Technical Report, CCSR, University of Cambridge (February 2001)

Security Tokens and Their Derivatives

Kanta Matsuura

Visiting Scholar (March 2000–March 2001) at
Centre for Communications Systems Research,
University of Cambridge (UK)
Lecturer at *Institute of Industrial Science,*
University of Tokyo (Japan)
Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, JAPAN

Abstract

The primary purpose of this paper is to model uncertain digital objects in view of financial risk management in an open network. We have made an abstraction of the objects and defined the security token, which is abbreviated into a word coinage *setok*. Each setok has its price, values, and timestamp on it as well as the main contents. Not only the price but also the values can be uncertain and may cause risks.

A number of properties of the setok are defined. They include value response to compromise, price response to compromise, refundability, tradability, online divisibility, and offline divisibility. Then, in search of risk-hedging tools, a derivative written not on the price but on the value is introduced. The derivative investigated is a simple European-type call option. With the help of stochastic theory, we have derived several option-pricing formulae. These formulae do not require any divisibility of the underlying setok.

With respect to applications, an inverse estimation of compromise probability is studied. The stochastic approach is extended to deal with a jump caused by the compromise and the resultant revocation. This extension gives a partial differential equation (PDE) to price the call option; given a set of parameters including the compromise probability, the PDE can tell us the option price. By making an inverse use of this, we can estimate the risk of compromise.

Key words: network security, digital object, setok, risk hedge, derivative, option pricing.

Contents

1 Introduction

Applied cryptography [1] opens a door to a market of digital products in a network society. With the help of advertisement attached[1], the products do not necessarily have positive prices; they can be free of charge. In this case, the recipients may not think of them as products. So we will use the phrase *digital objects*, instead of digital products, in the following.

Since digital data in general can keep their original bit strings virtually forever, one may expect that there would be no risk of change in qualities of digital objects. This is, unfortunately, not the case.

In addition to the prices, digital objects likely have other numerical values. For example, digital certificates may have confidence values or trust metrics [2]–[7]. Access-grant tickets may have priority numbers or QoS (Quality-of-Service) values reserved [8]–[11]. Digital images and multimedia contents may have confidence values about their innocence in terms of copyright protection [12], [13]. They may have their rank in a hit chart. Any product may be associated with some insurance contracts stating how much will be paid in case of a significant damage. Reward points may be attached. These additional values may change over time and cause risks.

A common way for hedging risks is to introduce *financial derivatives* or *options* written on underlying assets. For example, a *European call option* on a stock is a *right* to buy one share of stock at a particular *exercise date* in the future for a specified price. This price is called a *strike price*. If the stock price at the exercise date exceeds the strike price, the owner of the option will exercise it and buy the stock at the strike price. If the stock price at the exercise date is cheaper than the strike price, the owner will not exercise it; he would have neither gain nor loss in this case. With respect to such financial derivatives, a wide variety of studies, pricing theories and their applications in particular, have been developed. They were encouraged a lot by the seminal paper by Black and Scholes [14].

Then, which sort of theories can we develop for the uncertain digital objects? First of all, theories need models; we have to identify what are primary features of the objects. The purpose of this paper is to introduce a framework on this identification, and then to develop a basic theory of derivatives in the model identified. From the engineering point of view, we also explore new applications by using the framework. Specifically, the paper is organized as follows. First, in Section 2, we model uncertain digital objects as a *security token*, which will be abbreviated into a word coinage ***setok*** in contrast to an existing word *stock*. Written on a *tradable* setok, a European call option is defined and priced in Section 3, where discrete-time models are firstly studied. The last part of Section 3 deals with a continuous-time model. By using a well-known lemma in stochastic calculus, an option-pricing formula is derived. A comprehensive analysis of the formula is provided as well. Subsequently Section 4 makes an attempt to use the option-pricing technique for the inverse estimation of compromise probability. After a survey of related works in Section 5, Section 6 concludes the paper.

[1] The advertisement may be attached either to the products or to the protocol messages which carry the products.

2 Security Token

2.1 Network Society

We start with our basic architecture of the network society, which is illustrated in Fig. 1. The observation to have this architecture is as follows:

(Object Provider) Copyright management and related technical maintenance are not easy and trivial tasks with respect to digital objects. Management and maintenance of network-security infrastructure (*e.g.* public-key infrastructure) are not, either. These tasks may require some sort of trustworthiness and reliability. We need specialized entities which are eligible for them and thus can provide digital objects involved. Typically, they are trusted organizations or licensed firms. Object providers would be happier if the objects they provide are distributed and circulated more frequently in larger amounts; it would improve their reputation and/or make attached advertisement more profitable. They would have a motivation to give rewards for active usage of the objects. They are able to keep in touch with the up-to-date market information.

(Object Server) Selling digital objects to untrusted customers through poor communication channels is another difficult and non-trivial task. We need specialized entities which can do it and have a good connection with object providers. Typically, they are trusted organizations or firms; they can be less trusted in comparison with object providers but they must be more trusted than customers. Due to the rewards from object providers as well as their basic business reasons, object servers would like to enhance their trading activities with customers. One may think that it is easy to sell more because copying digital data in general is so easy. However, as already implied, this is not true for digital objects; if the object providers work well, they are the only entities who can increase the number of the objects either by copying or by creating a new version. Thus object servers would have a motivation to re-circulate the objects. They may be able to get the objects back from their customers in exchange for some refund. The refund may depend on the price and/or values of the object. Object servers are able to keep in touch with the up-to-date market information.

(Customer) We do not trust individuals in terms of (i) their own behaviour, (ii) their financial situation, and (iii) resources (for communication and computation) available to them. Some customers are able to keep in touch with the up-to-date market information but the others are not.

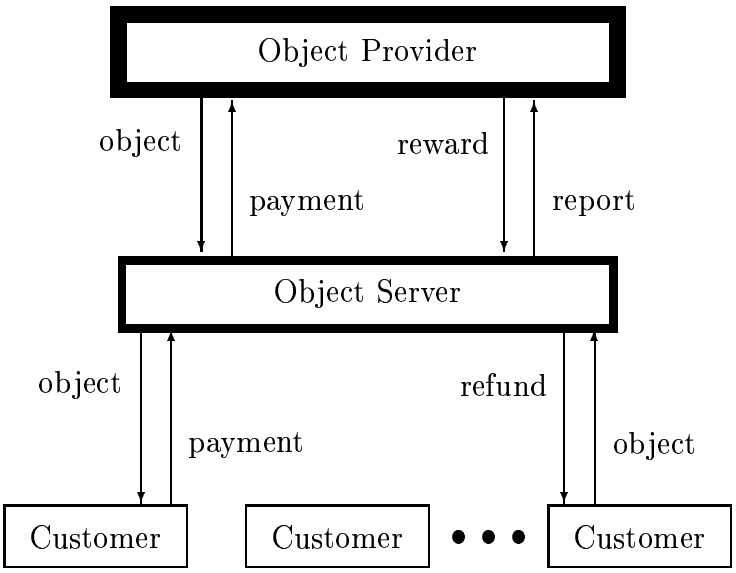

Figure 1: Basic architecture of the network society. Boxes with wider lines indicate that the entities inside are more trusted. The object provider and server are able to keep in touch with the up-to-date market information. Some customers are able to keep in touch with the up-to-date market information but the others are not. Due to better reputation and/or advertisement profits, the provider would be happier if the objects are distributed and circulated more frequently in larger amounts. The refund may depend on the price and/or values of the object. The payment from a customer may be regarded as a deposit, depending on the situation; this architecture can model a rental system as well.

2.2 Setok

In order to have a good fit for the basic architecture, we model uncertain digital objects as follows.

Definition 2.1 (Setok) *A* **security token** *or* **setok** *is a digital material which* **nominally contains** *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 when the setok is purchased by a customer,*
- *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 of each element imply better qualities regarding the feature represented by the element when the setok is purchased, and*
- *a* **timestamp** *which indicates when the setok is purchased,*

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 is specified as the occurrence of a* **price-interpretation process** $Y(t)=y(t, S(t))$; i.e. *the specific numerical value $y(t_0, S(t_0))$ is written as the explicit price of the setok which is purchased at time $t = t_0$. Each occurrence $y(t, S(t))$ is called the* **up-to-date price** *at time t. 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. Customers are unable to change the explicit price.*
- *The explicit values are specified as the occurrences of* **value-interpretation processes** $H_1(t)=h_1(t, V_1(t), V_2(t), \cdots, V_n(t))$, $H_2(t)=h_2(t, V_1(t), V_2(t), \cdots, V_n(t))$, $\cdots$, $H_m(t)=h_m(t, V_1(t), V_2(t), \cdots, V_n(t))$; i.e. *the specific numerical value $h_i(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0))$ is written as the i-th explicit value of the setok which is purchased at time $t = t_0$ (i = 1, 2, $\cdots$, m). Each occurrence $h_i(t, V_1(t), V_2(t), \cdots, V_n(t))$ is called the i-th* **up-to-date value** *at time t. 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**. *Customers are unable to change the explicit values.*

Definition 2.1 accepts not only purely financial digital materials but also digital commodities as setoks; we have not specified the contents.

Customers are untrusted. Depending on the payment scheme, customers may be even anonymous when they buy setoks. So each payment must be settled on site in exchange of the corresponding pieces of the setok. This should be done in a secure way; no customer can exploit a setok without payment, and no server can exploit a payment without sending the setok. Servers are trusted but we do not want to allow customers to lay frame-up accusation against servers. Thus setoks are transmitted to customers in pieces; *e.g.* "three pieces" are possible but "two and a half pieces" are impossible. In other words, we do not assume any accountability. A piece of setok will be referred to as a **share** of the setok.

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 $(\bar{S};\ \bar{V},\ m;\ t_0)$.

The price-interpretation function may be able to model the effect of taxes, transaction costs, regulatory issues, and so on. The value-interpretation functions may be able to model the effect of security policies, regulatory issues, editorial policies, transmission delay, and so on. Suppose that we make an electronic version of a stock in a way that each

share of the setok has the explicit values which tell the firm's information evaluated somehow. This evaluation may include *editorial* or *aggregation* procedures. It is impractical to write every history of the firm on a setok.

The "up-to-date" processes, $Y(t)$ and $H(t)$, are observable in the market and hence are adapted processes. This is a rather heuristic statement. In most occasions, it is sufficient to understand that we can observe any up-to-date processes as long as we have been get in touch with the market. For those who have studied probabilistic measure theory and prefer more rigorous statements, we place a formal definition as follows.

Definition 2.2 (Adapted Process) *Let* $(\Omega, \Gamma, \boldsymbol{P})$ *be the* probability space *whose sample space* Ω *is composed of all the possible states* **of the world considered**. *Let* (E, ε) *be the* measurable space *whose* σ-algebra ε *is generated by all the* random variables **in the market considered**. *A* stochastic process*, sometimes shorthandly referred to as a* process*, in the space* E *endowed with* ε *is a family* $(X_t)_{t\in\boldsymbol{\Theta}}$ *of random variables defined on* $(\Omega, \Gamma, \boldsymbol{P})$*, where* $\boldsymbol{\Theta}$ *denotes the set of time indices*[2]. *A* filtration *is an increasing family of* σ*-algebras included in* Γ.

Let $(\Gamma_t)_{t\in\boldsymbol{\Theta}}$ *be the* natural filtration *obtained from a filtration generated by all the stochastic processes in* E. *If* X_t *is* Γ_t*-measurable for any* $t \in \boldsymbol{\Theta}$*, the process* $(X_t)_{t\in\boldsymbol{\Theta}}$ *is said to be* adapted to Γ_t. In this framework*, such* $(X_t)_{t\in\boldsymbol{\Theta}}$ *is called an* **adapted process**.

It is obvious that processes observable in the market are adapted processes.
Note that

- some of the implicit processes $S(t)$, $V_1(t)$, $V_2(t)$, $\cdots$, $V_n(t)$ may be **not** adapted processes **even if**
  - the explicit value is one-dimensional (*i.e.* $m = 1$),
  - both of the price/value interpretation functions are easy to compute, and **strictly** monotone increasing functions with respect to some implicit price or implicit values, and
  - **the other** implicit price/value processes **are** adapted processes.

For not strictly monotone increasing functions, we may easily accept the note above. The following is a trivial example:

Example 2.1 *Let us consider a setok* $(S, Y; V, H, n, 1)$ *with a price-interpretation function* $y(t, s) = s$ *and a value-interpretation function* $h_1(t, v_1, v_2, \cdots, v_n) = h_0$ *where* h_0 *is a deterministic constant.* y *is strictly monotone increasing with respect to* s *but* h_1 *is not strictly monotone increasing with respect to any* v_j*. The implicit price process is an adapted process but the implicit value processes are not.*

---

[2]Intuitively, $\boldsymbol{\Theta}=\boldsymbol{R}$ (the set of real numbers) corresponds to a continuous-time model while $\boldsymbol{\Theta}\subseteq\boldsymbol{Z}$ (the set of integers) corresponds to a discrete-time model.

However, at a first glance, it would be more difficult or counter-intuitive, especially for those who are unfamiliar with information-security engineering, to see that strictly monotone increasing interpretation functions do not always guarantee the adaptation. We demonstrate it by using a one-way hash function.

Example 2.2 *Let us consider a setok* $(S, Y; V, H, 2, 1)$ *with a price-interpretation function* $y(t, s) = s$ *and a value-interpretation function*

$$h_1(t, v_1, v_2) = h(v_2) + p \cdot v_1$$

where $h(\cdot) : \boldsymbol{N} \to \boldsymbol{Z}_p$ *is a one-way hash function,* $\boldsymbol{N} = \{1, 2, 3, \cdots\}$ *is the set of positive integers, and* $\boldsymbol{Z}_p$=$\{0, 1, 2, \cdots, p-1\}$. *Let us suppose* $V_1(t) \in \{0, 1\}$, $V_2(t) \in \boldsymbol{Z}$ *for any* $t \in \boldsymbol{T}$. **Then** *y is strictly monotone increasing with respect to s, and* h_1 *is strictly monotone increasing with respect to* v_1. *The implicit price process is an adapted process.* V_1 *is also an adapted process because* $H_1(t) \geq p$ *implies* $V_1(t) = 1$ *and* $H_1(t) < p$ *implies* $V_1(t) = 0$. *Nevertheless,* V_2 *is not an adapted process.*

Implicit processes often remind us of the world behind, whereas interpretation/up-to-date processes often remind us of the market.

Remark 2.1 *Regarding stochastic variables, we follow the conventions in notation:*

- *Stochastic variables often appear with suppression in the following part of the paper;* e.g. *for readability reasons, we would write* S *instead of* $S(t)$ *nor* $S(t)[\omega]$ *where* $\omega \in \Omega$ *and* Ω *is the universe of the probability space considered.*
- *(1) An* **occurrence** *of a stochastic variable, and (2) corresponding* **arguments** *in functions describing other processes by the use of the stochastic variable, are usually written in small letters.*

In order to demonstrate the convention stated in Remark 2.1, we remind you of a well-known formula in stochastic calculus, usually called *Itô's Lemma*, which will be used later in this paper. Throughout the paper, a matrix or vector transpose is denoted by $\star$.

Theorem 2.1 (Itô) *Let us consider an n-dimensional stochastic process* $X = (X_1, X_2, \cdots, X_n)^\star$ *and let each component have a dynamics given by*

$$dX_i(t) = \mu_i(t)dt + \sum_{j=1}^{d} \sigma_{ij}(t)dW_j(t)$$

where $\mu_i(t)$ *and* $\sigma_{ij}(t)$ *are* **adapted processes** *and* $W_1, W_2, \cdots, W_d$ *are d independent* **Wiener processes**. *Let us define a d-dimensional Wiener process by*

$$W = (W_1, W_2, \cdots, W_d)^\star.$$

Let us furthermore define a process $F(t)$ by

$$F(t) = f\left(t, X\left(t\right)\right),$$

where $f : \boldsymbol{R}_+ \times \boldsymbol{R}^n \to \boldsymbol{R}$ is a $C^{1,2}$-mapping, i.e. *continuously differentiable with respect to t and twice continuously differentiable with respect to each x_i. $\boldsymbol{R}$ is the set of real numbers and $\boldsymbol{R}_+$ is the set of non-negative real numbers.*

Then *the process has a stochastic differential given by*

$$dF = \left\{ \frac{\partial f}{\partial t} + \sum_{i=1}^{n} \mu_i \frac{\partial f}{\partial x_i} + \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} C_{ij} \frac{\partial^2 f}{\partial x_i \partial x_j} \right\} dt + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} \sigma_i dW,$$

where the row vector σ_i is the i-th row of the **diffusion matrix** *σ defined by*

$$\sigma = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1d} \\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{n1} & \sigma_{n2} & \cdots & \sigma_{nd} \end{bmatrix}$$

and the matrix C is given by $C = \sigma\sigma^\star$.

Alternatively, *the differential is given by*

$$dF = \frac{\partial f}{\partial t} dt + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} dX_i + \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\partial^2 f}{\partial x_i \partial x_j} dX_i dX_j,$$

with the following formal multiplication table

$$\begin{cases} (dt)^2 &= 0, \\ dt \cdot dW &= \mathbf{0}, \\ (dW_i)^2 &= dt, \ i = 1, 2, \cdots, d, \\ dW_i \cdot dW_j &= 0, \ i \neq j. \end{cases}$$

2.3 Price and Value

Sufficient information to determine the implicit price and values is not always obtained through market observation, although the up-to-date price and values are observable in the market. Let us consider in more detail about the relationship or correlation among the implicit/up-to-date price and values.

The explicit values represent some qualities of the setok. They depend on the implicit values. The bridge between them is the value-interpretation functions. Changes in the implicit values may be relaxed through the interpretation. They may be exaggerated, too.

Let us suppose a value-interpretation function h_i which is monotone increasing with respect to the j-th implicit value. In this case, intuitively, the implicit value V_j also represents some sort of quality of the material. Let us suppose that some sort of *compromise* has just reduced the j-th implicit value to be zero. Hopefully best efforts are made to

make the up-to-date values reflect this emergency well enough. The efforts may include, for example, implementing the underlying directory system with real-time *revocation* as well as periodical/regular update. From the viewpoint of setok, an ideal situation is defined as follows.

Definition 2.3 (Value Response to Compromise) *Let a setok* $(S, Y; V, H, n, m)$ *have one or more value-interpretation functions which are monotone increasing with respect to one or more implicit values. Let* $\{V_{j_1}, V_{j_2}, \cdots, V_{j_s}\}$ *be the set of all such implicit value processes.*

Then, the setok is said to be **compromised** *if and only if* $V_{j_1}(t)=V_{j_2}(t)=\cdots=V_{j_s}(t) = 0$. *This setok is said to be* **compromise-responsive in value** *if and only if the following condition is satisfied.*

- *For any* h_i *which is monotone increasing with respect to one or more implicit values* $V_{j_1}, V_{j_2}, \cdots, V_{j_s}$, *a compromise* $V_{j_1}(t)=V_{j_2}(t)=\cdots=V_{j_s}(t) = 0$ *implies* $H_i(t) = 0$.

Do you accept a positive price for "compromised" material? The answer may be not unique and depend on the relationship between the contents and the implicit/explicit values. We shall define a special, but easier to accept, situation.

Definition 2.4 (Price Response to Compromise) *Let a setok* $(S, Y; V, H, n, m)$ *have one or more value-interpretation functions which are monotone increasing with respect to one or more implicit values. Let* $\{V_{j_1}, V_{j_2}, \cdots, V_{j_s}\}$ *be the set of all such implicit value processes.*

This setok is said to be **compromise-responsive in price** *if and only if the compromise* $V_{j_1}(t)=V_{j_2}(t)=\cdots=V_{j_s}(t) = 0$ *implies* $Y(t) = 0$.

2.4 Resale of Setoks

In our architecture, object servers would have a motivation to re-circulate the objects they have sold. They may be able to get the objects back from their customers in exchange for some refund, which would in turn motivate the customers to return the objects. This refund may depend on the price and/or values of the object. Formally, we define refundability and tradability.

Definition 2.5 (Refundability) *A share of setok is said to be* $\boldsymbol{T}$**-refundable** *if and only if the following two conditions are satisfied:*

- *The explicit price is positive.*
- *The holder can sell it at the explicit price whenever he wants during a set of time intervals* $\boldsymbol{T}$.

$\boldsymbol{T}$ is called a **refundable 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 set of them) are available. The refundable period can be either deterministic or stochastic. When the context does not need the refundable period, we can just say "refundable" instead of "$\boldsymbol{T}$-refundable".*

In particular, a share of setok is said to be **∞-refundable** *if and only if it is $[t_0, \infty)$-refundable where t_0 is the timestamp on it.*

Definition 2.6 (Strict Refundability) *A share of setok is said to be* **strictly $\boldsymbol{T}$-refundable** *if and only if the following three conditions are satisfied:*

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

When the context does not need the refundable period, we can just say "strictly refundable" instead of "strictly $\boldsymbol{T}$-refundable".

In particular, a strictly $\emptyset$-refundable setok is said to be **unrefundable** *where $\emptyset$ is the empty set.*

Definition 2.7 *At time t, a strictly $\boldsymbol{T}$-refundable setok with non-empty refundable period $\boldsymbol{T}$ is said to be* **still refundable** *if and only if there exists a time t' such that $t' > t$ and $t' \in \boldsymbol{T}$ where t is the current time.*

There are several important things to be pointed out. Firstly, note that we have defined the refundability with respect to a *share* of setok. Even for the same setok, shares sold at different time could have different refundable periods; the refundability of $(\bar{S};\ \bar{V},\ m;\ t_0)$ and that of $(\bar{S};\ \bar{V},\ m;\ t_1)$ $(t_1 \neq t_0)$ are not necessarily the same. This allows a dynamic change of management policies of a setok. For example, let us suppose a setok which has been managed so far in a way that all the shares are strictly refundable and the refundable period is very long. This policy gives an assurance to customers, but could cause too much financial load (*e.g.* reserve funds) on the server and/or too much administrative load (*e.g.* security-parameter directory) on the provider. If needed, the policy can be changed in a way that shares will be sold with a shorter refundable period, or even sold with no refundability, from now on. However, due to the former strict refundability, the refundable periods of the shares already sold cannot be changed accordingly. If their refundable periods were stochastic, the corresponding change would be (not mandatory but) possible. Thus, in our framework, we can accommodate a wide variety of situations by specifying which kind of refundability is used.

It should be also noted that the refund of a setok is possible only at its explicit price $\bar{S}$. Changes in values are not considered. This can model a rental system with deposit, for example. However, depending on the applications, a more flexible resale may be allowed. This is easier if the explicit value is one-dimensional.

Definition 2.8 (Single-Valued Setok) *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" when we denote the explicit value, the corresponding value-interpretation function, and the corresponding value-interpretation process. Hence we may write*

$$\bar{V} = H(t_0) = h(t_0, V_1(t_0), V_2(t_0), \cdots, V_n(t_0)).$$

Definition 2.9 (Tradability) *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.*
- *Whenever he wishes during a set of time intervals* $\boldsymbol{T}$*, 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*

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

$\boldsymbol{T}$ *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.*

In particular, a setok is said to be ∞**-tradable** *if and only if it is* $[t_0, \infty)$*-tradable where* t_0 *is the timestamp on it.*

It should be noted here that S_p can have a zero occurrence; there can be a trade at a price of zero.

Definition 2.10 (Strict Tradability) *A setok is said to be* **strictly** $\boldsymbol{T}$**-tradable** *if and only if the following three conditions are satisfied:*

- *The setok is* $\boldsymbol{T}$*-tradable.*
- *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* $\boldsymbol{T}$*.*

In particular, a strictly $\emptyset$*-tradable setok is said to be* **untradable**.

Definition 2.11 *A strictly* $\boldsymbol{T}$*-tradable setok with non-empty tradable period* $\boldsymbol{T}$ *is said to be* **still tradable** *if and only if there exists a time* t' *such that* $t' > t$ *and* $t' \in \boldsymbol{T}$ *where* t *is the current time.*

We have mentioned how flexible our refundability definition is. Likewise, we can accommodate a wide variety of situations by specifying which kind of tradability is used. Deterministic or stochastic? If stochastic, how?

Stocks are virtually valid forever as long as the firm survives. However, for information-security reasons, setoks likely have relatively short life time. So the period restriction by $\boldsymbol{T}$ in Definition 2.5 and in Definition 2.9 is one of the important features of such setoks. Hence we conjecture that the setok theory would be in close relation to project-investment theory; typically, project opportunities can exist for the time being but not forever.

2.5 Divisibility

Suppose a situation in which I need a single-valued setok $(S, Y; V, H, 1, 1)$ with an explicit value of 100. And suppose that I am so unlucky that the current market board says $H(t) = 95$. Shall I buy two shares of the setok? Do I have to reconsider my purchase plan? This annoyance depends on the divisibility of the setok.

Definition 2.12 (Online Divisibility) *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 the price-interpretation process 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 at the explicit price S_c and explicit values*

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

assigned where t_0 is the timestamp on it.

It should be noted here that we make an order by specifying the order price, not by specifying the explicit values. This may decrease communication overhead.

We may face a similar annoyance when we are going to sell a share of setok.

Definition 2.13 (Offline Divisibility) *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.

$$\bar{S}^1 + \bar{S}^2 = \bar{S}, \ \bar{S}^1 > 0, \ \bar{S}^2 > 0$$

and

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

---

3 Call Option on a Simple Setok

3.1 Simple Settings

In a network life, we would want to pay for digital products in electronic cash. Electronic cash systems could be more efficient if the monetary value of each cash or coin is less granular [15]. Some systems have only a few kinds of fixed-value coins. Therefore, if we want to allow as wide variety of electronic cash systems as possible, a fixed price would be helpful. This section assumes a setok whose price-interpretation process is an identity process.

We also assume here a strictly $\boldsymbol{T}$-tradable setok where $\boldsymbol{T} \neq \emptyset$. We have defined tradability only for single-valued setoks. Hence we consider a single-valued setok in this section. In the derivative theory, tradability and divisibility is important with respect to the *completeness* and *efficiency* of the market. Since a rigorous discussion would take a long time, we recommend those who are interested to consult good literatures such as [16]–[22]. For those who are less interested or otherwise too busy, it would be sufficient to see how the pricing procedure below in this section is simple and sound.

We do not assume any divisibility of the setok. This is because we prefer settings less restrictive against security protocol design and implementation.

The final important decision is how to regard the setok as a "project" during the time interval we keep it. Our framework considers the contents, which suggests that the possession of a setok might yield something. Again, this section chooses the simplest story: nothing happens.

With some more specifications made, we have the following assumptions.

Assumption 3.1 *In Section 3, a* **single-valued** *setok* $(S, Y; V, H, n, 1)$ *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* **not** *online divisible.*
3. *The setok is* **not** *offline divisible*
4. **No one can go short** *for the setok*[3].
5. *Each share of the setok is strictly* $\boldsymbol{T}$*-tradable.*
6. *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.*
7. *The possession of the setok has no meaning as a project and hence, in a financial term, yields no dividends.*
8. *All the up-to-date and implicit value processes are positive and finite.*

---

[3] A **short position** is a financial jargon. When we say "going short for three shares of a stock" at time $t = 0$, it means that we have sold three units of the stock at time $t = 0$. A mathematical interpretation will appear later in Assumption 3.2.

In the real world, as mentioned in Section 1, one of the simplest derivatives is European call options written on a stock. Stocks are supposed to be tradable and divisible. It is well-known that a seminal paper by Black and Scholes [14] presents a complete general equilibrium theory of pricing this kind of options. Their results are attractive particularly because the final formula is a function of *observable* variables. A key idea for deriving the formula is to replicate a riskless asset by using the option and the underlying stock. Can we borrow the Black-Scholes formula as it is? — Fortunately or unfortunately, we have assumed a fixed-price setok. We are not able to write any option on the price. What we can do is with respect to the values.

Definition 3.1 (A European Call) *We consider a single-valued setok* $(S, Y; V, H, n, 1)$ *which satisfies Assumption 3.1. Let* T *represent the fixed length of the strict tradability.*

Then, a European call option *on the setok, purchased at time* $t = t_0$*, is defined as a derivative which provides a* right *to buy one share of the setok with a reserved explicit value* K *at a particular time* $T_m < t_0 + T$ *in the future for its fixed price, 1, regardless of the up-to-date value* $H(T_m)$ *at* $t = T_m$*. 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**.

It should be noted that there is no obligation for the holder of the option to exercise the right on the exercise date. Obviously, he will exercise it if $H(T_m) < K$ and he won't if $H(T_m) \geq K$.

Our final setting statement is assumptions on the market.

Assumption 3.2 (Ideal Market) *We assume an ideal market which satisfies the following conditions.*

(a) *There are no transaction costs of trading both in time and in money: any transaction can be completed immediately, free of charge.*

(b) *The market is* completely liquid, *i.e. it is always*[4] *possible to buy and/or sell unlimited quantities. In particular, it is possible to borrow unlimited amounts from the bank (by selling bonds*[5] *short).*

(c) *There is no* bid-ask spread, *i.e. the selling price is equal to the buying price.*

(d) *The market is* free of arbitrage.

The four items above are common for both the setok market and the option market. In addition, the option market is assumed to have the following properties as well.

[4] Rigorously speaking in terms of probability measure theory, "always" means "at any time index in the probability space considered".

[5] An introduction of bonds and bank accounts will soon appear around Definition 3.2, Assumption 3.3, Definition 3.3, and Proposition 3.1.

(e) *The option can be bought and sold on a market at any fraction.*

(f) *Anyone can go short for the option.*

In mathematical terms, (e) and (f) mean that any real number is allowed to appear in a portfolio with respect to the amount of the option.

We consider different architectures for setoks and for options. Let us have a more close look at the difference and the common features by referring to the items in Assumption 3.1 and in Assumption 3.2.

The common features, (a), (b), and (c) in Assumption 3.2, are for simplicity. (a) for setoks is supported by secure timestamps; non-negligible delay may occur in the architecture of the setok world, but no one can abuse the delay for cheating. (d) in Assumption 3.2 is the most common in financial theory. The meaning of arbitrage is explained when we price the option subsequently in 3.2.

With respect to setoks, no divisibility is assumed (2. and 3. in Assumption 3.1). Going short is not allowed, either (4. in Assumption 3.1). This is due to the architecture described in 2.1 at the beginning of Section 2. By contrast, with respect to options, divisibility is assumed ((e) in Assumption 3.2) and going short is allowed ((f) in Assumption 3.2). This implies that participation in the setok-option market has the same requirements as in the conventional option market: security and reliability of the resources are good enough, and participants are trusted enough.

3.2 Pricing in Discrete-Time Models

3.2.1 Single-Period Binomial Model

This subsection is the first attempt to show option pricing in the setok world. We have Assumption 3.1. To get a simple but good and instructive start, we furthermore assume that the implicit value process V is one-dimensional, *i.e.* $n = 1$, and that the value-interpretation function is a deterministic function $h(v)$ such that $h(v) > 0$ for any $v \geq 0$. Furthermore, for a readability reason, we assign the time unity so that $T_m = 1$.

The simplest model used here is a single-period binomial model described in Fig. 2. 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, the state after upward change, occurs with probability p_u. Hence the latter, the state after downward change, occurs with probability $1 - p_u$. You do not know these probabilities. Please find a reasonable price of the European call option. This is the problem to be solved below.

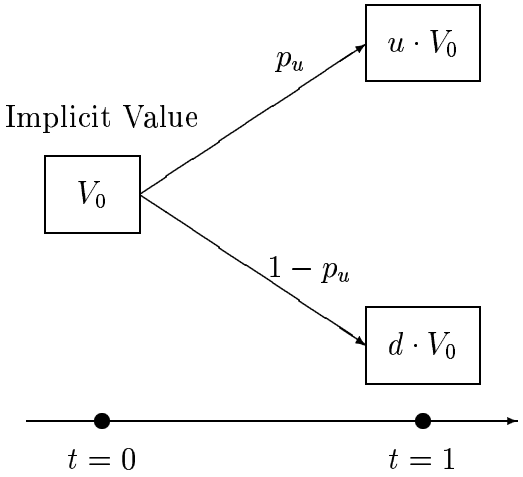

Figure 2: A single-period binomial model for pricing the European call option. The setok price is kept to be 1 all the time. At the beginning of the period ($t = 0$), the up-to-date value of the setok is $h(V_0)$. At the end of the period ($t = T_m = 1$), *i.e.* the maturity of the option, either the "upward" or the "downward" state has occurred: the former is with the option payoff C_u and the up-to-date value of the setok $h(uV_0)$ while the latter is with C_d and $h(dV_0)$, 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 pricing does not require these probabilities. They appear here just to tell you that the two states are the only possible states at $t = 1$. It is assumed that $h(uV_0) \neq h(dV_0)$, which differentiates the two states in the market as well as in the implicit world.

Firstly, we find that the option has a *payoff* of

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

in the case of the 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 Definition 2.9, Assumption 3.1, and Assumption 3.2, the holder can immediately resale this share for the value-proportional price

$$S_p = \frac{K}{h(uV_0)} \cdot 1 = \frac{K}{h(uV_0)}, \tag{2}$$

and achieve a positive gain of

$$S_p - 1 = \frac{K - h(uV_0)}{h(uV_0)}. \tag{3}$$

He is not obliged to exercise the option but he does. This is what is called the 'greedy' assumption in economics: anyone able to obtain anything of value for free will not hesitate to do so. On the contrary, if $h(uV_0) \geq K$, the holder of the option does not exercise it hence gets nothing. Eqn. (1) is a mathematical representation of this. Likewise, we find that the option has a payoff of

$$C_d = \frac{\max\{0, K - h(dV_0)\}}{h(dV_0)} \tag{4}$$

in the case of the downward change.

Our second concern, and the very key to the solution, is obtained by asking financial people to tell us what is *reasonable*. They surely tell us to price the option in a way that *no arbitrage* opportunity is available. Yes, we have assumed no-arbitrage condition in the statement (d) of Assumption 3.2. Then, what is an arbitrage opportunity? To see this, although this subsection investigates discrete-time models, let us be patient with a continuous-time setting for the time being.

In the financial theory, there is a riskless asset with *short rate*. Intuitively, the short rate can be interpreted as the *riskless rate of interest* over an infinitesimal time interval $[t, t+dt]$. Formally, we use the following typical financial definitions (Definitions3.2 and 3.3) and assumptions (Assumption 3.3).

Definition 3.2 (Zero-Coupon Bond) *A* **zero-coupon bond**[6] *with* **maturity date** T *is a contract which* guarantees *the holder a unit of currency, say, 1 dollar, to be paid on the date T. It is sometimes called a T-bond, and its price at time t is typically denoted by $p(t,T)$.*

Assumption 3.3 (Rich and Regular Bond Market) *We assume a sufficiently rich and regular bond market,* i.e.

- *There exists a frictionless market for T-bonds for* every $T > 0$.
- $p(t,t) = 1$ *holds for all t.*
- *For each fixed t, the bond price $p(t,T)$ is differentiable with respect to the maturity date T.*

A basic requirement for an economy is that there is no strategy that brings a positive monetary gain without any risk. The second assumption $p(t,t) = 1$ is necessary for this purpose. This is the no-arbitrage requirement. If $p(t,t)$ were smaller than 1, then we may buy the bond at the price $p(t,t)$ and then immediately obtain 1 dollar; hence a positive gain $1 - p(t,t)$ without any risk is possible. If $p(t,t)$ were larger than 1, then we may write a bond, obtain $p(t,t)$, and then immediately pay 1 dollar, which yields a positive gain $p(t,t) - 1$ without any risk.

Definition 3.3 (Short Rate and Money Account) *Let $p(t,T)$ be the price of T-bond at time t under Assumption 3.3.*

- *The* **instantaneous forward rate with maturity** T*, contracted at t, is defined by*

$$f(t,T) = -\frac{\partial \ln p(t,T)}{\partial T}.$$

[6] This is called *zero-coupon* bond because originally dividends were, if they were contracted, distributed as coupons attached and bonds without dividends had no coupon.

- *The instantaneous* **short rate** *at time t is defined by*

$$r(t) = f(t,t).$$

- *The* **money account process** *B is defined by a dynamics*

$$\begin{cases} dB(t) &= r(t)B(t)dt \\ B(0) &= 1. \end{cases}$$

The money account is risk-free because its dynamics has nothing but a drift term. This term is usually called a dt-term. The simplest model assumes that the short rate is a non-negative constant. In this particular case, the money account process becomes

$$B(t) = \exp(rt). \tag{5}$$

The discrete-time counterpart of this is a constant short rate r_f with the following properties:

- If we buy a riskless T_m-bond for the price 1 dollar at time $t = 0$, then we will surely obtain $1 + r_f (\geq 1)$ dollars at the maturity $t = T_m (= 1)$.
- If we write or sell a riskless T_m-bond for the price 1 dollar at time $t = 0$, then all we have to do at $t = T_m$ is to pay $1 + r_f (\geq 1)$ dollars.

In the following, we will assume that r_f is a deterministic constant.

Proposition 3.1 (Riskless Rate of Return) *Let r_f be the constant short rate.*
In the no arbitrage market, every riskless, i.e. *fixed-income, portfolio (an asset or combination of some assets) has the rate of return which is equal to r_f.*

Proof **:**
If there is a riskless portfolio with the rate $r' > r_f$, then you can achieve an arbitrary large amount of gain $(r' - r_f)M$ by the following steps *with probability 1.*

1. At time $t = 0$, go short for the bank and sell the riskless T_m-bond to get M dollars.
2. Immediately after that, *i.e.* also at $t = 0$, buy the portfolio by using all the M dollars.
3. At time $t = T_m$, sell the portfolio for the price $(1 + r')M$ dollars and pay $(1 + r_f)M$ dollars for the bond.

Likewise, if $r' < r_f$, you can surely achieve an arbitrary large amount of gain $(r_f - r')M$. Such a "free-lunch" dream is not permissible and hence $r' = r_f$. ***Q.E.D.***

The next one is another exercise for the use of no arbitrage, and gives an implicit constraint on the model in this section.

Lemma 3.1 *Let r_f be the constant short rate.*

In the binomial single-period model described in Fig. 2, the following must hold:

$$\frac{h(V_0)}{\max\{h(uV_0), h(dV_0)\}} \leq 1 + r_f.$$

Proof **:**

If $h(V_0)/\max\{h(uV_0), h(dV_0)\} > 1 + r_f$, then you can achieve an arbitrary large amount of gain $M\{h(V_0)/\max\{h(uV_0), h(dV_0)\} - (1 + r_f)\}$ by the following steps *with probability 1.*

1. At time $t = 0$, go short for the bank and sell the riskless T_m-bond to get M dollars.
2. Immediately after that, *i.e.* also at $t = 0$, buy M shares of the setok by using all the M dollars.
3. At time $t = T_m$, sell all the setok for the value-proportional price. This is possible because the setok is strictly T-tradable and $T > T_m$.
4. The value-proportional price is at least $h(V_0)/\max\{h(uV_0), h(dV_0)\}$. Hence what you obtain in total is at least $Mh(V_0)/\max\{h(uV_0), h(dV_0)\}$.
5. At the same time, you pay $(1 + r_f)M$ dollars for the bond.

This is not permissible. Therefore,

$$\frac{h(V_0)}{\max\{h(uV_0), h(dV_0)\}} \leq 1 + r_f.$$

Q.E.D.

Now, finally we have come back on the track. Our task is to find a riskless portfolio composed of one share of setok and M European call options. Let C be the price of one share of the option (at $t = 0$). Then our initial investment is given by

$$1 + MC. \tag{6}$$

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 (upward or downward). That is,

$$\frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u = \frac{h(V_0)}{h(dV_0)} \cdot 1 + MC_d. \tag{7}$$

Note that the first term of each side in Eqn. (7) represents the payoff resulting from one share of the setok. This is possible because the setok is strictly T-tradable and $T > T_m$. So now we can understand that

- the riskless portfolio strategy is possible **if there exists** a number M which satisfies Eqn. (7) and is **allowed** in the setok/option market assumed here.

After a manipulation on Eqn. (7) with the help of $h(uV_0) \neq h(dV_0)$, we have

$$M = \frac{h(V_0)}{C_d - C_u} \left\{ \frac{1}{h(uV_0)} - \frac{1}{h(dV_0)} \right\} \tag{8}$$

Because of the assumption of the ideal option market (Assumption 3.2), the portfolio is feasible regardless of the actual occurrence of M given by Eqn. (8); any $M \in \boldsymbol{R}$ is allowed.

Thus we have established a riskless portfolio. In order to achieve no arbitrage, the portfolio must have the rate of return exactly as low as the short rate r_f. Therefore, looking at the initial investment (Eqn. (6)), we notice that

$$(1 + r_f)(1 + MC) = \frac{h(V_0)}{h(uV_0)} \cdot 1 + MC_u \tag{9}$$

must hold. Let us insert Eqn. (8) into Eqn. (9), then, after some manipulations, we obtain

$$C = \frac{pC_u + (1-p)C_d}{1 + r_f} \tag{10}$$

where p is defined by

$$p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}}. \tag{11}$$

With a little bit more care added, the story above can be summarized as the following theorem.

Theorem 3.1 (Option-Pricing Formula (Single-Period Model)) *In the binomial single-period model described in Fig. 2, let us consider a European call option defined by Definition 3.1 under Assumption 3.1 and Assumption 3.2. Choose the option's maturity T_m as a time unit and assume that the short rate of interest is a constant r_f for the time unit. Let the price process and the strike value of the option be $C(t)$ and K, respectively. Then, the following* pricing formula *holds.*

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

where

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

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

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

We are happy because the pricing does not need p_u. We are also happy to see that

- no divisibility assumption on the setok is needed,

and that

- the setok is allowed to have a finite lifetime in tradability.

Both of them go well with the basic architecture which has been described in Fig. 1 at the beginning of this paper. From the engineering point of view, such a less restrictive situation most likely allows cheaper and more efficient protocols which are suitable for general customers.

3.2.2 Hedging Probability and Martingale Measure

Before proceeding, let us further investigate the meaning of p in the pricing formula (Theorem 3.1).

Lemma 3.2 (Hedging Probability) *If* $h(V_0)/\min\{h(uV_0), h(dV_0)\} \geq 1 + r_f$, *the parameter* p *given in Theorem 3.1 satisfies* $0 \leq p \leq 1$. *We refer to* p *as the* hedging probability.

Proof :

We have assumed that $h(v) > 0$ for any $v \geq 0$ and that $h(uV_0) \neq h(dV_0)$.

When $h(uV_0) > h(dV_0)$, we have $h(V_0)/h(dV_0) \geq 1 + r_f$ because of the assumption $h(V_0)/\min\{h(uV_0), h(dV_0)\} \geq 1 + r_f$. $h(uV_0) > h(dV_0)$ of course implies $1/h(dV_0) > 1/h(uV_0)$. Consequently,

$$p = \frac{\{(h(dV_0)\}^{-1} - (1 + r_f)\{h(V_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}} = \frac{\frac{h(V_0)}{h(dV_0)} - (1 + r_f)}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

By using $h(uV_0) > h(dV_0)$ and Lemma 3.1, we have $h(V_0)/h(uV_0) \leq 1 + r_f$. We remember $1/h(dV_0) > 1/h(uV_0)$. Hence

$$1 - p = \frac{(1 + r_f)\{h(V_0)\}^{-1} - \{(h(uV_0)\}^{-1}}{\{h(dV_0)\}^{-1} - \{h(uV_0)\}^{-1}} = \frac{(1 + r_f) - \frac{h(V_0)}{h(uV_0)}}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

When $h(uV_0) < h(dV_0)$, we have $h(V_0)/h(uV_0) \geq 1 + r_f$ because of the assumption $h(V_0)/\min\{h(uV_0), h(dV_0)\} \geq 1 + r_f$. $h(uV_0) < h(dV_0)$ of course implies $1/h(dV_0) < 1/h(uV_0)$. Consequently,

$$1 - p = \frac{(1 + r_f) - \frac{h(V_0)}{h(uV_0)}}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

By using $h(uV_0) < h(dV_0)$ and Lemma 3.1, we have $h(V_0)/h(dV_0) \leq 1 + r_f$. We remember $1/h(dV_0) < 1/h(uV_0)$. Hence

$$p = \frac{\frac{h(V_0)}{h(dV_0)} - (1 + r_f)}{h(V_0)\left\{\frac{1}{h(dV_0)} - \frac{1}{h(uV_0)}\right\}} \geq 0.$$

Q.E.D.

Proposition 3.2 (A Martingale Measure) *Let us* **discount** *the option price process $C(t)$ by the (***riskless***) short rate r_f, and define a process $\bar{C}(t)$ by*

$$\begin{aligned} \bar{C}(0) &= C(0) \\ \bar{C}(1) &= (1 + r_f)^{-1} C(1). \end{aligned}$$

Then,

1. *The hedging probability p provides a probability measure if we* **assign** *p as the probability of the upward change and $1 - p$ as the downward one.*

2. *Under this measure, the discounted price process $\bar{C}(t)$ has the* **martingale** *property such that*

$$\bar{C}(0) = E_0\left[\bar{C}(1)\right]$$

where E_0 denotes the expectation operator conditioned by the available information at $t = 0$.

Proof **:**

Let us denote the state after the upward change by "up", and that by the downward change by "down".

The first statement is trivial from the definition given by Eqn. (11) and Lemma 3.2.

To prove the second statement, please note that the no-arbitrage requirement gives $C(1)[\text{up}] = C_u$ and $C(1)[\text{down}] = C_d$; *i.e.* the option price at the maturity must be equal to the payoff. Therefore, we have

$$\begin{aligned} E_0\left[\bar{C}(1)\right] &= p\bar{C}(1)[\text{up}] + (1-p)\bar{C}(1)[\text{down}] \\ &= p(1+r_f)^{-1}C(1)[\text{up}] + (1-p)(1+r_f)^{-1}C(1)[\text{down}] \\ &= (1+r_f)^{-1}\{pC_u + (1-p)C_d\} \end{aligned}$$

Theorem 3.1 says that this equals to $C(0)$, which is by definition equal to $\bar{C}(0)$. ***Q.E.D.***

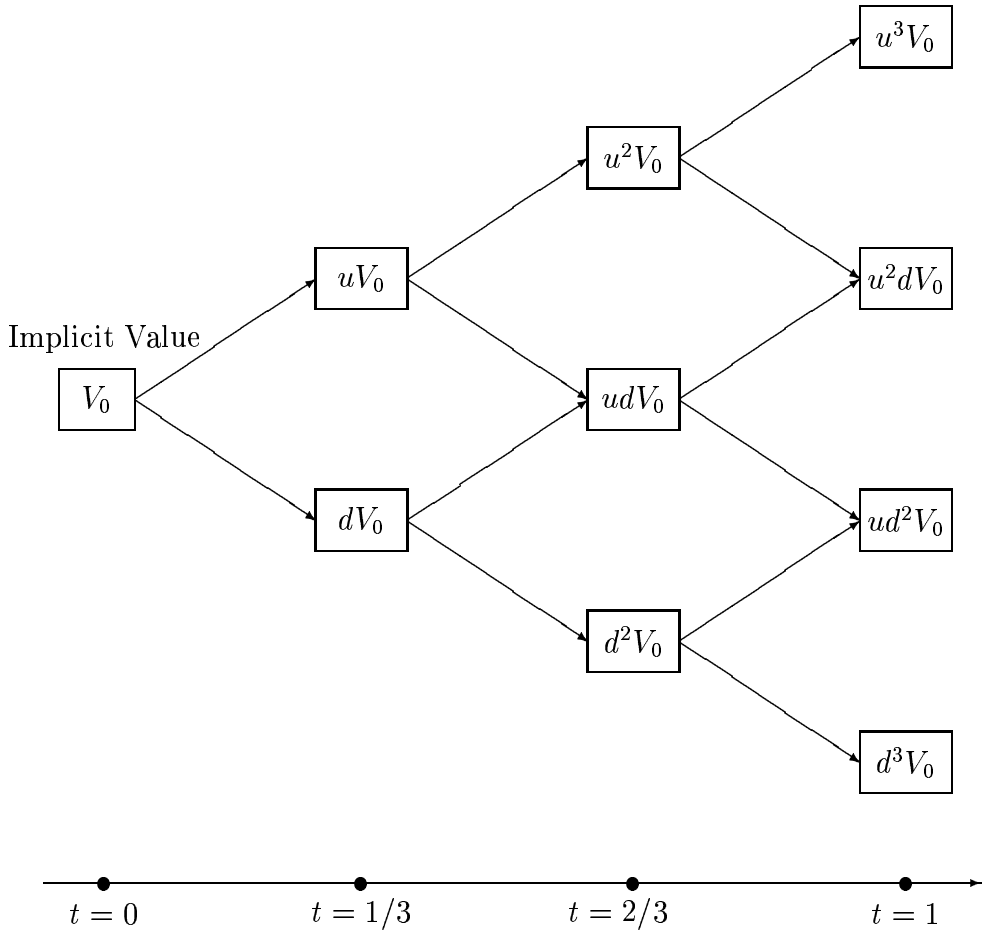

Figure 3: A multiple-period binomial model for pricing the European call option. For the drawing convenience, the illustration has only $N = 3$ periods. The setok price is kept to be 1 all the time. At the beginning of the period ($t = 0$), the up-to-date value of the setok is $h(V_0)$. At the end of the period ($t = T_m = 1$), *i.e.* the maturity of the option, we have N possible states denoted by the number j of upward changes which have occurred. We also denote each state at time $t = i/N$ by the number j of upward changes which have occurred. We suppress the transition probability, which was denoted by p_u and $1 - p_u$ in the case of the single-period model, because they are not used in the pricing. We assume that $H(i/N)[j] \neq H(i/N)[k]$ $(j \neq k)$ for any $i \in \{1, 2, \cdots, N\}$.

3.2.3 Multiple-Period Binomial Model

By repeating the binomial process, we can easily extend the single-period model to a multiple-period model (Fig. 3). Let the maturity T_m be 1 as in the previous subsection and divide the time interval $[0, 1]$ into a large number of periods, say, N periods: $[0, 1/N)$, $[1/N, 2/N)$, $\cdots$, $[(N-1)/N, 1)$. We must pay attention to three things:
(i) The short rate is defined as a rate of interest for a time unit. Hence we use r_f/N for each period.
(ii) At each edge of the periods, *i.e.* $t = i/N$ $(i = 1, 2, \cdots, N)$, the state is determined by how many upward changes have occurred. Let j be the number of upward changes

which have occurred during the first i periods. Then the up-to-date value of the setok at $t = i/N$ is given by

$$h\left(u^j d^{i-j} V_0\right). \tag{12}$$

In particular, the payoff of the option, which must be equal to the option price at the maturity, is given by

$$C(1)[j] = \frac{\max\{0, K - h(u^j d^{N-j} V_0)\}}{h(u^j d^{N-j} V_0)}. \tag{13}$$

(iii) In general, the hedging probability p depends on the state at the beginning of the period. For the period $[i/N, (i+1)/N)$,

$$\begin{aligned} p &= p\left(\frac{i}{N}\right)[j] \\ &= \frac{\{h(d \cdot u^j d^{i-j} V_0)\}^{-1} - \left(1 + \frac{r_f}{N}\right)\{h(u^j d^{i-j} V_0)\}^{-1}}{\{h(d \cdot u^j d^{i-j} V_0)\}^{-1} - \{h(u \cdot u^j d^{i-j} V_0)\}^{-1}} \\ &= \frac{\{h(u^j d^{i-j+1} V_0)\}^{-1} - \left(1 + \frac{r_f}{N}\right)\{h(u^j d^{i-j} V_0)\}^{-1}}{\{h(u^j d^{i-j+1} V_0)\}^{-1} - \{h(u^{j+1} d^{i-j} V_0)\}^{-1}} \end{aligned} \tag{14}$$

if j upward changes have occurred during the first i periods. Thus p is an adapted process.

Due to the property (iii), it is in general cumbersome to explicitly write the pricing formula. Instead, we had better firstly show the *backward* algorithm for computation:

Algorithm 1:

1. Stand at $t = (N-1)/N$ and compute $C\left(\frac{N-1}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ by using (or carefully speaking, "interpreting") Theorem 3.1 with the cares (i), (ii), and (iii) listed above. Thus you have

   $$C\left(\frac{N-1}{N}\right)[j] = \frac{p\left(\frac{N-1}{N}\right)[j] C(1)[j+1] + \{1 - p\left(\frac{N-1}{N}\right)[j]\} C(1)[j]}{1 + \frac{r_f}{N}}$$

   for $j = 0, 1, \cdots, N-1$, where $C(1)[j]$ $(j = 0, 1, \cdots, N)$ and $p\left(\frac{N-1}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ are given by Eqn. (13) and Eqn. (14), respectively.

2. Go back to $t = (N-2)/N$ and note that $C\left(\frac{N-1}{N}\right)[j]$ represents what you obtain if you sell one share of option at the state j at $t = (N-1)/N$. Compute $C\left(\frac{N-2}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ by using (or carefully speaking, "interpreting") Theorem 3.1. In place of the payoffs, use $C\left(\frac{N-1}{N}\right)[j]$. Thus you have

   $$C\left(\frac{N-2}{N}\right)[j] = \frac{p\left(\frac{N-2}{N}\right)[j] C\left(\frac{N-1}{N}\right)[j+1] + \left\{1 - p\left(\frac{N-2}{N}\right)[j]\right\} C\left(\frac{N-1}{N}\right)[j]}{1 + \frac{r_f}{N}}$$

   where $C\left(\frac{N-1}{N}\right)[j]$ $(j = 0, 1, \cdots, N-1)$ are given by the previous step. $p\left(\frac{N-2}{N}\right)[j]$ $(j = 0, 1, \cdots, N-2)$ are given by Eqn. (14).

3. Repeat the above procedure until you reach $t = 0$ and obtain

$$C(0) = \frac{p(0)[0]C(1/N)[1] + \{1 - p(0)[0]\}C(1/N)[0]}{1 + \frac{r_f}{N}}.$$

Let us explore a situation which gives an easy-to-write formula. Our concern is the dependence of the hedging probability 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. So let us consider

$$h(v) = av^b \tag{15}$$

where a and b are positive constants. Then, at each period and each state, we can use the same hedging probability given by

$$p = \frac{d^{-b} - \left(1 + \frac{r_f}{N}\right)}{d^{-b} - u^{-b}} \tag{16}$$

By following Algorithm 1 described above, we have

$$C(1)[j] = \frac{\max\{0, K - a(u^j d^{N-j} V_0)^b\}}{a(u^j d^{N-j} V_0)^b}, \tag{17}$$

$$C\left(\frac{N-1}{N}\right)[j] = \frac{pC(1)[j+1] + (1-p)C(1)[j]}{1 + \frac{r_f}{N}}, \tag{18}$$

$$\begin{aligned} C\left(\frac{N-2}{N}\right)[j] &= \left(1 + \frac{r_f}{N}\right)^{-1} \left\{pC\left(\frac{N-1}{N}\right)[j+1] + (1-p)C\left(\frac{N-1}{N}\right)[j]\right\} \\ &= \left(1 + \frac{r_f}{N}\right)^{-2} \left\{p^2 C(1)[j+2] + 2p(1-p)C(1)[j+1] + (1-p)^2 C(1)[j]\right\}, \end{aligned} \tag{19}$$

$\cdots$, and finally

$$\begin{aligned} C(0) &= \left(1 + \frac{r_f}{N}\right)^{-N} \sum_{j=0}^{N} \binom{N}{j} p^j (1-p)^{N-j} C(1)[j] \\ &= \left(1 + \frac{r_f}{N}\right)^{-N} \sum_{j=0}^{N} \binom{N}{j} p^j (1-p)^{N-j} \frac{\max\{0, K - a(u^j d^{N-j} V_0)^b\}}{a(u^j d^{N-j} V_0)^b} \end{aligned} \tag{20}$$

Eqn. (20) can be easily proved by mathematical induction outlined above. Intuitively, the following statements would be helpful.

- There are $\binom{N}{j}$ paths between the start ($t = 0$) and each final state j at the maturity ($t = 1$).
- Every path must experience exactly N changes.
- Each upward change makes the payoff be multiplied by $p\left(1 + \frac{r_f}{N}\right)^{-1}$.

- Each downward change makes the payoff be multiplied by $(1-p)\left(1+\frac{r_f}{N}\right)^{-1}$.
- So the contribution of each path to the state j with the payoff $C(1)[j]$ is

$$\left(1+\frac{r_f}{N}\right)^{-N} p^j (1-p)^{N-j} C(1)[j]$$

Thus, although it seems an artificial example, we have obtained a simple closed-form pricing formula. We would like to summarize it.

Theorem 3.2 (Option-Pricing Formula (Multiple-Period Model)) *In the binomial multiple-period model described in Fig. 3, let us consider a European call option defined by Definition 3.1 written on a setok which has the value-interpretation function $h(v) = av^b$ (a, b : positive constants). We have Assumption 3.1 and Assumption 3.2 as well as the following two assumptions:*

1. *The short rate of interest is a constant $\frac{r_f}{N}$ during each period of length $1/N$.*
2. *The maturity is $T_m = 1$ (chosen as the time unit).*

Let the price of the option now ($t = 0$) and the strike value of the option be $C(0)$ and K, respectively. Then, the following pricing formula *holds.*

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

where

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

If we further assume $K > aV_0^b d^N$, which is the condition for the option to have non-zero probability for a positive payoff at the maturity, then the formula can be expressed in a more (economically) instructive way:

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

where

$$n' = \left\lceil \frac{\ln\left(\frac{K}{aV_0^b d^N}\right)}{b \ln\left(\frac{u}{d}\right)} \right\rceil.$$

Although Theorem 3.2 mentions merely about the option price at $t = 0$, Algorithm 1 gives us whole the price process at $t \in [0, 1/N, 2/N, \cdots, 1]$. It should be also noted that the multiple-period pricing formula, Eqn. (20), holds even if the transition probabilities (p_u for the upward change and $1-p_u$ for the downward change) change period by period as

far as both the probabilities are positive. Suppose that you are a great person: security[7] minister of a large country. You are happy if the setok market is stable in terms of the up-to-date values. The value-interpretation function is fixed as the form of Eqn. (15). You have made best effort to achieve better stability. Your effort may contribute to

1. the reduction of the **volatility** factor of the value-interpretation function, *i.e.* a and b,
2. the reduction of the volatility factor of the implicit value process, *i.e.* $|u-d|$, or
3. the adaptive control of the transition probability; for instance, $p_u > 1-p_u$ when $H(t)$ is lower than a certain desirable value H_0 and $p_u < 1-p_u$ when $H(t) > H_0$.

The first two may be detected and you could be proud of it if you watch the setok and the option price processes, whereas the last one cannot. **There can be an administrative strategy which stabilizes the underlying setok with no influence on the option price.**

3.3 Pricing in a Continuous-Time Model

3.3.1 Model Description

The previous subsection 3.2 has investigated the models which are discrete both in time and in values. What happens if we consider not discrete but somewhat continuous models? Specifically, we are going to study the following model.

Assumption 3.4 (Continuous-Time Model) *In Section 3, we are investigating setok* $(S, Y; V, H, n, 1)$ *under Assumption 3.1, and the European call option on it. Let* $C(t) = c(t, H(t))$ *be the price process of the option.*

As a simple continuous-time model, we further assume the followings.

- *The function* $c(t,h)$ *is a* $C^{1,2}$*-mapping.*
- *The dynamics of the (observable) up-to-date value process* H *is given by*

$$dH = \mu(t, H(t))Hdt + \sigma(t, H(t))HdW$$

  where $\mu(t, H(t))$ *and* $\sigma(t, H(t))$ *are adapted processes and* W *is a Wiener process under the objective measure.*

- *Define* $G(t) = \{H(t)\}^{-1}$ *and corresponding occurrence as* $g = 1/h$*. We sometimes regard* c *as a function of* t *and* g*. To avoid confusion, we write* $\hat{c}(t,g) = c(t, 1/g)$*, where we assume the function* $\hat{c}$ *is also a* $C^{1,2}$*-mapping.*

[7] We use the word "security" with considering three notions at the same time: (1) Information security such as confidentiality, authenticity, integrity, non-repudiation, and availability, (2) official pieces of writing, *e.g.* bonds and stocks, and (3) what gives the owner the *right* to certain property.

- *The price process of the riskless asset is described by the dynamics*

$$dB(t) = r_f B(t)dt$$

where the short rate r_f is a deterministic constant. This is a special case of Definition 3.3.

In general, the process H driven by the assumed dynamics

$$dH = \mu H dt + \sigma H dW \tag{21}$$

is said to be the *geometric Brownian motion with drift* if μ and σ are deterministic constants. In this case, the absolute change in H over any finite time interval is *log-normally* distributed. The geometric Brownian motion with drift appear in a lot of random variables in the real society. We estimate μ and σ by using the observed market data; they are *exogenously* given parameters.

In fact, Assumption 3.4 is mathematically quite similar to the well-known Black-Scholes model[14] for pricing options on stocks. However, it is worth noting that Assumption 3.1 says the setok is neither online nor offline divisible. In addition, we cannot go short for it. These properties are different from those of stocks.

3.3.2 Pricing

We wish to derive a pricing formula for the European call option purchased at $t = 0$ and matured $t = T_m$, where T_m is not necessarily equal to 1 but smaller than T. Firstly, let us define an adapted process $G(t)$ by

$$G(t) = g(t, H(t)), \tag{22}$$

where

$$g(t, h) = \frac{1}{h}. \tag{23}$$

By using Theorem 2.1 and Eqn. (23), the dynamics of this process is given by

$$\begin{aligned} dG &= \left\{ g_t + \mu H g_h + \frac{1}{2}\sigma^2 H^2 g_h h \right\} dt + \sigma H g_h dW \\ &= \left\{ 0 - \frac{\mu H}{H^2} + \frac{1}{2}\sigma^2 H^2 \frac{2}{H^3} \right\} dt - \frac{\sigma H}{H^2} dW \\ &= \left(-\frac{\mu}{H} + \frac{\sigma^2}{H} \right) dt - \frac{\sigma}{H} dW \end{aligned} \tag{24}$$

where we denote partial derivatives by subscripts:

$$\frac{\partial g}{\partial t} = g_t, \ \frac{\partial g}{\partial h} = g_h, \ \frac{\partial^2 g}{\partial h^2} = g_{hh}. \tag{25}$$

In the rest of this paper, we may use this type of notation without clearly stating it as far as the context is clear.

Secondly, let us consider a portfolio composed of one setok and M options. The portfolio is dynamically changed, over and over again. As in the discrete-time multiple-period model, let us think of any infinitesimal time interval of length dt. Each dynamics is given in the form of SDE. Let F be the monetary value (in terms of the initial investment at the beginning of the infinitesimal time interval) of this portfolio:

$$F = 1 + MC. \tag{26}$$

We sell the setok for the value-proportional price and immediately buy one setok with the up-to-date value for the fixed up-to-date price 1 at the end of the time interval. By assumption, these procedures take no time and are allowed even in the case of the infinitesimal time interval. Thus, over the time interval, the "resale and buy" brings

$$\frac{G + dG}{G} - 1 = \frac{dG}{G} \tag{27}$$

and tells us that the dynamics of F is given by

$$dF = \frac{dG}{G} + M dC \tag{28}$$

We have to be careful about the fact that **stochastic differentials are the expected value at the beginning of the time interval.** So a more instructive notation for Eqn. (28) would be

$$E_t[dF] = \frac{E_t[dG]}{G(t)} + M(t) E_t[dC], \tag{29}$$

where E_t denotes the expectation operator conditioned by the information available at time t. We apply Theorem 2.1 for dC, and insert it as well as Eqn. (24) into Eqn. (28). Then we obtain[8]

$$\begin{aligned} dF &= \left\{ M \left(c_t + \mu H c_h + \frac{\sigma^2}{2} H^2 c_{hh} \right) - \mu + \sigma^2 \right\} dt + \left(M \sigma H c_h - \sigma \right) dW \\ &= \left\{ M \left(\hat{c}_t - \mu G \hat{c}_g + \sigma^2 G \hat{c}_g + \frac{\sigma^2}{2} G^2 \hat{c}_{gg} \right) - \mu + \sigma^2 \right\} dt - \sigma \left(M G \hat{c}_g + 1 \right) dW \end{aligned} \tag{30}$$

Thanks to the divisibility of the option, by choosing

$$M = -\frac{1}{G \hat{c}_g}, \tag{31}$$

we can make the portfolio risk-free, *i.e.* force the diffusion dW-term to be zero. Note that M can change over time. This is a dynamic replication of the risk-free asset.

Since any risk-free asset must have r_f as the rate of return (recall Proposition 3.1), we have

$$M \left(\hat{c}_t - \mu G \hat{c}_g + \sigma^2 G \hat{c}_g + \frac{\sigma^2}{2} G^2 \hat{c}_{gg} \right) - \mu + \sigma^2 = r_f F. \tag{32}$$

It should be noted that $F = F(t)$ on the right-hand side of Eqn. (32). Do not make a mistake such as $F = F(t + dt)$. **We are considering a rate of return.**

[8]It is elementary to see that $c_h = -G^2 \hat{c}_g$ and $c_{hh} = 2G^3 \hat{c}_g + G^4 \hat{c}_{gg}$.

Finally, we insert Eqn. (31) and Eqn. (26) into Eqn. (32). The resultant relation must hold for any occurrence of the adapted process G. So let us use g instead of G to obtain the *partial differential equation (PDE)*

$$\frac{\sigma^2}{2} g^2 \hat{c}_{gg} + r_f (g\hat{c}_g - \hat{c}) + \hat{c}_t = 0. \tag{33}$$

We solve this PDE under the boundary condition

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\}, \tag{34}$$

which says that the option price at the maturity must be equal to the payoff at that time[9]. The following theorem gives the summary and the notational remark.

Theorem 3.3 (Boundary Value Problem for Option Pricing) *Consider the European call option defined by Definition 3.1 written on the setok under Assumption 3.4. The maturity of the option is T_m and the strike value is K. $H(t)$ is the up-to-date value process of the setok.*

Then the only pricing function of the form $C(t) = c(t, H(t))$ consistent with the no-arbitrage condition is obtained when $c(t,h) = \hat{c}(t, 1/h)$ and $\hat{c}(t,g)$ is the solution of the boundary value problem

$$\frac{\sigma^2}{2} g^2 \hat{c}_{gg} + r_f (g\hat{c}_g - \hat{c}) + \hat{c}_t = 0$$

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\}$$

in the domain $[0, T_m] \times \boldsymbol{R}_+$.

In general, it is difficult to obtain an analytical closed-form solution for the boundary value problem in Theorem 3.3. However, we do not have to be disappointed. We can use numerical approach to obtain approximate solutions. The form of the PDE considered is not really strange.

We have to mention an extremely simple case: if μ and σ are deterministic constants, a closed-form solution is easily obtained. The result is as follows.

Theorem 3.4 (Option-Pricing Formula (Continuous-Time Model)) *Let the up-to-date value process follow the geometric Brownian motion with drift, i.e. μ and σ be deterministic constants. Then Theorem 3.3 yields the* pricing formula $C(t) = c(t, H(t))$, *where*

$$c(t,h) = \frac{K}{h} N\left[d_1(t,h)\right] - \exp\left\{-r_f(T_m - t)\right\} N\left[d_2(t,h)\right]$$

where N is the cumulative distribution function for the standard normal distribution, *i.e.*

$$N[d] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{d} \exp\left(-\frac{x^2}{2}\right) dx$$

[9]This must hold for any state at the maturity.

and

$$d_1(t,h) = \frac{1}{\sigma\sqrt{T_m - t}} \left\{ \ln\left(\frac{K}{h}\right) + \left(r_f + \frac{\sigma^2}{2}\right)(T_m - t) \right\},$$

$$d_2(t,h) = d_1(t,h) - \sigma\sqrt{T_m - t}.$$

Let us see on which parameters the option price in Theorem 3.4 depends. It depends on the diffusion σ, the maturity date T_m, the short rate r_f, the up-to-date value h, and of course the strike value K. By contrast, it does not depend on the drift μ and the length of the tradability period T.

3.3.3 Analysis of the Option-Pricing Formula

In order to investigate the characteristics of the option-pricing formula, we plot the current option price $C(0)$ given by Theorem 3.4 with changing the up-to-date value $H(0) \in [80, 120]$. We denote $C(0)$ by C, in the following. We choose one year as the time unit. We interpret the short rate r_f into the intuitive (yearly) rate r of interest for the bank account by

$$r = \exp(r_f) - 1 \tag{35}$$

and we use percentage representation when we refer to r.

The basic parameter assignments are as follows.

Maturity: $T_m = 1$ [year]

Volatility: $\sigma = 0.2$

Exercise Value: $K = 100$

Short Rate: $r = 0.5$ [%]

We will show four figures. Since smaller up-to-date values mean the option holders are in better positions now, the curves are monotone decreasing in each figure.

Firstly, we investigate the effect of the maturity. The plots for $T_m = 0.5$, 1, and 2 are given in Fig. 4. If the maturity is further away from now, things would become more uncertain. The uncertainty relaxes both chance and risk; curves for larger T_m are less changing. Roughly speaking, larger T_m bring lower option prices for $H(0) < K = 100$; the currently better position of the option holder is less evident under larger uncertainty. Also roughly speaking, larger T_m bring higher option prices for $H(0) > K = 100$; the currently worse position of the option holder is also less evident under larger uncertainty.

Secondly, we investigate the effect of the volatility σ. The plots for $\sigma = 0.1$, 0.2, and 0.4 are given in Fig. 5. If the volatility is larger, things would become more uncertain. Therefore, the effect is quite similar to that of the maturity; the uncertainty relaxes both chance and risk, and curves for larger σ are less changing.

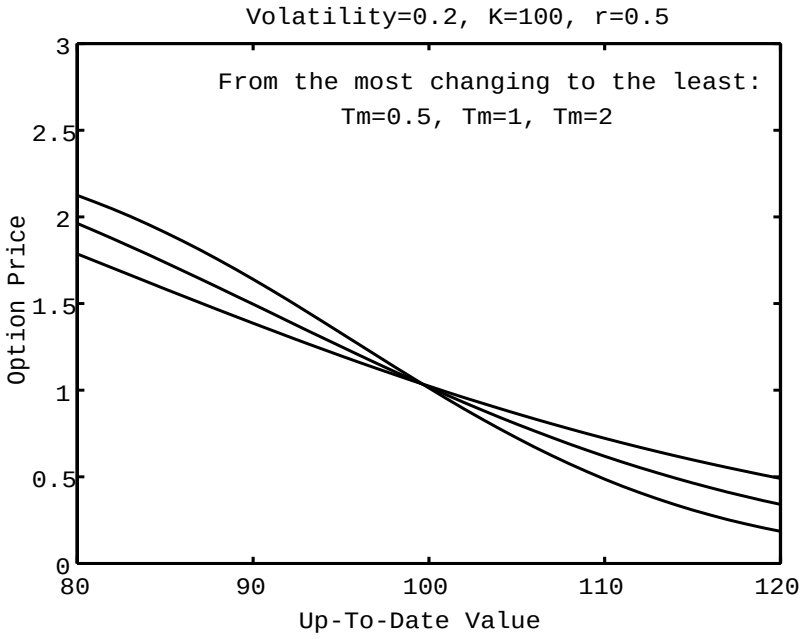

Figure 4: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the maturities $T_m = 0.5$, 1, and 2 are shown. Further maturities bring less changing curves by relaxing chances (for smaller up-to-date values) and risks (for larger up-to-date values).

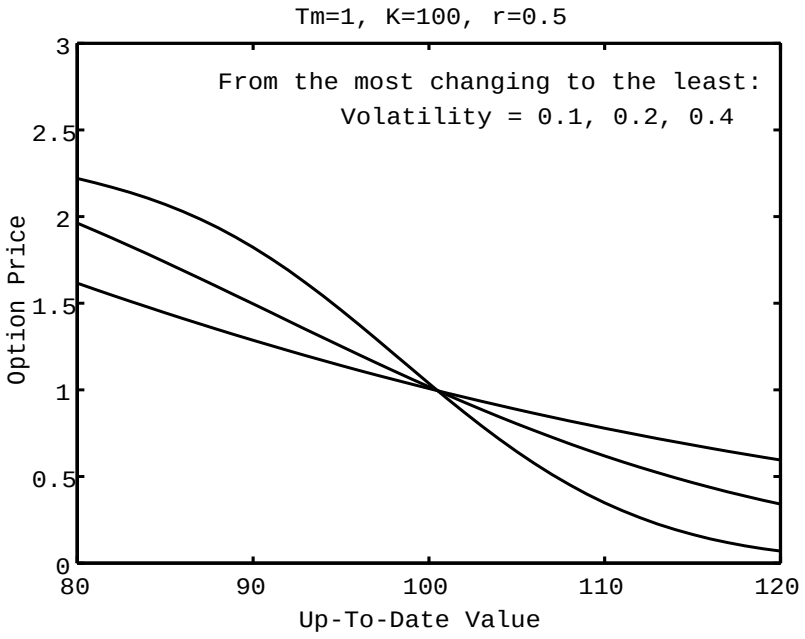

Figure 5: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the volatilities $\sigma = 0.1$, 0.2, and 0.4 are shown. Larger volatilities bring less changing curves by relaxing chances (for smaller up-to-date values) and risks (for larger up-to-date values).

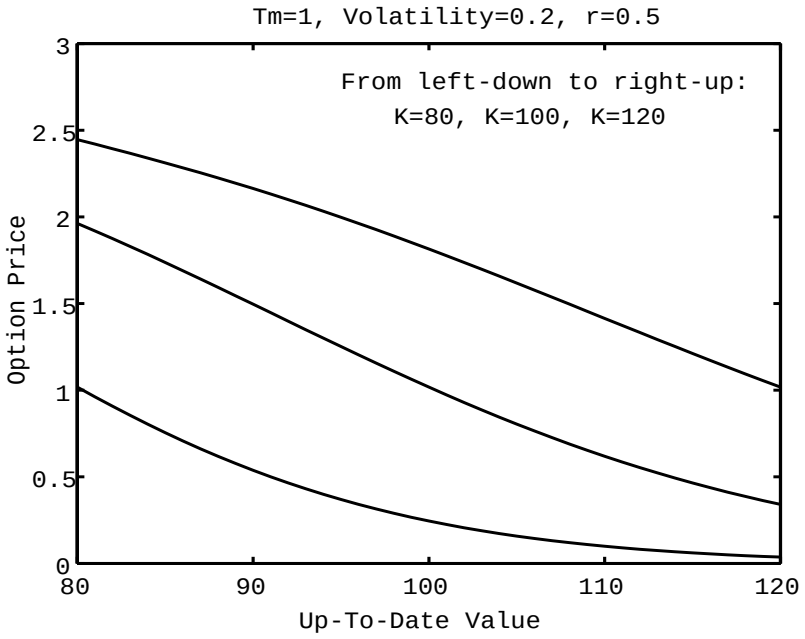

Figure 6: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the exercise values $K = 80$, 100, and 120 are shown. Higher exercise values mean currently better positions of the option holders, and hence bring higher option prices.

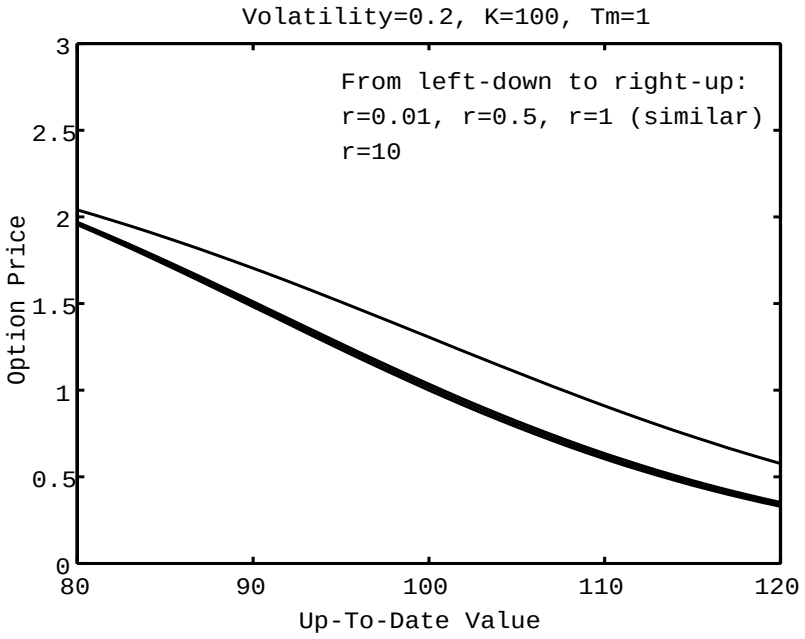

Figure 7: European call option price against up-to-date values of the setok whose price is fixed to be 1. The curves for the (yearly) short rates of interest $r = 0.01$, 0.5, 1.0 and 10.0 [%] are shown. Higher short rates make investments more profitable and give higher option prices.

Thirdly, we investigate the effect of the exercise value K. The plots for $K = 80$, 100, and 120 are given in Fig. 6. It is obvious that larger exercise values mean currently better positions of the option holder. Figure 6 represents this feature; larger exercise values bring higher option prices. It should be noted that the option price almost equals to the fixed setok price, *i.e.* $C \simeq 1 = Y(t)$, when the current position of the holder is neutral (*i.e.* when $H(0) \simeq K$).

Finally, we investigate the effect of the short rate. The plots for $r = 0.01$, 0.5, 1, and 10 [%] are given in Fig. 7. In general, higher short rates make investments more profitable[10]. Figure 7 represents this feature; larger short rates bring higher option prices. However, realistic short rates show little difference. Only the unrealistically high rate ($r = 10\%$) dominates evidently.

4 Compromise and Revocation

4.1 Observation and Implication

Suppose again that you are a great person: security minister. The setok world of your concern works mostly well but there are possibility of revocation: implicit values are sometimes compromised, and the compromise can cause a sudden and significant reduction in the corresponding up-to-date values and price. Depending on the contents, this reduction can be viewed as a revocation. You want to watch how often such a disaster *is likely to* happen. What can you do for that?

Of course, you can watch the market because an important person like you has resources as good as the object providers' and servers'. You can analyse the statistics. If the revocation frequency so far is not really high, you are probably happy. But you may still concern about the setoks which have never experienced revocation. You want to know the public opinion or public fear, in particular. You may distribute a questionnaire which includes a question: "How often do you think the setok $(S, Y; V, H, n, m)$ is likely to have revocation in value? Please specify it in percentage." This may cost a lot and the result may be too subjective. It takes time, too. The purpose of this section is to make an attempt to obtain less subjective opinion by observing the setok/option market: we expect that some parameters related with the compromise are *implied* by the market data including the option price. Thus we wish to have an option-pricing theory under a risk of compromise.

4.2 Extended Settings

The rest of this section will study a continuous-time model. As for the underlying setok, we will mostly follow Assumption 3.1. The difference is in its tradability: the tradability is assumed to be **not** strict here. Although the setok is T-tradable, T is stochastic. Let $H(0) > 0$ and $T(0) = T_0 > 0$. As long as the up-to-date value $H(t)$ is positive, T keeps the initial value T_0. However, in the case of revocation, the tradability is ruined; $T(t) = 0$

[10] Recall that the risk-free portfolio composed of the setok and the options has the same rate of return as the short rate.

for any t such that $H(t) = 0$. But the holders of the setok do not have to be completely discouraged. In place of the tradability, a refundability arises. We specify this formally.

Assumption 4.1 (Setok with Revocation) *In Section 4, a* single-valued *setok (S, Y; V, H, n, 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* **not** *online divisible.*
3. *The setok is* **not** *offline divisible*
4. **No one can go short** *for the setok.*
5. *The setok is T-tradable and the length of the tradable period is given by $T = \tau_T(t, H(t))$, where the function $\tau_T(t,h) : \boldsymbol{R}_+ \times \boldsymbol{R}_+ \to \{0, T_0\}$ is as follows.*

$$\tau_T(t,h) = \begin{cases} T_0 & \text{if } h > 0 \\ 0 & \text{if } h = 0. \end{cases}$$

   $T_0 > 0$ is a deterministic constant.

6. *The setok is T-refundable and the length of the refundable period is given by $T = \tau_R(t, H(t))$, where the function $\tau_R(t,h) : \boldsymbol{R}_+ \times \boldsymbol{R}_+ \to \{0, T_1\}$ is as follows.*

$$\tau_R(t,h) = \begin{cases} 0 & \text{if } h > 0 \\ T_1 & \text{if } h = 0. \end{cases}$$

   $T_1 > 0$ is a deterministic constant.

7. *The possession of the setok has no meaning as a project and hence, in a financial term, yields no dividends.*
8. *As long as no compromise has occurred, all the up-to-date and implicit value processes are positive and finite.*
9. *Compromise-responsive in value.*

The first property $Y(t) = 1$ in Assumption 4.1 implies that the setok is **not** compromise-responsive in price.

According to Assumption 4.1, we change the assumption on the maturity T_m of the option. In particular, we assume

$$T_m < \min\{T_0, T_1\}. \tag{36}$$

We are interested in the price process of the European call option. The difference from Section 3 is in the assumption on the underlying setok dynamics. In addition to a drift term and a diffusion term, the setok has a jump term which describes the effect of a compromise. Let us suppose that the compromise happens according to a *Poisson process*

with intensity λ. Once the Poisson jump occurs, the up-to-date value is revoked to be zero because of 9. in Assumption 4.1. Thus, instead of Assumption 3.4, we consider the model below.

Assumption 4.2 (Continuous-Time Model with Revocation) *In Section 4, we are investigating setok $(S, Y; V, H, n, 1)$ under Assumption 4.1, and the European call option on it. Let $C(t) = c(t, H(t))$ be the price process of the option.*

As an extended continuous-time model, we assume the followings.

- *The function $c(t, h)$ is a $C^{1,2}$-mapping in the domain $\boldsymbol{R}_+ \times \boldsymbol{R}_{++}$, and $c(t, 0) = 0$ for all $t \in \boldsymbol{R}_+$. $\boldsymbol{R}_{++}$ is the set of positive real numbers.*

- *The dynamics of the up-to-date value process H is given by*

$$dH = (1 - \lambda(t, H(t))dt) \{\mu(t, H(t))Hdt + \sigma(t, H(t))HdW\} + \lambda(t, H(t))dt \cdot (-H)$$

  where $\mu(t, H(t))$ and $\sigma(t, H(t))$ are adapted processes and W is a Wiener process (under the objective measure). An adapted process $\lambda(t, H(t))$ represents the intensity of the Poisson process. We regard the described revocation risk as a systematic risk (see 5.2).

- *Define $G(t) = \{H(t)\}^{-1}$ and corresponding occurrence as $g = 1/h$. We sometimes look at c as a function of t and g. To avoid confusion, we write $\hat{c}(t, g) = c(t, 1/g)$, where we assume the function $\hat{c}$ is also a $C^{1,2}$-mapping for $0 < g < \infty$.*

- *The price process of the riskless asset is described by the dynamics*

$$dB(t) = r_f B(t)dt$$

  where the short rate r_f is a deterministic constant.

4.3 Pricing

First, by using the multiplication table in Theorem 2.1, we notice that the dynamics of H is given by

$$dH = (\mu - \lambda)Hdt + \sigma HdW. \tag{37}$$

As usual, let us consider a riskless portfolio composed of one share of the setok and M options. Let F be the monetary value (in terms of the initial investment at the beginning of the infinitesimal time interval) of this portfolio. As long as no revocation happens, the dynamic strategy tells us to pay

$$F = 1 + MC \tag{38}$$

at the beginning of the infinitesimal time interval. After a revocation, we do not need to price. We want to see dF. Unfortunately, the revocation will not allow g to remain finite; $g \to +\infty$ as $h \to +0$. Therefore, without writing dG like Eqn. (24), we here consider the meaning of Eqn. (28) or equivalently and more instructively Eqn. (29). What we

are going to do is to write the expected gain conditioned by the information available at the beginning of the infinitesimal time interval. The refundability resulting from the revocation implies that the holder of the setok sells it for the fixed up-to-date price $Y(t) = 1$. So the contribution from one share of the setok to dF is

$$(1 - \lambda dt)\left\{-(\mu - \sigma^2)dt - \sigma dW\right\} + \lambda dt \cdot 1 = (\lambda - \mu + \sigma^2)dt - \sigma dW. \tag{39}$$

As for the option,

$$\begin{aligned} MdC &= M(1 - \lambda dt)\left\{\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg}\right)dt - \sigma G\hat{c}_g dW\right\} \\ &\quad + M\lambda dt \cdot (-c) \\ &= M\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} - \lambda c\right)dt - M\sigma G\hat{c}_g dW. \end{aligned} \tag{40}$$

The investigation above results in

$$\begin{aligned} dF &= \left\{M\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} - \lambda c\right) + \lambda - \mu + \sigma^2\right\}dt \\ &\quad -\sigma\left(MG\hat{c}_g + 1\right)dW. \end{aligned} \tag{41}$$

Thanks to the divisibility of the option, by choosing

$$M = -\frac{1}{G\hat{c}_g}, \tag{42}$$

we can make the portfolio risk-free. As usual, M can change over time.

Due to the no-arbitrage requirement, we have

$$\begin{aligned} M\left(\hat{c}_t - \mu G\hat{c}_g + \sigma^2 G\hat{c}_g + \frac{\sigma^2}{2}G^2\hat{c}_{gg} - \lambda c\right) + \lambda - \mu + \sigma^2 &= r_f F(t) \\ &= r_f(1 + MC). \end{aligned} \tag{43}$$

Next, we insert Eqn. (42) into Eqn. (43). The resultant relation must hold for any occurrence of the adapted process G as long as no compromise has occurred. So let us use g instead of G to obtain the following PDE

$$\frac{\sigma^2}{2}g^2\hat{c}_{gg} + (r_f - \lambda)g\hat{c}_g - (r_f + \lambda)\hat{c} + \hat{c}_t = 0. \tag{44}$$

We solve this PDE under the boundary condition

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\} \quad (0 < g < \infty). \tag{45}$$

The following theorem gives the summary and remarks.

Theorem 4.1 (Boundary Value Problem under a Revocation Risk) *Let us have Assumption 4.1 for the setok. Consider the European call option defined by Definition 3.1 written on the setok under Assumption 4.2. The maturity of the option is T_m and the strike value is K. $H(t)$ is the up-to-date value process of the setok.*

Then the only pricing function of the form $C(t) = c(t, H(t))$ consistent with the no-arbitrage condition is obtained when

$$c(t,h) = \begin{cases} \hat{c}(t, 1/h) & \text{for } h > 0 \\ 0 & \text{for } h = 0 \end{cases}$$

and $\hat{c}(t,g)$ is the solution of the boundary value problem

$$\frac{\sigma^2}{2} g^2 \hat{c}_{gg} + (r_f - \lambda) g \hat{c}_g - (r_f + \lambda)\hat{c} + \hat{c}_t = 0.$$

$$\hat{c}(T_m, g) = \max\{0, Kg - 1\}$$

in the domain $[0, T_m] \times \boldsymbol{R}_{++}$.

In general, it is difficult to obtain an analytical closed-form solution for the boundary value problem in Theorem 4.1. However, we do not have to be disappointed. We can use numerical approach to obtain approximate solutions. The form of the PDE considered is not really strange.

4.4 Inverse Estimation

Return back to the role of security minister.

Let us see on which parameters the option price obtained from Theorem 4.1 would depend. It does not depend on the drift μ, and the parameters regarding tradability/refundability periods, *i.e.* T_0 and T_1. By contrast, it would depend on the diffusion σ, the maturity date T_m, the short rate r_f, the up-to-date value h, and of course the strike value K. In addition, it would depend on λ: the risk of compromise. This suggests that the market data may give you some information on a public opinion about the risk of compromise which has not yet occurred. You want to estimate λ by using the market data observed. This is an inverse problem.

Consider the following procedure for the inverse estimation:
(Procedure 1)

1. By using recent market data excluding option prices, estimate the short rate r_f and the volatility σ of the up-to-date value.
2. Guess the risk of compromise λ.
3. Solve the boundary value problem in Theorem 4.1.
4. Compare the result with recent option price data. If there are a lot of options (on the same setok) with different maturities and/or different exercise values, use them as well. Compute the error of guess, *e.g.* in the least-square's sense. Some weighting may be helpful.

5. If the error is small enough, quit.

6. If you do not satisfied with the error, change the guess and repeat. Typically, if the computed prices are too high, increase the guess. This is an intuitive observation from the fact that a revocation makes the option worthless. Once compromised, one cannot expect any yield from exercising the option and immediately selling (refunding) the setok; that would be just a waste of time.

The boundary value problem may take time to be solved. Procedure 1 in total may be too heavy. But you may be more confident and feel more speedy than in the case of questionnaire.

What you want to do may be just to see whether λ exceeds a certain value, say, λ_0. The intuitive observation tells us that the option price would be lower for larger λ. There is a possibility that the following more practical procedure without repeat will work well. **(Procedure 2)**

1. By using recent market data excluding option prices, estimate the short rate r_f and the volatility σ of the up-to-date value.

2. Set $\lambda = \lambda_0$.

3. Solve the boundary value problem in Theorem 4.1.

4. Compare the result with the current option price data. If there are a lot of options (on the same setok) with different maturities and/or different exercise values, use them as well.

5. By using a tool for statistical test, examine whether you can say the computed prices are higher than the observed prices with non-negligible probability.

6. If the answer is Yes, think of it as an alarm. It might be time for you to demonstrate your administrative talent as a minister.

4.5 Effect of Derivatives

This framework is virtual in a sense that there has not been established such a setok world. If we really want to have an option market on the setoks, **we must be careful** about the possible change caused by the introduction of derivatives. Even in the existing finance, the effects of derivatives are on-going theoretical and empirical research topics. There are different opinions.

There is a common public and regulatory perception that derivative securities may increase volatility and can have a destabilizing effect on the underlying market. Basically, they are afraid that poorly informed speculators could have a destabilizing effect. Academic reports on this side are few. A theoretical example is [23] and an empirical example is [24].

Among academic people, however, the opposite opinion has been dominating so far: if derivatives promote information dissemination and collection, introduction of them would reduce volatility. The majority of studies have been in this direction. Examples of theoretical approaches include [25]–[28]. Empirical supports include [29]–[32]. There

are also empirical studies which show volatility decreases when the derivatives get more popular in trading quantity [33], [34]. If this is the case for setoks as well, we are happy to introduce derivatives.

5 Related Work

5.1 Foreign Derivatives and International Issues

The setok market may seem similar to the foreign exchange market; when we consider tradable single-valued setoks in particular, the ratio of the price to the value can have similar properties to those of foreign exchange rates. The theories of currency and foreign derivatives [35], [36] use different short rates in different countries, which is the major issue of the theory. Foreign currencies are regarded as tradable and divisible assets. This assumption makes the theory easier.

By contrast, our setok framework has been domestic so far; the key point is not in how to deal with the sort rate(s) but in how to model the tradability, refundability, and divisibility. Of course, international settings would be very interesting future work. If we assumed that several different virtual currencies are available over the network, the resultant theory would be more interesting: virtually international economy.

As for international issues, there are empirical studies which show that there are common features as well as different features in derivative statistics and questionnaire results among different countries [37]. Common features include

- Major participants in the option market are large firms.
- The highest motivation comes from hedging purposes rather than from speculating and arbitrage.
- The hedging activities are mainly aimed at hedging anticipated transactions within a year.

Different features include

- The highest concern is in the lack of information in some countries, but volatilities in others.
- How popular derivatives are.
- How popular currency derivatives are.

The study of the derivative effect in the setok framework would, if it starts, have to consider differences over countries and regions. Note that even regarding conventional financial derivatives, recently mandated disclosures have just enabled us to obtain a large number of samples to investigate firms' usage of derivatives [38].

5.2 Jump Processes

In the continuous-time model, we derived the PDEs for option pricing based on the no-arbitrage requirement:

- Any risk-free asset must have r_f as the rate of return (recall Proposition 3.1).

As far as Section 3, there is nothing to be appended here. However, the model with revocation in Section 4 needs more words here. In particular, about an assumption which is implied by Eqn. (43); in financial words, Eqn. (43) implicitly assumes that the revocation is a *systematic risk*. We mentioned it in Assumption 4.2 but have placed no discussion on it so far.

A related issue is found in the option-pricing theory which allows the underlying stock to have jumps in its price process [16], [18], [39], [40] [11]. They resorted to the conventional CAPM (Capital Asset Pricing Model) [42] by assuming that jump processes describe nonsystematic or idiosyncratic risks, which implies that risks such as firms' defaults have a too wide variety of backgrounds with no good reason to be pre-distributed to appear in a global risk premium. This is an extreme assumption and there are a lot of arguments about the systematic/nonsystematic jump processes [43]–[46]. In fact, jumps observed in stock prices are reported to be systematic across the market portfolio [47], and this phenomenon is more significant in the foreign exchange market than in the stock market [48]. The feature of the foreign exchange and currency option markets can be partly understood by the effect of news arrival [49], [50] and changes in monetary policies [51]. The mixture of idiosyncratic and systematic jumps are studied in [52], [53]. The empirical study on the jump-diffusion process of interest rates has not matured due to the difficulty of likelihood estimation [54], [55]. There are a lot of arguments about CAPM as well [56]–[58] [12].

We have used Eqn. (43), which is based on the systematic case. Heuristically speaking, the more similarly[13] network people or entities look at the revocation risk, the better model our choice of Eqn. (43) would give. In other words, we *hope* that related information is distributed more fairly with less hesitation, and revocation risks shall be more *open* than conventional default risks. This is also an assumption, and we could have neither empirical supports nor objections at present; the setok world has not been established yet. What we can say now is based on a technological insight: our choice could go well with the recent trend in the public-key infrastructure toward a single-directory system [59], [60].

6 Concluding Remarks

Toward financial risk management in an open network, we have made an abstraction of uncertain digital objects and defined the security token, which is abbreviated into a word coinage *setok*. Each setok has its price, values, and timestamp on it as well as the

[11] In early days, a study using a sample of NYSE listed common stocks reported that jumps in common stock returns leads relatively small deviations from the Black-Scholes formula [41], which suggests that the bias-elimination by [40] may be insignificant.

[12] These are nothing but examples; there are really a vast number of studies on utility functions and the CAPM.

[13] Microscopically, this corresponds to a strong positive correlation.

main contents. The model fits a hierarchical entity structure caused by network security requirements.

A number of properties of the setok were defined. They include value response to compromise, price response to compromise, refundability, tradability, online divisibility, and offline divisibility. Some of them were really used in the subsequent studies on setok derivatives, whereas the others were not. This is an on-going framework.

The derivative investigated is a simple European call option written on the up-to-date value of a setok. In continuous-time as well as discrete-time models, we have derived several option-pricing formulae. These formulae do not require any divisibility of the underlying setok. The basic features of the option price were examined numerically. An intuitive interpretation of the results was given as well.

In search of applications, an inverse estimation of the compromise probability was studied. The result suggests that we may be able to estimate the public opinion about the probability. We say *public* opinion because our financial approach is valid for the economic *equilibrium*. This opinion is expected to be less subjective than a naive questionnaire.

References

[1] Bruce Schneier. *Applied Cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc., 2nd edition, 1996.

[2] 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, pp. 325–350, 1996. Springer-Verlag.

[3] D. J. Essin. "Patterns of trust and policy". In *Proc. of New Security Paradigms Workshop '97*, pp. 38–47, September 1997.

[4] A. Abdul-Rahman and S. Hailes. "A distributed trust model". In *Proc. of New Security Paradigms Workshop '97*, pp. 48–60, September 1997.

[5] M. K. Reiter and S. G. Stubblebine. "Resilient authentication using path independence". *IEEE Trans. Comput.*, Vol. 47, No. 12, pp. 1351–1362, December 1998.

[6] 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, May 1999.

[7] 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, pp. 93–112, January 2000. Springer-Verlag.

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

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

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

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

[12] J. C. Davis. "Protecting intellectual property in cyberspace". *IEEE Technology and Society Magazine*, Vol. 17, No. 2, pp. 12–25, 1998.

[13] S. Katzenbeisser and F. Petitcolas (eds). *Information Hiding Techniques for Steganography and Digital Watermarking.* Artech House Publishers, Boston, London, 2000.

[14] F. Black and M. Scholes. "The pricing of options and corporate liabilities". *Journal of Political Economy*, Vol. 81, pp. 637–654, 1973.

[15] T. Eng and T. Okamoto. "Single-term divisible electronic coins". In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pp. 306–319, 1995. Springer-Verlag. Lecture Notes in Computer Science 950.

[16] A. G. Malliaris and W. A. Brock. *Stochastic Methods in Economics and Finance*, Vol. 17 of *Advanced Textbooks in Economics.* Springer: North-Holland, Amsterdam, 1982.

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

[18] Robert C. Merton. *Continuous-Time Finance (Revised Edition).* Blackwell Publishers, Cambridge: MA, 1992.

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

[20] Lenos Trigeorgis. *Real Options: Managerial Flexibility and Strategy in Resource Allocation.* MIT Press, Cambridge, 1996.

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

[22] J. C. Hull. *Options, Futures, and Other Derivatives.* Prentice-Hall, Upper Saddle River, London, 4th edition, 2000.

[23] J. C. Stein. "Informational externalities and welfare-reducing speculation". *Journal of Political Economy*, Vol. 95, No. 6, pp. 1123–1145, December 1987.

[24] L. Harris. "S & P 500 Cash Stock Price Volatilities". *The Journal of Finance*, Vol. 44, No. 5, pp. 1155–1176, December 1989.

[25] J.-P. Danthine. "Information, Futures Prices, and Stabilizing Speculation". *Journal of Economic Theory*, Vol. 17, pp. 79–98, 1978.

[26] S. J. Grossman. "An analysis of the implications for stock and futures price volatility of program trading and dynamic hedging strategies". *Journal of Business*, Vol. 61, pp. 275–298, 1988.

[27] J. Detemple and L. Selden. "A general equilibrium analysis of option and stock market interactions". *International Economic Review*, Vol. 32, pp. 279–304, 1991.

[28] H. Henry Cao. "Information acquisition and price behavior in a rational expectations equilibrium". *The Review of Financial Studies*, Vol. 12, No. 1, pp. 131–163, 1999.

[29] F. R. Edwards. "Futures Trading and Cash Market Volatility: Stock Index and Interest Rate Futures". *Journal of Futures Markets*, Vol. 8, pp. 421–440, 1988.

[30] D. J. Skinner. "Options Markets and Stock Return Volatility". *Journal of Financial Economics*, Vol. 23, pp. 61–78, 1989.

[31] J. Conrad. "The Price Effect of Option Introduction". *The Journal of Finance*, Vol. 44, No. 2, pp. 487–498, June 1989.

[32] R. Kumar, A. Sarin, and K. Shastri. "The Impact of Options Trading on the Market Quality of the Underlying Security: An Empirical Analysis". *The Journal of Finance*, Vol. 53, pp. 717–732, 1998.

[33] H. Bessembinder and P. J. Seguin. "Futures-Trading Activity and Stock Price Volatility". *The Journal of Finance*, Vol. 47, No. 5, pp. 2015–2034, December 1992.

[34] H. Bessembinder and P. J. Seguin. "Price Volatility, Trading Volume, and Market Depth: Evidence from Futures Markets". *Journal of Financial and Quantititative Analysis*, Vol. 28, No. 1, pp. 21–39, March 1993.

[35] G. S. Lucas. "Interest rates and currency prices in a two-country world". *Journal of Monetary Economics*, Vol. 10, pp. 335–360, 1982.

[36] G. S. Bakshi and Z. Chen. "Equilibrium valuation of foreign exchange claims". *Journal of Finance*, Vol. 52, pp. 799–826, June 1997.

[37] Per Alkebäck and Niclas Hagelin. "Derivative Usage by Nonfinancial Firms in Sweden with an International Comparison". *Journal of International Financial Management and Accounting*, Vol. 10, No. 2, pp. 105–120, 1999.

[38] Stephen R. Goldberg, Joseph H. Godwin, Myung-Sun Kim, and Charles A. Tritschler. "On the Determinants of Corporate Usage of Financial Derivatives". *Journal of International Financial Management and Accounting*, Vol. 9, No. 2, pp. 132–166, 1998.

[39] R. C. Merton. "On the Pricing of Corporate Debt: The Risk Structure of Interest Rates". *The Journal of Finance*, Vol. 29, pp. 449–470, May 1974.

[40] R. C. Merton. "Option Pricing When Underlying Stock Returns are Discontinuous". *Journal of Financial Economics*, Vol. 3, pp. 125–144, 1976.

[41] Clifford A. Ball and Walter N. Torous. "On Jumps in Common Stock Prices and Their Impact on Call Option Pricing". *The Journal of Finance*, Vol. 40, No. 1, pp. 831–842, March 1985.

[42] William F. Sharpe. "Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk". *The Journal of Finance*, Vol. 19, No. 3, pp. 425–442, September 1964.

[43] Chang Mo Ahn and Howard E. Thompson. "Jump-Diffusion Processes and the Term Structure of Interest Rates". *The Journal of Finance*, Vol. 43, No. 1, pp. 155–174, March 1988.

[44] Vasanttilak Naik and Moon Lee. "General equilibrium pricing of options on the market portfolio with discontinuous retuens". *Review of Financial Studies*, Vol. 3, No. 4, pp. 493–521, 1990.

[45] Chang Mo Ahn. "Option pricing when jump risc is systematic". Technical report, Michigan State University, 1991.

[46] David B. Colwell and Robert J. Elliott. "Discontinuous asset prices and non-attainable contingent claims". *Mathematical Finance*, Vol. 3, No. 3, pp. 295–308, July 1993.

[47] Robert A. Jarrow and Eric R. Rosenfeld. "Jump risks and the intertemporal capital asset pricing model". *Journal of Business*, Vol. 57, No. 3, pp. 337–351, July 1984.

[48] P. Jorion. "On jump processes in the foreign exchange and stock markets". *Review of Financial Studies*, Vol. 1, No. 4, pp. 427–445, 1988.

[49] M. Mussa. "Empirical regularities in the behavior of exchange rates and theories of the foreign exchange market". *Carnegie-Rocbester Conference on Public Policy*, Vol. 11, pp. 9–57, 1979.

[50] Jacob A. Frenkel. "Flexible Exchange Rates, Prices, and the Role of "News": Lessons from the 1970s". *Journal of Political Economy*, Vol. 89, No. 4, pp. 665–705, August 1981.

[51] Robert P. Flood and Robert J. Hodrick. "Asset Price Volatility, Bubbles, and Process Switching". *The Journal of Finance*, Vol. 41, No. 4, pp. 831–842, September 1986.

[52] Kaushik I. Amin and Victor K. Ng. "Option valuation with systematic stochastic volatility". *The Journal of Finance*, Vol. 48, No. 3, pp. 881–910, July 1993.

[53] Kaushik I. Amin. "Jump diffusion option valuation in discrete time". *The Journal of Finance*, Vol. 48, No. 5, pp. 1833–1863, December 1993.

[54] N. D. Pearson and T. S. Sun. "Exploiting the Conditional Density in Estimating the Term Structure: An Application to the Cox, Ingersoll, and Ross Model". *The Journal of Finance*, Vol. 49, No. 4, pp. 1279–1304, 1994.

[55] Bing-Huei Lin and Shih-Kuo Yeh. "Jump-Diffusion Interest Rate Process: An Empirical Examination". *Journal of Business Finance & Accounting*, Vol. 26, pp. 967–995, 1999.

[56] Ravi Jagannathan and Zhenyu Wang. "The Conditional CAPM and the Cross-Sections of Expected Returns". *The Journal of Finance*, Vol. 51, No. 1, pp. 3–53, March 1996.

[57] Eugene F. Fama and Kenneth R. French. "Multifactor Explanations of Asset Pricing Anomalies". *The Journal of Finance*, Vol. 51, No. 1, pp. 55–84, March 1996.

[58] Eugene F. Fama and Kenneth R. French. "The CAPM is Wanted, Dead or Alive". *The Journal of Finance*, Vol. 51, No. 5, pp. 1947–1958, December 1996.

[59] A. Buldas, P. Laud, and H. Lipmaa. "Accountable certificate management using undeniable attestations". In *Proc. of 7th ACM Conference on Computer and Communication Security*, pp. 9–18, Athens, Greece, November 2000.

[60] I. Gassko, P. S. Gemmell, and P. MacKenzie. "Efficient and fresh certification". 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, pp. 342–353, January 2000. Springer-Verlag.