A Derivative of Digital Objects and Estimation of Default Risks in Electronic Commerce

Kanta Matsuura

Institute of Industrial Science, University of Tokyo,
Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, Japan
kanta@iis.u-tokyo.ac.jp

Abstract. In electronic commerce, traded digital objects are likely associated with several numerical values as well as their prices. These values may change unpredictably over time and bring risks both to the providers and to the consumers of the application. One possible strategy for hedging the risks is to introduce derivatives regarding the uncertain values. This paper shows a theoretical pricing equation of the derivatives when the underlying digital objects have systematic default or revocation risks. We can make use of this pricing to estimate the risks.

1 Introduction

With the help of applied cryptography, we are going to trade more and more digital objects over an open network. Since digital objects can keep their original bit strings virtually forever, one may expect that there would be no risk of change. This is, unfortunately, not always the case. Digital objects can have not only prices but also other important numerical values. For example, digital certificates may have confidence values or trust metrics [1]. Access-grant tickets may have priority numbers or QoS (Quality-of-Service) values [2] reserved. Digitally-watermarked images [3] may have innocence values about their origins in terms of copyright protection. Any product may be associated with some insurance contracts [4]. Reward points may be attached. Those additional values and their effectiveness may change unpredictably over time and cause risks. At the worst case, the values get into defaults (*e.g.* the corresponding certificate is revoked) and the holder may have a large financial damage.

A popular way for hedging such stochastic risks is to introduce derivatives or options written on underlying assets, typically regarding their prices. In financial theory, encouraged by the seminal paper by Black and Scholes [5], option-pricing theories have been developed a lot. Most of them use assumptions including *divisibility* of the underlying assets, which is *not trivial* in the case of the digital objects. Thus we are motivated to study option pricing with models and assumptions suitable for digital objects. The rest of this paper consists of modeling (Sect. 2), pricing (Sect. 3), discussion including an application (Sect. 4), and conclusions (Sect. 5).

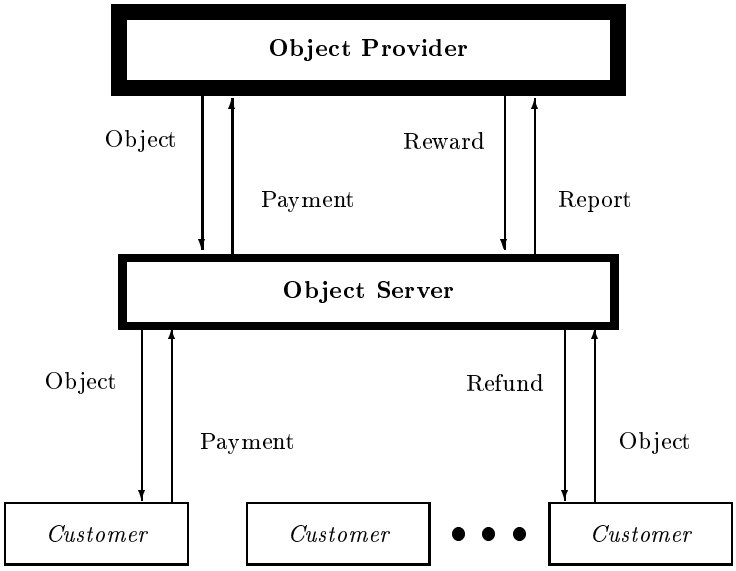

Fig. 1. A network commerce architecture where boxes with wider lines indicate that the entities inside are more trusted.

2 Objects with Default/Revocation Risks

Our model is based on an architecture illustrated in Fig. 1.

(Object Provider) Copyright management and related technical maintenance are difficult and non-trivial tasks. So are management and maintenance of network-security infrastructure (*e.g.* public-key infrastructure). These tasks may require sufficient trustworthiness and reliability. We need specialized entities. They 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.

(Object Server) Selling digital objects to untrusted customers through poor communication channels is difficult task, too. We need specialized entities.

(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.

In a network life, we would want to pay for digital objects in electronic cash. Such digital payment systems could be more efficient if the monetary value of each coin is less granular [6]. Therefore, if we want to allow as wide variety of electronic cash systems as possible, highly discrete (*i.e.* very sparse) prices would be helpful. So we firstly assume an object whose price is fixed. For notational simplicity, we assign this fixed price as the unit of network currency. Also for simplicity, we assume each share of the object has a single value. This value is

represented by a stochastic random variable $H(t)$. We assume that its dynamics is given by

$$dH = \mu(t, H(t))Hdt + \sigma(t, H(t))HdW \tag{1}$$

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

We assume a value-proportional tradability; the holder of a share of the object can sell it at a *value-proportional price* S_p defined by

$$S_p(t) = \frac{\bar{V}}{H(t)} \tag{2}$$

whenever he wishes as long as no default occurs. $\bar{V}$ is the nominal value of the share, which is equal to $H(t_0)$ where t_0 is the time the share is issued.

The default/revocation is assumed to happen according to a Poisson process with intensity λ. Once the Poisson event occurs, the value-proportional tradability is ruined but the holder can refund his share for the original unit price. Different from the conventional financial market, we do **not** assume the divisibility of the object. We do **not** assume that we can go short for it, either. Also different from the conventional financial market, we assume that the Poisson process represents a systematic risk which can fully appear in the risk premium. As for other issues, we assume a typical liquid and arbitrage-free market [7].

The derivative we study here is a European call option written not on the price but on the value as follows. We assign the issuing time of the option as the time origin (t=0) for notational convenience.

Definition 1 (A European Call). *A European call option on the object is a derivative which provides a* right *to buy one share of the object with a reserved value K at a particular time T_m 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*, and T_m is called the* maturity*.*

Let $C(t) = c(t, H(t))$ be the price process of the call option. As a continuous-time model, we place the following mathematical assumptions.

- 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 and $\boldsymbol{R}_+$ is the set of non-negative real numbers.
- The price process of the riskless asset is described by $dB(t) = r_f B(t)dt$, where the short rate r_f is a deterministic constant.

3 Pricing

By establishing a riskless portfolio composed of one share of the digital object and adjusted amount of options, we can reach the following pricing theorem. Due to the space limitation, the full proof [8] is not given here.

Theorem 1 (Boundary Value Problem for Pricing). *The only pricing function of the form* $C(t) = c(t, H(t))$ *is obtained when*

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

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

4 Discussion

4.1 Jump Processes

We derived Theorem 1 by using a systematic risk assumption. This is different from the conventional finance [9]. The conventional nonsystematic-risk assumption is an extreme assumption and there have been a lot of arguments about it [11]. In fact, jumps observed in stock prices are reported to be systematic across the market portfolio [12]. Heuristically speaking, the more similarly network entities look at the default/revocation risk, the better model our choice would give. Our choice could go better with the recent trend in the public-key infrastructure toward a single-directory system [13], [14].

4.2 Application

According to Theorem 1, the option price depends on σ, T_m, r_f, h, K, and the risk of default/revocation λ. This suggests that the market data (C, σ, T_m, r_f, h, K) may help us with an indirect measurement of the risk λ. This needs an inverse estimation, which may be too heavy. However, if what you want to do is just to see whether λ exceeds a certain value, say, λ_0, then you may be able to use a more practical strategy. That is, in the region where C is locally monotone-increasing/decreasing with respect to λ, the following procedure without repeat is worth a try.

1. By using recent market data, estimate the short rate r_f and the volatility σ.
2. Set $\lambda = \lambda_0$.
3. Solve the boundary value problem in Theorem 1.
4. Compare the result with the current option price data.
5. By using a tool for statistical test, examine whether you can say the computed price is higher(monotone-decreasing case)/lower(monotone-increasing case) than the observed price with sufficient probability.
6. If the answer is Yes, think of it as an alarm.

5 Concluding Remarks

We described an E-commerce architecture and a simple model of digital objects; each object has an abstracted value as well as a fixed price. The value can change stochastically and can be ruined at the worst case. The object is not divisible and we cannot go short for it. A European call option written not on the price but on the value was introduced. A PDE for pricing the option was derived. In the discussion, applications of the pricing were studied: to estimate the probability of revocation and to detect an alarm of high probability.

References

1. Reiter, M. K., Stubblebine, S. G.: Resilient Authentication Using Path Independence. IEEE Trans. Comput. **47** (1998) 1351–1362
2. Xiao, X., Ni, L. M.: Internet QoS: A Big Picture. IEEE Network. **13** (1999) 8–18
3. Katzenbeisser, S., Petitcolas, F. (eds.): Information Hiding Techniques for Steganography and Digital Watermarking. Artech House Publishers, Boston London (2000)
4. Reiter, M. K., Stubblebine, S. G.: Authentication Metric Analysis and Design. ACM Trans. Info. & Sys. Security **2** (1999) 138–158
5. Black, F., Scholes, M.: The Pricing of Options and Corporate Liabilities. J. Political Econ. **81** (1973) 637–654
6. Eng, T., Okamoto, T.: Single-Term Divisible Electronic Coins. In: De Santis, Alfredo (ed.): Advances in Cryptology — EUROCRYPT'94. Lecture Notes in Computer Science, Vol. 950. Springer-Verlag, Berlin Heidelberg New York (1995) 306–319
7. Björk, T.: Arbitrage Theory in Continuous Time. Oxford University Press, New York (1998)
8. Matsuura, K.: Security Tokens and Their Derivatives. Technical Reports, Centre for Communication Systems Research, University of Cambridge (2001) `http://www.ccsr.cam.ac.uk/techreports/tr29/index.html`
9. Merton, R. C.: Option Pricing When Underlying Stock Returns are Discontinuous. J. Financial Econ. **3** (1976) 125–144
10. Sharpe, W. F.: Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk. J. Finance **19** (1964) 425–442
11. Colwell, D. B., Elliott, R. J.: Discontinuous Asset Prices and Non-Attainable Contingent Claims. Math. Finance **3** (1993) 295–308
12. Jarrow, R. A., Rosenfeld, E. R.: Jump Risks and the Intertemporal Capital Asset Pricing Model. J. Business **57** (1984) 337–351
13. Buldas, A., Laud, P., Lipmaa, H.: Accountable Certificate Management Using Undeniable Attestations. In: Proc. 7th ACM Conf. on Comp. & Comm. Security, Athens (2000) 9–18
14. Gassko, I., Gemmell, P. S., MacKenzie, P.: Efficient and Fresh Certification. In: Imai, H., Zheng, Y. (eds.): Public Key Cryptography — PKC 2000. Lecture Notes in Computer Science, Vol. 1751. Springer-Verlag, Berlin Heidelberg New York (2000) 342–353