暗号通貨 対 伝統的システム

齋藤哲哉

プレゼンテーションの概要

- 伝統的通貨と暗号通貨のハイライト（概要のみ）
- 暗号通貨の価格形成理論
- 従来の決済手段との競争
- 今後の展望

暗号通貨と伝統的通貨の相違点

- *e-Cash by M.* フリードマン
- 暗号通貨と類似マネー
- 暗号通貨と分権化システム
- *PoW*は新しい概念？
  - 簡単なモデルによる分析
- 犯罪に利用されやすい？

e-Cash by M. フリードマン

- Satoshi Nakamoto (2008)から遡ること約10年
  - インターネットの解放から始まったe-Mailの誕生が郵便事業を激変させたように
  - e-Cashが金融システムを激変させることになるだろうと
  - 1999年に受けたインタビューで答えている
  - その実現時に問題となるのは、いかにダブルペイメントを防ぐことができるかという点であることも言及している

https://www.youtube.com/watch?v=6MnQJFEVY7s

暗号通貨と類似マネー

- 暗号通貨を単なる電子決済システムと考えることは誤解を生む原因となる
  - Suicaに入っている日本円は暗号通貨ではない（仮想通貨かも...）
  - JALのマイレージをAmazonのクーポンやSuicaのチャージに交換できるが、暗号通貨ではない
- 以前よく言われていたような、発行主体の有無が決定的な暗号通貨とその他の類似マネーを区別する特徴でもない
- 暗号通貨は（決済という）契約を交わす目的でデザインされた、暗号署名システムと捉えたほうがわかりやすい【詳細は次スライド】

暗号通貨と分権化システム

- 契約が交わされた事実を限りなく安全に保存しなければならない
  - 集権的なサーバーで管理しようとすると、かなりのコストを支払う必要がある
- 分権化によって、不特定多数のサーバーが契約履歴を保存していれば、紛失や改ざんのリスクが格段に低減される可能性がある
  - それぞれの暗号通貨は、それぞれの通貨が用いられた経緯（ブロックチェーン）を指紋のように持っており、それを照合する（マイニング）ことによって、それぞれの真贋が判定される
  - 契約の履行（決済）は指紋の多数決による照合作業が済んだ段階で行われるが、これには相当の電力が必要な場合がほとんどであるが、これが分散化されて行われており、生態系が保たれている（最初に作業が完了したマイナーが報酬を受け取る）
  - これを集権的に行おうとすると、相当な電力を負担しなくてはならない

PoWは新しい概念？

- PoW (Proof of Work)はBitcoinをはじめとする多くの暗号通貨で取り入れられている照合作業である
  - 他にも様々なバリエーションが考案されている
- これは本当に新しい概念なのか？
  - PoWは多重支払いや偽コインを排除するためのシステムである
  - 伝統的通貨にはこの機能が実装されていない？
    - 伝統的通貨の取引履歴を調べるのは非常に困難であるが、電子情報と違って、偽札は見た目でかなりの確率で判別できる
    - 偽札は取引の過程で排除されていく可能性が高いため、ホンモノであることが判別できれば、そのお札の取引履歴を調べる必要はないため、ブロックチェーンを確かめる必要はない（ホンモノの存在が見えないPoWになっている）

犯罪に利用されやすい？

- マネーロンダリング
  - 犯罪性のある取引を識別する技術が確立された
  - キャッシュアウトする時点で規制のかかった銀行等の金融機関を通過しなければならず、優れた媒体であるとは必ずしも言えない
- 脱税
  - オフショアの金融機関に預けているのと同様
  - 伝統的通貨に比べると、小規模な脱税は発生しやすいかもしれない
- 詐欺やハッキング等による窃盗、違法性取引
  - 伝統的な貨幣なら、詐欺や窃盗、違法性取引は起きないのか？
  - ハッキングは仮想通貨の大きな問題であるが、伝統的貨幣の世界でも、ネットバンキングへの攻撃や、物理的な強盗も存在する

暗号通貨の価格形成理論

- 暗号通貨は単なるバブル？
- 理論的枠組み
- 伝統的決済システムの均衡
- 新しい決済システムの導入

  【補論】*BTC*暴騰と決済
- 均衡分析による展望

暗号通貨は単なるバブル？

- 当初からよくバブルと言われており、残念ながら、これまでの多くの経済学系の実証論文の論調はこの通りである
  - 確かに投機的な動きは存在するが、それが「バブルの存在」＝「目に見える破綻」という構図のみで語るのは、分析者の横暴でしかない
    - 決済プラットフォーム（契約媒体）としての需要が発生することが予見されていれば、投機的な動きも発生することが容易に予見できる
  - FinTechが叫ばれてからは論調が変わりつつあるかもしれないが…
- 本来ならば、例えば暗号通貨の決済プラットフォーム（または契約媒体）としての需要と、その所有権への投資をベースとした、決済プラットフォームのレンタル市場での価格付けの議論をすべきである

通貨としての理論的枠組み

- ２種類の決済手段
  - 伝統的な手段（銀行など）と新しい手段（暗号通貨）
- 送り手（Buyer）
  - 財・サービスを消費する
  - 財・サービスの提供者が指定する決済手段で支払いを行う
- 受け手（Seller）
  - 財・サービスの提供相手から支払いを受ける
  - 着金まで時間がかかる
  - 期待収益からリスク項を引いた利得を最大にするように行動する

数理モデル

受け手の利得関数

$$v_{i,t,k} = \frac{\mu_{i,t+\tau_k}}{(1+s)^{\tau_k - 1}} - \frac{\phi}{2} \cdot \sigma_k^2 - c_{i,t},$$

$$\rho^2 = \sigma_1^2 / \beta_{i,t}^2$$

総金額と受取額

$$\mu_{i,t+1} = (1 + \omega_{t+1})\, \beta_{i,t}$$

$$1 + \omega_{t+1} = \pi_{t+1} / \pi_t$$

暗号通貨による送金の条件

$$v_{i,t,0} > v_{i,t,1}$$

$$(1 + \omega_{t+1}) - \frac{1}{(1+s)^{\tau - 1}} > \frac{\rho^2}{2} \cdot \psi\left(\beta_{i,t}\right),$$

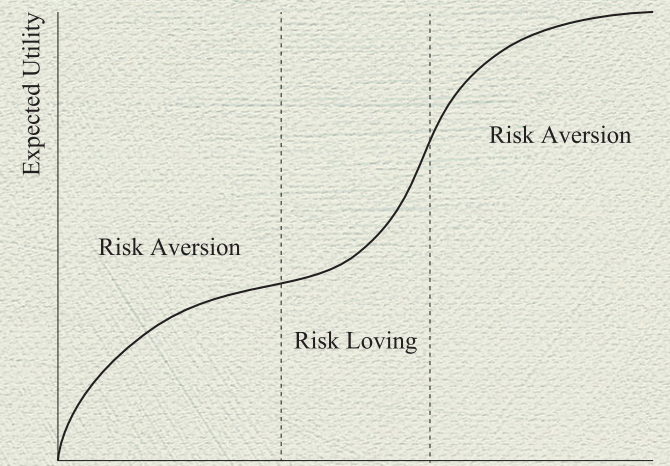
$$\delta = (1 + \omega_{t+1}) - \frac{1}{(1+r)^{\tau - 1}}.$$

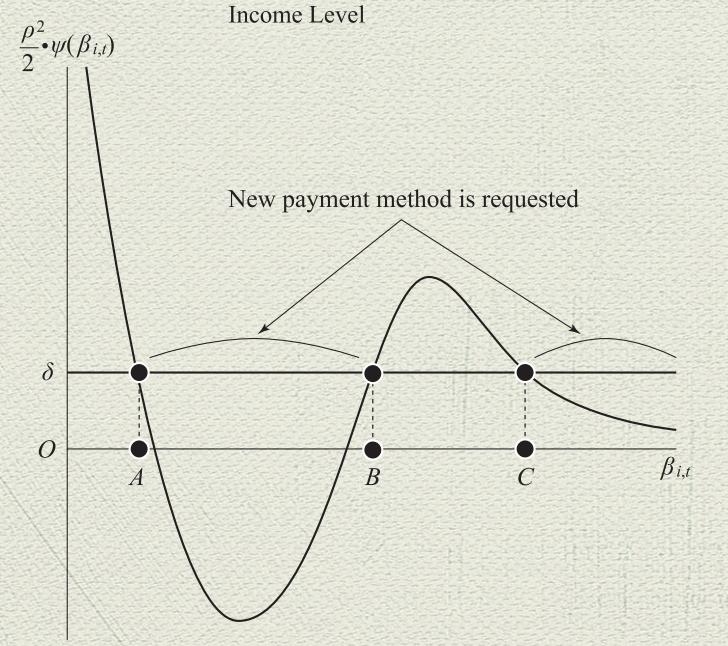
送金の総需要額

$$B_t = \sum_{i \in \Theta} \beta_{i,t}$$

需要と供給

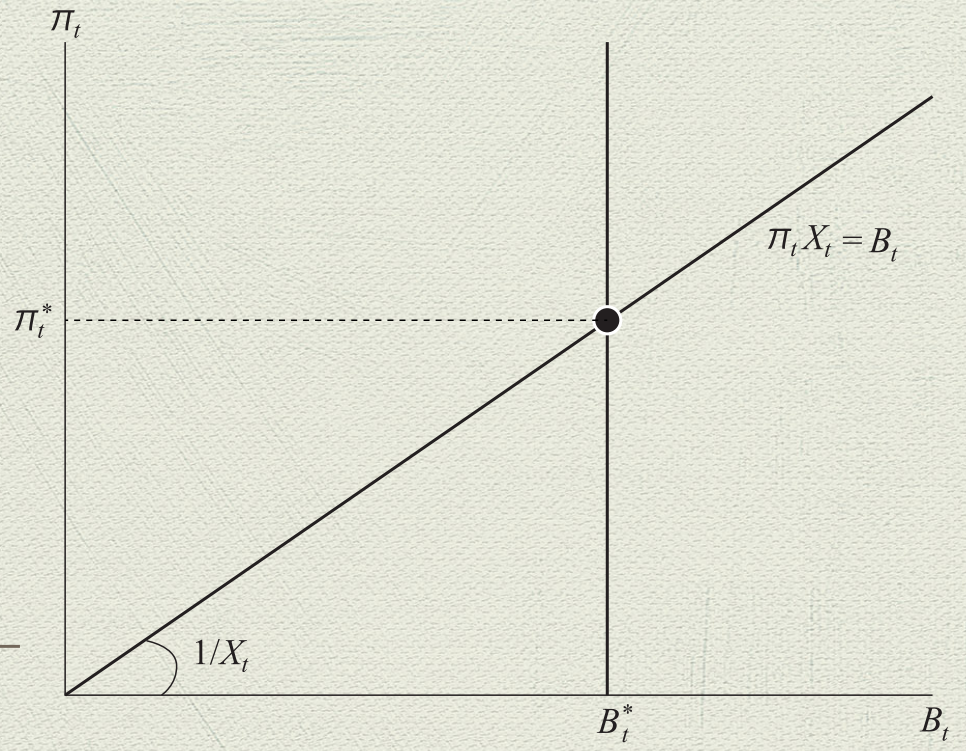
- 供給はあらかじめ決められているか、またはその価格に応じて眠っている供給が引き出される
- 需要は送金手段としての需要により発生する
- その結果として価値の発生が見込まれるようになり、投機の発生は避けられない





均衡価格

- 変数
  - B_t = 暗号通貨による送金総額
  - X_t = 暗号通貨供給量
  - π_t = 暗号通貨価格
- 暗号通貨の増加は価格の低下を招く
- 総金額の増加は価格の上昇を招く

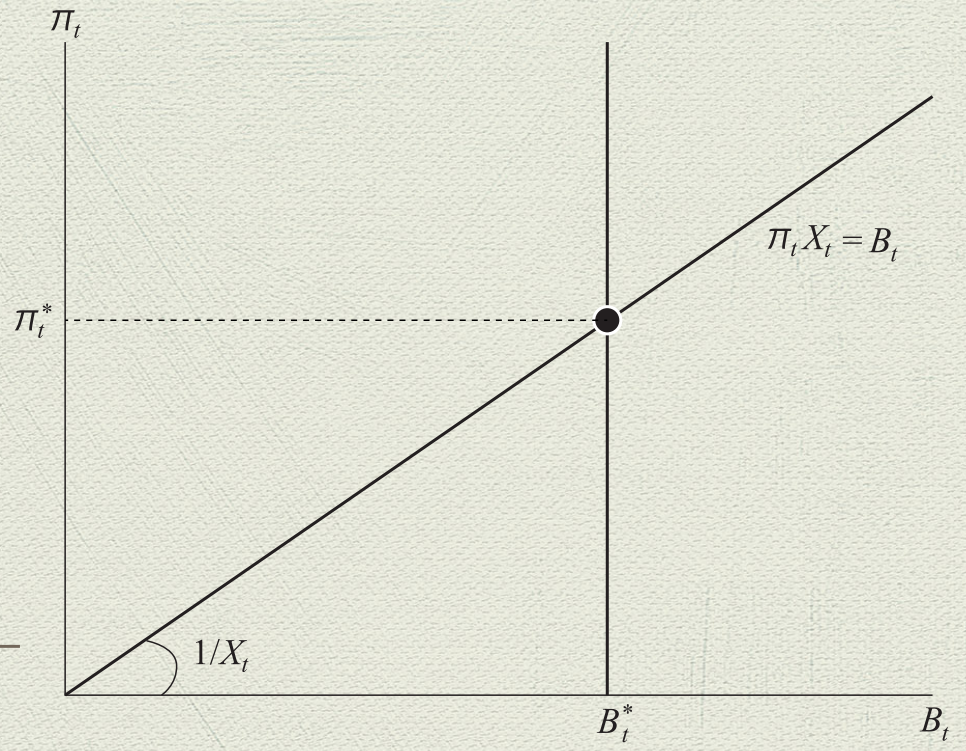


契約媒体としての再解釈

- １つの契約ごとにmコインが必要（下付け添え字省略）
  - 例えば、各契約ごとに１コイン、または、条文１つごとに１コインなど
- 契約に必要なコインの総数をM（下付け添え字省略）とすると、貨幣としての価格形成理論がそのまま応用できる

均衡価格

- 変数
  - B_t = 暗号通貨による契約総数
  - X_t = 暗号通貨供給量
  - π_t = 暗号通貨価格
- 暗号通貨の増加は価格の低下を招く
- 契約総数の増加は価格の上昇を招く



このモデルによる展望

- 暗号通貨の価格は暗号通貨の需要と供給によって決まる（当然の結果）
  - 需要は送金やその他の契約によって発生する
- 需要の発生が見込まれている市場での投機の発生は防ぐことができない
  - バブル性の取引も存在し得る
- 暗号通貨の価値が契約媒体として裏打ちされることで、逆説的ではあるが、通貨として流通する可能性が出てくる
  - しかし、高いボラティリティがある場合、通貨としては使いにくい
  - この時、Fiat MoneyではなくCommodity Moneyとしての性格が強くなるのでは？
  - ただし、巷で言われるような、ゴールドのような性格のものではない（供給量が制限されていることが価値の裏打ちにはならない）

従来の決済プラットフォームとの競争

- 理論的枠組み
  - 収束的均衡
  - シミュレーションの方法
- 通貨不安定国での競争
- 通貨安定国での競争
- 決済手段を超えた機能

理論的枠組み

- ２種類の決済手段
  - 伝統的な手段（銀行など）と新しい手段（暗号通貨）
- 送り手（Buyer）
  - 財・サービスを消費する
  - 財・サービスの提供者と交渉した結果に従って支払い手段のシェアを決める
    - ナッシュ交渉解
- 受け手（Seller）
  - 財・サービスの提供相手から支払いを受ける
  - 着金まで時間がかかる
  - 期待収益からリスク項を引いた利得を最大にするように行動する（CARA選好を仮定）

ナッシュ交渉解

- 買い手は与えられた予算全額（I）を消費する
- 売り手と買い手は財の価格（P）と暗号通貨による支払い額（$\beta = \pi B$）に関して交渉を行う（下付け添え字は省略）
- 利得関数は売り手・買い手ともに前出のモデルと同様

フィッシャー方程式

$$\bar{\delta}_{t+1} \equiv \bar{r}_{t+1} - \bar{\omega}_{t+1}.$$

CARAの下でのナッシュ交渉解

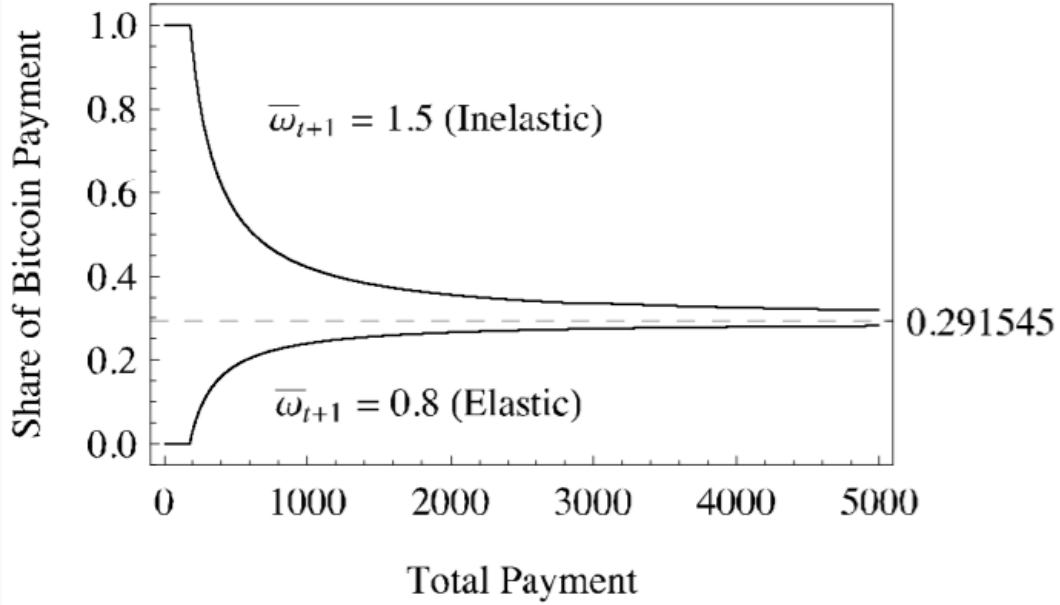
（γは従価的手数料率）

$$\beta_t = \frac{I_t Var[r_{t+1}] - \frac{\bar{\delta}_{t+1} + \gamma_t \bar{\omega}_{t+1}}{\phi}}{Var[r_{t+1}] + (1-\gamma_t)^2 Var[\omega_{t+1}]}.$$

収束的均衡

暗号通貨による支払いのシェア（$\theta = \beta / I$）

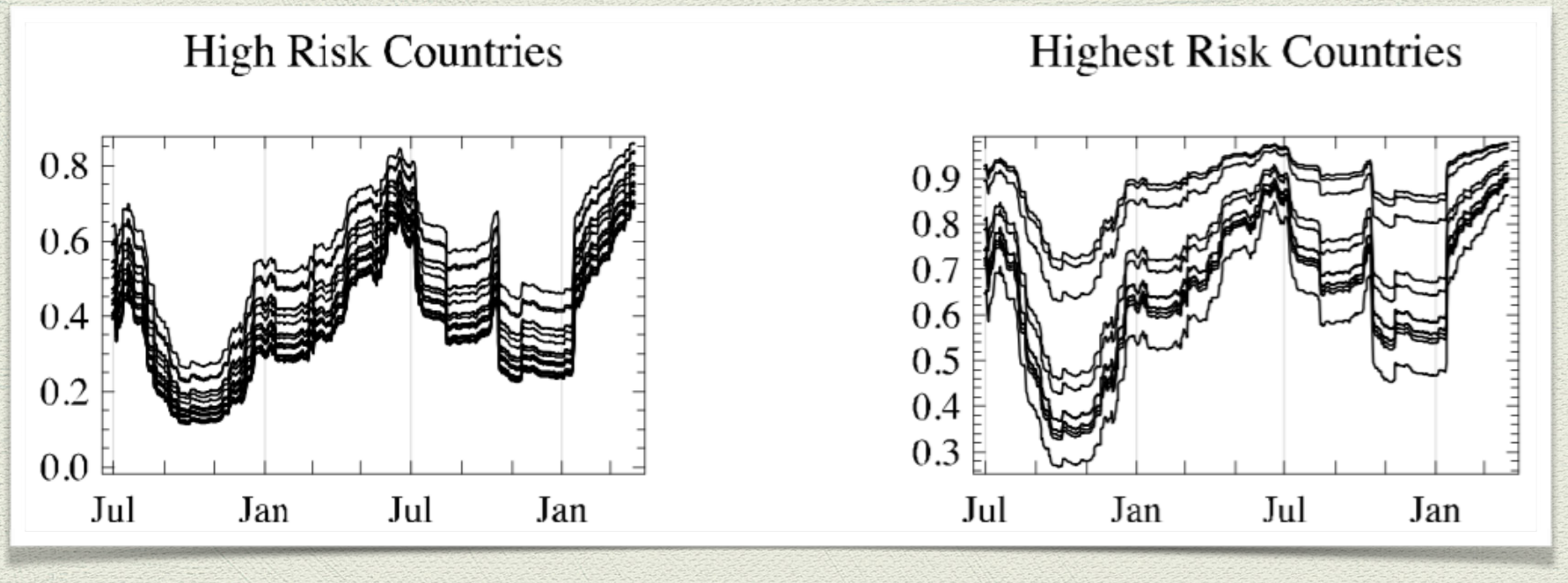
$$\theta_t = \frac{Var[r_{t+1}] - \dfrac{\bar{\delta}_{t+1} + \gamma_t \bar{\omega}_{t+1}}{\phi I_t}}{Var[r_{t+1}] + (1-\gamma_t)^2 Var[\omega_{t+1}]} \to \frac{Var[r_{t+1}]}{Var[r_{t+1}] + (1-\gamma_t)^2 Var[\omega_{t+1}]} \quad (I_t \to +\infty).$$



数値シミュレーション

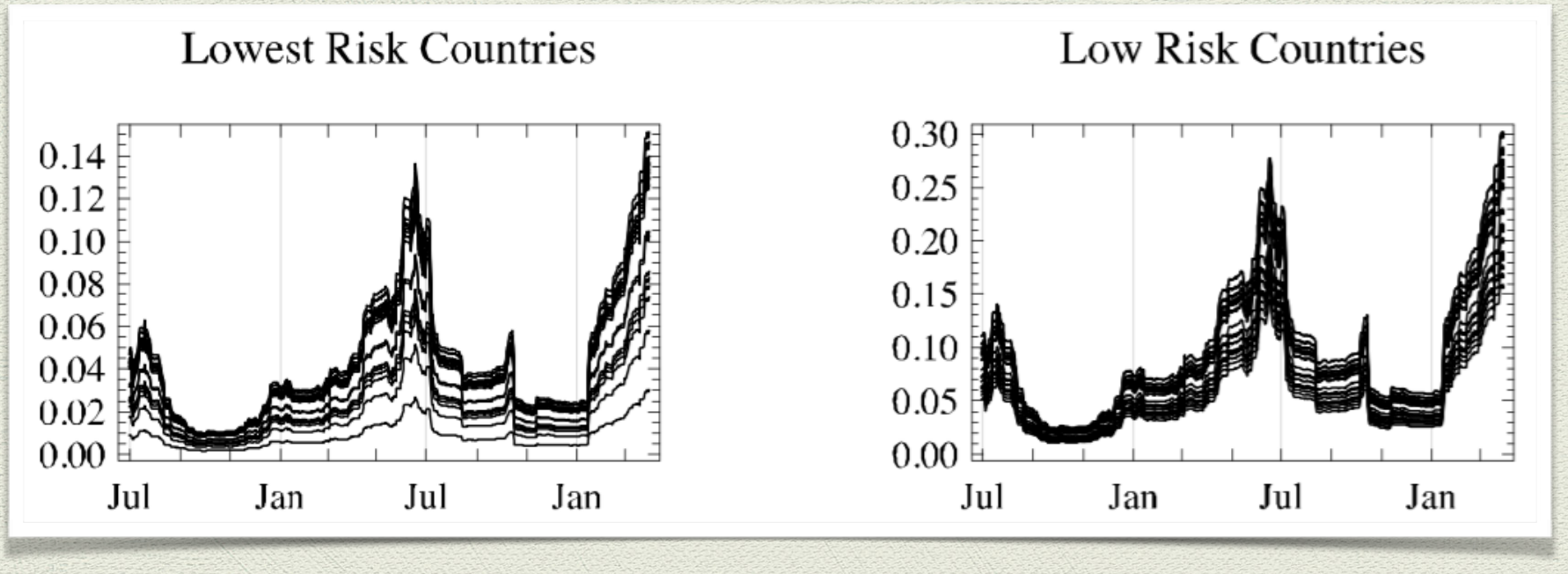
- シミュレーションの方法
  - 収束シェア（θ）をシミュレート
  - 伝統的通貨のフラつきは年次CPI（2009〜2015）を利用して計算
    - CPIのフラつきの大きさでそれぞれの国の通貨のリスクを計測
  - 暗号通貨のフラつきはBitcoinの日時データを使用（2010〜2015）
    - 90日の移動平均の分散を計算
- 結果
  - ハイリスク国では潜在的に８割以上の決済がBitcoinで行われる
  - ローリスク国では潜在的に１割程度の決済しかBitcoinで行われない

通貨不安定国での潜在的シェア



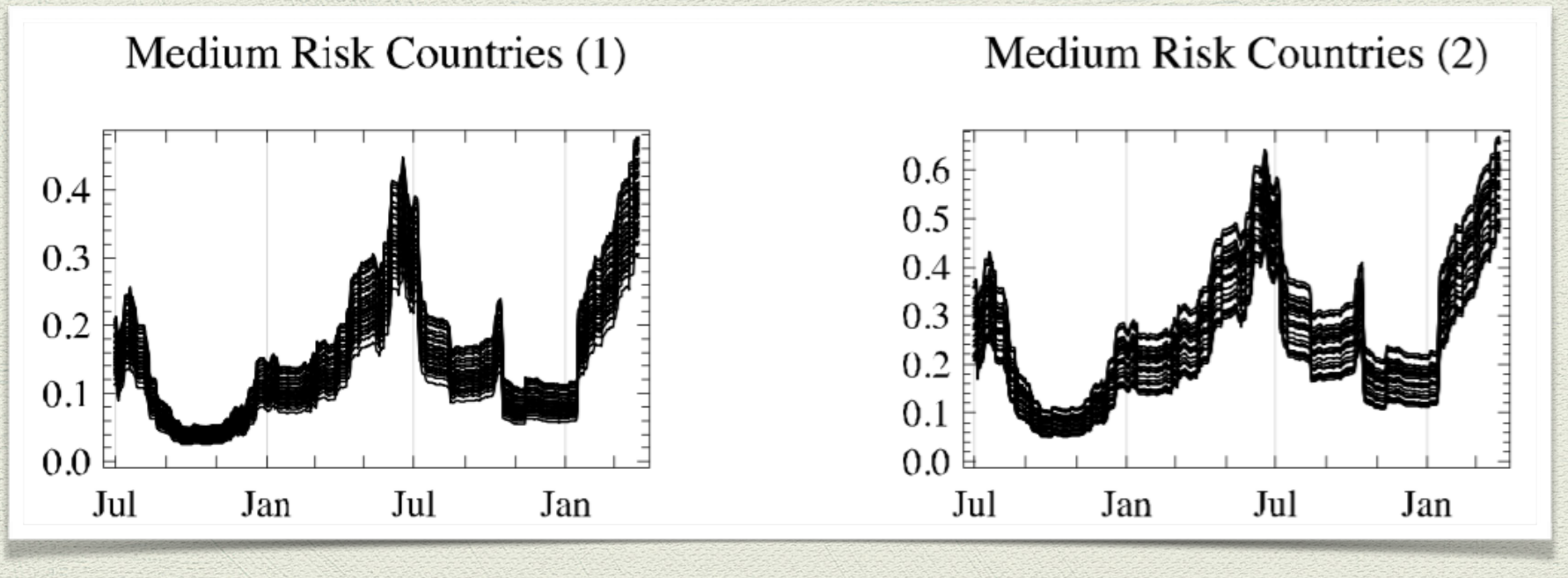
- 各国の通貨のリスクを物価変動リスク（CPIの分散）で測った場合、そのリスクが大きい国では、Bitcoinの潜在的なシェアはかなり高くなり、９割に届くような国も存在する

通貨安定国での潜在的シェア



- しかし、物価変動のリスクが小さい国々では、Bitcoinの通貨としての潜在性は非常に小さい
- ただし、後で議論するように、契約媒体としての需要を考えると、話は違ってくる可能性が大いにある

中間的な国々での潜在的シェア



- 中間的なリスクの国々では、当然ではあるが、小さいとは言えないシェア、例えば10%以上のシェアを獲得する可能性がある。

国別リスク

Table 2: Classification of countries by risk (volatility) of national currency

Lowest Risk Countries	MEX, NPL, CRI, CHE, DEU, MAR, COL, AUS, AUT, BRA,ARE, PHL, GMB, USA, NOR, FRA, SMR, CAN, NLD, NAM
Low Risk Countries	MYS, THA, VUT, BRN, PER, HND, TUN, URY, SVN, ZMB, IDN, ALB, LSO, ECU, MLT, DNK, JOR, NIC, KHM, LUX, TUR, BHS, FIN, KWT, CZE, HKG, GBR, GTM, ISR, ITA
Medium Risk Countries (1)	KOR, CHL, KAZ, ESP, SWE, RUS, BEL, OMN, TGO, CHN, ISL, JPN, IRL, HRV, MAC, PAN, HTI, BHR, SAU, MUS, MDA, NZL, NER, EGY, BWA, SEN, BTN, LTU, PRT, LKA
Medium Risk Countries (2)	MKD, SGP, CIV, CPV, BGD, POL, SVK, MDG, SLV, BIH, EST, BFA, MNE, CYP, ROM, PRY, LVA, IND, BGR, WSM, DOM, TON, JAM, GNB, QAT, MLI, NGA, DZA, HUN, ABW
High Risk Countries	ARM, KSV, GRC, BOL, MNG, GHA, PAK, RWA, STP, BEN, TJK, AGO, FJI, SRB, ZAF, AFG, SYC, KEN, SLE, GEO
Highest Risk Countries	TZA, KGZ, MDV, BDI, TMP, VNM, UKR, SUR, UGA, MWI, IRN, ETH

決済手段を超えた機能

- 暗号通貨の通貨としての機能では、ハイリスク国でしか潜在的な可能性はない
- しかし、契約媒体という機能が付け加わることで、ローリスク国でも需要が発生する可能性がある
- 取引量の増加は通貨の安定をもたらすとすれば、ローリスク国でも暗号通貨が通貨として流通する可能性がある
  - 安定がなければ、契約媒体の機能としてのみ（そしてそれに付随する投機的需要）の流通となる

今後の展望

- スタンダードな経済学モデルの確定
  - 理論・実証・実験による検証サイクル
  - ある程度共通のスタンダードに基づいた議論
  - 政策的含意を導いて実際に生かす
  - 経済学を含んだ学際的アプローチ
- 産官学の連携
  - 産業界にデータが集中している
  - 暗号通貨が台頭した際の金融政策
  - 実務的な法律と適正なビジネス環境の整備
  - 適正な暗号通貨産業の育成