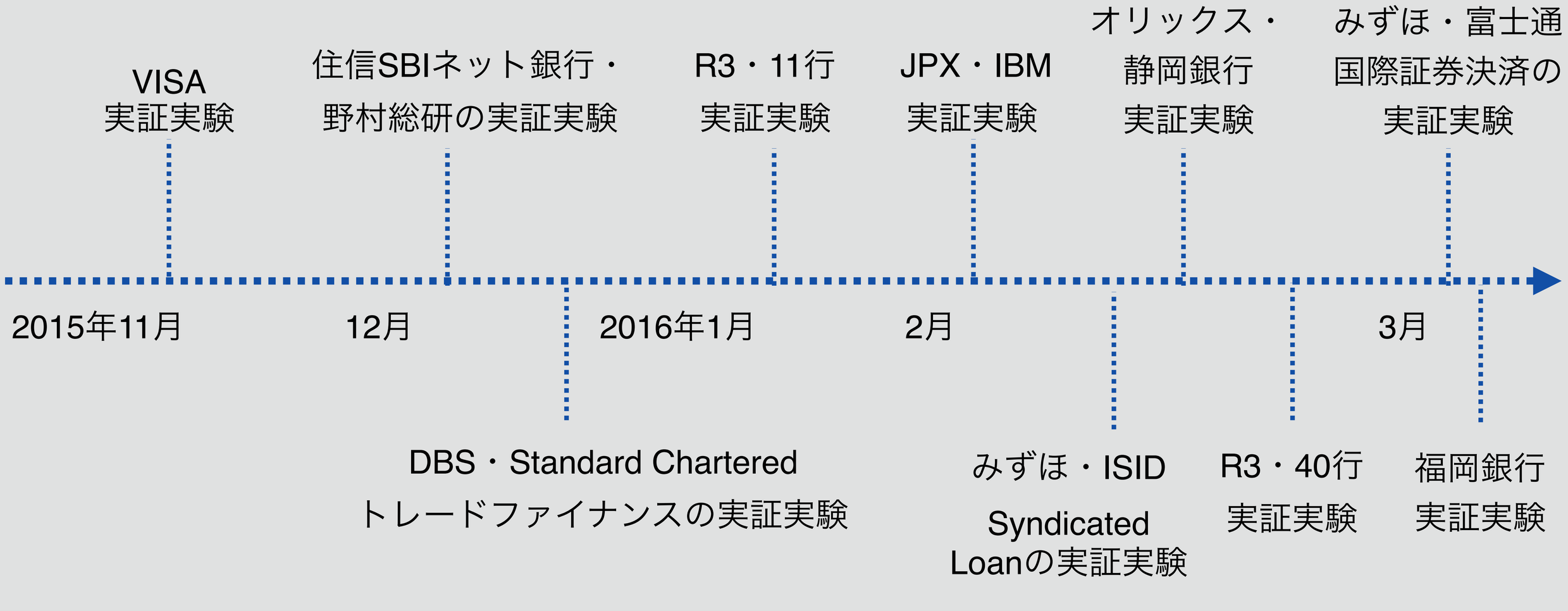

2014

| | nem<br>a new economy starts with you. | Bitcoin | Ethereum |
|---|---|---|---|
| P2P Time Service | ○ | ✕ | ✕ |
| サーバー評判 | ○ | ✕ | ✕ |
| 取引スパム フィルター | ○ | ✕ | ✕ |
| マルチシグ | ○ | △ | △ |
| デジタルアセット | ○ | △ | △ |

# ブロックチェーンの可能性（金融機関のブロックチェーン実証実験1/2）

**国内外の金融機関は、ブロックチェーン技術の活用を積極的に進めるために、ブロックチェーン技術を使ったシステム開発の実証実験を進めている。**

以下は、主に日本企業の直近の実証実験プレスリリースのタイムラインになります。



# ブロックチェーンの可能性（金融機関のブロックチェーン実証実験2/2）

**複数のブロックチェーン技術が存在しており、スタンダードが存在していない。**

| 参加者 | 分野 | ブロックチェーン | 開始時間 |
|---|---|---|---|
| **VISA** | 国際送金 | ビットコイン | ２０１５年１１月 |
| **住信SBIネット銀行・野村総研** | ブロックチェーンの一般 | NEM / MIJIN | ２０１５年１２月 |
| **DBS・Standard Chartered** | トレードファイナンス | Ripple | ２０１５年１２月 |
| **R3・11行** | ブロックチェーンの一般 | Ethereum | ２０１６年１月 |
| **JPX・IBM** | ブロックチェーンの一般 | Open Blockchain | ２０１６年２月 |
| **みずほ・電通** | Syndicated Loan | Ethereum | ２０１６年２月 |
| **R3・40行** | Commercial Paper Transactions | Ethereum, Eris, Chain, Open Blockchain | ２０１６年２月 |
| **オリックス・静岡銀行・NTTデータ・ドコモベンチャーズ** | ブロックチェーンの一般 | Orb | ２０１６年２月 |
| **みずほ・富士通** | 国際証券決済 | ビットコイン | ２０１６年３月 |
| **福岡銀行** | ポイント | ビットコイン | ２０１６年３月 |

# NEMの優位性は？

# nem とは？

- New Economy Movement （新経済運動）www.nem.io
- 次世代ブロックチェーンプラットフォーム（改良版ビットコイン）
- DAO（自律分散型組織）
- 3月31日より公開した
- 通貨の流通量は一定
- マイニングが無いことが特徴
- ブロックを作成するモチベーションは取引の際の手数料

# 非常に利便性の高い開発者向けAPIを準備

http://bob.nem.ninja/docs/
http://nem.io/ncc/index.html

```
import requests

req = requests.get('http://104.156.232.219:7890/account/get/forwarded?address=NC2ZQKEFQIL3JZEOB2OZPWXWPOR6LKYHIROCR7PK')

req.json()
```


```
{ u'account': {u'address': u'NALICE2A73DLYTP4365GNFCURAUP3XVBFO7YNYOW',
  u'balance': 15794218396666,
  u'harvestedBlocks': 1181,
  u'importance': 0.00159759393873245 64,
  u'label': None,
  u'publicKey': u'bdd8dd702acb3d88daf188be8d6d9c54b3a29a32561a068b25d2261b2b2b7f02',
  u'vestedBalance': 15792456424453},
  u'meta': {u'cosignatories': [],
  u'cosignatoryOf': [],
  u'remoteStatus': u'ACTIVE',
  u'status': u'LOCKED'} }
```

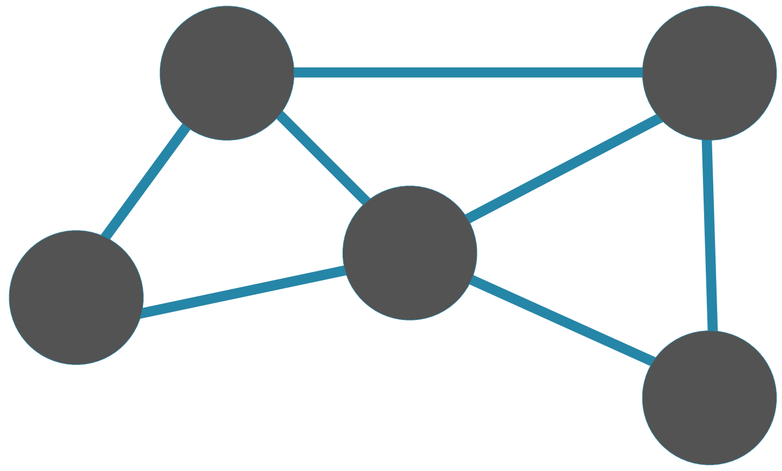
bitcoin

nem
a new economy starts with you.

coinbase

block.io

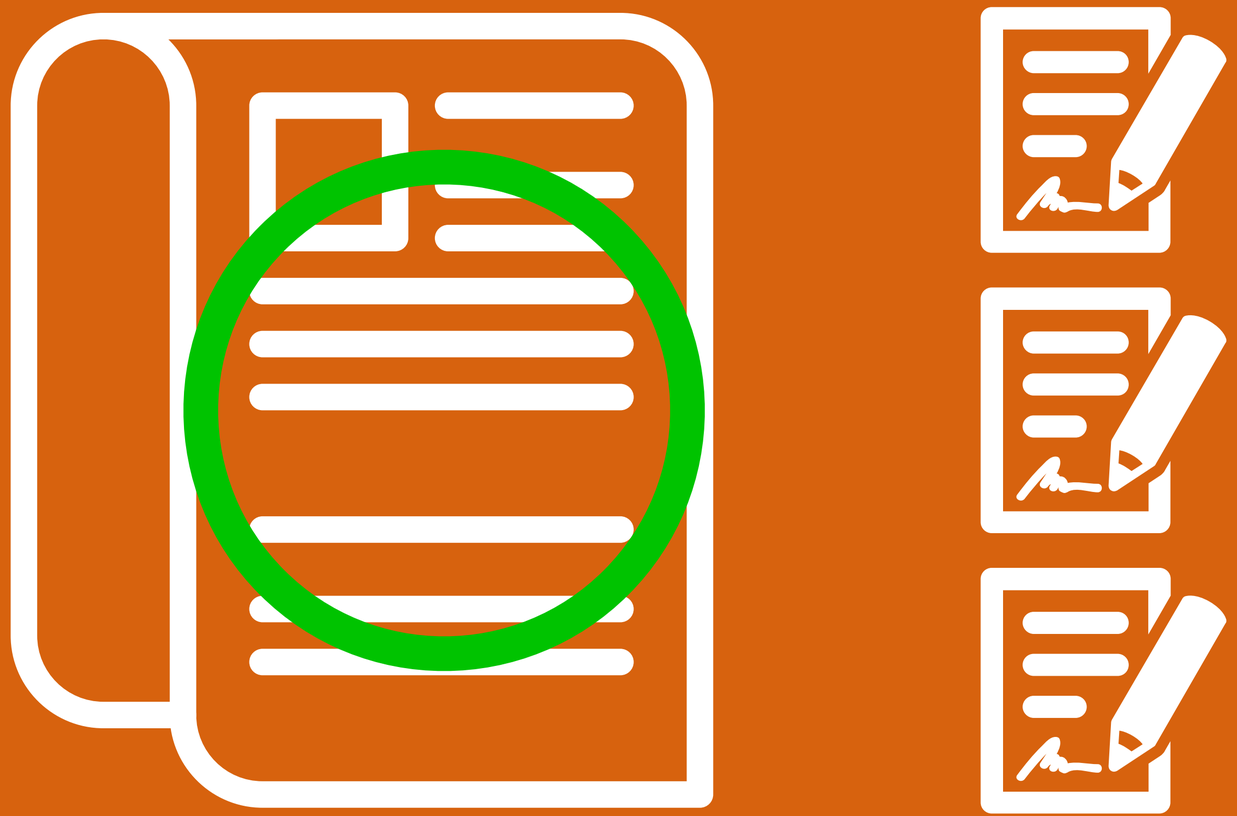
BLOCKCHAIN info



開発者向けのAPIがコアに用意しないで、中央サービスだけが一般的に利用している

各サーバーがAPIを提供して、完全に分散型でブロックチェーンの上にアプリを開発できる

nem
a new economy starts with you.



マルチシグなどの取引の安全性を保証する機能をシステムレベルでサポート

nem

a new economy starts with you.

マイニング無し

# 確率的ビザンチン合意形成 (中本合意形成)

- 中本哲史が提案した分散形合意形成アルゴリズムであり、皆で共有しているデータが正確であることを証明するもの
- それぞれのプルーフ・オブ・「何々」のアルゴリズムは中本合意形成を実現していて、参加者から次のブロックの作成者を決定するものである

# プルーフ・オブ・ワーク（PoW）

- ビットコインの代表的な「マイニング」
- アルゴリズム：
  - minerは取引集合をブロックに入れて、ブロックの全部のデータをハッシュする
  - →ハッシュは難易度より低かったら、**オッケー！**終わりとして、新しいブロックを作成する
  - →ハッシュは難易度より高かったら、**ダメ**なので、「nonce」という数字を変更する
  - **繰り返す**

## プルーフ・オブ・ワーク（PoW）

- ビットコインの代表的な「マイニング」

- アルゴリズム：
  - minerは取引集合をブロックに入れて、ブロックの全部のデータをハッシュする
  - →ハッシュは難易度より低かったら、**オッケー！**終わりとして、新しいブロックを作成する
  - →ハッシュは難易度より高かったら、**ダメ**なので、「nonce」という数字を変更する
  - **繰り返す**

**参加者の計算力を合わせて、ブロックのデータが正しいとの証明になる（ワークの証明）**

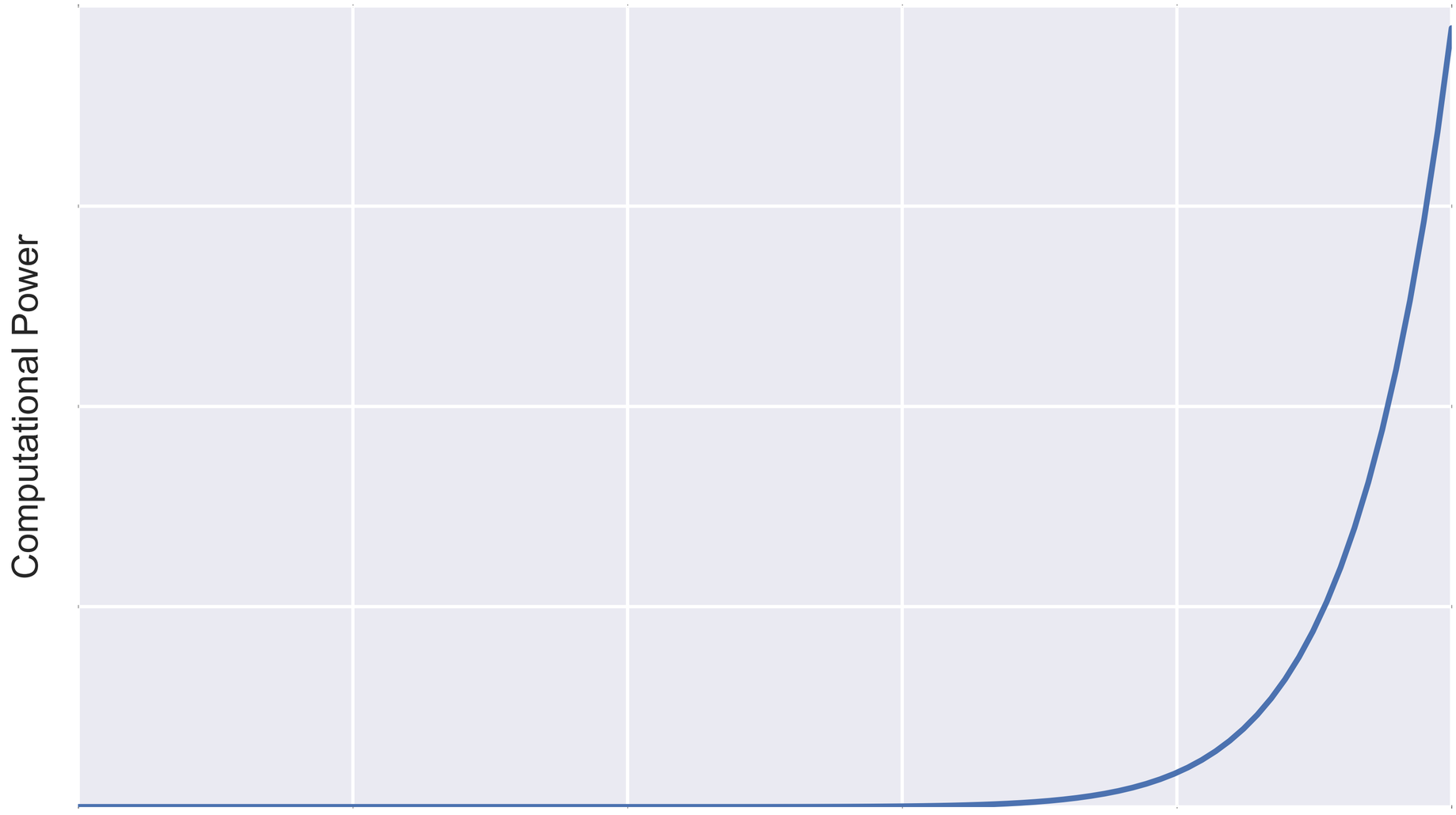
# PoWの問題点

- マイニング団体が力を持つことができれば、嘘のデータをブロックに入れることが可能、いわゆるダブル・スペンド攻撃の恐れがある
- P2Pノードを立ち上がるモチベーションがない
    - ブロック作成者だけが手数料などを得られる
- 電力が非常に無駄になる。地球の環境破壊につながる。お金もかかる（中国のあるところでは電気代が月８万米ドル！）

# PoWの一般的な働き

PoWはminerらの計算力を示す確率分布から

サンプルを取って、次のブロックの作成者を決定する



# PoWの問題の解決に向けて

計算力の確率分布からサンプルするのではなく、電力を無駄にしない分布からサンプルする

# Proof-of-Stake（取得した権利の残高の証明）

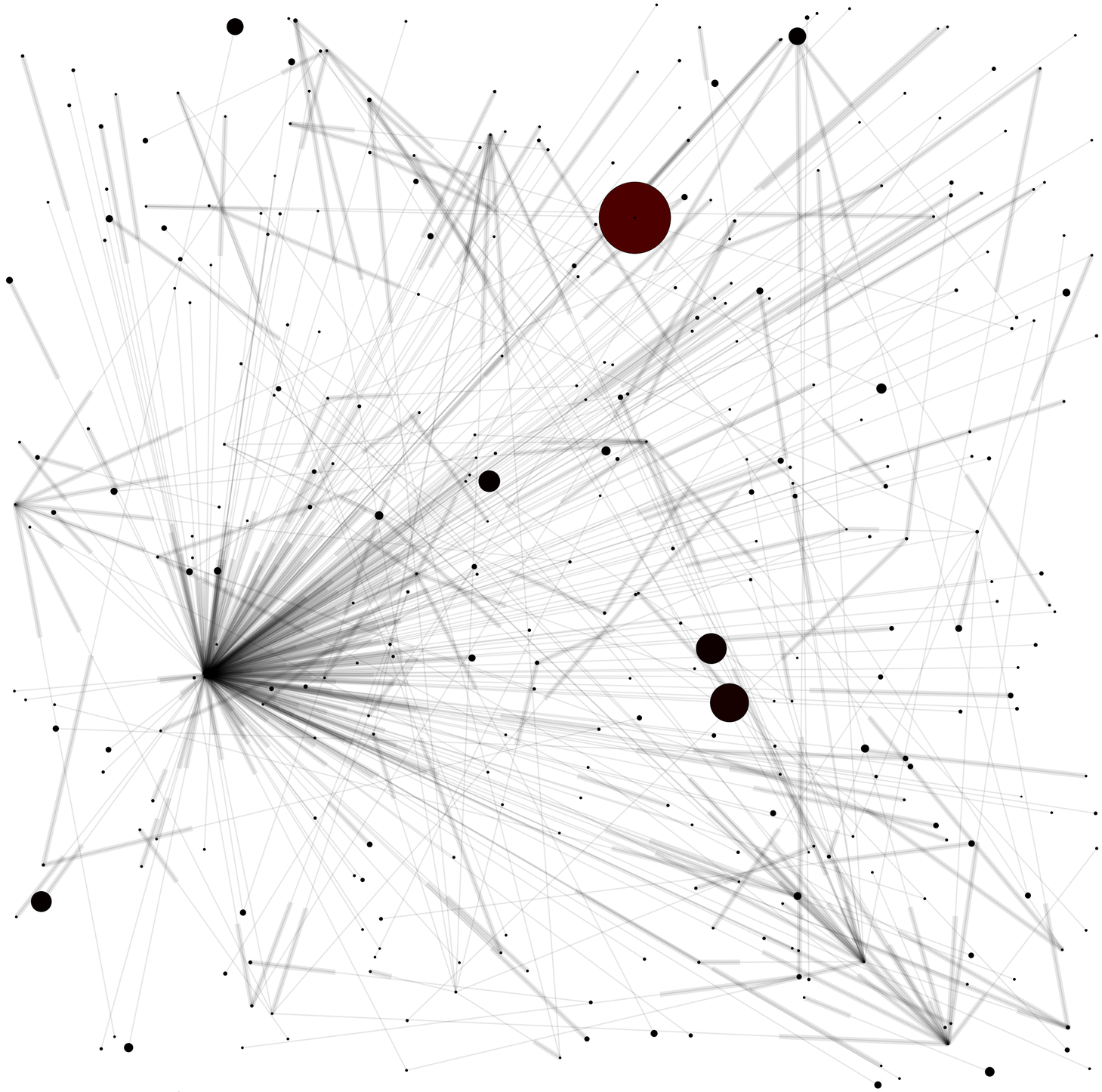
- 計算力の分布からブロックの作成者を決定せず、アカウント取得した権利の残高の分布を利用する
- これから説明するProof-of-Importanceと同様なので、ここではPoSの説明は省略する
- 問題：お金持ちがブロック作成者になると、参加資格の取得に不公平が生じる

# 重要性の証明(Proof-of-Importance; PoI)

- **NEM**が開発したアルゴリズム
- 経済に関するユーザー自身の重要性によって次のブロックを誰が収穫（作成）するのかを確率的に決める
- PoSと同じ様であるが、残高ではなく、重要性を計算に利用する

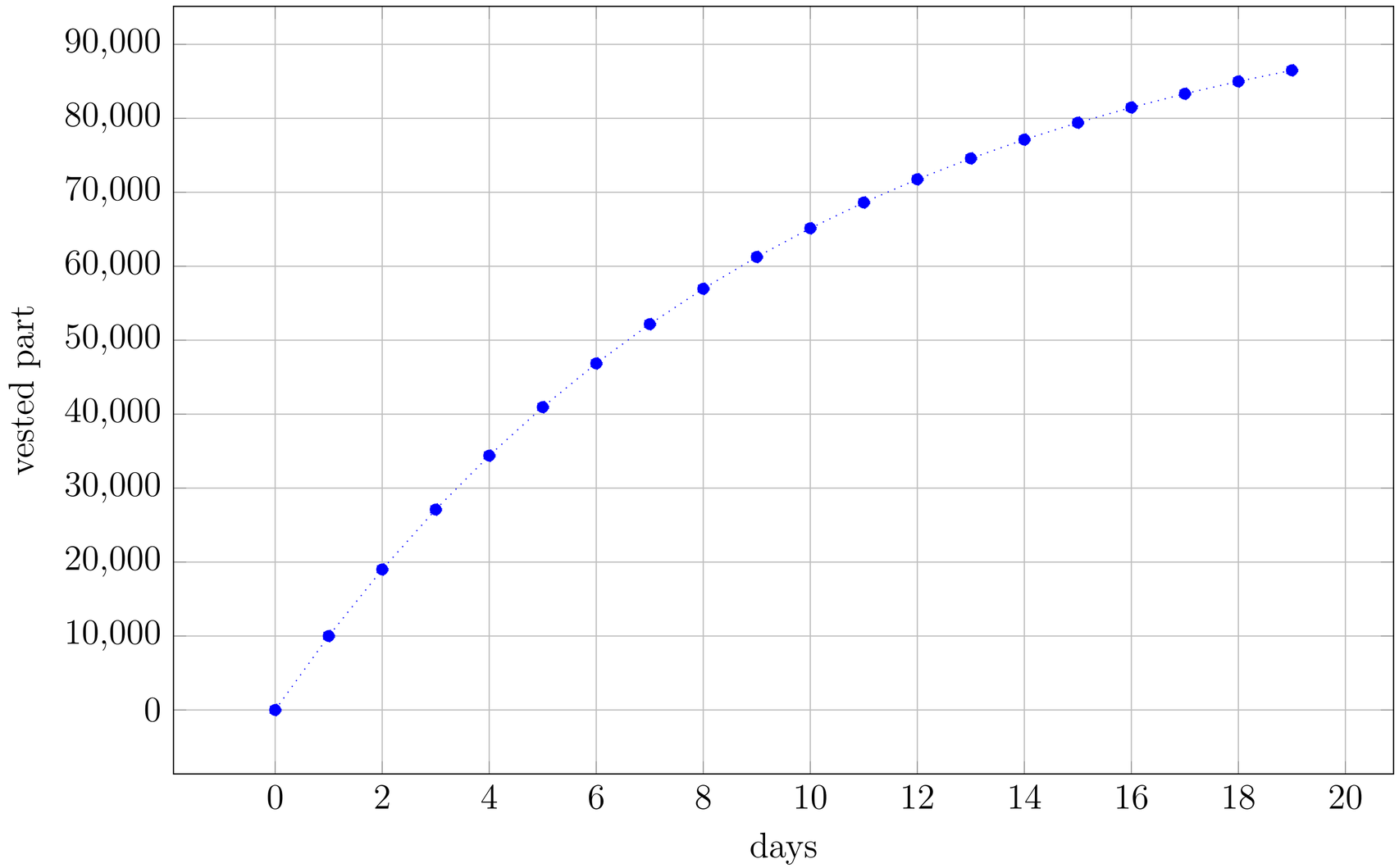
# 取引グラフ

非常に重要なデータ



# 付与された残高

- 残高に重みを付けて、時間が経つと重みが上がる
- 毎日残っている付与されてないの一割が付与される



# アウトリンク行列

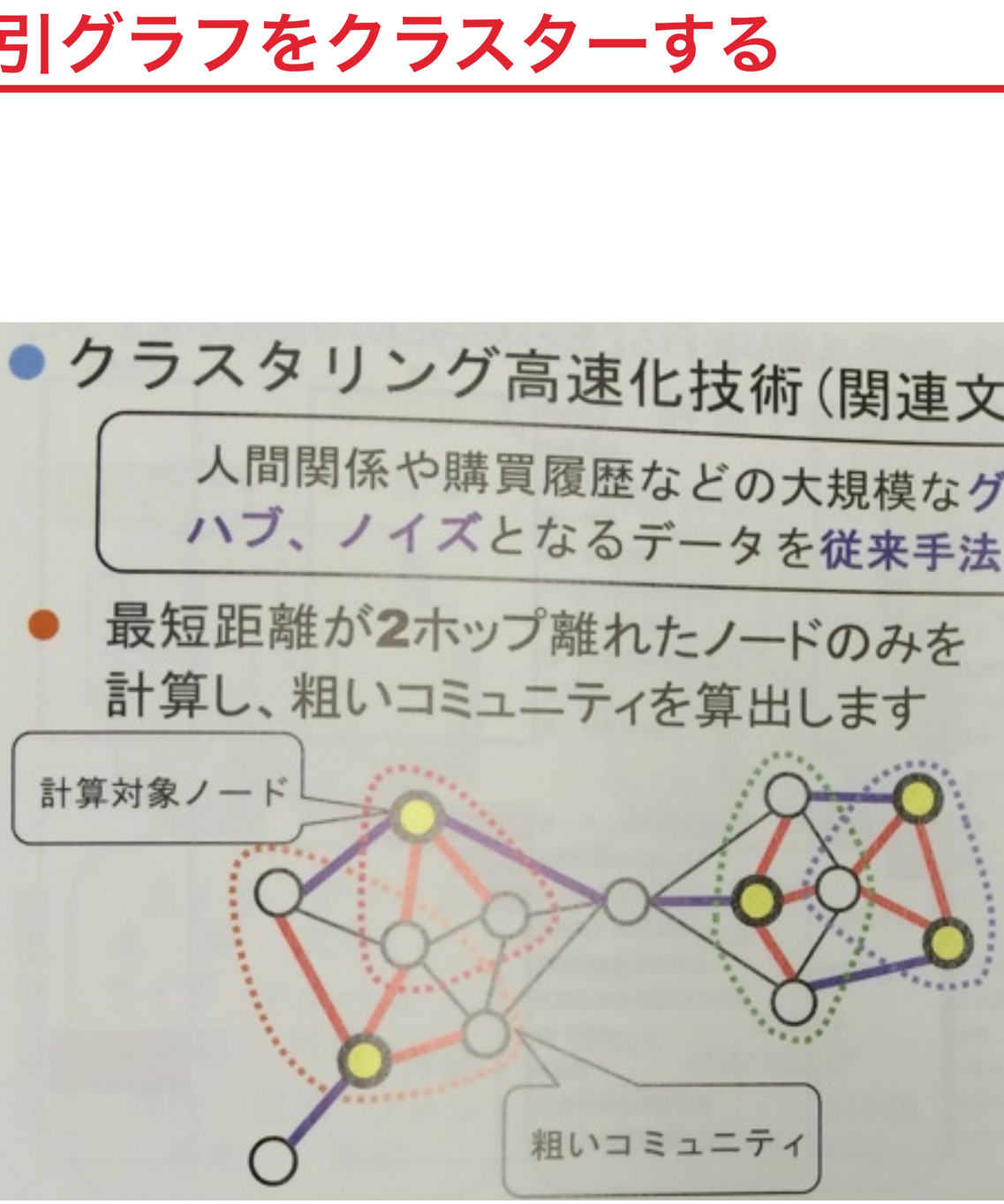
- アカウントからの取引はアウトリンクで、アカウント数 x アカウント数の行列は**アウトリンク行列**である

# 取引グラフをクラスターする

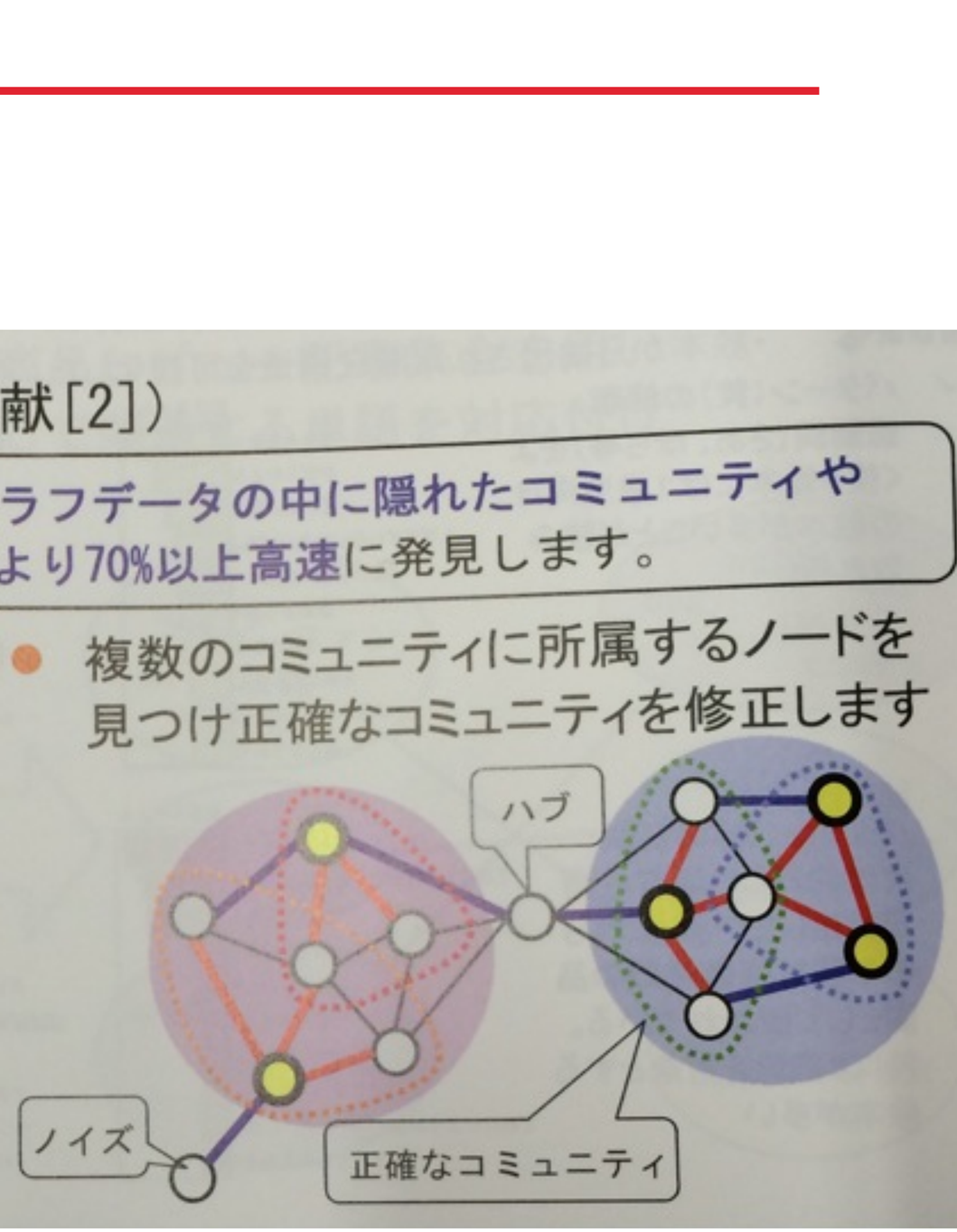
- クラスタリング高速化技術(関連文献[2])

  人間関係や購買履歴などの大規模なグラフデータの中に隠れたコミュニティやハブ、ノイズとなるデータを従来手法より70%以上高速に発見します。

- 最短距離が2ホップ離れたノードのみを計算し、粗いコミュニティを算出します




- 複数のコミュニティに所属するノードを見つけ正確なコミュニティを修正します




NTTで開発した**SCAN++**というアルゴリズムを利用する

DEIM Forum 2014 D6-2

# 構造的類似度に基づくグラフクラスタリングの高速化

塩川　浩昭† 　藤原　靖宏† 　鬼塚　真†

† 日本電信電話株式会社 NTT ソフトウェアイノベーションセンタ
〒 180–8585 東京都武蔵野市緑町 3–9–11
E-mail: †{shiokawa.hiroaki,fujiwara.yasuhiro,onizuka.makoto}@lab.ntt.co.jp

あらまし　グラフクラスタ分析はグラフの中に存在するコミュニティ構造を理解する上で重要な要素技術である．その中でもノード間の構造的類似度を用いたクラスタリング手法 SCAN は，グラフ中のクラスタを抽出するだけでなく，ハブや外れ値などのノードも併せて抽出可能な手法として知られている．しかしながら，SCAN は全てのエッジに対する計算を行うため，グラフに含まれるエッジ数を $|E|$ とした時に $O(|E|)$ の計算量を要する．この SCAN の計算量は，グラフに含まれるノード数を $|V|$ とした時に，最悪の場合 $|E| \approx |V|^2$ となることから最悪計算量が $O(|V|^2)$ となり，大規模なグラフへの適用が難しい．本稿では SCAN の高速化手法を提案する．提案手法では，最短ホップ数が 2 となる様なノードに接続したエッジのみを計算対象としてクラスタリングを行う．これにより，提案手法は SCAN と同一の結果をより高速に抽出ことを可能にする．本稿では，実データに対する評価実験を行い，SCAN の計算時間を最大で約 70% 短縮することを示した．

キーワード　グラフ，クラスタリング，コミュニティ抽出

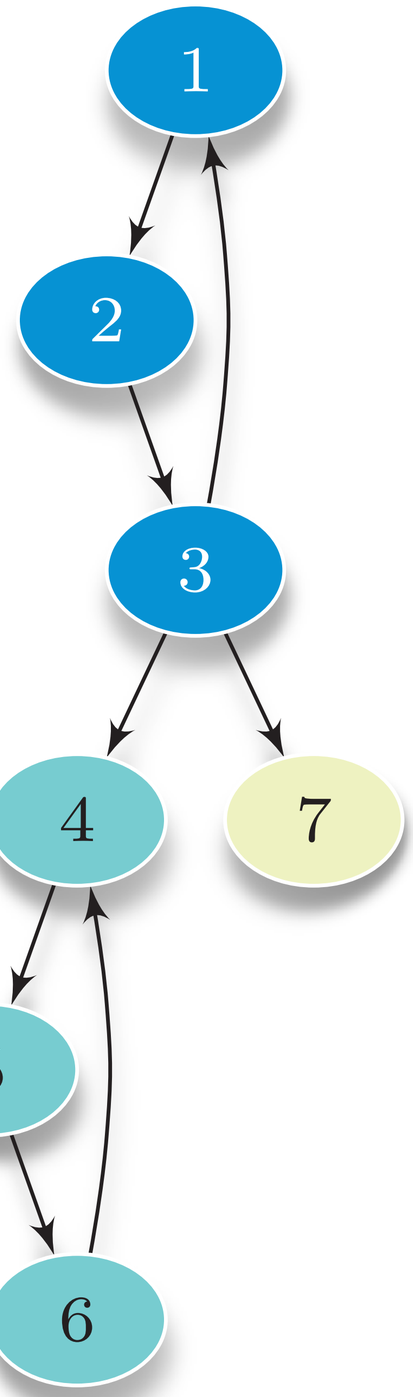
# NCDawareRank

- Googleの有名なPageRankと同様ですが、「NCD」awareの部分が新しい
  - NCD: Nearly Completely Decomposable (大体全てがdecomposable; Herbert Simonが考えた言葉)

参考：Nikolakopoulos, A. N., & Garofalakis, J. D. (2013, February). *NCDawareRank: a novel ranking method that exploits the decomposable structure of the web*. In Proceedings of the sixth ACM international conference on Web search and data mining (pp. 143-152). ACM.

# NCDawareRank

一言で、アカウントに付属するクラスタの情報を利用する PageRank



# NCDawareRank

$$\hat{\pi} = \mathbf{O}\eta\pi + \mathbf{M}\mu\pi + \mathbf{E}(1-\eta-\mu)\pi$$

$\mathbf{O}$ ≜ アウトリンク行列

$\mathbf{M}$ ≜ レベル間proximity行列（付属するクラスタの情報）

$\mathbf{E}$ ≜ teleportation行列

$\pi$ ≜ NCDawareRank

$\eta$ ≜ アウトリンクの重み

$\mu$ ≜ 近位アカウントの重み

# 重要性の計算

$$\psi = (\text{normalize}_1(max(0, \nu + \sigma w_o)) + \hat{\pi} w_i)\chi$$

$$\textbf{normalize}_1(v) \triangleq \frac{v}{\|v\|}$$

$\nu \triangleq$ 付与された残高

$\sigma \triangleq$ 重み付けた送金されたXEM

$\hat{\pi} \triangleq$ NCDawareRank値

$\chi \triangleq$ グラフ構造の重み（1 if cluster, else 0.9）

$w_o = 1.25$

$w_i = 0.1337$

# PoIでブロックの作成の仕方

$$h = H(\textit{generation hash of previous block, public key of account})$$
$$\text{interpreted as 256-bit integer}$$
$$t = \textit{time in seconds since last block}$$
$$b = 8999999999 \cdot (\textit{importance of the account})$$
$$d = \textit{difficulty for new block}$$

$$hit = 2^{54} \left| \ln \left( \frac{h}{2^{256}} \right) \right|$$

$$target = 2^{64} \frac{b}{d} t$$

**hit < target**の場合、参加者はブロックを作成できる

# NEMのブロック難易度計算

$$d = \frac{1}{n}\sum_{i=1}^{n}(\text{difficulty of block i}) \quad \text{平均難易度}$$

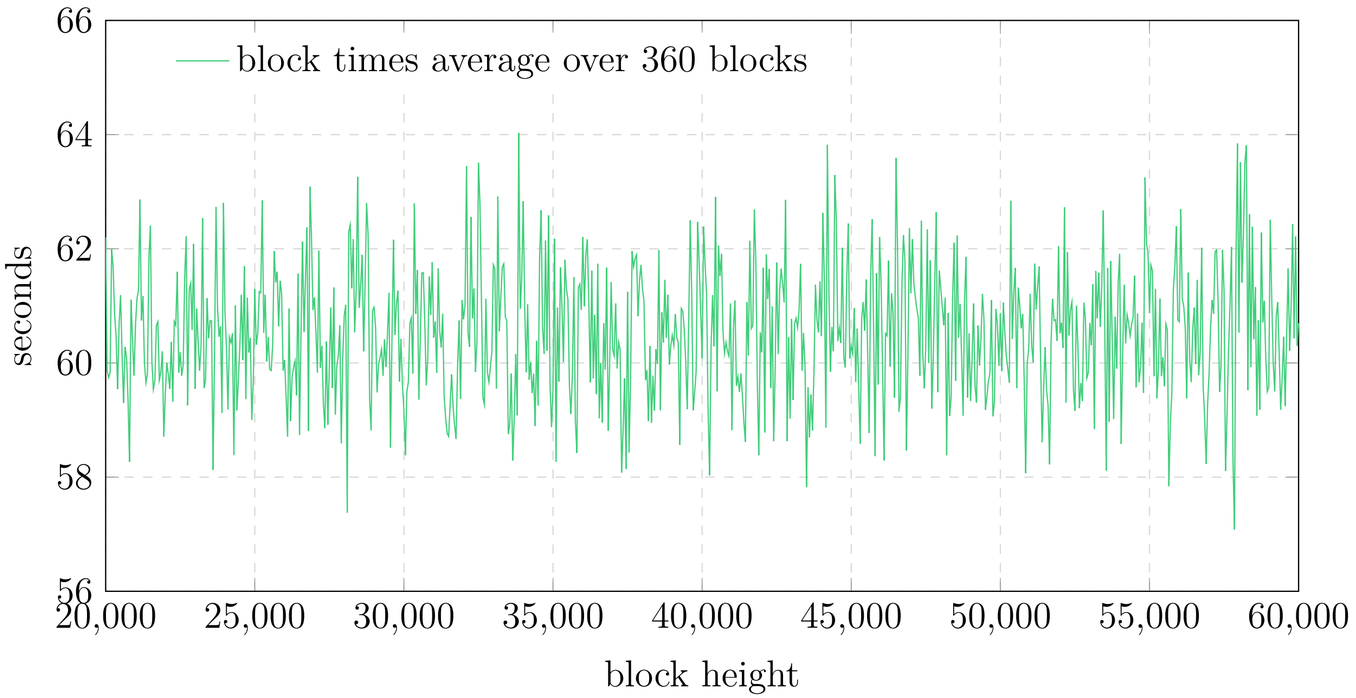
$$t = \frac{1}{n}\sum_{i=1}^{n}(\text{time to create block i}) \quad \text{平均ブロック間の時間}$$

$$difficulty = d\,\frac{60}{t} \quad \text{新しい難易度}$$

新しい難易度が前のブロックより５％以上と違ったら、５％までとする

# ブロック間の時間

- 理想的には６０秒、実際にばらつきがある
- ブロック難易度で決める
- **NEM**: ６０秒+/-0.5秒



nem
a new economy starts with you.

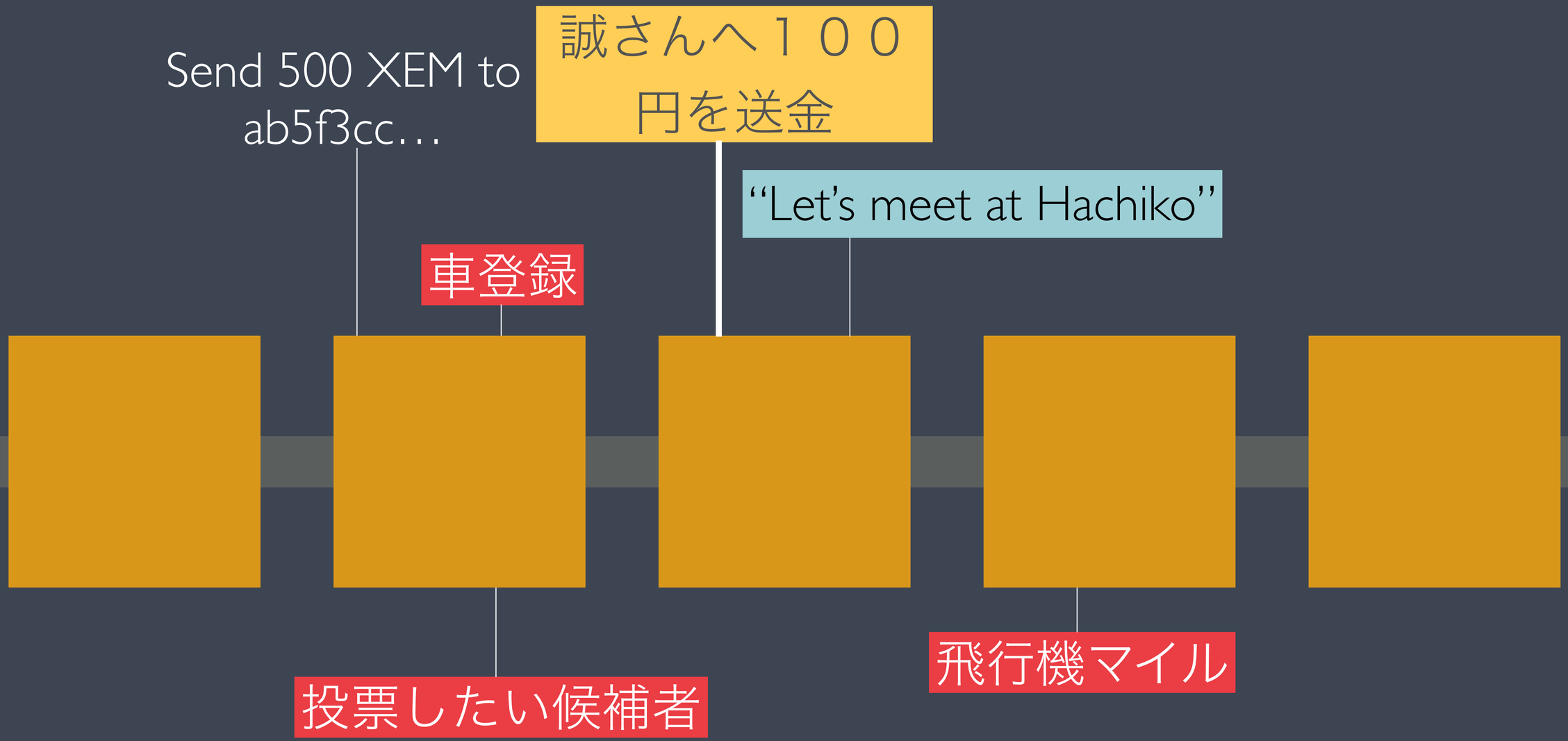
数多くのテストに耐えた信頼性が高いシステム
（６０００個以上のテスト）

nem
a new economy starts with you.

# ２年間開発を行っている

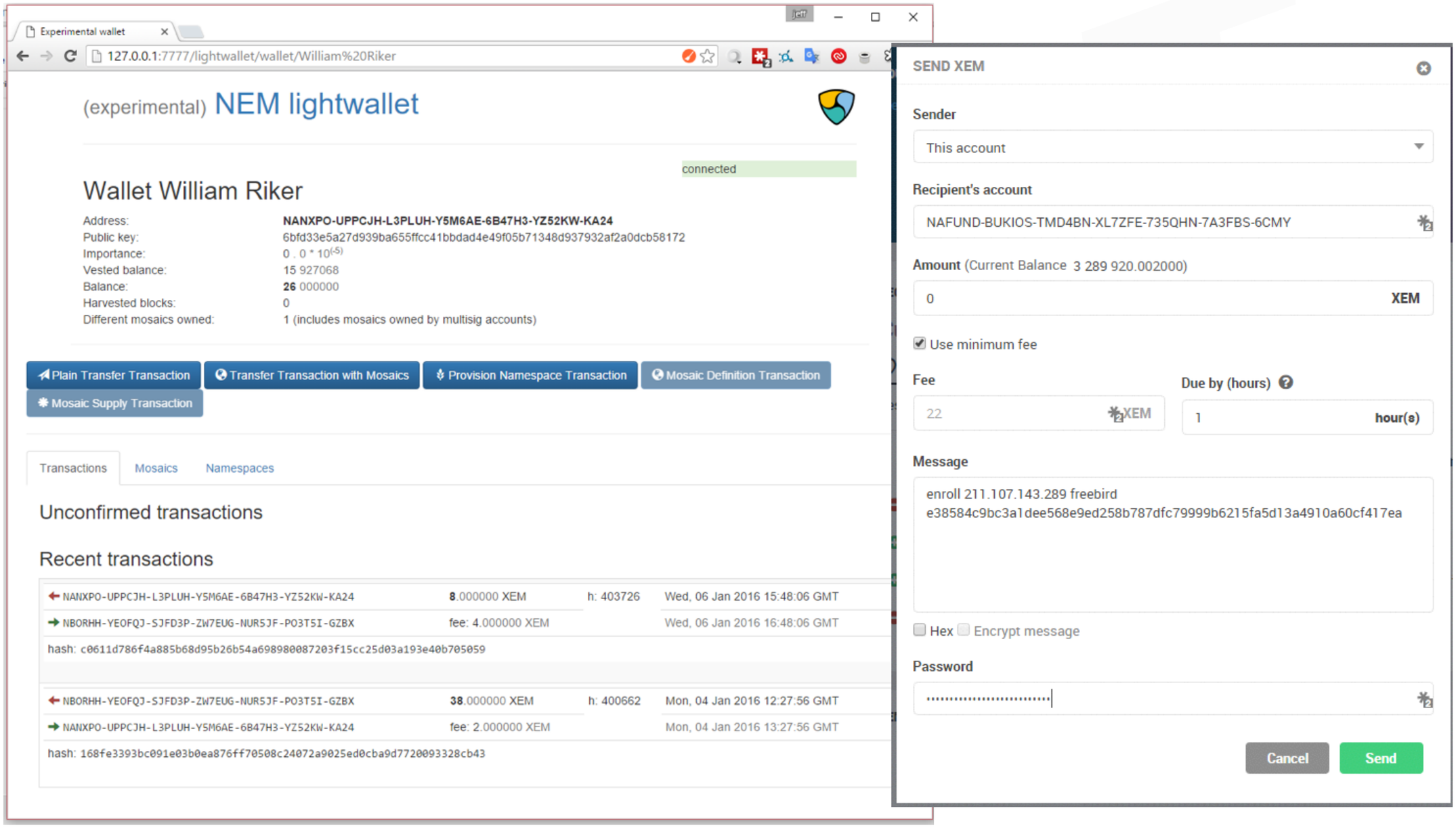
# NEMモザイクタイル

nem
a new economy starts with you.



# モザイクタイル（デジタルアッセト）

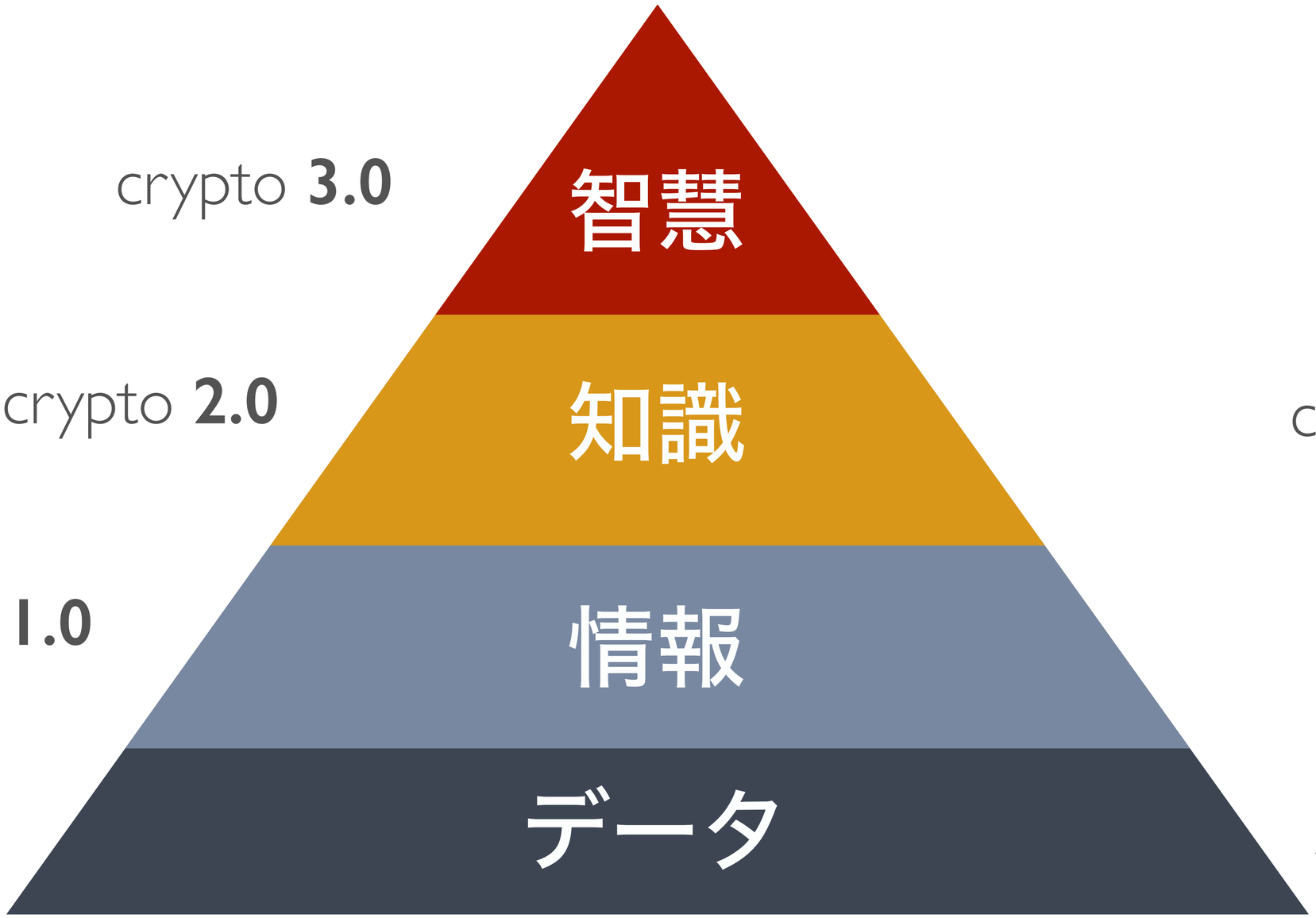
デジタルアセットを簡単に発行することができる、ブロックチェーンNEMの技術を利用する。



# Knowledge Pyramid

crypto **3.0**

intelligence？




crypto **2.0**

computation・Dapps

**1.0**

取引

アカウント残高等