仮想通貨（ビットコイン）
（基幹技術：ブロックチェーン）

2018年1月6日（土）

柏ビットコイン普及協会理事　中村

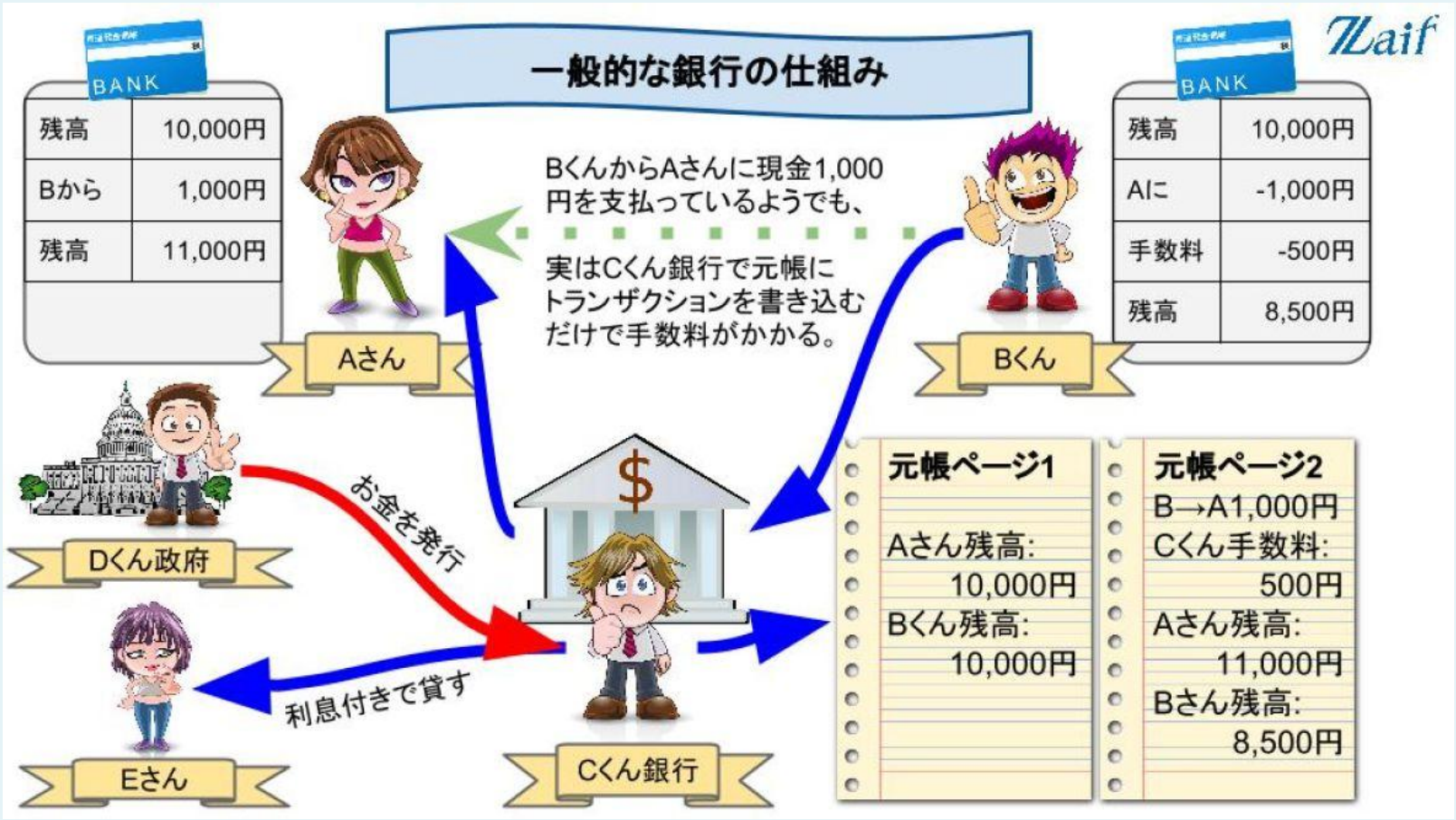
イラストで理解する
仮想通貨（ビットコイン）

朝山貴生氏のイラストを流用

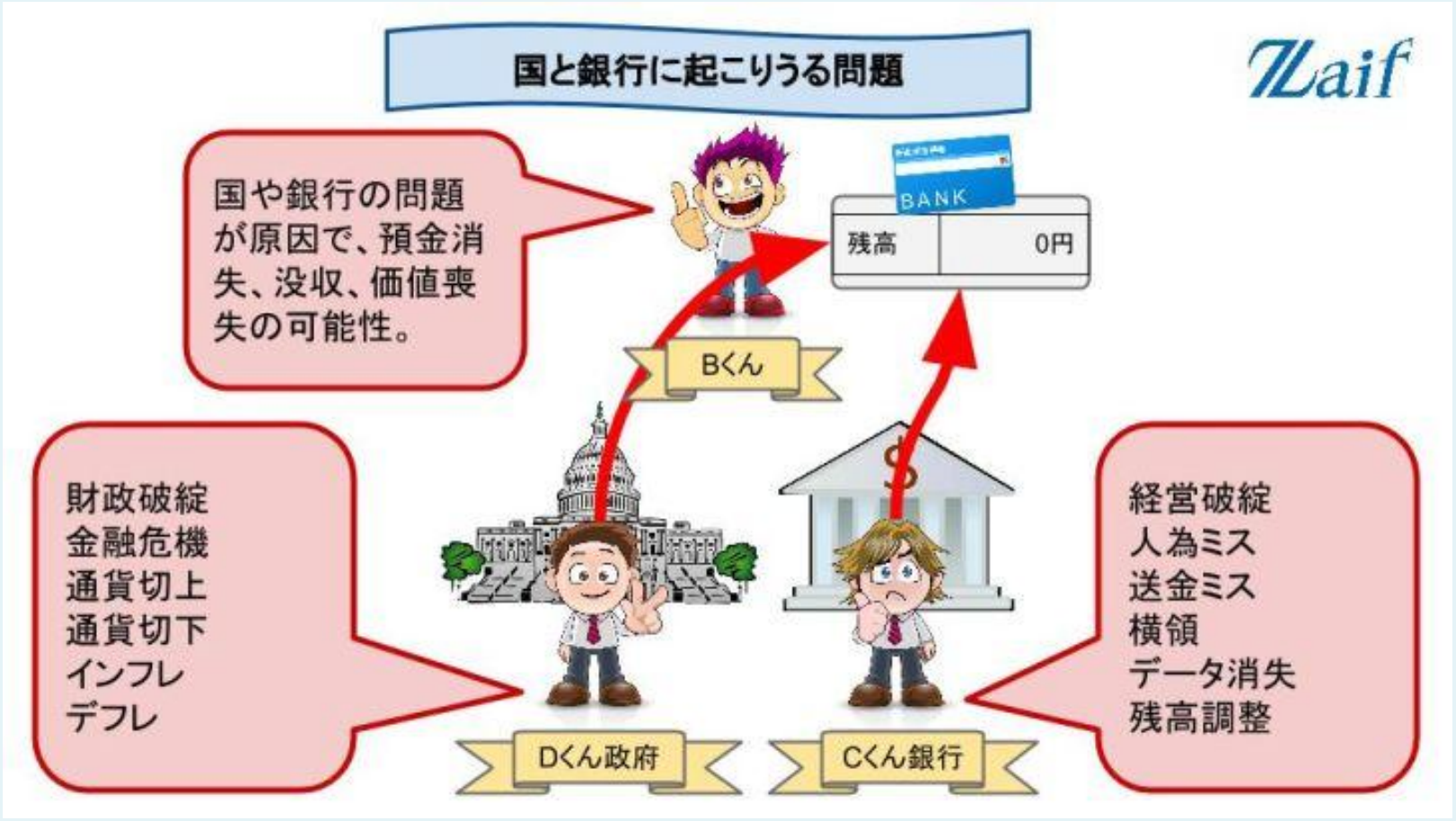
朝山氏：ビットコインと国産暗号通貨のモナーコインを扱う国内向け取引所の「Zaif Exchange」（ザイフ）を2015年3月初旬にオープンしたテックビューロの創業者で代表取締役

ビットコインの仕組み

ビットコインの仕組みと可能性； http://jp.techcrunch.com/2015/03/31/bitcoin-essay/



ビットコインの仕組み


国と銀行に起こりうる問題
Zaif
国や銀行の問題が原因で、預金消失、没収、価値喪失の可能性。
BANK
残高
0円
Bくん
財政破綻
金融危機
通貨切上
通貨切下
インフレ
デフレ
Dくん政府
Cくん銀行
経営破綻
人為ミス
送金ミス
横領
データ消失
残高調整

ビットコインの仕組み

Bitcoinはお金でなく決済システム

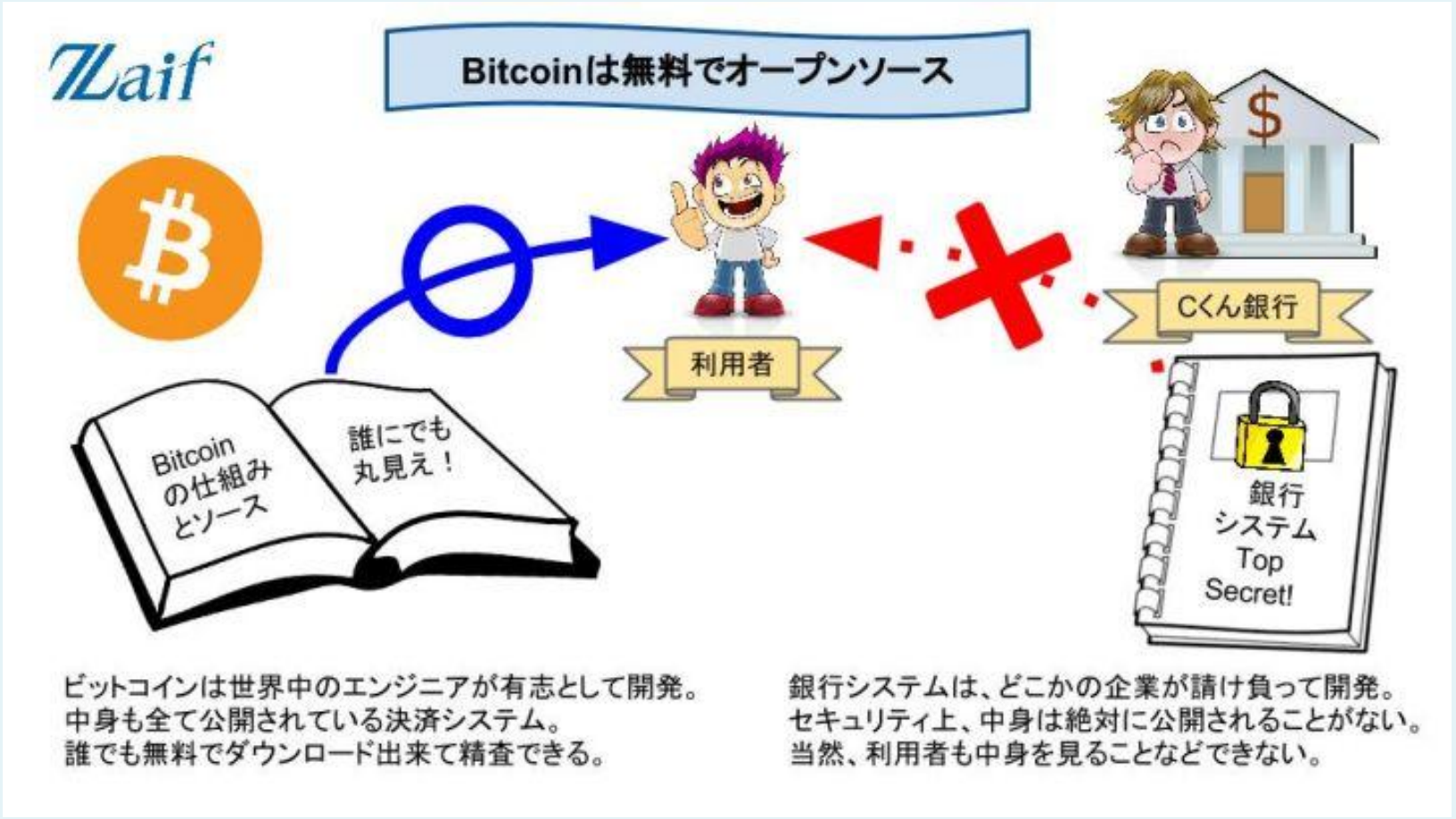
Zaif

お金 ✕

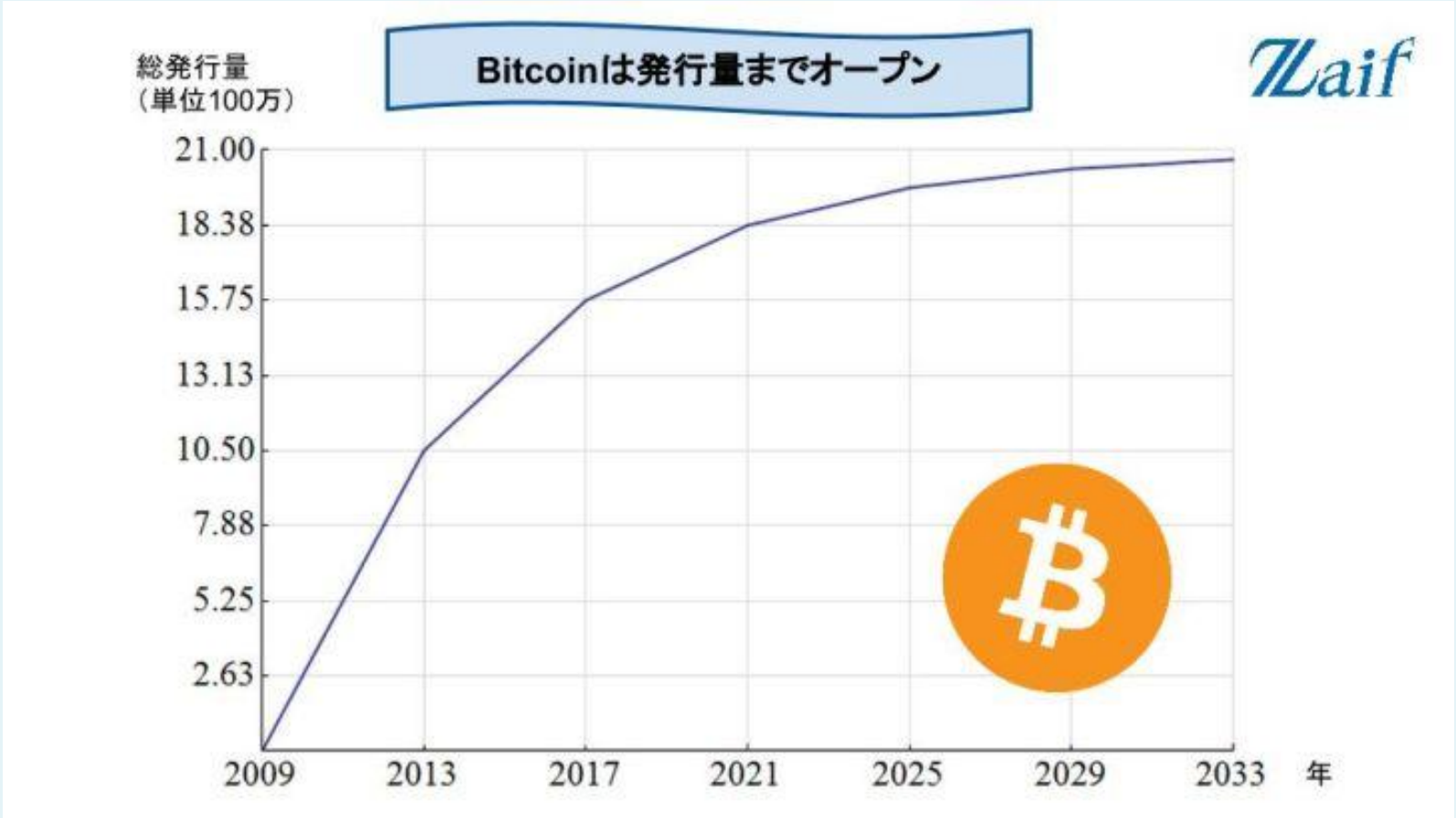
決済システム ○

元帳ページ1	元帳ページ2
Aさん残高: 10 BTC	B→A 1 BTC
Bくん残高: 10 BTC	Aさん残高: 11 BTC
	Bさん残高: 9 BTC

ビットコインの仕組み


Zaif
Bitcoinは無料でオープンソース
利用者
Cくん銀行
Bitcoin
の仕組み
とソース
誰にでも
丸見え！
銀行
システム
Top
Secret!
ビットコインは世界中のエンジニアが有志として開発。
中身も全て公開されている決済システム。
誰でも無料でダウンロード出来て精査できる。
銀行システムは、どこかの企業が請け負って開発。
セキュリティ上、中身は絶対に公開されることがない。
当然、利用者も中身を見ることなどできない。

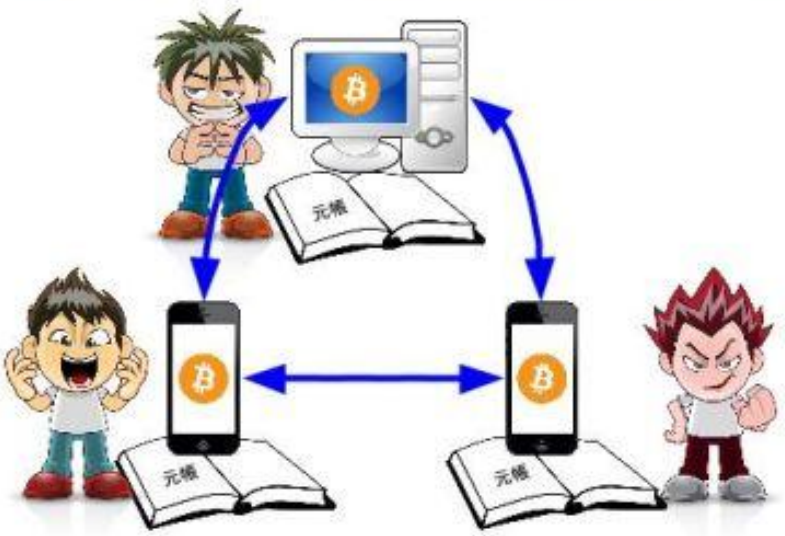
ビットコインの仕組み


Bitcoinは発行量までオープン
Zaif
総発行量
（単位100万）
21.00
18.38
15.75
13.13
10.50
7.88
5.25
2.63
2009
2013
2017
2021
2025
2029
2033
年

ビットコインの仕組み

Zaif

Bitcoinには中央管理者はいない



ビットコインでは、誰もがソフトウェアであるビットコインをインストールして、元帳データを持てる。中央管理者がいて業務を担っている訳ではない。

銀行では、銀行で働く人間が元帳を管理する。

＝中央管理者がいる。

ビットコインの仕組み

Zaif

Bitcoinの最小単位

最小単位

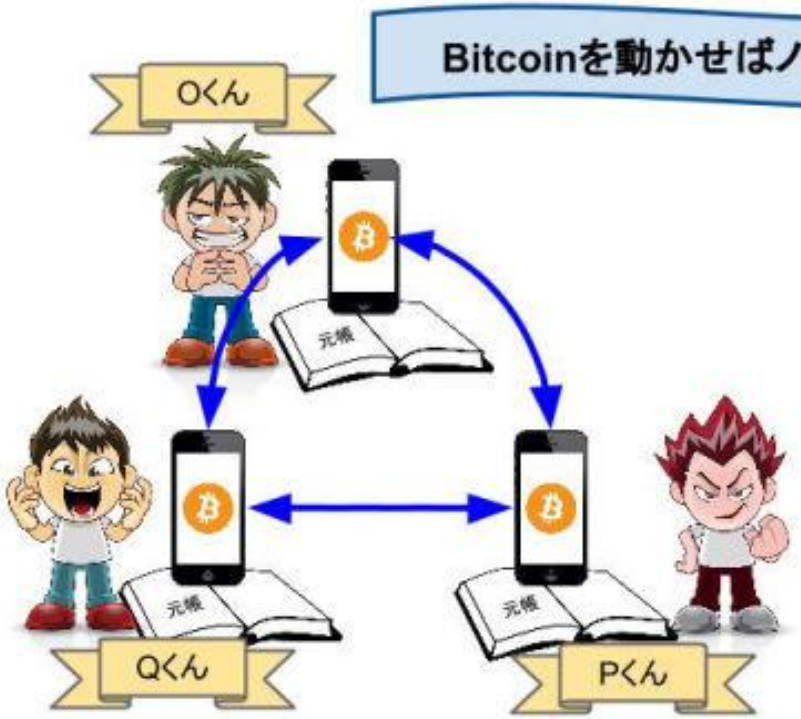
0.00000001BTC（1億分の1ビットコイン）
＝ 1 Satoshi ＝ 約0.0003円

最小送金可能金額

0.0005460BTC（1億分の5,460ビットコイン）
＝ 5,460 Satoshi ＝ 約1.638円

2015年3月中旬の1 BTC = 30,000円換算

ビットコインの仕組み



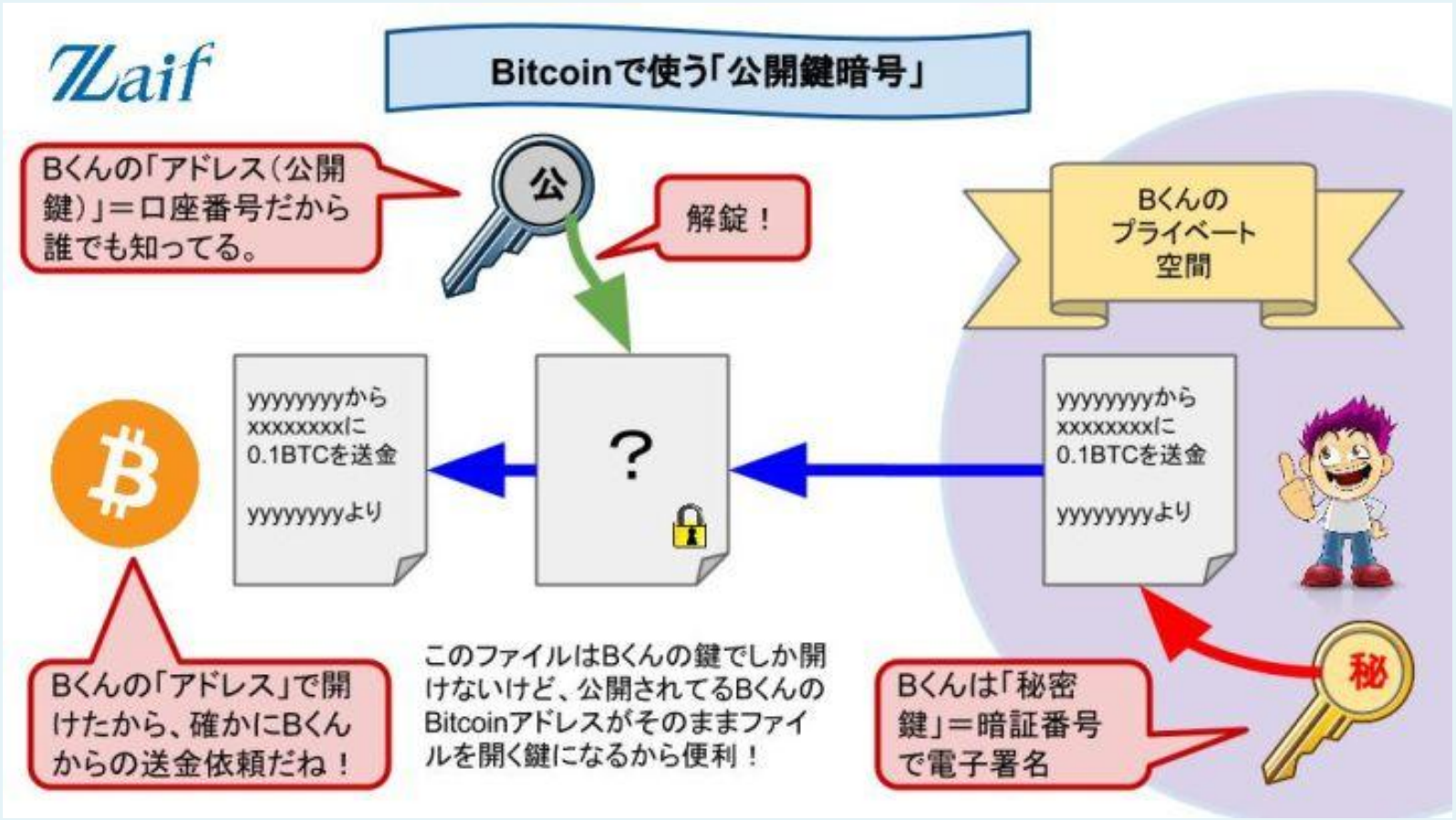
ノード（node）=接続ポイント

ビットコインは、決済システムの名前でもあり、それを動かすためのソフトウェアの名前でもある。

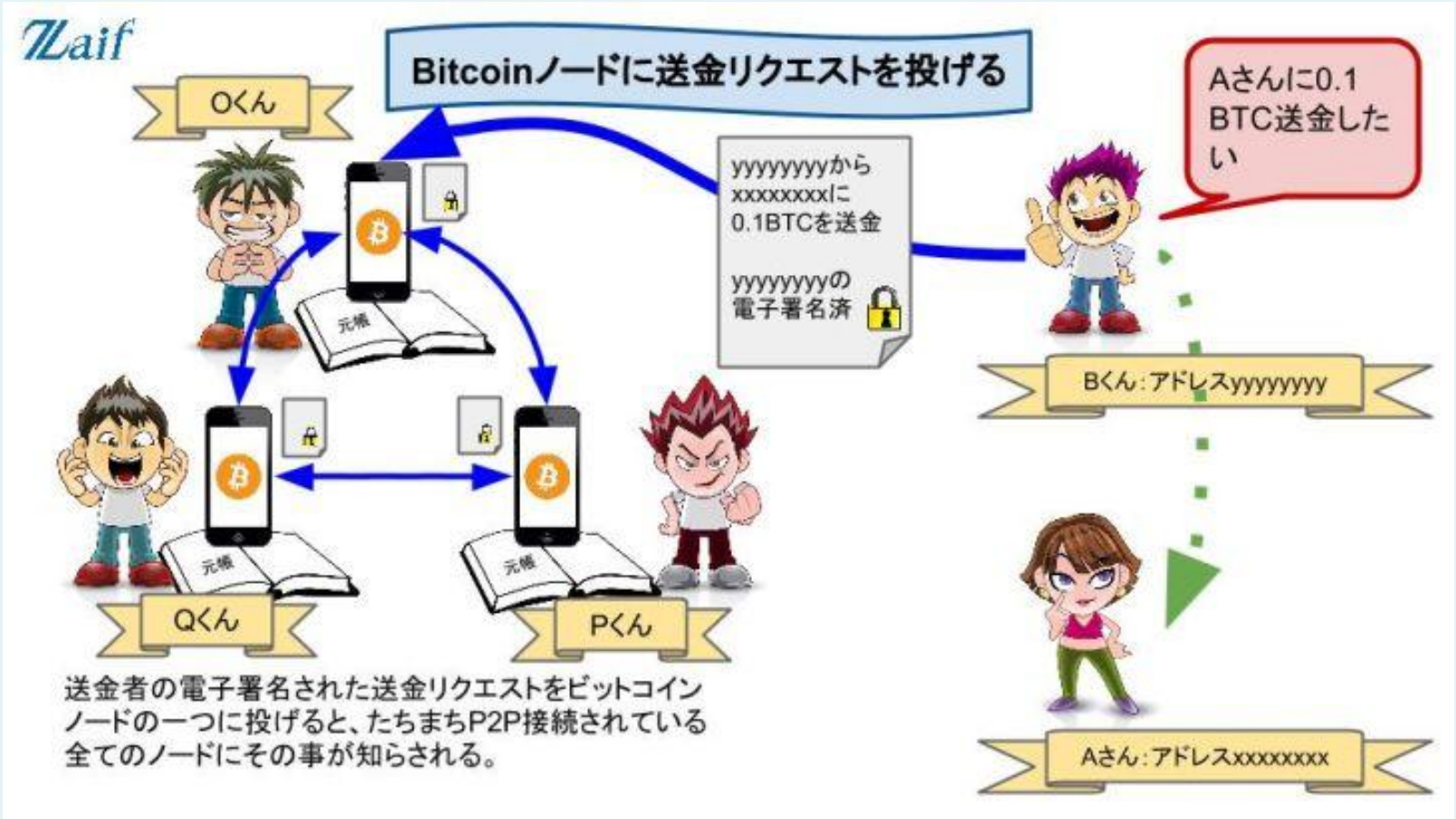
それをインストールすると、誰もがBitcoinのノードとなって運営できる。

ちなみに、元帳データも全部同期するフル機能のノードをFull Nodeと呼ぶ。

ビットコインの仕組み


Zaif
Bitcoinで使う「公開鍵暗号」
Bくんの「アドレス（公開鍵）」＝口座番号だから誰でも知ってる。
公
解錠！
Bくんのプライベート空間
yyyyyyyyから
xxxxxxxxに
0.1BTCを送金
yyyyyyyyより
?
yyyyyyyyから
xxxxxxxxに
0.1BTCを送金
yyyyyyyyより
Bくんの「アドレス」で開けたから、確かにBくんからの送金依頼だね！
このファイルはBくんの鍵でしか開けないけど、公開されてるBくんのBitcoinアドレスがそのままファイルを開く鍵になるから便利！
Bくんは「秘密鍵」＝暗証番号で電子署名
秘

ビットコインの仕組み


Zaif
Bitcoinノードに送金リクエストを投げる
Oくん
yyyyyyyyから
xxxxxxxxに
0.1BTCを送金
yyyyyyyyの
電子署名済
Aさんに0.1
BTC送金した
い
Bくん：アドレスyyyyyyyy
元帳
Qくん
Pくん
送金者の電子署名された送金リクエストをビットコイン
ノードの一つに投げると、たちまちP2P接続されている
全てのノードにその事が知らされる。
Aさん：アドレスxxxxxxxx

ビットコインの仕組み


Zaif
Bitcoin承認作業は連打パズルバトル？
元帳新規ページ
yyyyyyyy
- 0.1 BTC
xxxxxxxx
+0.1 BTC
お題:
Oくん
元帳
元帳最終ページ
お題:
00LhRlQs8A
このページは
僕が元帳に
足したい！
お題:
00LhRlQs8A
Nonce:
dK4L0k9GAb
計算結果:
Ui6fWK3w21
✖はずれ！
計算

ビットコインの仕組み


Zaif
パズルバトル勝者に賞金Bitcoin？
勝者だけが
自分が書いたページを
元帳にのり付けできる。
Pくん
元帳新規ページ
yyyyyyyy
- 0.1 BTC
xxxxxxxx
+0.1 BTC
zzzzzzzz（Pくん）
+25 BTC
お題:00ue7EG pV
元帳
元帳最終ページ
お題:
00LhRIQs8A
頭の「00」がそろったから正解！？
正解者の計算結果が、そのまま次の
バトルのお題に！
お題:
00LhRIQs8A
Nonce:
j63EzJ9ol1
計算結果:
00ue7EGxpV
計算
正解！
賞金25BTCゲット！

ビットコインの仕組み

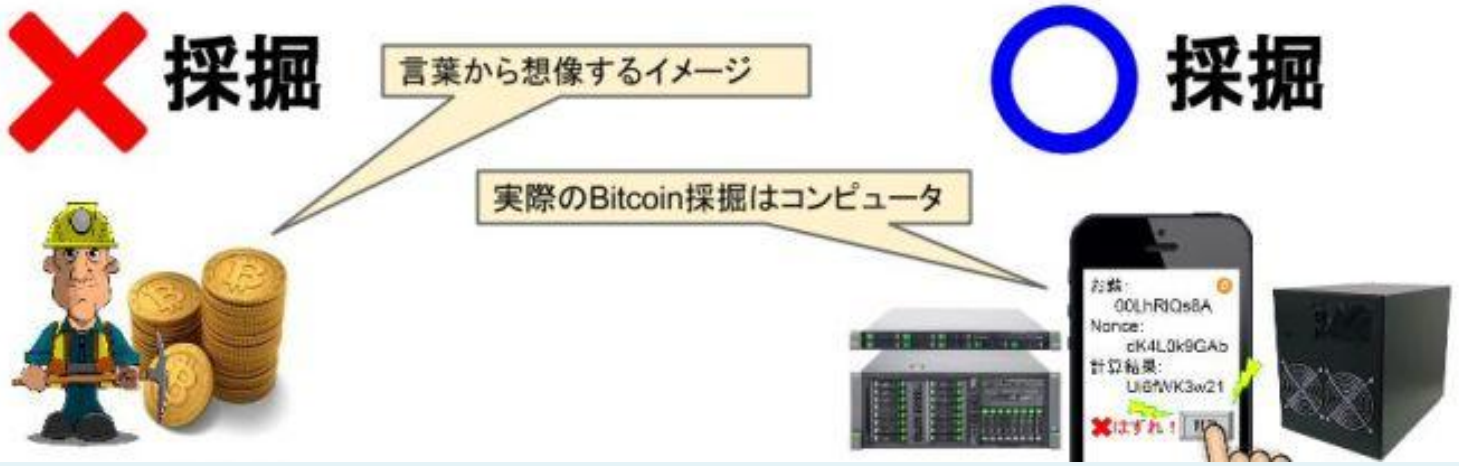
Zaif

採掘行為の正体は暗号パズルバトル

Bitcoin「採掘」といっても、本当に誰かが掘ってBitcoinを作っているわけではない。

実際は、新規に発行されるBitcoinを巡る、コンピュータ同士の暗号パズルバトル！
そのバトルが、送金リクエストを承認する作業の一部となっている。

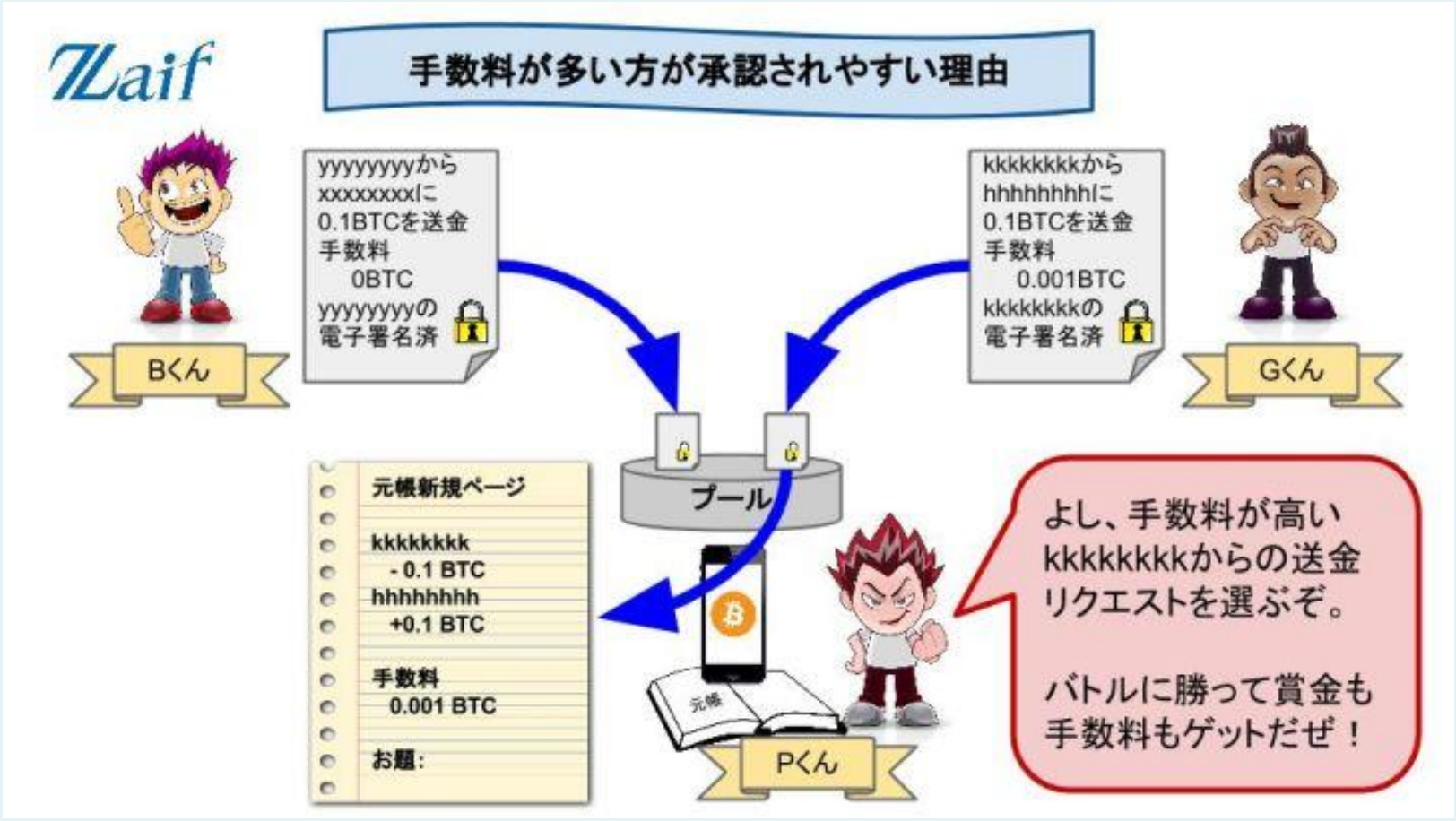
勝者は、送金リクエストをまとめた新規ページを作り、元帳に正式に採用される作業をする対価として、新規に発行されるBitcoinを受け取る仕組みになっている。



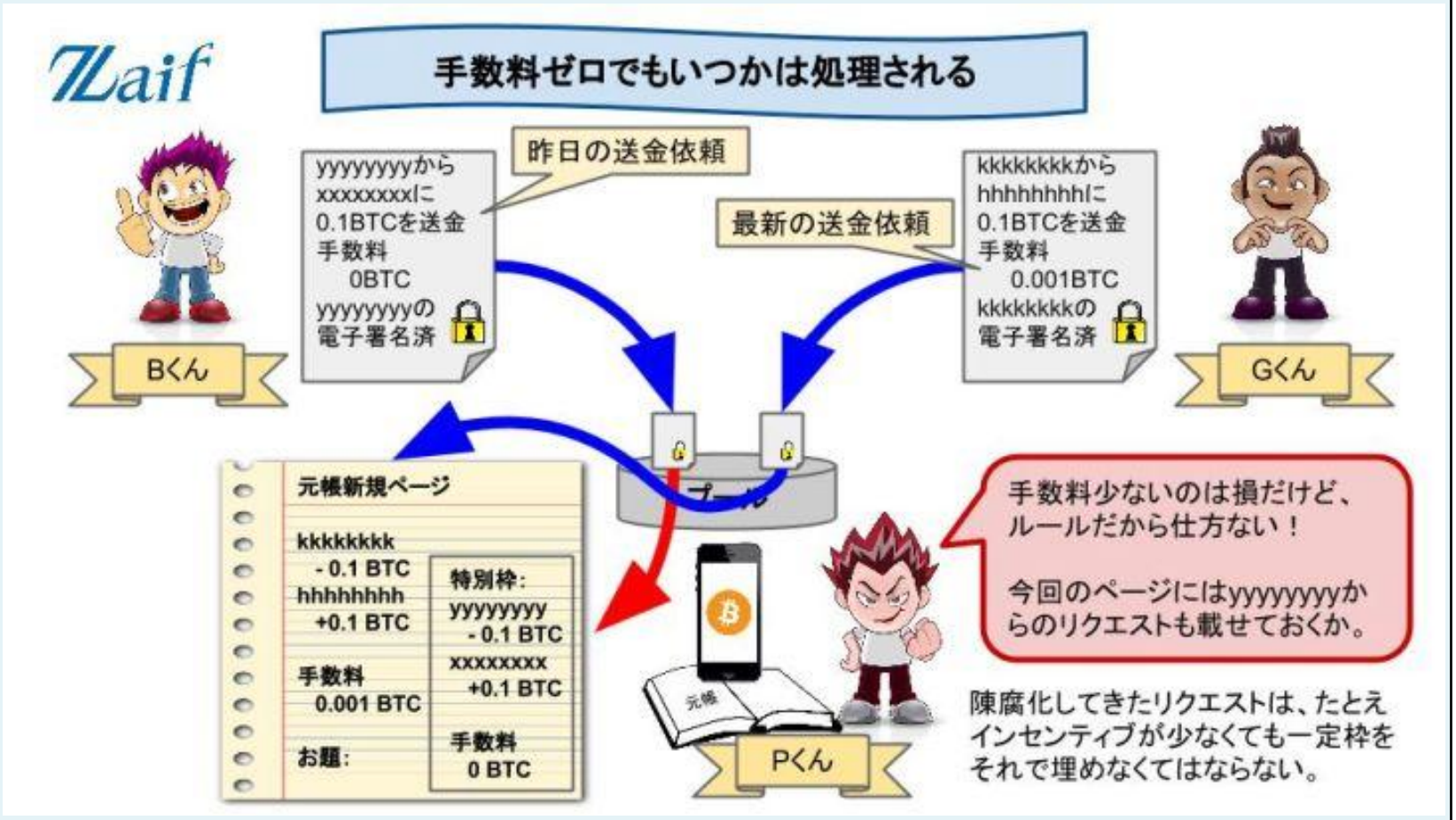
ビットコインの仕組み


Zaif
Bitcoin採掘は電気代が安い場所が有利
Oくん
Qくん
Pくん
電気代が高い国
VS
電気代が安い国
Sさん
Tさん
Uさん
電気代が高い国では、Bitcoin採掘の利幅が小さく、赤字の場合も多い。
その点電気代が安い国では、採掘専用機に多額の投資をしても回収できる可能性が高い。
このバトルは年々激しくなっている！
収益
コスト
（電気代）
収益
コスト
（電気代）

ビットコインの仕組み


Zaif
手数料が多い方が承認されやすい理由
yyyyyyyyから
xxxxxxxxに
0.1BTCを送金
手数料
0BTC
yyyyyyyyの
電子署名済
Bくん
kkkkkkkkから
hhhhhhhhに
0.1BTCを送金
手数料
0.001BTC
kkkkkkkkの
電子署名済
Gくん
プール
元帳新規ページ
kkkkkkkk
- 0.1 BTC
hhhhhhhh
+0.1 BTC
手数料
0.001 BTC
お題:
Pくん
よし、手数料が高い
kkkkkkkkからの送金
リクエストを選ぶぞ。
バトルに勝って賞金も
手数料もゲットだぜ！

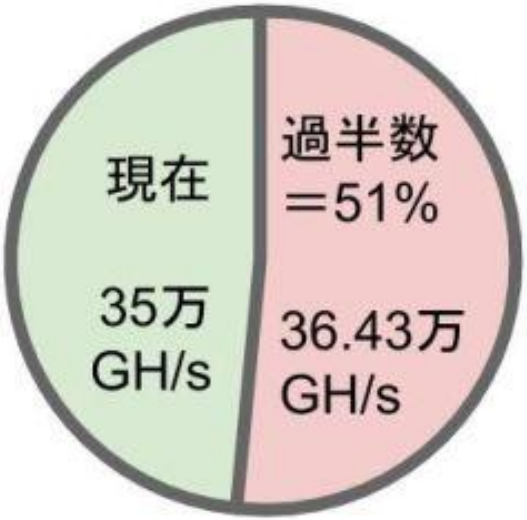
ビットコインの仕組み


Zaif
手数料ゼロでもいつかは処理される
昨日の送金依頼
yyyyyyyyから
xxxxxxxxに
0.1BTCを送金
手数料
0BTC
yyyyyyyyの
電子署名済
最新の送金依頼
kkkkkkkkから
hhhhhhhhに
0.1BTCを送金
手数料
0.001BTC
kkkkkkkkの
電子署名済
Bくん
Gくん
プール
元帳新規ページ
kkkkkkkk
- 0.1 BTC
hhhhhhhh
+0.1 BTC
手数料
0.001 BTC
お題:
特別枠:
yyyyyyyy
- 0.1 BTC
xxxxxxxx
+0.1 BTC
手数料
0 BTC
Pくん
手数料少ないのは損だけど、
ルールだから仕方ない！
今回のページにはyyyyyyyyか
らのリクエストも載せておくか。
陳腐化してきたリクエストは、たとえ
インセンティブが少なくても一定枠を
それで埋めなくてはならない。

ビットコインの仕組み

Zaif

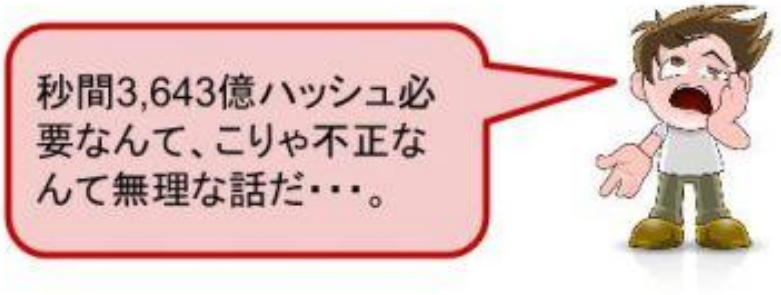
Bitcoinで不正を働くには？



2015年3月25日現在、ビットコインの採掘に費やされているハッシュレートは35万GH/s
＝秒間3,500億ものハッシュが計算されている。

不正をするためにBitcoinの元帳を書き換えるには、現在採掘に費やされている前計算能力（ハッシュレート）の過半数（51%以上）を超えなければならない。

新規参入をして今から不正を働くには、実に3,643億ハッシュを毎秒生成できる環境を整えねばならない。



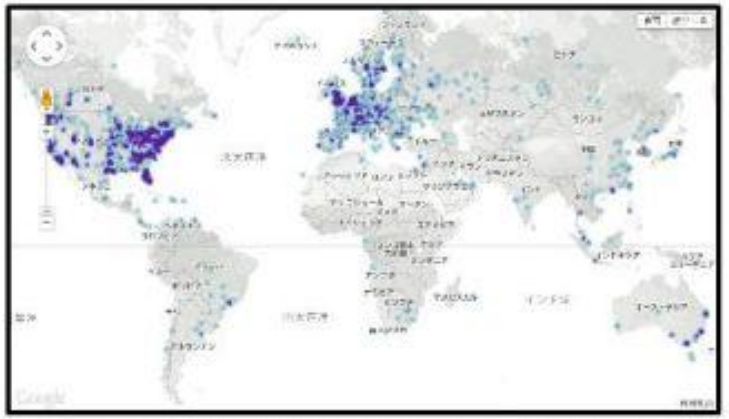
ビットコインの仕組み

Zaif

Bitcoinのデータを消し去るには？

銀行では、データが保管されている場所が破壊されれば、そのデータは全部消えてしまう。

Bitcoinの場合、世界中のノードが同じ元帳データを保管しているから、物理的に破壊することが不可能。



世界中に存在するビットコイン・ノードの分布図
BITNODES https://getaddr.bitnodes.io/ より。

ビットコインの仕組み

Zaif

元帳が複数種現れたらどちらが本物？

Bitcoinでは、たとえ元帳が複数種に分岐（Fork）
しても中身なんて精査しない。
とにかく、「ページ数が多い方が正しい」とする。

ビットコインの仕組み

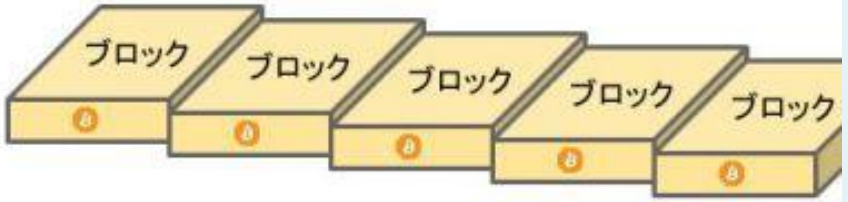
Zaif

Bitcoinの「ブロックチェーン」とは？

「ブロックチェーン」＝単にBitcoinの「元帳」のこと。
1「ページ」が、1「ブロック」と呼ばれる。

説明用のたとえ

ブロックチェーン



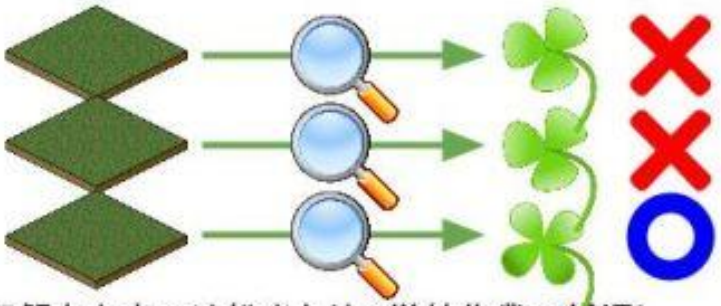
ビットコインの仕組み

Zaif

BitcoinのProof of Workとは？

広大な野原で四つ葉のクローバーを探すたとえ

四つ葉を見つけなさい。



正解を出すのは総当たりで単純作業の繰返し

検証するのは見つけたクローバーを目で見るだけで簡単にできる。参加者が増えて10分に1枚以上見つかるようになれば、葉の数を増やす。

ビットコインのProof of Work（Hashcash）

00LhRlQs8A（本ブロックのお題）＋

正解を出すのは総当たりで単純作業の繰返し

検証するのは同じ暗号プログラムに通すだけなので簡単にできる。採掘者が増えて10分に一人以上勝者が出始めたら、ゼロの数を増やす。

ビットコインの仕組み

Zaif

Bitcoinの特徴

- 電子マネー決済システムである
- オープンソースで誰でも精査できる
- アドレスは何個でも自分で作れる
- 「公開鍵」と「秘密鍵」が口座情報
- 誰でもインストールできる
- 取引データは全て一般公開
- 取引の透明性が高い
- オフラインでも送金依頼が作れる
- 簡単には盗めない
- 消したくとも消せない
- 中央管理者がいない（Decentralized）
- ビットコイン＝P2Pネットワーク
- 改ざんできない

- 個人情報の登録なしに使える
- 世界中の誰に向けても送金できる
- 勝手に残高が減らされることはない
- 採掘＝賞金承認の暗号パズルバトル
- 新規発行分は採掘者に与えられる
- 手数料もすべて採掘者に支払われる
- 手数料無料でも送金できる
- 手数料が高いものは優先される
- 手数料ゼロでも遅れて承認される
- ビットコインは止められない！

ビットコインの状況と仕組み

2018年1月6日（土）

柏ビットコイン普及協会理事　中村

仮想通貨について（ビットコイン）

１．初めに

ビットコインの基礎は「ナカモト論文」（中本哲史（ナカモトサトシ）2008年10月）である。
（ナカモトは英語をネイティブとしており日本人の可能性はないと考えられている。
　自ら採掘した100万BTCを保有していると言われている。）
ここで「１つの電子コインは、連続するデジタル署名のチェーン」と定義されている。
ビットコインを理解している人は少ない。従い将来に与える影響も理解していない。
ﾌｨﾝﾃｯｸ（ﾋﾞｯﾄｺｲﾝ含む）は現在の銀行ｼｽﾃﾑを破壊する力を持っている！！（現銀行の凋落の始まり）

２．通貨の特徴

①第三者機関を必要としない直接取引の実現
②非可逆的な取引の実現
③少額取引における信用コストの削減
④手数料の低コスト化
⑤二重支払いの防止

・世界中のビットコイン取引は、過去から現在に至るまですべて公開
・どのウォレット（ビットコインの財布）にいくら入っているかもわかる
・しかし、匿名性が極めて高い
・誰でも自由にいつでもウォレットを持てる
・銀行のようなシステム管理者はいない
・送金手数料が非常に安い
　（P2Pにより個人から個人への直接送金ができる。銀行や通貨交換所を通す必要がない）

仮想通貨について（ビットコイン）

３．ビットコインは通貨ではない。

プラットフォームだ！（ブロックチェーン）

管理体制が不要となり取引コストが大幅に低下する。→取引量が増大する。

・ブロックチェーンを用いた取引を金融資産一般に拡張。

個人が株や債券を証券会社を通さずに直接売買する。→証券市場、証券会社が不要となる。

現に外国為替は相対で取引されている。

・自動車や電気製品などの耐久消費財や不動産などの所有権移転に拡張。

４．税制など国の機関制度への深刻な挑戦

ビットコインのは匿名性から取引と個人や組織との対応関係が分からない。

税務署はビットコインでの取引を把握できない。

従い正直者は申告し税金を払うが、不正直者は申告せずに税金を払わない。

これにより不公平が生じるとともに税制度が破たんする。

仮想通貨（ビットコイン）の特徴（1）

種類	発行・管理	信用元	利点	欠点
通常の通貨	中央銀行/国	同左		
電子マネー	特定の企業	同左	管理が必要で、運用コストがかかる。（例:店舗側が売り上げの2～4%かかる） **特定通貨にリンクしており、国際送金に使用できない。**	
ビットコイン	無し	**ブロックチェーン**		

	通常の通貨	**ビットコイン**
送金手数料	先進国：送金額の2～3% 開発途上国：上記以上、または銀行システムがないため送金不可能	世界どこでも0に近い→コンテンツの切り売りが可能 新聞、書籍、雑誌、CD,DVD,映画など
導入コスト		特別な費用は無い
支払い時間	0	約10分かかる

参考；
●オンラインショッピング市場 家計消費の約3%（アメリカも同様）
●貿易決済 送金手数料、為替スプレッドが大きい。これがほぼ0になる。
●問題点
1）取引は追跡できるが、それを現実の個人や企業にむすびつけることは難しい
2）私設両替所など関連サービスの信頼性が確保されていない （→2017年4月に仮想通貨法が施行された）
3）ドルや円との交換価値が乱高下する →保有資産手段としてではなく送金手段として使用する。
多額の残高を長期の保持しない。
4）ハッカー攻撃の危険あり　など

仮想通貨（ビットコイン）の特徴（1-1）

小売店が導入するときの条件

クレジット	ビットコイン
①クレジット会社による審査に通る必要がある	不要
②SSL認証を得る必要がある	不要
③利用手数料（2～4%）が必要（売り手が負担	低コスト（1%）

仮想通貨（ビットコイン）の特徴（２）

◆ネットワークの中核を担う企業や政府の大型サーバーなしにすべての端末が対等な関係にあるP&Pの電子通貨システム
◆ 2017年9月末時点で世界で稼働しているサーバは約9,200台。
例：北朝鮮から日本に核攻撃があれば日本の銀行口座は全滅であるがビットコインはびくともしない！
ビットコインのブロックチェーンは2009年以降24 時間365 日の連続稼働を続けている。
◆銀行などを介さずに政府に知られることなく個人または企業間で直接、電子的に送金できる。
◆国や中央銀行のような管理者が不在で、信用の裏付けがなく、匿名性が高いインターネット上の通貨である。
◆匿名性が高く犯罪（ブラックマネー）に利用される可能性大
◆国の金融政策が効かない。（例：日銀の金利調整による経済の調整ができない。）
◆仮想通貨の取引量に占める日本の割合は世界1位。
2017年10月の取引量（日本円：42%、米ドル:36%、2016年度は中国元が90%）
◆ネットワーク上にのみ存在する仮想通貨で紙幣や硬貨は存在しない。
◆中央の管理者は置かないが、偽造や不正な取引を排除する仕組みがある。（ブロックチェーン）
◆送金時の手数料は自分で決める。ただでも良い。（円の送金は銀行が手数料を決める。）
◆決済方法
店舗側はタブレット又はスマホの画面に表示したQRコードを自分のスマホで読み取り内容を承認するだけ。
◆法律的にはビットコインは通貨ではなく物として扱われる。決済手段としても使える。（金（ゴールド）と同じようなものである。）

仮想通貨（ビットコイン）の特徴（3）

◆ビットコインで決済が可能な国内約1万店舗
（ビックカメラ、HIS・・・・・　）
◆ビットコイン決済は設備投資が不要
専用アプリをダウンロードするだけ。
店舗側が負担する手数料は決済金額の1%が基本。
（クレジットカードの場合は3～8%と高い）
◆2017年12月10日にシカゴ・オプション取引所（CBOE)で先物取引が開始。
◆三菱東京UFJ銀行が2018年度中に仮想通貨MUFGｺｲﾝを発行予定。(1ｺｲﾝ=1円固定）
◆みずほﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟは2020年までにJコインを実用化を計画。（全国の銀行が参加）

デジタル通貨をめぐる銀行の取り組み

	仮想通貨系			電子マネー系
名称	MUFGコイン	内外為替一元化コンソーシアム	ブロックチェーン連携プラットフォーム	Jコイン
提供者	三菱UFJフィナンシャル・グループ	SBIホールディングス	全銀協、富士通、ビットフライヤーなど	みずほフィナンシャルグループ
特徴	決済などに使える銀行版の仮想通貨。価格は1コイン＝1円で固定	リップルの技術を使った決済システム。来年春以降の実用化を目指す	既存の決済インフラでブロックチェーン技術を応用するための実験場	仮想通貨ではなく電子マネー。2020年の実用化を目指す
課題	法に触れる可能性あり	地銀の足並みそろわず	実用化のめどは全く立たず	従来サービスとの差別化が難点

仮想通貨（ビットコイン）の特徴（4）

◆ブロックチェーンを使用した銀行送金

銀行送金に仮想通貨技術、手数料大幅引き下げへ

2018年01月04日 07時10分　ツイート　おすすめ 162　G+　B! 2

仮想通貨の基盤となる「ブロックチェーン」技術を使い、銀行間の送金手数料を大幅に安くできるサービスが今年３月にも一部の銀行間で始まる見通しとなった。

手数料は１０分の１程度に下がる可能性がある。金融とＩＴを組み合わせた「フィンテック」が、個人の生活に恩恵をもたらす具体例となる。

国内メガバンクや、りそな銀行、地方銀行など約６０の金融機関がすでに実証実験を済ませた。このうち、インターネット銀行や地銀など数行が３月にも、スマートフォンのアプリを使って手軽で安価に送金できるサービスを開始する。参加する銀行は、順次増える見通しだ。

送金手数料は各行が決めるが、最も安くした場合は現在数百円の手数料を１０分の１程度に引き下げることもできるという。

仮想通貨（ビットコイン）の特徴（５）

◆キャッシュレス社会

スマホ決済が主流に。

◆中国の2016年スマホ決済が660兆円。（2年で6倍）

（2017年1月～9月：71兆元（約1,000兆円）

結婚式のご祝儀、乞食への施し、お賽銭、小さなお店（飲食店、八百屋・・・）、

友達間の送金、中国観光客の白タク激増。

◆金融機関の未来（2017年6月「未来投資戦略2017-Society5.0の実現に向けた改革－」

・手形・小切手・公金収納の電子化と効率化

・オープンAPIの導入　2020年までに80行以上の銀行でオープンAPI導入を目指す。

（139行（都市銀行・信託銀行・地方銀行・第二地方銀行の合計）

・キャシュレス化の推進

2027年までにキャッシュレス決済の約4割を目指す。（約120兆円）

キャッシュレス化率（日本≒2割、韓国≒9割）

仮想通貨（ビットコイン）の特徴（６）

◆今の形態の銀行は無くなる。
　・決済、貸付の大きな機能が銀行以外が主流になる。
　　銀行に行く必要がなくなる。支店は激減する。（ATMは無くなる。）
　　（ATM:2017年9月時点で約20万台（コンビニ型を含む）で年間管理運用費約2兆円）
　・全て電子決済になり、確定申告が不要になる。脱税が出来なくなる。
　　→・全てスマホ決済になる。スマホを持たないと生活ができなくなる。
◆銀行の現システムは負の遺産。
　●支店、ATMなどお資産が負の資産になっている。
◆イギリスで過去2年間に銀行の1,000店舗を閉鎖した。
◆アメリカでは2009年～2016年年平均で銀行の1,129店舗を閉鎖した。
◆スウエーデン　2012年にサービスが開始されたSwish(中央銀行、大手銀行が開発したモバイル決済の仕組みで銀行口座と連動してP2P送金、ショッピング決済ができる）は2017年では国民の50%、30歳以下では90%が使用している。大手Nordea Bankは支店での現金取り扱いを廃止し、の1000店舗を閉鎖した。
　又、中央銀行が仮想通貨を検討中。
◆2017年11月に南米ウルグアイで中銀が国家版仮想通貨「eペソ」発行した。

仮想通貨（ビットコイン）の特徴（7）

◆仮想通貨の規模は約30兆円（2017年12月時点）、22兆円のトヨタを超える。
◆拡大スピードが急激
　特に2017年8月に分裂が起きてからはバブル状態

◆現在は投機対象となり、本来の決済機能が無視されてしまっている。
　→将来的には決済機能が無くなる？？？？

おまけ
◆ナカモトサトシ探し
　本人であることの唯一の証明
　ブロックチェーンの最初のブロックに署名された“秘密鍵”を持っていること。
◆ビットコインでの最初の買い物
　2010年4月に1万ビットコインでピザ2枚を購入した。
　（2017年の価値で200億円でピザ2枚）

ビットコインの新規発行について

1. 各国の貨幣

諸情勢を考慮して**中央銀行が発行する**。
国の信頼度が保証

2. 金

金鉱脈から金を採掘
現物（金そのもの）が保証

3. ビットコイン

マイニング（採掘） これが面白い！！！
保証するものはない！（ブロックチェーンの仕組み自体が保証する）

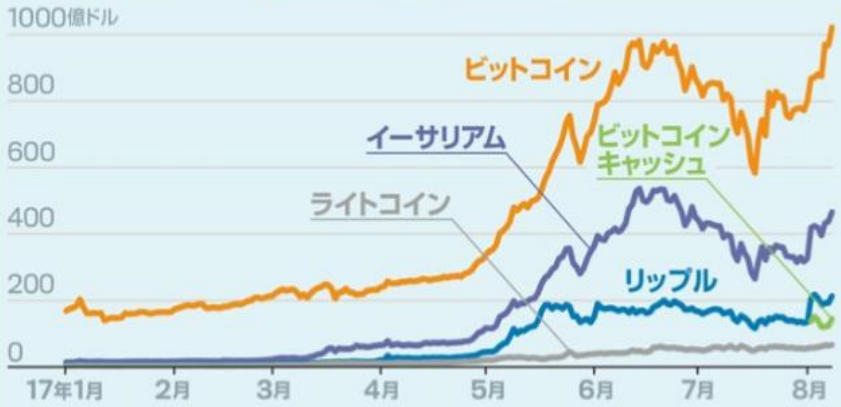
仮想通貨（ビットコイン）価格の推移

2017年12月7日15,000ドルを超えた（時価総額2,500億ドル）

膨張する仮想通貨の市場

2010年にピザ2枚と1万BTCを交換したのがビットコインを使った初の決済とされる。それから7年、仮想通貨市場はここまで膨れ上がった。

流れ込むマネー ■仮想通貨の時価総額推移

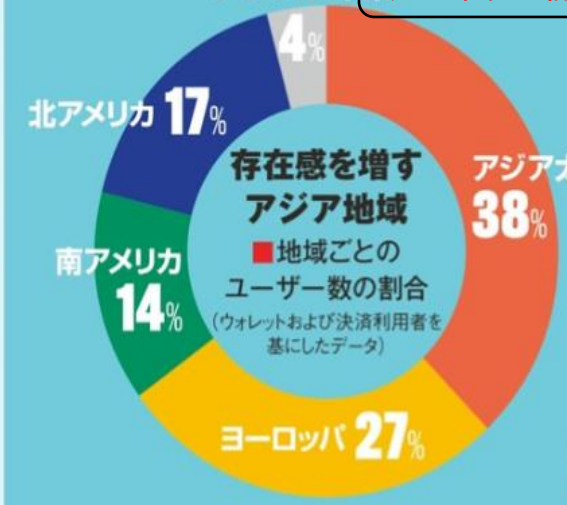


「ビットコイン」だけじゃない ■時価総額ランキング（11月10日現在）

1位	ビットコイン	1185億1000万ドル
2位	イーサリアム	304億6000万ドル
3位	ビットコインキャッシュ	137億5000万ドル
4位	リップル	83億1900万ドル
5位	ライトコイン	34億8400万ドル

（ビットコインキャッシュは11月初め3位に浮上）

2017年11月20日8000ドルを超えた（2016年末比8倍）



7459ドル（17年11月8日）

2017年11月29日10,000ドルを超えた

709ドル（16年11月8日）

443ドル（16年1月4日）

1年間で価値は10倍に

■ビットコイン価格の推移

16年1月　7月　17年1月　7月

仮想通貨の種類と時価総額

仮想通貨の時価総額ランキング

2017年10月10日時点

	仮想通貨	時価総額（ドル）	1単位当たりの価格（ドル）	備考
1	ビットコイン	800億9300万	4820.72	「サトシ・ナカモト」が生み出したとされる、世界初のブロックチェーン技術を利用した仮想通貨
2	イーサリアム	283億8000万	298.64	ヴィタリック・ブリテン氏が開発。取引データ以外にも、契約をブロックチェーンに埋め込める（スマートコントラクト）点に特色
3	リップル	95億800万	0.24	米グーグルが米リップルラボに出資したことで人気に火。国際送金システムに応用すべく研究が進められている
4	ビットコインキャッシュ	55億9600万	335.52	2017年8月にビットコインから分裂。ブロックサイズの上限を拡張してデータ処理速度の向上を図った
5	ライトコイン	26億9700万	50.61	元グーグルのエンジニアが開発したアルトコイン（ビットコイン以外の仮想通貨）の先駆け。送金にかかる時間をビットコインの4分の1に短縮
6	ダッシュ	22億500万	289.75	匿名性を高めたダークコインから名称を変更。「ダークセンド」という送金機能で送金元などの匿名化が可能
7	ネム	18億7400万	0.20	当初、開発チームに日本人がいたことで話題に。「富の再分配」を重視し、ネムのやり取りが活発な人に報酬を分配
8	ネオ	14億6400万	29.29	イーサリアムの技術を応用して、中国で開発されたアルトコインとして15年に登場。スマートコントラクト機能などを有する
9	モネロ	13億2900万	87.49	匿名性を強化したアルトコインとして14年に登場。ダッシュが取引情報をミックスするのに対して、モネロは分散によって匿名化
10	アイオータ	12億7100万	0.45	IoT（モノのインターネット）に最適化されたアルトコインとの触れ込みで16年7月に開始。送金手数料を完全無料化

（注）10月10日時点の数字。時価総額は10万ドル以下は切り捨て。1単位当たりの価格は小数点第3位以下は切り捨て
（出所）Coin Market Capデータより筆者作成

ダークウエブ（Silk Roadなど)

ダークウエブ
（発信元、送信先が追跡できない）

麻薬、武器、殺人依頼など違法商品が満杯

2011年に“Silk Road”サイトが開設

一般ウエブ

一般のブラウザーでアクセス
（IE,エッジ、クロム・・・）

Tor(The Onion Router（タマネギルーター）)ブラウザーでアクセス

Silk Raodサイトではビットコインでしか取引できない。
↓
ビットコインが注目され価格が大幅上昇した。

ビットコインに使われている大きな2つの技術

1. 暗号化技術

SSL（Secure Sockets Layer）暗号化を使用
（旧：1つの共通鍵を使用するのに対して、秘密鍵と公開鍵の2つを使用する）
例；
インターネットショッピングなどで個人情報（ｸﾚｼﾞｯﾄｶｰﾄﾞなど）を送る場合など
（ URL:https://www.amazon.co.jp/　頭に鍵マークがついている。）

2. ブロックチェーン（分散型台帳）

ブロックチェーンは現在の基本的な仕組みを変える可能性が大である。

過去の全取引が多数のコンピュータに記録されている。
（偽造貨幣、二重取引を排除し改ざんもできない。）

内容は一般に公開されている。→コインの使用者は問題がないかを
確認することができる。

ビットコインの仕組み（基本用語-1）

1．基本用語（これを理解すれば仕組みが分かる）

① 公開鍵
　秘密鍵から計算される。
② 秘密鍵(署名）51個の数字と記号の組み合わせ。
紛失（ハードディスク障害など）、盗難（ハッカー攻撃でPC内の秘密鍵を盗まれるなど）の危険性あり。無くすとそれに対応したビットコインは永久に失う。対策としてバックアップは必須。ハッカー攻撃を考えると紙の財布が推奨されている。（PCに保存せず、紙に書いて保存する。）

ビットコインの仕組み（基本用語-2）

③ 公開鍵暗号

対になる2つの鍵を使ってデータの暗号化・復号を行う暗号方式。
公開鍵暗号では暗号化に使う鍵と復号に使う鍵が分離されており、暗号化に使った鍵で復号を行うことはできず、片方からもう一方を割り出すことも容易にはできないようになっている。鍵の持ち主は復号に使う鍵のみを他人に知られないように管理し、暗号化に使う鍵は公開する。このため、暗号化に使う鍵は公開鍵、復号に使う鍵は秘密鍵と呼ばれる。
公開鍵暗号で秘密のメッセージを送受信する場合、送信者は受信者が公開している公開鍵を入手して暗号化を行う。暗号化されたメッセージは受信者の持つ秘密鍵でしか復号できないため、途中で第三者に傍受されても中身を解読されることはない。
公開鍵暗号が考案されるまでは、暗号と言えば暗号化と復号に同じ鍵を用いる秘密鍵暗号（共通鍵暗号、対称鍵暗号）しかなかった。秘密鍵暗号ではメッセージの送信者と受信者が同じ鍵（暗号表など）を共有する必要があるため、鍵を安全な経路で相手に届けなければならない。公開鍵暗号では暗号に使う公開鍵は第三者に知られても解読されないため、鍵の安全な輸送が必要なく、安全性も高い。
公開鍵暗号は秘密鍵暗号よりも処理が複雑になりがちであり、より多くの計算資源や時間を必要とする。このため、暗号通信に利用する場合は、実際の通信内容の暗号化には即興で鍵を生成した秘密鍵暗号を使い、その鍵を送信者と受信者の間で安全に交換するために公開鍵暗号を使うといった使い方をすることが多い。また、公開鍵暗号は非対称な鍵を用いる特徴から、デジタル文書の正当性を保証するデジタル署名にも応用されている。
公開鍵暗号を実装するための具体的な暗号方式はいくつかの方式が提案されている。最も有名なのは、巨大な整数の素因数分解の困難さを利用したRSA暗号で、現在では様々な分野で利用されている。他に、離散対数問題の解の困難さを利用したElGamal暗号、楕円曲線上の離散対数問題を利用した楕円曲線暗号などがある。

注）公開鍵、秘密鍵、アドレスは生成プログラムをダウンロードして自分で作ることができる。普通は両替所やウォレットのサービスで取得する。
ウォレット作成サービスは、さまざまなサイトで提供されている。

ビットコインの仕組み（基本用語-3）

③ アドレス（銀行の口座番号に対応する、公開鍵に対応）
27～34個の数字とアルファベットの組み合わせで、1 or 3で始まる。鍵から何度かのハッシュ計算により生成される。秘密鍵からいくらでもアドレスを生成できる。過去のアドレスは生きている。安全のために取引毎に異なるアドレスを使用するのが良いとされている。

④ ウォレット(財布、秘密鍵に対応）
ディスクトップ、モバイル、オンラインのものがある。ただ鍵のデータがあるだけである。
残高などのデータはブロックチェーンにあり、それをダウンロードして残高が分かる。Aから送られたかを確認するためには、Aから送られた署名をAの公開鍵で復号して行う。

注）公開鍵、秘密鍵、アドレスは生成プログラムをダウンロードして自分で作ることができる。普通は両替所やウォレットのサービスで取得する。
ウォレット作成サービスは、さまざまなサイトで提供されている

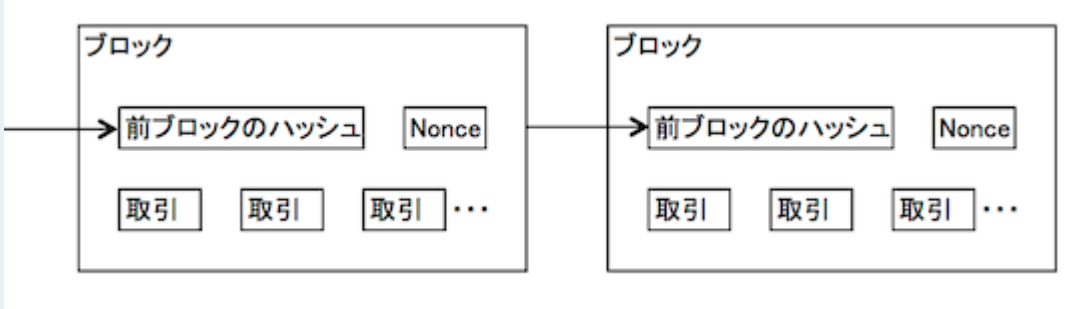
⑤ブロック
ブロックは「ヘッダー」と「トランザクション」で出来ている。
・「ヘッダー」：直前のブロックの「ヘッダー」を圧縮した情報＋今回の取引リストを圧縮した 「トランザクション」情報＋次のブロックを作るための「ノンス」
・「トランザクション」：ある時間内に行われた全ての取引（Aさんの口座からBさんの口座にXビットコインが支払われた）の記録

ビットコインの仕組み（基本用語-4）

⑥ブロックチェーン 構造上以下の4つの特徴がある。

（1）改ざんが極めて困難（事務手続、取引のチェックや監査作業の大幅削減が可能）
（2）ダウンタイムが実質ゼロのシステム実現。現金融機関のシステムは二重三重の安全策が
　　とられており、非常に高価なシステムになっている。
（3）安価に構築可能
（4）高いセキュリティー

「ブロック」（Block）は、多数のトランザクションと、あとで説明する「ナンス」（Nonce）と呼ばれる特別な値、そして直前のブロックのハッシュを持っている。「ブロック」に含まれた取引のみを「正しい取引」と認めることにする。そして、ネットワーク全体で「唯一のブロックの鎖」を持つようにする。これによって、一貫した取引履歴を全体が共有できる、というのがブロックチェーンのコンセプトである。



ここで用いられるのが*「仕事の証明」(proof-of-work, PoW; プルーフ･オブ･ワーク)*と呼ばれる仕組みである。それぞれのブロックについて、SHA-256ハッシュを取ることを考える。このハッシュの先頭に、一定の数以上の0が並んでいるブロックのみを、「正しいブロック」として、ネットワーク全体で認めることにする。ブロックには、ナンスと呼ばれる特別な値が含まれている。ナンスを変えることで、ブロック全体のSHA-256ハッシュを変化させることができるので、条件を満たすようなハッシュを持ったブロックを作ることができる。

ビットコインの仕組み（基本用語-5）

注）具体的には、
①入力　ヘッダーを構成する3つ
・直前のブロックのハッシュ
・今回ブロックに記録する取引情報
・ノンス（ランダムな変数）
②出力　入力値からのハッシュ（これになれば正解）時期により異なる。例頭数桁が0となる。
発掘者はノンスを変えて正解の出力になる”ノンス”を得た場合に成功者
（採掘者＝ビットコインを得ることができる。）となる。多数の競合者からの勝者のなる。

SHA-256などのような暗号学的ハッシュ関数は、ハッシュ値から、簡単にデータを逆算できないように設計されている。したがって、全探索・総当り以外の方法で、条件を満たすようなナンスを探すことはできない。これは、計算資源を使わないと、条件を満たすブロックを生成することができないということである。これによって、ブロックの作成に「誰でも作成できる訳ではないが、特定の誰かのみが作成する権限を持っている訳でもない」という性質を持たせることができた。P2Pネットワーク上の各ノードは、ナンス値を変化させながら、全探索・総当りをし、条件を満たすブロックを発見しようと努力する。そして、これをみつけたノードは、そのブロックを他ノードに配信し、ネットワーク上の全てのノードがこれを認めるのである。
ブロック生成の難易度は、過去のブロック生成速度に応じて、およそ10分に1個のブロックが発掘されるよう、適切な値が設定されるようになっている。コンピュータの性能は爆発的に向上してきていることが知られている。これは、もし探索の難易度（つまり、ハッシュの先頭にいくつ0が必要か）が一定のままだとすると、やがてブロックはただ同然の計算資源で生成できるようになってしまうということを意味する。また、ネットワークに参加するノードが増えるにつれてブロックの生成速度が次第に速くなっていってしまうということも意味し、これも同様に望ましくない。したがって、難易度を変化させる必要がある。
実際のブロックチェーンのデータは、Blockchain.infoなどで閲覧することができる。以上の仕組みによって、中央を持たずとも、Bitcoinネットワークは正しいブロックチェーンを作り上げていくことができる。しかし、ここまでの仕組みだけでは、ブロックチェーンが絶対に分岐しないことを保証するには不十分である。そのためBitcoinは、分岐点から先がより長いほうのブロックチェーンを、常に正しいブロックチェーンとして認める、という規則を導入している。

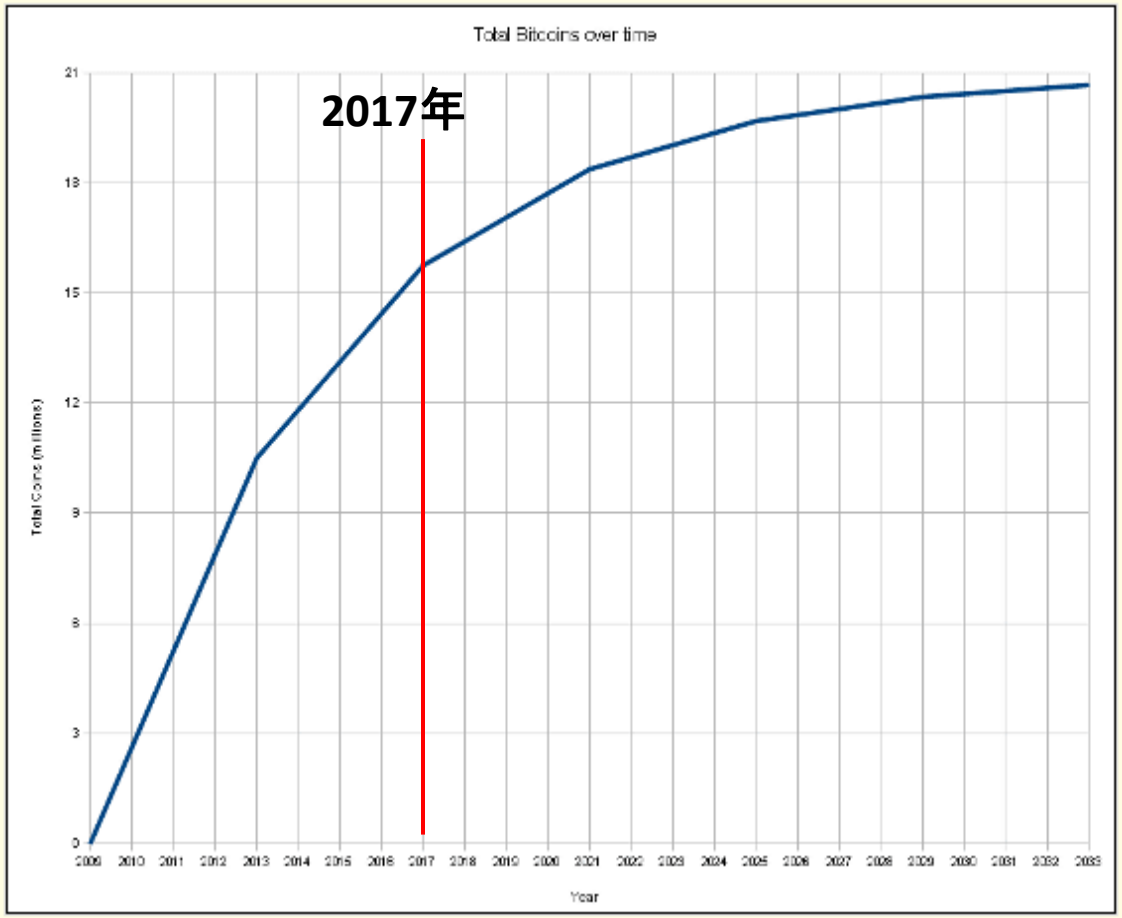
ビットコインの仕組み（基本用語-6）

⑦マイニング（採掘）

PCを持っている誰でもフリーソフト”miner"を使用してビットコインを作ることができる。
ただしマイニングの量は自動的にビットコインネットワークによって調整されて、総量は上限が決められている。
非常に強力なスペックのPCが必要（専用チップを搭載など）であり、PCの電気代は膨大で得られるビットコインでは賄えないとも言われている。「ブロックチェーン」の運営に貢献した人は報酬がもらえる、これが「マイニング」。
前の節で、ブロックの生成には計算資源を使う必要があることを説明した。しかし、ブロックの生成に見返りがなければ、わざわざコストをかけてコンピュータや機材を買って、ブロックを生成してくれる人はいないだろう。したがって、ブロックの生成には報酬がある。
報酬は、それぞれのブロックの先頭にある、コインベース（coinbase）と呼ばれる、特殊なトランザクションによって実現されている。このトランザクションは、誰かから誰かへのコインの譲渡を表すのではなく、コインの生成を表すトランザクションである。受取先はブロックの生成者である。この特殊なトランザクションのおかげで、ブロックを生成すると生成者は、一定額の定められたコインを報酬としてもらうことができる。
Bitcoinを金などの鉱物になぞらえたとき、ブロックの生成は採掘作業ともみなせる。よって、ブロックを生成することは一般に「マイニング」と呼ばれている。

ビットコインの仕組み

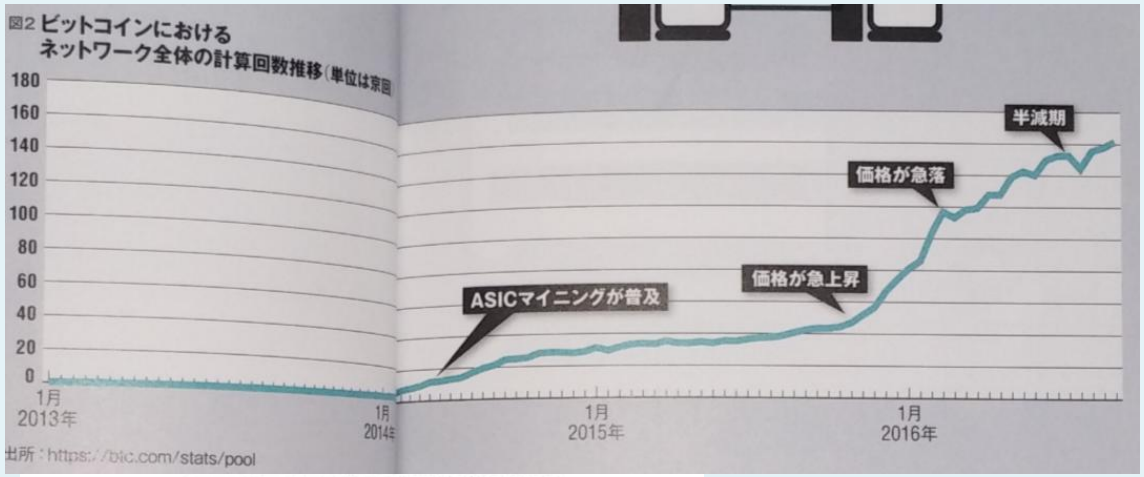
ビットコインのシステムリソースは、ビットコインクライアントを使ってマイニングをするエネルギーでまかなわれており、ビットコインは設定された2100万BTCのすべてが2140年中に掘り尽くされる予定です。



金は公式プールの3杯分、約21万トンと言われている。この21万に合わせたもの？

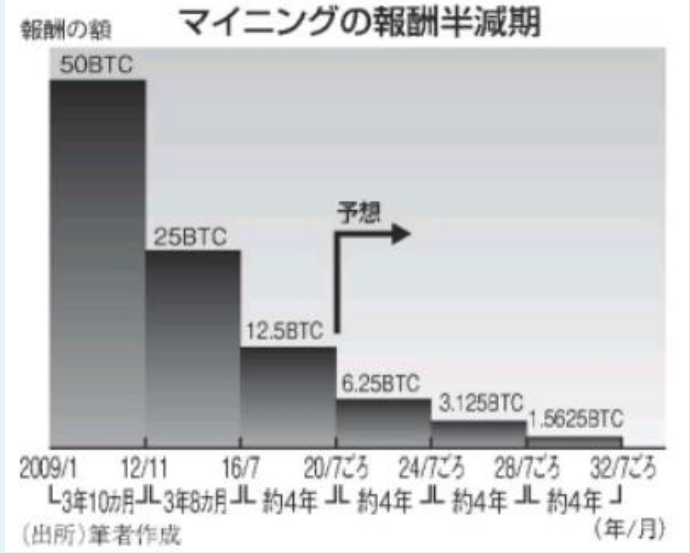
1ビットコイン（BTC)の１億分の1の単位はサトシ

ビットコインの仕組み



マイナーが行った計算回数（京回/秒）
イメージとしてMacBookAir1台で現在の条件の解を見つけるのに155万年かかる。

ASIC（Application Specific Integrated Circuit：特定用途向け集積回路）：一般デスクトップパソコンの100万倍以上の計算能力



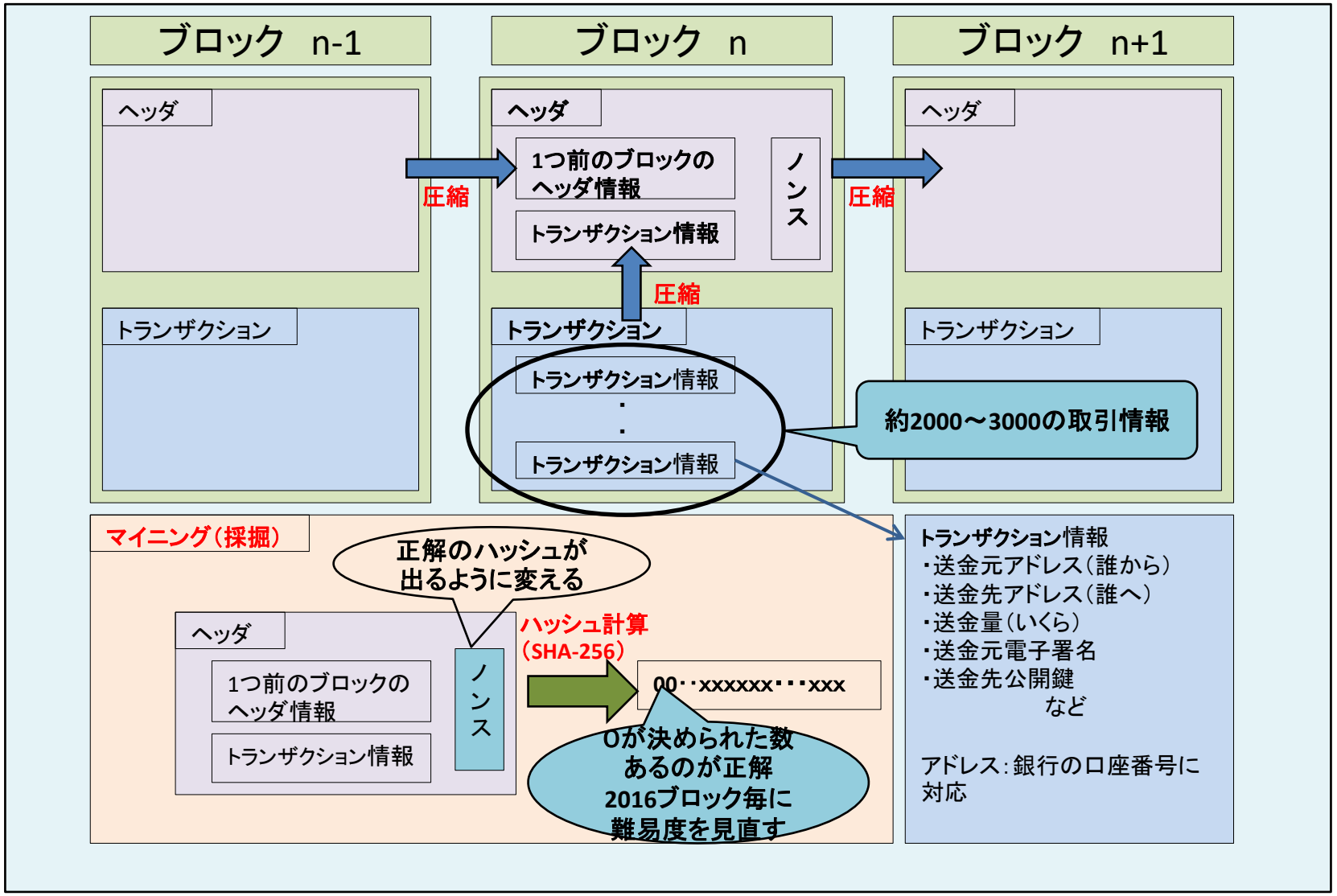
半減期：マイニングの報酬額を約4年間毎に半分にする。

マイニングに使用される電力（予想）2016年～2017年年間336万メガワット時（アメリカの平均家庭30万世帯分（約大型原発0．4基分）

マイニング業者

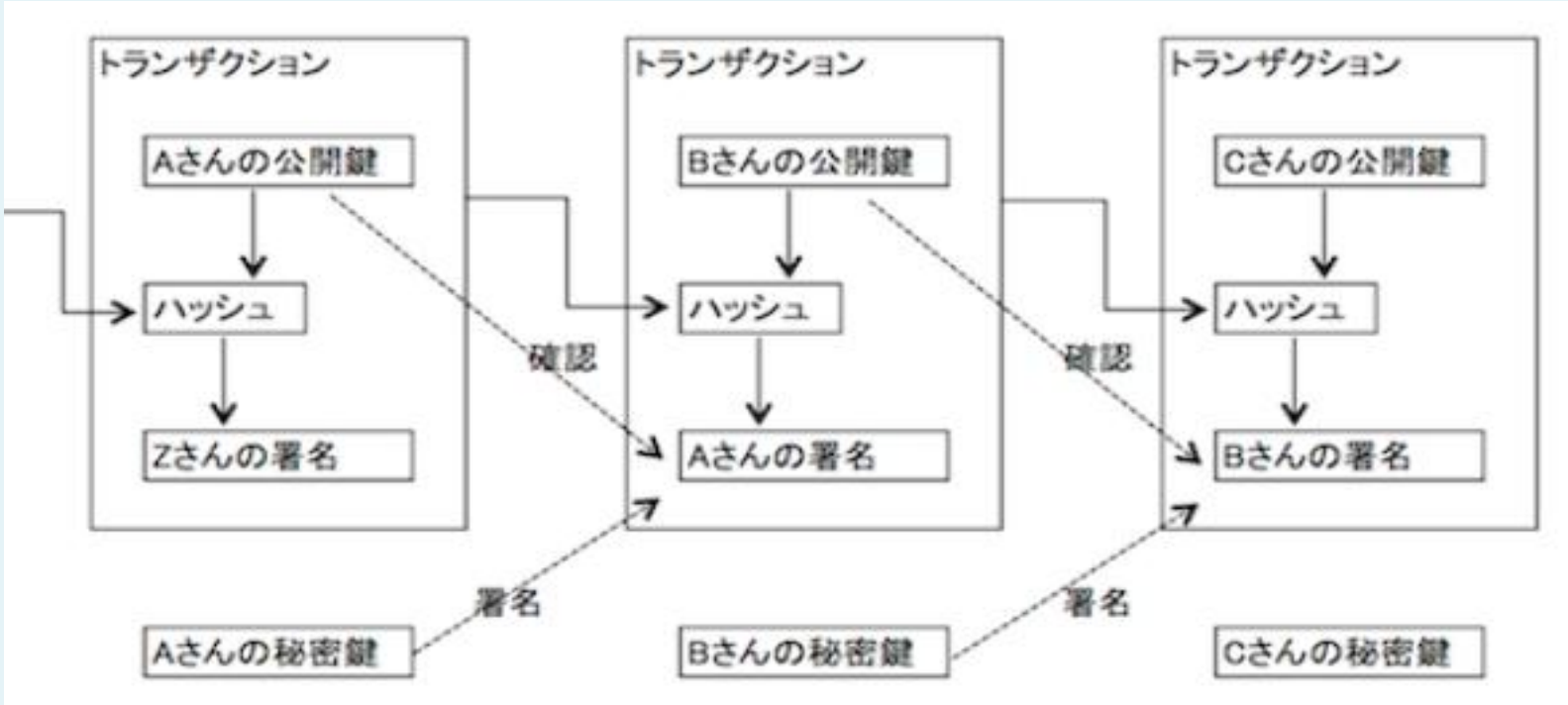
宝の山
中国のビットマイン・テクノロジーズが所有するビットコインの採掘施設

ビットコインの仕組み


ブロック　n-1
ブロック　n
ブロック　n+1
ヘッダ
1つ前のブロックの
ヘッダ情報
トランザクション情報
ノンス
圧縮
圧縮
圧縮
トランザクション
トランザクション情報
・
・
トランザクション情報
約2000～3000の取引情報
マイニング（採掘）
正解のハッシュが
出るように変える
ハッシュ計算
（SHA-256）
00‥xxxxxx‥‥xxx
0が決められた数
あるのが正解
2016ブロック毎に
難易度を見直す
トランザクション情報
・送金元アドレス（誰から）
・送金先アドレス（誰へ）
・送金量（いくら）
・送金元電子署名
・送金先公開鍵
など
アドレス：銀行の口座番号に
対応

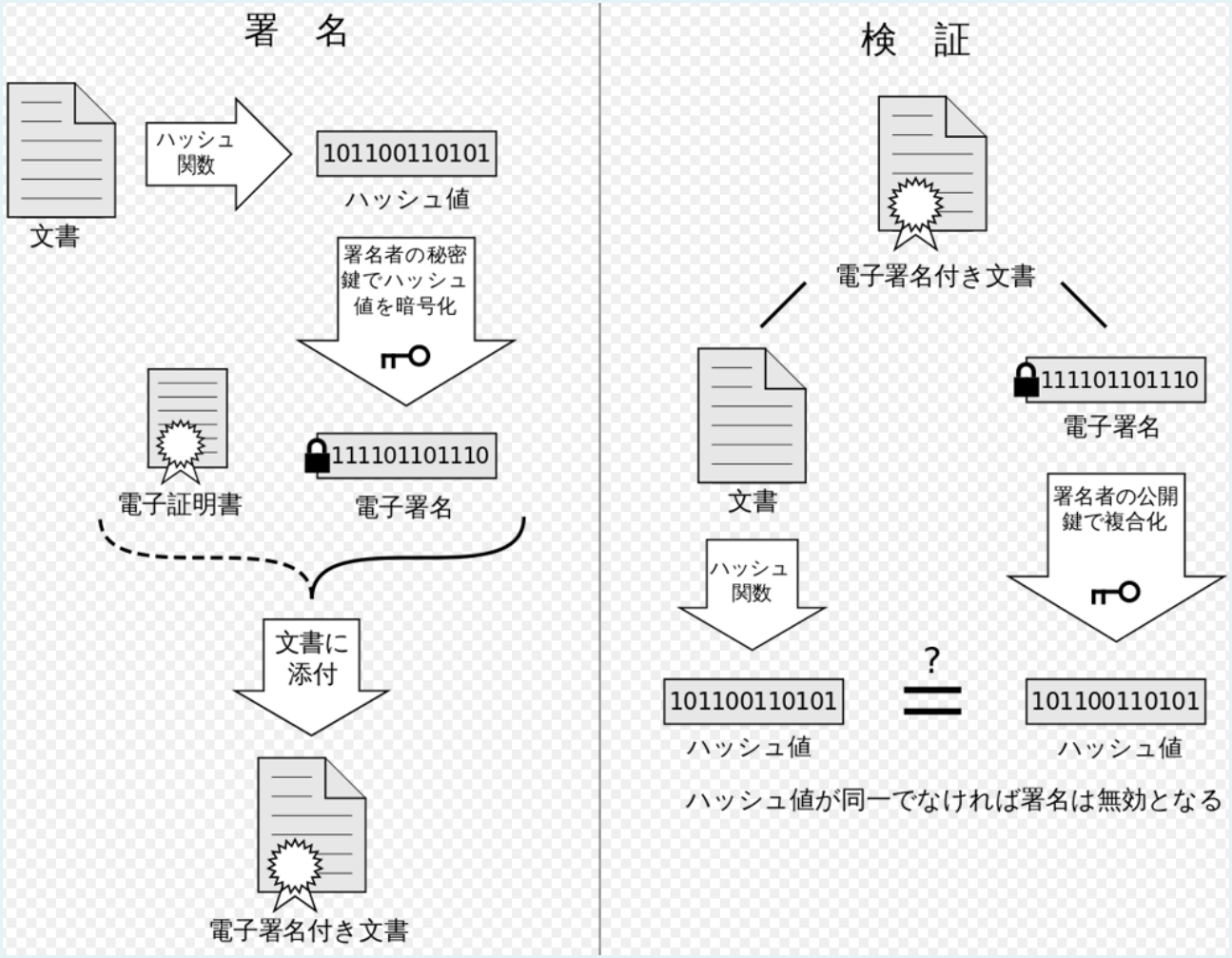
ビットコインの仕組み

関連トランザクションの流れ



ビットコインの仕組み

電子署名の適用と検証



ビットコインの仕組み

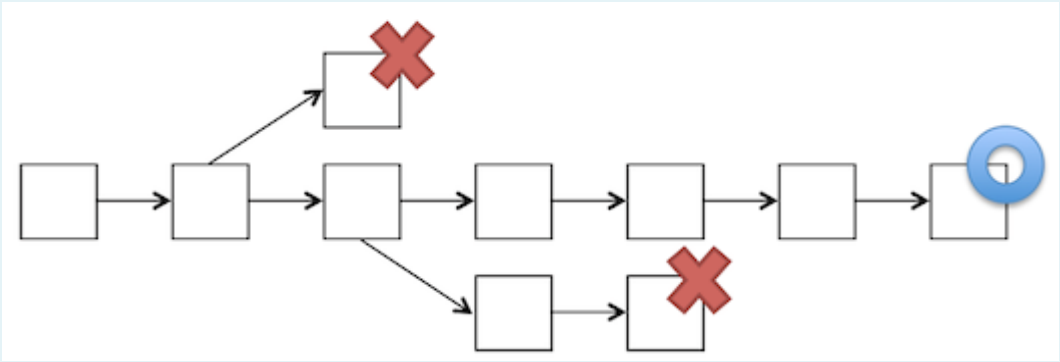
ハッシュ関数

ハッシュ関数とは、与えられた入力値から、規則性のない*固定長*の値を生成する演算手法。得られた値は「ハッシュ値」と呼ばれる。

ハッシュ関数には、同じ入力値からは必ず同じ値が得られる一方、少しでも異なる入力値からはまったく違う値が得られるという特徴がある。不可逆な一方向関数を含むため、ハッシュ値から入力値を割り出すことはできない。また、入力値がハッシュ値より長い場合、複数の異なる入力値から同じハッシュ値が得られる（ハッシュ値の衝突）が、ある入力値を元に、同じハッシュ値になる別の入力値を効率よく探索することはできない。

データの伝送や複製を行なう際に、入力側と出力側でハッシュ値を求め一致すれば、途中で改ざんや欠落などが起こっていないことを確認することができる。また、暗号や認証、デジタル署名などの要素技術として様々な場面で利用されている。

ビットコインの仕組み



これは単純な方法であり、一見してまだ不十分であるようにも見える。しかし、Bitcoinの原著論文では、これについて、確率論的な説明がなされている。（論文(PDF)の11章）論文によると、攻撃者とブロックチェーンの伸ばし合い競争をした場合、善意のノードの持つ計算資源が、攻撃者のそれより少しでも多いかぎり、攻撃者がブロックチェーンを乗っ取れる可能性はきわめて低いとされている。

ビットコインの仕組み

ブロックチェーンの適用範囲は拡大している。

金融分野	非金融分野
• 決済 • 送金、為替取引 • 電子マネー、ポイント、マイレージ • 地域通貨、地域振興券 • クラウドファンディング • ソーシャルレンディング • クレジットカードシステム • 銀行勘定系システム • 銀行内資金決済システム • 銀行間資金決済システム • 中央銀行システム • 証券取引システム • 証券決済システム • 債権管理システム • 電子記録債権 • 保険契約管理 • 遺言信託 • 信託管理システムなど	• 電子チケット • 著作権管理 （音楽、映像コンテンツなど） • 登記システム （不動産、債券、動産など） • 電子鍵システム （住宅、ホテル、車など） • レンタカー管理システム • 公的証明書発行 • サプライチェーン管理 • 電子カルテ • 裁判記録、犯罪記録 • SNS、メッセンジャーサービス • 投票システム • マーケットプレイス • ストレージサービス • IoT • 発電システムなど

仮想通貨（ビットコイン）の問題点

◆取引量が増えるについて取引が完了するまでの時間がかかっている。
　取引を処理できる量は約7取引/秒（ブロックの発生は約10分で1ブロック内には約2000～3000の取引情報を格納するのが限度）　参考：VISAは24,000取引/秒。
解決策は；
　トランザクションの圧縮（分離署名、1ブロックに格納される取引は約4倍になる）
　ブロックサイズの拡張

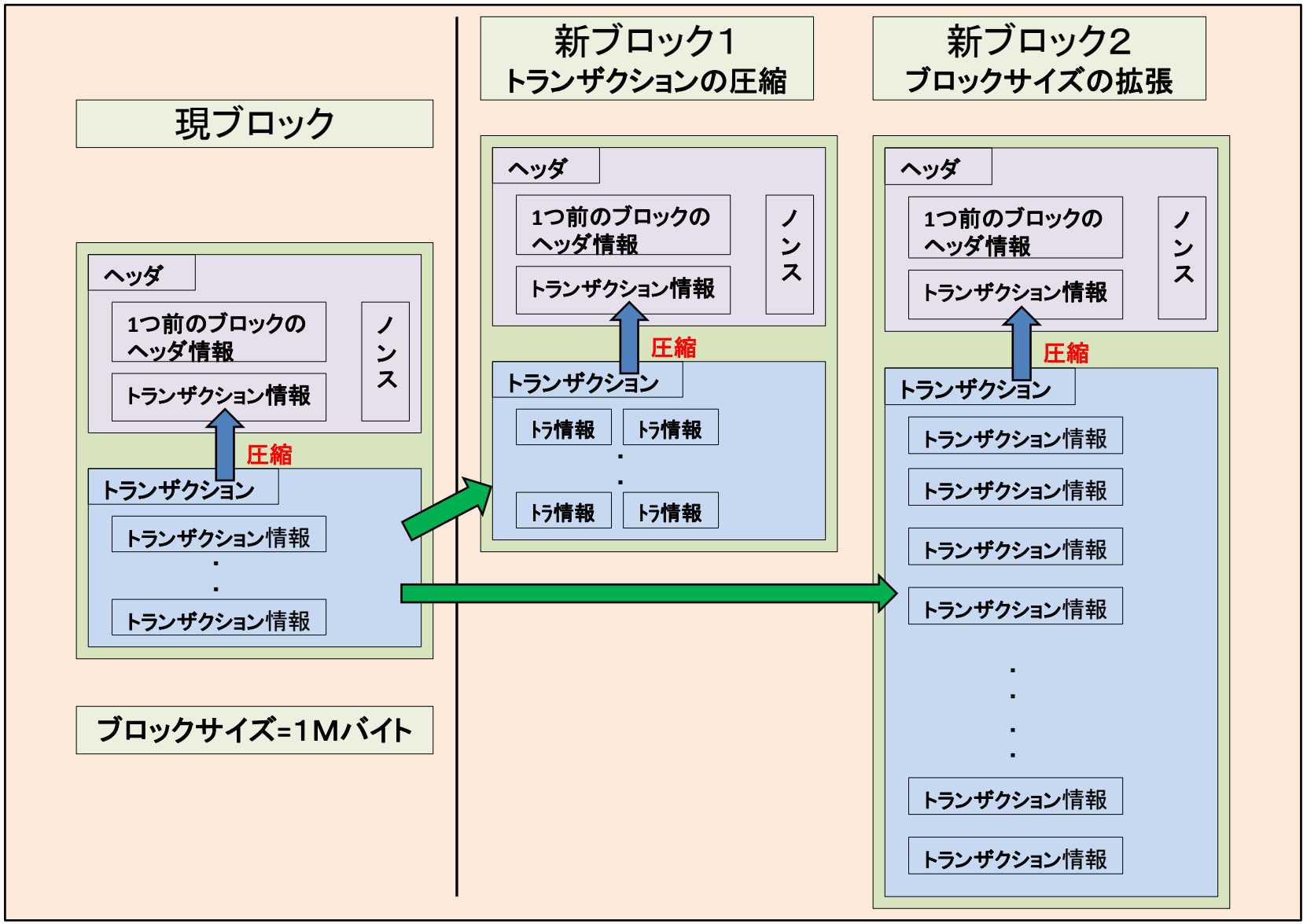
◆取引手数料の増加
　2017年11月時点の現在の平均取引手数料は10.17ドル　（エコノミストは10月時点では2ドル強）
　手数料は自分で決める。（銀行取引では銀行が決める）
　手数料を安く設定するとそれだけ取引完了までの時間がかかる。
　マイナー（採掘業者）は手数料の高い取引きから処理する。（ブロックチェーンに組み込む）

◆電力の浪費
　マイニングに使用される電力（予想）2016年～2017年年間336万メガワット時（アメリカの平均家庭30万世帯分（約大型原発0.4基分）

◆将来、マイニング業者が存続できるか？
　将来、マイニングの報酬は取引手数料だけになる。＝取引手数料の高騰になる。

◆ブロックの容量が管理しきれなくなる??
　計算すると　8M/10分X60分/時X24時/日X365日/年＝420,480M/年＝420Gバイト/年

仮想通貨（ビットコイン）の問題点

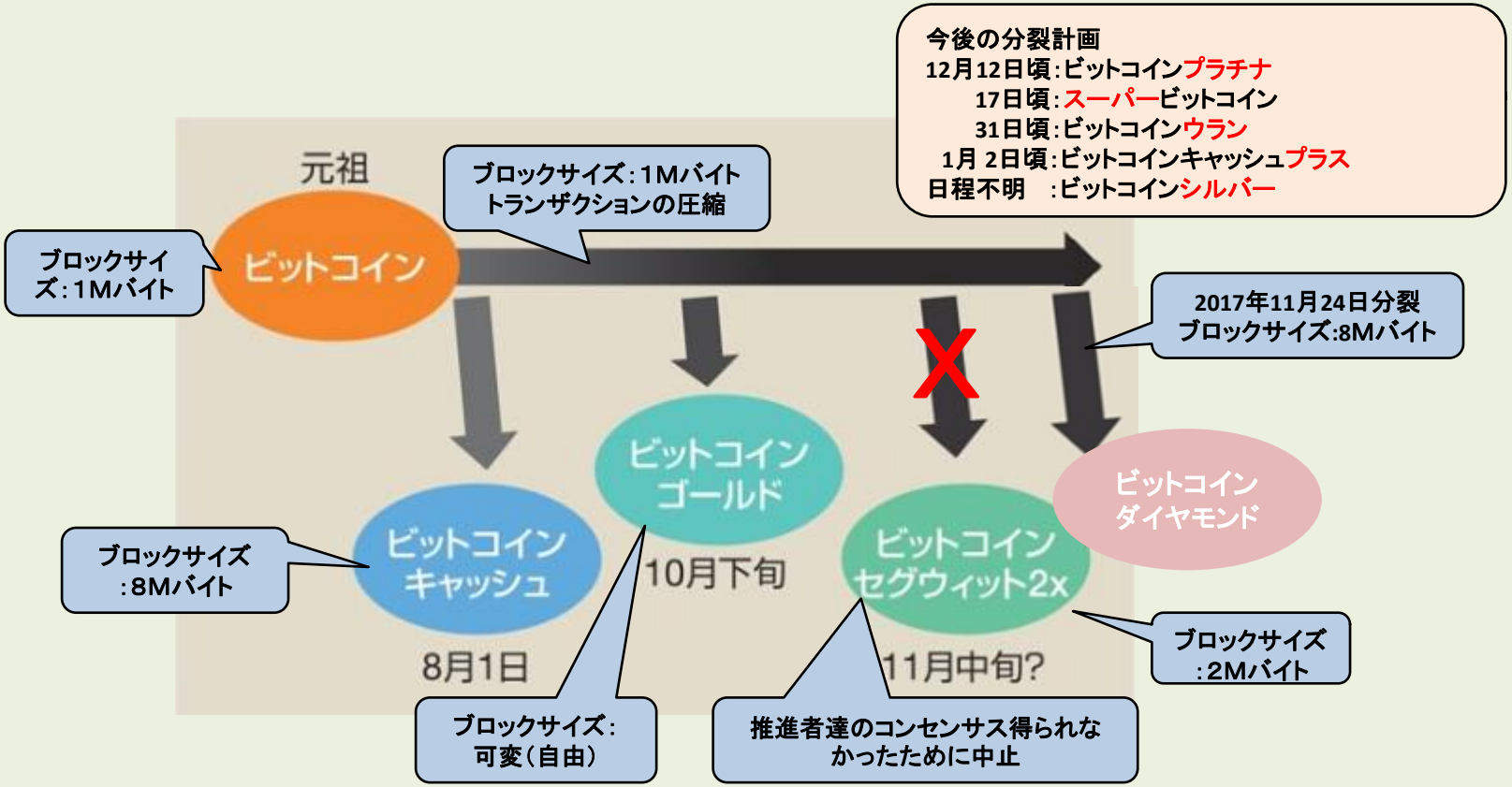


ビットコインの分裂

問題点：取引量が増え、その処理（トランザクションがブロックに記入されるまでの時間）に遅れが生じ出した。

解決方法：コア開発者とマイニング業者の意見の相違

- ●コア開発者：トランザクションの圧縮、不要データの削除→ソフト変更有
- ●マイニング業者：ブロックサイズの拡張→ソフトの変更なし



ビットコインの入手方法

米ドルのような外貨と同じく、日本円と交換する。その際、両替所の役割を果たすのが仮想通貨取引所。業者によって取扱通貨の種類(ビットコインやそれ以外の仮想通貨)、手数料、最低購入額などに違いがあるが、安全性や顧客への説明体制などの水準を金融庁が認めた登録業者を選ぶのが無難だ。

取引所に口座を開設する場合、銀行のように対面式の窓口はないので、インターネット経由で申し込み手続きを行う。ホームページやアプリでメールアドレスを登録してアカウントを作成し、免許証の写真など本人確認書類を送信。取引所からの書留を受け取ることで住所・本人確認をするのが一般的な流れだ。

口座ができたら、銀行やコンビニから日本円を取引所に入金。あとは値動きを見て「ここぞ」のタイミングで仮想通貨を購入という、株式投資やFX(外国為替証拠金取引)に似た取引となる。

ビットコインの管理方法

管理法

どこに保管しておくべき？

入手した仮想通貨を保管する方法は大きく分けて3つ。1つは取引所にそのまま置いておく方法だ。銀行預金に近い感覚だが、取引所へのサイバー攻撃や取引所が倒産するリスクがあるので、預け先の選択が重要になる。世界最大の取引所だったマウントゴックスは2014年、巨額のビットコインが消失する事件を起こして経営破綻した（右写真は盗難を主張するマルク・カルプレス代表）。

もう1つはスマートフォンやPCにインストールした「ウォレット・アプリ」（左写真）などに、取引所から通貨を移して保管する方法。実体のない仮想通貨を手元の「財布」に入れておくイメージで、事前に復元の設定をしておかないと、機器の紛失や破損で通貨が失われる可能性も。また、ウイルス感染すればハッキングで盗難されるリスクがある。

最後はネットに接続していないPCや専用端末に、自分の通貨情報を保存する方法。オフラインなのでハッキングされず安全性が高い一方、そのままでは取引や決済ができないのがデメリット。紙に通貨情報を転記・印刷しておく方法もある。

ビットコインの決済方法

決済

店での会計に使用する方法は?

ビットコインで支払いできる店は世界的に増加中で、海外でも両替の手間なく簡単に使えるのが魅力(決済に関しては他の仮想通貨は未発達)。ウォレットのほか一部の取引所のアプリでも決済ができ、方法も同じだ。

店員が代金をQRコード化した画面をタブレットなどで表示し、それを自分のスマホのアプリで読み取って、支払いボタンをタッチするだけ。取引所から支払うのに比べるとウォレット・アプリを使ったほうが、送金が確定するまでの時間は短い。

手数料の額は自分で決められるが、手数料の高い取引から優先的に承認されるため、少額だといつまでも取引が確定しないことも。手数料相場は上昇中で現在は数百円程度だ。値上がり中のビットコインを決済で手放したくないという人もおり、「通貨」としての決済機能には課題もある。