

仮想通貨の動向

岩下 直行 ●京都大学 公共政策大学院 教授
星 暁雄 ●IT ジャーナリスト

日本の仮想通貨法の成立をきっかけに、日本人の資金により仮想通貨が高騰。ICOブームでビットコイン以外のオルトコインにも資金が流入した。ビットコインのコミュニティでは「分裂」騒動が起きたが乗り越えた。仮想通貨の実利用の進展はまだまだであり、新技術Lightning Networkの進展に期待がかかる。

■はじめに

本稿の前半部分は、京都大学の岩下氏への取材に基づき星が執筆した。また、後半部分「家電量販店でビットコイン決済を提供」以降は、星の調査による執筆である。

■「仮想通貨法」施行で仮想通貨取引が活発に

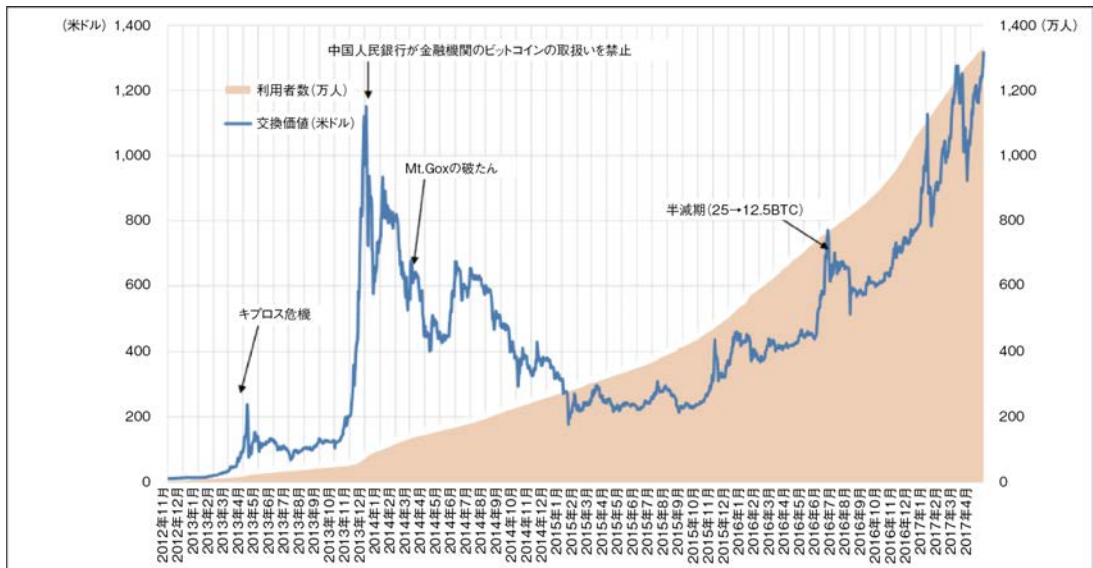
2017年、日本では仮想通貨に関する特筆すべき動きがあった。4月から改正資金決済法、いわゆる仮想通貨法が施行されたことである。ビットコイン（Bitcoin）を筆頭とする暗号通貨（Cryptocurrency、英語圏ではこの表現がよく使われる）は法的に「仮想通貨」の一種として定義された。合わせて仮想通貨取引所が金融庁の監督下に置かれることとなった。これにより、仮想通貨が「公認」されたと多くの人々が受け止めた。この法律の施行が1つのトリガーとなって仮想通貨への認知が大きく向上し、仮想通貨取引所のビジネスが急拡大した。日本国内で最大手の仮想通貨

取引所を運営するビットフライヤーによれば、同社1社で2017年内にユーザー数が100万人を超え、取引高（デリバティブ含む）も、1月の月間3268億円だったのに対し、12月は8.7兆円に成長した。

仮想通貨取引所のユーザー数と取引高の増大を反映し、2017年にビットコインを筆頭とする仮想通貨の価格は軒並み高騰した（資料5-3-1A、B）。2017年初の998ドルから2017年12月16日の1万9499ドルまで最大で19.5倍の上昇を見せ、その後2018年1月中旬にかけ1万ドル台まで戻した（Blockchain.infoの統計による）。

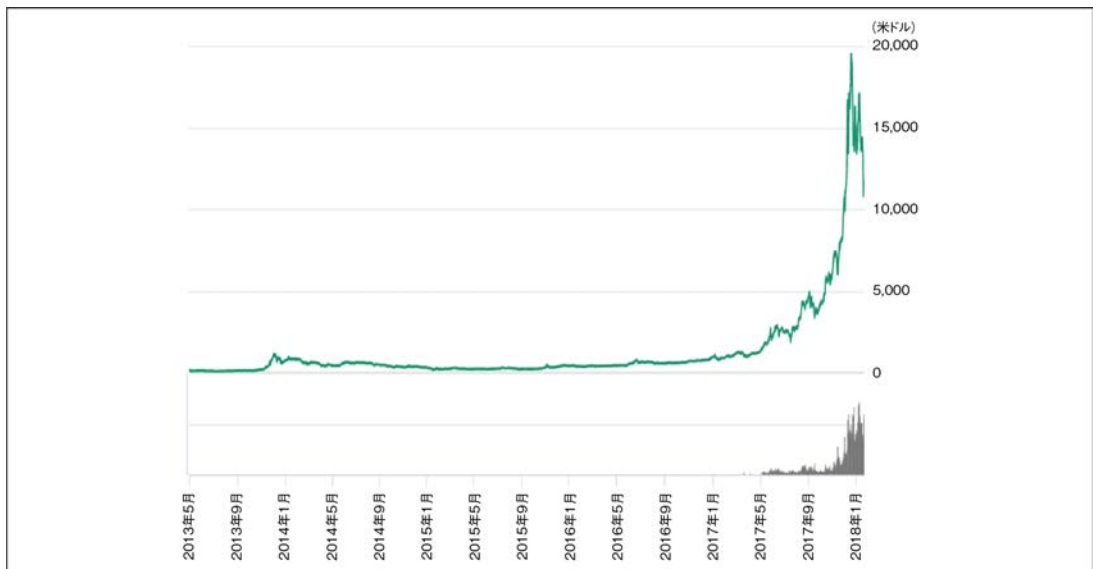
価格高騰が投機を呼び込んだ結果、仮想通貨相場が「バブル」状態にあると指摘する声が大きくなっている。一方、店舗やインターネットサービスの料金支払いへの利用、仮想通貨の背後で動くブロックチェーンの応用のような、仮想通貨分野の実利用は地道な普及拡大の過程にある。実利用に先行して投機が盛り上がったことが、2017年の仮想通貨を取り巻く状況だったといえるだろう。

資料5-3-1A ビットコインの価格と利用者数の推移（2017年4月まで）



出典：Web サイト Blockchain.info¹ より

資料5-3-1B ビットコインの価格の推移（2018年1月まで）



出典：Web サイト coinmarketcap.com² より

■一時的だった「中国ショック」

2017年は、相場に冷水を浴びせかける動きもあった。1つは中国の規制強化、もう1つはビッ

トコインのいわゆる「分裂」騒動である（後者については後述する）。

2017年9月、中国は仮想通貨への規制強化に

動いた。中国の中央銀行である中国人民銀行は、中国国内でのICO（Initial Coin Offering、仮想通貨による資金調達）を禁止し、また仮想通貨取引所の営業を停止させたのである。

この「中国ショック」により、仮想通貨の相場は暴落するのではないかと懸念も聞こえていた。9月のビットコイン相場は一時的に急落したが、その後すぐ価格を戻している。2017年1月時点ではビットコイン取引高の9割は中国の人民元建てと言われていたが、9月の値動きから言えることは、中国国内のビットコイン取引に関して仮想通貨取引所が公表していた数字は現実よりも大きかったと考えるのが自然ではないだろうか。別の角度から見れば、日本の個人投資家の需要は中国ショック以前から仮想通貨の相場を支えていたのだろう。

金融業界はコンプライアンスが厳しく、恣意的な数字の操作は御法度である。一方、仮想通貨の業界は規制が行き届いておらず、取引所はみな私設である。仮想通貨に関する数字も、私企業が発表した数字であって公的な共通の基準に基づくものではない。このことは注意しておいたほうが良いだろう。

また現状では同じ仮想通貨でも取引所により価格の違いが大きいことも注意が必要である。機関投資家による裁定取引がまだ本格的に行われてはいないことを示している。

2017年12月には、シカゴの2つの先物取引市場、CME（Chicago Mercantile Exchange）とCBOE（Chicago Board Options Exchange）でビットコイン先物の取り扱いが始まった。このニュースが流れただけでビットコイン価格が上がり、CMEの株価も上昇した。今後、機関投資家が先物市場を経由してビットコイン相場に参入し、相場の様相が変わることも考えられる。

■「投資家保護」に改善の余地あり

ビットコインを筆頭とする仮想通貨を扱う仮想通貨取引所や決済サービスが多数登場してきたが、投資家/消費者保護の観点からはまだ課題が多い。

最も基本的な仮想通貨の保有方法にしても、複数のやり方があり、現状では一長一短である。大きく分けると、(1) サーバー上のウォレット（仮想通貨取引所を含む）に預ける場合、(2) 秘密鍵を個人管理するウォレットで管理する場合に分かれる。前者の場合、注意が必要なのは、銀行とは異なり仮想通貨取引所は預かった資金が不正利用された場合の保証まではしてくれないということである。オンラインバンキングのサービスを使うような感覚で仮想通貨取引所を全面的に信頼して利用していると、例えばハッキングによる不正出金のような事故により資金を失う危険がある。なお、IDとパスワードに加えて「2要素認証」を設定することによりセキュリティ水準を高めることができる。仮想通貨取引所やウォレットサービスを使う場合、2要素認証を設定することは必ず行うべきだ。

一方、(2)の秘密鍵を個人管理するウォレットとは、さらに(a) PCやスマートフォンの上で動くウォレットアプリ、(b) 専用のハードウェアウォレット、(c) 紙に秘密鍵を印刷して保管するペーパーウォレットの3つに分かれる。秘密鍵を個人で管理する場合、秘密鍵を知られない限り他人が仮想通貨を不正使用する危険はない。その代わり、秘密鍵を紛失してしまうと自分の仮想通貨を取り戻す手段は永久に失われる。

すべてのユーザーが秘密鍵を自分で管理することにはまだ無理があると思われる。その意味でも、仮想通貨取引所やサーバー上のウォレットを運営する企業のユーザー保護対策がより強く求められるようになっていくだろう。なお関連する取

り組みとして、ビットフライヤーと三井住友海上火災保険は仮想通貨取引所のハッキングに対応する保険商品を開発している。

■ビットコインはバブルなのか？

ビットコインの高騰がバブルかどうか、という問いをよく聞く。通常の金融商品は、国債は国が、株は株式会社が価値を担保し、価格の理論値を計算することができる。ところがビットコイン価格には理論値がない。利息や配当が保証されるわけでもなく、株式会社の解散価値のような裏付けもない。経済学の立場では適正価格は「0円」ということになる。ビットコインの価格がいくらで取引されようと、本来0円のものに価格がついているなら経済学的にはバブルと言わざるを得ない（注：なおビットコインの価格形成については、採掘コストを反映していると考えられる説や、希少性やネットワーク効果により価格を説明できるとの説もあるが、まだ定説といえるものはない）。

ここで注意したいのは、ビットコインに価値を見出したのは、経済学者でもプロのトレーダーでもなく個人投資家だったことである。多くの金融のプロはビットコインを筆頭とする仮想通貨をまだ「怪しい」と見ている。一方で、相場に関

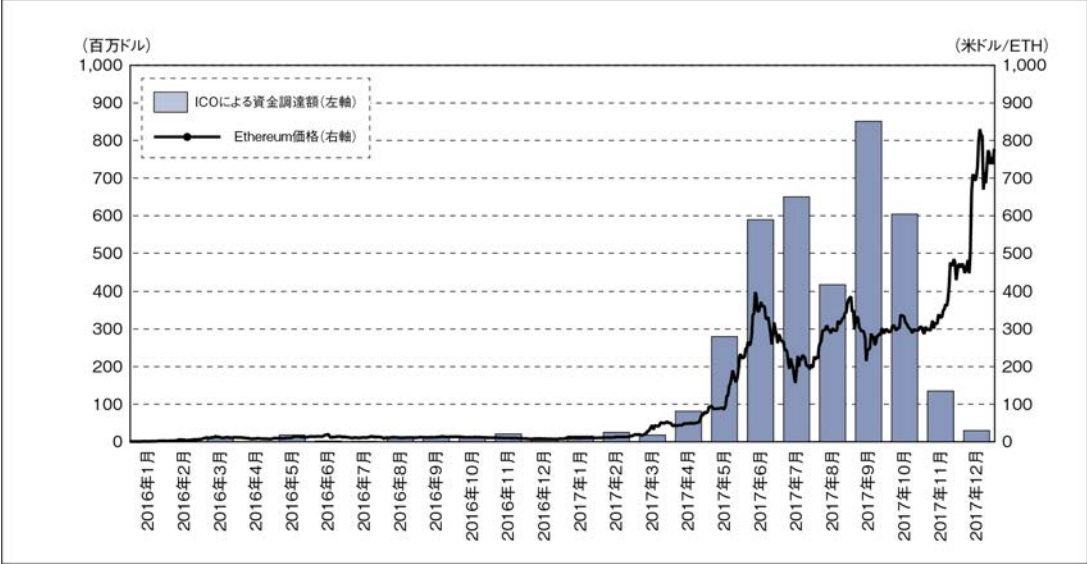
してはプロのトレーダーよりも個人投資家の肌感覚のほうが正しい判断をする場合がある。個人投資家に加えて機関投資家も参入しつつある仮想通貨の今後の相場は今まで以上に予測が難しく、注意深く見守っていく必要があるだろう。

■ICOブームからオルトコインブームへ

2017年はビットコイン価格が高騰したが、仮想通貨全体の時価総額に占めるビットコインの割合は減少した。つまり、ビットコイン以外の仮想通貨、オルトコインの比率が上がった。

オルトコインの価格高騰を主導したのは、ICOで使われたEthereum（イーサリアム）である。ICOのトークンセール（仮想通貨トークンの売り出し）の多くがEthereum建てで払い込み、Ethereumのブロックチェーン上で発行されるERC20仕様に基づくトークンを受け取る形で行われた。そこで、ICOに参加して新規発行トークンを購入するには、まずEthereumを買うことになる。この需要がEthereum相場を押し上げた。資料5-3-2は、ICOによる資金調達額とEthereumの価格推移を比較したグラフだが、両者には相関が認められる。

資料5-3-2 ICOによる資金調達額とEthereum価格の推移



出典：Web サイト www.coinschedule.com および www.coingecko.com より³

資料5-3-3は2017年の主なICO一覧だが、前年 に比べ大型案件が増えていることが分かる。

資料5-3-3 2016年、2017年の主なICO一覧

2016年のTOP10			2017年のTOP10		
順位	プロジェクト名	資金調達額 (ドル)	順位	プロジェクト名	資金調達額 (ドル)
1	Waves	\$16,436,095	1	Filecoin	\$257,000,000
2	Iconomi	\$10,576,227	2	Tezos	\$232,319,985
3	Golem	\$8,596,000	3	EOS Stage 1	\$185,000,000
4	SingularDTV	\$7,500,000	4	Paragon	\$183,157,275
5	Lisk	\$5,700,000	5	Bancor	\$153,000,000
6	Digix DAO	\$5,500,000	6	Kin Kik	\$97,041,936
7	FirstBlood	\$5,500,000	7	Status	\$90,000,000
8	Synereo	\$4,700,000	8	TenX	\$64,000,000
9	Decent	\$4,178,357	9	MobileGO	\$53,069,235
10	Antshares/NEO	\$3,608,378	10	KyberNetwork	\$48,000,000

2016年計
件数 46 件 調達額 \$96,389,917

2017年計
件数 235 件 調達額 \$3,700,682,293

出典：Web サイト coinschedule.com ⁴より

2017年後半には、ビットコイン、Ethereum以外の仮想通貨にも資金が流入する傾向が顕著になった。資料5-3-4で仮想通貨の時価総額シェアを観察すると、時価総額が大きく名前が知られた仮想通貨（ビットコイン、Ethereum、Bitcoin Cash、Litecoin、Ripple、Dash、NEM、Monero、

IOTA、NEO）以外の「その他（Others）」の分類が、2017年末時点で20%に達している（2018年1月13日には24%）。新しく無名の仮想通貨（あるいは仮想通貨テクノロジーで作られたトークン）に巨額の資金が流れ込んでいることが分かる。

資料5-3-4 仮想通貨の時価総額シェアの推移



出典：Web サイト coinschedule.com より

金融界には「低位株の循環物色」という言葉がある。株式相場で主要銘柄が値上がりしてしまった後に、まだ価格が低いこれから上昇する余地があると人々が考えた低位株の需要が増える現象を指す。同様に、今の仮想通貨相場は低位銘柄に資金が流れ込む段階にあるといえる。

ICO ブームは仮想通貨相場を大きく押し上げたが、その半面で多くの問題が表面化している。巨額の資金調達に成功する ICO が続出している一方で、プロジェクトの成功率が低いことが指摘されている。過去 48 件の ICO プロジェクトを調べたところ、プロダクトがいつさいない事例が 56.25% を占めるとの指摘がある⁵。

より悪質な問題も発生している。規制下にある金融商品では許されないような勧誘や相場操縦が、ICO やオルトコインでは見過ごされている。さらに ICO と見せかけて実質は詐欺行為である事案も報告されている。このような状況を受け、中国は ICO の全面禁止に踏み切っている。

投資家保護を考えれば、共通の基準に基づく適時開示や、相場操縦の禁止などが求められる。日本の金融庁は仮想通貨に関するタスクフォースを立ち上げている。今後の活動による市場の健全化に期待したい。

■家電量販店でビットコイン決済を提供

以下では、仮想通貨分野の実利用や技術、コミュニティの側面に目を向ける。改正資金決済法の施行に合わせ、2017年4月には、家電量販店大手のビックカメラがビットフライヤーのシステムを利用して店頭でビットコイン決済を導入した。日本国内での店舗やインターネットサービスでのビットコイン決済のサービスはこれが最初ではなく、ビットフライヤー、コインチェック、テックビューロがそれぞれ提供中だが、ビックカメラの事例はタイミングと知名度から大きな話題となった。

ビットコインの仕組みをインフラとして利用するサービスとして、5月末にローンチした「VALU」がある。これはサービスのユーザーが誰でもトレーディングカードのようなもの（これをVALUまたはVAと呼ぶ）を発行でき、ユーザー間で、ビットコイン建てで売買するサービスである。ソーシャルメディアで影響力がある個人が多額のビットコインを調達する事例も出て、賛否両論の話題となった。

■ビットコインの「分裂」騒動とフォークコイン乱立

2017年、ビットコインのコミュニティにおける、いわゆる「分裂」騒動は大きな話題となり、相場にも影響を与えた。

「分裂」騒動とは、ビットコインの送金件数の増大に伴い性能向上（スケーリング）の必要性が増し、解決策をめぐるビットコインを支えるコミュニティが2つの勢力に分裂した出来事を指す。この分裂の理由は、技術的合理性よりも利害や立場の違いによると考えられている。

分裂の過程は足かけ3年に及ぶ。大筋では次のようになる⁶。(1) 2015年、ビットコインのクライアントソフトウェア（Bitcoin Core）開発者

グループが性能向上のためブロックサイズを拡大するハードフォーク案（Bitcoin XT）を提案するが、コミュニティに受け入れられなかった。

(2) 2016年、ビットコイン開発者グループが新仕様SegWit（Segregated Witness、署名分離）を提案。バグ修正、スケーリング問題の緩和、新技術Lightning Networkへの発展可能性がポイントだった。SegWitはマイナー（ビットコイン採掘業者）の95%が賛成すれば有効化される手続きに入ったが、賛成票は30%以下と振るわず。ここでSegWit仕様を推す開発者グループと、SegWit仕様をあくまで拒否するマイナーの意見の対立が顕在化、膠着状態が続いた。

(3) 2017年春、マイニング機器製造とビットコイン採掘で大きなシェアを持つ中国 Bitmain Technologies 社らが、ビットコインのブロックサイズを動的に拡大する機能を追加して性能向上を図ったビットコインの派生版である Bitcoin Unlimited をマイナーの多数派を集め有効化しようとした。これは実現はしなかったが、ビットコインを実力で支配しようとする動きは大きな議論を巻き起こした。

(4) 2017年4月から7月にかけて開発者グループの一部有志らがUASF（User-Activated Soft Fork）と呼ぶ活動を展開した。2017年8月1日までにSegWitの有効化が実現されない場合、ビットコインのP2Pネットワークの機能が実質的に麻痺してしまうというもので、P2Pソフトウェアの特性を活用した一種の「ストライキ」だった。

(5) 5月、多くのビットコイン事業会社に投資する Digital Currency Group が、スケーリング問題の妥協案といえる NYA（ニューヨーク合意）を発表した。UASF 発動回避のため7月にSegWit有効化、11月にブロックサイズ拡大を実施する合意案である。米国の多くの事業会社、中国 Bitmain 社を含むマイナー各社、日本のビットフライヤー

を含む56社が署名した。ただしBitcoin Core開発者らは署名していない。

(6) 7月、NYAに基づきSegWit仕様が有効化されることが確定。(7) 8月、NYAとは別に一部の中国のマイナーが独自にBitcoin Cashを分岐させ採掘を開始した。実質的には前述のBitcoin Unlimitedを改名したもので、ブロックサイズ拡大を実現するもの。(8) 11月、NYAの定めたブロックサイズ拡大の実施が見送られた。もし実施された場合、さらなる分岐の懸念があった。

■騒動の決着とその後の課題

一連の騒動は、従来のビットコイン (SegWit仕様あり、ブロックサイズ従来通り) と、ビットコインから分岐した新たな仮想通貨Bitcoin Cash (SegWit仕様なし、ブロックサイズ拡大) の2系統がそれぞれ残る形で決着した。特に、上記の(2)のBitcoin Unlimited有効化、(4)のUASF、(8)のブロックサイズ拡大ハードフォーク (SegWit2Xと呼ぶ) の3件は、もし実施されていればビットコインのネットワークが不安定な状態に陥る可能性があったが、結果として回避できた。一連の騒動はビットコインにとって大きな試練だったといえる。一方で、騒動が決着したことで大きな不安材料が解消されたとの見方もできる。

今のところ、分岐してブロックサイズを拡大したBitcoin Cashよりも、本流のビットコインのほうが送金需要が多い。ビットコインのSegWit仕様は有効化したもののSegWit仕様のウォレットの普及は進まず、処理能力を高める効果は限定的である。そこでビットコインでは処理性能が上限に近い状態が続き、送金手数料が高騰、また送金遅延が発生しやすい状態が続いている。

解決手段となるのは、SegWit仕様ウォレットの普及と、高速高頻度の少額決済を可能とする新技術Lightning Networkである。Lightning

Networkは、ビットコインのブロックチェーンの1つ上の層 (レイヤー) で価値を移転する。このような技術全般を「2nd Layer」技術と呼ぶ。2017年にはLightning Networkの実装が登場し、テストネットが稼働を開始している。2018年には実利用が始まると期待されている。

■一時はハッシュレートの「シーソー現象」が

Bitcoin Cashの登場で、別の混乱も起きた。ビットコインとBitcoin Cashは両方とも同じハッシュアルゴリズム (SHA-256) を用いていて同じ機材で採掘できる。なおかつ、Bitcoin Cashは採掘の難易度を急激に変動させて調整するアルゴリズムを採用した。このことから、双方の仮想通貨の値動きと採掘難易度の変化に伴い、ビットコインを採掘するよりBitcoin Cashを採掘したほうが収益性がよくなる時期が周期的に到来し、ビットコインとBitcoin Cashの間でハッシュレート (ハッシュ計算能力) がシーソーのように急激に移動、双方のブロック生成間隔が極端に増減する現象が観測された。

これは双方の利用者にとって送金の所要時間が極端に増減し、利便性が損なわれることを意味する。この解決のため、Bitcoin Cashは11月に難易度調整アルゴリズムを改訂し、上記のシーソー現象は緩和された。

■「フォークコイン」が乱立

Bitcoin Cashの分岐後は、ビットコインとBitcoin Cashの双方の価格が上昇した。このことから、ビットコインの分岐により短期間で大きな利益が出せるとの見方が広がり、ビットコインを分岐させた「Bitcoin Gold」などの「フォークコイン」の発表が相次いだ。Bitcoin Gold以降のフォークコインは、ビットコインからの分岐で

あること、またSHA-256とは異なるハッシュアルゴリズムを採用していること（ビットコイン、Bitcoin Cashとは異なるマイニング機器を使うこと）が共通点である。中には単なる「いたずら」で発表された実態がないフォークコインもあった。

た。短期的にはフォークコインにより資産が増えたと喜ぶユーザーもいるだろうが、中長期的にはビットコインの信用を傷つけた出来事として記憶されるのではないだろうか。

1.<http://www.blockchain.info/>

2.<https://coinmarketcap.com/>

3.<http://www.coinschedule.com/>

<http://www.coingecko.com/en>

4.<http://www.coinschedule.com/>

5.10億集めたICOが何もプロダクトをローンチできない理由
（『BTCN』2017年9月1日、東晃慈）

<https://btcnews.jp/2ojkkse512376/>

6.ビットコイン、その「分裂」騒動の正体 反対派を動かした、ビットコイン流ストライキ（『日経テクノロジーオンライン』2017年9月4日、星暁雄）

<http://techon.nikkeibp.co.jp/atcl/feature/15/083100127/00001/>



1996, 1997, 1998, 1999, 2000...

[インターネット白書ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2018年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<https://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp

©1996-2018 Impress R&D