

仮想通貨の衝撃

ビットコイン、NEM、Zaif、・・・

仮想通貨取引所、仮想通貨販売所、仮想通貨交換業者、・・・

仮想通貨とは

◎資金決済に関する法律 衆議院 法律第五十九 (平二一・六・二四)

第二条 この法律において「前払式支払手段発行者」とは、次条第六項に規定する自家型発行者及び同条第七項に規定する第三者型発行者をいう。

第二条 5 この法律において「資金清算業」とは、為替取引に係る債権債務の清算のため、債務の引受け、更改その他の方法により、銀行等の中で生じた為替取引に基づく債務を負担することを業として行うことをいう。

解説 2018.05.19 検索 Wikipedia

資金決済に関する法律 (しきんけっさいにかんするほうりつ、平成21年6月24日法律第59号) は、商品券やプリペイドカードなどの金券 (電磁化された電子マネーを含む) と、銀行業以外による資金移動業について規定する日本の法律

仮想通貨に対する規制[編集] 第2条第5項で「仮想通貨」を

物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値 (電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。) であって、電子情報処理組織を用いて移転することができるもの (第1号)

不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの (第2号) と定義している。

第2条第7項で「仮想通貨交換業」を

仮想通貨の売買又は他の仮想通貨との交換 (第1号)

前号に掲げる行為の媒介、取次ぎ又は代理 (第2号)

その行う前二号に掲げる行為に関して、利用者の金銭又は仮想通貨の管理をすること。 (第3号)

のいずれかを業として行うことと定義している。

仮想通貨交換業について内閣総理大臣の登録制を導入し (第63条の2)、情報の安全管理、利用者の保護、紛争解決機関との契約義務などの業務について定める (第3章の2第2節) とともに、帳簿書類の作成・保存、報告書の作成・提出、金融庁による立入検査等などの監督について定めている (第3章の2第3節)。

改正法[2]附則第8条では、改正法の施行の際現に仮想通貨交換業を行っている者は、登録の拒否か廃止命令がなければ施行後6月間引き続きその仮想通貨交換業を行うことができ、その期間内に登録の申請をしたときは、登録か登録の拒否の処分があるまでその仮想通貨交換業を行うことができることが定められた (みなし仮想通貨交換業者)。

これらのことから、仮想通貨について定める第3章の2を指して、仮想通貨法と称されることがある[3]。

また、資金決済法で仮想通貨の法的地位が明確にされたことが、2017年 (平成29年) の日本での仮想通貨の盛り上がりにつながったとする見方もある[4]。

ICO (Initial Coin Offering) 注: モジッタ用語

IPO 新規株式公開

ICO 仮想通貨 企業側には情報公開義務や法定プロセスがなくリスクが高い

各国政府における寄贈通貨の取り扱い

日本、米国、中国、韓国、EU、

仮想通貨を支える仕組み: ブロックチェーン

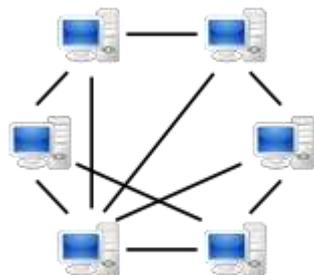
Wikipedia ブロックチェーン (英語: Blockchain、ブロックチェインとも[1][2]) とは、分散型台帳技術[3]、または、分散型ネットワークである[4]。ビットコインの中核技術 (サトシ・ナカモトが開発) を原型とするデータベースである。ブロックと呼ばれる順序付けられたレコードの連続的に増加するリストを持つ。各ブロックには、タイムスタンプと前のブロックへのリンクが含まれている。理論上、一度記録すると、ブロック内のデータを遡及的に変更することはできない。ブロックチェーンデータベースは、Peer to Peer ネットワークと分散型タイムスタンプサーバーの使用により、自律的に管理される。フィンテックに応用されるケースでは独占や資金洗浄の危険が指摘されることもある。

Wikipedia 技術的概要[編集] 下から上にブロックチェーンが形成される (図省略)

ブロックチェーンは、「ブロック」と呼ばれるデータの単位を一定時間ごとに生成し、鎖(チェーン)のように連結していくことによりデータを保管するデータベースである[2]。つまり、ここでいうブロックはノードである。主鎖(黒)の同一性は、起源ブロック(緑色)がもつハッシュ値を究極的な拠り所とする。主鎖は、起源ブロックから現在のブロックまでの最長の一連のブロックで構成されている。孤児ブロック(紫色)は、主鎖の外側に存在する。

あるブロックチェーンに参加する者のうち、プルーフ・オブ・ワーク(PoW)と呼ばれる、計算に時間のかかる値を最初に計算した者が、次のブロックを生成することができる[5](Proof-of-stake(PoS)など別の手法もある[5])。あるブロックの内容は直前のブロックのハッシュ値に依存するため、いったんチェーンに追加されたブロックを改竄することは(それ以降のブロックを全て破棄しない限り)できないとされている[6]。要約値とも呼ばれるハッシュ値は、データの同一性・関連性を認める際に目安となるが、その信頼性は衝突の頻度による。ブロックチェーンに応用した場合は、改竄でないデータを改竄として検出しないかどうか、応用自体の正否に立ち入った検証を必要とする。ブロックチェーンは孤児ブロックを検出すると、ハッシュ値に基づく「多数決」によって正統な主鎖を決定し、ブロック間の同期を確保する。日本ブロックチェーン協会は、独自に技術としてのブロックチェーンを定義している。ブロックチェーンは以下の諸点でビットコインよりも一般化された概念である。

1. 管理者を置けるし、取引履歴も非公開の形で運用できる[7]。
2. 採掘者(マイナー)[8]や、暗号通貨ないしトークンは設計次第で必ずしも要しない。
3. 企業などによって運用されている既存の決済・ポイントサービスなどのシステムを、記録が非公開で運用されるブロックチェーンのシステムに代替することにより運用コストが削減され、決済手数料等が抑えられると期待されている[9][10][11][3][12]。



P2P型ネットワーク(図はピュアP2P型)。コンピューター同士が対等に通信を行うのが特徴である。

P2P(ピアツーピア)

JPNICはインターネットの円滑な運営を支えるための組織です <https://www.nic.ad.jp/ja/basics/terms/p2p.html>

P2Pとはpeer-to-peerの略です。インターネットにおいて一般的に用いられるクライアント・サーバ型モデルでは、データを保持し提供するサーバとそれに対してデータを要求・アクセスするクライアントという2つの立場が固定されているのに対し、P2Pは各ピア(*1)がデータを保持し、他のピアに対して対等にデータの提供および要求・アクセスを行う自律分散型のネットワークモデルであり、サーバまたはクライアントのそれぞれの立場に固定されることがありません。

Fin Teckにおけるブロックチェーンの将来と課題(NTT data 赤羽喜治)

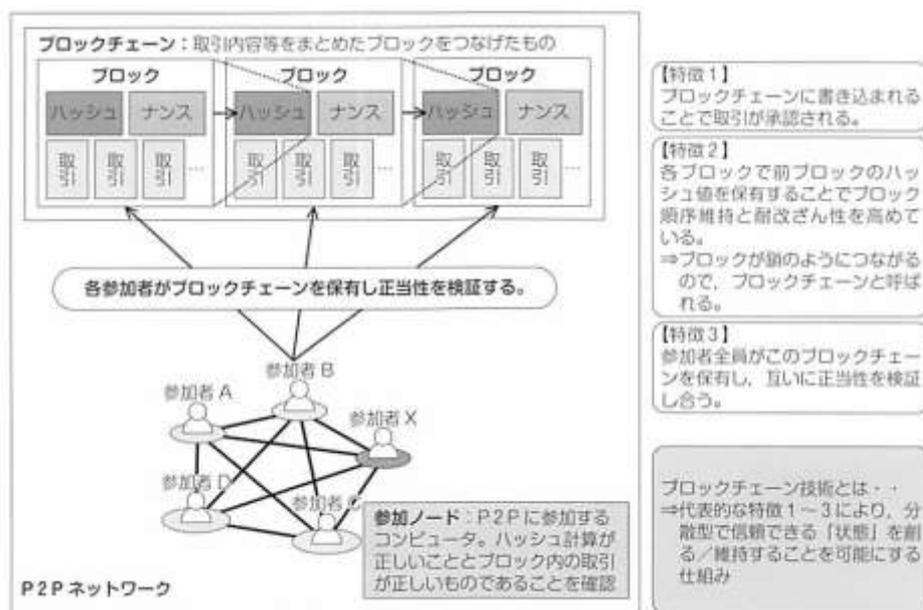


図2 ブロックチェーンの基本的な仕組み

P2P,ネットワーク

従来モノリシックだった金融機関のシステムは FinTech の時代には「サービスを外部に提供し、また外部から取り込む」「データも外部連携し、共有する」ことを通じて、エコシステム的なシステムへと変化し、環境変化への即応性を向上させていくと考えられます。

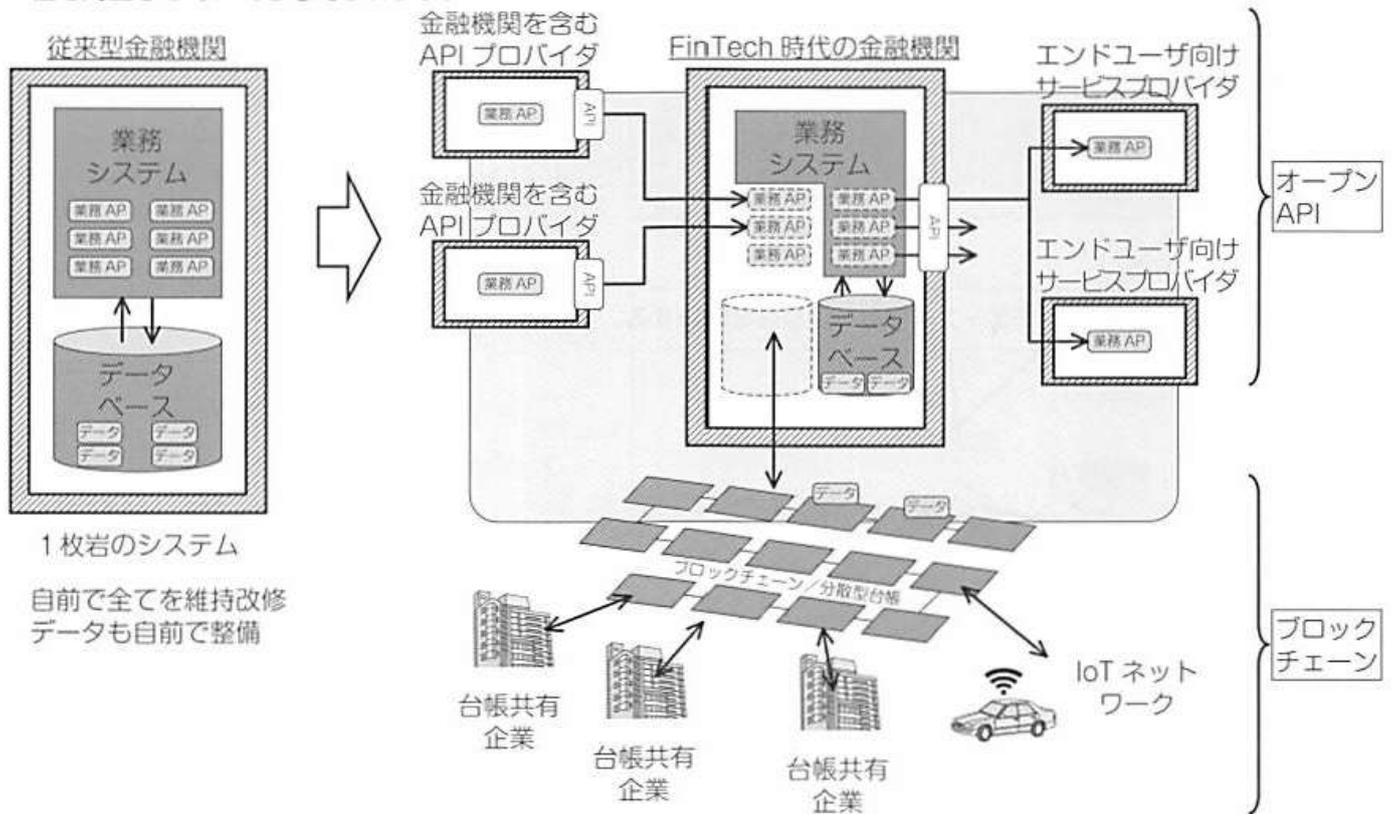


図1 FinTech時代の金融機関システム

参考資料 ブロックチェーン仕組みと理論 赤羽喜治・愛敬真生 (株)リック・20161028 ¥3,240.

データマイニング 【 data mining 】 IT用語辞典 e-Words

データマイニングとは、情報システムに蓄積した巨大なデータの集合をコンピュータによって解析し、これまで知られていなかった規則性や傾向など、何らかの有用な知見を得ること。「マイニング」(mining)とは「採掘」の意味で、膨大なデータの集積を鉱山になぞらえ、そこから有用な知見を見出すことを鉱石を掘り出すことに例えた表現となっている。

データマイニングの適用分野や目的、対象となるデータの種類の多様性だが、ビジネスの分野では企業が業務に関連して記録したデータ(過去の取引記録、行動履歴など)を元に、意思決定や計画立案、販売促進などに有効な知見を得るために行われることが多い。自然言語の解析やパターン認識、人工知能などの研究などでも利用される。分析・解析の手法も様々だが、代表的な手法としては、頻度の高いパターンの抽出や、相関関係にある項目の組の発見、データの特徴や共通点に基づく分類、過去の傾向に基づく将来の予測などがある。

ハッシュ関数 出典: フリー百科事典『ウィキペディア (Wikipedia)』

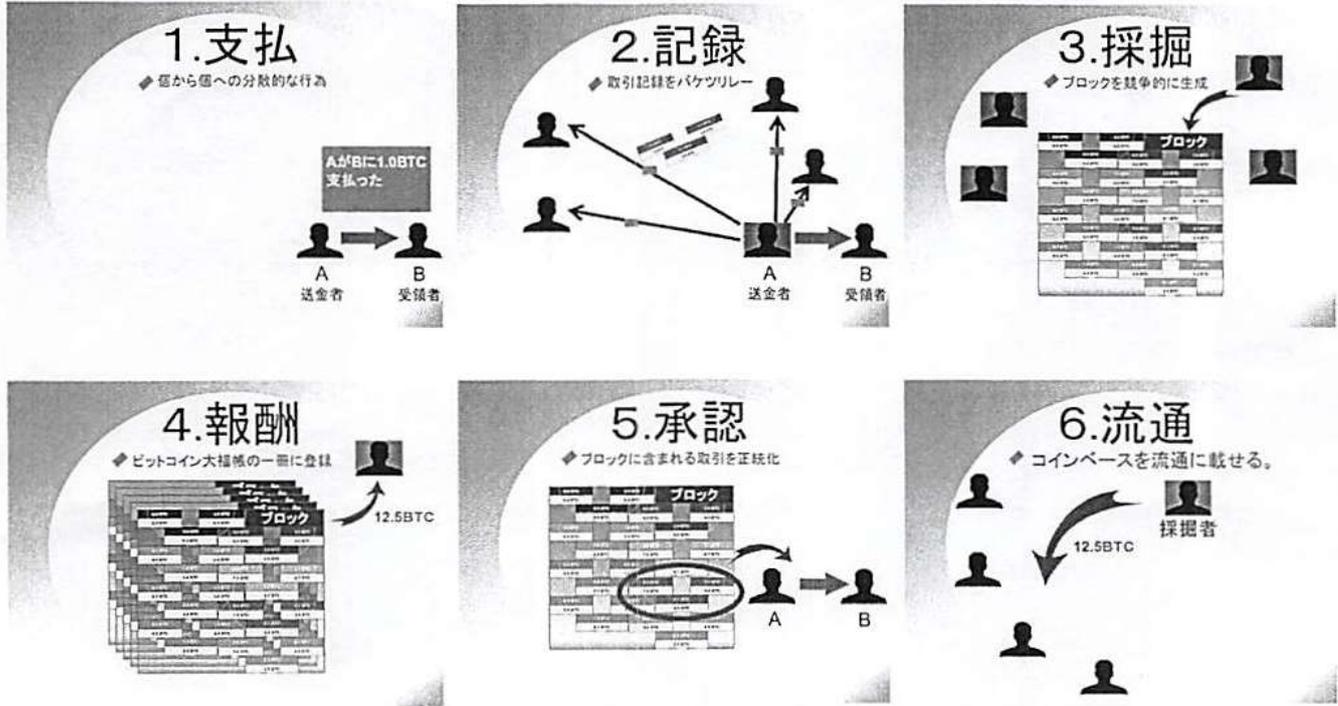
ハッシュ関数 (ハッシュかんすう、英: hash function) あるいは要約関数[1]とは、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のこと。ハッシュ関数から得られた数値のことを要約値やハッシュ値または単にハッシュという。

目次 [非表示] 1 用途 1.1 ハッシュテーブル 1.2 キャッシュ 1.3 ブルームフィルタ 1.4 重複レコードの検出 1.5 類似レコードの探索 1.6 類似部分文字列の探索 1.7 幾何学的ハッシュ 1.8 改竄の検出 2 特性 2.1 低コスト 2.2 決定性 2.3 一様性 2.4 可変な値域 2.5 データ正規化 2.6 連続性 3 ハッシュ関数のアルゴリズム 3.1 簡単なハッシュ関数 3.2 完全ハッシュ関数 3.3 最小完全ハッシュ関数 3.4 一様に分布するデータのハッシュ技法 3.5 その他の分布のデータのハッシュ技法 3.6 可変長データのハッシュ技法 3.7 特定用途のハッシュ関数 3.8 ハッシュとしてのチェックサム関数 3.9 暗号的ハッシュ関数 4 ハッシュ関数の安全性 4.1 原像計算困難性 4.2 第2原像計算困難性 4.3 衝突困難性 4.4 それぞれの困難性の関係 5 語源 6 脚注・出典 7 関連項目

ブロックチェーン・エコノミーの最新動向

= 分散台帳技術の可能性と課題を考察する =

ビットコイン・エコシステムの6ステップ



ビットコインは、支払→記録→採掘→報酬→承認→流通、の6ステップから構成される。

岡田仁志『決定版 ビットコイン&ブロックチェーン』東洋経済新報社 3

Hash関数

SHA256

- 64桁の^英数字
- 1与法定関数と言う

A97649D560A57AC4046A000A1B170AD1
16C90B10455090475A3ED37C8221F8AE

仮想通貨以外に広がるブロックチェーン

- | | |
|---------------|---------------------------------|
| Factom(ファクトム) | 貸付、証券、保険、医療、・・・ |
| Ascribe | 著作物の著作権、・・・ |
| 色々な会社 | 貿易と決済、自然資源、オイル、ハンバーガー通貨、ゲーム、・・・ |

プログラマブルブロックチェーン

Ethereum

スマートコントラクト

仮想通貨トークン

中央管理機関が無いシステム

例：NTTでの研究開発の取り組み

例：ビジネス化に向けた取り組み

参考文献等

20180507 現在-市川市図書館所蔵-ブロックチェーン 20冊

- 1 図書 ブロックチェーンをめぐる実務・政策と法 久保田 隆/編 中央経済社 2018.4
- 2 図書 教養としてのテクノロジー AI、仮想通貨、ブロックチェーン (NHK出版新書) 伊藤 穰一/著 NHK出版 2018.3
- 3 図書 入門ビットコインとブロックチェーン (PHPビジネス新書) 野口 悠紀雄/著 PHP研究所 2018.1
- 4 図書 アフター・ビットコイン 仮想通貨とブロックチェーンの次なる覇者 中島 真志/著 新潮社 2017.10
- 5 図書 超図解ブロックチェーン入門 新しいビジネスモデルがここから生まれる! 桜井 駿/著 日本能率協会マネジメントセンター 2017.9
- 6 図書 ビットコインとブロックチェーンの歴史・しくみ・未来 ニュー・サイエンティスト編集部/著 SBクリエイティブ 2017.9
- 7 図書 Blockchain Revolution How the Technology Behind Bitcoin is Changing Money, Business, and the World Tapscott,Don/A. Portfolio 2016.5
- 8 図書 The Business Blockchain Promise, Practice, and Application of the Next Technology Mougayar,William/A. Wiley 2016.5
- 9 図書 最新ブロックチェーンがよ〜くわかる本 ビットコインから学ぶ、ブロックチェーン! (図解入門) 石黒 尚久/著 秀和システム 2017.8
- 10 図書 60分でわかる!仮想通貨ビットコイン&ブロックチェーン最前線 仮想通貨ビジネス研究会/著 技術評論社 2017.6
- 11 図書 ブロックチェーン入門 (ベスト新書) 森川 夢佑斗/著 ベストセラーズ 2017.5
- 12 図書 仮想通貨とブロックチェーン (日経文庫) 木ノ内 敏久/著 日本経済新聞出版社 2017.4
- 13 図書 いまさら聞けないビットコインとブロックチェーン 大塚 雄介/[著] ディスカヴァー・トゥエンティワン 2017.3
- 14 図書 ブロックチェーン革命 分散自律型社会の出現 野口 悠紀雄/著 日本経済新聞出版社 2017.1
- 15 図書 ブロックチェーン・レボリューション ビットコインを支える技術はどのようにビジネスと経済、そして世界を変えるのか ドン・タプスコット/著 ダイアモンド社 2016.12
- 16 図書 この1冊でまるごとわかるブロックチェーン&ビットコイン 入門編 (日経BPムック) 日経ビッグデータ/共同編集 日経BP社 2016.12
- 17 図書 ブロックチェーン仕組みと理論 サンプルで学ぶFinTechのコア技術 赤羽 喜治/編著 リックテレコム 2016.10
- 18 図書 最新オープンソースがよ〜くわかる本 人工知能も、FinTech(ブロックチェーン)も、ビッグデータも、みんなオープンソースでできている! (図解入門ビジネス) 寺田 雄一/著 秀和システム 2016.9
- 19 図書 ビットコインとブロックチェーン 暗号通貨を支える技術 アンドレアス・M.アントノプロス/著 NTT出版 2016.7
- 20 図書 ブロックチェーンの衝撃 ビットコイン、FinTechからIoTまで社会構造を覆す破壊的技術 ビットバンク株式会社/著 日経BP社 2016.6