

# ビットコイン技術のインパクト

## ーネットワーク上の合意形成による価値基盤ー



新潟インターネット研究会 Apr. 05, 2014 鈴木一郎

Copyright©2014 Niigata Internet SOciety & I.Suzuki All Rights Reserved

## Bitcoinの一般的な理解

1. 怪しい仮想通貨
2. 決済コストが安い
3. 取引スピードが速い
4. 匿名性が高い
5. 相場の上昇が期待できる
6. スマホで簡単に利用できる
7. 海外でも使える
8. 預金の逃避先として使える

新潟インターネット研究会  
Niigata Internet Society

## もう少し詳しく、Bitcoinとは

- ・ P2P型の決裁システム上で利用可能な暗号通貨
- ・ 管理者はいない
- ・ ネット上の多数決ルールで安全性が確保されている
- ・ 全取引を誰でも見て検証できる
- ・ しかし、誰から誰に送られたかはわからない
- ・ 所有履歴をP2Pネットワーク上のノードで分散管理
- ・ 財布（ウォレット）→フリーのソフトウェア
- ・ 取引の正当性の確認→計算作業（採掘）
- ・ mining（採掘）によりインセンティブが与えられる
- ・ miningには上限がある（金に例えられる）
- ・ miningにより流通量は自動調整される（需要↑→miningは困難に）
- ・ オープンソース

新潟インターネット研究会  
Niigata Internet Society



2009年5月

## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Niigata Internet Society



## 中本哲史の正体

新潟インターネット研究会  
Niigata Internet Society

<http://www.i-cast.com/2013/12/27193222.html?p=all>



日本經濟新聞 3月7日 星期日



ビットコイン考案？「ナカモト氏」発見 米誌報道

米誌ニュースウィーク(電子版)は6日、インターネット上で流通する仮想通貨ビットコインの考察書として、米メディアルニクス・アンド・サンズ・インクが同誌に生む44歳の男性を写真付きで紹介した。米メディアはこの男性に話を聞こうと自身楽屋に押しかけた。

同誌によると日本系米国人の男性の名前は「サト・ハナカモト」。ビットコインが生まれる直前にネット上に公表された。盗刷期間を介さず「電子マネー」でビットコインの暗号を脱税した論文の署名と一致する。ネット上では「サト・ハナカモト」の名前がひびき渡り、「偽名だ」との批判が飛び交っていた。

ニュースウィークの取材に対してナカモト氏は「私はもうビットコインにハマってからは、お話しできない」「現在は引き継いだ他の人々が管理している。私はもう無関心だ」と述べた。ニュースウィークは、発言内容が考察者本人であることを示唆しているとの見方を示した。

ナカモト氏は大分県の別荘生まれで、子供の頃に米国に移民した。カリフォルニア州立工科大学を卒業した後、航空やIT(情報技術)などの企業で働く経験があるという。6人の子供が現在ではロサンゼルス近郊のデングルセンターにある邸宅で住む。

時価で4億ドル(約412億円)相当のビットコインを所有しているとされる。自家消費は日本車のセダンとみられ、取材に応じた時の服装はふわっちょのTシャツと着古した青いジーンズだったとニュースウィークは紹介した。

ナカモト氏の趣味は鉄道模型。ニュースウィークは「(無国籍通貨のアイデアは)鉄道模型を海外から取り寄せる際にかかる旅行の手数料や為替の交換レートにストレスを感じることが理由で、ぜひいらいと同氏の夢の発案が実現している。

<http://www.nikkei.com/article/DGXNAS>

[http://www.nikkei.com/article/DGXNASGM0701K\\_X00C14A3000000/](http://www.nikkei.com/article/DGXNASGM0701K_X00C14A3000000/)

7

## 一旦、仮想通貨という概念を捨てる

中本論文の欠点：  
実物経済の決済手段として使うならば、需要に合わせ、採掘コストを上げずに供給できる仕組みが必要と言われる

計算機科学的には：  
ビザンティン将軍問題の現実的解法

Bitcoinとは：  
オンラインゲームのアイテム

新潟インターネット研究会  
Niigata Internet Society

8

## ビザンティン将軍問題

裏切り者がいるネットワークで合意する  
多数決をとりたいが、失敗させられてしまう

新潟インターネット研究会  
Niigata Internet Society

[http://www.slideshare.net/11ro\\_yamasaki/bitcoin3](http://www.slideshare.net/11ro_yamasaki/bitcoin3)

9

## 古典的解：情報交換を繰り返し、認知レベルを上げる

第1段階、相互の意見の交換  
第2段階、自分が知った他の将軍たちの意見（意見ベクトル）の交換  
第3段階、...（意見ベクトルのベクトル）の交換  
1/3以上裏切り者がいると解が無い

新潟インターネット研究会  
Niigata Internet Society

[http://www.slideshare.net/11ro\\_yamasaki/bitcoin3](http://www.slideshare.net/11ro_yamasaki/bitcoin3)

10

## 3人の場合

新潟インターネット研究会  
Niigata Internet Society

11

## サトシ・ナカモトの解

ネット上の計算資源の総量が有限  
「攻撃」チーム VS 「和睦」チーム  
計算競争をして勝った方の意見を採用！ → 人間の欲望を利用

マイニング

何回戦かすると  
たまたま少数派が勝つ確率は  
極小になる

新潟インターネット研究会  
Niigata Internet Society

[http://www.slideshare.net/11ro\\_yamasaki/bitcoin3](http://www.slideshare.net/11ro_yamasaki/bitcoin3)

12

## Bitcoinのしくみ

新潟インターネット研究会  
Niigata Internet Society

13

## 取引 : Transactions

Transaction 1: Owner 1's Public Key, Hash, Owner 0's Signature, Owner 1's Private Key

Transaction 2: Owner 2's Public Key, Hash, Owner 1's Signature, Owner 2's Private Key

Transaction 3: Owner 3's Public Key, Hash, Owner 2's Signature, Owner 3's Private Key

新潟インターネット研究会  
Niigata Internet Society

14

## Timestamp Server

- 取引が発生したことを公開
  - タイムスタンプされた複数の取引をブロックとしてまとめる
  - ブロックのhashを公開する

新潟インターネット研究会  
Niigata Internet Society

15

## Proof-of-Work

- 要求されるゼロビット値が見つかるまでhash計算 (SHA-256) を繰り返す
- 計算したという証拠を示すだけの無意味な計算である
- 過去のデータチェーンを変更しようとするとは後のブロックを全て書き換えが必要 (hash値が変わる)
- 1CPU : 一票の多数決
- 計算速度と利益レートに対応するため、計算の難易度はブロック追加時間が平均的となるよう調整される
- 2016ブロック (10分x2016=約2週) 毎に難易度を調整
  - 2週より早い→難しく 2週より遅い→簡単に

新潟インターネット研究会  
Niigata Internet Society

16

## ネットワーク

- 新しい取引は全ノードに送信
- 各ノードが新しい取引をブロックに取得
- 各ノードがそのブロックのPoWを算出
- PoWが発見されたら、全ノードへ告知する
- 各ノードは過去の取引と重複のないことをチェックして承認
- 多重使用 (チェーンの分岐) のチェック  
→最も長いチェーン (計算量が多い) を信頼する

新潟インターネット研究会  
Niigata Internet Society

17

## ブロックのコンパクト化

Block Header (Block Hash): Prev Hash, Nonce, Root Hash

Hash01, Hash23, Hash0, Hash1, Hash2, Hash3

Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

新潟インターネット研究会  
Niigata Internet Society

18

## Bitcoinの仕組み (概要)

ブロックチェーン

プルーフ・オブ・ワーク

発見されたプルーフ・オブ・ワーク

新ブロック

新コイン 25BTC

ブロックのコンパクト化

ブロックヘッダーにはルートHashだけ

検証に必要なハッシュはP2Pネットワークから入手

http://www.shidoshare.net/111ro\_vamasaki/bitcoin2 より抜粋

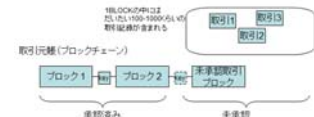
## Bitcoinの財布 Wallet

- bitcoinのセキュリティリスクとは？
  - 盗まれると追跡できない
  - キャンセルができない
- Hot wallet
  - ネット接続PC、タブレット等
- Cold wallet
  - ネット接続されないPC
  - メモリ
- Paper wallet
  - 公開アドレス+秘密鍵を記載
  - 公開アドレスに送金してwalletは金庫に保存



## 採掘 mining

- 100~1,000の取引をまとめてブロックという単位でチェーンに追加
- 承認済みのチェーンに未承認のブロックを追加する
- 採掘とは→追加するためのkeyとなる値を探す
  - 承認済みブロックを代表するような値"H0"を作る
  - ハッシュ計算  $\text{SHA}(H0, \text{key}) = d$
  - "d"の先頭のn桁がゼロとなると追加が可能となる→承認
  - 51%の計算力を支配できれば改ざんが可能？
    - Mining pool GHash.ioは42%の計算力を持っている
  - "d"を見つけた先着1名にはビットコインが与えられる
  - "d"が見つかるまで約10分となるよう調整されている (difficulty)
- ブロック記帳情報: <https://blockchain.info/ja>



## 採掘で稼げるか？

### solo mining

- 多数のminerが稼働しており、コインを得るのは実質不可能



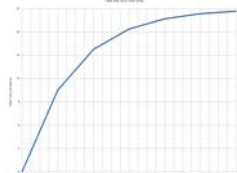
### pool mining

- グループ採掘して各自の仕事量に応じて対価を得る



## bitcoinには発行上限がある

- 総量は2,100万コイン (仕様)
- 現在1,200万コインが発行済み
- ブロックは6,929,999個が上限 (仕様)
- 採掘の報酬は徐々に減少する
  - 21万ブロック毎に採掘報酬は1/2となる (→上限が決まる)
    - 1-210,000ブロック → 50BTC/block
    - 210,001-420,000ブロック → 25BTC/block
    - 420,001-640,000ブロック → 12.5BTC/block
  - 10分/block x 6,929,999block = 132年 (2009-2141年)



## 採掘機 bitcoin miner

ビットコインBitcoinマイナー(採掘) 333MH/s USB ASIC MINER 日本語マニュアル付き



現在在庫切れです。在庫状況についてこの商品の購入希望者は必ずお読みください



ASRock LGA1155

価格: ¥ 9,310

2点在庫あり。在庫切れの場合は、ご注文のキャンセルとなります。

新品の出品: ¥ 8,280



Bitcoin ビットコイン A

価格: ¥ 240,000

3点在庫あり。在庫状況についてこの商品の購入希望者は必ずお読みください

新品の出品: ¥ 230,000

注意: Amazonポイントとは、Amazonギフト券とは異なります。マーケットプレイスのネットバンキング・電子マネーとは、(別)です。



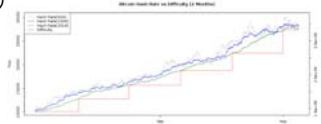
## 採掘に費やす電力は1,000MW/day





## bitcoinの採掘はもはや割りにあわない

- Difficultyが急上昇
  - 2週間毎に130% (37日で2倍)
  - 個人採掘はハードウェア投資的にも電気代的にも割りに合わない
- なぜ成功報酬は減ってゆくのか？
  - ブロック数の少ない初期段階で改ざんのリスクを減らす (改ざんく正当な発掘となるようなインセンティブ)
- 他の仮想通貨
  - litecoin (bitcoinに次ぐ規模)
  - monacoin (2ch発)

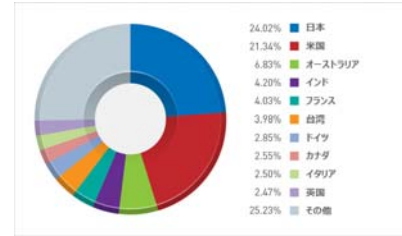


<http://bitcoinwisdom.com/bitcoin/difficulty>



## 不正発掘プログラムの感染状況

- miningプログラムを不正インストール
- 高性能PCが多い日本が狙われている



<http://blog.trendmicro.co.jp/archives/8324>



## Bitcoinを要求するランサムウェア

日本の  
注目！  
本投稿の BitCrypt ID: [redacted]

すべての重要なファイルは暗号化されています。データ復元には、BitCrypt v2.0 が必要です。これは、ITC に対して特別なプログラムを使用する必要があります。このランサムウェアは、世界中の専門家から報告されています。このランサムウェアは、世界中の専門家から報告されています。このランサムウェアは、世界中の専門家から報告されています。

1. 以下のリンクをクリックし、以下の手順に従ってください。  
2. torbrowser (http://[redacted]) をダウンロードし、インストールしてください。  
3. インストールした後、torbrowser を起動し、アドレスを入力します。

注意: 早に支払えば、早に暗号化されたファイルの復元が可能です。

Your computer was infected by BitCrypt v2.0 cryptovirus.  
For more information you should find txt file named Bitcrypt.txt on y

<http://blog.trendmicro.co.jp/archives/8801>



## 誰が通貨価値を担保するのか？

- 電子化されていることはあまり問題ではない
  - 円やドルも電子化されて銀行口座にある
  - 電子マネーが普通に使われている
- 通貨としての信頼性
  - 国家が通貨の利用と価値を担保
    - 日本では円決済が可能であることを強制 (日銀法)
    - 公定歩合の設定、貨幣流通量の調整や為替介入
  - bitcoinでは暗号化による証明



## 他のマネーと何が違うか？

|       | 誰が発行する？       | どう使われる？ | 法規制は？       |
|-------|---------------|---------|-------------|
| 通貨    | 中央銀行          | 買物など    | 外為法・金融商品取引法 |
| 電子マネー | 企業 (交通・流通・金融) | 買物など    | 資金決済法       |
| 証券    | 企業            | 投資      | 金融商品取引法     |
| 商品先物  | なし            | 投資      | 商品先物取引法     |
| 仮想通貨  | なし            | 買物・投資   | なし          |



## 仮想通貨としてのメリット

- 決済コストが安く少額決済に適する
- 匿名性が高い
  - アングラマネーのロンダリング



- 実際の用途としては資金取引 (送金)
- エスクロー取引にも利用できる (1アドレスに5マルチ鍵までの設定が可能)



## なぜ普及したか？

- 価格上昇
  - 2012年：1BTC=1から10セント程度
  - 2013年3月：キプロスの財政危機により100～1,000ドルに急騰
  - 2013年12月：中国人民銀行の警告により500ドル程度
  - 利用者は100万人程度



## バーナンキ



- 法執行や監督業務のリスクとなる可能性
- 長期的展望を持てる分野もある



## クルーグマン



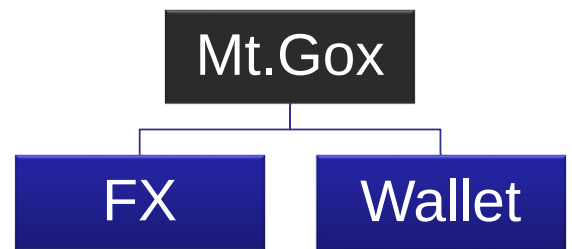
- 質問：信頼できる価値の貯蔵手段なの？
- 答え：すばらしい価値の交換手段である



## Bitcoin price (USD)



## Mt.Goxは何をやっていた？



仕組上ユーザのコントロールから離れる



## どのようにコインを盗まれたのか

- Walletソフトウェアのバグ  
(Transaction mutability/malleability)  
→2011年に解決済みの問題
- 犯罪者がMt.Goxの口座から自身のビットコインを自身の財布に送金
- 引き出しのトランザクションに手を加える
- 送金は成功しているのに失敗したように見せかける
- Mt.Goxに再送を通知
- 再度送金される
- 再び送金が失敗したように見せかける
- Mt.Goxの口座が空になる



## 管理がずさん？

- Walletソフト修正
- 再送金のチェック
- 顧客のbitcoinを一括管理
- Cald wallet (offline wallet)
- . . .
- bitcoinのアルゴリズムが破られたわけではない
- それにしても490億は巨額すぎる



## 規制の動き

- 米国：通貨でなく資産で課税対象（IRS 2014/3/25）
- 中国：金融機関での取引禁止（2013/12）
- タイ：2013/7に違法の判断→関連法制定
- 日本：3/7閣議決定
  - 通貨としては認めない
    - 強制通用力がない（受け取りを拒否できない）
    - 銀行法・金融商品取引法の対象外
    - 従って銀行はコインの売買仲介や口座開設はできない
  - 取引は課税対象（法人税・所得税・消費税）
  - マネロンに対しては犯罪収益移転防止法



## とりあえず財布を使ってみる

- デスクトップウォレット
  - 自分のPCでビットコインを保管する
    - 厳重な管理が必要
    - セキュリティレベルはそこそこ
    - ブロックチェーンをダウンロードするのでHDDスペースが多量
- ウェブウォレット
  - クラウドにビットコインを保管
    - 軽い
    - ブロックチェーンはクラウド上
    - セキュリティレベルやや落ちる
- モバイルウォレット
  - スマホやタブレット（電子通貨用途）



## とりあえず財布を使ってみる



### デスクトップウォレット

- 厳重な管理が必要
- セキュリティレベルはそこそこ
- ブロックチェーン保管スペースが必要



### Webウォレット

- ブロックチェーンはクラウド上にある
- 動作が軽い
- セキュリティレベルやや落ちる



### モバイルウォレット

- スマホやタブレット
- 電子通貨用途



## Web wallet

- Blockchain <https://blockchain.info/wallet>

Welcome Back  
Please enter your login details below:

Identifier: c836a200-b629-4668-950a-64621624ab  
Password:

Open Wallet

マイウォレット 自ら専ら専用の銀行になろう。

0.001 BTC \$ 0.68

Wallet Home 取引一覧 送金 受け取り インポート/エクスポート

送金履歴

| 送金先                         | 送金額       | 送金日時                | 送金先名    |
|-----------------------------|-----------|---------------------|---------|
| 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | 0.001 BTC | 2014/03/25 10:00:00 | Bitcoin |
| 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | 0.001 BTC | 2014/03/25 10:00:00 | Bitcoin |
| 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | 0.001 BTC | 2014/03/25 10:00:00 | Bitcoin |

Final Balance: 0.001 BTC

Partners: Spread Your Bitcoins

Bitcoin Store Bitcoin Options gTang Bitcoin

アカウント設定  
メールアドレス、パスワード、および連絡先を設定してアカウントを設定します。

アカウント設定



Wallet Home 取引一覧 送金 受け取り インポート/エクスポート

送金履歴

| 送金先                         | 送金額       | 送金日時                | 送金先名    |
|-----------------------------|-----------|---------------------|---------|
| 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | 0.001 BTC | 2014/03/25 10:00:00 | Bitcoin |
| 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | 0.001 BTC | 2014/03/25 10:00:00 | Bitcoin |
| 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | 0.001 BTC | 2014/03/25 10:00:00 | Bitcoin |

Final Balance: 0.001 BTC

Partners: Spread Your Bitcoins

Bitcoin Store Bitcoin Options gTang Bitcoin

アカウント設定  
メールアドレス、パスワード、および連絡先を設定してアカウントを設定します。

アカウント設定



1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m

Get Free Bitcoins

### Backup

送金履歴をバックアップして、万一の事故に備えます。Blockchain.infoは、送金履歴をバックアップして、万一の事故に備えます。Blockchain.infoは、送金履歴をバックアップして、万一の事故に備えます。

### Paper Wallet

送金履歴をバックアップして、万一の事故に備えます。Blockchain.infoは、送金履歴をバックアップして、万一の事故に備えます。Blockchain.infoは、送金履歴をバックアップして、万一の事故に備えます。

Scan to Load & Verify

1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m

Scan to Redeem

1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m



マイウォレット 自ら専ら専用の銀行になろう。

0.001 BTC \$ 0.68

Wallet Home 取引一覧 送金 受け取り インポート/エクスポート

Transactions お客様の最近の取引履歴

To From Date Amount Balance

| To                          | From                        | Date           | Amount    | Balance   |
|-----------------------------|-----------------------------|----------------|-----------|-----------|
| 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m | Today 10:00:41 | 0.001 BTC | 0.001 BTC |

Transaction Details

Address: 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m

Amount: 0.001 BTC

Fee: 0.00000000 BTC

Total: 0.001 BTC

Transaction ID: 1P7QM4NtU8pG6Z2DnR9VgZ5Nv5m

QR code for transaction



43

**Transaction Summary**

送金金額  
**0.0002 BTC (\$ 0.14)**  
取引時の価格 \$ 0.14

Hash: 5925c6ab5dce56c4dad2fd632...

送金時刻: 2014-03-04 09:31:55 (+40 minutes 確認)

認証済み: 1 認証済み

二重払い: 二重払いは検出されませんでした

Transaction Fee: 0.0001 BTC

新潟インターネット研究会  
Niigata Internet Society

44

**Transaction Summary**

送金金額  
**0.0002 BTC (\$ 0.14)**  
取引時の価格 \$ 0.14

Hash: 5925c6ab5dce56c4dad2fd632...

送金時刻: 2014-03-04 09:31:55 (+40 minutes 確認)

認証済み: 1 認証済み

二重払い: 二重払いは検出されませんでした

Transaction Fee: 0.0001 BTC

新潟インターネット研究会  
Niigata Internet Society

45

**bitcoinで買物できるか？**

新潟インターネット研究会  
Niigata Internet Society

46

**Monacoin**

新潟インターネット研究会  
Niigata Internet Society

47

**Monacoinなら採掘できそう**

新潟インターネット研究会  
Niigata Internet Society

48

**まとめ**

- ビザンチン將軍問題の実用的解法の応用である
- P2Pの暗号通貨である
- ネット上の多数決ルールで安全性が担保される
- 通貨量には上限がある
- 採掘による承認と対価
- 採掘には莫大な電力を消費（計算パワーの無限連鎖講）
- Mt.Gox問題はbitcoinの原理によるものではない
- 用途は資金取引と投機（電子マネーではない）
- 今後法的な規制がかかる可能性がある
- ネットワーク上の権利保護や契約への応用が考えられる

新潟インターネット研究会  
Niigata Internet Society



49

## Bitcoinとは？

今のところ

皆でハッシュを  
探し当てる

オンラインゲーム

ネットワーク上の  
新たな  
価値基盤の仕組み  
となる可能性

新潟インターネット研究会  
Niigata Internet Society

50



### what?

Ethereum is a platform and a programming language that makes it possible for any developer to build and publish next-generation decentralized applications.

Ethereum can be used to codify, decentralize, secure and trade just about anything: voting, domain names, financial exchanges, crowdfunding, company governance, contracts and agreements of most kind, intellectual property, and even smart property thanks to hardware integration.

Ethereum borrows the concept of decentralized consensus that makes bitcoin so resilient, yet makes it trivial to build on its foundation. To find out more about how Ethereum works, consult [the whitepaper](#).

What will you build out of the Ether?

新潟インターネット研究会  
Niigata Internet Society

<https://www.ethereum.org>

51

## 参考文献

1. Bitcoin: A Peer-to-Peer Electronic Cash System  
<https://bitcoin.org/bitcoin.pdf>  
<http://www.bitcoin.co.jp/docs/SatoshiWhitepaper.pdf> (日本語訳)
2. ビットコイン取引の仕組み  
<http://www.digitalmoney.or.jp/2013/12/how-transaction/>
3. bitcoinに迫る  
<http://app-review.jp/news/165211>
4. Bitcoin勉強会 3  
[http://www.slideshare.net/11ro\\_yamasaki/bitcoin3](http://www.slideshare.net/11ro_yamasaki/bitcoin3)
5. ビットコイン、世界最大級の取引所の破綻の影響は  
<http://business.nikkeibp.co.jp/article/topics/20140302/260428/?P=4>
6. Nomad研究所  
<http://nomad-ken.com/>
7. Ethereum  
<https://www.ethereum.org/>

新潟インターネット研究会  
Niigata Internet Society