ディジタル・トークンの不確定性と二項モデルによるリスクヘッジ評価

松浦幹太
(東京大学大学院情報学環・生産技術研究所)

あらまし： セキュリティ技術のおかげで電子取引可能になるトークンには、価格変化以外にも不確定性リスクが伴う。例えば、その使用に必要な証明書等の信頼度が時間的に変化すれば実質的な価値も変化せざるを得ない。この種の変化は予測不可能であり、リスクが生じる。本稿前半では、そのようなトークンを、4つの属性（価格、価値、時刻印、内容）を有する security token(setok) としてモデル化する。

近現代金融は、ディリバティブ評価理論によってリスクヘッジ実務を大きく発展させた。より動きの速いディジタルの世界では、評価理論はさらに重要となろう。本稿後半では、二項モデルに従う単純な一次元価値 setok を例に取り、リスクヘッジ評価の基礎理論を示す。

Uncertainty of Digital Token and Risk-Hedge Evaluation in a Binomial Model

Kanta Matsuura
(IIS, University of Tokyo)

Abstract: Network-security technologies allow us to trade various digital tokens. In addition to their prices, the tokens are likely associated with other important numerical values. These values may change unpredictably over time and cause risks. This paper models those tokens as *security token*, which is abbreviated into a word coinage *setok*. Each setok has its explicit price, explicit values, and timestamp on it as well as the main contents. For risk-hedging purposes, a derivative written not on the prices but on the values is introduced to a single-valued token. The derivative is priced in a binomial model.

1 はじめに

セキュリティ技術のおかげで、様々なトークンが電子取引可能となる。それらのトークンには当然価格があり、予測不能な価格変動に起因するリスクが存在するのは通常の商品と同様である。しかし、信頼できるディレクトリにすべてのエンティティが実時間アクセスできるとは限らないネットワークの世界では、第一義的な価格変動以外にも不確定性リスクが伴う。例えば、その使用に必要な証明書等の信頼度が時間的に変化すれば実質的な価値も変化せざるを得ない。この種の変化は予測不能であり、リスクが生じる。ここでは、この価値を背景価値 (implicit value) と呼ぶことにする。

図 1 のようなトークン循環アーキテクチャを考えよう。特殊な管理業務（例えば著作権管理や鍵管理）が必要なため、誰もがトークンを作成できるわけではない。常に個々の背景価値を把握しているプロバイダ (Object Provider) が作成する。業務審査基準を満たして認可を受けたような（少なくともその意味では信頼できる）組織が典型的であろう。トークンには、発行時の背景価値を額面価値 (explicit value) としてプロバイダが書き込むことができる。

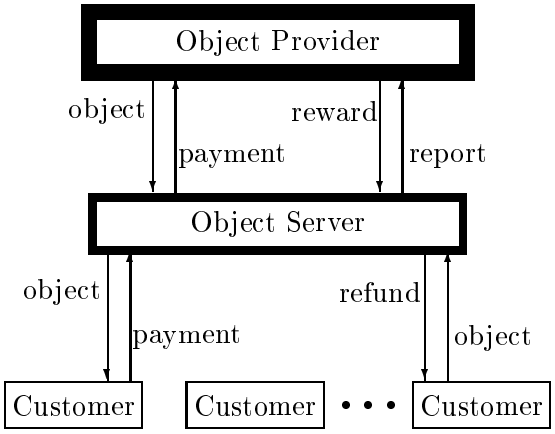

図 1: 管理が容易でないディジタル・トークンの流通アーキテクチャ

顧客 (Customer) は信用できない。しかるべき認証を経なければ情報セキュリティの観点から信用できないのは当然であるが、通信回線品質やしたがって背景価値の把握度、さらには経済的な信頼性も貧弱である。そのような不特定多数の顧客にトークンを販売または配布するためには、また特殊なサービス技能を要する。したがって、プロバイダから卸を受けたサーバ (Object Server) がこの業務を担う。不特定多数のいわば通りすがりの顧客を相手にするので、現存の金融機関と顧客の関係のように口座制 (accountability) を仮定することはできない。よって任意に細かい額をやり取りすることは原則として無理であり、トークン単位の制約を受ける。なお、プロバイダと優先的に通信できるサーバは、背景価値の現在値にランダムアクセスできる可能性がある。

トークンに添付された広告や取引量拡大による名声、管理上のメリットなどが動機となって、プロバイダはより多くのトークンがより頻繁に流通することを望む。自身が適切な管理をしているためトークンは一般には複製自由ではないから、循環を促すために報酬 (reward) を用意する。顧客がトークンを手放してくれなければ循環は進まないので、購入価格と比べて額がどの程度かはともかくとして、何らかの払い戻し (refund) が望まれる。再販の容易性は、そのトークンがかつて購入された際の価格だけでなく、額面価値や背景価値にも依存し得る。

以上を念頭に置き、第 2 章ではトークンをモデル化し、諸性質を定義する。第 3 章では、単純なトークンに対してリスク・ヘッジのためのディリバティブを定義し、その評価を行う。

2 トークンモデルと諸性質

2.1 モデル化

Definition 2.1 (Setok)
security token (setok) とは、4 つの属性

内容 (contents): 必要ならば MAC や電子署名等も含む。

額面価格 (explicit price): 顧客が購入時に支払った非負の価格。$\bar{S}$ で表す。

額面価値 (explicit values): 購入時における内容の質を表現する非負の数値の組。$\bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m$ で表す。m は額面価値の**次元**と呼ぶ。各要素 $\bar{V}_i$ が大きければ大きいほど、高い質を表す。

時刻印 (timestamp): 購入時刻 t_0 を信頼できる方式で示す。

を額面に持ち、

背景価格 (implicit price): 時間とともに変動し得る非負の数値。S で表す。

背景価値 (implicit values): 時間とともに変動し得る非負の数値の組。$V_1,\ V_2,\ \cdots,\ V_n$ で表す。n は背景価値の**次元**と呼ぶ。

と次のように関連づけられているディジタル・オブジェクトである。

- 額面価格は**価格解釈過程** *(price-interpretation process)* $Y(t)=y\left(t, S\left(t\right)\right)$ の購入時における実現値 *(occurrence)* である。価格解釈過程は非負過程である。$y=(t,s)$ は**価格解釈関数** *(price-interpretation function)* と呼ばれ、s に関して単調増加である。顧客は額面価格を書き換えることはできない。
- 額面価値は**価値解釈過程** *(value-interpretation processes)* $H_1(t)=h_1(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$, $H_2(t)=h_2(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$, $\cdots$, $H_m(t)=h_m(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$ の購入時における実現値 *(occurrence)* である。すべての価値解釈過程は非負過程である。$h_1(t,\ v_1,\ v_2,\ \cdots,\ v_n)$, $h_2(t,\ v_1,\ v_2,\ \cdots,\ v_n)$, $\cdots$, $h_m(t,\ v_1,\ v_2,\ \cdots,\ v_n)$ は**価値解釈関数** *(value-interpretation functions)* と呼ばれる。顧客はどの額面価値も書き換えることはできない。

システムとしての *setok* は、*notation* を明示したい時には $(S, Y; V, H, n, m)$ などと表記する。発行済みの個々のデータオブジェクトとしての *setok* は**シェア** *(share)* と呼ばれ、$(\bar{S}; \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m; t_0)$ などと表記される。

Definition 2.2 (Single-Valued Setok) *setok* は、その額面価値が 1 次元である場合かつその場合に限り、**一次元価値である** *(single-valued)* といわれる。この時、添字を省略して $\bar{V} = H(t_0) = h(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0))$ などと書く。

2.2 諸性質

Definition 2.3 (Tradability) 一次元価値である *setok* の *share* は、以下の *2* つの条件が満たされた場合かつその場合に限り、***T*-取引可能** *(**T**-tradable)* **である**といわれる。

- 額面価値 $\bar{V}$ が正である。
- 時域 $\boldsymbol{T}$ 内ならばいつでも、価値解釈過程が正であって所有者は**価値比例価格** *(value-proportional price)*

$$S_p = \frac{\bar{V}}{h(t, V_1(t), V_2(t), \cdots, V_n(t))} y\left(t, S\left(t\right)\right)$$

でその *share* を売却できる。

$\boldsymbol{T}$ は**取引可能期間** *(tradable period)* と呼ばれる。取引可能期間は確定的であるとは限らない。特に、時刻印を t_0 として $[t_0, \infty)$-取引可能である場合には、**∞-取引可能** *(∞-tradable)* といわれる。取引可能期間を特に明示しない場合は単に取引可能であるという。

Definition 2.4 (Strict Tradability) *setok* は以下の *3* つの条件が満たされる場合かつその場合に限り、**厳密に *T*-取引可能** *(strictly **T**-tradable)* **である**といわれる。

- 任意の *share* は取引可能である。
- 取引可能期間は確定的である。
- 所有者は、取引可能期間外にはいかなる価格でも *share* を売却できない。

特に、厳密に $\emptyset$-取引可能な *setok* は、**取引不可能である** *(untradable)* といわれる。

Definition 2.5 (Online Divisibility) *setok* $(S, Y; V, H, n, m)$ は、条件

- 価格解釈課程の実現値が正である時は必ず、誰もが任意の**注文価格** *(order price)* $S_c(>0)$ を指定して、それに対する**比例額面価値** *(proportional explicit values)*

$$\frac{S_c}{Y(t_0)} h_i(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0)) \ (i = 1, 2, \cdots, m)$$

  を記載された *share* を購入できる。ここに、t_0 は時刻印である。

を満たす場合かつその場合に限り、**オンライン分割可能である** *(online-divisible)* といわれる。

Definition 2.6 (Offline Divisibility) 正の額面価格 $\bar{S}$ を有する *share* $(\bar{S}; \bar{V}_1, \bar{V}_2, \cdots, \bar{V}_m; t_0)$ は、所有者がその *share* を**価格比例的に** *(price-proportional manner)* 任意の割合で二分割できる場合かつその場合に限り、**オフライン分割可能である** *(offline-divisible)* といわれる。ここに、価格比例的であるとは、$(\bar{S}^1; \bar{V}_1^1, \bar{V}_2^1, \cdots, \bar{V}_m^1; t_0)$ と $(\bar{S}^2; \bar{V}_1^2, \bar{V}_2^2, \cdots, \bar{V}_m^2; t_0)$ に分割した際に次が成立することである:

$$\bar{S}^1 + \bar{S}^2 = \bar{S}, \ \bar{S}^1 > 0, \ \bar{S}^2 > 0, \ \bar{V}_j^i = \frac{\bar{S}^i}{\bar{S}} \bar{V}_j, \ (i = 1, 2; j = 1, 2, \cdots, m)$$

3 ディリバティブ

3.1 コール・オプション

ネットワーク生活では、支払いも電子的に行いたいであろう。一般に電子マネーなどの支払い方式では、使用可能な通貨単位のきめ細かさと効率がトレード・オフの関係にある [1]。したがって、購入単位の価格が固定されていれば利用可能な支払い方式の選択肢が広がる。そこで、ここでは、価格解釈プロセスが単位プロセス（常に実現値が確定的に 1 であるプロセス）である一次元価値 $\mathrm{setok}(S, Y; V, H, 1, 1)$ を扱う。さらに、setok は厳密に $(t_0, t_0 + T]$-取引可能 $(T > 0)$ であるとする。

従来、ディリバティブ理論では、取引可能性や分割可能性、そしてショート・ポジション（setok を所有していることにしてそれを「売却」し、短期的に無利子で資金を得ること。自分で勝手にを setok を発行することに相当する）の可能性が、市場の完備性や効率性を考える上で重要である [2]–[7]。しかし我々は、第 1 章で述べたアーキテクチャを念頭に据え、setok に関しては分割可能性は一切仮定せず、ショート・ポジションも許さない。ただし数学的取り扱いを容易にするため、任意の時刻 t において $0 < H(t) < \infty$, $0 < V_j(t) < \infty$ (j=1, 2, $\cdots$, n) であるとする。

Definition 3.1 (A European Call) 時刻 $t = t_0$ に発行される**ヨーロッパ型コール・オプション** *(European call option)* とは、「将来の指定された時刻 $T_m(< t_0 + T)$ において当該 *setok* の *share* を *1* 単位、ある約束した額面価値 K を記載したものを、固定単位価格で購入することができる」という権利を所有者に与えるディリバティブ（派生物）証券である。T_m は**満期** *(maturity)*、K は**行使価値** *(strike value* または *exercise value)* と呼ばれる。

3.2 価格評価

派生物は標準化された市場で売買される。そこでは、短期無リスク金利 (確定的正定数 r_f とする) の融資が利用でき、派生物に関するショート・ポジションが許される理想的な市場環境が仮定される。その下で、図 2 のような単一期間二項モデルに従う満期 $T_m = 1$ のヨーロッパ型コール・オプションの現在 $(t = 0)$ における価格 C を考える。

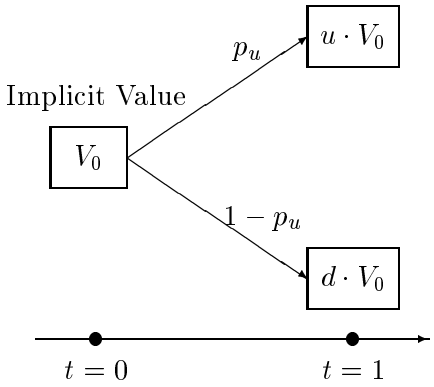

図 2: 一次元価値 setok の単一期間二項モデル

価値解釈関数は確定的正値関数 $h(v)$ であり、価値解釈過程の現在の実現値は $h(V_0)$ である。満期における価値解釈過程の実現値は $H(T_m)[\mathrm{up}] = h(u \cdot V_0)$ または $H(T_m)[\mathrm{down}] = h(d \cdot V_0)$ のいずれかである（d と u は $0 \leq d < 1 < u$ を満たす定数で $h(uV_0) \neq h(dV_0)$ とする）。前者の状態への遷移（上方遷移）は確率 p_u で起こり、後者（下方遷移）は確率 $1 - p_u$ で起こる。残念ながら p_u は既知ではないが、合理的なオプション価格 C を求めたい。

$h(uV_0) < K$ ならばオプション所有者は権利行使するが、そうでなければ行使しない。行使すればその直後に setok を価値比例価格で売却して利益が得られるので、ペイオフは

$$C_u = \frac{\max\{0, K - h(uV_0)\}}{h(uV_0)} \tag{1}$$

と書ける。下方遷移についても同様である:

$$C_d = \frac{\max\{0, K - h(dV_0)\}}{h(dV_0)} \tag{2}$$

share とオプションの個数が各々1, M であるような無リスクポートフォリオを考える。初期投資は $1 + MC$ である。無リスクであるためには、満期時の状態にかかわらず、ペイオフが同じでなければならないから

$$\frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u = \frac{h(V_0)}{h(dV_0)} \cdot 1 + MC_d \tag{3}$$

が成り立つ。両辺の第一項は share の寄与である。式 (3) と $h(uV_0) \neq h(dV_0)$ から

$$M = \frac{h(V_0)}{C_d - C_u} \left\{ \frac{1}{h(uV_0)} - \frac{1}{h(dV_0)} \right\} \tag{4}$$

が得られる。一方、無リスク資産の収益率は短期無リスク金利と等しくなければならないので

$$(1 + r_f)(1 + MC) = \frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u \tag{5}$$

が得られ、式 (4) を式 (5) に代入すれば最終的にオプション価格評価の公式

$$C = \frac{pC_u + (1 - p)C_d}{1 + r_f}, \quad p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}} \tag{6}$$

が得られる。詳細は [8] 等に譲るが、公式 (6) に確率 p_u が不要であることは、「リスク中立確率測度 (risk-neutral measure) のみを知っていればよい」と言い換えることができる。

4 むすび

本稿では、ネットワーク社会で新たなリスクを生むトークンを、４つの属性を有する security token(setok) としてモデル化した。価値属性は、「価格以外の、何らかの重要かつ時間とともに変化し得る数値」の抽象化である。また、そのリスクをヘッジする単純なコール・オプションを導入し、単一期間二項モデルにおける価格評価公式を導出した。近現代金融では、連続時間モデルを扱うブラック・ショールズ理論 [9] に触発されてオプション理論が発展し、その後主として実務的な観点から二項モデルが開発された [10]。両者の関係もよく研究されているが [11]、動きの速い実際の市場応用では、モデルの拡張が比較的容易で計算機処理に適した二項モデルの方がむしろ重要である。ネットワーク社会では、さらに動きが速いことが予想されるので、本研究ではまず二項モデルから基礎理論を築いている。紙面の都合で割愛したが、本稿で示した公式を満期から現在に向かって順次繰り返して適用していくことにより、多期間モデルにおけるオプション価格を得ることができる。

公開鍵基盤では、公開鍵証明書の信頼度を定義する際に保険の概念を導入することも考えられている [12]。保険も派生物の一種であり、ネットワークにふさわしいリスク・ヘッジ理論は今後重要な研究分野を構成する可能性がある。種々の拡張や工学的応用も含め、機会をあらためて議論したい。

参考文献

[1] T. Eng and T. Okamoto. "Single-Term Divisible Electronic Coins". In *Advances in Cryptology — EUROCRYPT'94*, pp. 306–319, 1995. Springer-Verlag. LNCS 950.

[2] A. G. Malliaris and W. A. Brock. *Stochastic Methods in Economics and Finance*, Springer, 1982.

[3] T. E. Copeland and J. F. Weston. *Financial Theory and Corporate Policy.* Addison-Wesley, 3rd edition, 1992.

[4] Robert C. Merton. *Continuous-Time Finance (Revised Edition).* Blackwell Publishers, 1992.

[5] Darrell Duffie. *Dynamic Asset Pricing Theory.* Princeton University Press, 2nd edition, 1996.

[6] Tomas Björk. *Arbitrage Theory in Continuous Time.* Oxford University Press, 1998.

[7] J. C. Hull. *Options, Futures, and Other Derivatives.* Prentice-Hall, 4th edition, 2000.

[8] K. Matsuura. "Security Tokens and Their Derivatives". Technical Reports, Centre for Communication Systems Research, University of Cambridge, February 2001.
`http://www.ccsr.cam.ac.uk/techreports/tr29/index.html`

[9] F. Black and M. Scholes. "The Pricing of Options and Corporate Liabilities". *Journal of Political Economy*, Vol. 81, pp. 637–654, 1973.

[10] C. J. Cox, S. Ross, and M. Rubinstein. "Option Pricing: A Simplified Approach". *Journal of Financial Economics*, Vol. 7, pp. 229–263, 1979.

[11] F. H. Page, Jr. and A. B. Sanders. "A General Derivation of the Jump Process Option Pricing Formula". *Journal of Financial and Quantitative Analysis*, Vol. 21, No. 4, pp. 437–446, 1986.

[12] M. K. Reiter and S. G. Stubblebine. "Authentication Metric Analysis and Design". *ACM Transactions on Information and System Security*, Vol. 2, No. 2, pp. 138–158, 1999.