講　演　録

日本FP学会第21回大会
開催日：2020年9月5日（土）
会　場：大手町サンケイプラザ

暗号資産（仮想通貨）について 知られていること，知られていないこと

財務省財務総合政策研究所客員研究員　　石田　良

本日は，「暗号資産（仮想通貨）について知られていること，知られていないこと」とのタイトルで，暗号資産，いわゆる仮想通貨について，改正資金決済法の表現にならって，今後は仮想通貨との表現を用いずに暗号資産との表現を用いることにしますが，一体これは何なのか，どのような歴史的背景があるのか，どんな規制があるのかなどの諸々について，私の研究成果も交えながら報告させていただきたいと考えています．なお，意見に亙る部分は全て個人的見解であり，私の所属機関の見解ではありません．

＜はじめに＞

私は，2015年にアメリカのミシガン大学で経済学の博士号を取得しており，その際の専門は公共経済学だったのですが，その後2016年ごろから暗号資産にも関心を抱き，主にファイナンスの観点から論文も書いているところです．斯界の学術論文を眺めると，暗号資産の研究は今でもファイナンスの観点からの研究が多いです．ただ，後ほどご説明しますが，ブロックチェーンの記録を網羅的に解析して価格操縦のエビデンスを報告するなど，足下ではファイナンスの枠内にとどまらない研究も多数刊行されてきています．そのあたりの動向については，例えば経済セミナーなどに寄稿したりしていますので，ご関心があればご覧いただければ幸いです．

暗号資産とは？

まず暗号資産とは何なのか．何となくビットコンとかそういう名前や電子的にやり取りする何物かとか，そういったイメージはあるかと思います．実は，暗号資産は資金決済法で明確に定義付けられています．まず，不特定の者に対して代価の弁済に使用でき，かつ，不特定の者を相手方として法定通貨と相互に交換できるという要件です．仲間内だけでとか，ゲーム内だけでとか，そういったものは暗号資産ではないわけです．次に，電子的に記録され，移転できるという要件です．これは暗号資産のイメージと合致すると思います．最後に，法定通貨又は法定通貨建て資産ではないという要件です．つまり，電子マネーの類は，だいたい暗号資産にならないわけです．要件はこれだけですので，実は暗号資産に該当するものはたくさんあります．ビットコインやイーサリアム，リップルといったメジャーな暗号資産だけでなくて，例えばCoinMarketCapというウェブサイトを見ていただければ，2,000を優に超える暗号資産が載っています．法的に細かいところを述べれば，ここに載っているもの，例えばステーブルコインと言われるものですが，全て暗号資産に該当するかどうかは，ちょっと微妙なところがありますが，今回は，そのあたりの法的に細かいところには，あまり拘泥しないことにします．

電子的に財産的価値をやり取りするというのは，資金決済法の要件の通りです．また，一般的に，法定通貨の裏付けはありません．もっとも一部例外はあってですね，例えばテザーという暗号資産は，1ドル＝1テザーとなるよう調整されていて，これは法定通貨と連動することをうたっているステーブルコインと呼ばれるものであるところ，これは発行体がドルのリザーブを用意していると言っていますので，そういう例外はありますが，一般的には法定通貨の裏付けがないものがほとんど

表1　ビットコインと法定通貨との違い

特徴		ビットコイン	法定通貨（日本円）	電子マネー（第三者型前払い式支払手段）
発行・管理	発行者	■ システムが自動的に発行	■ 日本政府（通貨） ■ 日本銀行（紙幣）	■ 電子マネー事業者（第三者型前払式支払手段発行者）
	管理者	■ P2Pネットワーク参加者が管理	■ 日本政府 ■ 日本銀行	■ 電子マネー事業者（第三者型前払式支払手段発行者）
価値	発行上限額	■ 決まっている（2,100万BTC）	■ 無し	■ 事前入金された金額（日本円）の範囲で発行
	価値の裏付け	■ システムへの信用	■ 日本政府への信用	■ 供託された日本円（入金額の1／2） ■ 電子マネー事業者への信用
送金処理	送金の方向	■ 双方向	■ 双方向	■ 一方向（利用者⇒加盟店）
	送金の処理時間	■ 約10分間隔でブロックを作成 ■ 約60分で確定と見なす	■ 直接の受取であれば即時 ■ 長距離・大量だと時間がかかることもある	■ 加盟店に支払われるまで数日～1．5ヶ月程度
	送金の手数料	■ 少額 ■ 送金者負担	■ 高額 ■ 場合によって両方負担	■ 受取者（加盟店）負担
匿名性	取引の匿名性	■ 取引履歴は明らかだが、匿名性がある	■ 高い	■ 低い（履歴は電子マネー事業者が管理）
	取引履歴の公開	■ 公開	■ 非公開	■ 一般に非公開

（出所）経済産業省

です．さらに，多くの場合，暗号資産については，その取引記録などを行う中央管理機関が存在しません．これはピア・トゥ・ピアで分散管理されています．

ビットコインは，時価総額最大の暗号資産ですが，分散管理の典型で，世界のどこにもビットコインを運営している組織は存在せず，それでいながらビットコインの仕組みが回っていくという巧妙な仕組みになっています．これは技術的にはすごいことです．例えば電子マネーは，SuicaであれICOCAであれ，管理する組織というのがあって，そこが全取引データを管理しているわけです．そういった管理機関がなく取引データがピア・トゥ・ピアで分散して保存されていながら，きちんと暗号資産の仕組みが回っていくというわけですから，これはすごいことです．もっとも例外はありまして，リップルとか，ステーブルコインであるテザーとか，そういうのは中央管理機関が存在します．ただ，多くの暗号資産には，中央管理機構が存在しません．

表1は，その時価総額最大の暗号資産であるビットコイン，法定通貨，電子マネーを比較したものです．これを見ると一目瞭然なんですが，ビットコインの顕著な特徴は，管理者が存在しないことです．ピア・トゥ・ピアネットワーク参加者が管理とありますが，別に参加者にはビットコインの管理義務はないんです．それでもうまく回るのは，ビットコインのシニョリッジすなわち通貨発行益と取引手数料，これらが，参加者が自発的に行うビットコインの管理に資する行為に対する報酬としてあてられているんですね．このようにシステムが自律的に回るようにうまいインセンティブ付けが行われています．あと，ビットコインは，システムが自動的にマネタリーベースを決めており，発行上限も設けられているところ，だんだんとマネタリーベースの伸びが逓減していくという仕組みになっています．このように金融政策が事前に設定されているという仕組みになっていますが，このあたりの仕組み方は，暗号資産によってかなり異なるところです．例えば，マネタリーベースの伸びが逓減して頭打ちになるというのは，それこそフリードマンのk％ルールとは違うわけです．このあたりの金融政策の仕組み方は，いろいろとありまして，暗号資産によって様々なやり方を採用しています．

また，取引記録は，ビットコインの場合，完全にオープンとなっています．このアカウントとあのアカウントとの間で0.1ビットコインの送金が行われたとかはオープンです．もっとも，そのアカウントを誰が保有しているかとかは，オープンになっているデータからは分かりませんので匿名性はあります．皆さんがお持ちのSuicaとかPASMOに係る取引履歴は，当然ながら非公開なわけです．ですから，取引履歴がオープンである

というのは，よくよく考えるとすごい性質なわけです．もっともこれは，ビットコインの性質であって，さらに匿名性を高くした「匿名通貨」と言われるような暗号資産も知られているところではあります．

なぜ暗号資産が話題になっているか

さて，ここまで暗号資産の概要をご説明しましたが，なぜ暗号資産がここまで話題になったんでしょうか．これはやはり，価格変動の大きさが一因だと思います．一番話題になったのは，2017年後半から2018年頭ぐらいでしょうか．この価格のピークは，下のグラフをご覧いただければ分かります通り，2017年12月ですが，価格のあまりの高騰に，いろいろと巷間で話題になったことは覚えている方も多いのではないかと思います．新聞紙上を賑わせるとともに，流出事件もありました．不正アクセスにより顧客から預かっていた暗号資産が流出したという事件が何回かあったことは記憶に新しいところです．また，価格変動の大きさゆえに，「億り人」なんていうふうに呼ばれた人が何人も出てきたことが報道されました．これは，価格の高騰により1億円以上の資産を築いた人を指すそうですが，国税庁の報道発表では，暗号資産取引を含めた収入が1億円以上あったと申告した人が300人超に及んだとのことです．なお，報道では，「実際にはもっと多いはず」との指摘もありました．

暗号資産は，学術的にも話題になりました．暗号資産をよくよく考えていくと，結局「貨幣とは何か？」という究極の問題に行き当たります．過去には，大きな石，タバコのMarlboroなど，様々なものが貨幣として通用したわけですが，今回は有体物ですらない電子データです．岩井克人先生によると，暗号資産は，これまであった貨幣の中で究極の形だということです．貨幣は貨幣として使えるから貨幣であるという自己循環論法が貨幣の本質であって，暗号資産というのは電子データですが，貨幣として使えるから貨幣だと，そういう考え方に行き着くというふうなことをおっしゃっています．なぜ，法定通貨とか貴金属などのような裏付けのない暗号資産に価値があるのか．理論的な回答の一つとしては，こういうのがあり得るのかもしれません．

暗号資産の歴史

ここで暗号資産の歴史を振り返ってみたいと思います．当然，そんなに長い期間じゃありませんが，それでも何十年という歴史があります．暗号資産の前史から見ていきます．どこまで振り返ってよいか分かりませんが，とりあえず公開鍵暗号という暗号技術にまで振り返ってみます．

暗号というのは，通信の秘匿性を高めるための技術なんですが，普通に考えて，暗号化だけでなく復号化にも，つまり暗号化するだけでなくそれを元に戻すためにも鍵が必要なんですが，その鍵

○ 価格変動の大きさ

○ 事件

大手仮想通貨取引所のコインチェック（東京都渋谷区）は26日、外部から不正なアクセスを受け、顧客から預かっていた仮想通貨「NEM（ネム）」約580億円分が流出したと発表した。（朝日新聞2018/1/27）
インターネット上の仮想通貨ビットコインの取引所「マウントゴックス」を運営するMTGOX（東京・渋谷）が28日、東京地裁に民事再生法の適用を申請し、同日受理されたと発表した。債務が資産を上回る債務超過に陥っていた。顧客が保有する75万ビットコインのほか、購入用の預かり金も最大28億円程度消失していたことが判明した。（日本経済新聞2014/2/28）

○ 暗号資産で稼いだとの報道

国税庁は25日、2017年に仮想通貨取引を含めた収入が1億円以上あったと申告したのは331人だったと発表した。同年分の確定申告を集計した。仮想通貨の高騰で1億円以上の資産を築いた人が、ヒット映画の題名をもじった「億り人」と呼ばれて話題となるなどしており、業界関係者は「実際はもっと多いはず」と指摘している。（日本経済新聞 2018/5/26朝刊）

図1　価格変動の大きさ

を受け渡す時に第三者に傍受されてしまっては暗号にならないわけです．ですから，この鍵をどうやって暗号を受け取って欲しい人に渡すのかというのが，インターネット上で暗号を使うときには非常に問題になるわけです．それで，公開鍵暗号というのは，またすごい方法でして，これは整数論を使った巧妙な方法により，素数同士の掛け算は簡単だけどその逆演算である素因数分解が非常に計算量理論的に難しいというところを使ってるんですけれど，普通の文章を暗号化するための鍵と暗号化された文章を元に戻すための鍵が異なるようにしたわけです．そうすれば，暗号化するための鍵を公開したところで，それを傍受されても，問題ないんですよ．なぜならば，その鍵を使って暗号化された文章を解読できるのは自分だけですから．このように2つの鍵をつくるというのが，公開鍵暗号というものです．これを使ってインターネット上で誰もが暗号技術を使えるようになったのですが，技術的にはこれが非常に大きなブレイクスルーだったわけです．これは1977年に開発されたのですが，これが現代暗号技術の黎明だったわけです．これにより，国家とか，中央管理機関でなくても誰もが暗号技術を用いて情報をやり取りできるようになりました．

情報のやり取りができるのであれば，次は財産的価値のやり取りをしたいと．そのような暗号技術をもとに，国家とか，中央管理機関によらずにインターネット上で分散的に価値をやり取りしたいと．これは非常にリバタリアン的な発想なんですが，サイファーパンク思想と言われ，盛んになります．これが1990年代のことです．暗号技術とインターネット，この2つがあいまってサイファーパンク思想が盛んになったわけです．ただ，電子情報というのは，コピーが容易なんです．情報であればいいんですが，財産的価値となると，コピーをして二重払いを行うという不正行為をどう防ぐのか，これが非常に難しいんです．そのため財産的価値のやり取りを暗号技術を用いてインターネット上で行うこと，しかも，二重支払いを防ぐための中央管理機関なしで行うというのは非常に難しかったわけです．

こうした状況の中，出てきたのが，2018年のサトシ・ナカモトによるペーパーです．この方はビットコインの創始者で，素性は一切不明です．日本人みたいな名前ですが，日本人かどうかも不明です．約100万ビットコイン，日本円にすると概ね1～2兆円ぐらいを保有しているとも言われています．

このペーパーには，財産的価値をインターネット上で中央管理機関なしでやり取りするための仕組みが書かれています．これは非常に巧妙な仕組みで，ビットコインの取引履歴をブロックチェーンと呼ばれる鎖状の履歴保存システムに保存し，改竄が困難な仕組みを作り上げると同時に，二重支払いを防ぐために，マイナーと呼ばれる人に自発的にコンピューターの計算能力を提供してもらい，その謝礼として新規に発行されたビットコインを確率的に付与するという，Proof-of-Workと言われる仕組みを提示したわけです．そして，仕組みを提示するだけでなく，自らそれを実装し，更にきちんと運用できることも実証しています．

今，ブロックチェーンとProof-of-Workと言いましたが，まずブロックチェーンというのは非常にうまい仕組みで，最新のブロックは前のブロックの情報のダイジェスト版を含んでいます．ダイジェスト版を，暗号学でハッシュ値と呼びますが，それを次のブロックが含むという仕組みをとっています．前の前のブロックを改竄しようとしたら，そのハッシュ値を含む前のブロックも改竄しなきゃいけないわけです．そうすると，その前のブロックのハッシュ値を含む最新のブロックも改竄しなきゃいけないという仕組みなので，最新のブロックだけであればまだ改竄できるかもしれませんが，古いブロックの改竄はほぼ不可能になってしまうという，そういううまい仕組みになっています．

次に，Proof-of-Workという仕組みも非常に巧妙です．これは，二重支払いを防ぐためにマイナーと呼ばれる者に自発的にコンピューターの計算能力を提供してもらいます．このマイナーというのは，完全に自発的にコンピューターの計算能力を提供するんですが，なぜそんなことをするのかと言いますと，コンピューターの計算能力の提供に対して，謝礼として新規に発行されたビットコイン，あと取引手数料もありますが，それを確率的に贈呈するという仕組みになっています．つまりシニョリッジ，通貨発行益をシステム管理のための謝礼にあてるというインセンティブ付けが行われているわけです．

このようにしてビットコインというのができて，暗号資産の幕が開けたわけです．2009年1月に運用が開始されたんですが，初めて取引，実際の物と取引されたのは，2010年5月，ピザ購入に使われたときです．2011年から13年には，Silkroadと呼ばれる麻薬等の取引ウェブサイトでビットコインが利用されました．2013年には，ビットコインの価格が高騰しました．これは，キプロス危機やSilkroadなどが原因ではないかと言われています．2013年から14年には，MtGox事件という流出事件があったことは，ご記憶の方も

多いかと思います．このMtGox事件のあたりから，人口にも膾炙してきまして，一部エンジニア以外の方も結構暗号資産というのを知ることになったところです．2015年には，金融活動作業部会という国際的な枠組みでも，どのような規制を行うかというような議論が行われ，2017年には改正資金決済法が施行されました．2017年12月にかけて，ビットコインの価格が高騰し，1ビットコインが1千ドルから2万ドルまで上がったということがありました．2018年1月にコインチェック事件という流出事件がありました．

こうしたことを受けて，特に2015年あたりから国際的な議論というのも行われてきたところです．今でも行われています．G7，G20，金融活動作業部会，いろいろな場面で議論が行われています．法整備も進んできています．例えば暗号資産を消費税法上，非課税対象取引とするとか，最新の改正資金決済法が令和2年5月に施行されて仮想通貨の呼称が暗号資産に変更されたとか，さらに暗号資産交換業に係る制度整備，暗号資産を用いたデリバティブ取引や資金調達取引に関する規制の整備というのが行われたところです．

諸外国でもいろいろと規制を行なっています．例えば，シンガポール，韓国，アメリカ，EU，英国，インドネシア，中国など，いろいろな規制が日々検討されて行われてきています．

最近の暗号資産の話題

最近の暗号資産の話題について触れておきます．いくつか話題ありますが，例えば，国内外の銀行において，銀行発行コインの開発が進められています．これは大手の三菱UFJ，みずほ，UBSなどです．

他の話題，懸念点では，匿名性の高い暗号資産に対して，様々な懸念が呈されています．あとビットコインのマイニングです．もともとは，個人の持っているようなパソコンでもできたんですが，今ではもう「軍拡競争」と言われて，1つのパソコンどころか，写真をご覧になった方は分かると思いますが，もう凄まじくでかいです．スーパーコンピューターみたいなもんです．専用のコンピューターを用いた大規模なマイニングというのが設けられていて，そこに伴う電力消費が膨大になっているということが懸念されています．

アカデミックにもいろいろと話題になっています．例えばビットコインの市場は，昔は非効率だったものの最近は結構成熟してきており，昔よりは非常に効率的になってきたというのが，経済学というかファイナンスにおけるコンセンサスになっています．また，ビットコインの採用しているProof-of-Workは，先ほど写真でも見ていただきましたように，電力の消費量が大きくなりがちであると．一説によるとアイルランドの電力消費量に匹敵するのではないかというふうに言われているぐらいです．あとは，ビットコイン市場における価格操縦を指摘していたりするような研究もあります．例えば2013年の価格上昇は，Journal of Monetary Economicsという一流誌に掲載されたのですが，2つのダミーアカウントによる価格操縦があったのではないかとの報告があります．また，2017年の価格上昇は，別の暗号資産を通じた価格操縦があったのではないかと言われています．後者のほうは，ブロックチェーンのデータを全て読み込んで，そこから，このようなエビデンスが見つかったという，非常に重厚な研究であり，Journal of Financeという一流誌に掲載されています．このように，暗号資産に関する研究も非常にたくさん出てきています．

私などの研究も掻い摘んでご説明させていただきます．1つは，暗号資産の先物市場の話です．暗号資産，特にビットコインは，2017年12月にピークを迎えた後に価格の暴落が起こりましたが，実は同じ2017年12月にアメリカのシカゴにある大手取引市場であるCBOEとCMEで相次いでビットコインの先物が導入されました．先物の導入とビットコインの価格暴落というのが，時期的に非常に近いんです．これについては，Hale et al.という論文（FED・サンフランシスコ）で，ビットコインの先物導入がビットコインの現物市場の暴落を招いたというような説が唱えられています．私たちの研究では，イントラデイデータを使ってVAR，Vector Autoregressionを行なって，ビットコイン先物の取引がビットコイン現物価格に影響を与えているとは言えないというようなことを，すなわちこのHale et al.を否定するような結果を出しています．つまり，ビットコイン先物の導入は，ビットコインの価格暴落を招いたという説は間違っているのではないかという論文を書いたところです．こちらはNorth American Journal of Economics and Finance誌にforthcomingとなっています．

次は，暗号資産の現物市場と先物市場の間に裁定機会が存在するかということを，これもイントラデイデータを用いて確認しました．通常は，裁定機会は存在しない．だから，非常に効率的であると．ただし，先物導入直後の市場暴落期には，裁定機会は存在したというふうな結果を出しているところです．こちらはJournal of Futures Markets誌にforthcomingとなっています．

今後の進展

最後に，今後，暗号資産はどうなっていくかということについて話しておきたいと思います．例えばビットコインではブロックチェーンが使われていると言いましたが，このブロックチェーンをビットコイン以外のところでも要素技術として使おうという取り組みが，いろいろ行われているところです．東証が，ブロックチェーン技術を検証実験して，証券取引の後工程の業務効率化の可能性を指摘しています．諸外国では，ホンジュラスが，土地登記の記録簿にブロックチェーンを使うことを検討する等，要素技術としてのブロックチェーンが，プロミッシングなところであがっています．

あとは，スマートコントラクトです．契約の自動執行なんですが，時価総額が2番目に多いイーサリアムが得意な分野なんですが，この分野も訴訟に革命をもたらすのではないかというふうな期待を持っている人もおります．

最近ですとICOというよりIEOが多いかもしれませんが，資金調達をトークン，暗号資産みたいなものですが，で行うというふうな取り組みもいろいろと関心を呼んでいるところです．

国際的にも様々なところで議論されていて，今後どのように国際社会が暗号資産を取り扱っているかというところも非常にウォッチすべきところかなと考えています．

ちょっと駆け足ではありましたが，暗号資産の現状についてご報告させていただきました．ご清聴ありがとうございました．