Security Token and Its Derivative in Discrete-Time Models

Kanta MATSUURA
Institute of Industrial Science, University of Tokyo
Meguro-ku, Tokyo 153-8505, Japan

ABSTRACT

Aiming at modeling uncertain digital materials in the network society, we define the 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. The values are uncertain and may cause risks. Several important properties of the setok are defined. Then, in order to provide risk-hedging opportunities, a derivative written not on the price but on the value is introduced. The derivative investigated is a simple European-type call option. We derive option-pricing formulae in a single-period model and in a multiple-period model. These formulae do not require any divisibility of the underlying setok.

Keywords: Electronic Commerce, Security Token, Uncertainty, Derivative, Option Pricing, Binomial Model.

1. INTRODUCTION

Applied cryptography triggers a market of digital materials. They have their prices. In addition, they likely have other numerical values. For example, digital certificates may have confidence values [1]–[4]. Access-grant tickets may have priority numbers or QoS (Quality-of-Service) values [5]–[8]. Digital images may have confidence values about their innocence in terms of illegal-copy regulation. Any product may be associated with some insurance contracts [9]. Reward points may be attached. Those additional values may change unpredictably over time and cause risks.

A common tool for hedging risks is a *financial derivative*. In the existing finance, a lot of theories have been developed. Likewise, we want to develop appropriate theories in the digital world. In the first place, theories need models. The purpose of this paper is to model the uncertain digital materials and introduce a derivative written on them. This modeling is described in Section 2. Subsequently, by using binomial processes, Section 3 demonstrates how to price the derivatives based on the model. Finally Section 4 concludes the paper.

2. MODELING

Setok

Let us start with typical entities in network commerce:

- *Provider:* Digital copyright management is neither easy nor trivial. Maintenance of security infrastructures (*e.g.* public-key infrastructure) is not, either. We need specialized entities which are eligible for them. Typically, they are trusted organizations or licensed firms. Providers would be happier if the digital materials they provide are circulated more frequently in larger amounts; it would improve their reputation and make attached advertisement more profitable. They would have a motivation to give rewards for active usage of the digital materials.
- *Customer:* We do not trust individuals in terms of (i) behaviour, (ii) financial situation, and (iii) resources (for communication and computation).
- *Server:* Selling digital materials to untrusted customers is another difficult and non-trivial task. We need specialized entities which can do it and can have a good connection with providers. Typically, they are trusted organizations or firms; they can be less trusted in comparison with providers but they must be more trusted than customers. Due to the rewards from providers as well as their basic business reasons, servers would like to enhance their trading activities with customers. So servers have a motivation to re-circulate the digital materials. They may get the digital materials back from their customers in exchange for some refund. The refund may depend on the price and/or values of the material.

The observation above makes us model uncertain digital materials as follows.

((Definition 1)) A *security token* or *setok* is a digital material which has the following four attributes:

- *contents* which may include MAC (message authentication code), digital signatures, or other security-related control sequences if necessary,
- a non-negative *explicit price* (denoted by $\bar{S}$) which is paid on purchase,
- a set of non-negative *explicit values* (denoted by $\bar{V}_1$, $\bar{V}_2$, $\cdots$, $\bar{V}_m$ where m is referred to as the *dimension* of the explicit values) which represents some qualities of the contents in a way that larger values imply better qualities regarding the corresponding feature, and
- a *timestamp* which indicates when the setok is issued,

and is associated with

- a non-negative *implicit price* (denoted by S) and
- a set of non-negative *implicit values* (denoted by V_1, V_2, $\cdots$, V_n where n is referred to as the *dimension* of implicit values)

in the following way.

- The explicit price $\bar{S}$ is specified as the occurrence of a *price-interpretation process* $Y(t) = y\left(t, S\left(t\right)\right)$; *i.e.* $y\left(t_0, S\left(t_0\right)\right)$ is written on the setok as the explicit price of the setok which is purchased at time $t = t_0$. This occurrence is also called the *up-to-date price.* The price-interpretation process is a non-negative process and also called the *up-to-date price process.* $y = (t, s)$ is called a *price-interpretation function* and monotone increasing with respect to s. Once written, the explicit price is *never* changed.
- The explicit values are specified as the occurrences of *value-interpretation processes* $H_1(t)$ $= h_1(t,\ V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$, $H_2(t) = h_2(t,$ $V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$, $\cdots$, $H_m(t) = h_m(t,$ $V_1(t),\ V_2(t),\ \cdots,\ V_n(t))$. These occurrences are also called the *up-to-date values.* The value-interpretation processes are non-negative processes, and also called the *up-to-date value processes.* $h_1(t,\ v_1,\ v_2,\ \cdots,\ v_n)$, $h_2(t,\ v_1,\ v_2,\ \cdots,$ $v_n)$, $\cdots$, $h_m(t,\ v_1,\ v_2,\ \cdots,\ v_n)$ are called *value-interpretation functions.* Once written, the explicit values are *never* changed.

The up-to-date processes $Y(t)$ and $H(t)$ are observable in the market. A setok in the market is denoted by $(S;\ Y;\ V_1,\ V_2,\ \cdots,\ V_n;\ H_1,\ H_2,\ \cdots,\ H_m)$ or sometimes shorthandly by $(S,\ Y;\ V,\ H,\ n,\ m)$. Likewise, a share of the setok already purchased and held by someone is denoted by $(\bar{S};\ \bar{V}_1,\ \bar{V}_2,\ \cdots,\ \bar{V}_m;\ t_0)$ or sometimes shorthandly by $(\bar{S};\ \bar{V},\ m;\ t_0)$.

Definition 1 accepts not only purely financial digital materials but also digital commodities as setoks; we have not specified the contents. For simplicity, the rest of this paper studies a special case: a single-valued setok defined as follows.

((Definition 2)) A setok is said to be *single-valued* if and only if it has one-dimensional *explicit* value. In the case of a single-valued setok, we often omit the subscript "1".

Setok Properties
For single-valued setoks, we define several important properties.

((Definition 3)) A share of single-valued setok is said to be $\boldsymbol{T}$*-tradable* if and only if the following two conditions are satisfied:

- The explicit value $\bar{V}$ is positive.
- At any time $t \in \boldsymbol{T}$, the value-interpretation process is positive and the holder of the setok can sell it. This resale is possible only at the *value-proportional price* S_p defined by

$$S_p = \frac{\bar{V}\cdot y\left(t, S\left(t\right)\right)}{h(t, V_1(t), V_2(t), \cdots, V_n(t))}. \tag{1}$$

$\boldsymbol{T}$ is called a *tradable period* and allowed to be composed of open and closed time intervals; all of the forms $[T_L, T_U]$, $[T_L, T_U)$, $(T_L, T_U]$, and (T_L, T_U) (and a set of them) are available. The tradable period can be either deterministic or stochastic.

((Definition 4)) A $\boldsymbol{T}$-tradable setok is said to be *strictly* $\boldsymbol{T}$*-tradable* if and only if the following two conditions are satisfied:

- The tradable period $\boldsymbol{T}$ is deterministic.
- The holder of it cannot sell it at any price when it is out of the tradable period $\boldsymbol{T}$.

Since non-trivial security cares are needed to provide or serve setoks, divisibilities of setoks are not trivial. For example, it would be difficult for customers to divide digitally signed contents into two or more valid pieces. We define two properties with respect to this issue.

((Definition 5)) A setok (S, Y; V, H, n, m) is said to be *online-divisible* if and only if the following condition is satisfied.

- Whenever the occurrence of $Y(t)$ is positive, anyone can purchase arbitrary fraction of the setok with keeping *proportional explicit values*; *i.e.* at an arbitrary *order price* $S_c > 0$, he can buy the setok at the explicit price S_c and explicit values

  $$\frac{S_c}{Y(t_0)} h_i(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0)) \qquad (2)$$

  assigned where t_0 is the timestamp on it ($i = 1, 2, \cdots, m$).

((Definition 6)) A share of setok ($\bar{S}$; $\bar{V}_1$, $\bar{V}_2$, $\cdots$, $\bar{V}_m$; t_0) which has a positive explicit price $\bar{S}$ is said to be *offline-divisible* if and only if the holder of it can divide it into two pieces ($\bar{S}^1$; $\bar{V}_1^1$, $\bar{V}_2^1$, $\cdots$, $\bar{V}_m^1$; t_0) and ($\bar{S}^2$; $\bar{V}_1^2$, $\bar{V}_2^2$, $\cdots$, $\bar{V}_m^2$; t_0) in a *price-proportional manner*, *i.e.*

$$\bar{S}^1 + \bar{S}^2 = \bar{S},\ \bar{S}^1 > 0,\ \bar{S}^2 > 0 \qquad (3)$$

$$\bar{V}_j^i = \frac{\bar{S}^i}{\bar{S}} \bar{V}_j \ (i = 1, 2; j = 1, 2, \cdots, m). \qquad (4)$$

Option
When we study pricing theories for options, we have to specify market assumptions. Although we do not intend to stick to a single scenario, the rest of this paper consider the following case.

((Assumption 1)) In the models below, a strictly $\boldsymbol{T}$-tradable single-valued setok (S, Y; V, H, 1, 1) with the following properties is studied.

1. The price-interpretation process is an identity process, *i.e.* $Y(t) = 1$ for all t.
2. The setok is *neither* online *nor* offline divisible.
3. We *cannot* go *short* for the setok.
4. The tradable period $\boldsymbol{T}$ is composed of a single time interval of a fixed positive length T. We will make it explicit by saying "T-tradable", where T is not boldfaced.
5. The possession of the setok has no meaning as a project.
6. All the up-to-date and implicit value processes are positive and finite.
7. Value-interpretation function $h(t, v)$ is a deterministic function $h(v)$ such that $h(v) > 0$ for any $v \geq 0$.

((Assumption 2)) We assume an ideal market which satisfies the following conditions.
(a) Any transaction can be completed immediately, free of charge.
(b) It is always possible to buy and/or sell unlimited quantities. In particular, it is possible to borrow unlimited amounts from the bank (by selling bonds short). The riskless short rate is denoted by r_f and assumed to be a deterministic constant.
(c) The selling price is equal to the buying price.
(d) The market is *free of arbitrage.*
(e) The option can be bought and sold on a market at any fraction.
(f) Anyone can go short for the option.

The use of the constant price in Assumption 1 is because electronic cash systems are more efficient if the monetary value of each cash or coin is less granular [10]. That is, we want to allow as wide variety of different electronic cash systems as possible.
Now we are ready for introducing an option written on a setok.

((Definition 7)) A *European call option* on the single-valued strictly T-tradable setok (S, Y; V, H, 1, 1), purchased at time $t = 0$, is a derivative which provides a *right* to buy one share of the setok with a reserved explicit value K at a particular time $T_m < T$ in the future for its fixed price, 1, regardless of the up-to-date value $H(T_m)$ at T_m. The reserved value K is called the *strike value* or the *exercise value*, and T_m is called the *exercise date* or the *maturity date*, or just simply the *maturity.*

3. OPTION PRICING

This section is the first attempt to show option pricing in the setok world. For a readability reason, we assign the time unity so that $T_m = 1$ where T_m is the maturity of the option considered.

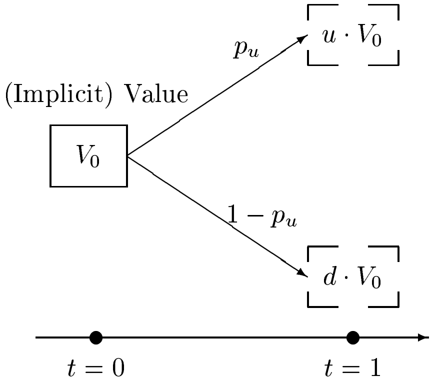

Figure 1: A single-period binomial model. At the end of the period ($t = T_m = 1$), either the "upward" or the "downward" state has occurred: the former is with the up-to-date value $h(uV_0)$ while the latter is with $h(dV_0)$, where $0 \leq d < 1 < u$. Although this illustration shows that the upward-change probability is p_u and the downward-change probability is $1 - p_u$, the option pricing does not require these probabilities. We assume that $h(uV_0) \neq h(dV_0)$.

Single-Period Model

The first model used here is a single-period binomial model described in Fig. 1. At present ($t = 0$), the up-to-date value is $H(0) = H_0 = h(V_0)$. At the maturity, there are two possible states: $H(T_m)[\text{up}] = h(u \cdot V_0)$ and $H(T_m)[\text{down}] = h(d \cdot V_0)$ where d and u are positive constants such that $0 \leq d < 1 < u$. The former occurs with probability p_u. Hence the latter occurs with probability $1 - p_u$. You do not know these probabilities. Please find a reasonable option price C. This is the problem to be solved below.

Firstly, we point out that the option has a *payoff* of

$$C_u = \frac{\max\{0, K - h(uV_0)\}}{h(uV_0)} \tag{5}$$

in the case of upward change. That is, if $h(uV_0) < K$, the holder of the option exercises it; he buys one share of the setok at the price 1, with the strike value K. Thanks to the tradability, the holder can immediately resale this share for the value-proportional price

$$S_p = \frac{K}{h(uV_0)} \cdot 1 = \frac{K}{h(uV_0)}, \tag{6}$$

and achieve a positive gain of

$$S_p - 1 = \frac{K - h(uV_0)}{h(uV_0)}. \tag{7}$$

On the contrary, if $h(uV_0) \geq K$, the holder of the option does not exercise it hence gets nothing. Likewise, the downward change gives a payoff of

$$C_d = \frac{\max\{0, K - h(dV_0)\}}{h(dV_0)}. \tag{8}$$

Our task is to find a riskless portfolio composed of one share of setok and M options. The initial investment for this portfolio is $1 + MC$. In order to achieve risk-freeness, the portfolio must have exactly the same payoff at the maturity $t = T_m = 1$ regardless of the state. That is,

$$\frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u = \frac{h(V_0)}{h(dV_0)} \cdot 1 + MC_d. \tag{9}$$

After a manipulation on Eq. (9) with the help of $h(uV_0) \neq h(dV_0)$, we have

$$M = \frac{h(V_0)}{C_d - C_u} \left\{ \frac{1}{h(uV_0)} - \frac{1}{h(dV_0)} \right\}. \tag{10}$$

Due to Assumption 2, this portfolio is feasible.

In order to achieve no arbitrage, the portfolio must have the rate of return exactly as low as the short rate r_f [11]. Therefore,

$$(1 + r_f)(1 + MC) = \frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u. \tag{11}$$

From Eq. (10) and Eq. (11), we obtain

$$C = \frac{pC_u + (1-p)C_d}{1 + r_f} \tag{12}$$

where p is defined by

$$p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}}. \tag{13}$$

The following theorem gives the summary.

((Theorem 1)) In the binomial single-period model described in Fig. 1, let us consider a European call option defined by Definition 7 under Assumptions 1, 2 and the common frictionless no-arbitrage market assumptions. Let the price process of the option be $C(t)$. Then, the following *pricing formula* holds.

$$C(0) = \frac{pC_u + (1-p)C_d}{1 + r_f} \tag{14}$$

where

$$C_u = C(1)[\text{up}] = \frac{\max\{0, K - h(uV_0)\}}{h(uV_0)} \tag{15}$$

$$C_d = C(1)[\text{down}] = \frac{\max\{0, K - h(dV_0)\}}{h(dV_0)} \tag{16}$$

$$p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}}. \tag{17}$$

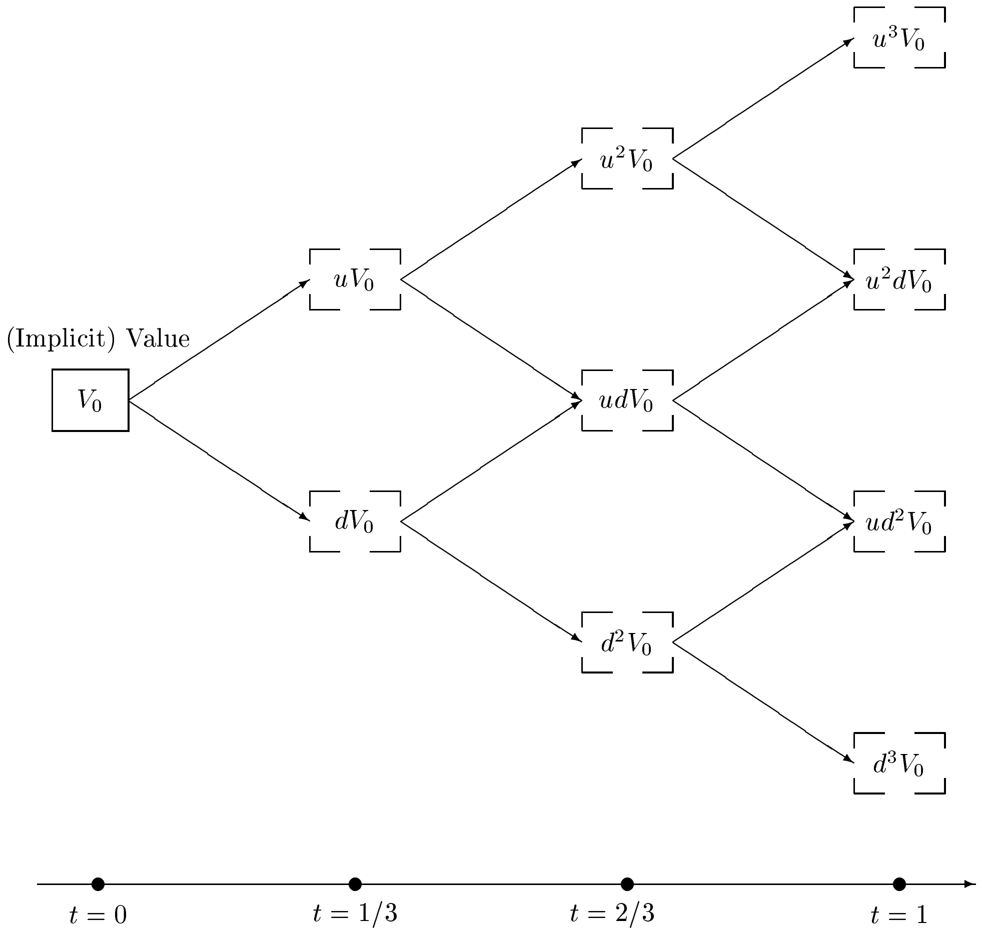

Figure 2: A multiple-period binomial model. For the drawing convenience, the illustration has only $N = 3$ periods. Each state is denoted by the number j of upward changes which have occurred. It is assumed that $H(i/N)[j] \neq H(i/N)[k]$ $(j \neq k)$ for any $i \in \{1, 2, \cdots, N\}$.

Multiple-Period Model

It is easy to extend the option pricing for dealing with a more realistic multiple-period model described in Fig. 2; we can use the single-period pricing recursively from the final period to the first.

It is in general cumbersome to explicitly write the pricing formula in the multiple-period model. This is because the parameter p given by Eq. (17) in Theorem 1 depends on the state. So we had better firstly show the *backward algorithm* for computation:

((Algorithm 1))

1. The option price at the maturity is equal to the payoff.
2. Stand at $t = (N-1)/N$ and look at the final period. Compute $C\left(\frac{N-1}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ by using Theorem 1.
3. Go back to $t = (N-2)/N$ and compute the option prices $C\left(\frac{N-2}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ by using Theorem 1. In place of the payoffs, use $C\left(\frac{N-1}{N}\right)[j]$.
4. Repeat the above procedure until you reach $t = 0$ and obtain $C(0)$.

Let us explore a situation which gives an easy-to-write formula. Our concern is the dependence of the parameter p on the up-to-date value of the setok at the beginning of each period. We want to avoid this dependence by assigning a specific form of value-interpretation function h. An example which achieves this independence is given in the following theorem. Due to the space limitation, this paper does not show the proof which is available from the author upon request.

((Theorem 2)) In the binomial multiple-period model described in Fig. 2, let us consider a European call option defined by Definition 7 written on a setok which has the value-interpretation function $h(v) = av^b$ (a, b : positive constants). The other assumptions are the same as in the single-period model, except that the short rate is a constant r_f/N during each period of length $1/N$. Then, the following pricing formula holds.

$$C(0) = \left(1 + \frac{r_f}{N}\right)^{-N} \times \sum_{j=0}^{N} \binom{N}{j} p^j (1-p)^{N-j} \frac{\max\{0, K - a(u^j d^{N-j} V_0)^b\}}{a(u^j d^{N-j} V_0)^b} \tag{18}$$

where

$$p = \frac{d^{-b} - \left(1 + \frac{r_f}{N}\right)}{d^{-b} - u^{-b}}. \tag{19}$$

Although Theorem 2 mentions merely about the option price at $t = 0$, Algorithm 1 gives us whole the price process at $t \in [0, 1/N, 2/N, \cdots, 1]$.

4. CONCLUSIONS

We have made an abstraction of uncertain digital materials in the network society and defined the 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. Three important properties of the setok were defined: tradability, online divisibility, and offline divisibility.

Written on the setok values, a simple European call option is introduced. In multiple-period as well as single-period models, we have derived option-pricing formulae. These formulae do not require any divisibility of the underlying setok, which is easier for information-security technologies to accept.

One might criticize this paper for using too simplified situations. However, what we really want to do by this paper is to trigger a new series of research. In the conventional finance, encouraged by the seminal paper by Black and Scholes [12], option-pricing theories have been developed a lot. This history has quite a reputation although the Black-Scholes theory itself had a lot of assumptions to make things too simple and had a lot of biases. Likewise, we would be very happy if a lot of studies emerge after this paper.

REFERENCES

[1] U. Maurer. "Modelling a Public-Key Infrastructure". In E. Bertino, H. Knuth, G. Martella, and E. Montolivo, editors, Computer Security — ESORICS'96, Lecture Notes in Computer Science 1146, Springer-Verlag, 1996, pp. 325–350.

[2] D. J. Essin. "Patterns of Trust and Policy". In Proc. of New Security Paradigms Workshop '97, 1997, pp. 38–47.

[3] M. K. Reiter and S. G. Stubblebine, "Resilient Authentication Using Path Independence", IEEE Trans. Comput., Vol. 47, No. 12, 1998, pp. 1351–1362.

[4] R. Kohlas and U. Maurer. "Confidence Valuation in a Public-Key Infrastructure Based on Uncertain Evidence". In H. Imai and Y. Zheng, editors, Proc. of Third International Workshop on Practice and Theory in Public Key Cryptosystems (PKC 2000), Lecture Notes in Computer Science 1751, Springer-Verlag, 2000, pp. 93–112.

[5] R. Edell and P. Varaiya, "Providing Internet Access: What We Learn from INDEX", IEEE Network, Vol. 13, No. 5, 1999, pp. 18–25.

[6] X. Xiao and L. M. Ni, "Internet QoS: A Big Picture", IEEE Network, Vol. 13, No. 2, 1999, pp. 8–18.

[7] E. W. Knightly and N. B. Shroff, "Admission Control for Statistical QoS: Theory and Practice", IEEE Network, Vol. 13, No. 2, 1999, pp. 20–29.

[8] B. Titelbaum, S. Hares, L. Dunn, R. Neilson, V. Narayan, and F. Reichmeyer, "Internet2 QBone: Building a Testbed for Differentiated Services", IEEE Network, Vol. 13, No. 5, 1999, pp. 8–16.

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

[10] T. Eng and T. Okamoto, "Single-Term Divisible Electronic Coins". In Alfredo De Santis, editor, Advances in Cryptology — EUROCRYPT'94, Lecture Notes in Computer Science 950, Springer-Verlag, 1995, pp. 306–319.

[11] T. Björk, Arbitrage Theory in Continuous Time, New York: Oxford University Press, 1998.

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